



# **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)

## Target Audience / How to Use This Document

This document was developed by the Cybersecurity and Infrastructure Security Agency (CISA) working with the Resilient Power Working Group (RPWG) to provide resilient power best practices for critical facilities and sites (excluding electrical and natural gas utility companies). It is recommended that personnel, including contractors and vendors, involved in the following read or browse this document:

- Chief engineers or power managers/engineers
- Continuity planning, government, and business emergency preparedness
- Operations and maintenance
- Procurement and those involved in the acquisitions of power related systems or components
- Security: Cybersecurity, physical security, and facilities
- Telecommunications, electromagnetic (EM) security, and information technology (IT) when responsible for specifying the telecommunications solutions, installing telecommunications or IT equipment, or EM protection
- Executives and managers with responsibilities for any of the above.

It is suggested that individuals in these categories start by reading the Executive Summary. Subsequently, each user can quickly focus on just one topic at a time if desired taking advantage of the document being broken down into chapters, sections, and subsections. However, to effectively implement the solutions and processes outlined in this document, target audiences should ultimately read or browse what is indicated below in Table 1.

**Table 1. Target Audience Matrix**

Role	Ch 1 Introduction	Ch 2 Best Practices	Ch 3-4 Cyber, Physical, and EM Security	Ch 5-7 Core Components	Ch 8-9 Clean Energy
<b>Executives</b>	Browse, Read 1.4	Browse, Read 2.1, 2.2	Browse	-	Browse if considering
<b>Power Management/ Engineering</b>	Read	Read	Read	Read	Browse/ Read if considering
<b>Continuity Planning</b>	Read	Read	Read 3, 4.1	Browse/Read	Browse/ Read if considering
<b>Procurement</b>	Browse, Read 1.4	Read 2.1, 2.2, 2.3 Browse 2.4, 2.5	Read 3.1 Supply Chain Security	Browse	Browse if considering
<b>Cybersecurity</b>	Browse, Read 1.4	Browse	Read 3, and 4.4; Browse 4.1-4.3	-	-

Role	Ch 1 Introduction	Ch 2 Best Practices	Ch 3-4 Cyber, Physical, and EM Security	Ch 5-7 Core Components	Ch 8-9 Clean Energy
Physical Security	Browse, Read 1.4	Browse 2.3	Read 3, 4.4		
Telecom, IT, EM Security	Browse, Read 1.4	Browse 2.1, 2.2, Read 2.3 - 2.5	Browse 3, Read 4		

To reduce costs and improve resiliency, implementation of these best practices and guidelines should be performed holistically. For instance, cybersecurity, physical security, EM security, and fuel considerations could impact the selection and location of the backup power generation solution so these best practices should be considered in unison. In this example, not only should Chapter 5 *GENERATORS AND FUEL* be read, but also the other chapters/sections indicated in Table 1 to ensure that an appropriate resilient power solution is identified, implemented, and maintained.

# Executive Summary

This *Resilient Power Best Practices for Critical Facilities and Sites* document was created after members of the federal interagency Continuity Communications Managers Group (CCMG) determined that most widespread, long-term communications outages were caused by loss of power and that there was no best practices document addressing this issue from an enterprise/agency perspective. Further, per the U.S. Energy Information Administration (EIA), the average number of hours of power interruptions due to major events has increased since the EIA began collecting electricity reliability data in 2013 from less than two hours in 2013 to more than six hours in 2021 (power outages excluding major events was consistent at about two hours).

This document addresses the above power issues from a non-utility perspective and helps the reader improve their understanding of resilience, determine the criticality of their systems to remain operational, identify the risk factors and make educated business decisions on both small and large investments in resilient power solutions that will help ensure business continuity.

The potential solutions discussed in this document consider dependability, cost, long-term capabilities, and applicable regulations. These best practices recognize that nothing is 100% reliable nor protectable under all conditions and that there are trade-offs that often must be made between resiliency and budget with the best solution dependent upon the mission needs and risks.

Nevertheless, the RPWG expects that many critical infrastructure facilities will attain significantly better resilience with a positive return on investment (including the Value of Lost Load) if they implement the best practices in this document (e.g., both use cases discussed in the *Renewable Energy Hybrid System (REHS) Sample Use Cases* section show a positive return on investment).

**For many sites, implementing these resiliency best practices is inexpensive and will increase resiliency.**

To easily identify the resilient power best practices that stakeholders may want to use for planning, procurement, and implementation purposes, four resilience levels are defined. Similarly to the use of levels with other organizations (e.g., Cybersecurity Maturity Model Certification, [Program Review for Information Security Assistance | CSRC \(nist.gov\)](#)), the higher the level, the better the resilience in general.

These levels, summarized below, are based upon the organization's risk management plan and FEMA's "all hazards" concepts, which in [Glossary \(fema.gov\)](#)<sup>1</sup> is defined as "natural, technological, or human-caused incidents that warrant action to protect life, property, environment, and public health or safety, and to minimize disruptions of school activities." Thus, local, utility, and facility risk factors may dictate a lower or higher resilience level for some threats/hazards than for others. Local conditions including the time required for power to be restored and for fuel to be delivered under the identified risk factors may lead to more or less time than suggested below for backup power to be maintained.

- **Level 1 Resilience** – Incorporates cost effective best practices to maintain power to critical operations. Typically, expendable supplies, such as fuel, should be maintained for three days under "all hazards" that are germane to the risk management plan.
- **Level 2 Resilience** – Extends Level 1's cost-effective practices to further improve power resiliency. Typically, expendable supplies, such as fuel, should be maintained for seven days under "all hazards" that are germane to the risk management plan.

- **Level 3 Resilience** – Implements additional measures beyond Level 2 to further improve power resiliency. Typically, expendable supplies, such as fuel, should be maintained for around 30 days under “all hazards” that are germane to the risk management plan.
- **Level 4 Resilience** – Power should be sustained with no unplanned downtime. Typically this is limited to the most critical military/federal/National Essential Functions.

Although backup power timeframes provided in the above definitions are for fuel related best practices, the primary drivers of this timeframe are the threat environment, the vulnerabilities, and the organizational risk tolerance associated with the identified risks. For instance, some critical facilities are designed to operate for only a short period of time on backup power while critical operations are transferred.

To help select and implement the best resilient power solution for your situation, this document provides an overview of the key traditional (e.g., generators) and newer (e.g., renewables, microreactors) backup power technologies, processes, regulations, and agencies that could affect the selection. *Table 2* highlights best practices that can help the owner/operator implement and maintain the best resilient power solution for their critical infrastructure based upon the organization’s Resilience Level and risk management plan. These are further explained in the main body of the document in Section 2.3, which should be consulted prior to implementing any of the below listed recommended best practices.

**Table 2. Recommended Best Practice Highlights**

Functional Area	Design and Process Best Practice Highlights (each resilience level may vary based upon specific facility or site risks and specific mission needs)
<b>Process, Governance and Maintenance</b>	<ul style="list-style-type: none"> <li>• Document a risk management plan that includes the resilient power threat environment, the vulnerabilities, and the organizational risk tolerance associated with the identified risks.</li> <li>• Determine resilience level needed, document requirements, and conduct gap analysis.</li> <li>• Join appropriate sector/geographically based information sharing organizations such as <a href="#">InfraGard</a>, the <a href="#">National Council of ISACs</a> and preparedness networks like your local Community Emergency Response Team (<a href="#">CERT</a>).</li> <li>• Schedule regular audits to ensure that the Planning, Organization, Equipment, Training, and Exercises (POETE) in the O&amp;M Plan supports the desired resilience level.</li> <li>• Include preparedness of employees and vital external businesses in the O&amp;M Plan to ensure continuity of operations during extreme events.</li> <li>• Establish processes to “stress test” readiness through periodic plan reviews, operational tests, and table-top and “real world” exercises.</li> </ul>
<b>Backup Generation Sources</b>	<ul style="list-style-type: none"> <li>• Maintain at least two backup generation sources for Level 3 resilience and typically for Level 2 unless the primary and backup power sources are resilient enough to meet Level 2.</li> <li>• Level 4 resilience sites should utilize two independent utility/primary power sources plus two independent and geographically separated (within the site) back-up power sources.</li> <li>• Ensure the backup generation sources achieve longevity per the desired resilience level.</li> <li>• Perform and document regularly scheduled maintenance and load testing.</li> <li>• Consider fuel diversification to prevent fuel supply disruptions.</li> </ul>

Functional Area	Design and Process Best Practice Highlights (each resilience level may vary based upon specific facility or site risks and specific mission needs)
Fuel	<ul style="list-style-type: none"> <li>• Store enough fuel onsite to meet the desired “all hazards” resilience level.</li> <li>• Deploy a fuel maintenance process, including fuel rotation.</li> <li>• Document emergency delivery alternatives and regularly assess fuel delivery contracts to help ensure that third parties will be able to deliver during outages.</li> </ul>
Control Systems and Microgrids	<ul style="list-style-type: none"> <li>• Segment power loads and conserve resources so that critical loads are adequately powered.</li> <li>• Consider implementing an all-hazards secure microgrid in Level 3 sites or on large campuses.</li> <li>• Maintain a protected, redundant industrial control system (ICS) and electrical distribution system.</li> </ul>
Renewable Energy and Energy Storage	<ul style="list-style-type: none"> <li>• Consider implementing a renewable energy hybrid system (REHS), which combines renewables with an energy storage system (ESS) and a 24/7 backup generation system, to extend fuel supplies and improve power resilience while reducing annual electricity costs.</li> <li>• Deploy hardened uninterruptible power supply (UPS) systems to support sensitive critical systems.</li> </ul>
Tele-communications	<ul style="list-style-type: none"> <li>• Ensure critical telecommunications are prioritized for emergency power and integrated into the Operations and Maintenance Plan.</li> <li>• Deploy telecommunications diversity (e.g., cellular, satellite, landline, high frequency [HF] radio) and follow the PACE model (Primary, Alternate, Contingency, and Emergency) if immediate communications are needed.</li> </ul>
Cybersecurity	<ul style="list-style-type: none"> <li>• Include supply chain security (e.g., third-party access to the control software) and a zero-trust security model in the cybersecurity plan.</li> <li>• Follow industry cybersecurity standards, e.g., North American Electric Corporation (NERC) CIP-009-6, NIST Cybersecurity Framework.</li> </ul>
Physical Security	<ul style="list-style-type: none"> <li>• Add specific threats, existing security, and site vulnerabilities into the physical security plan.</li> <li>• Red team the physical security plan by working with law enforcement and security contractors.</li> </ul>
Electromagnetic (EM) Security	<ul style="list-style-type: none"> <li>• Implement mitigations per the Risk Management Plan to help protect against the EM effects of lightning, high-altitude EM pulse (HEMP), EM Interference (EMI) and Intentional EMI (IEMI).</li> </ul>

Given the growing potential consequences of grid-related power outages, it is recommended that organizations needing to be Level 1-4 resilient power per their risk management plan quickly achieve at least a Level 1 or 2 resilience capability. Implementing the best practices for these resilience levels is relatively inexpensive and the initial investment might be recuperated after only one short-duration power outage. To get the most impact per dollar, a holistic approach is recommended since it will do little good if, for example, an organization has plenty of fuel but has not maintained the fuel properly or if its only generator fails.

These *Resilient Power Best Practices for Critical Facilities and Sites* should be a part of comprehensive, risk-informed Business Continuity and Continuity of Operations (COOP) plans, developed per [Federal Emergency Management Agency \(FEMA\) guidance](#)<sup>2</sup>. These best practices can help improve the resiliency of power systems during all durations of power outages and can help the nation “withstand and recover rapidly from deliberate attacks,

accidents, natural disasters, as well as unconventional stresses, shocks and threats to our economy and democratic system.”<sup>3</sup>

These resilient power implementation best practices were developed working with the [Resilient Power Working Group | CISA](#)<sup>4</sup> (RPWG) comprising of representatives from various federal, state, and local government departments and agencies, non-governmental organizations, and private industry. The effort was supported by the federal CCMG, which coordinates national security/emergency preparedness (NS/EP) communications planning and operations in support of federal continuity programs.

The importance of preparedness, networking (developing personal relationships), and information sharing *prior* to a power outage cannot be understated. Together, we can reduce the consequences from short-term outages while preparing for long-term outages that could cause substantial economic and societal issues including loss of life.

# Table of Contents

Target Audience / How to Use This Document .....	i
Executive Summary .....	iii
Table of Contents .....	vii
List of Figures .....	ix
List of Tables.....	x
<b>1. INTRODUCTION.....</b>	<b>1</b>
1.1. Purpose and Target Critical Infrastructure Sectors.....	1
1.2. Scope .....	3
1.3. Problem Background.....	5
1.4. Definition of Resilience Levels .....	9
<b>2. BEST PRACTICES .....</b>	<b>12</b>
2.1. Risk Management Plan .....	12
2.2. Resilient Power Requirements .....	15
2.3. General Design and Process Best Practices Summary.....	17
2.4. Operations and Maintenance (O&M) Plan.....	21
2.5. Telecommunications.....	24
<b>3. CYBERSECURITY AND PHYSICAL SECURITY .....</b>	<b>28</b>
3.1. Cybersecurity .....	28
3.2. Physical Security.....	36
<b>4. ELECTROMAGNETIC (EM) SECURITY .....</b>	<b>39</b>
4.1. E1 High-Altitude EM Pulse (HEMP).....	40
4.2. E2 HEMP and Lightning .....	45
4.3. E3 HEMP and GMD .....	46
4.4. Electromagnetic Interference (EMI) and Intentional EMI (IEMI).....	48
<b>5. GENERATORS AND FUEL .....</b>	<b>52</b>
5.1. Diesel and Gas Generator Overview .....	52
5.2. Diesel versus Natural Gas/Propane Comparison .....	56
5.3. Fuel and Generator Maintenance Procedures .....	61
5.4. Diesel and Natural Gas/Propane Fuel Deliveries.....	67
5.5. Emergency Generator Deliveries and Mobile Power.....	71
<b>6. POWER TRANSFER SYSTEMS AND MICROGRIDS .....</b>	<b>74</b>
6.1. Power Transfer System .....	74
6.2. Microgrid Definition and Purpose.....	76
6.3. Microgrid Benefits and Issues .....	78
<b>7. ENERGY STORAGE.....</b>	<b>83</b>
7.1. Energy Storage System (ESS).....	83
7.2. Centralized Versus Local Energy Storage (LES).....	84
7.3. UPS Guidance.....	87
7.4. Battery Energy Storage Systems (BESSes).....	87
7.5. Other Energy Storage System (ESS) Technologies.....	90
<b>8. RENEWABLE ENERGY.....</b>	<b>92</b>
8.1. Renewable Energy Overview.....	93



8.2.	Solar Power .....	95
8.3.	Fuel Cells.....	99
8.4.	Wind Power and Other Renewable Energy Sources.....	102
8.5.	Intermittent Renewable Energy Hybrid System (REHS) Guidance .....	104
8.6.	Renewable Energy Hybrid System (REHS) Sample Use Cases.....	109
<b>9.</b>	<b>NUCLEAR SMALL MODULAR REACTORS (SMRs) .....</b>	<b>114</b>
9.1.	General SMR Background.....	114
9.2.	SMR Technical Details and Benefits.....	116
9.3.	SMR Procurement Opportunities and Activities .....	119
<b>Appendix A.</b>	<b>REGULATORY AND UTILITY POWER GENERATION ENVIRONMENT .....</b>	<b>A-1</b>
<b>Appendix B.</b>	<b>NIST CYBERSECURITY FRAMEWORK CORE FUNCTIONS.....</b>	<b>B-1</b>
<b>Appendix C.</b>	<b>ADDITIONAL E3 HEMP AND GMD DETAILS.....</b>	<b>C-1</b>
<b>Appendix D.</b>	<b>REMOTE HOSPITAL SOLAR-BASED REHS USE CASE .....</b>	<b>D-1</b>
<b>Appendix E.</b>	<b>NUCLEAR SMR VENDOR OFFERINGS .....</b>	<b>E-1</b>
<b>Appendix F.</b>	<b>ACKNOWLEDGEMENTS.....</b>	<b>F-1</b>
<b>Appendix G.</b>	<b>ACRONYMS .....</b>	<b>G-1</b>
<b>Appendix H.</b>	<b>REFERENCES .....</b>	<b>H-1</b>

## List of Figures

Figure 1. Three Regional Interconnection Grids	6
Figure 2. Flooding during Hurricane Katrina	7
Figure 3. 1962 Starfish Prime HEMP impacted electronics with a relatively small peak field	39
Figure 4. Generic HEMP waveform (ref. Meta-R-324)	41
Figure 5. Frequency ranges of lightning, EMP, and IEMI	44
Figure 6. CISA's Public Safety Resiliency Toolkit	50
Figure 7. Natural Gas Distribution	54
Figure 8. Basic backup power system includes island mode	77
Figure 9. Smart microgrid system enables grid augmentation	77
Figure 10. Conceptual microgrid architecture consists of a REHS and load segmentation	78
Figure 11. Open-loop Pumped-Storage Hydropower (courtesy of DOE)	90
Figure 12. Natural gas and renewables have increased significantly since 2000	92
Figure 13. Wind and solar power have substantially increased since the early 2000s	93
Figure 14. A REHS microgrid has multiple sources of onsite power generation	94
Figure 15. U.S. solar irradiance is strongest in the southwest	97
Figure 16. Traditional Wind Farm (courtesy of DOE)	102
Figure 17. Compact Wind Turbine (courtesy of American Wind, Inc.)	102
Figure 18. Wind speeds indicate that the Plains states are excellent for wind power	103
Figure 19. U.S. monthly solar production shows strong seasonal dependency	107
Figure 20. REHS triples outage survivability versus using only a diesel generator (NREL)	110
Figure 21. Site's resiliency increases to Level 2 with a REHS (courtesy of muGrid Analytics)	111
Figure 22. Decreasing the critical load increases resiliency (courtesy of muGrid Analytics)	113
Figure 23. Migration to Gen IV Nuclear Reactors (courtesy of Idaho National Laboratory)	115
Figure 24. NuScale Power Module (courtesy of NuScale)	117
Figure 25. Sources of U.S. Electricity (source: Monthly Energy Review, EIA, Aug 2021)	A-3
Figure 26. Site's power resiliency doubles with a REHS (courtesy of muGrid Analytics)	D-1
Figure 27. A small load reduction leads to Level 3 resilience (courtesy of muGrid Analytics)	D-3
Figure 28. Broad landscape of non-LWR advanced reactor designs (NRC)	E-1

## List of Tables

Table 1. Target Audience Matrix	i
Table 2. Recommended Best Practice Highlights	iv
Table 3. Resilient Power Best Practices Summary	17
Table 4. Potential Telecommunications Capabilities	26
Table 5. Leading Types of Cybersecurity Attacks	30
Table 6. Recommended Cybersecurity Mitigations (applicable to all resiliency levels)	31
Table 7. E1 HEMP Waveform Specifications	41
Table 8. E2 HEMP Specifications and Mitigations	46
Table 9. E3 HEMP and GMD Specifications	47
Table 10. EMI/IEMI Protection Recommendations for Critical Sensitive Equipment	50
Table 11. ISO 8528 Generator Ratings	53
Table 12. Costs of Diesel Generators Compared to Natural Gas/Propane Generators	56
Table 13. Non-cost Related Issues of Diesel versus Natural Gas/Propane Generators	57
Table 14. Diesel and Natural Gas/Propane Best Practices	59
Table 15. Example Showing Benefits of Using Smaller Generation Sources	60
Table 16. Diesel and Natural Gas/Propane Generator Maintenance Activities	65
Table 17. Fuel and Generator Delivery Responsibilities	68
Table 18. Potential Microgrid Benefits Versus Traditional Power Backup Capabilities	79
Table 19. Comparison of Lithium-ion versus Lead Acid Batteries	88
Table 20. Solar Power Resiliency Best Practices	98
Table 21. An Intermittent REHS Compared to a Standby Generator Solution	105
Table 22. Fuel Type Versus Energy Density	116
Table 23. Types of Operating Reserve Bulk Power Electricity Generation (normal operation)	A-4
Table 24. NIST Cybersecurity Framework Core Functions	B-1
Table 25. Sample SMR Vendors, Highlights, Costs, and Status	E-2