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
Executives	Browse, Read 1.4	Browse, Read 2.1, 2.2	Browse	-	Browse if considering
Power Management/ Engineering	Read	Read	Read	Read	Browse/ Read if considering
Continuity Planning	Read	Read	Read 3, 4.1	Browse/Read	Browse/ Read if considering
Procurement	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
Cybersecurity	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.

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

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).

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)*[1] 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)
Process, Governance and Maintenance	• Document a risk management plan that includes the resilient power threat environment, the vulnerabilities, and the organizational risk tolerance associated with the identified risks. • Determine resilience level needed, document requirements, and conduct gap analysis. • Join appropriate sector/geographically based information sharing organizations such as InfraGard, the National Council of ISACs and preparedness networks like your local Community Emergency Response Team (CERT). • Schedule regular audits to ensure that the Planning, Organization, Equipment, Training, and Exercises (POETE) in the O&M Plan supports the desired resilience level. • Include preparedness of employees and vital external businesses in the O&M Plan to ensure continuity of operations during extreme events. • Establish processes to "stress test" readiness through periodic plan reviews, operational tests, and table-top and "real world" exercises.
Backup Generation Sources	• 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. • 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. • Ensure the backup generation sources achieve longevity per the desired resilience level. • Perform and document regularly scheduled maintenance and load testing. • Consider fuel diversification to prevent fuel supply disruptions.

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	• Store enough fuel onsite to meet the desired "all hazards" resilience level. • Deploy a fuel maintenance process, including fuel rotation. • Document emergency delivery alternatives and regularly assess fuel delivery contracts to help ensure that third parties will be able to deliver during outages.
Control Systems and Microgrids	• Segment power loads and conserve resources so that critical loads are adequately powered. • Consider implementing an all-hazards secure microgrid in Level 3 sites or on large campuses. • Maintain a protected, redundant industrial control system (ICS) and electrical distribution system.
Renewable Energy and Energy Storage	• 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. • Deploy hardened uninterruptible power supply (UPS) systems to support sensitive critical systems.
Tele-communications	• Ensure critical telecommunications are prioritized for emergency power and integrated into the Operations and Maintenance Plan. • 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.
Cybersecurity	• Include supply chain security (e.g., third-party access to the control software) and a zero-trust security model in the cybersecurity plan. • Follow industry cybersecurity standards, e.g., North American Electric Corporation (NERC) CIP-009-6, NIST Cybersecurity Framework.
Physical Security	• Add specific threats, existing security, and site vulnerabilities into the physical security plan. • Red team the physical security plan by working with law enforcement and security contractors.
Electromagnetic (EM) Security	• 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).

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[2]. 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."[3]

These resilient power implementation best practices were developed working with the Resilient Power Working Group | CISA[4] (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

List of Figures

List of Tables