Resilient Power Best Practices for Critical Facilities and Sites

with Guidelines, Analysis, Background Material, and References

NOVEMBER 2022

Cybersecurity and Infrastructure Security Agency (CISA)
Resilient Power Working Group (RPWG)

4. ELECTROMAGNETIC (EM) SECURITY

Target Audience:

- Executives, Continuity & Planning: Browse
- Power Management/Engineering, Telecommunications and IT Installation: *Read all*
- Cybersecurity: Browse, *Read 4.4*
- Physical Security: *Read 4.4*

This chapter provides an overview and high-level mitigation best practices against electromagnetic (EM) threats for critical infrastructure stakeholders excluding energy-related utility companies (as per the *Scope*). In particular, it covers the following:

- *Section 4.1 E1 High-Altitude* EM Pulse (HEMP) – This broadband field pulse induces abnormally high voltages and currents on short cables, antennas, and long lines. The fast-rising EM pulse (EMP) can travel through lightning surge protection devices (SPDs) before the surge protection has time to activate. Today's electronics are much more sensitive than in 1962 when power and communication systems were disrupted and damaged in Hawaii from a HEMP nighttime test event 900 miles away – see Figure 3.[67]

Figure 3. 1962 Starfish Prime HEMP impacted electronics with a relatively small peak field

- *Section 4.2 E2 HEMP and Lightning* – E2 HEMP induces pulsed voltages and currents on long lines similar to those induced by nearby lightning strikes. Long (>1000m) interconnecting cables with no lightning protection may need E2 protection. Note: Lightning protection is very important to EM security in most parts of the country, but this topic is only briefly discussed since many specific lightning standards and handbooks exist.
- *Section 4.3 E3 HEMP and* Geomagnetic Disturbance (GMD*)* – The focus of this section is to protect critical infrastructure's onsite generation sources and related equipment. This includes *E3 HEMP and Geomagnetic Disturbance (GMD) Mitigations* such as protecting against E3 HEMP and GMD transformer overheating and harmonics that can damage DC power supplies and protections for long cable lines containing metal.
- *Section 4.4 Electromagnetic Interference (EMI) and Intentional EMI* – Caused by both mobile and stationary high-power EM sources, the effects on systems are similar to E1 HEMP but at higher frequencies and over much smaller areas.

The 2017 National Security Strategy stated that "the vulnerability of U.S. critical infrastructure to cyber, physical, **and electromagnetic attacks** means that adversaries could disrupt military command and control, banking and financial operations, the electrical grid, and means of communication."[68] The severe consequences of the terrorist attacks which took place on 9/11/2001 and of the Covid-19 global pandemic demonstrate the importance of planning and preparedness for low probability events.

This chapter includes more background and theoretical material than provided in other parts of the document because EM security tends to be less understood by practitioners than most other topics discussed in this document and there are far fewer referenced resources. The background and theory are intended to orient the employee or contractor that will be implementing EM security so that they can make better choices to defend against the EM threats discussed in this chapter. Lastly, the resilient power timeframe (e.g., three days of onsite fuel) discussed under *Definition of Resilience Levels* is not directly applicable to this chapter since EM security typically either protects the equipment or it doesn't.

Although mitigations presented in this chapter are relevant today, many of these mitigations are expected to undergo significant improvements over the next few years given the increased focus on these threats. Technology innovations are underway to bring down costs or improve the protection against these EM threats. More testing is ongoing or is expected to be conducted during the next few years to better understand and mitigate the risk.

4.1. E1 High-Altitude EM Pulse (HEMP)

This section starts with the *Background and Importance of E1 HEMP Protection* followed by the *E1 HEMP Technical Overview* since many readers likely do not understand what HEMP is. Subsequently, suggested *E1 HEMP Mitigations* are covered.

Note: The term EMP is often used interchangeably with HEMP as in the case of the EMP Executive Order, but EMP can include other types of nuclear EMP such as Source Region EMP (SREMP).[69] SREMP is only covered in *Appendix C* since the impact range is much smaller than with HEMP and mitigations against SREMP are generally only recommended for the most critical facilities.

Background and Importance of E1 HEMP Protection

The need for HEMP protection has increased in importance in recent years, which is part of the reason for the 2019 issuance of Presidential Executive Order 13865. It states that an EMP "*has the potential to disrupt, degrade, and damage technology and critical infrastructure systems. Human-made or naturally occurring EMPs can affect large geographic areas, disrupting elements critical to the Nation's security and economic prosperity, and could adversely affect global commerce and stability*."

HEMP is created when a nuclear weapon is detonated above 30 kilometers (km) (per International Electrotechnical Commission (IEC) 61000-2-9, p. 13) and can have continental scale impacts, especially if there are multiple high altitude nuclear detonations. Given the potential wide-area, long-term debilitation from HEMP with a significant amount of equipment damaged or upset, these best practices recommend that all critical infrastructure stakeholders consider implementing the mitigations listed in this chapter. Note: the term upset refers to the effects to components that causes an interruption, disruption, and degradation of services.

E1 HEMP Technical Overview

The nuclear HEMP attack threat is a national security risk and is addressed in Executive Order 13865. E1 HEMP is a concern because of its very fast rise time (as shown in Figure 4) combined with its wide geographical area effects and the cascading disruption and damage that HEMP from one or a few high-altitude bursts.

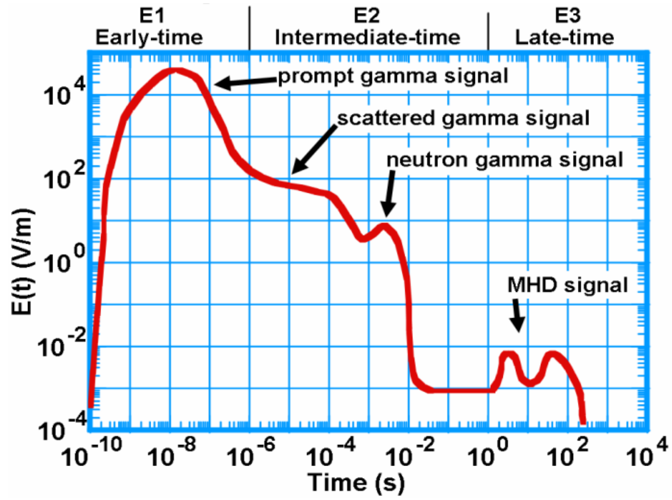

Figure 4. Generic HEMP waveform (ref. Meta-R-324)

For the specific E1 HEMP waveform that should be used to determine whether the site's protections are adequate or for use in procuring new equipment, shielding, and filtering including using SPDs (devices that suppress line conducted voltages and currents), see Table 7 below. There are two HEMP specifications that are particularly applicable: radiated and conducted energy. The rise time of the HEMP waveform is calculated as the time interval between 10% to 90% of the peak pulse amplitude.

The conducted specification, IEC 61000-2-10[70] referenced in Table 7 assumes that the E1 HEMP field couples efficiently to outdoor conductors (such as cables and wires) with a worst-case HEMP field polarization (orientation of the electric vector) and angle of incidence to the orientation of the conductor. It is also permissible to use MIL-STD-188-125 specifications for waveforms on penetrating lines (this is mandatory at some military sites for critical systems/areas), which uses a conducted pulse rise time specification of ≤ 20 nanoseconds (ns) rise time at the point of entry to a building.

Table 7. E1 HEMP Waveform Specifications

E1 Transmission	Environment	Specifications*	Protection Considerations (for sensitive electronics)
Radiated Waveform (DOE Waveform)[71]	Line-of-sight path to the HEMP detonation source	• 2.5 ns rise time • 50 ns pulse width	Protection recommendations are provided in the next subsection.
Conducted / Induced (most damage will likely occur through conducted currents) (IEC 61000-2-10)	Aboveground	• 10 ns rise time • 100 ns pulse width • 4 kilo-amperes (kA) peak current worst-case exposure	SPDs need to be able to handle much faster rise times than the rise time from lightning.
	Belowground	• 25 ns rise time (IEC) • 500 ns pulse width • Substantially lower peak current than 4 kA	Installing cables underground (versus aboveground) can substantially lower risks and make protection easier.

E1 HEMP Mitigations

Many assume that to protect sensitive electronics against HEMP, MIL-STD-188-125-1 must be implemented, which includes costly facility-level shielding and add-ons to existing infrastructure. However, **most of the best practices in this section range from no additional cost** (e.g., ensure a good grounding and bonding) **to minimal extra cost** (e.g., purchase HEMP-rated SPDs). Further, some of these HEMP best practices, such as using a flat ground cable instead of a round one, are recommended only when there will be a minimal extra implementation cost (e.g., during new buildouts and system replacement programs).

This subsection focuses on E1 HEMP mitigation best practices for all resiliency levels, most of which are inexpensive or no extra cost to implement if designed into the installation. These HEMP mitigations generally will also help against lightning, EMI, and IEMI when a cable is attached (tethered) to sensitive electronics and equipment (e.g., control, IT, and communications equipment). The mitigations include:

- **Lightning and EMI/EM Compatibility (EMC) Protection** – Effective lightning protection is a good start to protect against EMP, such as those noted in the *Lightning Protection, EMP Protection and Grounding* section within the *ANSI APCO Public Safety Grade Site Hardening Requirements*.[72] Implementing EMI/EMC standards, which are useful to protect against lightning, is strongly recommended to help mitigate E1 HEMP effects as well.
- **EMP-Rated SPDs** – An EMP-rated Surge Protection Devices (SPD) is recommended for lines/cables carrying AC power, RF, or data when the lines/cables have the potential to pick up significant levels of EMP. Typically if a cable needs to be protected against lightning, it needs to be protected against EMP (note: the EMP SPD also will protect against lightning). The one exception is if the cable is carrying a timing signal and the SPD introduces a variable delay. Ferrites or filters can also help with RF lines (typically best to add ferrites near building egress).
- **Uninterruptible Power Supply (UPS) –** A double conversion online (preferred) or high-quality line interactive UPS can be added to an AC circuit and used instead of a standalone SPD to eliminate potential HEMP E1 issues (see *Section 7.3 UPS Guidance*).
- **Shielded Cables** – Unless the cable is either non-electrically conductive, very short or well protected from EMP, a grounded shielded cable should generally be used to prevent EMP voltage/induced current from being conducted onto the cable. Using double shielding will effectively eliminate the EMP voltage/current if the shielding is sufficiently grounded. Whether an unshielded cable can be used may be determined if the following are known:
  - The maximum length of the cable in any direction (coiled cables are less of a concern).
  - The EMP protection/attenuation (in decibels [dB]) of the building/room in which the cable is located.
  - Maximum voltage or ampere input that can be handled by the device to which the cable is connected.
  - The EMP peak amplitude that needs to be protected against (see the applicable EMP standard/guidelines that your organization is using).
  - Note: Shielded cables should have the shield circumferentially bonded and grounded at each termination.

- **Bury Cables** – Buried cables couple 10-20 dB less E1 energy than non-buried cables.
- **Fiber –** Fiber (without metal) cables eliminate EM voltages/currents being conducted into the cable. The fiber typically should not contain metal since it can conduct EM (note: metal is sometimes added to fiber to distribute power or to improve the cable strength).
- **Bonding –** Solid bonding is needed to help prevent arcs/sparks due to differential voltage and to ensure good ground connections.
- **Grounding** – Excellent grounding is needed including high frequency grounding.
    - Follow lightning grounding standards – see *E2 HEMP and Lightning* section below.
    - Use wide, flat grounding copper or stainless-steel straps (3" is good, 6" is better) that can carry the higher frequencies from EMP much better than an equivalent amount of copper in a round conductor (often used for lightning protection) due to the skin effect at higher frequencies. However, connecting equipment ground to a metal plate or the building's metallic structure/frame is even better.
    - A thicker flat grounding strap (e.g., 0.085") is likely needed for Earth-ground systems due to corrosion, but a thinner grounding strap (e.g., 0.022") may be preferred where corrosion is less of an issue.
    - Ground the shielding on both ends of shielded cables.
    - Periodically test the ground system impedance as part of the O&M procedures. Corrosion of buried ground system components can degrade ground system performance over time.
- **Spares** – For critical equipment that is inexpensive or at sites needing a high level of resiliency, spares should be procured and maintained. Storing spares can also be a much lower cost alternative to hardening.
- **EM Interference (EMI) and Electromagnetic Compatibility (EMC) Standards** – Each site should procure electronic equipment that meet EMI/EMC standards, including meeting IEC/EN 55035, which provides EMC immunity requirements (e.g., equipment should tolerate at least 3 V/m).
- **Facility or Room Shielding –** If feasible, place sensitive, unshielded critical infrastructure equipment and cables in inner rooms, the basement, shielded cabinets or closets, or at least so that there is no direct line-of-sight to the sky through any non-metallic structure walls/roofs, which generally offer very little EMP protection (concrete is better than most windows or wood). Presently, it is <u>not</u> cost effective for most Level 1-3 facilities to add room or facility shielding.
- **Processes** – Simple process related protections typically should be implemented such as:
    - Shunt an antenna to ground or disconnect it when the antenna is not in use.
    - Reduce unintended antennas by smoothing surfaces, eliminating edges, and not using long, straight cables.
    - Boot up equipment in a useable state if it is reset.
    - Table 7 *E1 HEMP Technical* Overview above shows the advantages of **burying cables** to protect against E1 or keeping the cables close to the ground. The

impact from the ground will help substantially reduce the pulse rise time and the peak voltage, which are the two major issues from E1.

> **"The DoD experience with facility and weapon system hardening indicates designed-in protection costs are 10 times lower than retrofit protection."**
> **Dr. George H. Baker,**
> Microgrids
> -A Watershed Moment
> (2020)

Although there may be some failures from radiated HEMP in untethered standalone equipment, this is generally considered low risk for most sites assuming that there are not any long, unshielded wires within outdoor equipment. However, **critical** sites may need to protect against radiated HEMP particularly with outdoor equipment or extremely critical equipment. Level 4 resilience may also employ other additional mitigations that are beyond the scope of this document. These may include Faraday cages, add-on EM resistive materials, and metal-lined conductive concrete with grounding in the walls/floors/ceilings. Typically, these are much less expensive to implement when either constructing a new building or making a major renovation versus a retrofit simply to add hardening.

For most organizations, the above can be implemented as a "**rolling change**" versus discarding existing equipment and immediately implementing the above but this should be based upon your risk management plan. For instance, when purchasing new SPDs, it is recommended that HEMP-rated ones be purchased instead of ones that are just used for lightning protection. A HEMP-rated SPD will likely cost more initially, but some of these SPDs do not degrade over time, which saves replacement costs and ensures protection against lighting and HEMP without needing to replace the SPD as frequently as every 1-2 years depending upon the location and the number of nearby lightning strikes. It is also expected that the cost of these SPDs will decrease with an expanded market share. Some of the other recommendations are only suggested for new buildouts for most organizations so that there will be minimal additional implementation cost (e.g., when installing large grounding cables in a new building, use flat copper cables instead of round ones). Each organization's timeframe will be different based upon its resilience level, its existing power resiliency solution, its resiliency power plans, and available funds.

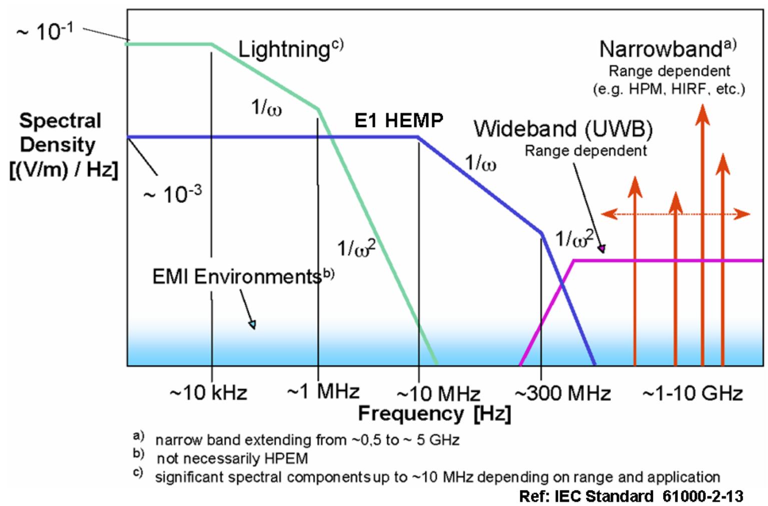

Figure 5. Frequency ranges of lightning, EMP, and IEMI

When applying E1 HEMP mitigations to protective relays, the potential for unintended consequences of the mitigation should be considered in the design process and appropriate measures taken to ensure that system performance is not adversely affected. As shown in Figure 5, the E1 HEMP electric field "is generally most important at frequencies below 300 MHz" (IEC 61000-2-13, p. 11).

Generator E1 HEMP Mitigations

Procure EMP tested and certified generators if possible. Limited testing of unprotected backup generators has shown that E1 HEMP can damage control electronics on some units. Therefore, these control electronics should be HEMP protected as discussed above. With respect to the actual generator, U.S. government radiated testing of some **portable** diesel generators revealed no problems, but these tests were performed without conductive cables attached and on just a limited set of portable generators (most larger sites use fixed generators). EMP certification testing of generators by the manufacturer or customer is necessary for confidence in generator survivability. Given the need for more testing, the following **generator-related protections** are recommended per resilience level depending on your site's risks:

- Level 1 – If a power cable is left outdoors and permanently attached to a generator, either (i) shield the cable or (ii) run the power cable underground or on the ground and connect the cable to an SPD prior to connecting it to any important equipment.
- Level 2 – Use shielded power cables if left permanently attached to the generator.
- Level 3 – Only use shielded, circumferentially-bonded power cables. Enclose generator in an EMP-resilient metal container (common cargo containers as an example) or use an EMP tested generator.
- Level 4 – Shield cables and either apply EM shielding around the generator or use EMP-survivable generator systems that have been certified by threat-level tests for critical infrastructure applications. Since EMP vulnerabilities are primarily caused by conducted transients on incoming conducting lines, pulse current injection testing on generator system shielded cables is essential to certify generator survivability.

Success Story

Some critical infrastructure owners use multi-purpose modules to protect equipment and people against several threats including HEMP, lightning and IEMI for minimal incremental cost versus previous solutions without the extra protections.

4.2. E2 HEMP and Lightning

Except in areas where lightning is uncommon, a fundamental part of critical infrastructure power system designs is good lightning protection. This also protects against HEMP E2 unless the line is long as described in Table 8.

Engineering guidelines and standards are readily available for lightning protection. These include the following documents, which are recommended for use in achieving lightning protection (and are also applicable to E2 HEMP and E1 HEMP in some cases):

- Motorola *R56 Standards and Guidelines for Communication Sites*[73] or other recognized grounding standard that provides grounding guidelines for communications sites.
- NFPA Code 780 *Standard for the Installation of Lightning Protection Systems*[74] coverage includes system installation lightning protection for traditional building structures and newer ones such as wind turbines and solar arrays. It is used in many parts of the world, including the U.S.
- *UL 1449 Standard for Surge Protective Devices (SPDs)*.[75]

- *TM 5-690 GROUNDING AND BONDING IN COMMAND, CONTROL, COMMUNICATIONS, COMPUTER, INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (C4ISR) FACILITIES*

If the site does not have lightning protection since presumably it is in an area where there is little or no lightning, protecting against E2 (and E1) HEMP should be added per these best practices. One potential difference between lightning and E2 protection is that when a conductive cable is run aboveground for more than 1 km, extra surge protection may be needed per IEC 61000-2-10 (p. 25) as shown below in Table 8 (see IEC 61000-2-10, p. 49). This is because the E2 field can remain consistent over long distances while a lightning EM field will quickly drop off as the distance increases from the lightning strike.

Table 8. E2 HEMP Specifications and Mitigations

Cable Length and Position	**Maximum E2 Conductivity** (assumes cable is conductive)	**Suggested Mitigations versus Standard Lightning Protection**
> 1 km, Buried	• **Same as at 1 km** unless there is very poor ground conductivity • Peak currents vary only with the ground conductivity	No extra surge protection is generally required.
> 10 km, Elevated	• With Good Ground Conductivity = 140 A • With Poor Ground Conductivity = 350 A • With Very Poor Ground Conductivity (over industrial area or polar ice cap[76]) = 850 A • Pulse width at half maximum of 693 μs (IEC 61000-2-9, p. 31).	• Typically use a heavy-duty industrial SPD.
> 1 km and < 10 km, Elevated	• Approaches above specifications as cable length approaches 10 km.	• Use a heavy-duty SPD if > 200 A. • Can use wall outlet SPD if < 200 A.

4.3. E3 HEMP and GMD

E3 HEMP is the result of a high-altitude nuclear explosion and GMD is the result of solar flares that are followed by coronal mass ejections (CMEs) of charged and magnetized particles into space. The probability of an E3 HEMP act of war or terrorist event, which would occur when an E1 HEMP event also occurs, is currently being assessed by DHS but is likely to be considered low probability. A major solar geomagnetic disturbance (GMD) has a known probability of 10% - 12% per decade.[77] However, either event could cause power grid and communication network debilitation over large geographical regions and therefore are national security concerns.

The high-level technical specifications are listed below in *Table 9. E3 HEMP and GMD Specifications* with further discussion in *Appendix C* subsections *E3 HEMP and GMD Technical* Characteristics and *E3 HEMP and GMD* Impacts. Because the impact from E3 HEMP and GMD events is strictly with long conducting lines (more than 10 km), this section only directly addresses the potential harmonics generation caused by E3 HEMP and GMD. If long lines (over 10 km) with metal are deployed, such as might occur in an archipelago (multiple microgrids connected together), a long telecommunications or networking line containing metal, or large manufacturing plants that are connected to long power lines, please read *Appendix C*

ADDITIONAL E3 HEMP AND GMD DETAILS. Note: E3 EMP and GMD can also increase drag on very-low-earth-orbit satellites (below 400 km); however, this situation is not within scope of this document.

Table 9. E3 HEMP and GMD Specifications

EM Type	**Maximum Conductivity** (assumes cable is conductive)
E3 HEMP (DOE Waveform)	• Rise time on the order of seconds to 10s of seconds • Pulse duration on the order of 10 to 100 seconds.
GMD	• Has a significantly lower maximum radiated field strength than E3 HEMP but can extend over a much greater region than a single E3 HEMP event. • Can have multiple pulse trains lasting for hours to days with individual pulses persisting for minutes.

E3 HEMP and Geomagnetic Disturbance (GMD) Mitigations

To mitigate the AC voltage harmonics issue discussed in *Appendix C E3 HEMP and GMD Impacts* and prevent upsets or damage, the following are generally recommended:

- **Implement Harmonics Standards** – To reduce potential harmonics of all types, follow a standard such as IEEE 519-2014 – IEEE Recommended Practice and Requirements for Harmonic Control in Electric Power Systems[78] or protect the equipment at an individual level.
- **Install Redundant Switchover Mechanism** – All sites should have a secondary method to switchover its power system if the primary automated transfer switch (ATS) fails as discussed in *Section 6.1 Power Transfer System*. This secondary mechanism should not have a potential common E3/GMD related failure mode with the primary ATS. For instance, having two ATS systems hooked up independently to the electrical grid where both are collocated, or both could fail due to an EMP is not fully redundant.
- **Add Time Delay if ATS Fails** – If an ATS is damaged or is upset (e.g., reboots unexpectedly), the site should remain in island mode either until it is determined why the ATS was damaged or upset, or it can be confirmed that no EM stress is still occurring (see Section 6.1 *Power Transfer System*).
- **Use EM Resilient UPSes** – See Section 7.3 *UPS Guidance* for the best UPSes to use, such as an online double conversion UPS or a high-quality line interactive UPS with good surge suppression and noise filtering that can prevent the harmonics from traveling further into the site's power system.
- **Work with Utility (Level 3 or 4 Resilience)** – Consider working with the utility company to ensure that the utility's distribution system will not introduce or pass harmonics into the site's power system and to understand how long it might take to perform a black start under worst case conditions if an excessive number of transformers are lost. Note: Per TPL-007-4, NERC requires all power companies to have implemented corrective action plans no later than the end of 2028 to address a 100-year GMD event. However, these protection levels may not be sufficient since they are based upon an outdated 1D Earth model and not on the latest 3D GMD calculations and magneteulliric (MT) survey data.

- **Protect Onsite Transformers (typically only applicable to large campuses)** – Campuses with high voltage transformers on site that are connected to long power lines (at least over 10 km) should consider working with their utility provider or their electrical contractor to protect the transformer. This may include adding modest low levels of additional resistance at the transformer neutral. This low-cost additional resistance can reduce GMD currents that otherwise have the potential to damage transformer windings (usually at the lower voltage end) or that could cause harmonic distortion, vibration, or other damage.
- **Prepare HEMP and GMD Action Plans** – Create *operational procedures* to minimize the impact and recovery time from the effects of HEMP or GMD after receiving notification of a potential or imminent GMD or HEMP event from a reputable source (e.g., *Space Weather Prediction Center*, FEMA's National Public Warning System) or from a nuclear event detector. These procedures should include when to switch to island mode to prevent potential harmonics from entering the critical infrastructure power system and include restoration procedures.

A low pass filter that passes 60 Hz but filters 120 Hz and higher can eliminate the AC voltage harmonics issue. This approach works well for communication lines but is difficult to implement on power lines. Allowing 60 Hz AC to pass while eliminating 120 Hz or 180 Hz harmonics is difficult to impossible with today's technologies.

Because local enterprise power systems do not use long line infrastructure unless an archipelago is implemented (multiple connected microgrids and control networks), E3 and GMD will likely not damage a site's independent power system when in island mode except under extenuating circumstances assuming that the power equipment is in reasonable shape. Even microgrids that are implemented on large campuses (up to several miles long) are unlikely to be damaged by E3 and GMD when disconnected from the grid although HEMP E1 can damage or upset equipment as discussed in the previous section.

4.4. Electromagnetic Interference (EMI) and Intentional EMI (IEMI)

With more and more wireless transmitters together with improvements in technology enabling higher power attacks with smaller, mobile devices, both EMI and IEMI are becoming bigger potential issues. For instance, "devices that can be used as [Radio Frequency Weapons] RFWs have unintentionally caused aircraft crashes and near-crashes, pipeline explosions, large gas spills, computer damage, medical equipment malfunctions, vehicle malfunctions such as severe braking problems, weapons pre-ignition and explosions, and public water system malfunctions that nearly caused flooding." RFWs have also been used intentionally to "defeat security systems, commit robberies, disable police communications, induce fires, and disrupt banking computers."[79]

Although EMI and IEMI are very localized compared to HEMP, their field peak power levels can be much higher than with the HEMP EM fields. Plus, both EMI and IEMI often involve broadband or narrowband sources that typically operate at much higher frequencies (up to 10 GHz or higher), particularly with the IEMI sources. The limited range of IEMI sources can be partially overcome by mounting them on UAVs. In addition to the EM source's duration, bandwidth, and pulse repetition, the coupled energy from an EMI or IEMI into a device or system is dependent on the following:

- The distance between the EM source and the target

- The susceptibility of the electronics and the system to the source EM field
- The propagation loss including the attenuation properties of intervening barriers/shielding.

Both cybersecurity and physical security personnel need to understand their role in protecting against these EM spectrum attacks partially since IEMI may be used in combination with physical and cyberattacks.

To be resilient against EMI and IEMI, at-risk critical infrastructure sites should implement the below best practices including those listed in Table 10. Most of these best practices for Levels 1-3 typically should be implemented to protect against physical, HEMP, or EMI threats so the cost to defend specifically against IEMI is often very minimal.

- **E1 HEMP Protection** – Implement the E1 HEMP best practices noted earlier in this chapter, which add progressively increased protection for each resilience level, is one of the first steps to help protect against both EMI and IEMI.
    - Procure electronic equipment that meet EMI standards, such as IEC/EN 55035 "Electromagnetic compatibility of multimedia equipment – Immunity requirements" (equipment should tolerate at least 3 V/m) to protect against IEMI frequencies that can be up to or even beyond 10 GHz, which is significantly higher in frequency than E1 HEMP. While adhering to such standards will help ensure good engineering practices from an EMI perspective, the very low electric field levels associated with these standards means that, where feasible, efforts should be undertaken to reduce the potential incident field levels caused by IEMI using local EM shielding techniques.
    - If HEMP shielding is installed, extend the shielding frequency domain effectiveness up to 10 GHz and protect against repetitive pulse or continuous wave attacks.
- **Telecommunications Resiliency** – All critical infrastructure facilities can gain IEMI and EMI protection against jamming and equipment disruptions by implementing Section *2.5 Telecommunications,* which includes each site having multiple communications capabilities. Also, see the CISA *Radio Frequency Interference Best Practices Guidebook*[80], which is also included in the "Jamming" cloud in CISA's Public Safety Toolkit (see Figure 6 below).
- **IEC 61000-2-13**, High Power Electromagnetic (HPEM) Environments, Radiated and Conducted.

Figure 6. CISA's Public Safety Resiliency Toolkit

Because IEMI is typically limited to either damaging or upsetting equipment at a single nearby site or jamming the wireless communications in a localized area (e.g., within part of a city), implementing IEMI protections beyond the above recommendations is probably not cost effective for most **Level 1** resilience facilities. Note: The amount of protection against IEMI that needs to be implemented is also dependent upon how much downtime the site can endure since IEMI attacks that do not damage equipment can be thwarted given enough time to detect, locate, and stop the attack.

Table 10. EMI/IEMI Protection Recommendations for Critical Sensitive Equipment

Resilience	Recommended Protections
Level 1	Follow the best practices listed previously in this section.
Level 2	Level 1 protections plus: • Implement at least a small secure perimeter as discussed in *Section 3.2 Physical Security* or add EM barriers such as metal enclosures, thin film wall liners, or conductive window treatments between a potential EMI/IEMI source and critical equipment. • Sensors should use wired communications or IEMI-resistant wireless.

Resilience	Recommended Protections
Level 3	Level 2 protections plus: • If only a small secure perimeter is implemented, the critical electronics should be shielded. • Protect against jamming and potential RFW accidents and attacks that may damage or disrupt the readings of a critical sensor. • Broadband RF detectors are helpful to alert operators to the presence of abnormal EM fields. • Implement at least some aspects of the CISA publication "*Protecting Against the Threat of Unmanned Aircraft Systems (UAS)*" including posting signs that UAVs are not allowed. • Use the above protections and others if needed to protect against IEMI attacks at higher frequencies including either using SPDs that can mitigate multiple pulses or storing spare SPDs.
Level 4	Level 3 protections plus: • Implement a large secure perimeter. • Protect against unknown vehicles and drones that might either contain a powerful RF Weapon (for example, see Boeing: CHAMP – Lights Out[81] where a cruise missile emitted bursts of high-powered energy and disrupted rows of computers inside a building) or could conduct a physical attack. • Follow the recommendations in the CISA publication "*Protecting Against the Threat of Unmanned Aircraft Systems (UAS)*" (November 2020). • Perform an EM spectrum audit of the facility using available geospatial and terrain data to determine the most likely approaches for IEMI threats to the facility. • Based upon the EM spectrum audit and worst-case threat assessment model (including existing barriers), install EM spectrum shielding to protect equipment and cables, move equipment to better shielded areas, and bury cables underground. • Broadband RF detectors should be deployed to alert operators to the presence of abnormal EM fields.

If an organization uncovers an RF Weapon or IEMI attack, it should immediately notify law enforcement. People should avoid being in the path of an RF Weapon's EM field since exposures can create damaging thermal effects in body tissues.