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

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

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
• 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.	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, 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.	In addition to Level 2 … • 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.	In addition to Level 3 … • 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.

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 (SREMPTAPS) 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

List of Figures

List of Tables

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 *EMP Protection and Restoration Guidelines for Equipment and Facilities* 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 *EMP Protection Guidelines for Equipment, Facilities, and Data Centers, Version 6.0, 11 May 2015*.
11/14/2018	2.0	Changed title to *Electromagnetic Pulse (EMP) Protection and Resilience Guidelines for Critical Infrastructure and Equipment*. 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 *Executive Overview* and *Acknowledgments and Authors* 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.

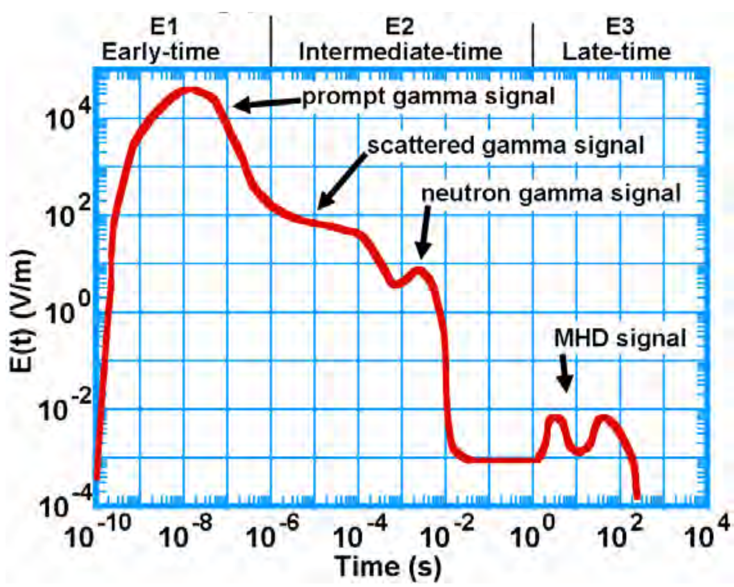


Figure 1. Generic HEMP waveform (ref. Meta-R-324)

The E2 (intermediate-time) HEMP component, between 1 μs 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 lighting at higher frequencies. Therefore, E2 is not as significant a risk as E1 HEMP, SREMP, and IEMI and so will only be briefly discussed.

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.

Time waveform:

$$E_1(t) = \begin{cases} 0 & t \le 0 \\ E_{01}k_1\left(e^{-b_1 t} - e^{-a_1 t}\right) & t > 0 \end{cases}$$

$$E_{01} = 50{,}000\ \mathrm{V/m}$$

$$k_1 = \left(\frac{a_1}{a_1 - b_1}\right)\left(\frac{a_1}{b_1}\right)^{\left(\frac{b_1}{a_1 - b_1}\right)} = 1.3$$

$$a_1 = 6\times10^{8}\ \mathrm{s}^{-1}$$

$$b_1 = 4\times10^{7}\ \mathrm{s}^{-1}$$

IEC E1 HEMP Waveform Properties

Characteristic	Value
Waveform peak	$E_{peak} = 50{,}000\ \mathrm{V/m}$
Spectrum peak	$E_{low\ freq} = 0.00152\ \mathrm{V/m/Hz}$
Waveform peak power	$P_{peak} = 6.64\times10^{6}\ \mathrm{W/m^2}$
Spectrum peak power	$P_{low\ freq} = 6.11\times10^{-9}\ \mathrm{W/m^2/Hz}$
Total energy	$W_{total} = 0.115\ \mathrm{J/m^2}$
Time of peak	$t_{peak} = 4.84\ \mathrm{ns}$
Rise time, 10% to 90% of peak	$t_{10-90} = 2.47\ \mathrm{ns}$
Pulse width, full width at half maximum	FWHM = 23.0 ns
Pulse width, total energy over peak power	$W_{total}/P_{peak} = 17.3\ \mathrm{ns}$
Spectrum width, total energy over peak spectrum power	$W_{total}/P_{low\ freq} = 18.8\ \mathrm{MHz}$

Spectrum:

$$E_1(\omega) = \int_{-\infty}^{+\infty} E_1(t)e^{-j\omega t}dt = E_{01}k_1\frac{a_1 - b_1}{(a_1 + j\omega)(b_1 + j\omega)}$$

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*].

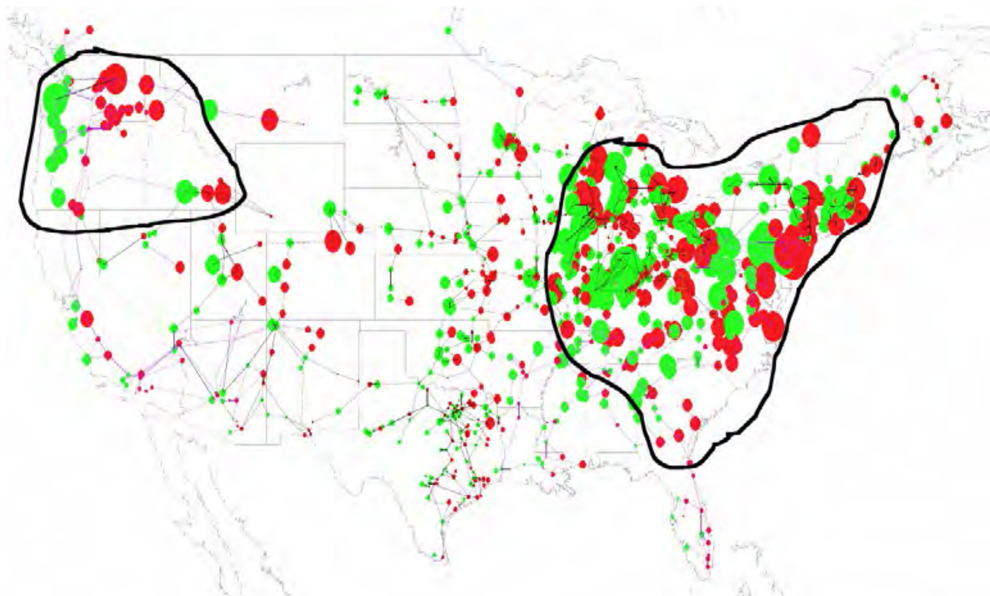


Figure 3. 100 Year geomagnetic storm – 50 degree GMD scenario (ref. Fig. 3-25)

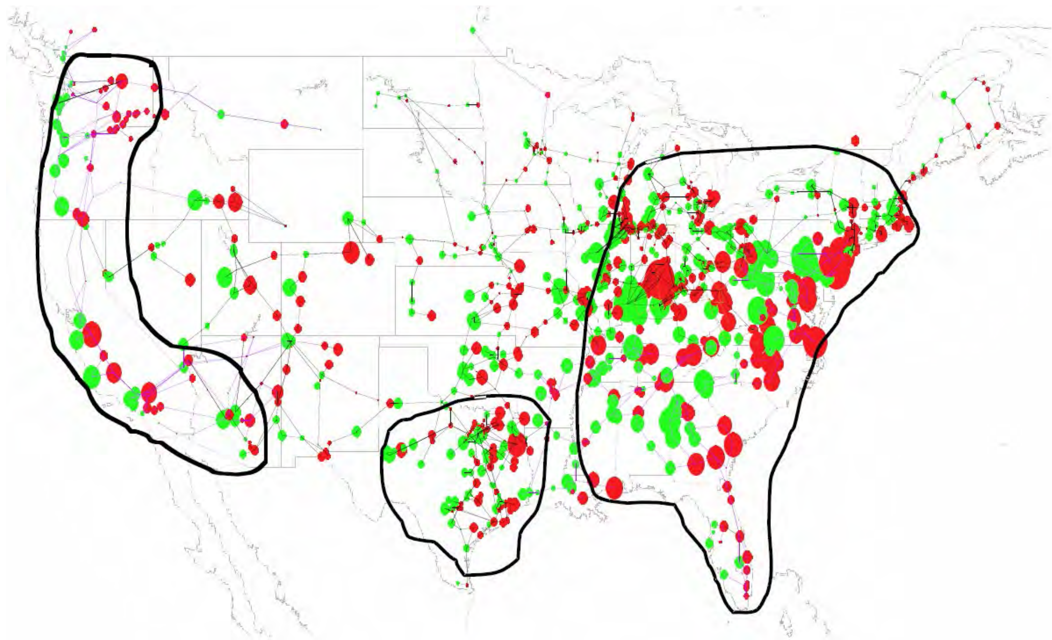


Figure 4. 100 Year geomagnetic storm – 45 degree GMD scenario (ref. Fig. 3-26)

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).

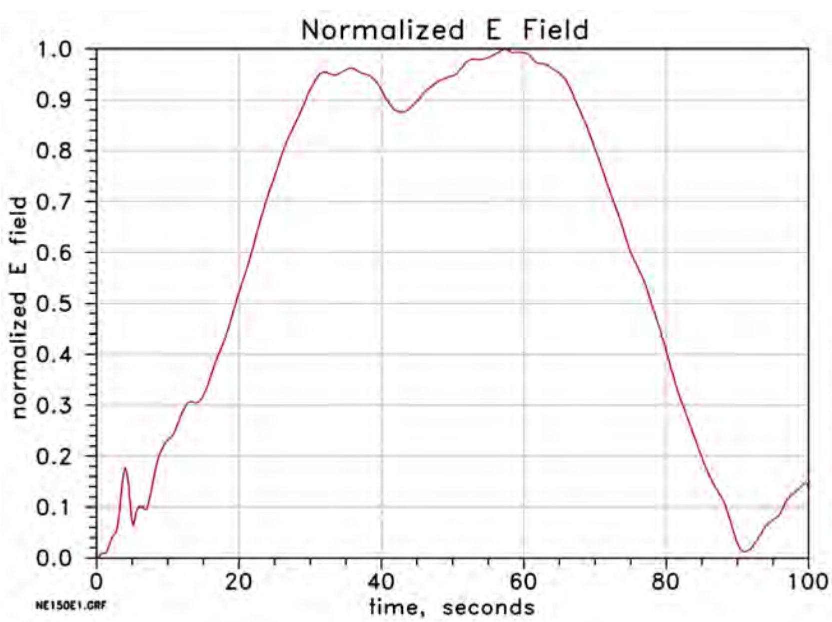


Figure 5. Normalized E3 Heave E field waveform from the 150 km burst height scenario

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).

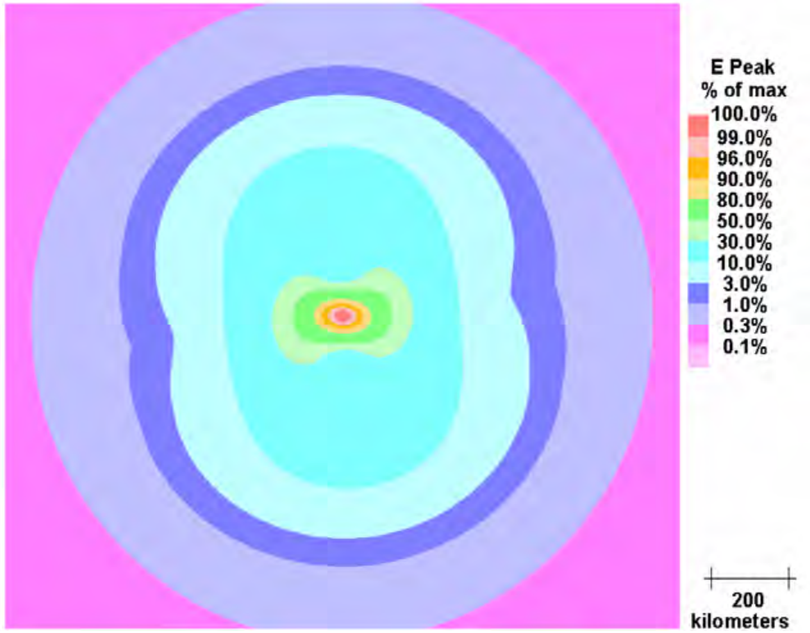


Figure 6. Normalized E peak contour pattern from the 150 km burst case

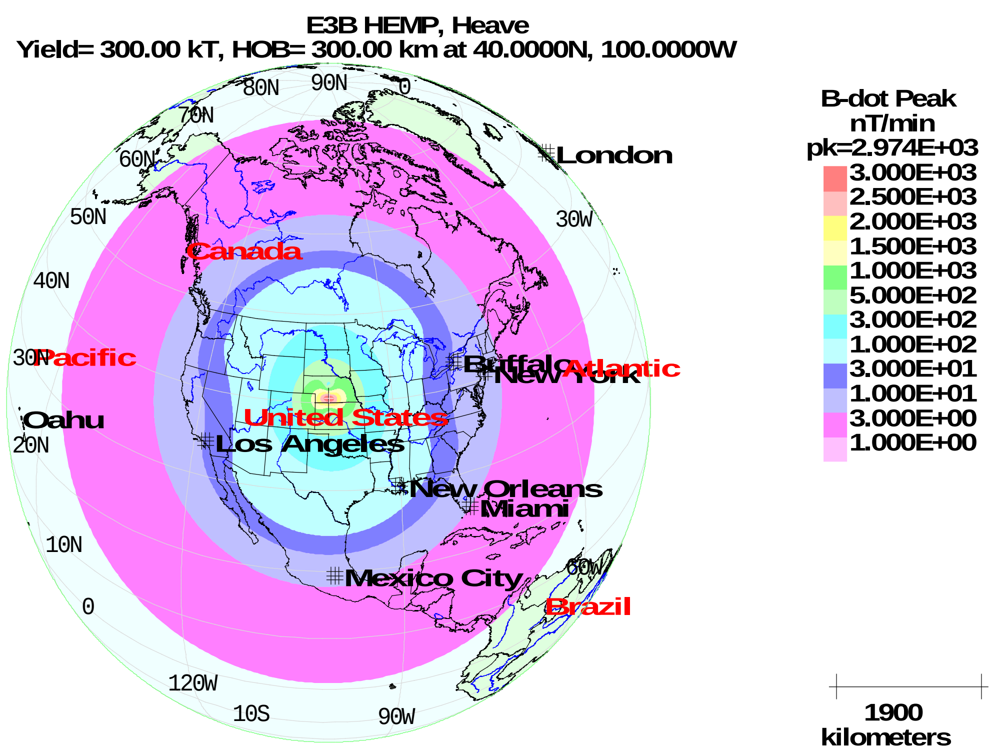


Figure 7. B-dot Magnetic Field Peak contour pattern from a 300 km burst case (from EMAT)

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	*E1:* High peak field – quick rise time *E2:* Medium peak field *E3:* low peak field, but quicker rise time and higher field than for GMD (possibly 3 times higher)	No comparable E1 wave forms No comparable E2 wave forms *E3:* low peak field – fluctuating magnitude and direction
Duration	*E1:* less than a 1 microsecond *E2:* less than 10 millisecond *E3 Blast:* ~10 seconds *E3 Heave:* ~1 – 2 minutes	No comparable E1 wave forms No comparable E2 wave forms *E3:* hours
Equipment at Risk	*E1:* telecommunications, electronics and control systems, relays, lightning arrestors *E2:* lightning: power lines and tower structures – "flashover", telecommunications, electronics, controls systems, transformers. *E3:* transformers and protective relays – long run transmission and communication - generator step-up transformers	*E3:* 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).

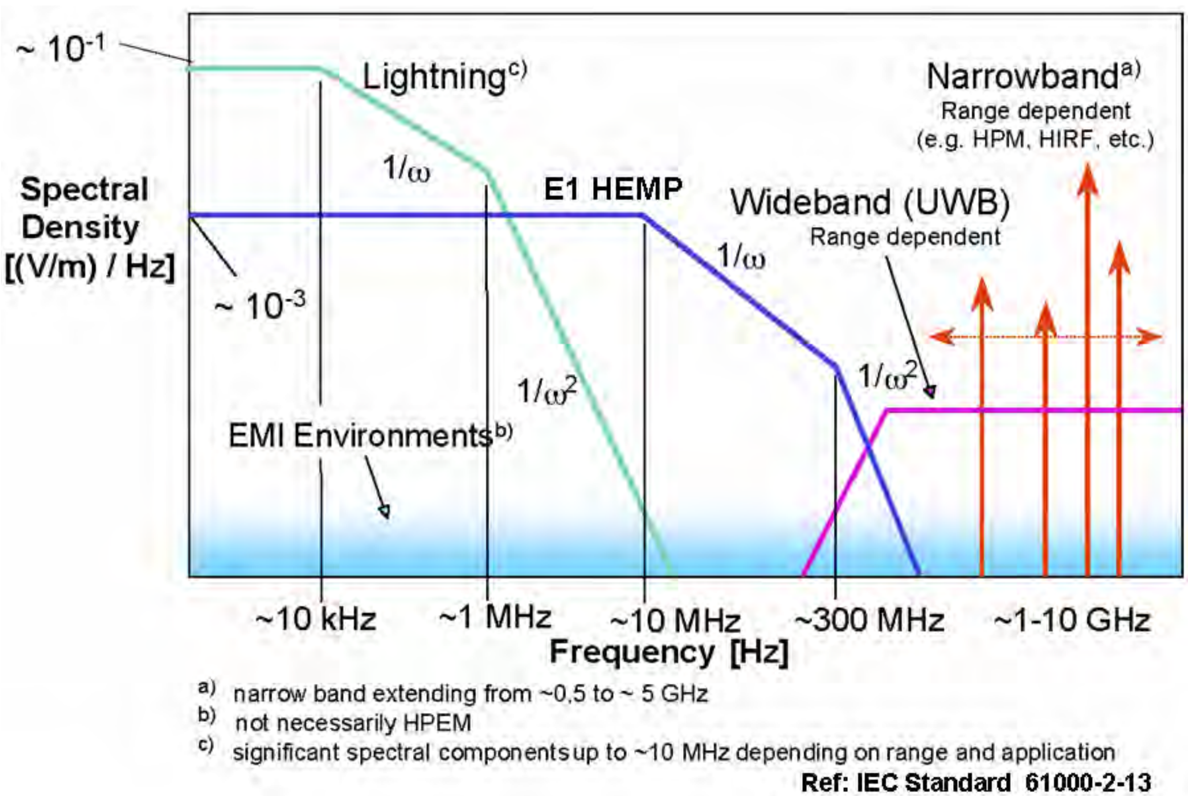


Figure 8. Frequency ranges of Lightning, HEMP, and IEMI [3]

High-altitude EMP (HEMP) Risks

> ***"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)***

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.

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.

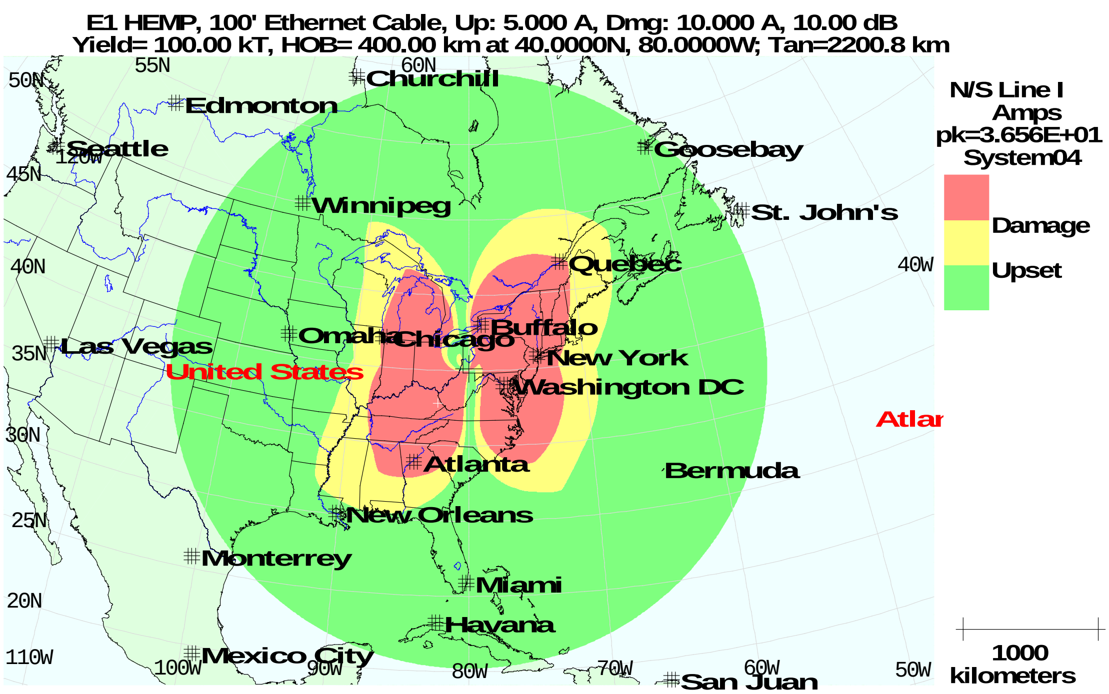


Figure 9. Potential disruption for 100' Ethernet-connected equipment from 100 kT HEMP

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.

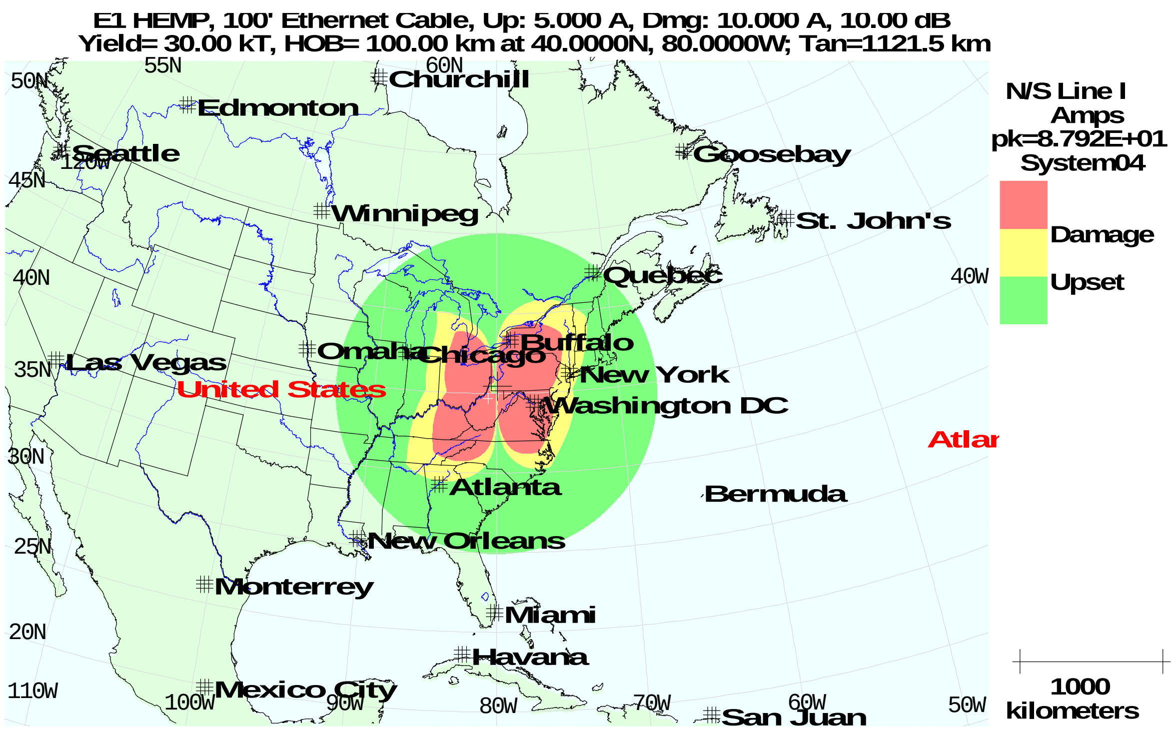
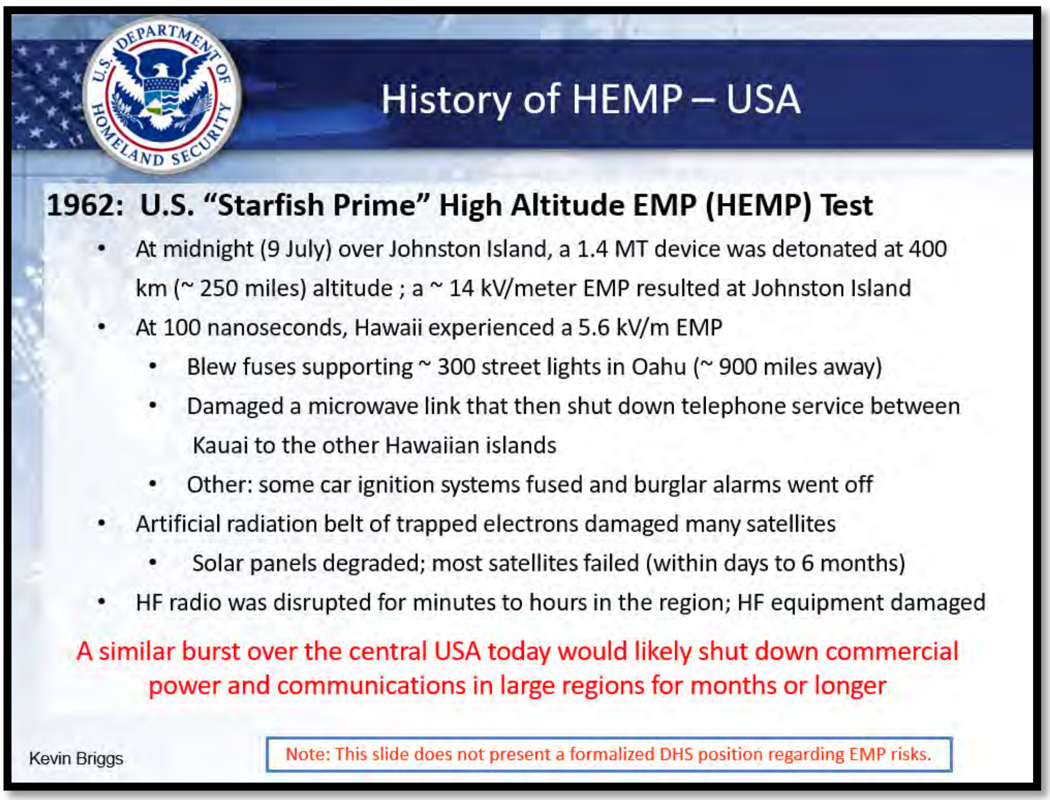


Figure 10. Potential disruption for 100' Ethernet-connected equipment from 30 kT HEMP

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.



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	• Hundreds to thousands of miles • Minutes to hours	• 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	• Hundreds to thousands of miles • Minutes to hours	• 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	• Hundreds to thousands of miles • Minutes to hours	• 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)	• Hundreds to thousands of miles • Minutes to hours	• 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	• Few miles to hundreds of miles • Minutes to tens of minutes	• Reduces range and quality of signal. • 99% of EMP energy is found below 100 MHz.
Ultra High Frequency (**UHF**) (300 MHz – 3 GHz)	Absorption	• Few miles to hundreds of miles • Seconds to few minutes	• 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.

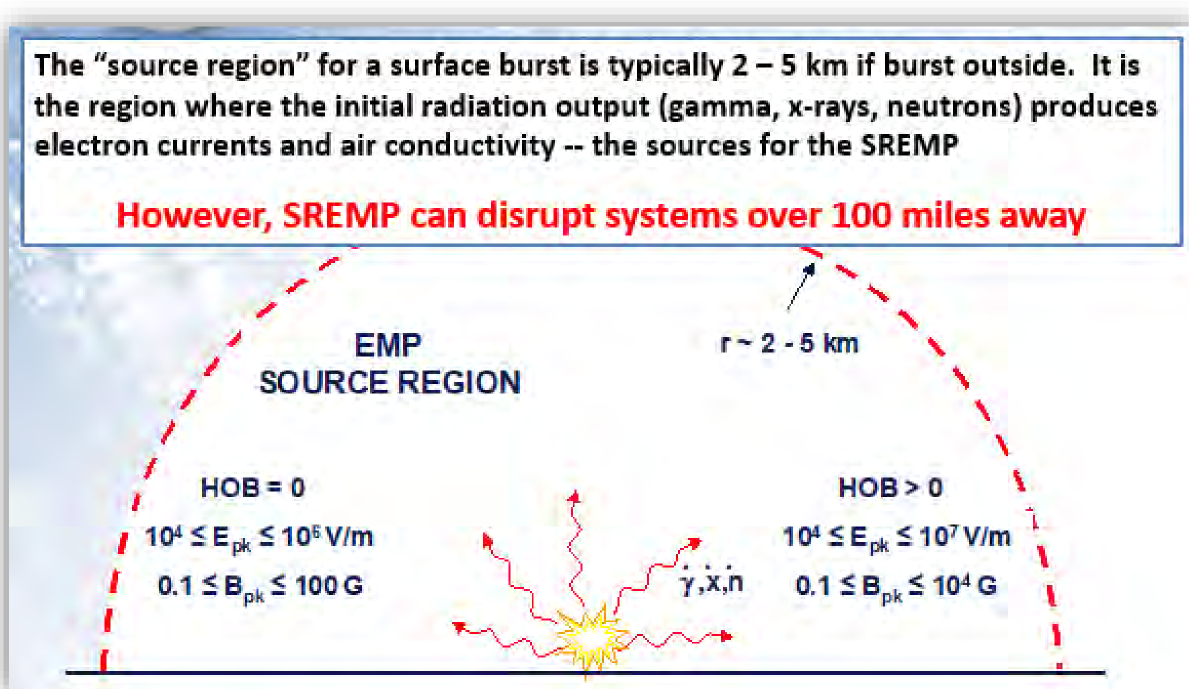


Figure 12. Generation of Source Region EMP (SREMP) from a ground burst

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.

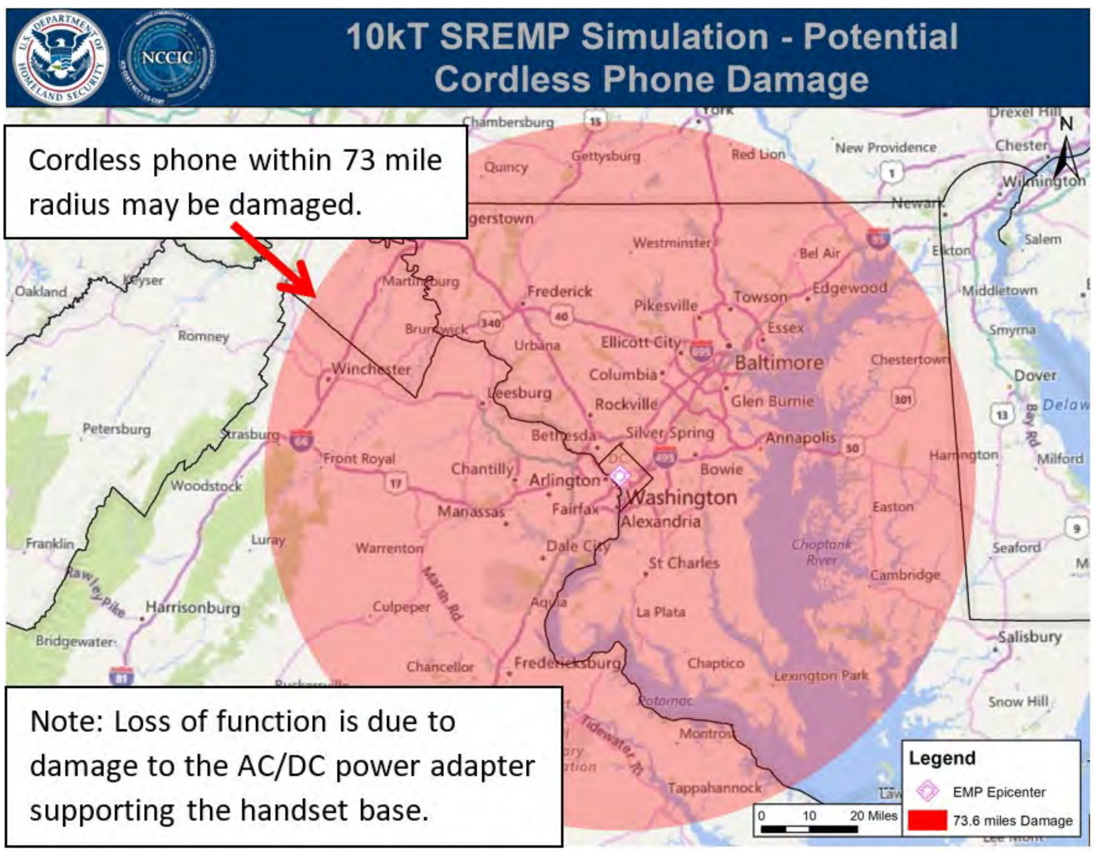


Figure 13. Potential 10 kT SREMP disruption of AC/DC adapters

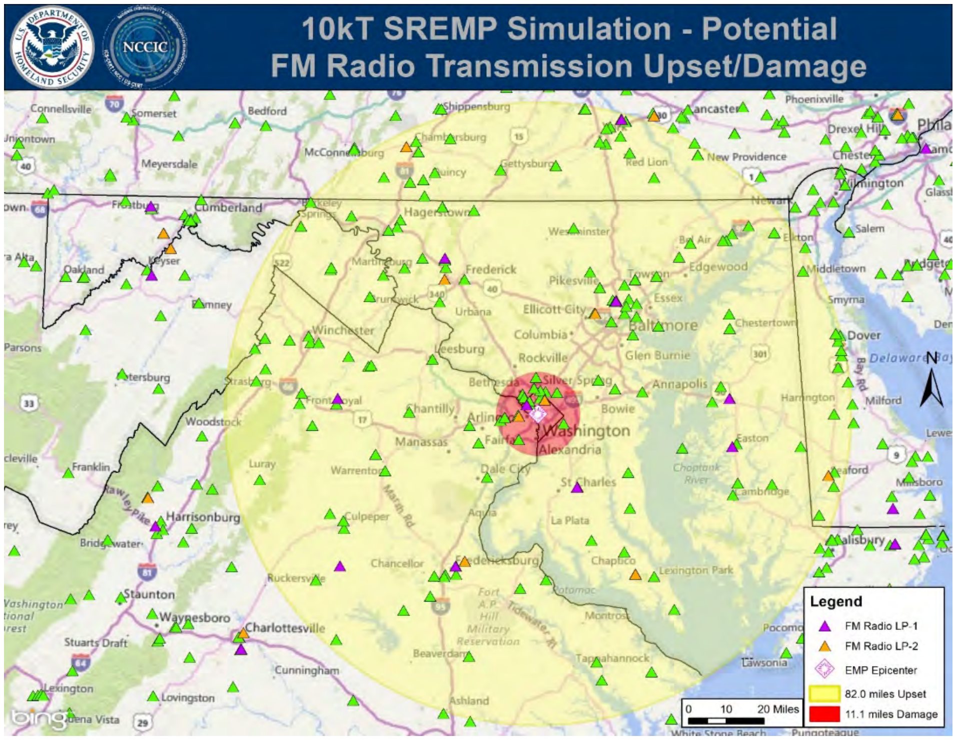


Figure 14. Potential 10 kt SREMP Upset/Damage to FM Radio Transmission

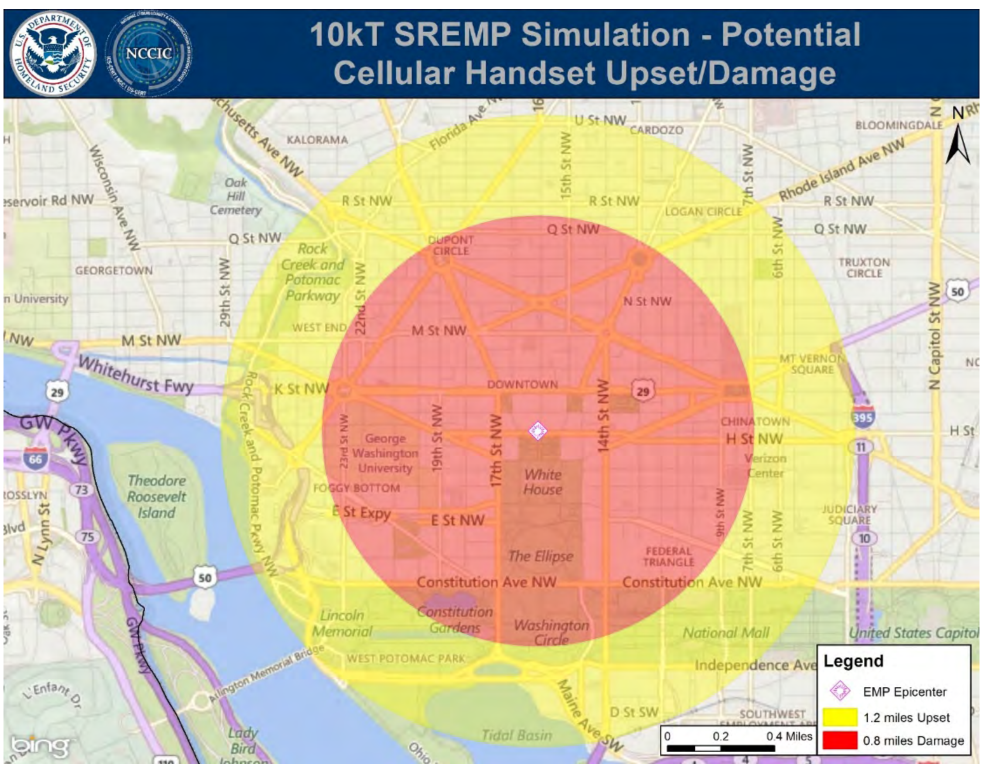


Figure 15. Potential 10 kt SREMP Upset/Damage to Cellular Handsets

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."

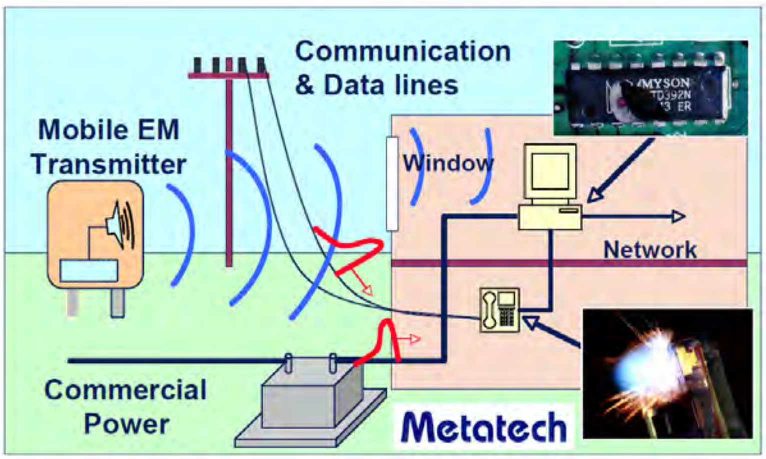


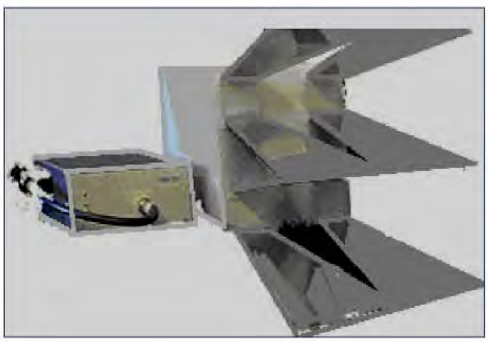
Figure 16. Typical IEMI interaction of radiated fields

"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

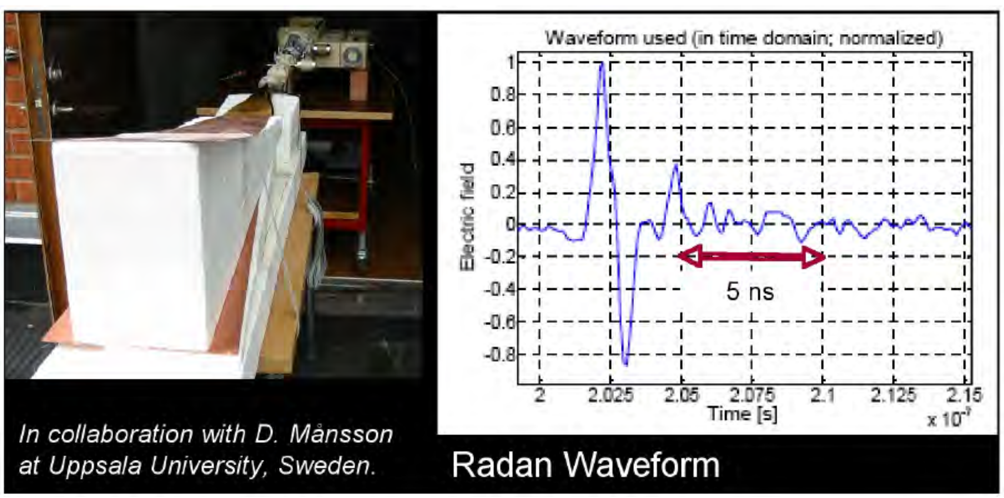


Figure 19. RADAN 303B hyperband generator used in Sweden

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	1/10th 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)**	• 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**	• 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**	• 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 µs and a pulse width of ~ 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 ~300 kV and the worst-case internal induced cable voltages are ~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 µs, 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 helpful[12].
- **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.

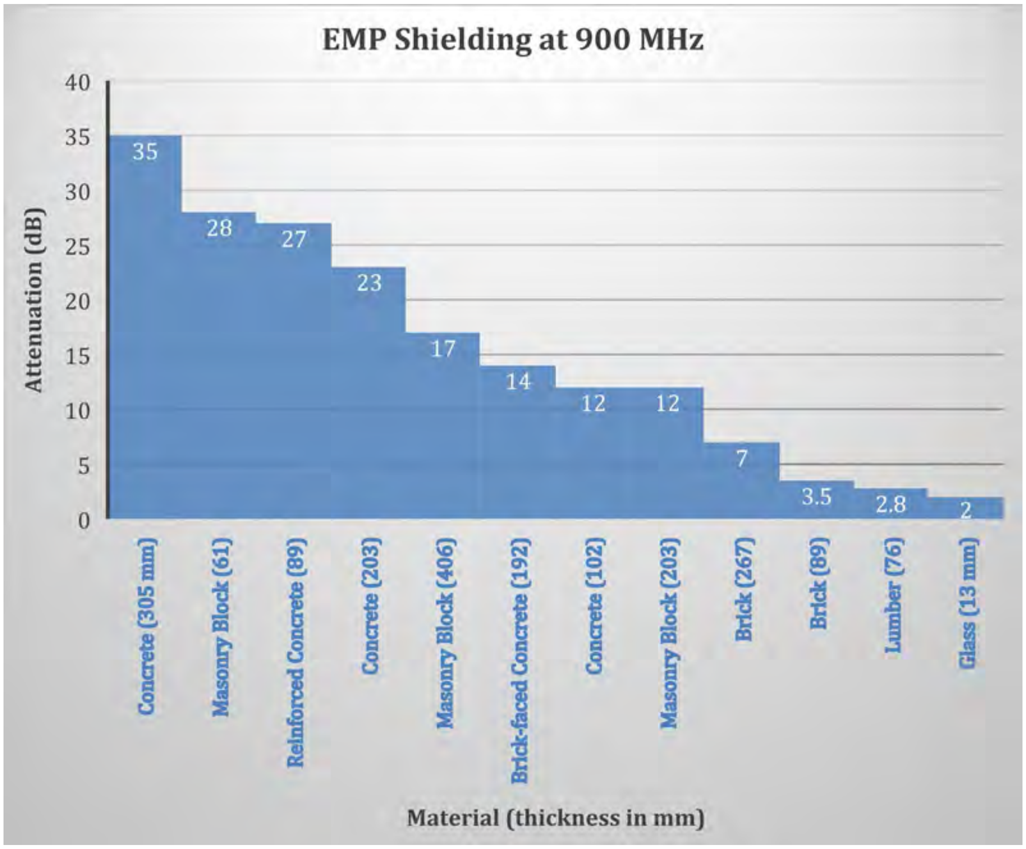


Figure 21. Effect of Building Materials on EMP Attenuation[13]

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. <u>Use a power surge protector device (SPD) that provides fire protection</u>.

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. <u>Use heavy-duty aluminum foil or inexpensive Faraday bags/cases</u>.

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 <u>heavy-duty</u> 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. <u>Ensure your backup generation system is not directly connected to commercial power</u> (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. <u>Use battery operated AM/FM/NOAA radios to receive alerts</u>

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)

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.*"

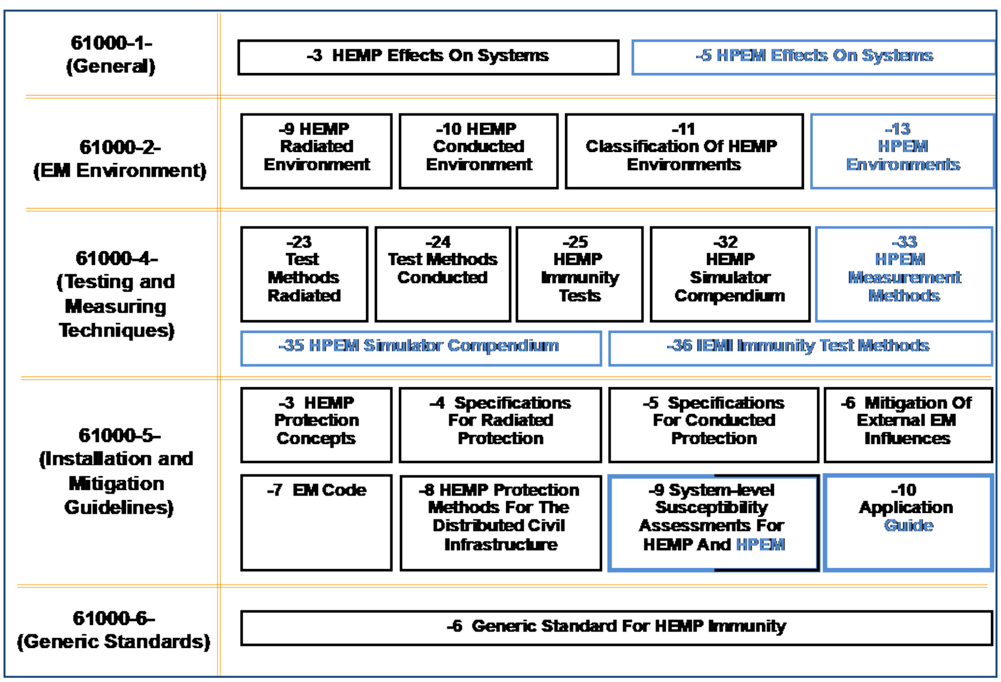
Considerations with shielded cables include:

- 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.

5. LEVEL 3 EMP GUIDELINES

Level 3: Only minutes of mission outages are permitted
In addition to Level 2… • 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 Continental U.S. (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.

The following IEC publications apply to Level 3 Protection and are shown in summary in the figure below and in detail in the Bibliography (Appendix F) at the end of this report:



Note: Black text indicates publications dealing with HEMP, while blue/grey text indicates HPEM/IEMI publications.

Figure 22. Organization of the current IEC SC 77C publications

The Level 3 Facility EM barrier should be designed with the same features and provisions as with Level 4 with the exceptions of both Provision 1 noted below and only one entryway door is required instead of a double-door entry as in Level 4. With only a single door, an alarm or automatic closing feature should be installed to prevent the door from inadvertently remaining open for an extended period thus reducing the hardness of the facility.

The evaluation of the shielding effectiveness as identified in Provision 5 for Level 4 ("*EM Barrier Hardness Validation Testing*") is not required for Level 3. Commercial radio signal techniques may be used to evaluate the shielding effectiveness or IEEE 299 can be used [see Reference 13]. This shielding effectiveness testing is only required for the acceptance of the shielded enclosure, as verification testing is not required (as it is in Level 4). Also, non-linear filter PCI testing may be performed in the laboratory and is not required to be performed on site (as it is in Level 4).

1. <u>Six-sided EM shield barrier</u>

The shield barrier can be constructed using 3-6 mm thick steel sheeting (or by using other shielding materials, such as aluminum or nickel composites) which provides the required level of shielding. *Shielding can be accomplished using a combination of bolt-together designs and welded designs.* If a large number of facilities need to be EMP protected, bolt-together designs that are carefully tested in the factory to meet the required protection levels are more economical.

Copper, aluminum, conductive plastics or other materials may be used if they can provide the required shielding effectiveness and are fully compatible with the POE protective treatments and grounding requirements. Steel is typically preferred because of its superior shielding effectiveness at lower HEMP/SREMP frequencies and its mechanical strength. Using metal screen or wire mesh for the barrier presents problems related to inadequate inherent shielding properties and problems posed in circumferentially bonding cable conduit, vent, and piping penetrations to mesh/screen materials.

2. <u>Uninterruptible power supply (UPS) considerations</u>

When selecting a UPS for protecting equipment from EMP, it is recommended that a true on-line, double-conversion type of UPS always be used as recommended in the Level 2 EMP Protection Guidelines. As this UPS will be installed inside the shielded volume in protection level 4, there is no concern over high frequency transient performance as they must be dealt with before entering the building shield. However, the UPS selected shall be tested against high harmonic currents and voltages (especially the 2nd harmonic), which is generated during E3 HEMP and/or GMD events.

Calculated Level 3 Mitigation Effects

Level 3 EMP Protection recommends a minimum of 30 dB of attenuation from a protective shield through 10 GHz. How much additional shielding may be required beyond 30 dB is best determined through an EM Threat Site Assessment Survey. Additional shielding may be required based on the facility's specific operational requirements including factors such as building construction, physical site layout, the types and amount equipment to be protected, and how distributed or contained the power systems and wired infrastructure are extended beyond the building or campus.

The figures that follow illustrate that just applying the minimum recommended level of 30 dB of attenuation can mitigate the EMP threat to typical cables and devices found inside almost every building. The upper models in each example show the unshielded directionally oriented effects from a 1000 kT burst at 250 miles (400 km) above the center of the continental United States. The bottom model in each example shows the survivable effect provided by 30 dB of shielding attenuation. In addition all external currents coupled to cables outside the building must be reduced before entering a building in order to prevent damage to equipment inside the building connected to those cables (e.g. power).

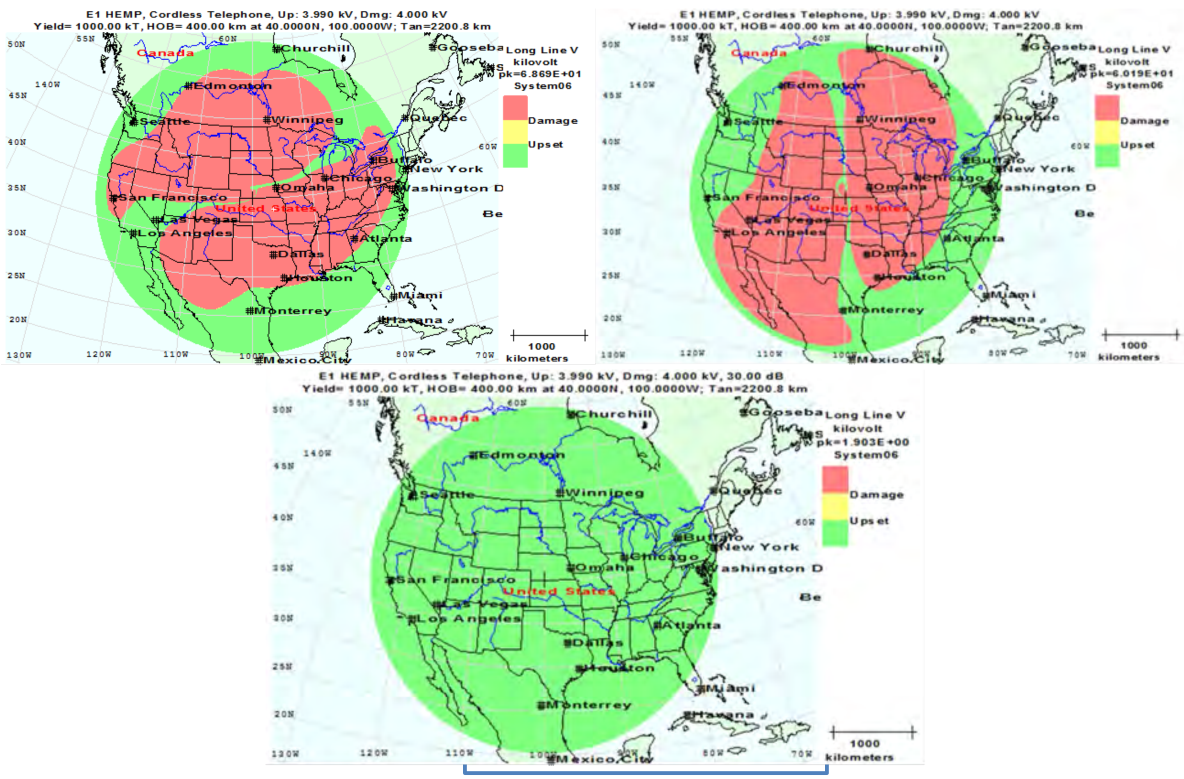


Figure 23. Protective effects on cordless telephones with recommended 30 dB shielding

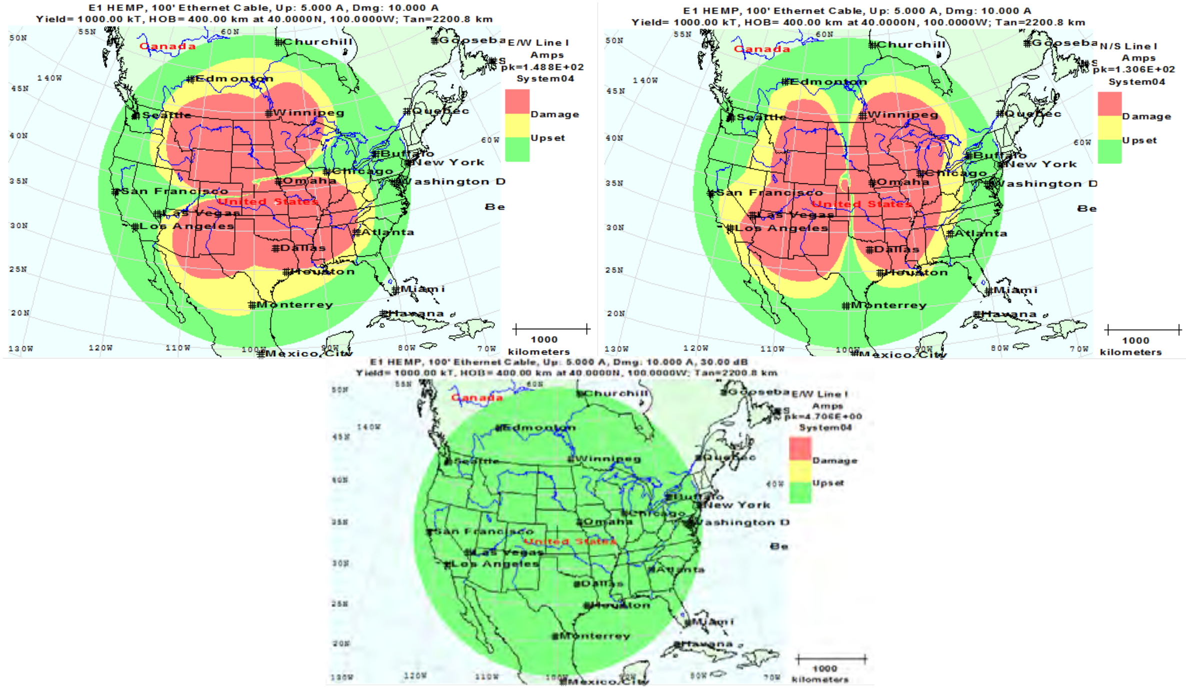


Figure 24. Protective effects on a 100' Ethernet cable with recommended 30 dB shielding

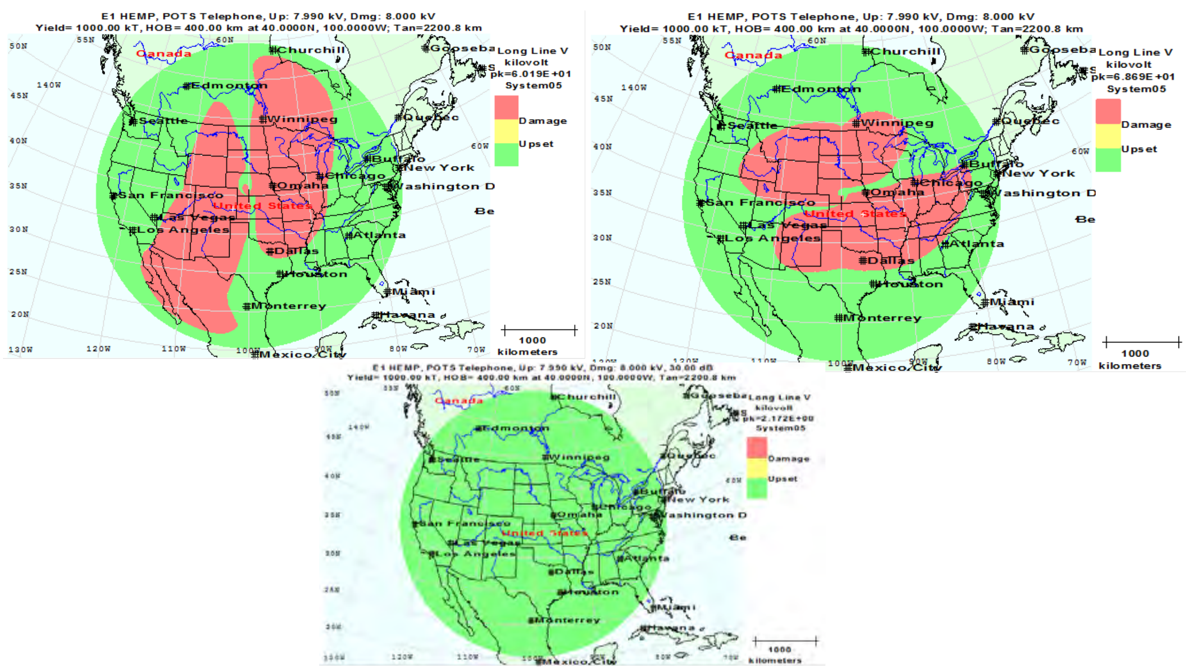


Figure 25. Protective effects on a Plain Old Telephone Service Line with 30 dB shielding

6. LEVEL 4 EMP GUIDELINES

Level 4: Only seconds of mission outages permitted
In addition to Level 3… • Use Military HEMP Standards (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.

The military standard for the EM barrier design is MIL-STD-188-125-1 [see Reference 1], which specifies the following hardening program elements for the protection of HEMP:

1. **<u>The facility shield.</u>**

The facility EM shield is a continuous conductive enclosure that meets or exceeds specified shielding effectiveness requirements. In MIL-STD-188-125-1 this requirement is generally 80 dB up to 1 GHz. For this document we recommend that this requirement of 80 dB be extended to 10 GHz, which will also protect against the IEMI threat. In addition, this level and frequency range is achievable for shielded rooms constructed by industry today.

2. **<u>Shield points of entry (POEs) including wire penetrations, conduit/pipe penetrations, doors, and apertures.</u>**

The number of shield POEs shall be limited to the minimum required for operational, life-safety, and habitability purposes. Each metallic cable POE is protected with a current limiting device that satisfies the standard's performance requirements.

3. **<u>Double surge protect critical external lines entering EMP protected areas.</u>**

Redundant RF surge protection is required on critical external lines entering EMP protected areas in case either (1) the first SPD fails and continues to pass voltage or (2) the SPD is faulty and cannot stop the EMP pulse. In the first case with a double EMP event, the first burst could take out the primary SPD (or something like lightning could take it out), and without a secondary SPD the second EMP burst could take out critical equipment. In the case where the SPD is faulty, the SPD might simply pass an EMP pulse through the line into the equipment if there isn't a secondary SPD to protect the equipment. Lastly, two SPDs will block EMP better than one.

In the above cases, if the cable enters the building via a non-EMP protected area, then the primary SPD should be placed at the building egress with a secondary SPD connected to the cable either within the EMP area or immediately prior to it entering the EMP area. These guidelines are applicable to RF, data, and power cables.

4. HEMP Shield and POE testing.

The standard requires protection performance certification by testing. The protection program includes quality assurance during facility construction and equipment installation, acceptance testing for the EM barriers, and verification testing of the completed and operational facility.

5. Life Cycle Hardness Maintenance and Hardness Surveillance (HM/HS).

HM/HS is included in the facility planning, design, and construction phases to assure that hardness features stay intact over the life cycle of the protected facility and systems. The guidance provided for Level 4 Protection draws heavily on MIL-STD-188-125-1 and the accompanying implementation guidance provided in MIL-HDBK-423 [see References 1 and 2 in Appendix G].

Although the primary method used over the years for protecting equipment from the effects of a HEMP event is to enclose all critical equipment within a steel-shielded electromagnetic (EM) barrier, alternative methods exist including the use of shielded boxes interconnected by non-metallic lines including optical fiber or fluidic control lines.

Generally, an EM barrier for Level 4 Protection is constructed using metal plate (copper, aluminum, and/or steel walls, ceiling, and floor) with all seams continuously brazed or welded. To be complete, the barrier must include treatments on all penetrations to limit currents on the penetrating cables and the EM fields incident on doors, windows, vents, and pipes. Figure 26 provides a conceptual representation of a complete EM barrier. For the shield portion of the barrier, steel plate is preferred over copper for the bulk of the construction because of its superior shielding effectiveness at lower frequencies and its mechanical strength. MIL-STD-188-125-1 provides more detailed requirements for EM barrier construction. Additional information on construction of EM protected facilities is also provided in the following military standards, as referenced in Appendix G:

- MIL-STD-785 addresses reliability
- MIL-STD-470 addresses maintainability
- MIL-STD-2165 addresses testability
- MIL-STD-729 addresses corrosion control

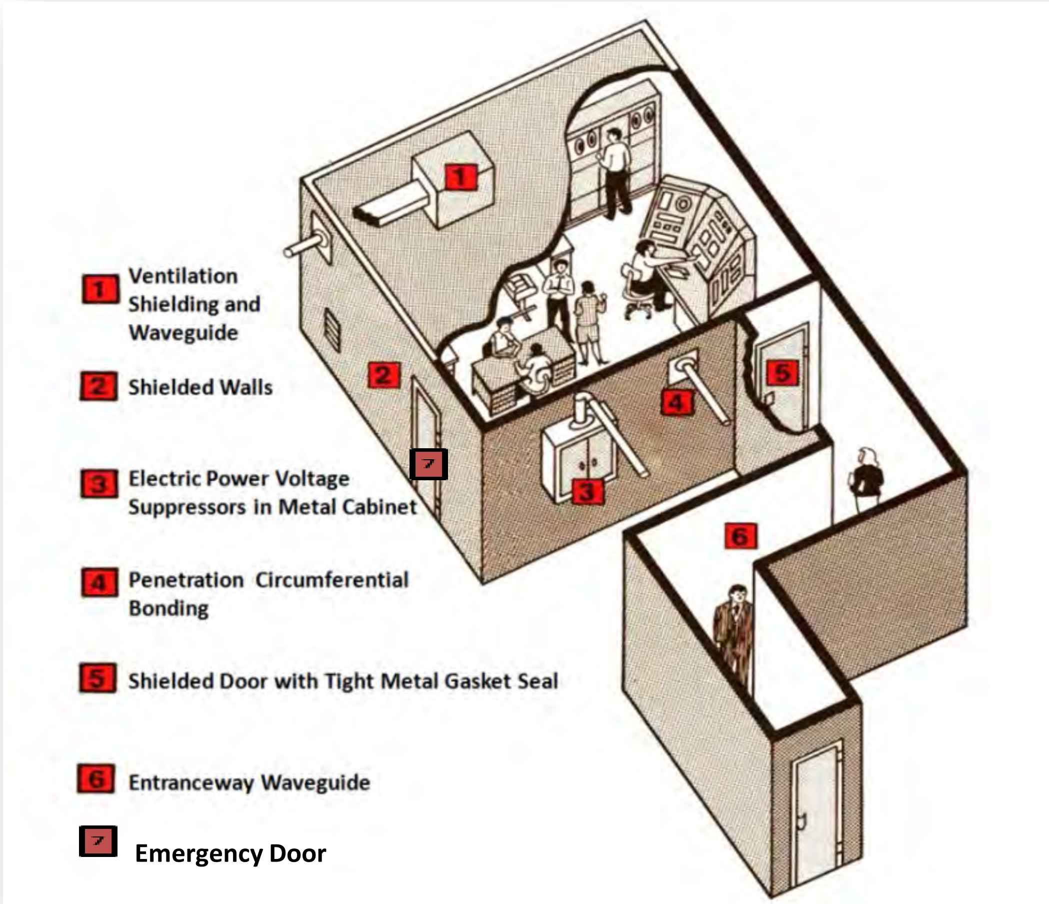


Figure 26. Low-risk EMP barrier protection for facilities (per MIL-STD-188-125-1)

The installation of an EM protection barrier provides a level of immunity to multiple EM environments for electronic equipment. Specifically, the EM barrier provides a shield against EMP and helps accomplish the following:

- Protects MC systems from harmful EM fields.
- Diverts HEMP, SREMP radiating fields and lightning currents to ground.
- Provides immunity to external EMI and IEMI environments,
- Contains classified emissions, which provides Transient EMP Emanation Standard (TEMPEST) protection.
- Provides a sharing path for GMD long-line currents.
- Acts as an excellent ground for internal systems, and, if good contact is made with earth ground, an excellent grounding surface for nearby external systems.

Note that the building surface that in contact with the earth or concrete provides a very low inductance to ground. This is desirable for HEMP and IEMI. Ground rods have high inductance, and while necessary for lightning, are of limited help against high frequency transient phenomena.

The EM barrier provides an EM isolated environment that enables commercial-off-the-shelf (COTS) equipment and systems with no special EM protection to be incorporated within the shielded facility. If the shield is maintained over time, the EM barrier greatly simplifies interior system upgrades and configuration management as systems are moved or replaced. This shifts the focus of system configuration control to maintaining the integrity of the EM barrier.

6. Six-sided EM shield barrier

Shielding will be in accordance with MIL-STD-188-125-1 [see Reference 1], and related military standards. The shield barrier should be constructed using 3-6 mm thick welded steel sheeting, which provides at least 80 dB of shielding. Copper or other materials may be used if they can provide the required shielding effectiveness and are fully compatible with the POE protective treatments and grounding requirements. Steel is preferred because of its superior shielding effectiveness at low frequencies and its mechanical strength. Using metal screen or wire mesh for the barrier presents problems related to inadequate inherent shielding properties at lower and higher frequencies and presents problems relating to circumferentially bonding cable conduits, vents, and piping penetrations to mesh/screen materials.

7. Protection of barrier breaches and cable/piping points of entry (POEs)

Treatment of Protection Barrier Breaches and POEs will be in accordance with MIL-STD-188-125-1 [1], and related military standards. The number of shield breaches and cable/piping POEs should be limited to the minimum required for mission operation, life-safety, and habitability purposes. As a design objective, there should be a single penetration entry area on the EM barrier for all piping and electrical POEs except those connected to external conductors less than 10 m (32.8 ft.) in length. To eliminate cross coupling, the penetration entry area should be located as far from normal and emergency personnel and equipment accesses and ventilation breaches in the shield, as is permitted by the facility floor plan. Each POE should be "treated" with a POE protective device. Guidance for specific types of penetrations follows.

Electrical POEs. EM protection for electrical POEs, including all power, communications, and control penetrating conductors whether shielded or unshielded, should be provided with main barrier transient suppression/attenuation devices. The main barrier transient suppression devices should consist of filters (linear elements) and surge arresters (nonlinear elements), as required to satisfy the shielding effectiveness requirements and residual transient limiting requirements. Figure 27 illustrates a typical cable POE protection design including filters and surge arresters. POE protection should be installed in a manner that does not degrade the shielding effectiveness of the facility EM shield.

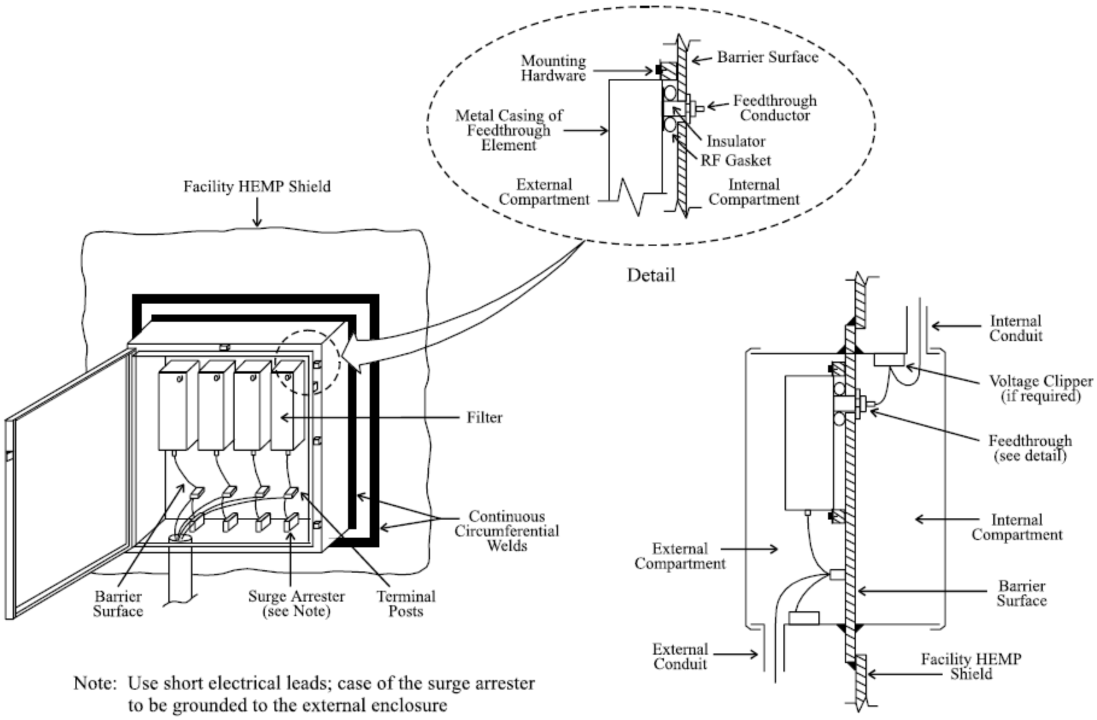


Figure 27. Typical cable POE protection design

In the case of audio and data line penetrations through the shield, it is highly recommended that fiber-optic signal lines be used exclusively. Likewise, if possible, bring radio antenna signals into the barrier-protected space using fiber optic cables by employing copper-to-fiber converters outside of the barrier, preferably as close to the antenna as possible to minimize loss and reduce EMI. In all cases, fiber optic cables that penetrate the shield must use a metallic waveguide-below-cutoff (WBC) entry. In the case of copper-to-fiber converters outside the barrier, these converters must either be hardened to EMP or the communication system must not be a critical one, as the converter is likely to be damaged.

With regard to electrical power service and associated barrier penetrations, the facility should be provided with a backup EM-hardened electrical power generation and distribution capability sufficient to perform missions, without reliance upon commercial electrical power sources. In cases where external power sources are necessary or if internal power sources are used to power external equipment, individual power feeder lines must be protected by installing an electrical surge arrester (ESA) and MIL-STD-188-125 tested low pass filter within a shielded compartment or “ESA vault” (see Figure 28) at both ends of these power cables. To prevent the enterprise-side MOVs from shorting or blowing up, fuses or circuit breakers should be placed in series with each phase line between the Distribution Transformer and the Filter/ESA Enclosure (these are not shown). The facility should be designed to operate for more than 30 days for this protection level using backup power in case the external transformers are damaged.

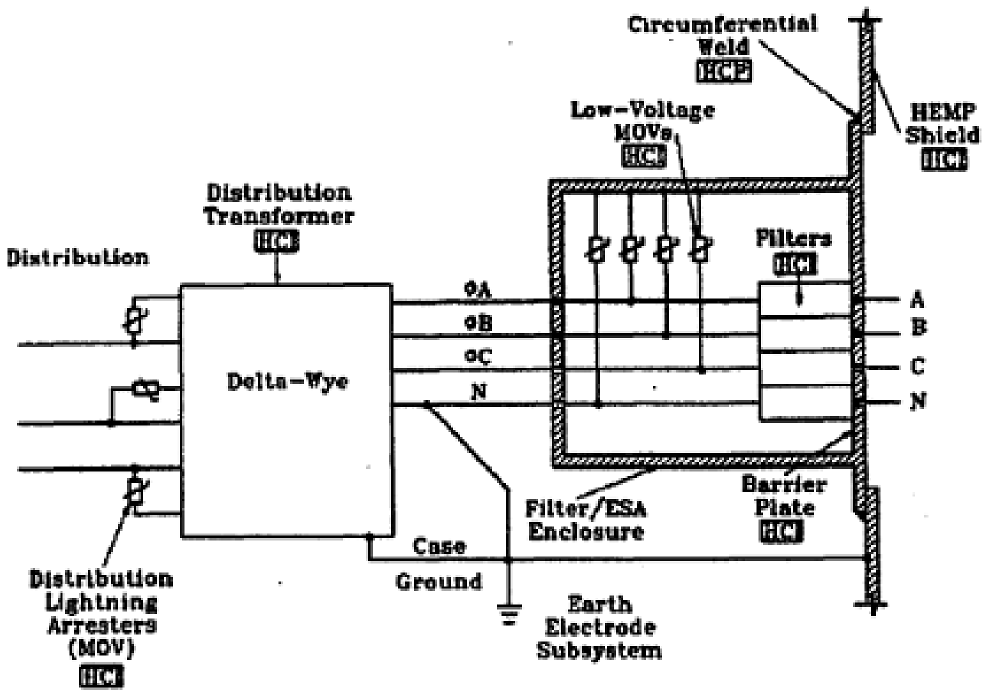


Figure 28. Commercial electric power POE protection

Metallic commercial power entering a critical facility or room that is closer than 50 miles from an urban center with 50,000 or more people (and hence, more likely to be subject to SREMP long line current threats) should be electrically isolated from the power grid. This can be accomplished through either physical separation (disconnection while operating on backup power during periods of heightened threats) or through the use of both an isolation transformer and the use of motor generators outside of the shielded facility or room, etc. As an alternative, fuel cell power technology has been considered in the past for this problem with the fuel passed through the shield.

See Figure 29 to see an example of a power line POE protection approach using a motor-generator set. The input power connection drives a motor external to the EM barrier shield connected to a generator by a dielectric shaft penetrating the shield wall within a WBC. A typical installation would use a flywheel on the motor to electromechanically filter power line disturbances and provide a short, few second UPS function. The primary advantage of a motor-generator set is that there are no metallic power penetrations through the shield. As a result, the motor-generator set provides protection against SREMP, injection-type EM weapons, as well as HEMP (although the essential need for this type of protection is for SREMP). If properly maintained, a motor-generator set can last for more than two decades. The only requirement is to protect the motor against naturally occurring power line transients, such as lightning. This can be accomplished with a Transient Voltage Suppression System (TVSS) usually consisting of MOVs installed at the power input to the motor. In addition, the power line entry to the external motor and any external controls for its operation must be protected against the full set of EMP transients. This is also true if a fuel cell system were used.

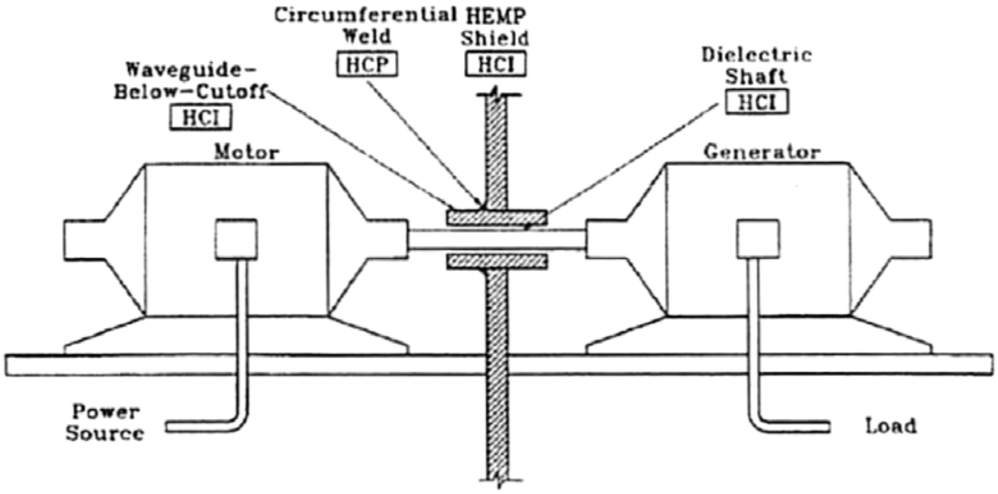


Figure 29. Power line POE protection using a motor-generator set

Personnel and utility breach-type POEs. For personnel entryways, two designs are permissible. The first uses double doors separated by a shielded waveguide-below-cutoff (WBC) vestibule as illustrated in Figure 30. This design provides additional protection for frequencies below ~50 MHz, although for higher frequencies the waveguide alone is not sufficient.

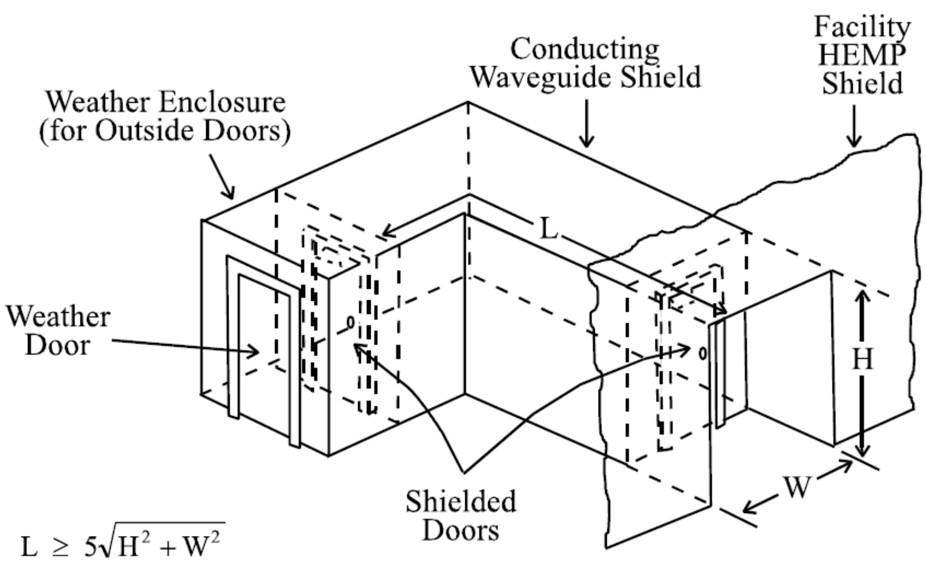


Figure 30. Entryway using two doors separated by a WBC [14]

Figure 31. Sample door with gaskets protecting against EMP threats

The second option uses two doors separated by a metal-enclosed vestibule preferably with an interlock to ensure that only one door is open at a time (including a door interlock). The interlock is needed to ensure that E1 HEMP fields above 50 MHz do not scatter through the waveguide and that the IEMI fields that extend up to 10 GHz do not enter the Facility HEMP Shield when both doors are open (a sample outer door is shown in Figure 31 on the left). This approach is the best in order to deal with all of the EMP threats. In either case, inflatable gaskets or metal fingerstock should be used to ensure electromagnetically tight door.

In the case of barrier penetrations to accommodate utility pipes and conduits, one should circumferentially weld any metal pipe or conduit penetrations at the exterior surface of the metal shield. Waveguide-Below-Cutoff (WBC) designs for air vents and pipes are illustrated in Figure 32 and Figure 33. The cutoff frequency for air filled waveguides can be estimated as f_c (Hz) = 1.5×10^8 / d, where d in meters is the largest dimension of a rectangular waveguide or the diameter of a circular waveguide. Given the cutoff frequency, the length of the waveguide needs to be greater than 5 times the largest transverse dimension of the waveguide.

It should be noted that for ventilation pipes, while a 10 cm diameter is adequate for HEMP purposes, waveguide dimensions of 1 cm are needed to protect against IEMI threats. Industry typically makes ventilation waveguides that are effective up to 18 GHz, satisfying IEMI and TEMPEST requirements in addition to E1 HEMP. In most cases, even if TEMPEST is not a requirement, the use of 1 cm diameter waveguide meshes create less of a mechanical stress on the shield walls, but if hot exhaust is an issue, then the typical 18 GHz meshes cannot be used if they are made from Aluminum, which cannot withstand high temperatures. In addition, small diameter waveguide meshes will likely require some oversizing of the entire mesh to overcome the air resistance factor.

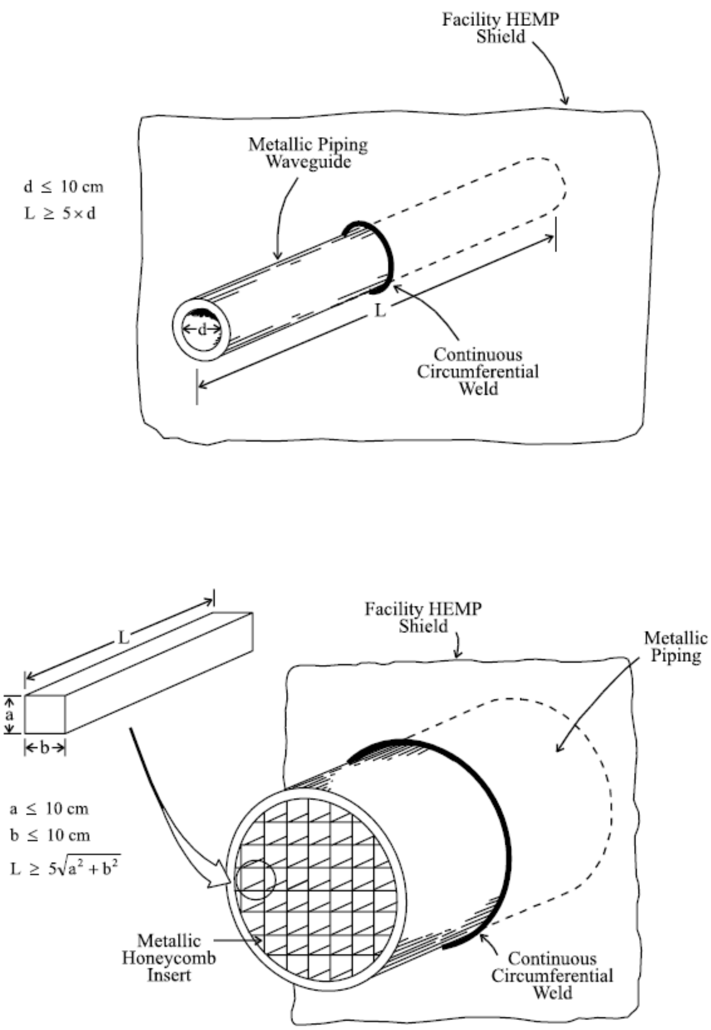
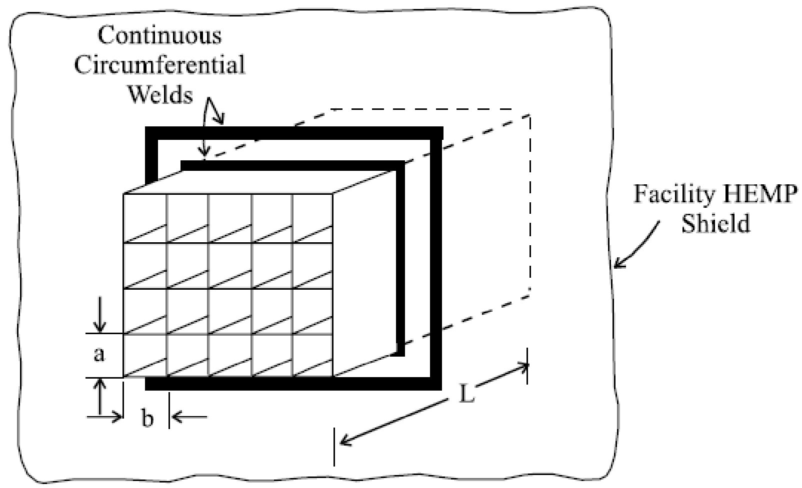


Figure 32. Typical waveguide-below-cutoff (WBC) piping POE protective design for E1 HEMP



$a \leq 10$ cm

$b \leq 10$ cm

$L \geq 5\sqrt{a^2 + b^2}$

Figure 33. Typical waveguide-below-cutoff ventilation POE protective design for E1 HEMP [15]

8. Designation of Mission Critical (MC) Systems

MC Systems include such items as communications electronics equipment, data processing equipment, supervisory control and data acquisition (SCADA) systems, local portions of hardened network interconnects, and critical support subsystems such as power generation, power distribution, transformers, and environmental control systems. All MC Systems, with the exception of equipment that must access the external environment (e.g. antennas, heat exchangers), should be installed within the EM barrier.

EM special protective measures include additional shielding, additional transient suppression/attenuation devices, fiber optic cables, and equipment-level protection required to achieve EM hardness. To facilitate life cycle system hardness, maintenance, surveillance, and configuration management, it is important to minimize the number of subsystems requiring special protective measures. The three categories requiring special protective measures are as follows:

- MC Systems that must be located outside the EM barrier and, therefore, are not protected by the barrier (e.g., cables, radio antennas, evaporative heat exchangers).
- MC Systems that are enclosed within the EM barrier and experience mission aborting damage or upset during verification testing, even though the barrier elements satisfy all performance requirements. (It is noted that this is an exceptional situation that normally indicates that there is in fact a failure of a barrier element.)
- Special protective volumes and barriers to provide supplementary isolation when POE protective devices cannot satisfy the barrier requirements without interfering with facility operation. (This often occurs when it is not possible to prevent in-band HEMP, SREMP or IEMI penetration on antenna lines leading to a transmitter inside the barrier; in this case it is recommended to build a special shielded area for the transmitter equipment inside of the barrier.)

9. EM shield barrier grounding

The barrier grounding practices described here apply to HEMP, SREMP, EM weapons, and lightning. The grounding required for these effects are part of the total facility-grounding network with the ultimate path to ground being the earth electrode subsystem. The lightning subsystem and its earth grounding electrode subsystem are the main interfaces with the EM protection system. It is important that the grounding system be properly designed and constructed to provide the most direct and lowest possible impedance to the earth ground at all frequencies of interest.

The barrier shield exterior should be multi-point grounded to a buried earth electrode system at the corners of the barrier and at 20 foot intervals around the perimeter of the barrier [7-8] (see Figure 34). This approach is particularly important if the shield barrier is not in direct contact with the soil under the facility (when there is soil contact, the shield is grounded in a low inductance fashion providing an excellent path for high-frequency currents on the shield to flow to ground). This buried earth electrode system should also be used as the common ground counterpoise for the EM protection systems of external equipment. Ground straps or cables used to connect the barrier shield to the earth electrode subsystem should be electrically bonded to the external surface of the barrier shield. At least one such low-inductance ground strap, cable or plate should be located at each penetration entry area. Grounds for equipment and structures outside the barrier shield should be electrically bonded to the outside surface of the barrier shield or to the buried earth electrode subsystem.

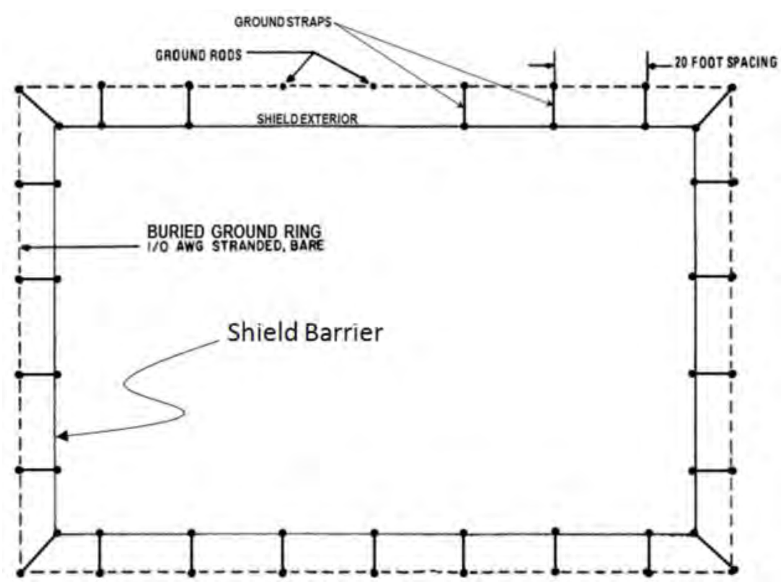


Figure 34. Shield barrier earth electrode system

Grounds for equipment and structures enclosed within the protected volume should be electrically bonded to the inside surface of the shield. Internal equipment should be single-point grounded to the inside of the barrier shield to avoid inductive ground loops, although this aspect is not critical if the shield reduces the external fields correctly. It is a concern for equipment not inside of a shielded volume. All grounding connections to the facility EM shield should be made in a manner that does not create POEs by breaching the shield.

10. EM Barrier Hardness Validation Testing

EM barrier testing is important to ensure the integrity of the shield and the POE protection. The testing should include quality assurance testing during facility construction and equipment installation, acceptance testing for the EM barrier and special protective measures, and verification testing of the completed and operational facility.

Initial EM protection acceptance testing. Initial certification of the EM barrier protection effectiveness should be based upon successful demonstrations of compliance with shielding effectiveness (SE) tests for the barrier and pulsed current injection (PCI) tests of all conducting penetrations. Initial acceptance tests of the EM barrier and special protective measures should be conducted after all related EM barrier shield and PoE construction work has been completed. Initial acceptance test procedures and results should be documented and retained for use as hardness maintenance and hardness surveillance (HM/HS) baseline configuration and performance data.

Operational verification testing. After completion of the EM protection subsystem and installation, operational checks, and installation/acceptance of all system equipment, the EM hardness of the facility should be verified through a program of tests and supporting analysis. The verification program should result in a definitive statement that the critical time-urgent mission functions of the barrier and its contents are certified to withstand exposure to the EM environments of concern. Verification test procedures and results should also be documented and retained for use as hardness maintenance and surveillance (HM/HS) baseline configuration and performance data.

Validation testing types. Both initial acceptance testing and operational verification testing include (1) shielding effectiveness tests, (2) pulsed current injection testing of all electrical POEs and (3) grounding system tests.

(1) **Shielding effectiveness testing is** used to certify that the facility EM shield, with all POE protective devices installed, provides at least the minimum shielding effectiveness shown in Appendix A, Figure A1 for HEMP (80 dB up to 1 GHz). This protection level is sufficient for the radiated fields associated with HEMP and SREMP. To extend the protection to encompass the threat of EM weapons producing IEMI, it is recommended that the shielding effectiveness requirement be extended at the 80 dB level up to 10 GHz. Shielding effectiveness testing should be conducted with barrier POEs and their protective devices in a normal operating configuration, using shielding effectiveness test procedures described in Appendix A of MIL-STD-188-125-1 [1].

(2) **HEMP pulsed current injection (PCI) testing** is well prescribed and involves injecting the pulses prescribed in Appendix A, Table A1 of this document for each electrical POE. This baseline testing for HEMP gives confidence that POE protection will withstand HEMP, radiated SREMP and EM weapon threats up to 1 GHz. To extend the PCI testing to higher frequencies, the IEC has developed test waveforms for EM threats above 1 GHz [9]. The EM barrier passes the test if the POE protective devices attenuate voltages and currents measured inside the shield to the upper bound levels prescribed for each class of electrical POE (as provided in Appendix A, Table A2). Additionally, the main barrier protective device should be rated to withstand a sufficient number of test pulses at the prescribed peak injection current without damage or unacceptable performance degradation to accommodate life cycle testing.

(3) **Ground system testing.** The resistance to earth of the earth electrode subsystem should be tested using the fall-of-potential method. The completed grounding system should be "Megger tested" at the service disconnect enclosure grounding terminal, and at earth electrode system ground test wells. Measure ground resistance not less than 2 full days after the last trace of precipitation, and without the soil being moistened by any means other than natural drainage or seepage and without chemical treatment or other artificial means of reducing natural ground resistance. It is recommended that the tests be performed using the two-point method according to IEEE 81, "Guide for Measuring Earth Resistivity Grounding Impedance and Earth Surface Potentials of Ground Systems." Unless otherwise specified by facility drawings, the earth ground resistance should be 10 ohms or less.

11. Hardness Maintenance and Hardness Surveillance (HM/HS)

A built-in test capability should be installed to at least qualitatively monitor for EM shield leakage. The built-in shield monitoring system should include:

- Radiating antenna(s) external to the barrier shield
- Receiving antenna(s) internal to the shield
- Test control, antenna source, and data analysis electronics inside the shield

To facilitate HM/HS, the barrier shield design should include a crawl space underneath the shield floor to enable inspection for floor plate defects due to maintenance or corrosion and shielding effectiveness testing. On the other hand, if the barrier shield floor can be constructed in direct contact with the soil, high frequency currents induced on the other 5 sides of the shield will be severely attenuated at the soil/barrier interface.

12. Treatment of Mission Critical (MC) Systems outside the EM barrier

For MC Systems that must be located outside of the barrier shield, special protective measures should be implemented to ensure effective EM protection. Special protective measures for MC Systems outside the main barrier may include:

- Cable, conduit, and local volume shielding
- Use of fiber optic cables for signaling
- Linear and nonlinear transient suppression/attenuation devices
- Equipment-level hardening (reduced coupling cross-section, dielectric means of power transport, use of inherently robust components)
- Moving sensitive circuits associated with external MC Systems to locations within the protected volume
- Automatic recycling features or operator intervention schemes, when the mission timeline permits
- Other hardening measures appropriate for the particular equipment to be protected

Performance requirements for the special protective measures should ensure that the highest EMP-induced, peak time domain current stresses reaching the equipment are less than the vulnerability thresholds of the equipment.

RF communications antennas outside the main EM barrier and any associated antenna-mounted electronics, tuning circuits, and antenna cables located outside the main electromagnetic barrier should be treated as MC Systems that are placed outside the EM barrier. Performance requirements for the EM protection should ensure that the highest EM threat-induced peak time domain current stresses at the antenna feed are less than the vulnerability thresholds of the MC Systems located outside the barrier.

Front door in-band protection is one of the more challenging (but not insurmountable) EM protection problems. The high gains associated with most “front door” coupling paths make these potentially the most susceptible portion of radio communication systems. However, these well-characterized front door receive paths have been the subjects of much attention in terms of protection engineering. Radar systems are often protected from their own or neighboring transmitters by a receiver protector or RP. Similar protection can be applied to communication receivers against in-band EM weapon environments. A typical RP uses plasma and diode limiter stages. At a given threshold the most sensitive diode turns on, forming a shunt across the waveguide. At higher energies, the other stages activate in parallel. The plasma “vial” stages turn on at the highest powers through a process similar to air breakdown and are capable of diverting large amounts of energy to ground without damage. Most vial limiters use halogen gas as the breakdown medium. If the system is transmitting, it will be necessary to unkey the transmitter to extinguish the ignited plasma devices. As an example, the schematic of a Westinghouse RP design is provided in Figure 35.

Effective and robust waveguide filters are available for out-of-band front door EM weapon environments. The challenge is to provide protection at the same time minimizing insertion loss effects on normal operation.

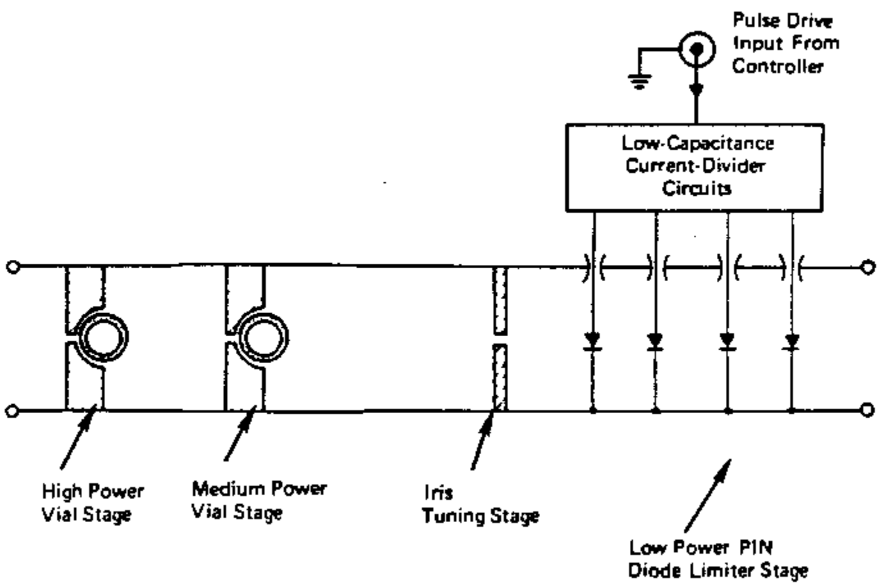


Figure 35. Example receiver protector unit diagram.

13. Special protective volumes

Special protective volumes for piping POEs. As discussed earlier in this section, when a pipe POE diameter must be larger than 1/5 of the pipe's length and a WBC array insert cannot be used, a special protective volume should be established inside the EM barrier. The protective volume should include a special protective barrier that should completely enclose the non-compliant piping. The protective volume should be protected at the barrier shield outer wall using the WBC technique having a cutoff frequency of at least 1.0 GHz for HEMP and SREMP, but should extend to 10 GHz for IEMI and 18 GHz for TEMPEST. The special protective barrier may be a separate shield with protected penetrations, or it may be implemented by extending the metal walls of the piping system itself as shown in the figure below. Performance requirements for the special protective barrier should ensure that the total shielding effectiveness, measured through the main EM barrier and special protective barrier, satisfies at least the minimum requirements shown in Appendix A, Figure A1.

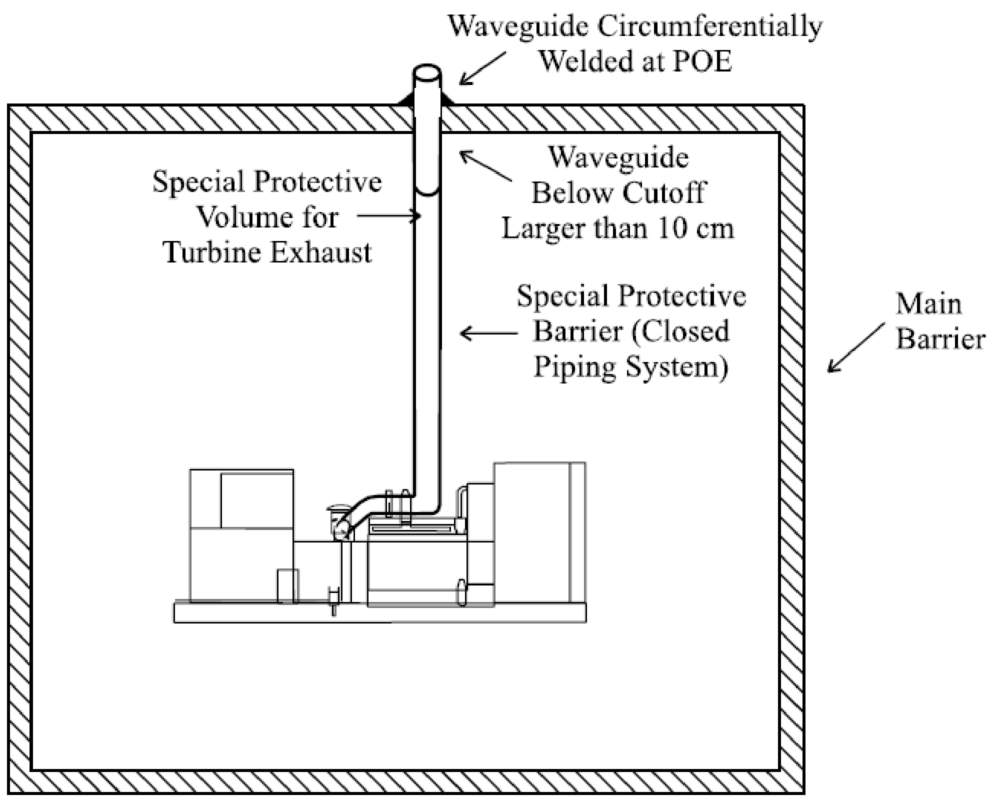


Figure 36. Special protective volume for piping POE for E1 HEMP

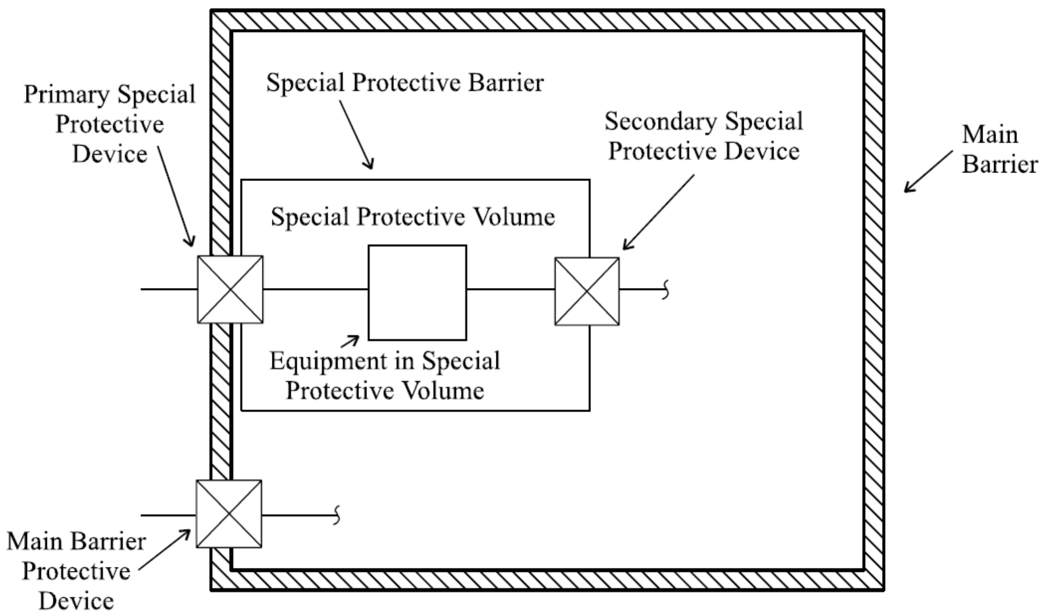


Figure 37. Special protective volume for electrical equipment

Special protective volumes for **electrical** POEs. When a main barrier protective device cannot be designed to achieve the transient suppression/attenuation performance prescribed for the particular class of electrical POE without interfering with operational signals it is required to pass, a special protective volume should be established inside the main EM barrier as shown in Figure 37 above. A special protective volume should be enclosed by a special protective barrier with primary and secondary special electrical POE protective devices, as required to meet the performance requirements prescribed. The special protective barrier should completely enclose wiring and equipment directly connected to a primary special electrical POE protective device. The special protective barrier may be a separate shield, or it may be implemented using cable and conduit shields and equipment cabinets. Performance requirements for the special protective barrier should ensure that the total shielding effectiveness, measured through the main EM barrier and special protective barrier, satisfies at least the minimum requirements shown on Appendix A, Figure A1 (*HEMP Shielding Effectiveness Requirement*).

Secondary special electrical POE protective device requirements. When the combination of the primary special electrical POE protective device and the directly connected equipment cannot be designed to achieve the transient suppression/attenuation performance prescribed for the class of electrical POE (per Appendix A, Table A2), a secondary special electrical POE protective device should be used. The secondary special electrical POE protective device should be designed so that the total transient suppression/attenuation, measured through the primary special protective device, the connected equipment, and the secondary special protective device, satisfies at least the minimum requirements prescribed for the class of POE without device damage or performance degradation.

MC Systems in a special protective volume. Special protective measures should be implemented as necessary to harden MC Systems in a special protective volume to the EM-induced stresses that will occur in that volume. Special protective measures for MC Systems in a special protective volume may include the use of the following:

- Cable, conduit, and volume shielding
- Fiber-optic cables
- Transient suppression/attenuation devices
- Equipment-level hardening
- Remote locating of sensitive circuits
- Automatic recycling or failover
- Operator intervention features
- Other hardening measures appropriate for the particular equipment to be protected.

Performance requirements for the special protective measures should ensure that the highest EM-induced peak time-domain current stresses reaching the equipment are less than the vulnerability thresholds for the equipment. Adequate WBC EM attenuation occurs if the length (L) is greater than $5\sqrt{H^2+W^2}$ where H is the height and W is the width of the conduit or passageway.

14. Special Protection at the box level

While a facility-level barrier ("global" shielding and POE protection) is preferred, there are situations where box-level protection can be used. A conceptual diagram of global vs. box-level protection appears below in Figure 38.

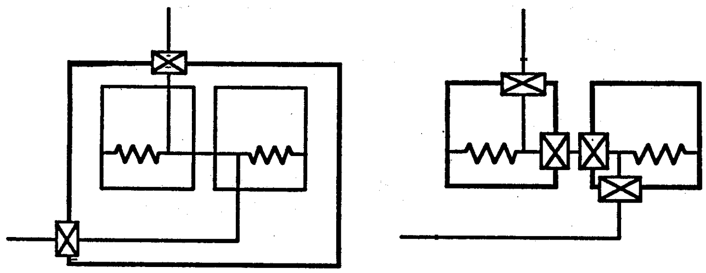


Figure 38. Global barrier vs. box-level protection

A complete facility EM barrier provides the best protection. Its effectiveness is easy to verify using CW field illumination, which facilitates initial protection certification and HM/HS activities. It is the preferred method for critical systems where internal electronic boxes are being changed or upgraded often. It has been successfully implemented for the HEMP protection of the U.S. backbone communication and strategic missile systems. However, for many systems global shielding may impose unacceptable cost and weight increases.

Alternatively, a combination could also be implemented where a 30 dB or more shielded facility is used for equipment and cables that are less important or less sensitive. An additional EM barrier of 50 dB or more in this example could then also be used for more important or more sensitive equipment.

Box level protection can be very effective, especially in the case where only a few pieces of equipment are critical. Well-designed electronic boxes using RF gaskets and cable treatment have been demonstrated to be very effective to the point that internally coupled RF levels are indistinguishable from noise levels. Non-fiber optic cables must be well shielded with high quality connectors circumferentially bonded to the cable shield. Box level hardening techniques are depicted below in Figure 39.

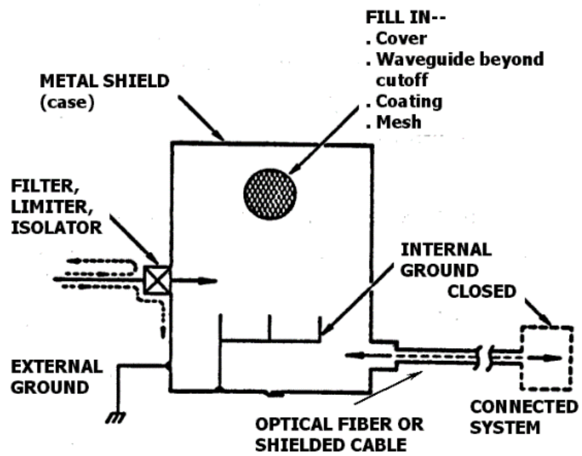


Figure 39. Box-level hardening techniques

15. Multiple shielded buildings or shielded volumes connected by conduits

EMP protection for cables running between two shielded facilities or rooms may be provided by using continuous conduit shielding or highly shielded and tested cables, when the lengths of the runs do not exceed the applicable maximums provided in Table 10 that follows.

Table 10. HEMP Specifications for Cable Runs Between Two Protected Areas

Type of Cable Run and Conduit	Maximum Conduit Length (m)		
	5 cm ≤ OD < 10 cm	10 cm ≤ OD < 15 cm	15 cm ≤ OD
Signal and Low Current Power Lines			
Buried Conduit	37	75	112
Nonburied Conduit	6	12	18
Medium Current Power Lines			
Buried Conduit	200	600	1120
Nonburied Conduit	60	120	180
High Current Power Lines			
Buried Conduit	200	600	1,200
Nonburied Conduit	200	600	1,200

Table Definitions:

(1) **Signal Line**: Contains one or more control or signal conductors.
(2) **Low Current Power Line**: Contains one or more conductors with maximum operating currents less than 1.0 A.
(3) **Medium Current Power Line**: The maximum operating current on the lowest rated conductor is between 1.0 A and 10 A.
(4) **High Current Power Line**: Contains only power lines with operating currents greater than 10 A.
(5) **Buried Conduit:** No more than 1 m (3.3 ft.) of its total length is not covered by earth or concrete fill.
(6) **Nonburied Conduit**: More than 1 m (3.3 ft.) of its total length is not covered by earth or concrete fill.

Main barrier ESAs and filters are not required on the penetrating conductors under conditions where cable runs are shorter than shown in the previous Table and the conduit or cable is bonded to the shields at both ends.

Some design and certification test requirements are shown below. Additionally, "*Figure 40. EMP protected conduit*" on the right shows as a sample conduit running from an EMP filtered area to a 120 dB EMP protected container.

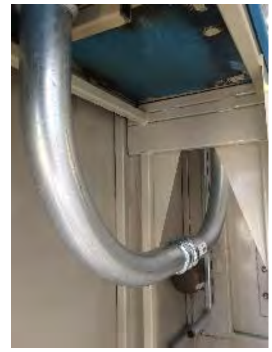


Figure 40. EMP protected conduit

- Conduit design requirements. EMP protection conduits should be rigid metal conduits, with circumferentially welded, brazed, or threaded closures at all joints and couplings, pull boxes, and at both ends of penetrations through the facility EMP shields.

- Conduit certification test requirements. A pulsed current injection (PCI) source, producing an 800-A short-circuit current on a buried signal or low current power line conduit and a 5000-A short-circuit current on a non-buried signal or low current power line conduit, 20 ns risetime and 500-ns pulse width (full width at half maximum), and source impedance ≥ 60 Ω, should produce a residual internal transient stress no greater than 0.1 A on the wire bundle inside the conduit.

The same PCI source connected on the outer surface of a medium or high current power line conduit should produce a residual internal transient stress no greater than 10 A, when the operating current on the lowest rated conductor in the wire bundle inside the conduit is greater than 10 A, and no greater than 1.0 A when the operating current is between 1.0 A and 10 A.

If a multi-conductor shielded cable can be tested in the laboratory to the pulses described in the second bullet above, and it can achieve the required peak residuals, then a shielded cable can be used instead of a conduit.

7. HEMP MODEL MITIGATION RESULTS

This section uses a HEMP protection effectiveness model based upon: IEC recommendations, known nuclear yields by nuclear-capable countries, and real-world testing of commonly used cables and equipment. This model was developed to better understand the ramifications of a HEMP attack and how much protection is needed to prevent damage or upsets (resetting the device). This protection would also be critical for SREMP and IEMI attacks. The model showed that even though minimal protection of 10 dB helps significantly, 20 dB is much more helpful, and 30 dB eliminates almost all damage.

The above is excellent news since 10 dB can often be met simply by following good lightning protection practices, including ensuring low inductance ground connections. 20 dB can generally be met and sometimes 30 dB can also be met by making small, inexpensive modifications. These EMP improvements include using EMP rated SPDs, adding ferrites, burying external cables, and moving operations toward the middle of a building perhaps in the basement with more walls between the cable runs and the potential HEMP burst.

These simple EMP related changes or additions could substantially reduce the risks associated with an EMP attack and prevent it from devastating the country.

7.1. Model Assumptions

This section discusses the results of an EMP model that was created to better understand the relationship between improved EMP protection and decreased equipment damage and upsets. The key parameters in the model are shown in Table 11 below.

Table 11. Modeling Parameters Used to Calculate HEMP Damage

Parameter	Assumption
Nuclear Yield	100 kiloton (kT) or a peak field of 50 kV/m (peak field is per IEC recommendation)
Height of Burst	400 km (about 250 miles) (per IEC recommendation)
Latitude and longitude of burst	40.0 North, 100.0 West
100 ft. Ethernet	• 0.1m height over ground; aligned radially • Current into 100 ohms • Maximum of calculations for 0.01 S/m or 0.001 S/m ground conductivity • Damage at 10 A; Upset at 5 A (per actual testing)
POTS Telephone	• Voltage calculation for 1 km radial line • Damage at 8 kV; no upsets (per actual testing)
Cordless Telephone	• Voltage calculation for 1 km radial line • Damage at 4 kV (AC/DC Power Adapter failed) (per actual testing)

The baseline of 0 dB shown in the results assumes that the item in question has a clear line of sight to the HEMP burst and that the cables are not shielded.

7.2. Model Results

Below are the modeling results using the assumptions discussed under *Model Assumptions* above. The first subsection below reviews the *High Level HEMP Model Results*. The next three subsections show the damage and upset areas for the following: (i) *100' Ethernet Model Results*, (ii) *POTS Telephone Model Results*, (iii) *Cordless Telephone Model Results*. These results include protections of 0 dB, 10 dB, 20 dB, and 30 dB.

High Level HEMP Model Results

The high level HEMP modeling results shown in Table 12 demonstrate the potential devastating national impact of a 100 kT HEMP burst. Fortunately, the results also demonstrate the potential to substantially reduce the impact with 20 dB of protection and essentially eliminate it with 30 dB of protection. These results drive the government's desire to ensure that at least the critical infrastructure has adequate EMP resiliency, particularly given the minimal cost that is often involved in obtaining improved resilience.

Table 12. Example HEMP Model Damage and Upset Mitigation Results

Scenario – with amount of Protection in dB	Damage Area US (sq mi)	Damage % US	Upset Area US (sq mi)	Upset % US	Total Damage + Upset Area US (sq mi)	Total Damage + Upset % US
100 ft Ethernet – 0 dB	1,600,214	54.2%	458,229	15.5%	2,058,443	69.7%
100 ft Ethernet – 10 dB	617,929	20.9%	588,277	19.9%	1,206,206	40.8%
100 ft Ethernet – 20 dB	49,642	1.7%	193,159	6.5%	242,801	8.2%
100 ft Ethernet – 30 dB	0	0.0%	0	0.0%	0	0.0%
POTS Telephone – 0 dB	1,522,461	51.5%	0	0.0%	1,522,461	51.5%
POTS Telephone – 10 dB	380,791	12.9%	0	0.0%	380,791	12.9%
POTS Telephone – 20 dB	0	0.0%	0	0.0%	0	0.0%
POTS Telephone – 30 dB	0	0.0%	0	0.0%	0	0.0%
Cordless Telephone – 0 dB	2,305,017	78.0%	0	0.0%	2,305,017	78.0%
Cordless Telephone - 10dB	970,088	32.8%	0	0.0%	970,088	32.8%
Cordless Telephone - 20dB	129,791	4.39%	0	0.00%	129,791	4.4%
Cordless Telephone - 30dB	0	0.00%	0	0.00%	0	0.0%

100’ Ethernet Model Results

As shown in the figures below, the amount of EMP upset/damage to equipment connected to 100’ Ethernet cables could be substantially reduced or eliminated with 20 dB or 30 dB of protection.

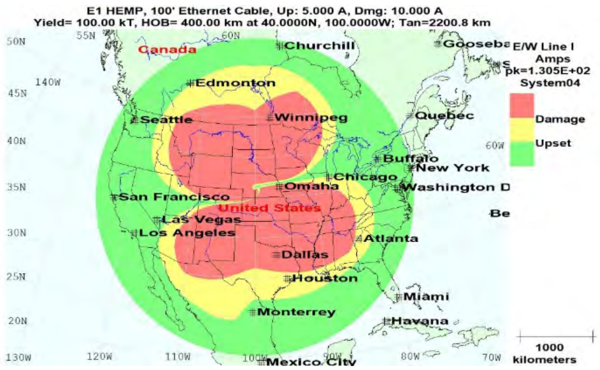


Figure 41. Potential upset/damage of equipment connected to 100’ Ethernet cable with 0 dB protection

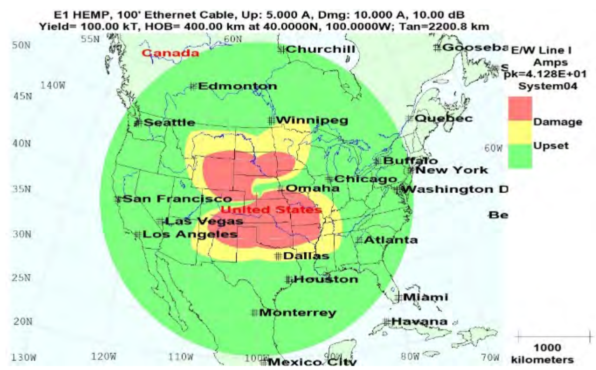


Figure 42. Reduced damage with 10 dB protection to 100’ Ethernet cable connected equipment

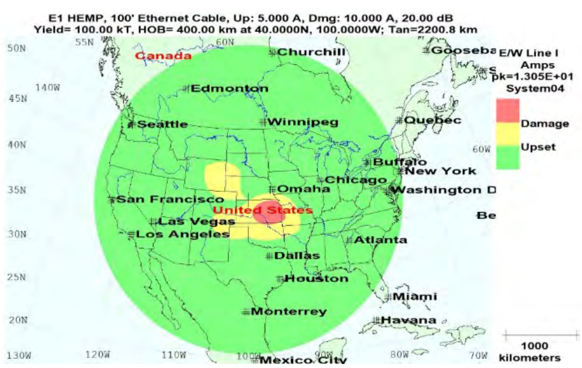


Figure 43. Localized damage only with 20 dB protection with 100’ Ethernet cable

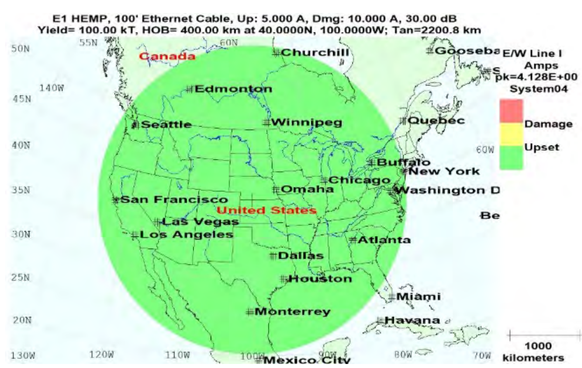


Figure 44. No damage with 100’ Ethernet cable and 30 dB protection

POTS Telephone Model Results

As shown in Figure 45 through Figure 48 below, the amount of damage to a POTS telephone could be substantially reduced or even eliminated with 20 dB or 30 dB protection.

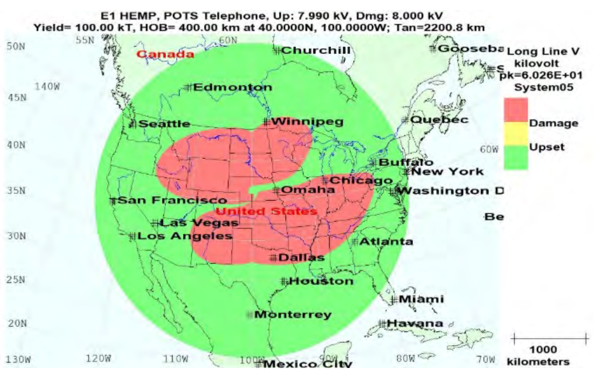


Figure 45. Devastating POTS telephone damage with 0 dB protection

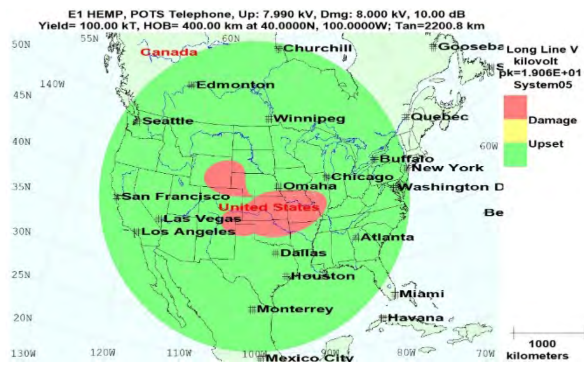


Figure 46. Significantly reduced damage with 10 dB protection

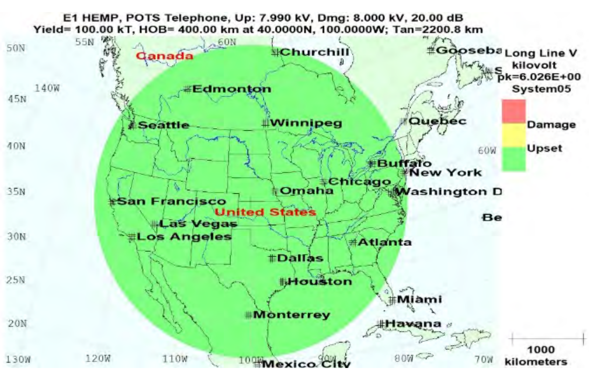


Figure 47. No POTS telephone damage with 20 dB protection

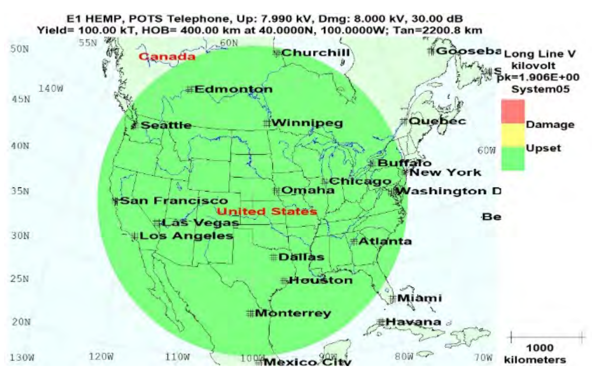


Figure 48. No POTS telephone damage with 30 dB protection

Cordless Telephone Model Results

As shown in Figure 49 through Figure 52 below, the amount of damage to a cordless phone base could be substantially reduced or even eliminated with 20 dB or 30 dB protection. In all cases, the damage was due to the AC/DC power adapter failing (not the handset).

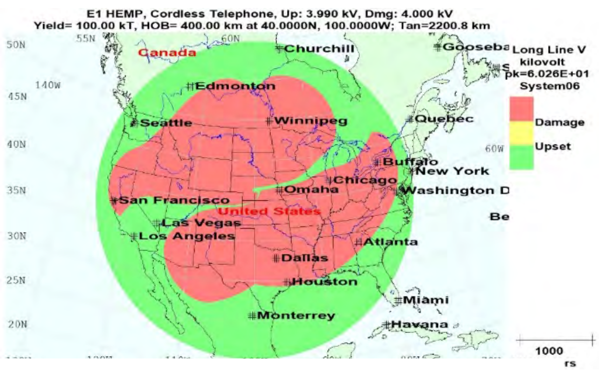


Figure 49. Devastating cordless telephone AC/DC adapter damage with 0 dB protection

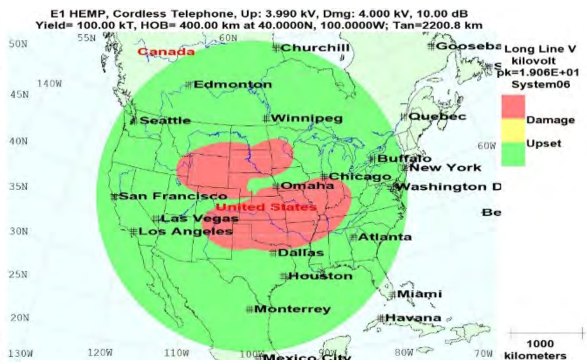


Figure 50. Significantly reduced damage, but still huge with 10 dB protection

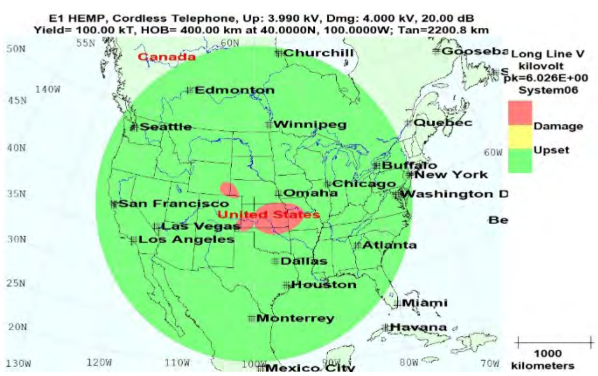


Figure 51. Only localized damage to cordless telephones with 20 dB protection

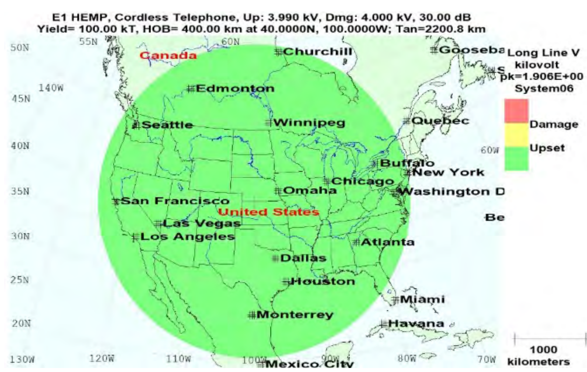


Figure 52. No cordless telephone damage with 30 dB protection

8. NEXT STEPS

There are several next steps planned for this document to better support the DHS released "*Strategy for Protecting and Preparing the Homeland against Threats of Electromagnetic Pulse and Geomagnetic Disturbances*" document released on October 9, 2018. In particular, these next steps include the following with references to the DHS EMP Strategy in parentheses:

- Review additional "intra-Departmental, Federal interagency, and civilian scientific research on EMP and GMD and their effects on critical infrastructure." (1.2)
- Include both more real world test data and additional prior research on the effects of EMP on critical infrastructure systems. (1.2.1)
- List EMP knowledge gaps and prioritize potential research opportunities that could reduce vulnerabilities in a cost-effective manner. (1.2.1, 1.2.2, 1.2.3, and 2.2.3)
- Discuss additional EMP-GMD response and recovery mechanisms, particularly guidelines that can help make the critical infrastructure operational again or help technically mitigate the damage. (2.2.2)
- Further prioritize the critical infrastructure operational resilience activities based on risk management principles. (2.3.1, 2.3.3 , 3.1.1, and p. 6 of 3rd Core Principle)
- "Identify the technological advances likely to significantly enhance resilience or reduce vulnerability of critical infrastructure to electromagnetic incidents." (2.3)

Some of the above next steps are iterative by nature and the timeframe to complete each of the above next steps will vary, which will likely lead to one or more incremental releases of this document.

Appendix A. EMP PROTECTION TEST AND ACCEPTANCE CRITERIA

From Reference 1. See notes at end of Table A-3.

Table A-1. Injected Pulse Characteristics

Class of Electrical POE	Pulsed Current Injection Requirements[1]			
	Type of Injection	Peak Short-Ckt Current (A)	Risetime (s)	FWHM[2] (s)
Commercial Power Lines (Intersite)				
Short Pulse	Common mode	5,000	$\leq 2\times10^{-8}$	5×10^{-7}–5.5×10^{-7}
Short Pulse	Wire-to-ground	2,500	$\leq 2\times10^{-8}$	5×10^{-7}–5.5×10^{-7}
Intermediate Pulse	Common mode	250	$\leq 1.5\times10^{-6}$	3×10^{-3}–$5\text{x}10^{-3}$
Intermediate Pulse	Wire-to-ground	250	$\leq 1.5\times10^{-6}$	3×10^{-3}–$5\text{x}10^{-3}$
Long Pulse	Common mode	[3]1,000	≤ 0.2	[3]20–25
Long Pulse	Wire-to-ground	[3]1,000	≤ 0.2	[3]20–25
Other Power Lines (Intrasite)				
Unrestricted Lines				
Short Pulse	Common mode	5,000	$\leq 2\times10^{-8}$	5×10^{-7}–5.5×10^{-7}
Short Pulse	Wire-to-ground	2,500	$\leq 2\times10^{-8}$	5×10^{-7}–5.5×10^{-7}
Restricted Lines				
Short Pulse	Common mode	800	$\leq 2\times10^{-8}$	5×10^{-7}–5.5×10^{-7}
Short Pulse	Wire-to-ground	[4]$800/\sqrt{N}$ or 500	$\leq 2\times10^{-8}$	5×10^{-7}–5.5×10^{-7}
Audio/Data Lines (Intersite)				
Short Pulse	Common mode	5,000	$\leq 2\times10^{-8}$	5×10^{-7}–5.5×10^{-7}
Short Pulse	Wire-to-ground	[4]$5{,}000/\sqrt{N}$ or 500	$\leq 2\times10^{-8}$	5×10^{-7}–5.5×10^{-7}
Intermediate Pulse	Common mode	250	$\leq 1.5\times10^{-6}$	3×10^{-3}–$5\text{x}10^{-3}$
Intermediate Pulse	Wire-to-ground	250	$\leq 1.5\times10^{-6}$	3×10^{-3}–$5\text{x}10^{-3}$
Long Pulse	Common mode	[3]1,000	≤ 0.2	[3]20–25
Long Pulse	Wire-to-ground	[3]1,000	≤ 0.2	[3]20–25
Control/Signal Lines (Intrasite)				
Unrestricted Low-Voltage Lines[5]				
Short Pulse	Common mode	5,000	$\leq 2\times10^{-8}$	5×10^{-7}–5.5×10^{-7}
Short Pulse	Wire-to-ground	[4]$5{,}000/\sqrt{N}$ or 500	$\leq 2\times10^{-8}$	5×10^{-7}–5.5×10^{-7}
Unrestricted High-Voltage Lines[5]				
Short Pulse	Common mode	5,000	$\leq 2\times10^{-8}$	5×10^{-7}–5.5×10^{-7}
Short Pulse	Wire-to-ground	[4]$5{,}000/\sqrt{N}$ or 500	$\leq 2\times10^{-8}$	5×10^{-7}–5.5×10^{-7}
Restricted Lines				
Short Pulse	Common-mode	800	$\leq 2\times10^{-8}$	5×10^{-7}–5.5×10^{-7}
Short Pulse	Wire-to-ground	[4]$800/\sqrt{N}$ or 500	$\leq 2\times10^{-8}$	5×10^{-7}–5.5×10^{-7}
Conduit Shields				
Signal and Low Current Power[6]				
Buried[7]	Conduit-to-gnd	800	$\leq 2\times10^{-8}$	5×10^{-7}–5.5×10^{-7}
Nonburied	Conduit-to-gnd	5,000	$\leq 2\times10^{-8}$	5×10^{-7}–5.5×10^{-7}
Medium Current Power[6]				
Buried[7]	Conduit-to-gnd	800	$\leq 2\times10^{-8}$	5×10^{-7}–5.5×10^{-7}
Nonburied	Conduit-to-gnd	5,000	$\leq 2\times10^{-8}$	5×10^{-7}–5.5×10^{-7}
High Current Power[6]				
Buried[7]	Conduit-to-gnd	800	$\leq 2\times10^{-8}$	5×10^{-7}–5.5×10^{-7}
Nonburied	Conduit-to-gnd	5,000	$\leq 2\times10^{-8}$	5×10^{-7}–5.5×10^{-7}

From Reference 1. See notes at end of Table A-3.

Table A-2. Residual internal stress limits for classes of electrical POEs

Class of Electrical POE	Residual Internal Stress Limits			
	Type of Measurement	Peak Response Current (A)	Peak Rate of Rise (A/s)	Root Action ($A - \sqrt{s}$)
Commercial Power Lines (Intersite)				
Short Pulse	Bulk current	≤ 10	$\leq 1\times10^{7}$	$\leq 1.6\times10^{-1}$
Short Pulse	Wire current	≤ 10	$\leq 1\times10^{7}$	$\leq 1.6\times10^{-1}$
Intermediate Pulse	Bulk current	No damage or performance degradation		
Intermediate Pulse	Wire current	No damage or performance degradation		
Long Pulse	Bulk current	No damage or performance degradation		
Long Pulse	Wire current	No damage or performance degradation		
Other Power Lines (Intrasite)				
Short Pulse	Bulk current	≤ 10	$\leq 1\times10^{7}$	$\leq 1.6\times10^{-1}$
Short Pulse	Wire current	≤ 10	$\leq 1\times10^{7}$	$\leq 1.6\times10^{-1}$
Audio/Data Lines (Intersite)				
Short Pulse	Bulk current	≤ 0.1	$\leq 1\times10^{7}$	$\leq 1.6\times10^{-3}$
Short Pulse	Wire current	≤ 0.1	$\leq 1\times10^{7}$	$\leq 1.6\times10^{-3}$
Intermediate Pulse	Bulk current	No damage or performance degradation		
Intermediate Pulse	Wire current	No damage or performance degradation		
Long Pulse	Bulk current	No damage or performance degradation		
Long Pulse	Wire current	No damage or performance degradation		
Control/Signal Lines (Intrasite)				
Low-Voltage Lines[5]				
Short Pulse	Bulk current	≤ 0.1	$\leq 1\times10^{7}$	$\leq 1.6\times10^{-3}$
Short Pulse	Wire current	≤ 0.1	$\leq 1\times10^{7}$	$\leq 1.6\times10^{-3}$
High-Voltage Lines[5]				
Short Pulse	Bulk current	≤ 1.0	$\leq 1\times10^{7}$	$\leq 1.6\times10^{-2}$
Short Pulse	Wire current	≤ 1.0	$\leq 1\times10^{7}$	$\leq 1.6\times10^{-2}$
Conduit Shields				
Signal and Low Current Power[6]				
Buried[7]	Bulk current	≤ 0.1	$\leq 1\times10^{7}$	$\leq 1.6\times10^{-3}$
Nonburied	Bulk current	≤ 0.1	$\leq 1\times10^{7}$	$\leq 1.6\times10^{-3}$
Medium Current Power[6]				
Buried[7]	Bulk current	≤ 1.0	$\leq 1\times10^{7}$	$\leq 1.6\times10^{-2}$
Nonburied	Bulk current	≤ 1.0	$\leq 1\times10^{7}$	$\leq 1.6\times10^{-2}$
High Current Power[6]				
Buried[7]	Bulk current	≤ 10	$\leq 1\times10^{7}$	$\leq 1.6\times10^{-1}$
Nonburied	Bulk current	≤ 10	$\leq 1\times10^{7}$	$\leq 1.6\times10^{-1}$

Table A-3. Injected pulse characteristics and residual internal stress limits for antenna POE

Class of Electrical POE	Pulsed Current Injection Requirements[8]				
	Type of Injection	Dominant Response Frequency[9] (MHz)	Peak Short-Circuit Current (A)	Risetime (s)	FWHM[2] (s)
RF antenna line shield					
Buried[7]	Shield-to-gnd	Not applicable	800	$\leq 2\times10^{-8}$	5×10^{-7}–5.5×10^{-7}
Nonburied	Shield-to-gnd	Not applicable	5,000	$\leq 2\times10^{-8}$	5×10^{-7}–5.5×10^{-7}
RF antenna line signal conductor	Wire-to-shield	≤30	Threat-level[9]	$\leq 2\times10^{-8}$	5×10^{-7}–5.5×10^{-7}
	Wire-to-shield	>30	Threat-level[9]	$\leq 5\times10^{-9}$	Variable[9]

Class of Electrical POE	Residual Internal Stress Limits			
	Type of Measurement	Peak Response Current (A)	Peak Rate of Rise (A/s)	Root Action ($A-\sqrt{s}$)
Receive only antenna line	Shield Current	≤0.1	$\leq 1\times10^{7}$	$\leq 1.6\times10^{-3}$
	Wire Current	≤0.1	No damage or performance degradation	
Transmit and receive antenna line	Shield Current	≤0.1	$\leq 1\times10^{7}$	$\leq 1.6\times10^{-3}$
	Wire Current	≤1.0	No damage or performance degradation	

Notes for Tables A-1, A-2 and A-3.

1 Pulse current injection requirements are in terms of Norton equivalent sources. Short-circuit currents are double exponential waveshapes. Source impedances are ≥ 60 Ω for the short pulse, ≥ 10 Ω for the intermediate pulse, and ≥ 5 Ω for the long pulse.

2 FWHM is pulse full-width at half-maximum amplitude.

3 The long pulse peak short-circuit current (1,000 A) and FWHM (20-25 s) are design objectives. Any double exponential waveform with peak short-circuit current ≥ 200 A, risetime ≤ 0.2 s, and peak current x FWHM product ≥ 2×10^4 A-s satisfies the minimum requirement.

4 Whichever is larger. *N* is the number of penetrating conductors in the cable.

5 Low-voltage control/signal lines are those with maximum operating voltage < 90 V. High-voltage control/signal lines are those with maximum operating voltage ≥ 90 V.

6 High-current power lines have maximum operating current > 10 A. Medium-current power lines have maximum operating current between 1 A and 10 A. Low-current power lines have maximum operating current < 1 A.

7 An antenna shield is considered buried when it terminates at a buried antenna and less than 1 m (3.3 ft.) of its total length is not covered by earth or concrete fill. A conduit is considered buried when it connects two protected volumes and less than 1 m (3.3 ft.) of its total length is not covered by earth or concrete fill.

8 Pulse current injection requirements are in terms of Norton equivalent sources. The short pulse generator, with a source impedance ≥ 60 Ω, is used for shield-to-ground injections and for wire-to-shield injections at dominant response frequencies ≤ 30 MHz. A charge line pulser, with a source impedance ≥ 50 Ω, is used for wire-to-shield injections at dominant response frequencies > 30 MHz.

9 The dominant response frequency (or frequencies) and threat-level peak short-circuit current are determined from extrapolated coupling measurements. The length l of the charge line of the charge line pulser is the quarter-wavelength of the dominant response frequency: $l = 0.25\, c/f$, where $c = 3 \times 10^8$ m/s and f is frequency in Hz.

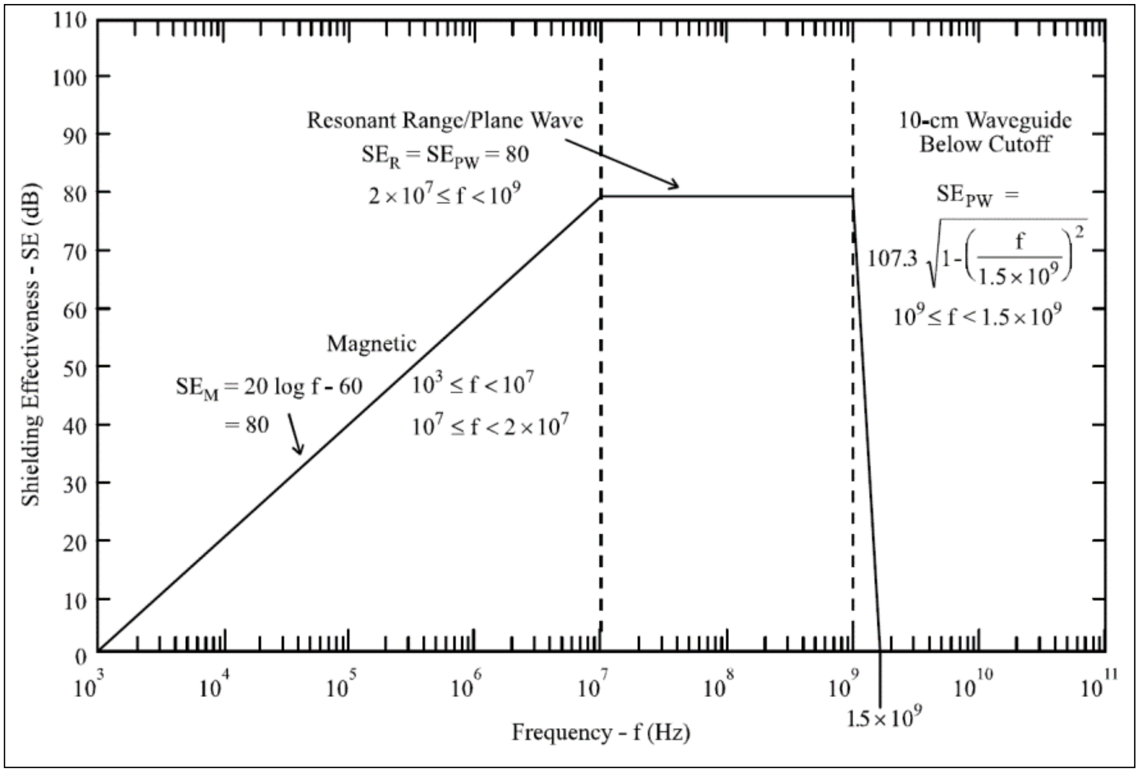


Figure A-1. HEMP Shielding Effectiveness Requirement

Appendix B. EMP PROTECTION VENDORS AND SERVICES

This appendix is intended to familiarize those considering EMP protection options with the types of solutions currently available in the U.S. marketplace. The companies listed offer specialized products or services that address the threats from HEMP, radiated SREMP, and IEMI. This list is not a comprehensive source listing of companies who offer EMP related products and services. If you are a business who offers related products or services and would like to be included in future releases of this document, please contact Kevin.Briggs@hq.dhs.gov and include, where possible, any independent testing data that verifies product claims and customer references from previous work, if applicable.

Disclaimer: **Reference to any specific company's product or service herein does not represent an endorsement by the Department of Homeland Security (DHS) or the NCC as to the effectiveness or adequacy of any product or service, nor should this Appendix be considered an approved or recommended vendor list. Use of any vendor product or service listed in this Appendix should be based entirely on the buyer's own analysis of alternatives and research of vendor capabilities.**

EMP Protection Levels

Achieving cost effective protection from EM threats requires a "defense-in-depth" approach to progressively increase equipment immunity and resiliency and ultimately harden critical systems and infrastructures. It is not necessary or financially feasible to harden all systems and infrastructure to survive and operate through an EMP event. System prioritization and planning for an EMP event should be an integral part of each organization's continuity and contingency planning efforts.

DHS EMP Protection Level 1 generally uses manual procedures to isolate off-line equipment from EM threats and adding ferrite devices to cables to attenuate unwanted HF cable signals. These are intended to be added by existing site personnel for minimal cost. Level 2 measures focus on increasing resiliency by installing active and passive components to mitigate the conductive effects that threaten on-line systems. Level 2 measures can be performed by skilled in-house personnel or obtained through contracted services.

Levels 3 and 4 measures address the radiated effects of EM threats by installing layers of EM shielding around prioritized systems to harden operations. Shielding a new or existing facility is typically performed by an experienced contractor who will design, engineer, install and test the solution to meet the unique site requirements and performance specifications.

EMP Protection Level 1

Level 1 protection measures are the first line of defense in protecting essential equipment from the conductive and radiated effects of EM threats. These manual isolation procedures can protect off-line and spare equipment from the initial EM effects for little to no cost. Simply unplugging the cables from equipment that is only required for continuity or backup purposes will create physical and electrical separation and provide protection from EMP induced currents.

Add ferrite clip-on beads to equipment cables that must remain connected and on-line. To best shield against the radiated effects of EMP, off-line equipment must be stored behind protective metal barriers. Placing larger equipment in a Faraday case and storing it in a steel constructed warehouse is preferable to on-the-shelf in an office or operations building.

Faraday Bags

Faraday bags are the most basic type of shielding available and are widely available online. They are primarily designed to protect small electronics such as cell phones, key fobs, tablets, laptops, and handheld radios from EMI. The frequency range covered is dependent upon the Faraday bag, but some work as low as 10 MHz and others shield as high as 18 GHz. Most Faraday bags at least cover the pre-5G cellular range as well as the frequency ranges for RFID (315 MHz in North America), the GPS bands, and many cover Wi-Fi bands (the higher Wi-Fi frequency is at 5.9 GHz).

Bag size, construction and the level of protection can vary greatly although one bag should be sufficient for most Level 1 and Level 2 protection situations. Nesting within multiple bags or storing the bags in a metal container to create more layers will increase the level of protection. Be aware that many bags marketed as Faraday bags are designed for evidence collection and may only provide electrostatic protection. Prices range from a few dollars for small disposable bags to a couple or few hundred dollars for backpacks or heavy-duty duffel bags. Also, while the material in some bags can provide high levels of EM attenuation, often the closing method for the bags are the main leakage point. Look for bags, which indicate that the entire bag has been tested.

Vendors selling Faraday bags can easily be found using a search engine or popular general online shopping sites (e.g., Amazon, Walmart). Specific vendors include (see Disclaimer on page B-1):

Defender Shield: www.defendershield.com

Faraday Defense: https://faradaydefense.com/

Mission Darkness: (MOS Equipment) https://mosequipment.com/

Faraday Containers

If portability is required, a Faraday **container** offers a more durable solution than a Faraday **bag**. These rigid containers are suitable for transport and can be stacked to store equipment off-line until needed. Containers range in size from briefcase-sized for phones and laptops to suitcase size containers and transit cases for large components or multiple devices. Prices typically range from a few dollars to several hundred dollars although less expensive and more expensive containers are available. Custom engineered cases can cost between $10K-$40K with deployable system solutions offering onboard power, interfaces and thermal management ranging from $40K to over $100K.

Vendors selling Faraday containers include (see Disclaimer at the beginning of this Appendix):

Conductive Composites (www.conductivecomposites.com/SystemSolutions) offers a line of injection molded and laminated electronics enclosures that provides shielding performance across a broad range of frequencies that meets MIL STD 461, 464 and 188-125 requirements.

EMP Engineering (http://empengineering.com/storage-faraday-boxes) makes a line of welded aluminum Faraday cases ranging from several hundred dollars to over a thousand ($787 - $1171 dollars in July 2018).

Ferrite Cores/Beads

Ferrite beads are widely available online and cost just a few dollars each. Normally more than one bead is required to achieve significant attenuation (~10 dB). They can be clamped on, snapped on or slipped over cables near the equipment end to attenuate unwanted high-frequency cable signals. Type 61 (HF) ferrites made of Nickel Zinc are recommended. These are designed for inductive applications to attenuate interfering pulses from 200 MHz to 2 GHz. They can be added to existing cables or purchased with ferrites pre-built in common cable types. A wholesale distributor such as **Digi-Key Electronics (**http://www.digikey.com/product-search/en/filters/ferrite-cores-cables-and-wiring/3408554?WT.srch=1) allows for filtering any combination of sizes and specifications to fit requirements (see Disclaimer at the beginning of this Appendix).

Other suppliers include:

Amindon Corporation: http://www.amidoncorp.com/61-material-ferrite-toroids/

API Delevan: http://www.delevan.com/

Bourns: https://www.bourns.com/

Fair-Rite Products: https://www.fair-rite.com/

Kemet: http://www.kemet.com/Ferrite_Products

Laird: https://www.lairdtech.com/

Leadertech: https://leadertechinc.com/

muRata: https://www.murata.com/en-us/products/emc/ferrite

Palomar Engineers: http://palomar-engineers.com/ferrite-products

TDK: tdk.com or https://product.tdk.com/info/en/products/ferrite/index.html

Toshiba: Toshiba.com or https://toshiba.semicon-storage.com/us/product/amorphous/high-permeability-cores.html

Wurth: https://www.wuerth.com or https://www.we-online.com/web/en/wuerth_elektronik/start.php

EMP Protection Level 2

Level 2 adds active and passive components designed to limit the conductive effects of EMP while essential systems remain operational and connected to external power and network connections. The cost to add Level 2 measures to an existing facility is relatively low proportional to the quantity of power and communications connections that must be protected.

Surge Suppressors and Filters

Many commercially available power strips have surge protection built in. These should be used to protect all essential equipment and must have response characteristics as discussed in Section 2 "*EMP PROTECTION AND RESILIENCE CONSIDERATIONS"* (see Disclaimer at the beginning of this Appendix):

Alpha Delta https://www.alphadeltacom.com/ Transi-Trap ATT3G50 coaxial surge protectors have replaceable GDT elements for different power levels. A Transi-Trap has an N female connector on both ends (no suffix) or SO-239 UHF female connectors (U suffix). They are available for either stud mounting (no suffix) or bulkhead mounting (B suffix). One of the UHF connectors is 1.5 inches long with a UBXL suffix. The standard version of the ATT3G50 is suitable for protecting a 125-watt transmitter, and the HP version is suitable for protecting a 1 kW transmitter. Transmitters operating at other power levels can be better protected by selecting GDTs with different voltages.

Alpha-Delta uses standard 6x8-mm (height x diameter) GDTs which are available from GDT manufacturers/distributors in voltages of 90, 230, 350, 470, 600, 900, 1000 and higher for less than $3 each. Alpha-Delta uses GDTs from: EPCOS (https://en.tdk.eu/arresters) and Littelfuse (http://www.littelfuse.com/~/media/electronics/product_catalogs/littelfuse_gdt_catalog.pdf.pdf). Littelfuse also has a variety of catalogs featuring their other surge protection devices (e.g., datacenter lines) at http://electronicscatalogs.littelfuse.com/app.php?RelId=6.7.0.18.4

Alpha-Delta stocks only the 350 and 1,000-volt rating GDTs, suitable for 125 and 1,000-watts, respectively, based on a VSWR of 3:1 or better (lower). VSWR is a function of the impedance mismatch between the radio (which is almost always 50-ohms) and the antenna impedance, which can vary widely as a function of frequency. If your worst (highest) VSWR is more or less than 3:1, different voltage GDTs should be used. The GDT voltage is a concern because the voltage across the GDT increases with transmitter power and antenna VSWR, which can cause the GDTs to trigger and wear out prematurely if the GDT voltage-rating is too low. Although lower voltage-rating GDTs provide better protection for the radio equipment, a GDT with a high enough voltage-rating needs to be used so it won't be triggered from normal operating voltages.

APC's ProtectNet (http://www.apc.com/products/family/index.cfm?id=145&ISOCountryCode=us) line of surge protection devices provide protection against power transients traveling over telecommunications lines and meet rating requirements to be effective for EMP types of transients. These types of devices should be used to protect all essential equipment at each power, phone and network connection. Its SurgeArrest protectors will alert the user if they are damaged or compromised. Prices range from $15 to $40 dollars per device.
http://www.apc.com/products/family/index.cfm?id=145&ISOCountryCode=us

Emprimus (www.emprimus.com) is a research and development company partnered with ABB, a global leader in power and automation technologies, working with major utilities to produce effective products to protect the electric power grid (both AC and HVDC) against stray DC currents, Solar Storm/Geomagnetic Induced Currents (GIC), EMP including Nuclear EMP (E3 Pulse), and Intentional Electromagnetic Interference (IEMI) caused by Radio Frequency Weapons. The SolidGround™ neutral blocker is a solution to help protect the electric power grid from stray DC, Solar Storms (GMD) and Nuclear EMP E3.

ETS Lindgren (www.ets-lindgren.com) is an international manufacturer of components and systems that measure, shield and control electromagnetic and acoustic energy. Their Red Edge Technology line of EMP rated power filters is designed to MIL-STD-188-125 for both TEMPEST and non-TEMPEST applications.

Huber+Suhner (http://empselector.hubersuhner.com/) makes a line of EMP coaxial, data and power components. Their EMP Protector Tool Box helps you select the correct EMP devices to meet your requirements.

The H+S series of N-type connector inline GDT protector housings 3401.17.A and 3402.17.A, have replaceable GDT elements for different voltage levels.

Huber+Suhner (H+S) has a very helpful on-line calculator for finding the recommended GDT for various VSWRs and power levels at http://empselector.hubersuhner.com/gdtcalculator/index.php. The H+S on-line calculator determines the voltage for specifying a GDT when the power and VSWR are known. The VSWR should be measured at the point where the RF surge protector will be located. The VSWR should also be measured at whatever operating frequency produces the highest (worst) VSWR. Using the H+S on-line calculator, insert the “RF CW Power in W” (Watts), the “DC Supply Voltage” (normally zero), the maximum antenna “VSWR” (normally at least 3), and the “Impedance Z” (normally 50), and then click on the “Calculate” button.

Using the H+S online calculator for three typical powers of 100, 400, and 1000 watts (with a 3:1 VSWR) results in the following required GDT voltage ratings:

- 100 watts has a peak voltage of 150 volts, which x1.5 = 225 volts – requires a 350-volt GDT.
- 400 watts has a peak voltage of 300 volts, which x1.5 = 450 volts – requires a 600-volt GDT.
- 1,000 watts has a peak voltage of 474 volts, which x1.5 = 712 volts – requires a 900-volt GDT.

There are two reasons why the required GDT voltages in the above three examples are so much higher than the calculated peak voltages: (1) The on-line calculator multiplies the calculated peak voltage by 1.5 to provide a safety factor against false triggering, and (2) GDTs have nominal voltages specified with a 15 or 20% tolerance. Therefore, the calculated tolerance voltage must be subtracted from the nominal voltage to determine the GDT’s minimum striking voltage. That is, the 350-volt GDT may strike at only 298 volts, the 600-volt GDT may strike at only 510 volts, and the 900-volt GDT may strike at only 765 volts.

Going into more detail for the last example above, a 900-volt GDT is used despite a calculated striking voltage of 712 volts (to protect an amplifier with an output power of 1,000 watts) because it might strike at a voltage as low as 765 volts with its 15% tolerance. This means that the voltage induced in the antenna lead from a lightning strike or EMP will reach at least 765 volts before the GDT fires. But the induced voltage could go up into the thousands of volts without the surge protector. Also, a VSWR of 3 may only be nominal: Many VSWRs will be higher, requiring GDTs with even higher voltage ratings. Disregarding the safety factor and the tolerance would result in selecting a GDT with a striking voltage that is too low, compounding false triggering problems.

NexTek (http://nextek.com) was founded in 1986 to supply EMI/EMC solutions to the electronics industry. It designs and manufactures its products in the USA for the communications, aviation, computer, military, and medical electronic industries. The core product portfolio is based upon two basic product types; coaxial RF protector designs using gas discharge, quarter-wave, and filter technology, and the high-current feedthrough C-type EMI/RFI filters. The industry-leading coaxial arrestor product portfolio delivers both superior performance and value for wireless communications, telecom, WiMAX, Wi-Fi, aviation, military, and homeland security applications. The filter solutions provide similarly class-leading performance and compact form factors for mobile power system, industrial laser, medical device, and aerospace applications.

PolyPhaser, an Infinite Company, has several lines of GDT type coaxial line filters that can provide EMP protection. The PolyPhaser IS-50NX-C0 (http://www.polyphaser.com/products/rf-surge-protection/is-50nx-c0) limits at 600 Volts (+/- 20%) to protect transceivers with transmitter output powers of 400 watts (with a 3:1 VSWR as was assumed previously with the H+S GDTs).

The PolyPhaser IS-NEMP-C0 has a lower turn-on voltage limiting at 330 Volts to provide better protection against HEMP damage for a 100-watt transceiver.

Both of the above PolyPhaser protectors have female N connectors on both ends, but they are also available with one female and one male N connector, or with UHF connectors instead (with different part numbers). Both of these protectors contain capacitors in series with their center pins, so they cannot pass a DC voltage (which some installations require for powering a remote antenna tuner or switch). Both protectors contain non-replaceable GDTs.

See www.polyphaser.com for more information.

Transtector, an Infinite Company, (https://www.transtector.com/) product offering includes AC, DC, high speed data and signal protection, EMP/EMI filters, power conditioners, UPS and power distribution units. Their products include a 6 outlet AC Surge Protection device *SL-V Surge Cord P/N 1101-058*, which uses a silicon avalanche suppression diode and has a published surge suppression response time of <5 ns. Some of its products have been tested to MIL-STD-188-125 E1 and E2 environments, such as the AC EMP product *APEC IMAX HT*, which is applicable to 120/208 VAC, 240 VAC, and 120 VAC applications.

Other vendors supplying EMP rated filters and suppressors include:

Captor Corporation – http://www.captorcorp.com/index.html

EMP Shield – www.myempshield.com/compliance-tests/ www.myempshield.com

Fischer Custom Communications – http://www.fischercc.com/transient-protection-devices/

Glenair EMI/EMP Filter Connectors and TVS Devices - www.glenair.com/filter/index.htm

LCR Electronics (under Astrodyne TDI) **–** http://www.lcr-inc.com/emi-rfi-filters/

Technical Sales Solutions, LLC – http://mytechnicalsalessolutions.com

Double Conversion On-line and Line Interactive UPS

A true on-line, double-conversion type UPS or a high quality line interactive UPS is recommended for protecting equipment from EMP. Double Conversion On-Line UPS provide continuous output power from the battery backup through an inverter and not directly from the AC power source. This design provides isolation from transients on the AC power line and continual power without transfer. A high quality line interactive unit is often used for lower power applications (a few pieces of equipment or a rack) and it uses a combination of surge suppression, line noise filtering, and switchover to a battery to prevent damage to sensitive equipment.

Double Conversion On-line UPS are available from (see Disclaimer at the beginning of this Appendix):

APC – http://www.apc.com/products/family/index.cfm?id=163

CyberPower – http://www.cyberpowersystems.com/products/tools/selector/ups

Dell – www.dell.com

Emerson-Liebert (a business of Vertiv) **–** http://www.emersonnetworkpower.com/en-US/Products/ACPower/Pages/default.aspx or https://www.vertivco.com/en-us/products-catalog/critical-power/uninterruptible-power-supplies-ups/

Tripp-Lite – http://www.tripplite.com/products/ups-systems~11

EMP Protection Levels 3 and 4

The next two levels of protective measures involve adding protective metallic shielding to the operating environment. These solutions can range from a single equipment rack, to an operations room, to an entire building or facility. Level 3 is designed and installed to meet commercial IEC standards. Level 3 protection can be achieved with bolt-together shielded panels around all six-sides of a room or an equipment rack or by relocating essential equipment into a pre-built shipping container-size shielded enclosure. Nesting equipment behind multiple barriers has an additive effect. For example, placing essential equipment radios in a moderately shielded container or room in the middle of the basement of a building may be as good as placing the equipment near the window of a building in a shielded container.

Level 4 increases the degree of protection to the higher MIL-STD-188-125-1. Level 4 requires electrically bonded and tested joints. All penetrations into the shielded enclosure must be bonded and grounded. Food, fuel and supplies should be provisioned to operate in an EMP environment for up to 30 days.

Shielded Enclosures, EMP/GIC Testing, Engineering and Consulting Services

Building a shielded enclosure into a new or existing facility is the traditional proven method of EM hardening. Many companies with EMP hardening experience support the Department of Defense

(DoD). They are very experienced in designing, engineering, installing and testing RF shielded enclosures to meet MIL-STD-188-125-1 and -2 applications (note: see Disclaimer at the beginning of this Appendix). As more industries begin to address EMP threats, companies will offer more solutions for commercial and civil applications with different site requirements and performance specifications that the military specifications do not cover.

Advanced Fusion Systems, LLC (AFS), (203-270-9700) is a division of Stratum (http://stratum-technologies.com/). Its products include an EMI coating.

ARMAG Corporation (www.armagcorp.com) Armag Corporation has a rich history of client partnership, particularly in U.S. Defense and Government, in developing and manufacturing secure facilities to provide uncompromised physical security. Armag designs and manufactures prefabricated steel, both large and small, to protect against HEMP, IEMI, GMD, and a broad spectrum of threats. Armag incorporates over forty years of experience in consultation with the client to provide solutions that meet their specific requirements. ARMAG has successfully produced and provided third party testing of facilities in order to certify RF Shielding protection in accordance with MIL-STD-188-125-2 and NSA 94-106.

ATEC Industries (http://www.atecindustries.com/) ATEC Industries is a full-service general contractor headquartered in Elkridge, Maryland specializing in the design/build delivery of RF shielded facilities. ATEC has the expertise to provide a turnkey solution for both new construction and renovations of varying size and scope. Since 1987 ATEC Industries has been continuously involved in the design, fabrication, construction and testing of RF shielded facilities. ATEC specializes in EM/RFI shielding for governmental, military and medical facilities, both as stand-alone projects and as part of larger integrated construction projects. RF attenuation requirements have varied in the magnetic and electric fields from 50 dB at 1 kHz to 100 dB at 100 KHz to 100 dB at 50 MHz and microwave performance of 115 dB at 18 GHz to 80 dB at 50 GHz.

Braden Shielding Systems, LLC (www.bradenshielding.com) designs, manufactures, integrates and tests EM shielding systems for medical, industrial and defense applications. A core competence of the company is hardening of critical infrastructure facilities for protection against the damaging effects of EMP, IEMI and GMD.

For more than 30 years, Braden Shielding has manufactured a comprehensive line of proven RF shielding products at its facility in Tulsa, OK. The company provides a number of high-performance shielding systems and a broad range of RF shielded facility penetrations designed specifically to address every Point of Entry (POE) to the EM shield, such as shielded doors, power/signal/data and fiber optic filters, waveguide penetrations for mechanical, fire protection and HVAC systems, as well as custom POE's for hardness critical items outside the main shielded barrier, e.g., cooling towers, generators and telecommunications.

Braden's staff of experienced design, engineering, fabrication, installation, testing and project management personnel deliver turn-key RF shielding solutions for any shielding project. The Company utilizes the latest 3-D design and Building Information Modeling (BIM) technology and offers comprehensive design support for: Hardened facility planning, architectural/structural/electrical and mechanical design integration, special protective measures and hardness maintenance/hardness surveillance.

CenterPoint Energy (www.centerpointenergy.com) CenterPoint Energy embarked on an initiative to identify an effective, cost efficient solution for High-Power Electromagnetic (EM) mitigation for new and retrofit installations. The focus of mitigation efforts was substation assets used for the protection and control of the power delivery network. The design basis required the identified electromagnetic protection not compromise the reliability of existing substation functions, result in minimal increases to maintenance costs, and avoid significant changes in normal operating procedures. The development of a solution was achieved in 2018 and is rapidly progressing to the field pilot phase. The practical application of EM mitigation design practices in an unobtrusive method will speed the time for implementation, lower initial installation costs, and minimize ongoing maintenance. Each of the aforementioned achievements are realized while meeting the shielding effectiveness requirements of MIL-188-125.

The EM module will be installed as a backup protection and control system as well as online monitoring while the legacy protection and controls are still in service. If an EM event occurs, the mitigation system could be used in response. By having the system as a redundant parallel backup, the field technicians would not have to interface daily with the EM enclosure, which would help maintenance cost and ensure the integrity of the module. The field technicians also would not need to instantly change their skill sets learning the grounding, bonding and digital protection that would be required on a complete EM control house. Lastly, the EM module has enhanced data gathering and reporting capabilities for control center information which exceeds legacy systems.

From a financial perspective, the proposed solution is cost effective when compared to building a new EM control house. Based on initial estimates, a new EM control house will cost over one million dollars. The EM module enclosure would be less than 10% of a new EM control house. In conclusion, utilizing a module based approach would be a cost effective retrofit solution to harden substations for EM events. By being a redundant system, the module also provides a backup for non-EM emergencies such as control house fire or flooding and it does not intrude on present protection and control systems.

Contacts: Eric.Easton@CenterPointEnergy.com or Kevin.Bryant@CenterPointEnergy.com

EMP Engineering (http://empengineering.com/) is dedicated to the analysis, design, fabrication and installation of specialized shielding, components and systems to mitigate the harmful effects of EMP and Geomagnetic Storms on buildings, vehicles and structures world-wide. Their team of highly skilled professional engineers, project managers and fabricators have worked on military, government and private projects world-wide. Services include custom evaluations, installation and commissioning services, shielding, verification testing, hardness, hardness assurance, maintenance and surveillance and EMP solutions that integrate with Architectural, Structural, Electrical, and Mechanical Engineering services to create a secured and safe shelter / bunker environment.

They provide full service professional architectural, engineering solutions and products for hardened facilities including CBRE (chemical, biological, radiological, explosive) filters, structural engineering, blast engineering and electrical/mechanical engineering are keep designed environments effective against evolving threats now and in the future. All designs and projects are HEMP hardened per MIL-STD-188-125-2. EMP Engineering also provides portable, custom designed HEMP resistant electrical generators; communications centers and data centers fabricated in ISO shipping containers at 10, 20, 30 and 40 foot lengths. These can be ballistic/blast hardened with CRBN Air-Filtration systems.

ETS-Lindgren, an Esco Technologies Company**.** (http://www.ets-lindgren.com/). ETS-Lindgren is an innovator of systems and components for the detection, measurement and management of EM, magnetic and acoustic energy. ETS-Lindgren has the experience and expertise gained from over 70 years' experience of designing and installing more than 10,000 shielded systems worldwide. Their *RedEdge Pulse Protection* brand provides certified EMP Shielding to protect equipment and points of entry and a higher level of protection for continuous data operations with independent, uninterrupted power and utilities. Their solutions include welded steel construction, modular panel systems, doors, filters, waveguide vents and penetrations and fiber optic penetrations.

HV TECHNOLOGIES, Inc. (https://hvtechnologies.com/hv-equipment) sells (N)EMP test equipment and hardened video camera products. 8526 Virginia Meadows Drive, Manassas, VA 20109

Instant Access Networks, LLC (www.stop-emp.com) is a veteran-owned Maryland based company whose on-demand services center on the protection of mission critical facilities and infrastructure from EMP primarily through its commercial-off-the-shelf products and services. IAN has produced and tested products that provide shielding from 30 dB to 140 dB and include EMP-safe inserts that fit into standard cargo containers or trailers and can come with biological/chemical/radiological air filter systems making an all-hazards safe system. IAN also developed and tested EMP-protected solar arrays, wind turbines and diesel turbines. IAN is working with over 40 companies in its DTRA SBIR contract to provide EMP protected microgrids and communications systems and welcomes additional collaborators.

Jaxon (https://www.jaxon-em.com/) Jaxon is one of the leading High Altitude Electromagnetic Pulse (HEMP) specialty engineering firms in the country. Jaxon is a woman owned, small business located in Colorado Springs, CO. Jaxon's staff represents one of the largest and most experienced full service EMP service teams in the world. It designs, builds, tests and maintains EMP hardened structures for government and commercial clients around the world.
Jaxon has developed multiple sets of 'Next Generation' HEMP test equipment. This equipment exceeds Mil STD 188-125 requirements with leading performance characteristics. Jaxon's state of the art test equipment and engineering staff accelerate the test process and minimize mission down time requirements. Jaxon management serves on the FBI's InfraGard EMP Special Interest Group as one of their Subject Matter Experts.

Keystone Compliance (https://keystonecompliance.com/emp/) in New Castle, Pennsylvania is a full-service regulatory compliance laboratory offering solutions for nearly all EMC/EMI, environmental, ISTA-certified package and ingress protection testing requirements. Their EMC/EMI lab reportedly features five test chambers, including three anechoic/ferrite lined 3-meter chambers. Keystone Compliance has extensive experience with shielding effectiveness and EMP testing and works with manufacturers and citizens to determine if their equipment and shielding can handle natural or man-made EMPs. MIL-STD 461 contains test methods and levels to determine a device's immunity to EMP from both a radiated and conducted immunity standpoint. Radiated immunity in RS105 assesses the impact of radiated exposure. Conducted immunity in CS116 assesses the impact of damped sinusoidal transients on the cables of equipment.

L-3 Advanced Technology, Inc. (L-3 ATI), is a subsidiary of L-3 Communications. (https://www2.l3t.com/ati/solutions/redesign.htm) L-3 ATI is known worldwide for its contributions in pulsed high-voltage and high-current systems. Engineers and scientists on the EMS team have pioneered the use of most of the high-power techniques taken for granted today: oil and water dielectric pulse forming line and Blumleinpulse generators; Marx generators; intense bremsstrahlung, z-pinch, plasma radiation and X-ray sources; high-resolution x-radiography; low-jitter, multi-site switching systems, and more. The systems that it has delivered include EMP Generators and Large Area EMP Simulators.

Its ancestor **Jaycor** provided the first High-Altitude EMP (HEMP) shielding technologies to mission-critical U.S. assets. It was formed in 1975 to perform nuclear weapon effects survivability hardening and testing. The JAYCOR EME division formed by Mike Bell in Colorado Springs in 1977 became the pre-eminent underground nuclear test organization. JAYCOR - Colorado Springs worked on many major weapon system EMP hardening programs (Minuteman, Peacekeeper, B-52, B-1, B-2, Polaris, Trident, M-1 Abrams, AH-64). JAYCOR EME began hardening and testing to MIL-STD-188-125 requirements in 1999 for Air Force Space Command. They have performed over 500+ Appendix A SE, 150 Appendix B PCI and 100 Appendix C CWI test sequences since 2011. These tests have been performed on over 400 test objects ranging from facilities buried in mountains to small shielded rooms buried in large buildings to small telecommunications cabinets, from small mobile systems to 12 story fixed radar sites. They have MIL-STD-188-125 tested for AFSPC, NORTHCOM, STRATCOM, ACC, GMD, NMCC, DTRA, PM DCATS, DISA, Bechtel, Harris, and Boeing.

Shield Rite was formed in 1987 by Dr. Dave Merewether as a manufacturer of high quality RF doors and RF shielding. The Shield Rite door is a patented design installed in over 360 locations worldwide. Over the past 38 years, the main business has been the fabrication of extremely robust, HEMP Shielded doors, but has expanded to provide custom designed hardened shelters and facilities. Shield Rite was purchased by JAYCOR in mid - 2002 along with all manufacturing rights, patents for various Shield Rite technologies.

LBA Group Inc. (https://www.lbagroup.com/about) is a North Carolina Top 50 Hispanic minority-owned small business and is CVMSDC-certified. It has over 50 years of experience in providing technology and risk management for industrial and telecommunications infrastructure assets in the radio frequency and electromagnetic spaces. The group includes LBA Technology, Inc., a leading source and integrator of radio frequency systems, lightning protection, and EMC equipment for broadcast, industrial, and government users worldwide.

Little Mountain Test Facility (LMTF) is a USAF nuclear hardness simulation facility hosted by the ICBM Systems Directorate (AFNWC/NI). LMTF is a state-of-the art laboratory dedicated to simulation testing of radiation, shock and vibration, and electromagnetic effects for defense and commercial systems. Since 1974 the Boeing Company has operated and maintain LMTF. The Boeing Company operates, maintains, and upgrades all critical test capabilities at LMTF.

LMTF has over 40 years of experience in EMP harness design and testing a complete and comprehensive approach to EMP test programs. LMTF extensive experiences includes site surveys, system architecture and cost/schedule analysis to assist in a successful test program. Developing a comprehensive test plan includes addressing system topology, operational scenarios, test mythologies, test levels and points, and pass/fail criteria provides success for the basis for a successful test execution.

LMTF has a long term working relationship with ICBM and MILSTAR in performing EMP test planning/integration and test execution both per adapted EMP requirements in the systems' specifications and per MIL-STD-188-125. LMTF developed complete MIL-STD-188-125 Hardness Maintenance Hardness Surveillance (HMHS) programs for several programs.

Government customers may fund work efforts by MIPR or AF Form 616. Commercial customers work with LMTF through a Cooperative Research and Development Agreement (CRADA).

Metatech Corporation (http://www.metatechcorp.com/) is a small veteran-owned and operated business of highly-qualified scientists and engineers with broad experience in developing technically sound and innovative EM environmental solutions. Offerings include EM compatibility (EMC), protection designs and testing procedures, geomagnetic storm protection, nuclear EMP prediction for any burst situation, assessments, protection and standardization (e.g. HEMP and SREMP), and IEMI assessments, protection and standardization.

Metatech is a key contributor to EMP research in the areas of HEMP and SREMP environments and coupling and in the development of hardening and testing technologies including military standards, specifications, handbooks, and software. Major programs include SREMP testing and analyses at flash x-ray simulators, SREMP and HEMP standards development, HEMP environment and long-line coupling calculations and direct support for the design of facilities to achieve HEMP hardening. Their IEMI activities have involved performing assessments of critical infrastructure facilities, performing tests to determine the IEMI susceptibility of equipment and designing protection for the high-frequency portions of HEMP and IEMI together.

Metatech has also been a leader in participating in the development of 22 International Electrotechnical Commission (IEC) high power transient (HEMP and IEMI) protection standards for commercial applications through IEC Subcommittee 77C. These standards were developed for commercial usage and fully consider the immunity of commercial electronics to EMI in the protection methods to be used for HEMP, SREMP, IEMI and GMD disturbances.

Michael A. Caruso, (carusomi54@gmail.com, 847-226-8849) is an independent consultant based in Arizona offering consulting services for TEMPEST, SCIF, and EMP protected facility design. Mr. Caruso has been involved in the business working with both Government and private clients for over 30 years and offers an independent perspective of risk evaluations, various mitigation techniques and available vendor materials.

Noovis (www.noovis.com) provides critical communication and IT-based infrastructures which have core advantages from those currently deployed including EMP resilience, reduced energy consumption, higher bandwidth, expedited post-event recovery, and reduced CapEx and OpEx requirements. It designs, installs and integrates core IT infrastructures using passive optical networking that drastically reduces copper connectivity and its associated power requirements within communication and Information systems.

The Noovis passive, fiber-rich designs and infrastructures are intrinsically more resistant to EMP and high power microwave (HPM) attacks, thus complimenting existing risk mitigation strategies and disaster recovery plans. This is accomplished, in part, as the Noovis network topology effectively eliminates the need for access switches, within a Local Area Network (LAN) and provides an entirely passive and encrypted optical pathway for data to support communication networks, typical end user devices as well as critical Industrial Control Systems (ICS), Supervisory Controls and Data Acquisition (SCADA) networks. Noovis designed networks can run miles without the insertion of electronics versus the requirement for electronics approximately every 300 feet for many current networks. In addition, this creates substantially reduced power consumption over traditional network connectivity, decreasing the draw on microgrid generated power, allowing the reallocated energy to be used for additional critical needs.

NVIS Communications (www.nviscom.com) and its systems integration partner Pepro LLC (http://www.peprollc.com/) designs and manufactures shielded enclosures using a patented Faraday Cage technology to protect sensitive communications equipment against lightning strikes, EMP, EMI, Passive Intermodulation (PMI), and Radio Frequency Interference (RFI). Their equipment has endured many thousands of amps/joules in very rigorous industry standard testing criteria and always performed flawlessly.

Each product has the ability to be customized in order to best address a variety of potential applications and needs. These needs range from remote, difficult to reach fixed sites to small/medium and very large deployable mobile platforms all the way to very compact rapid deployable (C130/C17 transportable) kits. It provides ongoing support for all of its products as well as a strong warranty.

Scientific Applications & Research Associates (SARA), Incorporated (https://sara.com) was formed in 1989 to harness the creativity, innovation and entrepreneur spirit of engineers and scientists. SARA, Inc. is employee-owned and is managed by leaders that each has 20+ years of experience in Defense and Aerospace. SARA has nearly 100 innovative scientists and engineers doing research and development for government, military, and industrial clients. It has world-class expertise in understanding, modeling, fabricating, testing and adapting high power EM (EMP and HPM) transmission, propagation, detection, diagnosing and shielding/hardening and low signal level EM and RF sensing and signal processing, including passive EM detecting. Their “Cradle to Grave Hardening” offers architectural and engineering services for EMP subsystem/electrical subsystem integration, hardness maintenance and surveillance, EMI/EMP modeling, testing and analysis and power quality and reliability of EMP related components.

Storm Analysis Consultants (http://solarstormconsultant.com/) provides consulting and information on severe solar storms, space weather, geomagnetic storms and the electrical power grid impacts. Principal Consultant John Kappenman has been a one of the leading advisors for power companies both nationally and globally on the effect of solar storms to utilities. Storm Analysis Consultants analysis services include (1) Assessing the Space Weather Threat Environment, (2) Assessing Impact on Critical Infrastructures & Systems with PowerCast™, (3) Geomagnetic Storm NowCasting and Forecasting Technology…Tailored to the Electrical Power Industry, (4) Simulate Historic and Probable Threat Scenarios, (5) Model Complex Geologies for Accurate GIC Calculation, (6) Scalability of PowerCast to Model Large Geographic Regions and Multiple Interconnected Power Grids, (7) Assessing Space Weather Threat Environment Over Broad Ocean Regions, and (8) Modeling Geo-potentials on cross undersea cables.

TEMPEST Inc. (http://www.tempest-inc.com/ 703-836-7378) provides TEMPEST security engineering services including EMSEC, HEMP, high power microwave (HPM), and EMC testing with cybersecurity, intelligence, surveillance, and reconnaissance (ISR) systems, as well as design services in accordance with current U.S. DoD, FCC, Australian and European community requirements.

Triton Metals Inc. (http://www.tritonmetals.com/) is one of the largest metal manufacturers on the East Coast. Together with Electromagnetic Associates, LLC (www.emag-associates.com) they provide EM threat hardening, design and integration, as well as EM threat project management and construction administration/construction management services of critical infrastructure systems and life-safety systems that must work during and after a HEMP/EMP attack, such as power systems, controls, data centers, CBRN air-filtration systems, water systems, communications systems and sensor systems.

Trusted Systems (http://www.trustedsys.com/) is the pioneer and industry leader in the development and deployment of the Information Processing System Security Container or SCIF in a Box® which combines the physical strength against near blast protection and magnetic shielding of a GSA Class 5 IPS Container with EMP shielding exceeding MIL-STD-188-125. Their product line offers sizes and configurations from COOP sites, to remote critical infrastructure facilities to office and large data centers.

Page Southerland Page, Inc. (Page) (http://pagethink.com/v/iemi-hemp-protection/)
A 400-plus person architecture and engineering firm working in the U.S. and abroad offering specialty design and engineering services for Critical Infrastructure facilities. Services include planning, programming, design, commissioning and construction administration for facilities protected from HEMP, IEMI, GMD and other high- and low-frequency EM radiation. Page offers complete solutions, drawing upon experience protecting buildings and campuses owned by government, public utilities, universities, healthcare, research, petrochemical, and manufacturing companies from many types of threats: explosion, espionage, terrorism, floods and hurricanes. Page has extensive experience with EM shielding for network operations centers, embassies, data centers, and medical and biotechnology research facilities. Page can manage a critical design project from program concept to completion of construction, working with experienced partners to ensure that shielded facilities perform as designed. Page's recent portfolio includes two large (>70,000 SF), privately-owned HEMP and IEMI-shielded SCADA control and data centers, each serving markets of over 2 million customers.

Shielded Data Centers

If a hosted solution is an option for data storage, particularly for a disaster recovery environment, two companies are known to offer data center services within their EM hardened data centers (see Disclaimer at the beginning of this Appendix).

Cyber Innovation Labs (CIL) (http://www.cyberinnovationlabs.com/) is a premier provider of enterprise-class managed Infrastructure-as-a-Service (IaaS) solutions and professional services. CIL's Protected Platform as a Service (PPaaS) can provide EMP, HEMP, and IEMI shielded colocation and 100% private, single-tenant cloud solutions for delivery of mission critical applications and services to customers, at price points on par with less robust traditional offerings. CIL offers custom designed steel wall, slab-to-roof facility shell, installed with 360 degree EMP shielded protective hardened enclosure. Customer facilities include all shielding, housing, filtering and/ or hardening for all electrical, mechanical and related MEP/FP infrastructure and related subsystems. All facilities are designed, installed and tested per MIL-STD-188-125-1/2 standards.

EMP Grid Services LLC, (http://www.empgridservices.com/) is a consortium of industry-leading advanced engineering and data-center centric design/build specialists who have delivered over 10 million square feet of premier global enterprise data center facilities and represent over $1.4 B in annual revenues. Its team embody decades of experience in the data center build, commission and delivery of EMP, HEMP, IEMI and Geomagnetic Storm Protected facilities. The EMP GRID Services Team possesses core enterprise data center competencies that include:

- Master Technology Planning
- Facility Design/Build/Delivery
- Turn-key Program Management
- Infrastructure Commissioning
- Certification/Test-out
- Technical/Operational Service Support

New Approaches to EMP Protection

Hardening a new facility with welded steel can be cost prohibitive. Retrofitting an existing facility adds operational disruption to the complexity and cost of a major renovation project. Depending on your site specific mission and requirements, this may remain the best approach. However, two alternative solutions are now commercial and address EM threats for civil and commercial applications which may be more cost effective and less disruptive to current operations (see Disclaimer at the beginning of this Appendix).

1. Conductive Composites (http://www.conductivecomposites.com/) has developed and commercialized a line of multifunctional electrically conductive and EM shielding materials. In essence, they make plastics and composites conduct and shield like metals, creating a whole new realm of possibilities and opportunities for plastic and composite products. They provide cost effective shielding across a broad spectrum of EM threats for numerous types of applications. They offer multifunctional structural materials that integrate directly into typical manufacturing architectures, in addition to installation, test, and certification services.

Solutions include conductive wallpapers, paints, adhesives, stuccos, concretes, and window screens. Facilities shielded with these materials have been shown to effectively attenuate EMI/RFI as well as shield against EMP threats. A key differentiating feature is that the materials can be easily retrofitted into existing facilities as well as new construction. Conductive Composites is considered critical to the defense industrial base, with rated production contracts and classified programs, and has been awarded numerous funding phases from the Defense Production Act (DPA) Title III program.

2. Omni-Threat Structures, LLC (OTS) (www.omnithreatstructures.com) designs and builds multi-threat structures protecting against HEMP, IEMI, Emanations, Ballistic/Blast, and extreme natural disasters. OTS's proprietary construction methods have been deployed successfully to build steel and concrete structures that are threat configurable, scalable, and cost effective. The company completed the world's first shielded concrete structure that exceeded the shielding requirements of MIL-STD-188-125. OTS has successfully completed multiple specialty and hardened and shielded structures throughout the country for utility, commercial, and government clients. Notable projects include the successfully completed Vertical Electro-Magnetic Pulse Simulator (VEMPS) at Patuxent River Naval Air Station, Patuxent River, Maryland as well as a 65,000 square foot utility control and data center in Texas that incorporates commercial, hurricane-resistant, and HEMP shielded structures all in one building.

Omni-Threat Structures' team has three decades of success as a high integrity industrial GC, over a decade of success with specialized design-build hardened structures and experience in the nuclear power industry, building Fukushima Flex/Beyond Design Basis structures that meet NRC Regulatory Guide 1.76 standards. Building on a history of success, OTS now constructs EMP – IEMI shielded structures that also incorporate protection from ballistic/blast, natural threats, including Cat 5 hurricanes, EF-5 tornados, and seismic events.

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

The Department of Homeland Security (DHS) Emergency Communications Division (ECD), formerly the Office of Emergency Communications (OEC), offers priority services programs to mitigate the impacts of communications threats such as EMP and to enhance the ability of our critical national security and emergency preparedness personnel to communicate during disasters. In addition, the DHS National Coordinating Center for Communications (NCC) provides resilient backup communications services through the SHARES program.

Priority Telecommunications Services

DHS/ECD provides priority telecommunications services to support national security and emergency preparedness communications for government officials, emergency responders, critical infrastructure personnel, and industry members. The Government Emergency Telecommunications Service (GETS), Wireless Priority Service (WPS), and Telecommunications Service Priority (TSP) programs ensure key Federal, State, local, Territorial and Tribal governments, and first responder and industry organizations have communications capabilities available to support emergency response incidents.

GETS provides priority access on the landline networks:

- Increases call completion during telephone network congestion.
- Does not require special phone equipment.
- No charge for test calls or enrollment.
- Priority access, including calls to most cellular devices.

WPS provides priority access on the wireless networks:

- Increases call completion on cell phones during network congestion.
- Is an add-on feature to your cell phone.
- Can be used in conjunction with GETS to provide priority access.

FirstNet provides resilient, reliable wireless access on AT&T's network:

- Public safety receives preemption and priority access to the network with no throttling.
- FirstNet has a public safety only core that comes with FIPS 140-2 compliant end-to-end security solutions.
- The wireless coverage reaches more than 99 percent of Americans and covers 76.2 percent of the continental United States with further improvements ongoing.
- Deployables improve resiliency and can be used to extend coverage when needed.

TSP provides priority installation and repair of critical communications circuits:

- Federal Communications Commission (FCC) mandated program prioritizes restoration and installation of circuits.
- Vendors restore or install TSP circuits prior to servicing other non-TSP circuits.
- Covers voice and data circuits that support emergency operations.

Government Emergency Telecommunications Service (GETS)

During emergencies, the public telephone network can experience congestion due to increased call volumes and/or damage to communications infrastructure, hindering the ability of critical personnel to complete their calls. GETS is accessible nationwide providing authorized personnel priority access and processing during an emergency or crisis situation when the landline networks are congested and the probability of completing a call is reduced. GETS facilitated response and recovery efforts during and after events such as 9/11 and Hurricanes Katrina, Ike, and Sandy by providing over a 95 percent call completion rate.

GETS is an easy-to-use calling card service that works on both local and long distance networks; no special phones are required. Calls placed through GETS will receive priority over normal calls; however, GETS calls do not preempt calls in progress or prevent the general public's use of the telephone network. GETS allows users to communicate even during the highest levels of network congestion and also provides priority calling to cell phones during times of congestion on most major carrier networks. There is no charge to enroll in GETS or to make calls to the familiarization line. When making GETS calls, subscribers can be charged the equivalent of long distance phone rates.

Wireless Priority Service (WPS)

During emergencies, cellular networks can also become congested, hindering the ability of national security and emergency preparedness personnel to complete emergency calls on their cell phones. The WPS program is available nationwide, and is intended to provide authorized personnel priority access in an emergency or crisis situation when the cellular networks are congested and the probability of completing a call is reduced. After the April 2013 bombing at the Boston Marathon, up to 93 percent of calls placed through WPS were successfully completed, allowing critical personnel to carry out their missions to assist the public.

WPS is an easy-to-use, add-on feature that is offered by all nationwide cellular service providers. Authorized personnel can subscribe to WPS on a per-cell phone basis. Calls placed via WPS will receive priority over normal cellular calls; however, WPS calls do not preempt calls in progress or prevent the general public's use of the cellular networks. WPS subscribers are responsible for any cellular carrier charges for initial enrollment and monthly subscription, as well as per-minute usage fees.

FirstNet

FirstNet is an independent authority within the U.S. Department of Commerce (DoC). Its "mission is to deploy, operate, maintain, and improve the first high-speed, nationwide wireless broadband network dedicated to public safety."[16] The AT&T-based public safety communications platform includes all of the features found in commercial cellular networks together with several public safety related improvements:

Preemption & Priority

- First responders receive guaranteed priority and preemption versus public traffic.

- Priority levels within public safety can also be boosted during an emergency.
- FirstNet users will not be throttled even if they are on unlimited plans.

Network Security

- "The FirstNet core comes with FIPS 140-2 compliant VPN solutions, radio, transport and network core encryption, and advanced physical and logical security protocols to keep all traffic on the network protected."[17]
- FirstNet lab certifies applications and devices for public safety use although certification is not mandated.
- Certified applications can be downloaded from the FirstNet Applications Store.

Coverage

- "Wireless coverage will reach more than 99 percent of Americans, extending to 2.74 million square miles, covering 76.2 percent of the continental United States."[18]
- AT&T is improving its coverage in each state and territory per commitments made in each of its FirstNet State Plans.
- Deployables can be used to extend coverage when needed.

Resiliency

- With a dedicated FirstNet core, resiliency is significantly increased.
- Deployables are available to provide communications to FirstNet users when the network is down or when extra capacity is required.
- Hardening of the network is expected to become more of a focus once the initial requirements (e.g., coverage) have been met.

First Responders include fire, law enforcement, emergency medical services, and emergency managers by default, but also includes authorized national security personnel. These users have access to all of AT&T's commercial network. Further, as stated above, the public safety users receive priority on this network and can even preempt an existing user on any of the bands (not just the 700 MHz Band 14 that public safety was allocated). Dedicated care is also provided for additional support as needed.

Mission Critical Voice (MCV) is the only indispensable wireless voice service that is just partially implemented by FirstNet. Several MCV features have been implemented including Full Duplex, Talker Identification, Emergency Alerting, and Audio Quality. However, because the following MCV features have not been implemented, many MC personnel are continuing to use land mobile radio (LMR) in addition to cellular or FirstNet:

- **Mission Critical Push-To-Talk (MC PTT)** was finalized in Release 13 of the 3rd Generation Partnership Project (3GPP) LTE standards in March 2016 and is being implemented. FirstNet has committed to going live with this feature set by March 2019. The standard includes high availability/reliability, low latency, support for group calls and 1:1 calls, talker identification, and clear audio quality.
- **Device-to-Device Communications (D2D)** can be supported via Proximity Services (ProSE), but has not been implemented per public safety requirements where one cellular phone can contact another phone that might be 0.25 miles away without infrastructure. This is an area of research.

- **Coverage and resiliency**, including preventing EMP damage, may be better with some local LMR networks than it is with FirstNet. These are issues that need to be worked out by public safety agencies before relying upon FirstNet for MCV.

With the implementation of MC PTT, it is expected that more agencies will move their non-MC users fully onto FirstNet or Verizon and off LMR in areas where the FirstNet or Verizon coverage is adequate. Additionally, most agencies use these cellular networks for broadband data and FirstNet is continuing to move forward with features such as MC Video and MC Data, which are planned to be rolled out with 3GPP Releases 14 and 15.

Some MC users will move off LMR as well, but many agencies need more proof of the cellular networks resiliency or require improved D2D communication capabilities. Once the above have been resolved, cost concerns may continue to hinder some organizations from fully using FirstNet since they already have spent the capital for an LMR system.

The bottom line is that FirstNet's and Verizon's public safety services can help improve communications resiliency. However, until there is more evidence that these networks are resilient across many threats including EMP, it is recommended that agencies also consider other backup communications such as LMR and satellite. Agencies needing EMP Level 3 or 4 resiliency should include EMP hardened solutions using satellite communications and HF as discussed earlier in this document.

Verizon's Priority Services

To better meet the needs of public safety, Verizon has rolled out FirstNet-like features that are specific to public safety, most of which are at no additional cost. Similar to FirstNet, this includes a Public Safety Private Core (PSPC), preemption and priority, excellent coverage, and deployables (see www.verizonenterprise.com/Public-Safety). Further, Verizon is no longer throttling public safety users even if they have an unlimited data plan that states users may be throttled after they've used a specified amount of data.

Verizon is also working on MCV and D2D similarly to FirstNet and plans to offer MC PTT in 2019. Perhaps the primary differences between the Verizon and FirstNet offerings are coverage and performance that are dependent upon the local network capabilities. However, FirstNet also has an independent team that represents public safety and helps set the priority of public safety related requirements for AT&T. As part of this public safety support, this FirstNet team certifies new devices and applications for the network, which helps ensure that new features work as advertised.

Telecommunications Service Priority (TSP)

Following hurricanes, floods, earthquakes, and other natural or man-made disasters, telecommunications service vendors can experience a surge in requests to restore existing services and/or install new services. TSP authorizes national security and emergency preparedness (NS/EP) organizations to receive priority treatment for vital voice and data circuits. The TSP program provides service vendors an FCC mandate to prioritize requests by identifying those services critical to NS/EP. A TSP assignment ensures that it will receive priority attention by the service vendor before any non-TSP service.

An organization can only receive a TSP assignment if it maintains services or infrastructures that are considered critical NS/EP communications assets. TSP subscribers are subject to minimal telecommunications carrier charges for initial enrollment and monthly subscription fees.

In the aftermath of Hurricane Sandy, TSP was critical to restoration and recovery efforts by facilitating the rapid repair of damaged circuits and processing over 200 requests to install new circuits for the response community.

TSP Eligibility Criteria

The national security and emergency preparedness community spans the Federal, State, local, Tribal and Territorial governments, public safety and emergency responders, industry partners who are responsible for maintaining the Nation's critical infrastructure, and other authorized users. Organizations that rely on telecommunications on a daily basis to provide public health, maintain law and order, ensure public safety, or provide financial or utility service should enroll in these vital priority services.

Typical GETS, WPS, and TSP users are responsible for the command and control functions critical to management of, and response to, national security and emergencies. There are five (5) broad categories that serve as criteria for determining eligibility for the priority telecommunications services:

- Serve national security leadership;
- Support the national security posture and U.S. population attack warning systems;
- Support public health, safety, and maintenance of law and order activities;
- Maintain the public welfare and the national economic system; or
- Are critical to the protection of life and property or to national security and emergency preparedness and disaster recovery activities during an emergency.

TSP Enrollment Process

The first step in the enrollment process is to establish a point of contact (POC) for your organization. Many organizations already have established POCs who facilitate the enrollment process. To determine the POC and enroll in the priority services programs, please contact the **DHS Priority Telecommunications Service Center at (866) 627-2255**, or visit one of the following websites: www.dhs.gov/GETS, www.dhs.gov/WPS, or www.dhs.gov/TSP.

SHARES Program

National security and emergency preparedness (NS/EP) personnel need to transmit critical messages to coordinate emergency operations even when traditional means of communicating via landlines and cellphones are damaged or destroyed. The SHAred RESources (SHARES) Program, administered by the DHS National Coordinating Center for Communications (NCC), provides an additional means for users with NS/EP missions to communicate when landline and cellular communications are unavailable.

SHARES members use existing HF radio and other communications resources of government, critical infrastructure, and disaster response organizations to coordinate and transmit **emergency** messages. SHARES users typically rely on HF radio and satellite communications to perform critical functions, including those areas related to leadership, safety, maintenance of law and order, finance, and public health. This program also provides the emergency response community with a single interagency emergency message handling and frequency sharing system. SHARES promotes interoperability between HF radio systems and promotes awareness of applicable regulatory, procedural, and technical issues.

More than 2,100 HF radio stations, representing 104 federal, state, and industry organizations located in all 50 states, the District of Columbia, and several locations overseas, are resource contributors to the SHARES HF Radio Program. Nearly 500 emergency planning and response personnel participate in SHARES. Approximately 180 HF radio channels are available for use by SHARES members.

Membership in the SHARES program by government (federal, state, and county), critical infrastructure, and disaster response organizations is voluntary. SHARES is available on a 24-hour basis and requires no prior coordination or activation to transmit messages. Members consult the *SHARES Handbook* to find stations, frequencies and/or Automatic Link Establishment (ALE) addresses of participating organizations they need to communicate/coordinate with. Participating SHARES HF radio stations accept and relay messages until a receiving station is able to deliver the message to the intended recipient.

Further information on SHARES may also be obtained at https://www.dhs.gov/shares or by contacting the SHARES Program Office at 703-235-5329 or nccshares@dhs.gov.

Appendix D. EXCERPTS FROM 2017 BRIEF TO INFRAGARD SUMMIT

UNCLASSIFIED

Communication Vulnerabilities & HEMP Mitigation

InfraGard Electromagnetic Pulse Special Interest Group (EMP SIG™)
Dupont Summit
1 December 2017

Homeland Security

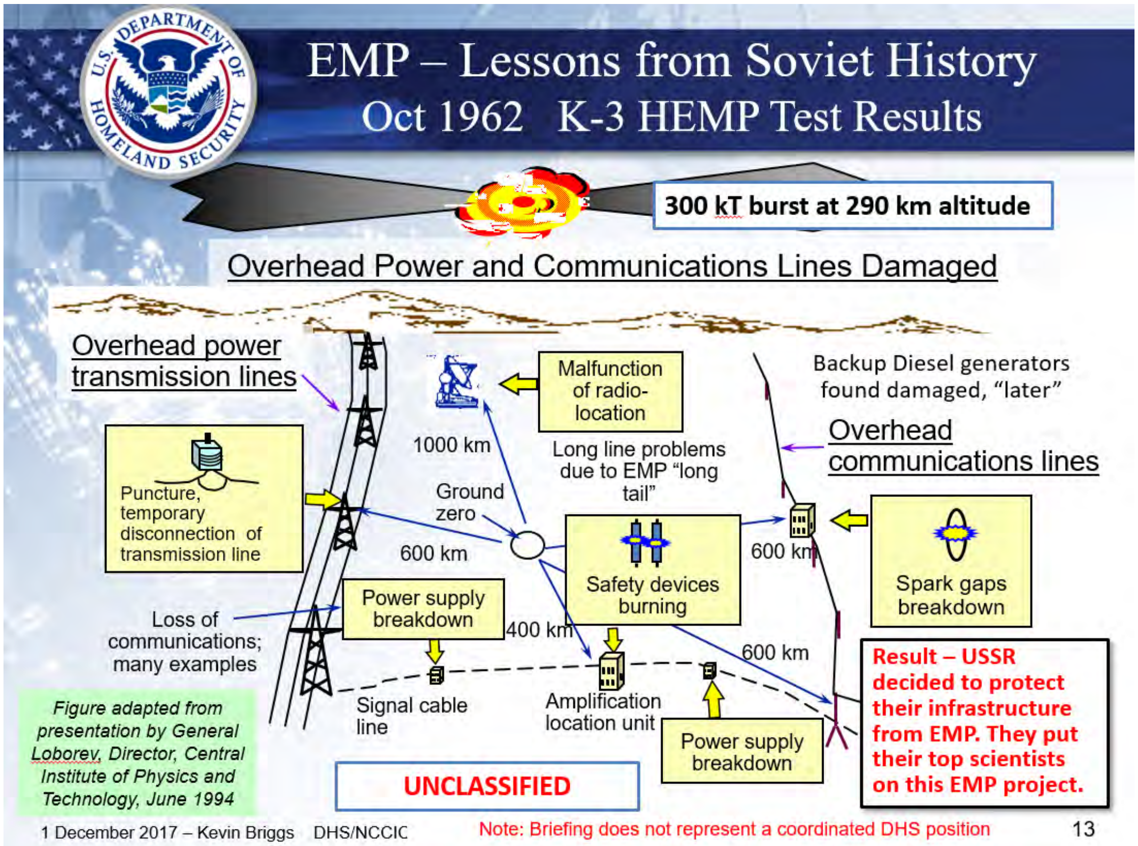
Kevin G. Briggs
Kevin.Briggs@hq.dhs.gov
Chief of Continuity Assessment & Resilience
National Coordinating Center for Communications (NCC)
National Cybersecurity & Communications Integration Center (NCCIC)

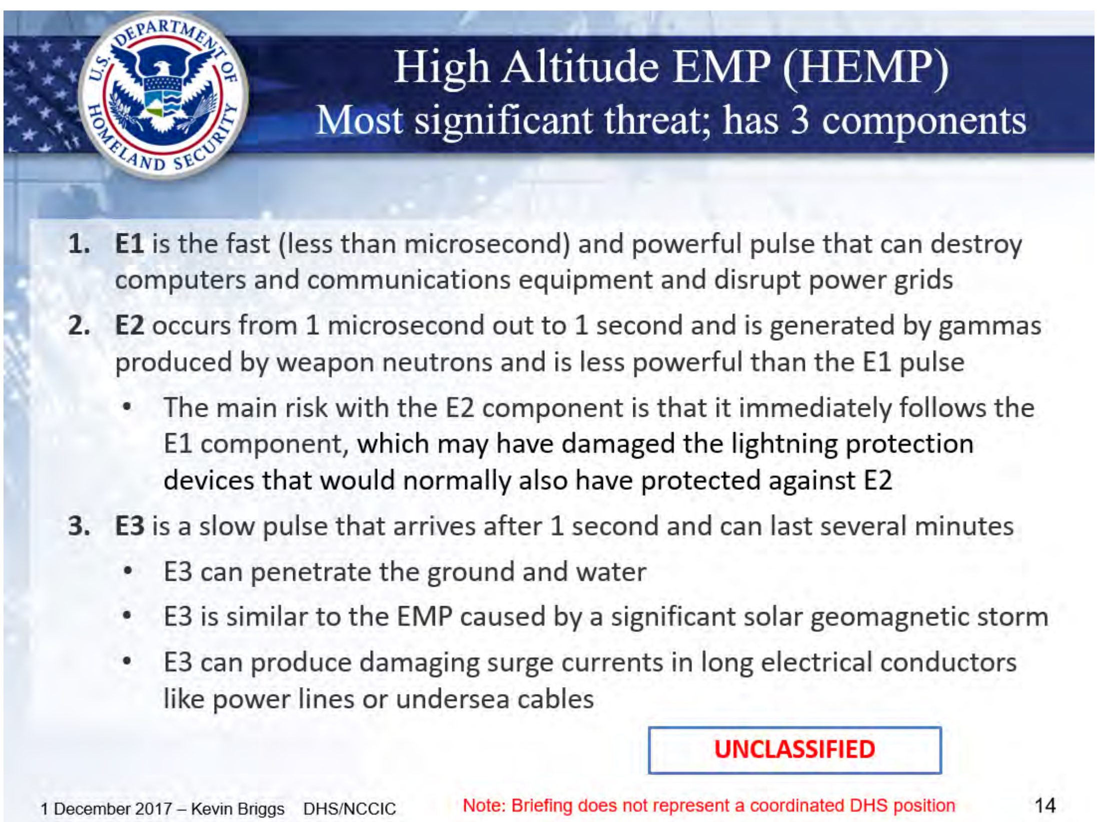
Note: Briefing does not represent a coordinated DHS position

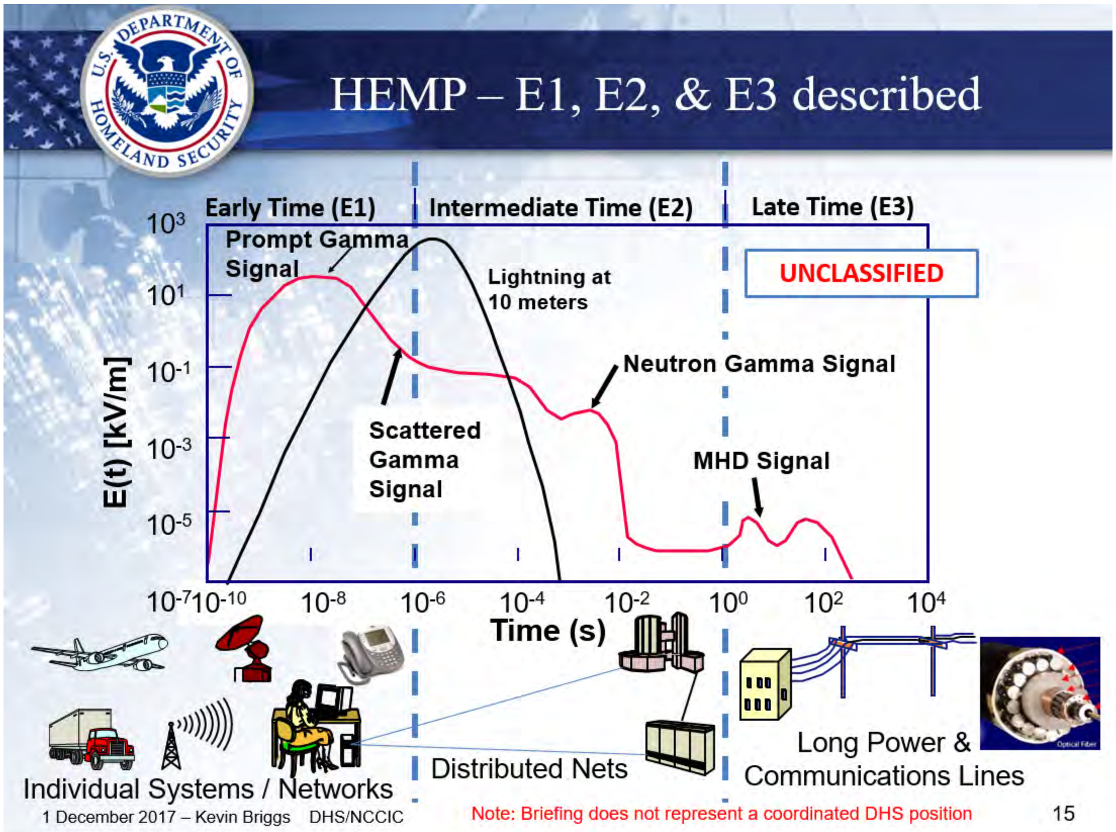
Electromagnetic Pulse (EMP) Background

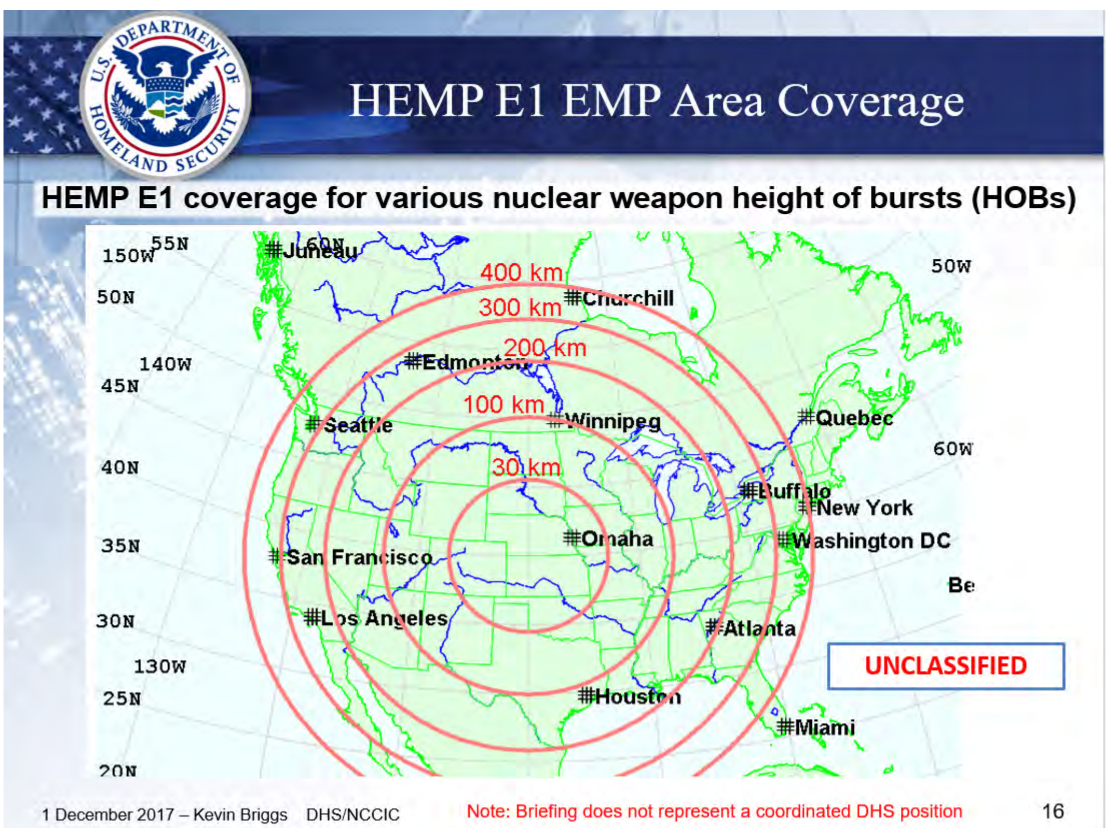
- Over the past several decades, the EMP threat has grown
  - 9/3/2017 N. Korea tested "H-bomb"; claimed a "super-powerful EMP" capability
  - 11/28/2017 North Korea successfully demonstrated the Hwasong-15 ICBM
- Today's power grid and information networks are much more vulnerable to EMP than those of a few decades ago
- We take seriously the U.S. EMP Commission's recommendation that DHS "play a leading role in spreading knowledge of the nature of prudent mitigation preparations for EMP attack to mitigate its consequences" (Ref: 2008 EMP Commission Report, page 181)
- Presidential Policy Directive 21 (Critical Infrastructure Security and Resilience): "The Secretary of Homeland Security shall 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."

1 December 2017 – Kevin Briggs DHS/NCCIC Note: Briefing does not represent a coordinated DHS position 2


EMP – Lessons from Soviet History
Oct 1962 K-3 HEMP Test Results
300 kT burst at 290 km altitude
Overhead Power and Communications Lines Damaged
Overhead power transmission lines
Malfunction of radio-location
Backup Diesel generators found damaged, "later"
1000 km
Long line problems due to EMP "long tail"
Overhead communications lines
Puncture, temporary disconnection of transmission line
Ground zero
600 km
Safety devices burning
600 km
Spark gaps breakdown
Power supply breakdown
400 km
Loss of communications; many examples
600 km
Result – USSR decided to protect their infrastructure from EMP. They put their top scientists on this EMP project.
Signal cable line
Amplification location unit
Power supply breakdown
Figure adapted from presentation by General Loborev, Director, Central Institute of Physics and Technology, June 1994
UNCLASSIFIED
1 December 2017 – Kevin Briggs DHS/NCCIC
Note: Briefing does not represent a coordinated DHS position
13


High Altitude EMP (HEMP)
Most significant threat; has 3 components
1. E1 is the fast (less than microsecond) and powerful pulse that can destroy computers and communications equipment and disrupt power grids
2. E2 occurs from 1 microsecond out to 1 second and is generated by gammas produced by weapon neutrons and is less powerful than the E1 pulse
• The main risk with the E2 component is that it immediately follows the E1 component, which may have damaged the lightning protection devices that would normally also have protected against E2
3. E3 is a slow pulse that arrives after 1 second and can last several minutes
• E3 can penetrate the ground and water
• E3 is similar to the EMP caused by a significant solar geomagnetic storm
• E3 can produce damaging surge currents in long electrical conductors like power lines or undersea cables
UNCLASSIFIED
1 December 2017 – Kevin Briggs DHS/NCCIC
Note: Briefing does not represent a coordinated DHS position
14


HEMP – E1, E2, & E3 described
Early Time (E1)
Intermediate Time (E2)
Late Time (E3)
UNCLASSIFIED
Prompt Gamma Signal
Lightning at 10 meters
Neutron Gamma Signal
Scattered Gamma Signal
MHD Signal
E(t) [kV/m]
Time (s)
Individual Systems / Networks
Distributed Nets
Long Power & Communications Lines
1 December 2017 – Kevin Briggs DHS/NCCIC
Note: Briefing does not represent a coordinated DHS position
15


HEMP E1 EMP Area Coverage
HEMP E1 coverage for various nuclear weapon height of bursts (HOBs)
400 km
300 km
200 km
100 km
30 km
Juneau
Churchill
Edmonton
Seattle
Winnipeg
Quebec
Buffalo
New York
Washington DC
Omaha
San Francisco
Los Angeles
Atlanta
Houston
Miami
UNCLASSIFIED
1 December 2017 – Kevin Briggs DHS/NCCIC
Note: Briefing does not represent a coordinated DHS position
16

North Korean missile threats against Guam

- **From NY Times (9 August 2017) article by Choe Sang-Hun**
  - **"North Korea said Thursday that it was drawing up plans to launch four intermediate-range ballistic missiles into waters near Guam** in the Western Pacific to teach President Trump a lesson, after the president warned of "fire and fury" against the North if it persisted in threatening the United States."
  - "If the North were to follow through on its threat to launch an "enveloping strike" in the vicinity of Guam, it would be the first time that a North Korean missile landed so close to an American territory. The North's official **Korean Central News Agency reported** that, according to the plan, **four of the country's Hwasong-12 intermediate-range ballistic missiles would fly over the three southern Japanese prefectures of Shimane, Hiroshima and Koichi before hitting the ocean about 19 to 25 miles from the coast of Guam.**"

UNCLASSIFIED

1 December 2017 Kevin Briggs DHS/NCCIC/NCC Note: Briefing does not represent a coordinated DHS position 17

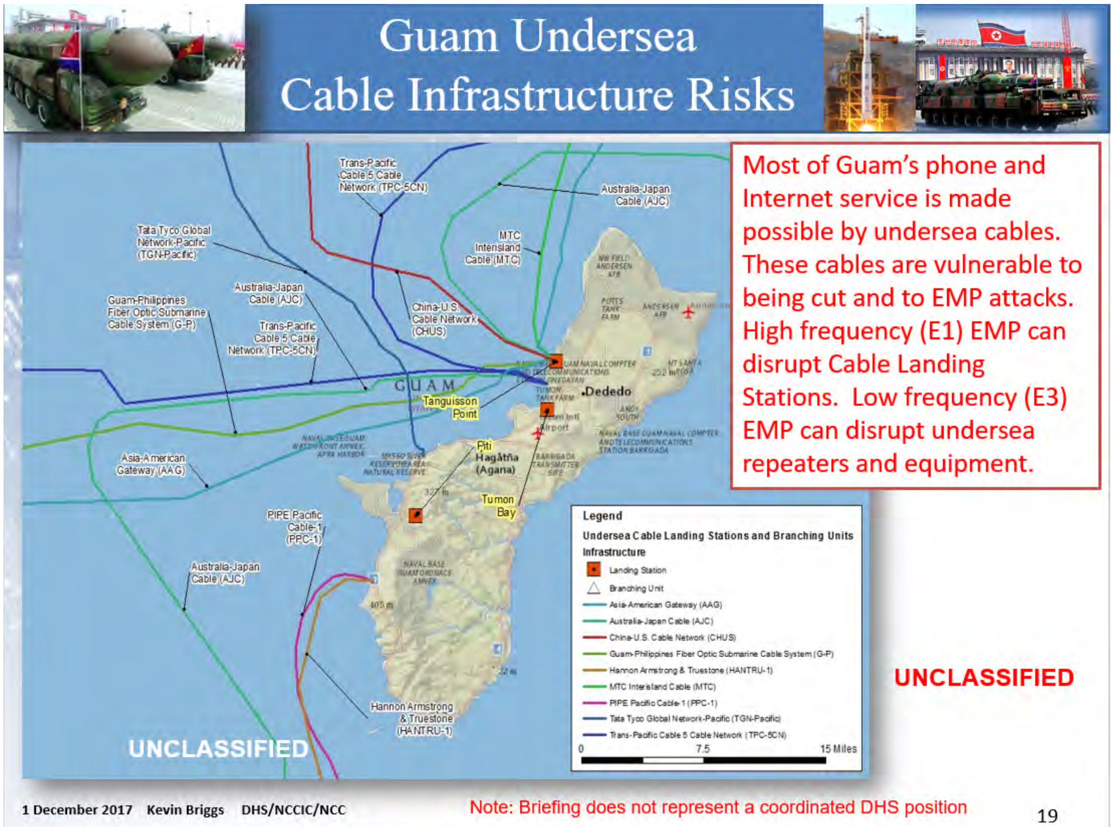
North Korean threatened "test" over the Pacific

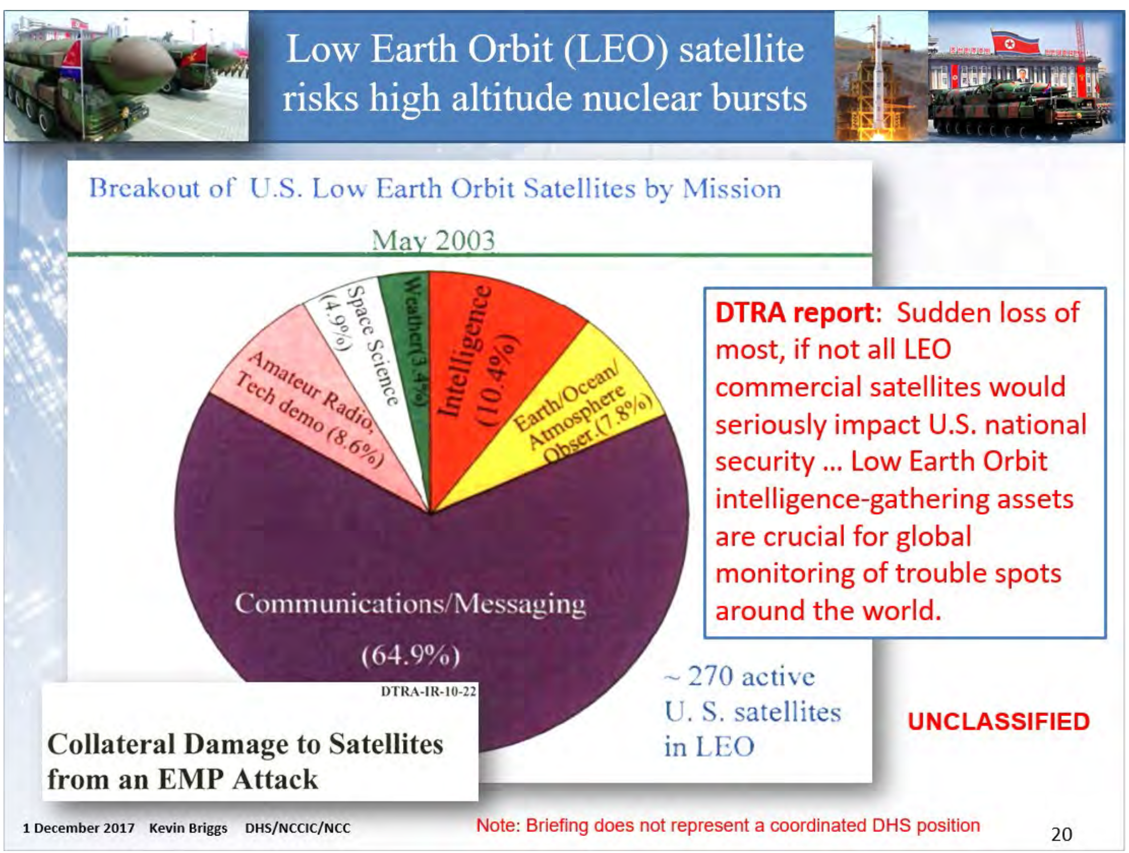
From Reuters (22 Sep 2017) article "A North Korea nuclear test over the Pacific? Logical, terrifying" by Hyonhee Shin, Linda Sieg

- **North Korean Foreign Minister Ri Yong Ho suggested leader Kim Jong Un was considering testing "an unprecedented scale hydrogen bomb" <u>over the Pacific</u>** in response to U.S. President Donald Trump's threat at the United Nations to "totally destroy" the country.
- "It may mean North Korea will fire a warhead-tipped (intermediate range) Hwasong-12 or Hwasong-14 intercontinental ballistic missile and **blow it up a few hundred kilometers above the Pacific Ocean**," said Yang Uk, a senior researcher at the Korea Defence and Security Forum in Seoul.
- "They may be bluffing, but there is a need for them to test their combined missile-bomb capability. They could have already prepared the plan and are now trying to use Trump's remarks as an excuse to make it happen," said Yang.

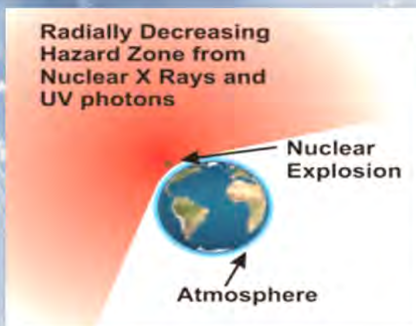
[Note: Red letter highlight added by Kevin Briggs] UNCLASSIFIED

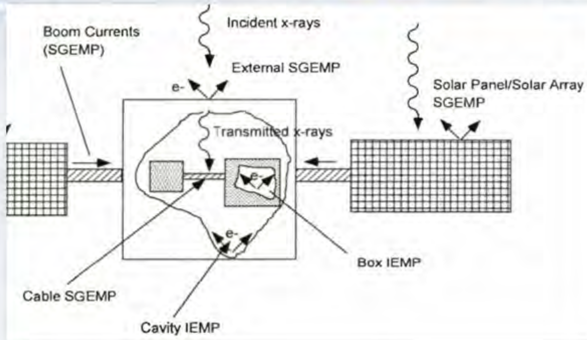
1 December 2017 Kevin Briggs DHS/NCCIC/NCC Note: Briefing does not represent a coordinated DHS position 18


Guam Undersea
Cable Infrastructure Risks
Most of Guam's phone and Internet service is made possible by undersea cables. These cables are vulnerable to being cut and to EMP attacks. High frequency (E1) EMP can disrupt Cable Landing Stations. Low frequency (E3) EMP can disrupt undersea repeaters and equipment.
Trans-Pacific Cable 5 Cable Network (TPC-5CN)
Australia-Japan Cable (AJC)
Tata Tyco Global Network-Pacific (TGN-Pacific)
MTC Interisland Cable (MTC)
Guam-Philippines Fiber Optic Submarine Cable System (G-P)
China-U.S. Cable Network (CHUS)
Asia-American Gateway (AAG)
PIPE Pacific Cable-1 (PPC-1)
Hannon Armstrong & Truestone (HANTRU-1)
GUAM
Dededo
Tanguisson Point
Piti
Hagåtña (Agana)
Tumon Bay
Legend
Undersea Cable Landing Stations and Branching Units Infrastructure
Landing Station
Branching Unit
Asia-American Gateway (AAG)
Australia-Japan Cable (AJC)
China-U.S. Cable Network (CHUS)
Guam-Philippines Fiber Optic Submarine Cable System (G-P)
Hannon Armstrong & Truestone (HANTRU-1)
MTC Interisland Cable (MTC)
PIPE Pacific Cable-1 (PPC-1)
Tata Tyco Global Network-Pacific (TGN-Pacific)
Trans-Pacific Cable 5 Cable Network (TPC-5CN)
0 7.5 15 Miles
UNCLASSIFIED
UNCLASSIFIED
1 December 2017 Kevin Briggs DHS/NCCIC/NCC
Note: Briefing does not represent a coordinated DHS position
19


Low Earth Orbit (LEO) satellite
risks high altitude nuclear bursts
Breakout of U.S. Low Earth Orbit Satellites by Mission
May 2003
Space Science (4.9%)
Weather (3.4%)
Intelligence (10.4%)
Earth/Ocean/Atmosphere Obser. (7.8%)
Amateur Radio, Tech demo (8.6%)
Communications/Messaging (64.9%)
DTRA-IR-10-22
Collateral Damage to Satellites from an EMP Attack
~270 active U. S. satellites in LEO
DTRA report: Sudden loss of most, if not all LEO commercial satellites would seriously impact U.S. national security … Low Earth Orbit intelligence-gathering assets are crucial for global monitoring of trouble spots around the world.
UNCLASSIFIED
1 December 2017 Kevin Briggs DHS/NCCIC/NCC
Note: Briefing does not represent a coordinated DHS position
20

Prompt satellite risks from high altitude nuclear burst





EMP Commission: "Where not shadowed by the Earth or shielded by atmospheric attenuation, X-rays and UV photons travel great distances from a high-altitude nuclear detonation where they may inflict damage to satellites."

Derived from DTRA Report: System Generated Electromagnetic Pulse (SGEMP) is depicted above. When X-rays irradiate a system, photo-Compton electron currents are emitted from the various surfaces, and are driven throughout the various system materials. Timescale: ~ 1 millisecond

UNCLASSIFIED

1 December 2017 Kevin Briggs DHS/NCCIC/NCC

Note: Briefing does not represent a coordinated DHS position 21

Delayed satellite risks from high altitude nuclear effects

UNCLASSIFIED

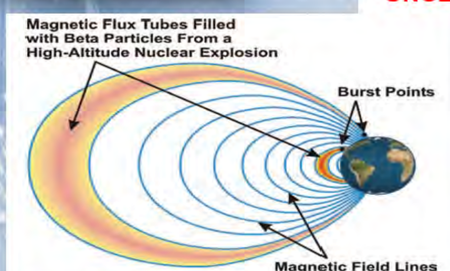


Figure 10-5. Schematic diagram of relative intensities of trapped fluxes from two identical high-altitude nuclear detonations.

EMP Commission: An EMP attack … could cause serious damage to LEO satellites. The STARFISH high-altitude nuclear burst greatly enhanced the high-energy electron environment in LEO, resulting in the early demise of several satellites on orbit at the time.

DTRA report table: "Far Eastern Events"

Location	Yield (kt)	HOB (km)	Time to failure (days)		
			NOAA	TERRA	ISS
35.7N	20	150	25	60	200
36N	100	120	60	200	200
36N	500	120	4	6	3
22.5N	100	200	10	20	30
22.5N	500	200	1	3	4
22.5N	5000	200	0.1	0.1	0.1

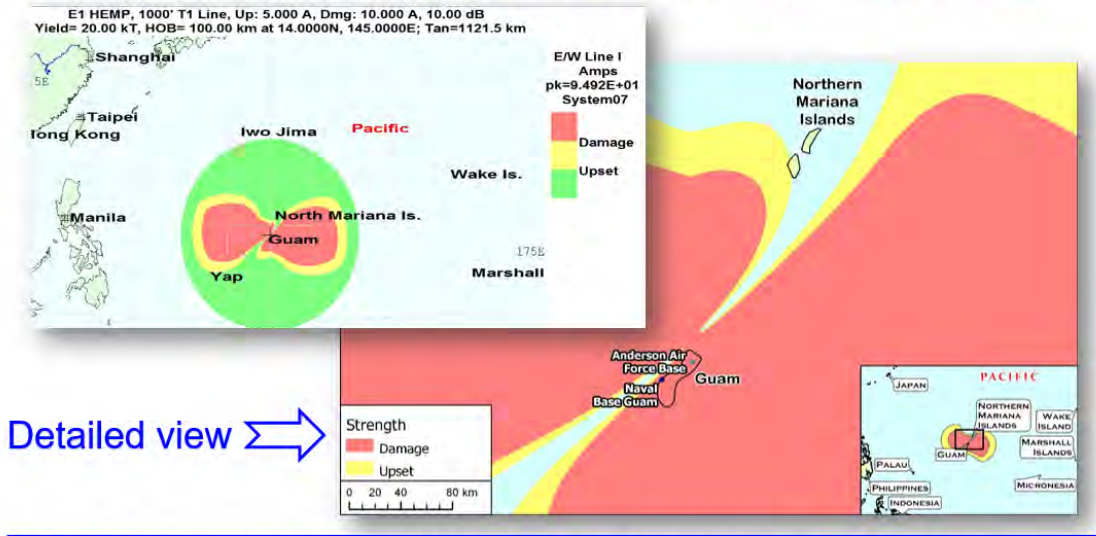
DTRA report: The … analysis on LEO satellites assumed that the satellites started with their full 2-times-natural radiation budget. In reality, satellites on-orbit have various radiation margins remaining due to cumulative time on orbit. For example, a satellite launched 10 years ago will most likely fail more quickly than a comparable satellite launched only a year ago.

1 December 2017 Kevin Briggs DHS/NCCIC/NCC

Note: Briefing does not represent a coordinated DHS position 22

UNCLASSIFIED

EMP impacts from a hypothetical 20 kT weapon: 100' long Ethernet

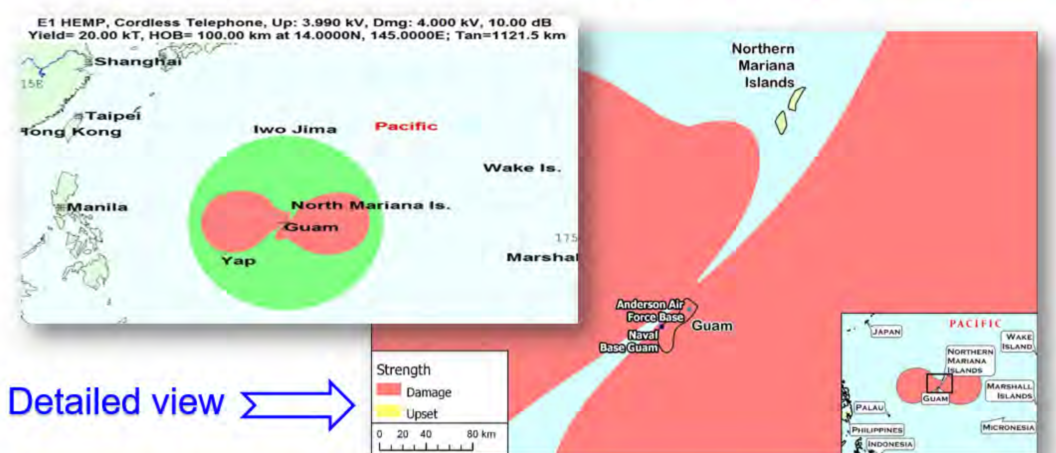


Above: A 20 kT "generic" nuclear weapon detonated at 100 km altitude could generate EMP that could damage and/or upset devices connected to **100' long Ethernet cables** (oriented east to west inside a building that provides **10 dB of shielding**). **The areas shown in Red or Yellow, show the regions of possible damage or upset, respectively, to computers, phones, routers, switches, printers, and other Ethernet connected devices.**
All of Guam is in the possible "damage zone" for unprotected Ethernet connected devices.

1 December 2017 Kevin Briggs DHS/NPPD/NCCIC/NCC Note: Briefing does not represent a coordinated DHS position 25

UNCLASSIFIED

EMP impacts from hypothetical 20 kT weapon: AC/DC power adapters

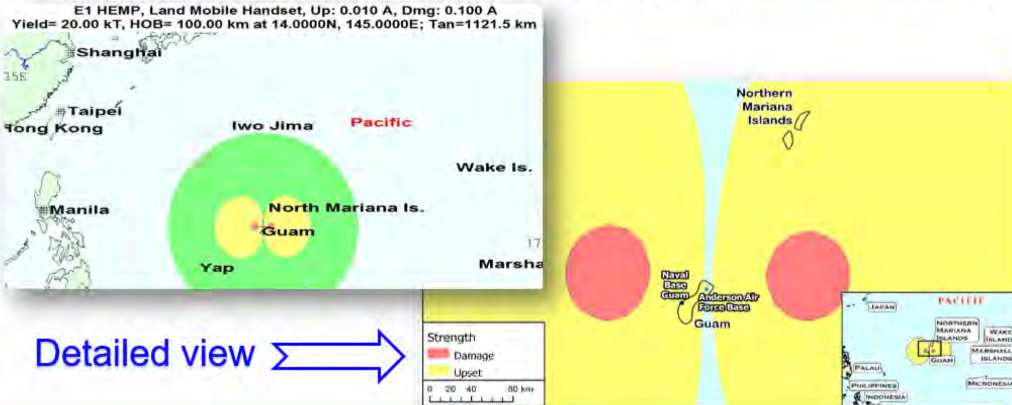


Above: A 20 kT "generic" nuclear weapon detonated at 100 km altitude could generate EMP that could damage and/or upset AC/DC power adapters (like a "wall wart") used to power cordless phones and numerous other devices. This slide assumes a modern solid state AC/DC adapter with 10 dB of protection, that has a damage threshold of 4 kV … a reasonable worst case based on NCC's testing of devices. **The Red areas show the regions of possible damage to AC/DC adapters.**
All of Guam is in possible "damage zone" for unprotected AC/DC adapters.

1 December 2017 Kevin Briggs DHS/NPPD/NCCIC/NCC Note: Briefing does not represent a coordinated DHS position 27

UNCLASSIFIED

EMP impacts from a hypothetical 20 kT weapon: Land mobile radio

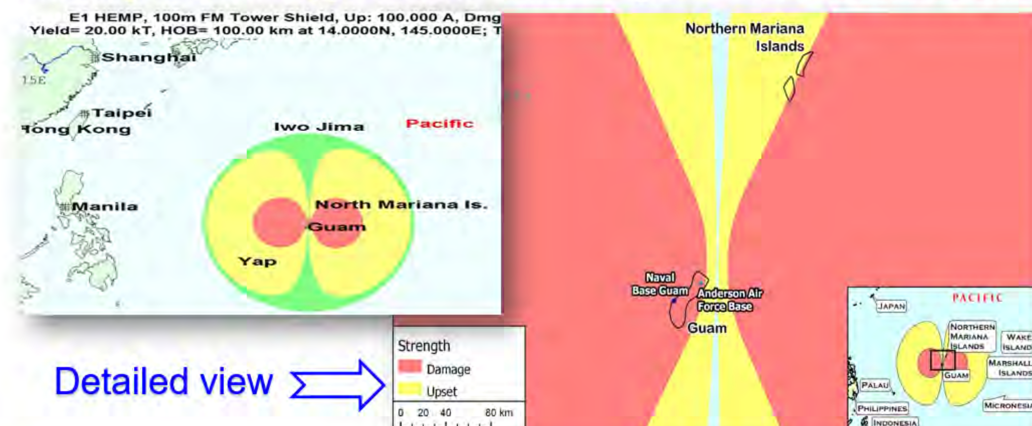


Above: A 20 kT "generic" nuclear weapon detonated at 100 km altitude could generate EMP that could upset Land Mobile Radio handsets used by public safety officials (like fire, EMS, and police). Land mobile radios that rely on wireline trunking would likely be "red", but those that use direct radio-to-radio connection between handsets could be "yellow" (upset, but not damaged, if "on" when EMP occurs), as shown on this slide. If a Land Mobile Radio handset is "off" at the time of the EMP, it is likely to be "green" and work properly. If it is on at the time of the EMP, the radio may need to be cycled "on and off" to work properly. Trunked systems have a large wireline infrastructure that would likely be damaged. Backup generators may be needed to recharge radios. Most of Guam in potentially "upset zone" for unprotected Land Mobile Radio.

1 December 2017 Kevin Briggs DHS/NPPD/NCCIC/NCC Note: Briefing does not represent a coordinated DHS position 28

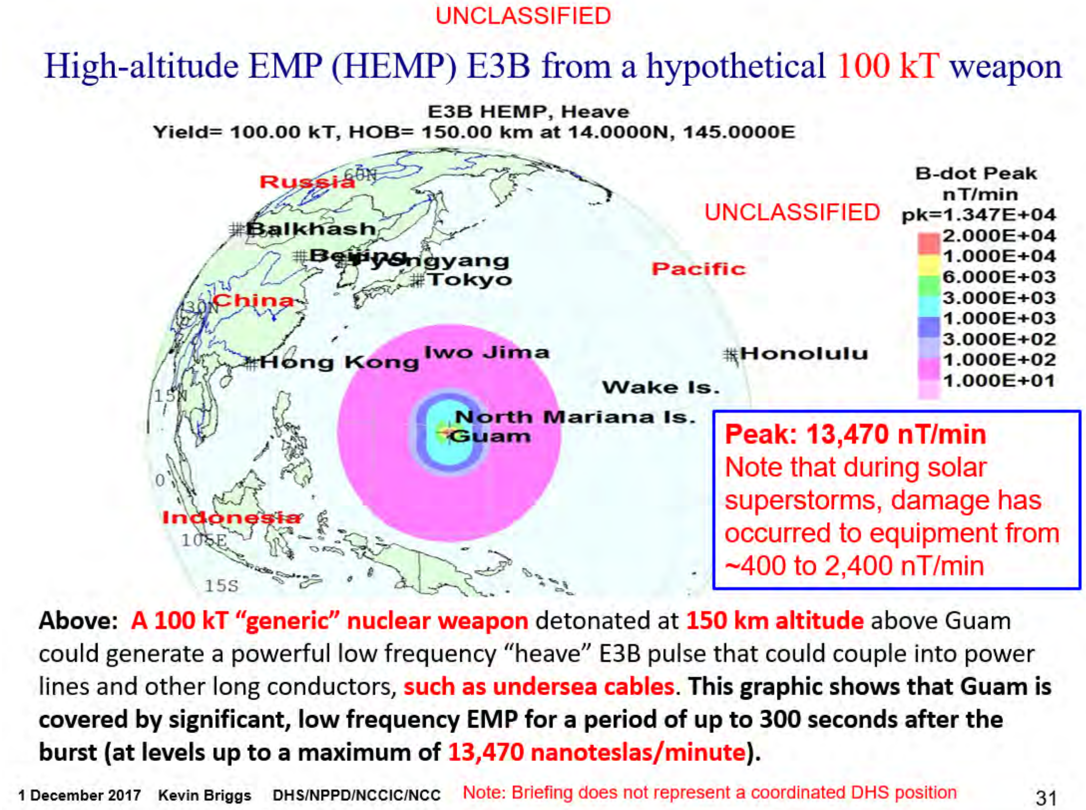
UNCLASSIFIED

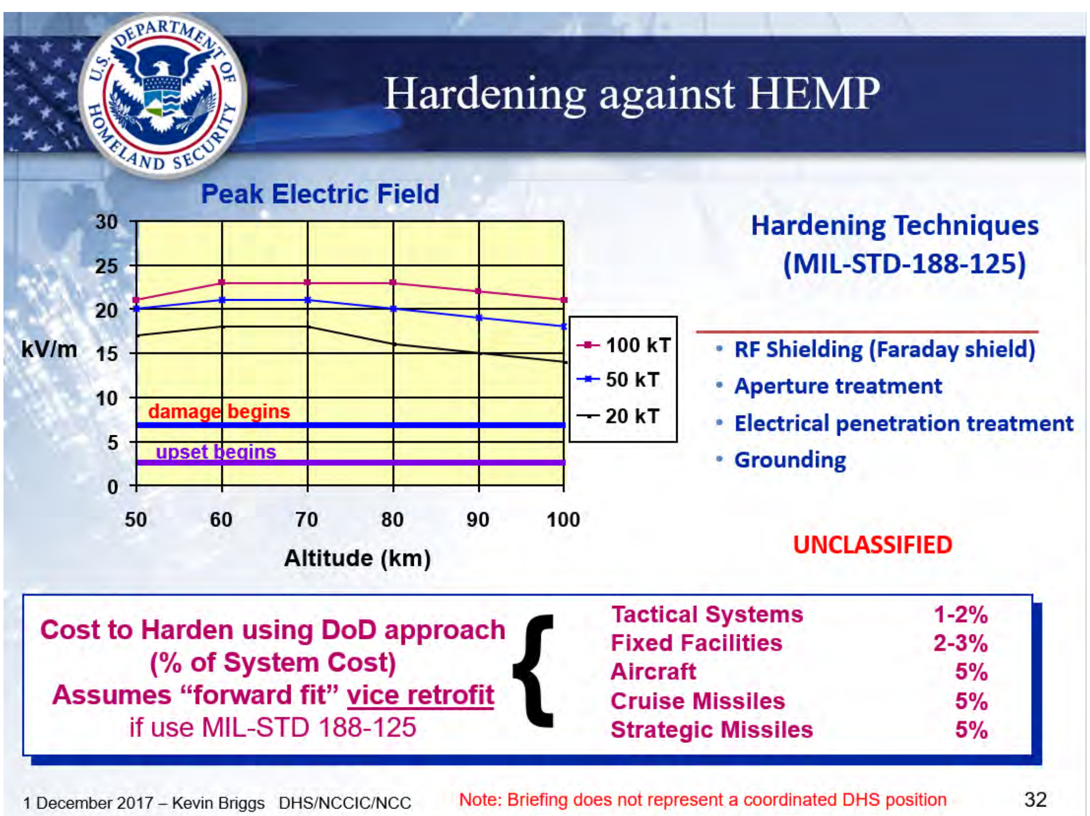
EMP impacts from hypothetical 20 kT weapon: 100m FM Radio tower



Above: A 20 kT "generic" nuclear weapon detonated at 100 km altitude could generate EMP that would likely upset or damage FM radio station equipment at the base of a 100 meter FM radio transmission tower if the FM equipment isn't properly EMP shielded. Handheld "battery operated" FM radios and those in cars are likely to work, if cycled "off and on" or if turned "off" prior to the time of the EMP burst. 200 meter AM radio towers, if not EMP protected, are likely to fare worse than the FM stations. Hence, if a radio station is shielded, as with those Emergency Alert System (EAS) Primary Entry Point (PEP) radio stations with "in-line" EMP hardening, then public alert, warning, and messaging can occur to those with handheld or car-based radios. Result: All of Guam is in the potentially "upset or damage zone" for unprotected FM (and AM) radio stations.

1 December 2017 Kevin Briggs DHS/NPPD/NCCIC/NCC Note: Briefing does not represent a coordinated DHS position 30


UNCLASSIFIED
High-altitude EMP (HEMP) E3B from a hypothetical 100 kT weapon
E3B HEMP, Heave
Yield= 100.00 kT, HOB= 150.00 km at 14.0000N, 145.0000E
Russia
Balkhash
Beijing
Pyongyang
Tokyo
China
Hong Kong
Iwo Jima
Pacific
Honolulu
Wake Is.
North Mariana Is.
Guam
Indonesia
UNCLASSIFIED
B-dot Peak
nT/min
pk=1.347E+04
2.000E+04
1.000E+04
6.000E+03
3.000E+03
1.000E+03
3.000E+02
1.000E+02
1.000E+01
Peak: 13,470 nT/min
Note that during solar superstorms, damage has occurred to equipment from ~400 to 2,400 nT/min
Above: A 100 kT "generic" nuclear weapon detonated at 150 km altitude above Guam could generate a powerful low frequency "heave" E3B pulse that could couple into power lines and other long conductors, such as undersea cables. This graphic shows that Guam is covered by significant, low frequency EMP for a period of up to 300 seconds after the burst (at levels up to a maximum of 13,470 nanoteslas/minute).
1 December 2017 Kevin Briggs DHS/NPPD/NCCIC/NCC
Note: Briefing does not represent a coordinated DHS position
31


Hardening against HEMP
Peak Electric Field
kV/m
30
25
20
15
10
5
0
damage begins
upset begins
50
60
70
80
90
100
Altitude (km)
100 kT
50 kT
20 kT
Hardening Techniques
(MIL-STD-188-125)
RF Shielding (Faraday shield)
Aperture treatment
Electrical penetration treatment
Grounding
UNCLASSIFIED
Cost to Harden using DoD approach
(% of System Cost)
Assumes "forward fit" vice retrofit
if use MIL-STD 188-125
Tactical Systems 1-2%
Fixed Facilities 2-3%
Aircraft 5%
Cruise Missiles 5%
Strategic Missiles 5%
1 December 2017 – Kevin Briggs DHS/NCCIC/NCC
Note: Briefing does not represent a coordinated DHS position
32

Possible impacts to infrastructures resulting from High-altitude EMP (HEMP)

UNCLASSIFIED

Infrastructure (rating assumes not EMP protected)	Days ⟺ Months
Undersea Cable Infrastructure (main risks: E1 + E3)	Upset and damage
Satellite in space (System Generated EMP (SGEMP) + radiation belts)	Upset/degradation
Satellite terminals/support (vulnerable to HEMP E1)	Upset and damage
HF radio equipment (vulnerable to HEMP E1)	Upset and damage
HF sky wave media (heals in hours); HF groundwave not impacted	HF propagation
Computers and Ethernet Interfaces (vulnerable to HEMP E1)	Upset and damage
Desk phones (vulnerable to E1 EMP conducted on power/data cords)	Upset and damage
Cell phones (risk to towers/backhaul from E1; handsets generally OK)	Upset and damage
Routers and phone switches (vulnerable to HEMP E1)	Upset and damage
Radio and TV stations (likely to go off-air immediately due to E1)	Upset and damage
Portable battery operated radios (eventual power problem)	Battery dependent
Land mobile radios (OK if not trunked; eventual power problem)	Power dependent
Unprotected parts of the electric grid (main risks: E1 + E3)	Upset and damage

1 December 2017 Kevin Briggs DHS/NCCIC/NCC — Note: Briefing does not represent a coordinated DHS position — 33

EMP Mitigation Conclusions

- **The risk of not protecting critical infrastructures is profound**
  - One HEMP burst can severely disrupt continental U.S. infrastructures
  - One SREMP burst can severely disrupt infrastructures within a 100 miles
- **Significant, low-cost EMP protection can be implemented quickly**
  - For example, FirstNet sites could be HEMP protected for < 5% of cost/site
- **EMP protection guidance is needed for more than just HEMP**
  - Key satellites need System Generated EMP (SGEMP) protection
  - Key facilities need SREMP protection, if near a major city or possible target
- **Need to implement EMP protections for all critical infrastructures, not just communications (such as power, water, transportation …)**

UNCLASSIFIED

1 December 2017 – Kevin Briggs DHS/NCCIC — Note: Briefing does not represent a coordinated DHS position — 34

Appendix E. ACRONYMS AND EXPLANATION OF DECIBELS

3GPP	3rd Generation Partnership Project
A	Ampere or Amp
AC/DC	Alternating Current/Direct Current
AEHF	Advanced Extremely High Frequency
AM	Amplitude Modulation
ARO	Amateur Radio Operator
CCMG	Continuity Communications Managers Group
COTS	Commercial off the shelf
D2D	Device-to-Device Communications
dB	Decibel (see Table E1 at the end of this Appendix for additional information)
DHS	Department of Homeland Security
DoC	Department of Commerce
DoD	Department of Defense
DTRA	Defense Threat Reduction Agency
DTV	Digital Television
EAS	Emergency Alert System
ECD	Emergency Communications Division
EFT	Electric Fast Transient
EM	Electromagnetic
EMAT	Electromagnetic Assessment Tool
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EMP	Electromagnetic Pulse
ESA	Electrical Surge Arrester
FCC	Federal Communications Commission
FM	Frequency Modulation
GDT	Gas Discharge Tube
GETS	Government Emergency Telecommunications Service
GIC	Geomagnetically Induced Current
GMD	Geomagnetic Disturbance
HCI	Hardness Critical Item
HEMP	High-Altitude Electromagnetic Pulse
HF	High Frequency

HIRF	High-intensity Radiated Field
HM/HS	Hardness Maintenance/Hardness Surveillance
HOB	Height of Burst
HPM	High Power Microwave
HV	High Voltage
HVAC	Heating, Ventilation, and Air Conditioning
IC	Integrated Circuit
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IEMI	Intentional Electromagnetic Interference
IMT	Infrastructure Mapping Tool
IND	Improvised Nuclear Device
ISR	Intelligence, Surveillance, and Reconnaissance
IT	Information Technology
ITU	International Telecommunication Union
IRA	Impulse Radiating Antenna
kA	kiloamp
km	Kilometers
kT	Kiloton
kV/m	Kilovolts/meter
kW	Kilowatt
MA	Mega Amp
MC	Mission Critical
MC PTT	Mission Critical Push-To-Talk
MCV	Mission Critical Voice
MHD	Magneto hydrodynamic
MOV	Metal Oxide Varistor
ms	Millisecond
MT	Megaton
MHz	Megahertz
NB HPRF/M	Narrowband, High Pulse Repetition Frequency mode Microwave
NCC	National Coordinating Center for Communications
NOAA	National Oceanic and Atmospheric Administration
ns	Nanosecond

OEC	Office of Emergency Communications
PBX	Private Branch Exchange
POE	Point of Entry
POTS	Plain Old Telephone System (wireline)
ProSE	Proximity Services
ROM	Rough Order of Magnitude
RF	Radio Frequency
RFW	Radio Frequency Weapon (RFW)
RP	Receiver Protection
SCADA	Supervisory Control and Data Acquisition
SHARES	SHAred RESources
SPD	Surge Protection Device
SREMP	Source Region Electromagnetic Pulse
TBB	Telecommunications Bonding Backbone
TEMPEST	Transient Electromagnetic Pulse Emanation Standard
TPD	Terminal Protection Device
TOP	Test Operations Procedures`
TRX	Transceiver
TSP	Telecommunications Service Priority
TVSS	Transient Voltage Suppression System
UHF	Ultra High Frequency
UPS	Uninterruptible Power Supply
µs	Microsecond
USSR	Union of Soviet Socialist Republics
UWB	Ultra-wideband
VHF	Very High Frequency
VSWR	Voltage Standing Wave Ratio
WBC	Waveguide Below Cutoff
WPS	Wireless Priority Service

Table E-1. Explanation of Decibel (dB)

	POWER (like mW/cm²)			**FIELD** (like V/m or kV/m)		
dB	Power Ratio	% Attenuation	% Transmission	Field Ratio	% Attenuation	% Transmission
0	1.000	0	100	1.00	0	100
1	1.259	21	79	1.12	11	89
2	1.585	37	63	1.26	21	79
3	2.000	50	50	1.41	29	71
4	2.512	60	40	1.58	37	63
5	3.162	68	32	1.78	44	56
6	4.000	75	25	2.00	50	50
7	5.013	80	20	2.24	55	45
8	6.310	84	16	2.51	60	40
9	7.941	87	13	2.82	65	35
10	10	90	10	3.16	68	32
15	31.6	96.8	3.2	5.62	82	18
20	100	99	1	10	90	10
25	316	99.7	.3	17.8	94.4	5.6
30	1,000	99.9	.1	31.6	97	3
35	3,162	99.97	.03	56.2	98.2	1.8
40	10,000	99.99	.01	100	99	1
50	100,000	99.999	.001	316	99.7	.3
60	1,000,000	99.9999	.0001	1,000	99.9	.1
80	100,000,000	99.999999	.00001	10,000	99.99	.01
100	1,000,000,000	99.99999999	.000001	100,000	99.999	.001

Appendix F. IEC SC 77C BIBLIOGRAPHY

The below are publications dealing with the protection of civil equipment and systems from the effects of HEMP and IEMI issued by the International Electrotechnical Commission (IEC) SC 77C. For dated references, only the edition cited applies.

1. IEC/TR 61000-1-3 Ed. 1.0 (2002-06): Electromagnetic compatibility (EMC) – Part 1-3: General – The effects of high-altitude EMP (HEMP) on civil equipment and systems. Basic EMC publication.

2. IEC/TR 61000-1-5 Ed. 1.0 (2004-11): Electromagnetic compatibility (EMC) – Part 1-5: General – High power electromagnetic (HPEM) effects on civil systems. Basic EMC publication.

3. IEC 61000-2-9 Ed. 1.0 (1996-02): Electromagnetic compatibility (EMC) – Part 2: Environment – Section 9: Description of HEMP environment – Radiated disturbance. Basic EMC publication.

4. IEC 61000-2-10 Ed. 1.0 (1998-11): Electromagnetic compatibility (EMC) – Part 2-10: Environment – Description of HEMP environment – Conducted disturbance. Basic EMC publication.

5. IEC 61000-2-11 Ed. 1.0 (1999-10): Electromagnetic compatibility (EMC) – Part 2-11: Environment – Classification of HEMP environments. Basic EMC publication.

6. IEC 61000-2-13 Ed. 1.0 (2005-03): Electromagnetic compatibility (EMC) – Part 2-13: High-power electromagnetic (HPEM) environments – Radiated and conducted. Basic EMC publication.

7. IEC 61000-4-23 Ed. 1.0 (2000-10): Electromagnetic compatibility (EMC) – Part 4-23: Testing and measurement techniques – Test methods for protective devices for HEMP and other radiated disturbances. Basic EMC publication.

8. IEC 61000-4-24 Ed. 2.0 (2015-11): Electromagnetic compatibility (EMC) – Part 4-24: Testing and measurement techniques – Test methods for protective devices for HEMP conducted disturbance. Basic EMC Publication.

9. IEC 61000-4-25 Ed. 1.1 (2012-05): Electromagnetic compatibility (EMC) – Part 4-25: Testing and measurement techniques – HEMP immunity test methods for equipment and systems. Basic EMC publication.

10. IEC/TR 61000-4-32 Ed. 1.0 (2002-10): Electromagnetic compatibility (EMC) – Part 4-32: Testing and measurement techniques – High-altitude electromagnetic pulse (HEMP) simulator compendium. Basic EMC publication.

11. IEC 61000-4-33 Ed. 1.0 (2005-09): Electromagnetic compatibility (EMC) – Part 4-33: Testing and measurement techniques – Measurement methods for high-power transient parameters. Basic EMC publication.

12. IEC/TR 61000-4-35 Ed. 1.0 (2009-07): Electromagnetic compatibility (EMC) – Part 4-35: Testing and measurement techniques – High power electromagnetic (HPEM) simulator compendium. Basic EMC publication.

13. IEC 61000-4-36 Ed. 1.0 (2014-11): Electromagnetic compatibility (EMC) – Part 4-36: Testing and measurement techniques – IEMI immunity test methods for equipment and systems. Basic EMC publication.

14. IEC/TR 61000-5-3 Ed. 1.0 (1999-07): Electromagnetic compatibility (EMC) – Part 5-3: Installation and mitigation guidelines – HEMP protection concepts. Basic EMC publication.

15. IEC/TS 61000-5-4 Ed. 1.0 (1996-08): Electromagnetic compatibility (EMC) – Part 5: Installation and mitigation guidelines – Section 4: Immunity to HEMP – Specifications for protective devices against HEMP radiated disturbance. Basic EMC Publication.

16. IEC 61000-5-5 Ed. 1.0 (1996-02): Electromagnetic compatibility (EMC) – Part 5: Installation and mitigation guidelines – Section 5: Specification of protective devices for HEMP conducted disturbance. Basic EMC Publication.

17. IEC/TR 61000-5-6 Ed. 1.0 (2002-06): Electromagnetic compatibility (EMC) – Part 5-6: Installation and mitigation guidelines – Mitigation of external EM influences. Basic EMC publication.

18. IEC 61000-5-7 Ed. 1.0 (2001-01): Electromagnetic compatibility (EMC) – Part 5-7: Installation and mitigation guidelines – Degrees of protection by enclosures against electromagnetic disturbances (EM code). Basic EMC publication.

19. IEC/TS 61000-5-8 Ed. 1.0 (2009-08): Electromagnetic compatibility (EMC) – Part 5-8: Installation and mitigation guidelines – HEMP protection methods for the distributed infrastructure. Basic EMC publication.

20. IEC/TS 61000-5-9 Ed. 1.0 (2009-07): Electromagnetic compatibility (EMC) – Part 5-9: Installation and mitigation guidelines – System-level susceptibility assessments for HEMP and HPEM. Basic EMC publication.

21. IEC/TS 61000-5-10 DTS (2017-105): Electromagnetic compatibility (EMC) – Part 5-10: Installation and mitigation guidelines – Guidance on the protection of facilities against HEMP and IEMI. Basic EMC publication.

22. IEC 61000-6-6 Ed. 1.0 (2003-04): Electromagnetic compatibility (EMC) – Part 6-6: Generic standards – HEMP immunity for indoor equipment. Basic EMC publication.

Appendix G. REFERENCES

1. MIL-STD-188-125-1, "High-Altitude Electromagnetic Pulse (HEMP) Protection For Ground-Based C4I Facilities Performing Critical, Time-Urgent Missions, Part 1: Fixed Facilities," April 7, 2005.
2. MIL-HDBK-423, "High-Altitude Electromagnetic Pulse Protection for Fixed and Transportable Ground-Based Facilities, Volume I: Fixed Facilities."
3. TM 5-690, "Grounding and Bonding in Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities."
4. MIL-HDBK-419, "Grounding, Bonding, and Shielding for Electronic Equipment and Facilities."
5. MIL-STD-464C, DOD Interface Standard: Electromagnetic Environmental Effects Requirements for Systems, 1 December 2010.
6. MIL-STD-470, "Maintainability Program for Systems and Equipment."
7. MIL-STD-785, "Reliability Program for Systems and Equipment Development and Production."
8. MIL-STD-729, "Corrosion and Corrosion Prevention Metals."
9. MIL-STD-2165, "Testability Program for Electronic Systems and Equipment."
10. MIL-STD-2169B, High Altitude EMP (HEMP) Environment, 17 December 1993.
11. IEC 61000-4-36 Ed. 1.0 (2014-11): Electromagnetic compatibility (EMC) - Part 4-36: Testing and measurement techniques – IEMI immunity test methods for equipment and systems.
12. IEEE-Std 81-2012, "Guide for Measuring Earth Resistivity, Grounding Impedance, and Earth Surface Potentials of a Ground System."
13. IEEE Std 299-2006, "Standard Method for Measuring the Effectiveness of Electromagnetic Shielding Enclosures."
14. Meta-R-319, *Geomagnetic Storms and Their Impacts on the U.S. Power Grid*, John Kappenman, Metatech Corporation, for Oak Ridge National Lab, January 2010.
15. Meta-R-320, *The Early-Time (E1) High-Altitude Electromagnetic Pulse (HEMP) and Its Impact on the U.S. Power Grid*, by Dr. Edward Savage, Dr. James Gilbert, and Dr. William Radasky, Metatech Corporation, for Oak Ridge National Lab, January 2010.
16. Meta-R-321, *The Late-Time (E3) High-Altitude Electromagnetic Pulse (HEMP) and Its Impact on the U.S. Power Grid*, by Dr. James Gilbert, Dr. Edward Savage, John Kappenman, and Dr. William Radasky, Metatech Corporation, for Oak Ridge National Lab, January 2010.
17. Meta-R-322, Low-Frequency Protection Concepts for the Electric Power Grid: Geomagnetically Induced Current (GIC) and E3 HEMP Mitigation, by John Kappenman, Metatech Corporation, for Oak Ridge National Lab, January 2010.
18. Meta-R-323, Intentional Electromagnetic Interference (IEMI) and Its Impact on the U.S. Power Grid, by Dr. William Radasky and Dr. Edward Savage, Metatech Corporation, for Oak Ridge National Lab, January 2010.
19. Meta-R-324, High-Frequency Protection Concepts for the Electric Power Grid, by Dr. William Radasky and Dr. Edward Savage, Metatech Corporation, for Oak Ridge National Lab, January 2010.

20. TIA-607, Revision C (2015-11), “Generic Telecommunications Bonding and Grounding (Earthing) for Customer Premises.

21. M.A. Messier, K.S. Smith, W.A. Radasky, M.J. Madrid, “Response of Telecom Protection To Three IEC Waveforms, Zurich EMC Symposium, 2003.

22. QSTAG 244, Edition 4: Nuclear Survivability Criteria for Military Equipment, 19 January 1993.

23. QSTAG 620, Edition 2: Nuclear Survivability Criteria for Communications-electronics Equipment, 29 January 1993.

Appendix H. EXAMPLE EMP IMPLEMENTATION FOR HF COMMUNICATIONS SITE

Many Federal Government departments and agencies use high frequency (HF) radio transceivers for backup voice and email communications. To enable better interoperability using HF during emergencies, the Department of Homeland Security operates the SHARES Program (see *SHARES Program* in Appendix C). It is recommended that all critical infrastructure operators with a national security and/or emergency preparedness mission join the SHARES program.

The three most commonly used SHARES HF transmitter power ratings are 100-150 W, 500 W, and 1 kW. The lower power ratings are typically good for regional communications while the higher power ratings may be required for communicating across the country although the actual area covered is highly dependent upon many factors (for example: location, antenna type/position, solar weather, and time of day). For amateur radio operators, the lower power options are the most popular due to lower costs and ease of operations.

The sample EMP implementation in this Appendix is designed to help enterprises better understand the equipment, supplies, and rough order of magnitude (ROM) funds needed to install an HF transceiver system with EMP resiliency versus installing it with protection only against lightning. If the site already exists, these estimates could increase depending upon the EMP level being implemented and the existing equipment and installation. Costs shown do not include maintenance partially because those costs are operationally dependent and since the EMP material maintenance costs are minimal (e.g., replace a very inexpensive GDT every few years).

For this sample implementation, it is assumed that the site consists of the following:

- **Equipment**
  - HF transceiver, power supply, built-in antenna tuner, and power amplifier (PA) connected to a combined microphone and speaker that are a 1 meter (m) away.
  - Antenna system including RF antenna cable
  - UPS for computer and networking equipment (only required for Level 2 and 3 with data)
  - Computer (optional for data).
- **Data Cables**
  - Fiber connection from external data source (i.e., outside of the equipment building/room) to an internal fiber optic media converter (assumed fiber is standard from the facility operator or the communications provider).
  - 20 m Ethernet cable from fiber optic media converter to computer.
  - 3 m meandering Ethernet cable from computer to HF transceiver.
  - 1 m – 2 m speaker/microphone cable
- **Rooftop** – The antenna is placed on top of a building and has a 100’ RF cable running from the antenna to the HF base station.
  - This antenna could be placed on an antenna tower instead of a rooftop with no technical impact on the HF EMP prevention suggestions.
  - Deploying an antenna on a tower could impact the labor costs to deploy the HF equipment, but in many cases this deployment will occur at the same time as when either installing the HF equipment initially, making an upgrade, or performing

maintenance in which case the additional labor to add the EMP improvements discussed below would be minimal.
    - Excellent grounding is available and can easily be connected to.
- **Equipment Building/Room** – The equipment building/room provides **10 dB** of protection (bricks, wood, and windows are not good shielding material as discussed in "Figure 21. Effect of Building Materials on EMP Attenuation" and "Table 9. Building shielding "rules of thumb" for E1 HEMP"). See Table E-1 for more information on decibels (dBs).

Potential solutions to achieve EMP Level 1, 2, and 3 results with the above assumptions are shown below in two sets of tables. The first set, consisting of Table H-1 through Table H-3 below, discusses the technical requirements that are specific to an HF site to make an HF site Level 1, 2, or 3 EMP resilient. The second set consists of just one table shown in Table H-4, which discusses non-HF specific requirements, such as food and fuel supplies.

As shown below in Table H-1, an enterprise can meet EMP Level 1 guidelines with no equipment costs beyond implementing best practices for lightning protection.

Table H-1. Level 1 EMP Resilient HF Site Specific Technical Costs

HF Specific Requirement	Level 1 EMP Cost Details	Cost
Unplug power and data lines from spare or backup equipment where feasible.	Best practice for lightning and energy savings and there is no extra cost to leave a cable unplugged.	$0
Turn off equipment that cannot be unplugged and is not actively being used.	Best practice for lightning and energy savings and there is typically no extra cost to turn off something.	$0
Use at least a lightning rated surge protection device (SPD) on power cords, antennas, and data cables; maintain spare SPDs	Best practice for lightning and energy savings as well as EMP; thus, assume these are already deployed or will be used if it's a new installation. • Power Supply SPD (e.g., $15 for 6 outlet APC SurgeArrest that will alert the operator when it's no longer fully operational). • SPDs with Gas Discharge Tubes (GDTs) that are not soldered are preferred for easy replacement. For example, the Alpha Delta TT3G50 lightning SPD costs around $50, its replacement cartridge costs under $15.	$0
Wrap spare electronics with aluminum foil or put in Faraday containers.	Store spare electronics in an area with at least 20 dB protection. This is adequate for smaller electronic devices (or battery powered devices) as might be required for an HF site.	$0
Join SHARES, if applicable.	There are no fees and the effort is negligible to join SHARES. This is also independent of EMP.	$0
Consider HF radios	This HF site meets suggestion.	$0
Level 1 EMP Resilient HF Site Incremental Technical Costs		$0

For Level 2, the HF specific EMP changes from Level 1 are the following:

- Implementation of a power SPD with a clamp time of 10 ns or less.
- Addition of an EMP rated RF SPD.
- Addition of ferrites to the antenna cable (minimal cost)
- Use of a UPS, which in this case is a line interactive unit since it is less expensive and more efficient at low power loads than an online unit.
- A small amount was also allocated for a shielded Ethernet cable.

The material cost to implement Level 2 versus Level 1 is $630, which includes providing the site with extra functionality via a UPS.

Table H-2. Level 2 EMP Resilient HF Site Specific Technical Costs

HF Specific Requirement(s)	Level 2 Cost Details	Cost
Use EMP-rated SPDs on power cords, antennas, and data cables to protect critical equipment. Also… 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.	**HF Transceiver & PA Power Supply SPD** – To obtain an SPD for the power cable that protects against EMP, the SPD's recovery time should be 10 ns or less. Note: The $200 Transtector 6 outlet AC Surge Protection device SL-V Surge Cord has a published tested specification of 5 ns. It costs about $180 more than a lightning only SPD.	$200
	Shielded RF Antenna Cable – No extra cost since low inductance and lightning protected cables can be selected that also provide EMP protection. For instance, RG-214 is double shielded/braided, or can use low loss LMR-400, which is braided plus has a foil (this is not as good as double shielded/braided).	$0
	Antenna RF Cable SPD –The NexTek HF (1-50 MHz) sub-ns response SPD part FPNNMNFBCA3B, which has been tested per MIL-STD-188-125-1, costs approximately $200 (minimum order may apply). Note: This is $150 more than the Level 1 SPD listed (plus the replacement cost is considerably higher).	$200
	Antenna Cable Ferrites – Can buy a package of these for under $10.	$10
	Antenna Tuner SPD – Use extra SPD outlet purchased above or can connect into the UPS for surge protection.	$0
	Computer Power Cable SPD – Connect to UPS for surge protection.	$0
	Fiber Optic Media Converter SPD – Connect to UPS for surge protection.	$0

HF Specific Requirement(s)	Level 2 Cost Details	Cost
	20 m Ethernet Cable to Computer – Use a shielded Ethernet cable from the fiber optic media converter to the computer. Ground shield at one end only. Wireless can also be used to connect to the computer.	$20
	Computer Microphone and Speaker Cable – Use EM shielded cabling, which likely came with the system. Thus, there it is assumed that there is no extra cost (no SPD is required given the short distance.	$0
	Meandering 3 m Ethernet Cable to HF Transceiver – Use a shielded Ethernet cable from the computer to the HF transceiver. Note: Could use an unshielded Ethernet cable in this case since the cable is inside and it's not straight, but a shielded cable is better for consistency and improved EMP protection with no material cost increase. Regardless, no SPD is required given the above.	$0
Use on-line/double-conversion uninterruptible power supplies (UPS) or a high quality line interactive UPS.	• The UPS includes back up power for everything but the HF transceiver and the HF power supply. • The pricing assumes the purchase of an interactive UPS for Level 2 (and an online UPS for Level 3).	$200
Implement EMP protected, high frequency (HF) voice and email for long-distance communications.	The above includes a computer and data connection to enable these communications.	$0
Level 2 EMP Resilient HF Site Costs (includes Level 1 costs)		$630*

** Can save $90 if going straight to Level 2 and not purchasing standard lighting SPDs then replacing them as well as installing shielded Ethernet cable from the start.*

For Level 3, shown in the table below, the HF specific EMP changes from Level 2 are the following:

- **UPS** – Level 3 uses an online UPS instead of a line interactive unit in this example although a line interactive unit could have been used.
    - The online version will block EMP by default through its design.
    - Unless the line interactive unit has been specifically tested for EMP, there is a risk that it may not effectively block the EMP pulse if the built-in surge protection is insufficient. Therefore an online version is used in this table.
- **IEC and SPDs** – The surge suppression components in Level 3 must the IEC requirements. However, in this case all Level 2 surge suppression components meet Level 3.
- **Maintenance Program** – Although the upfront costs of this are minimal (create a plan and procure spare equipment), the ongoing costs to replace UPS units and SPDs, surveil the antenna site, etc. can impact the budget although most of the maintenance program

should be implemented for a normal lightning protected site (e.g., swap out defective power SPDs).

The estimated material cost for Level 3 is over $7,000, but most of this cost is driven by buying a Faraday enclosure which is the most expensive option listed and often will not be required. Further, this assumes that Level 2 has not been implemented and therefore those parts cannot be reused. Lastly, Level 3 uses an online UPS instead of a less expensive line interactive UPS.

In addition to the material costs, there is labor involved to maintain the system and potentially resources involved to test the HF transceiver to ensure that it can tolerate higher levels of EMP transients that bypass the selected voltage level of an SPD.

Table H-3. Level 3 EMP Resilient HF Site Specific Technical Costs

HF Specific Requirement(s)	Level 3 Cost Details	Cost
Use International Electrotechnical Commission (IEC) EMP and IEMI protection standards (IEC SC 77C series).	• Equipment vendors should use the IEC SC 77C generated series of standards. In particular, the 61000 series of standards could be listed, which were prepared by the 77C subcommittee. • These standards include specifying the EMP test and measurement techniques. • The standardized EMC test for immunity to surges is IEC/EN 61000-4-5 • Alternatively, MIL-STD-188-125-1 and MIL-HDBK-423 may be met.	$0 (cost occurs under other require-ments)
UPS (see Level 2 requirement)	• Assumes use of online UPS. • Online UPS cost shown is around $500 ($300 more than the Level 2 line interactive UPS)	$500
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.	**First Option**: Appropriately shield all internal components to meet 30 dB protection requirement (shielding is additive). Note: Since it is assumed that the building offers 10 dB of protection, the shielding may just offer 20 dB of protection to meet the 30 dB requirement. • **Shield Cables** – Ensure all RF, data, and power cables are shielded. RF cables should already be shielded. Using shielding on data cables is very low cost (assume $10). Shielded power cables are also very inexpensive, but assume a few of these needs to be replaced for $10 each. • **Shield Equipment** – Some equipment is manufactured with all sensitive electronics in a	$40

HF Specific Requirement(s)	Level 3 Cost Details	Cost
	fully enclosed metal shield and do not require extra shielding. • This option is usually the least expensive for smaller EMP-protected operations.	
	Second Option: Shield the room to at least 20 dB or put the equipment in a shielded enclosure. Note: This protection together with the assumed 10 dB of shielding from the building will equal 30 dB. • Might be able to move the equipment from a room with windows into a room in the middle of a building with no windows or into a more protected area of the basement. • Could put EMP composite on walls and ceiling in sealed windowless room to improve EMP protection (may need to use EMP rated ventilation guides). • Procure a Faraday cage for the equipment. The cost of a Faraday cage varies depending upon several characteristics, but this example assumes that it costs $6,000 together with the necessary accessories.	$6,000 (assumed; Faraday cage costs can vary significantly)
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.	• This requirement is primarily applicable to long power and communications cables, such as used in the electric grid or undersea – this is part of the reason behind the required EMP protected backup power. • As part of the maintenance plan, power SPDs should not be replaced during an E3 HEMP event, which can last for hours, unless there are plenty of spare power SPDs.	$0
Use EMP tested SPDs and equipment.	• The Level 2 Transtector power SPD is sufficient for Level 3 as well since it's tested to MIL-STD-188-125. List price is around Level 2: $200. • The Level 2 NexTek HF (1-50 MHz) SPD part FPNNMNFBCA3B can continue to be used since it has been tested per MIL-STD-188-125-1. List price is around Level 2: $200. • The HF transceiver should be tested to ensure that it can tolerate higher levels of EMP transients that bypass the selected voltage level of an SPD. The cost shown assumes that the	$400

HF Specific Requirement(s)	Level 3 Cost Details	Cost
	organization can reuse someone else's test results.	
Institute hardening maintenance and surveillance (HM/HS).	• HM/HS combines preventive maintenance, inspection, test, and repair activities accomplished on a HEMP protected operational facility to ensure that HEMP hardness is retained throughout the lifecycle. • The cost shown assumes that spare SPDs are purchased as part of the HM/HS program.	$400 upfront (On-going effort is required)
Level 3 EMP Resilient HF Site Upfront Costs (includes Level 2 costs)		$7,340 *

** If reusing Level 2's SPDs and line interactive UPS and if the first shielding option can be used, these material costs can be substantially reduced to $40 plus the cost of the spare parts (which likely would have been purchased in Level 2).*

General EMP Requirements

General EMP requirements help sites prepare for a HEMP or SREMP event, but are also applicable to other manmade disasters as well as natural disasters. These requirements impact the overall operations or the site characteristics (e.g., priority phone service, EMP protected backup power). The suggested requirements and the general nature of the costs to implement the requirements are shown in the table below. The estimated costs are not specified both because they are highly variable and they are not HF specific requirements.

Table H-4. General, Non-HF Specific EMP Requirements for Levels 1-3

Level	Non-HF Specific Site Requirement	Details
1	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).	• A 3 kW generator could backup all of the equipment, including a 1 kW transmitter. • If using a lower power transmitter or a battery backup system for the HF transceiver system, then a smaller generator could be used with improved fuel efficiency.
2, 3	Use EMP protected backup power that is not vulnerable to EMP coupled through the power grid.	The backup power generation is often handled by the facility.
1, 2	Have one (1) week of on-site fuel or equivalent (e.g., renewable source).	The fuel supplies is often handled by the facility's emergency planners.

Level	Non-HF Specific Site Requirement	Details
3	Have thirty (30) days of EMP protected fuel/power.	It may be helpful to shut off power to all non-essential equipment to meet this requirement.
1,2,3	Use priority phone services like GETS, WPS (for cell phones), and TSP.	The costs for these services are dependent upon the service provider, but they tend to be minimal as discussed under Appendix C.
1,2,3	Consider land mobile radios with standalone capabilities and FirstNet.	There is no extra cost to use FirstNet or Verizon's priority services versus one of their non-priority cellular services.
1,2,3	Use battery operated AM/FM/NOAA radios to receive Emergency Alerts.	Need just one of these radios to receive alerts.
1,2	Store one week of food, water, and other supplies for personnel.	Could work with on-site food provider, such as a cafeteria to help ensure that food is available.
3	Store 30 days of food, water, and critical supplies for personnel.	Maintenance of the critical supplies also needs to occur.
2,3	Consider geosynchronous earth orbit (GEO) satellite services, like BGAN. Avoid low-earth orbit (LEO) satellite supported communications, unless EMP protected.	LEOs could be damaged or become dysfunctional due to a HEMP event. GEO satellites are too far from potential HEMP events to be significantly impacted.
2,3	Shortwave radio for situational awareness.	This consideration is for the overall facility and not just the HF site.
3	Use time-urgent EMP resilient comms, like X, Ku and Ka satellite, and either HF groundwave or Automatic Link Establishment (ALE) HF.	The higher satellite frequency bands are more resilient to EMP bursts until the ionosphere stabilizes.

Appendix I. ENDNOTES

1 Title 47: Telecommunication, PART 215—FEDERAL GOVERNMENT FOCAL POINT FOR ELECTROMAGNETIC PULSE (EMP) INFORMATION, https://ecfr.io/Title-47/pt47.5.215

2 The White House, National Security Strategy of The United States of America (Dec 2017), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

3 Graph courtesy of Metatech (Oct 2018)

4 Quartz Media LLC, North Korea's latest missile test traveled 10 times higher **THAN THE** ISS**,** https://qz.com/1140566/north-koreas-latest-missile-test-traveled-10x-height-of-iss-and-suggests-it-could-hit-us/ (7/16/18)

5 Statement Dr. Peter Vincent Pry, EMP Commission Staff Before The United States Senate Subcommittee on Terrorism, Technology and Security and Homeland Security, March 8, 2005, Foreign Views of Electromagnetic Pulse (EMP) Attack, http://web.archive.org/web/20121108204504/http://kyl.senate.gov/legis_center/subdocs/030805_pry.pdf

6 Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack (July 2017), Recommended E3 HEMP Heave Electric Field Waveform for the Critical Infrastructures, Courtesy of Los Alamos National Laboratory

7 William Radasky, Edward Savage, Intentional Electromagnetic Interference (IEMI) and Its Impact on the U.S. Power Grid (Jan 2010), https://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity/ferc_meta-r-323.pdf

8 ibid

9 Homeland Security Council, National Continuity Policy Implementation Plan (August 2007), https://www.hsdl.org/?view&did=482817

10 National Communications System (NCS), Volume I EMP/Transient Threat Test of Protection Devices for Amateur/Military Affiliate Radio System Equipment (October 1985)

11 Motorola Publication R56, "Standards and Guidelines for Communications Sites" (2005), www.ronet.co.za/downloads/R56%20Guidelines.pdf

12 ARRL, Grounding and Bonding for the Radio Amateur (2017), www.arrl.org/shop/Grounding-and-Bonding-for-the-Radio-Amateur

13 Digi, Indoor Path Loss (June 2012), http://ftp1.digi.com/support/images/XST-AN005a-IndoorPathLoss.pdf

14 MIL-STD-188-125-1 (7/17/1998), HIGH-ALTITUDE ELECTROMAGNETIC PULSE (HEMP) PROTECTION FOR GROUND-BASED C4I FACILITIES PERFORMING CRITICAL, TIME-URGENT MISSIONS, Part 1, Fixed Facilities, http://futurescience.com/emp/MIL-STD-188-125-1.pdf

15 ibid

16 https://www.firstnet.com/ (9/27/2018)

17 https://www.firstnet.gov/newsroom/blog/firstnet-core-delivers-promise-dedicated-network-public-safety (9/27/2018)

18 https://www.firstnet.com/coverage