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

1. INTRODUCTION

Target Audience:

- Power Management/Engineering, Continuity & Planning: *Read all*
- Executives, Procurement, Cybersecurity, Physical Security, Telecommunications and IT Installation: *Browse 1.1 – 1.3, Read 1.4*

1.1. Purpose and Target Critical Infrastructure Sectors

Purpose

"By failing to prepare, you are preparing to fail."
-- Benjamin Franklin

This document provides resilient power implementation best practices to federal, state, local, and industry critical infrastructure stakeholders to help ensure national continuity, which includes Business Continuity, and Continuity of Operations (COOP). Continuity is not strictly a governmental responsibility or limited to specific disciplines. National continuity, inclusive of federal and non-federal entities including all critical infrastructure owners and operators, encompasses an interdependency concept and culture that reaches across all communities, organizations, and individuals. All levels of leadership should consider continuity in operational planning.

Given that continuity of operations/business/government is a critical part of ensuring a resilient nation, it is imperative that federal and non-federal entities strengthen the power supply resiliency of their infrastructures against all hazards that could cause loss of critical infrastructure operations. This document was created to help fulfill the responsibilities of the Cybersecurity and Infrastructure Security Agency (CISA) Director and the Secretary of Homeland Security to:

- ''*Recommend measures necessary to* ***protect*** *the key resources and* ***critical infrastructure*** *of the United States* ***in coordination with other Federal Government agencies****, including Sector-Specific Agencies,* ***and in cooperation with State, local, tribal, and territorial government agencies and authorities, the private sector, and other entities.***" [The Cybersecurity and Infrastructure Security Agency Act of 2018, SEC. 2202 (e)(1)(F)] [December 2018]
- "*… 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.***" "*Critical infrastructure must be secure and able to* ***withstand and rapidly recover from all hazards***." [Presidential Policy Directive (PPD) 21 - Critical Infrastructure Security and Resilience] [February 2013]
- "*Develop a plan to* ***mitigate the effects of EMPs*** *on the vulnerable priority critical infrastructure systems, networks, and assets.*" [Executive Order 13865, Coordinating National Resilience to Electromagnetic Pulses (EMP), Sec. 6 (d)(i)] [March 2019]
- "*Promote the ability of emergency response providers and relevant government officials to* ***communicate in the event of natural disasters, acts of terrorism, and other man-made disasters***." [Emergency Support Function (ESF) #2 – Communications Annex of the National Response Framework (NRF)] [June 2016]

- *"… 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, Sec. 5.2. (b)] [July 2012]

To continue to operate and serve the country, operators of critical infrastructure need to rely on their own resilient backup power systems if a grid outage or collapse occurs that affects their systems. Therefore, CISA recognizes that an essential part of each of the above policies and of the organization's risk management plan is to promote and facilitate the adoption of *resilient power* capabilities for critical infrastructures – particularly those capabilities that are required to be resilient to *all hazards*. These best practices are also supported by the federal interagency Continuity Communications Managers Group (CCMG) to coordinate NS/EP communications planning and operations in support of the COG program.

This document provides best practices with background material, analysis, and guidelines on resilient power from the dependability, cost, and regulatory perspectives. It recognizes that nothing is 100% reliable under all conditions and that there are trade-offs that must be made between resiliency and budget with the best solution dependent upon the mission needs. The Resilient Power Working Group (RPWG) expects that in many cases, critical infrastructure facilities will obtain a positive return on investment (includes Value of Lost Load) if they implement these best practices as discussed in Section *8.6 Renewable Energy Hybrid System (REHS) Sample Use Cases*.

The document also addresses critical infrastructure protections against multiple potential power outage risks including various possible durations of power outages. It encourages stakeholders to understand the required resilience level for their critical infrastructure and develop appropriate resilient power requirements. This information can then be used to proactively assess and reassess the resilience and dependability of the back-up and emergency power equipment and to implement the needed changes and updates to meet the requirements. This includes the dependability of their various supply chains in a prospective grid-down scenario, and the preparedness to endure a long-term outage.

Critical Infrastructure Sectors

The audience for this document is **all governmental and civilian** stakeholders **of critical infrastructures** excluding the electric utilities and natural gas pipeline systems. 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 sector risk management agencies (SRMAs) (see www.dhs.gov/cisa/critical-infrastructure-sectors for more information):

1. Chemical (SRMA: DHS)
2. Commercial Facilities (SRMA: DHS)
3. Communications (SRMA: DHS)
4. Critical Manufacturing (SRMA: DHS)
5. Dams (SRMA: DHS)

6. Defense Industrial Base (SRMA: Department of Defense (DOD))
7. Emergency Services (SRMA: DHS)
8. Energy (SRMA: Department of Energy (DOE)) (guidelines for this sector are generally not included in this document)
9. Financial Services (SRMA: Department of Treasury)
10. Food and Agriculture (SRMAs: Department of Agriculture and Department of Health and Human Services (HHS))
11. Government Facilities (SRMAs: DHS and General Services Administration (GSA))
12. Healthcare and Public Health (SRMA: HHS)
13. Information Technology (IT) (SRMA: DHS)
14. Nuclear Reactors, Materials, and Waste (SRMA: DHS)
15. Transportation Systems (SRMAs: DHS and the Department of Transportation (DOT))
16. Water and Wastewater Systems (SRMA: Environmental Protection Agency (EPA))

Document guidance is applicable to requirements of Executive Order 13961—*Governance and Integration of Federal Mission Resilience.* The document can also be used as best practices for entities *not* associated with critical infrastructure. The nation's resilience will increase as more Americans embrace increased levels of personal preparedness and their employers, both in government and in the private sector, adopt methods of increased self-sufficiency, including all-hazards resilient power.

1.2. Scope

"There are no secrets to success. It is the result of preparation, hard work, and learning."
-- Colin Powell

This document recommends resilient emergency and backup power best practices for critical facilities and sites. The best practices cover resilient power in a holistic manner recognizing that systems, equipment, and operations typically can be operated only within specified environments (e.g., the temperature is not too high or too low for the equipment nor for the people working in the environment). Thus, for IT equipment or communications networks to function as intended, climate control systems, safety systems (e.g., fire detection and suppression), lighting, physical entry control, industrial control systems (ICSes), and support equipment also need power.

These best practices can be applied to a small site such as a public safety or cellular communications tower or they can be implemented to improve resilience at a large campus. More specifically, this document covers the following to appropriately reduce the risk of power outages according to a pre-defined power resiliency "level" (explained further below under *Definition of Resilience Levels*) from the time when a blackout commences until grid power is restored:

- **Process and maintenance** to help ensure that a resilient power architecture is implemented effectively and efficiently and that the power-related equipment and supplies are maintained properly. Best practices covering Planning, Organization, Equipment, Training, and Exercises (POETE) are also discussed.

- **Emergency or backup power generation systems**, including traditional diesel and gas generators, renewable energy generation systems ("renewables") (e.g., solar, wind, fuel cells, hydropower) and small modular reactor (SMR) units considering both cost and resiliency.
- **Power transfer systems and microgrids** to help ensure resilient power and to optimize the use of power generation sources.
- **Energy storage** both to ensure continuous regulated power prior to emergency power generation/distribution and to increase resiliency using renewables.
- **Cybersecurity, physical security, and electromagnetic (EM) security** to protect the power supply system. Cybersecurity is particularly important if any critical equipment is connected to the Internet, an enterprise's Intranet, or Supervisory Control and Data Acquisition (SCADA) networks. Physical security, which can often become more important during a blackout, is critical to protect against attacks, natural hazards, and theft. EM security is essential since scenarios exist where EM effects from a single event can shut down large portions of the North American grid simultaneously for a long period of time.[5]

The above procedures, equipment, and supplies are discussed mostly from a high-level perspective although the document does provide detailed technical guidance partially through references to other technical documents. Hyperlinks to these references and technical documents are provided where feasible to assist the reader.

This document's scope does **not** provide resilient power best practices for the following entities or situations:

- Electrical and natural gas utility companies, including the utilities' power generation systems, transmission systems, and distribution systems except when it is considered a core part of the enterprise's emergency and backup power system. This exception might occur if the utility plant was co-located with the enterprise or if a facility planned to rely upon a utility company as a key part of its power resiliency.
- General federal response efforts such as that provided in the Federal Emergency Management Agency's (FEMA's) *Power Outage Incident Annex: Managing the Cascading Impacts from a Long-Term Power Outage* (POIA) (except for federal response backup/emergency power systems). That document "provides guidance for federal level responders to provide response and recovery support to local, state, tribal, territorial, and insular area efforts while ensuring the protection of privacy, civil rights, and civil liberties."

Note that this document uses the term "**backup power**" to cover emergency power and standby power unless stated otherwise. *IEEE Standard 446-1195* defines an **emergency power** system as "an independent reserve source of electric energy that upon failure or outage of the normal source, automatically provides reliable electric power within a specified time to critical devices and equipment whose failure to operate satisfactorily would jeopardize the health and safety of personnel or result in damage to property." The above IEEE source defines a **standby power** system as "an independent reserve source of electric energy that, upon failure or outage of the normal source, provides electric power of acceptable quality so that the user's facilities may continue in satisfactory operation."

1.3. Problem Background

> **"We cannot solve our problems with the same thinking we used when we created them."**
> - *Albert Einstein*

While electrical power has become even more important to critical infrastructure operations, the legacy architecture often has aging equipment that make it difficult and costly to resiliently use all available modern energy sources. This is occurring while electricity is continuing to become more important to society and there is an increasing number of events that could cause damage to the electrical grid and precipitate a blackout. In fact, DOE estimates that as of 2015, the cost of power outages in the U.S. was $44 billion (B), an increase from $26B in 2002 (or $35B in 2015 dollars). 70 percent of the costs are borne by the commercial sector and the industrial sector accounts for 27% of the costs.[6] See *Appendix A REGULATORY AND UTILITY POWER GENERATION ENVIRONMENT* for high level background information regarding the grid.

From a policy perspective, *Section 316 of the FY 2021 National Defense Authorization Act (NDAA)* states "the Secretary of Defense shall issue standards establishing levels of availability relative to specific critical missions, with such standards providing a range of not less than 99.9% availability per fiscal year and not more than 99.9999% availability per fiscal year, depending on the criticality of the mission."[7]

While promising substantial increases in effectiveness and efficiency, new and emerging technologies have concurrently increased the potential for disruptions and even a catastrophic grid collapse. With these potential power disruptions and availability requirements in mind, several previously published documents have discussed the need for improved long-term power outage resiliency, including the following:

- The President's National Infrastructure Advisory Council (NIAC) stated that the "U.S. infrastructure and services will fail as a system" if there is a catastrophic power outage (per the December 2018 document Surviving a Catastrophic Power Outage).
- The above NIAC 2018 document also suggests developing a flexible, adaptable emergency communications system that is self-powered and protected against any potential disaster "to support critical service restoration and connect infrastructure owners and operators, emergency responders, and government leaders."
- The National Communications System (NCS) stated that a long-term outage where the fuel supply chain breaks down and backup generators stop functioning properly, "… would have catastrophic effects on the sectors themselves and would likely lead to cascading effects on other sectors, such as the financial sector, the transportation sector, and the health care sector. In addition, emergency services, Government operations, and other critical services would be either inoperable or severely limited"[8] (per the February 2009 document Long-Term Outage Study).

The power outages resulting from the incidents listed below demonstrate severe negative impacts to most critical infrastructures and life sustaining services, including communications, transportation, water and wastewater facilities, mass transit, and public health.[9] It is important to note that electric power is crucially important for post-incident operation and restoration activities. Further, because of the interconnectivity of the grid as shown in Figure 1. a significant interruption in one area of the grid could impact other parts of that grid.

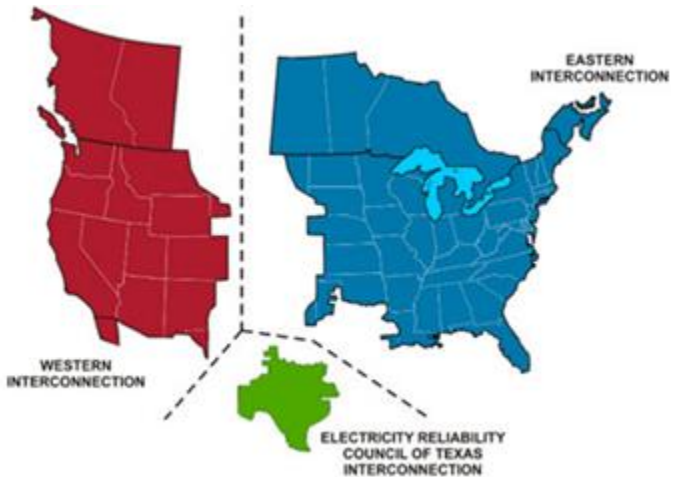

Figure 1. Three Regional Interconnection Grids

Cold Weather

Texas Blackout, 2021 – Three severe winter storms and record-breaking cold weather caused many power outages statewide over a 17-day period with an estimated 246 deaths. Close to two-thirds of the deaths were from hypothermia and about 8% were from carbon monoxide poisoning.[10] Diesel fuel was very difficult to procure, and many companies could not obtain it unless they had a contract from a fuel supplier who could bring in fuel from out of state once the roads were open. Further, many generators would not start due to temperature-related issues, a common one being generator start batteries failing in extreme cold.[11] This created problems with critical infrastructure and caused some city water systems and data centers to not operate.[12] [13]

Halloween Nor'easter, 2011 – Heavy snow in October 2011 brought down trees, resulting in 3.2 million residents across 12 states losing power. The storm arrived just two months after Hurricane Irene caused extensive power outages and property damage in the Northeast, with the 2011 New England tornado outbreak also causing damage in Western Massachusetts. In Connecticut, the outage lasted more than 11 days.

High Winds (non-hurricane)

California Public Safety Power Shutoff Due to High Winds, 2019 – Potential wildfires due to high winds and dry conditions caused Pacific Gas and Electric (PG&E) to shut off power to many counties in Northern California and several areas in Southern California from October 9 – November 1 and on November 20, 2019. A total of over 3 million people lost power during the various public safety power shutoffs.

Hurricanes/Superstorms

Hurricane Maria, 2017 – A category 5 hurricane devastated Puerto Rico and the U.S. Virgin Islands. Full grid power restoration to every part of Puerto Rico took over a year (nearly all customers had power in the US Virgin Islands after four months). Not only did Hurricane Maria knock down power lines, but generators stopped working, fuel was stolen, and fuel deliveries were very limited until the seaports and roads were reopened. Incompatible nozzles and fuels also caused fuel delivery issues. This single event caused substantial outages to critical equipment and facilities and led to continued deaths after the storm due to electricity outages. All mainstream communications were lost. Cellular had multiple issues and "cable system and wireline phone service remained generally non-existent, owing mostly to the lack of power."[14] It also consumed "an extraordinary share of available emergency generators and key support personnel for the entire United States."[15]

During Hurricane Maria, the lack of power prevented communications from working causing it to take much longer to restore power because there were no communications.

Superstorm Sandy, 2012 – In October 2012, 20 northeastern states plus the District of Columbia experienced significant power outages because of Superstorm Sandy. "About one-quarter of cell sites across ten states were out of commission, and a substantial portion of these outages resulted from the loss of power."[16] Over 8.5 million customers lost electric power, and significant damage occurred to the energy infrastructure. It required two weeks to restore power to 99% of customers.

During Superstorm Sandy, many areas ran out of fuel and assets as far away as California were called upon to assist.

Hurricane Katrina, 2005— Hurricane Katrina left an estimated 2.7 million customers without power across Alabama, Florida, Louisiana, Mississippi, and Texas. "The Federal Communications Commission (FCC) tallied three million customer lines, more than one thousand cell sites and 37 of 41 radio stations (two AM & two FM survived) lost in Louisiana, Mississippi and Alabama."[17] Within two weeks, power was restored in Alabama, Florida, and Mississippi, yet full restoration in Louisiana took almost another month due to extensive flooding and hurricane damage that required reconstruction of energy and other supporting infrastructure.

Figure 2. Flooding during Hurricane Katrina

Overgrown Trees

Great Northeast Blackout, 2003 – Overgrown trees contacted electric transmission in Ohio, precipitating a blackout that left an estimated 50 million people without power, some for two weeks. It included "trapping 800,000 people in New York's subways, and stranding thousands more in office buildings, elevators, and trains."[18] The U.S. and Canada jointly conducted a technical analysis that noted four primary groups of causes for this blackout in the "*Final Report on the August 14, 2003 Blackout in the United States and Canada*."[19] Causes included failing to maintain adequate tree growth near transmission rights-of-way, lost situational awareness, lack of visual tools, and computer disruptions, exacerbated by unavailability of experienced operating personnel.

Solar Flare Geomagnetic Disturbance (GMD)

Quebec GMD Power Outage, 1989 –In less than 2 minutes, the entire Quebec power grid lost power due to a coronal mass ejection from the sun. "During the 12-hour blackout that followed, millions of people suddenly found themselves in dark office buildings and underground pedestrian tunnels, and stalled elevators… Service to 96 electrical utilities in New England was also interrupted while other reserves of electrical power were brought online."[20]

Terrorism/Manmade

Metcalf Sniper Attack, 2013 – Gunfire from semiautomatic weapons did extensive damage to 17 transformers at the Metcalf transmission substation south of San Jose in April 2013. "The bullet holes caused the transformers to leak thousands of gallons of oil, and ultimately overheat. Grid operators scrambled to reroute power from elsewhere to keep the system from collapse. The power stayed on, but just barely, because it happened during a time when demand for electricity was very low."[21] The incident could have brought down power to Silicon Valley. Along these lines, there are just nine substations needed to be taken out in the U.S. to knock out the entire grid.[22]

Despite the substantial losses in the above examples, these can be considered "gray sky events." Outside resources were brought in and, except in isolated cases and with Hurricanes Katrina and Maria, services were restored within a "socially tolerable" timeframe that prevented significant loss of life and permanent population displacement.

However, a state actor or a natural event, such as an extremely large geomagnetic disturbance (GMD), could cause substantially larger outages than any of the above events. For instance, it is estimated that a GMD the size of the 1859 Carrington Solar Storm Event could destroy many of the high-voltage transformers in the electrical grid in multiple regions of the country. The period to replace the large transformers could be substantial due to the limited spare inventory, long transformer procurement lead times (one year or more[23]), and the difficulty of moving transformers over land.[24] Although outside resources could substantially help in this situation, this type of event could cause numerous and large disruptions to both electricity and fuel energy subsectors, as well as the infrastructures on which they depend. In turn, these disruptions could have a catastrophic impact on the population and on societal institutions.

Regardless of the severity of the event, it will be important for the U.S. to keep critical equipment and sites powered so that government, public safety, and restoration services can continue to function, resources could be appropriately allocated, repaired, and replaced to serve the public (e.g., ensure that fuel is available for generators) and rebuilding can take place much more effectively.

1.4. Definition of Resilience Levels

As part of each risk management plan, federal, state, and local critical infrastructure owners or operators should determine the importance of resilient power to their critical missions including:

- The critical missions of the installation per the *National Critical Functions Set*[25] including whether the operations can be handled elsewhere.
- The power and communications requirements of those critical missions.
- The duration that those power requirements are likely needed in the event of a disruption or emergency and whether it is acceptable if the power is interrupted.
- The importance of the infrastructure to the organization and to society (if the societal impact is unclear, the owner/operator may want to reach out to FEMA or CISA for their assessment).

Resilience: "Ability to withstand and recover rapidly from deliberate attacks, accidents, natural disasters … to our economy and democratic system."
-- 2017 National Security Strategy

After performing the above assessment and following the best practices in *Section 2.1 Risk Management* Plan, the critical infrastructure organization should determine its basic resilient power requirements. To help the organization implement these requirements, four levels of resilient power are introduced for the following reasons:

- **Easier Identification and Communication of Best Practices** – More easily identify the best practices needed for a particular facility/site and for that facility/site to better communicate its best practices to customers. For instance, a certain level could be specified in an acquisition (with exceptions noted) and then that level could easily be communicated to its customers.
- **Consistency** – Provides more consistency between the various sections of this document and helps ensure a well thought out implementation. For instance, maintaining 7 or even 30 days of fuel should be balanced with a generation system resilient enough to operate continuously and reliably for at least 7 or 30 days.
- **Cost Efficiency and Effectiveness** – Without multiple levels of resiliency being defined, many organizations may unnecessarily implement all the "best practices" including the Level 4 protections that are just intended for the most critical essential functions, typically associated with national security.

These resilience levels can help organizations implement their requirements and should not supersede them.

When determining the requirements and the resilience levels, consider the concept of "all hazards." Per FEMA's "*Federal Continuity Directive 1*" issued 1/17/2017, "all hazards" is "a classification encompassing all conditions, environmental or manmade, that have the potential to cause injury, illness, or death; damage to or loss of equipment, infrastructure services, or property; or alternatively causing functional degradation to social, economic, or environmental aspects. These include accidents, technological events, natural disasters, space weather, domestic and foreign-sponsored terrorist attacks, acts of war and chemical, biological (including pandemic), radiological, nuclear, or explosive (CBRNE) events."

Your Risk Management Plan (see *What is project risk management? - Institute of Project Management*) may dictate a lower or higher resilience level for some threats/hazards than for others based upon FEMA's "*Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) Guide.*"[26] The costs to implement robust protections against some hazards might be too expensive given that the facility is already built. Or, if a certain threat occurred, critical operations might be halted regardless of whether power was available. Another example is that the likelihood of some threats/hazards may be very low in certain geographic locations.

Taking the above officially identified all hazards (*"all hazards")* clarifications into account and using this manual to update the site's risk management plan, four resilience levels are defined to help with implementing the power requirements (not to replace them). See Section *2.1* to better understand which of the below resiliency levels is most applicable to your facility or site.

- **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 where the importance of operating far outweighs concerns about cost. Due to the complexities with implementing Level 4 best practices and since Level 4 requirements can differ substantially, only partial best practices are provided in this document for Level 4 Resilience.

Backup Power Timeframe

The primary drivers of the fuel related timeframe for your facility or site 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 using backup power while critical operations are transferred.

The timeframe should enable the facility or site to maintain power until additional fuel or power can be delivered to meet your risk management plan and your requirements. Thus, for Level 1, it is recommended that most facilities and sites store three days of fuel or stored energy onsite. However, at some sites, this might just be a couple of days perhaps because the site reliably generates solar power, or it can obtain fuel from a nearby storage facility. At other sites, four days of fuel might be stored onsite because of the difficulty in delivering fuel to the site.

See the *Vulnerabilities, External* Factors*, and* Stakeholder Needs subsection in Section *2.1* for a brief discussion of the operational, environmental, and external factors that can impact the above suggested timeframe. Also note that the timeframe is not applicable to Chapter *3 CYBERSECURITY AND PHYSICAL SECURITY* or to Chapter *4 ELECTROMAGNETIC (EM) SECURITY* since those topics do not directly impact the fuel related timeframe.

Systemic Risks and System-wide Resources

When determining the resiliency requirements and the resilience level, potential systemic, widespread impacts and system-wide resources need to be included in the risk assessment. For instance, sufficient geographical separation of a backup facility from the primary facility might provide sufficient resiliency for many of the identified risks.

Another example of using system-wide resources is that a cellular carrier's coverage could meet the definition of Level 3 even if most of its transceiver sites within an area only met Level 1 resilience due to the overlapping nature of the coverage from the transceivers. However, since power is a common mode failure between sites, fault tree analysis would be needed since something like a cyberattack is a systemic risk and could take down all the sites at the same time.

2. BEST PRACTICES

Target Audience:

- Executives and Procurement: *Browse, Read 2.2*
- Power Management/Engineering, Continuity & Planning: *Read all*
- Cybersecurity, Telecommunications, and IT Installation: *Read 2.3*

This chapter covers resilient power specific lifecycle best practices. It does not discuss general best practices such as writing a charter, developing a project management plan, etc. If the best practice is technology specific or technical, it is discussed in the applicable technical section. For instance, the best practices to maintain diesel fuel are listed in the *Fuel and Generator* Maintenance Procedures section.

Given the many best practices that should be incorporated, this chapter is broken down into five sections:

- ***Risk Management Plan*** (Section 2.1) – Focuses on risk management that is specific to resilient power.
- ***Resilient Power Requirements***(Section 2.2) – Covers *Overall Sector Goals* and *Vulnerabilities, External Factors, and Stakeholder Needs*.
- ***General Design and Process Best Practices*** (Section 2.3) – Provides guidelines for resilient architecture, design, and high-level installation considerations.
- ***Operations and Maintenance (O&M) Plan*** (Section 2.4) – Discusses the activities, resources, procedures, responsibilities, and time required to help ensure that the resilient power system will function properly during grid power outages and will continue to operate as planned during extended outages.
- ***Telecommunications*** (Section 2.5) – Covers the need for communications and identifies some wireline and wireless technologies that should be considered. This is essential to ensure that the necessary off-site equipment and supplies can be obtained during a combined grid power outage and general telecommunications outage.

Buy-in for the risks, resiliency goals, and high-level requirements from the owner, operator, or management responsible for the site is critical throughout this process and to help drive the resiliency goals.

2.1. Risk Management Plan

> **"It is never wrong to do the right thing."**
> *-- Mark Twain*

The first recommended step to implement the needed resilience for your critical infrastructure facility or site is to develop a risk management plan. These best practices do not describe how to write a risk management plan since there is a substantial amount of material published about this including from the Project Management Institute and FEMA (e.g., see the *FEMA Local Mitigation Planning Policy Guide*). Instead, this section focuses on those risk management aspects that are more specific to critical infrastructure and resilient power.

Unlike many enterprises that can just view their resilient power requirements independently of their overall sector, it is recommended that critical infrastructure owners and operators strongly

consider the cascading effects of their specific facility or site being inoperable at the same time that other similar infrastructure is also adversely impacted by an event. Thus, the first subsection below is the *Overall Sector Goals*. This is then followed by the *Vulnerabilities, External Factors, and Stakeholder Needs*. These will then drive the development of the *Resilient Power Requirements* and the needed resilience level.

Overall Sector Goals

To create a risk management plan and to document resilient power requirements, **the first step is to understand the sector's resilience goals.** Some of the key resilient power goals that should be considered include:

- Need for uninterrupted power.
    - Is power needed continuously 24/7?
    - Can power be lost for tens of milliseconds (ms), seconds, or minutes or hours?
- Length of time that power is required.
    - Must power be maintained for days, weeks, or even months?
- The cost, including the Value of Lost Load (VoLL), if power is lost.
    - Should preparations just cover known moderate and high-probability risks, or should they include known low probability risks or even black swan events?

Defining the facility or site resilient power level per Section 1.4 *Definition of Resilience Levels* can be very helpful with the risk management process**.** If the infrastructure provides services listed as a *National Critical Function*[27] by CISA, implementing at least Level 1 Resilience best practices should be strongly considered during the risk planning process. There may be some exceptions where the function is considered critical and may be unexpectedly shut down for a few days or even several days without significant harm. However, even those functionally specific enterprises should implement some of these best practices such as the *Cybersecurity Best Practices*.

If the loss of a particular infrastructure will likely result in a significant or serious harm to life or economic well-being, then Level 2 or 3 Resiliency may be more appropriate for that infrastructure. For instance, water is a lifeline function for reasons explained in the June 2016 NIAC *Water Sector Resilience Final Report and Recommendations*[28] document. Therefore, the risk planning process should strongly consider requiring critical water plants that perform lifeline functions for an urban area or mission support for critical national functions to meet Level 2 or even Level 3 resilience. However, not all water system facilities need to be at Level 2 or Level 3 since in some cases minimal service levels can still be maintained when a facility designated as Level 1 fails. Water utility operators need to analyze their system holistically and from a risk management perspective when determining the needed levels of resiliency within the system. For more information regarding water and wastewater resiliency, visit *Increase Power Resilience at Your Water Utility | US EPA*, *Drinking Water and Wastewater Resilience | US EPA*,or contact *wsd-outreach@epa.gov*.

As part of creating the risk management plan, **common mode failures**, where there are widespread failures in large-scale networks or across a sector due to a common problem or risk, need to be considered. For example, if all cellular sites in an area only have three days of fuel onsite, then the entire area could be offline for multiple days after the onsite fuel is depleted so that the system would not meet its Level 2 or Level 3 goals. However, given the significant

coverage overlap between cellular sites in many areas, perhaps just some of the sites need to meet Level 2 fuel requirements. Alternatively, it may be feasible to power cycle through the neighboring sites to extend fuel availability once it is known that the power outage may be extended. There may be spots that no longer have coverage and the overall capacity will decrease with fewer cellular sites, but this may be acceptable to meet the required availability goals.

Vulnerabilities, External Factors, and Stakeholder Needs

Key stakeholders should be identified for each requirements development process.

After the overall sector and enterprise goals are defined in the risk management plan, the site/facility vulnerabilities, external factors, and the stakeholder needs should be discussed. A good starting point is to define the resilience level that the site should meet. The resilient power project manager can then use the resilience level definition together with the following to determine the high-level site power requirements.

- **Vulnerabilities** – Many vulnerabilities are dependent upon the location. For instance, if the site is located where flooding can occur such that the road leading to the site could be flooded for several days, then several days of fuel may need to be stored onsite. On the other hand, cyberattacks are typically not directly dependent upon the location.
- **External Factors** – There are a number of external factors that may have direct or cascading effects that could impact the requirements. These include how long your facility or site might be out of power (consult with the utility company), how long fuel might take to be delivered, whether the employees or contractors will be able to commute to the site or work remotely, if the site's water supply will be lost based upon the risk factors, etc.
- **Stakeholders Power Needs** – This is further discussed below.

To capture the stakeholders' resilient power user needs, the following should be documented and prioritized (e.g., Tier 1 Mission-Critical, Tier 2 Priority) for each system/subsystem:

- List the systems, subsystems, equipment, and devices that need more resilient power than what the utility company can offer.
- Prioritize the power needs to include the most critical infrastructure components that must be kept operational and the components that could be "unplugged" if necessary.
    - Include the minimum support systems required to keep the critical infrastructure operational (e.g., badging or access control systems, lights) and those that might be used only during an emergency.
    - Define the amount of time that each system or subsystem needs power. For instance, two or three elevators may be needed for the first couple of hours after a power outage, but then perhaps just one elevator is needed.
- Understand the performance required such as whether 24/7 operations are needed or if the system can be down for a few minutes, or even for several hours.
- Consider long-term outages such as weeks or even months perhaps from a black swan event and the benefit of having resilient power or even intermittent power throughout the outage.

Prioritize the needs and actions to reduce risk via an engineering-based Failure Modes and Effects Analysis (FMEA) or similar risk reduction method. Sites that need to meet Resilience Levels 2-4 usually need to be more resilient than Level 1 sites both for a short period of time and for a longer period without outside equipment or supplies. Further, sites needing to meet Level 2-4 are likely to need more spare parts on hand and redundant equipment than Level 1 sites, but this is dependent upon the specific requirements for the facility or site.

2.2. Resilient Power Requirements

After creating a risk management plan, the resilient power requirements should be defined. For small organizations with a moderately low risk (e.g., Level 1), the requirements capture may be less formal than with larger organizations with multiple sites or ones operating or owning Level 2-4 infrastructure sites. Those with more complex requirements or needing more resilience will probably want to follow a more rigorous requirements process, such as that defined by the Project Management Institute or by ISO/IEC/IEEE 29148-2018.[29]

- **Estimate power usage for loads requiring backup power under various situations:**
    - Determine the maximum load within the last year and the average load per day. The peak demand kW noted on many utility bills is a simple method to identify how seasonal power use changes. Note that if segmenting the loads, determining the maximum and average loads will just be a starting point to calculate the power usage per load tier.
    - If the loads requiring backup power are subdivided into multiple categories, such as Tier 1 Mission-Critical, Tier 2 Priority, and Tier 3 Non-Critical as defined in Section 6.2, the energy manager or chief engineer should estimate the power usage per tier based upon the stakeholder requirements.
    - Record the total power usage of the resources under question, preferably by 15-minute or one-hour increments.
    - Include situations from short-term power outages from ms or hours to long-term outages lasting days or weeks, or even months for high resilience level sites.
    - Identify planned increases or changes in loads or loading patterns anticipated in the near and mid-term.
    - Use power meters in multi-facility sites to better understand the power demands of each facility, particularly for the critical equipment and areas that must continue to operate during a sustained event.
    - Take real world factors into account, such as the likelihood of employees not showing up at work during prolonged outages as well as extra employees arriving at the site during a blackout because other facilities shift work to your site.
    - Analyze whether energy efficiency can be improved.
    - Use the above to estimate the minimum generation power needed to back up the critical resources and the fuel that will be required.
    - Implement a tested operational plan (checklist) of what and how to “turn off” all non-critical loads by tier.
- **Baseline existing primary power and backup power system:**

- Review the existing power system architecture and equipment installed.
- Identify backup power system(s) and any helpful redundancies.
- Determine which components are past or near their life expectancy and should be replaced.
- List the components that should be reused to save money.
- Calculate the reliability of the existing system and subsystems.
- Where power system reliability is unknown, take steps, including testing of backup systems, to determine any system mean time between failures (MTBF) and vulnerabilities to threats of concern.

- Survey power system environment:
  - Understand the existing regulatory environment as discussed under *Appendix A REGULATORY AND UTILITY POWER GENERATION ENVIRONMENT.*
  - Estimate how quickly and reliably spare equipment and additional supplies (e.g., fuel) might be delivered to the critical infrastructure site during events of concern. For higher resiliency level sites, this should include long-term outages.
  - Differentiate between internal requirements and external requirements that will be fulfilled by another company or agency.
  - Conduct a threat and risk analysis using an FMEA or equivalent analysis of the existing system.
  - Either assume that there is just one simple, unreliable connection to the power plant or determine the following:
    - The connection reliability to the utility power plant or power plants including whether there are dual connections using different paths to both the grid and to the power plant.
    - The electricity generation reliability including whether power is dependent upon just one supplier.
    - Whether the facility is in an area where power is likely to be restored quickly on a priority basis.
- Use the information gathered in *Appendix A REGULATORY AND UTILITY POWER GENERATION ENVIRONMENT* for the following:
  - Document the risks including the systemic risks that could impact multiple primary or backup sources and distribution lines.
  - Understand the economic benefits from implementing a Demand Response Program and the potential value in selling power back to a utility.

An example of the power system environment that could impact requirements is that a remote site might have environmental conditions that make it difficult to ship fuel, supplies, or spare equipment versus an urban area that has many roads, warehouses, and stores and fewer transportation environmental impediments. On the other hand, urban areas can have their own risks and transportation might become difficult if civil order breaks down. Also, an urban site might need extra security protection.

After developing the requirements, a gap analysis and implementation plan should be developed. Available budget and value are a key part of the implementation plan. For instance, one solution might improve resiliency, reduce energy usage, and lower the cost per megawatt-hour (MWh) albeit at a high capital cost. Another solution might involve partnering with a third party to reduce capital costs but include higher operating costs.

2.3. General Design and Process Best Practices Summary

Some important design and installation considerations for safe and reliable operation of onsite emergency and standby power are discussed below in Table 3. For each specific technology (e.g., diesel generators, solar), see the applicable section in this document for the specific details, rationale, and background behind these best practices.

To reduce costs and improve resiliency, implementation of these best practices and guidelines should be performed holistically. For example, cybersecurity, physical security, EM security, and fuel considerations could impact the selection and location of the backup power generation solution so they should be considered in unison. System redundancy or site overlap could also meet many of the best practices. For instance, two redundant sites each with a single backup generator could meet Level 2 Resilience and perhaps Level 3 Resilience (with adequate fuel, cybersecurity, etc.) since if one generator stops functioning, the redundant site could take over operations.

Table 3. Resilient Power Best Practices Summary

Component or Function	Recommended Design and Process Best Practices (each level should implement the previous level's best practices plus the additional listed best practices based upon your risk management plan)
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 resiliency needed, document requirements, and conduct gap analysis. • Join appropriate sector/geographically based information sharing organizations such as InfraGard, the National Council of Information Sharing and Analysis Centers (ISACs) and preparedness networks like your local Community Emergency Response Team (CERT). • Implement the O&M Plan including updating the required documentation, and performing regular maintenance, testing, repair, and upgrade activities. • Schedule regular audits to ensure that 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 COOP during extreme events. • Establish processes to "stress test" readiness through periodic plan reviews, operational tests, and table-top and "real world" exercises.

Component or Function	**Recommended Design and Process Best Practices** (each level should implement the previous level's best practices plus the additional listed best practices based upon your risk management plan)
Level 1 Generation System	• Either deploy a backup power generation source or connect to two different utility generation sources via two independent transmission paths. • Maintain generator(s) per the "*Diesel and Natural Gas/Propane Generator Maintenance (excludes fuel* maintenance)" subsection including testing the generator monthly under load as recommended under *Table 16. Diesel and Natural* Gas/Propane Generator Maintenance Activities.
Level 2 Generation System	• Deploy at least two independent generation sources or equivalent so that the site is not dependent upon a common single source of failure. • Consider deploying multiple networked smaller generation sources with load shedding rather than deploying two large generators each of which meets maximum load requirements. This can improve fuel efficiency and resiliency as well as reduce costs. • Other possibilities to effectively meet the two independent generation sources or equivalent include: ○ Implement two independent connections to two different utility generation sources in addition to having a single backup generation source. ○ Implement a Renewable Energy Hybrid System (REHS), which includes both a renewable and a 24/7 generation source as well as an energy storage system (ESS). ○ Use a single highly reliable power generation source that approximates or is more resilient than two well maintained diesel generators with onsite fuel (e.g., a fuel cell that has been tested to be very reliable).
Level 3 Generation System	• Maintain multiple 24/7 generation sources capable of being operated for the timeframe required with N+1 redundancy (having one more generator than needed). • It is recommended that the power generation solution be implemented in an all-hazards resilient island-mode capable microgrid. • There should be a means to bypass and isolate any component for repair or replacement without deenergizing critical power to the mission. • Consider using multiple types of energy sources, such as diesel and natural gas, which provides better resiliency than using a single type of energy source. • The above should be implemented even if there are two independent connections to two different electric utility generation sources.
Level 4 Generation System	• Sites should receive two independent utility/primary power sources and establish two independent and geographically separated (within the site) back-up power sources. • Install generators that can be operated continuously. • Mitigate potential common mode failures as much as feasible so that it is difficult for the same natural hazard or manmade attack to damage both systems. • A dispatchable nuclear microreactor (see Chapter 9 *NUCLEAR SMALL MODULAR REACTORS (SMRs))* with an ESS and a generator could provide excellent resilient power against long-term power outages.

Component or Function	**Recommended Design and Process Best Practices** (each level should implement the previous level's best practices plus the additional listed best practices based upon your risk management plan)
Fuel	• Sufficient fuel should be guaranteed for "all hazards", typically by storing the fuel onsite for the following minimum amount of time although this is dependent upon the requirements: ○ Level 1: Circa three days ○ Level 2: Circa seven days ○ Level 3: Circa 30 days ○ Level 4: Generally, more than 30 days. • Work with the utility company to reduce the maximum power outage time period and work with the fuel supply company to reduce the worst-case fuel delivery time period for the risks identified. • Coordinate with government officials who will prioritize resources distribution. • Natural gas can be used as a best practice in all the following cases: ○ As a primary generation source if combined with onsite propane or natural gas storage. ○ For Level 1 and Level 2 Resilience, when the natural gas delivery system implements the protections/mitigations discussed in *Table 14. Diesel and Natural Gas/Propane Best Practices*. ○ For Level 1 Resilience, implemented as part of a REHS. ○ As one of the generation sources in an N+1 deployment. • Renewables and better energy efficiency can significantly reduce fuel consumption and improve resiliency. • Diesel fuel must be adequately maintained, including being rotated, to prevent the fuel from damaging the generator as discussed in Section 5.3 *Diesel Fuel Maintenance*.
Load Segmentation and Microgrids	• Properly size the generator(s) to the load as discussed under *Resilient Power Requirements* in Section *2.2*. • Level 3 (and Level 2 consideration): Segment the most critical loads so that they receive prioritized power as discussed under Section *2.2* and in *Chapter 6 POWER TRANSFER SYSTEMS AND MICROGRIDS*. • Level 3: New installations should network smaller generators together to meet the maximum load demand so that there is N+1 redundancy: ○ Saves fuel and improves generator reliability during a power outage when significantly less than the maximum load is required. ○ Increases the chances of receiving properly sized generators during an emergency. ○ For example, if 950 kW peak power is needed but off-peak power is only 200 kW, it is usually more resilient and less expensive to deploy three 500 kW generators in an all-hazards resilient microgrid than two 1 MW generators. ○ Short-term power usage spikes where peak power is needed can be handled by the uninterruptible power supply (UPS) network or an energy storage system (ESS).

Component or Function	Recommended Design and Process Best Practices (each level should implement the previous level's best practices plus the additional listed best practices based upon your risk management plan)
Automatic Transfer Switch (ATS) and Control System	• Use a hardened automatic transfer switch (ATS) as discussed in Section 6.1 *Power Transfer System* to disconnect from the utility grid quickly and automatically. • Implement a manual method to bypass the ATS and control electronics and ensure that this process and the power shutdown and startup procedures are well documented (ideally with photos) and rehearsed. • Ensure the backup power system is fully disconnected from the grid before energizing. • Level 3: Use protected, redundant ATSs and control systems to switch generators online and to control generators running in parallel.
Energy Storage and Uninterrupted Power	• Implement a high-quality UPS system to support sensitive critical systems that need continuous power until emergency or standby power comes online (see Section *7.3 UPS Guidance*). • Assess whether a less expensive ESS such as a battery ESS (BESS) can be used instead of a UPS. A BESS, which is often integrated with renewable systems, is typically significantly less expensive than a UPS and can supply continuous power to systems that can withstand tens or hundreds of ms without power.
Renewable Power	• Resilience should be included in any renewable energy cost-benefit analysis. • Renewable power should be combined with an ESS and a generator to create a renewable energy hybrid system (REHS) within a microgrid. • A REHS can substantially extend the fuel supply, save electricity costs (on an annual basis), and improve resiliency. • Solar is the most common renewable power generation source for enterprise systems but also consider other new technologies that have made fuel cells, wind, and others more competitive.
Telecommunications	• Ensure mission critical telecommunications are prioritized for emergency power and integrated into the Operations and Maintenance (O&M) Plan. • Deploy telecommunications diversity (e.g., cellular, satellite, landline, high frequency [HF] radio) with at least two independent services deployed for Level 1 Resilience increasing to at least four independent services used for Level 4 together with increased hardening and encryption. • Test the backup communications services per the Maintenance Plan. • Follow the PACE model (Primary, Alternate, Contingency, and Emergency) if immediate communications are needed.
Cybersecurity	• Follow industry cybersecurity standards, e.g., NERC CIP-009-6, NIST Cybersecurity Framework. • Include a supply chain security and a zero-trust security model in the cybersecurity plan. • The cybersecurity plan should include the network and user device requirements and the highest levels of management as discussed in Section *3.1 Cybersecurity*.

Component or Function	**Recommended Design and Process Best Practices** (each level should implement the previous level's best practices plus the additional listed best practices based upon your risk management plan)
Physical Security	• The physical security plan should include specific threats, existing security, and site vulnerabilities. • Employ a red team that attempts to find issues with the physical security plan from an attacker's perspective by working with local law enforcement and security contractors/experts. • The site's physical security plan should discuss the risks covered in the *Physical Security* section while considering the site's resilience level as well as its existing security plan and processes.
Electromagnetic (EM) Security	• The recommended protections against EM security are generally more cost effective if designed into an installation or major upgrade. • Specific options include installation process changes, EMP-rated surge protection devices (SPDs), shielded cables, as well other changes (e.g., room or facility shielding) (see Chapter *4 ELECTROMAGNETIC (EM) SECURITY*). • Sites should consider the potential for extensive geographical impact from HEMP or GMD events and the impact upon the grid, generators, controls, and electronics in preparing for these potential threats. • EM Security should be addressed by a combination of those responsible for HEMP/GMD and information technology (IT), plus facility engineering/management and maintenance personnel.

2.4. Operations and Maintenance (O&M) Plan

All critical infrastructure organizations should implement an O&M resilient power plan or equivalent. Often, much of what should be in a power related O&M plan is effectively implemented through the maintenance activities that must be completed by a third-party vendor as part of their contract, but this is not sufficient by itself. The O&M activities, resources, procedures, responsibilities, and time required should be understood to help ensure that the resilient power system will function properly for a minimum of the prescribed period of power resiliency during grid power outages.

In addition to the above, some specific parts of the **O&M plan** should include the following:

- **High-Level Best Practices** – The best practices discussed under *Table 3.* Should be part of the O&M Plan. These best practices should extend to contracts with third parties responsible for maintaining the equipment or supplies.
- **Technology Specific Best Practices** – The best practices discussed under each applicable technology section later in this document should be covered. For example, generator maintenance activities might involve periodic running of the generator including load testing. This should include manufacturer maintenance recommendations unless there is a known issue with the recommendations. These may need to be added later if it is unknown which equipment will be procured at this time.
- **Parts, Tools, and Supplies** – Important power system spare parts, maintenance parts, tools and supplies should be kept on hand partially due to supply chain risks.

- Include the types and quantities of parts and equipment needed to troubleshoot and fix common issues, such as the problems associated with old/dirty spark plugs and filters, dirty carburetors, old fuel, surge protection devices (SPDs), etc.
- Level 3 and Level 4 Resilience facilities should contain parts for less common but still very significant problems such as programmable logic controllers, master controllers, etc.
- A list of hardness critical items (HCIs) should be maintained that includes parts, repair materials, and supplies that must be readily accessible and locally stocked. If feasible, HCI's should have distinctive markings, tags, or labels to alert operators and maintenance personnel to the importance of the item to site operation in adverse environments.
- The expected fuel usage during a power outage should be documented along with the onsite storage capacity and potential fuel suppliers (see *Section 5.4 Diesel and Natural Gas/Propane Fuel Deliveries)*.
- Non-fuel supplies should also be given the appropriate attention per the resilience level desired. For instance, if the generator is water cooled, then water should be guaranteed for the period required and it shouldn't be assumed that a local water utility will deliver the water.
- Routinely check the inventory of important filters (oil, fuel, and air) and important lubricants and maintain enough inventory per *Table 16. Diesel and Natural Gas/Propane Generator Maintenance Activities* to handle a power outage per your site's defined resiliency level.
- Consult with experienced engineers and equipment operators within and outside the organization to create the inventory list since those items may not be available in the wake of a disaster.

- **Load Prioritization** – Create a prioritization list or tiers of the loads in the event of shortages.
  - Prioritize power such that only the most critical equipment can continue to receive power if it appears that fuel may run out.
  - Electricity conservation should be built into the plan, such as increasing the temperature at which the air conditioning is turned on.
  - Periodically test the load prioritization processes.
- **Employee and External Business Preparedness** – Include preparedness of employees and vital external businesses.
  - Individual readiness should include family readiness if applicable. See *How to Build a Kit for Emergencies | FEMA.gov*[30] and *Plan Ahead for Disasters | Ready.gov* for minimum recommended equipment and supplies that critical personnel should keep on hand so that they will be more likely to drive to work without needing to stay home to ensure their family's safety.
  - Consider how employees will drive to work (possibly due to family obligations) under all hazards. At some Level 4 or Level 3 sites, critical employees and families may need to be accommodated onsite or nearby.
  - The organization and the specific person responsible for each activity should be defined together with a designated trained backup.

- Additional planning is recommended for higher resilience level sites for systemic, unexpected, and even "never happened" events including roads being shutdown, a group meal making everyone on the team sick, a pandemic, staff including contractors not showing up to work, random accidents, etc.
- For Level 2-4 Resiliency infrastructure, critical power operations should not depend upon any one or even any two people.

- **Training and Exercises** – To ensure proper implementation of the O&M plan, training and exercises should be performed.
  - Conduct initial new employee and annual refresher individual training on employee emergency response actions, facility emergency operations, and individual roles and responsibilities. Alternatively, this could be covered in a corporate training plan.
  - Conduct semi-annual (Level 3 and 4 Resiliency) or annual department, facility, or complex exercises that test individual training readiness, response, and emergency procedure effectiveness. These tests and exercises should validate the level of emergency electricity use and requirements since actual energy use may be much different than planned.
  - Consider integrating facility emergency field and tabletop exercises with external agencies such as local utilities, law enforcement, emergency response teams, local or state emergency planners, federal partners, National Guard, or local Department of Defense installations. Most of these agencies develop training and exercise plans three or more years in the future and seek additional entities and events to test their own response capabilities.
  - Establish an exercise planning team to assist in setting training goals, collaborative exercise development with external elements, and turning feedback from training programs and exercises into plans and procedural changes that improve the O&M Resilient Power Plan.
  - Include cybersecurity, physical security, and EM security in exercises.
  - People can often be trained locally through either the manufacturer, a college, or the insurance company.
  - Note: FEMA defines an exercise as "an instrument to train for, assess, practice, and improve performance in prevention, protection, response, and recovery capabilities in a risk-free environment."
  - Do not overlook human factors and employees' family needs in training exercises. Use exercises to identify these needs before the real disaster strikes.
- **Electric Utility Communications** – Outline the communications process with the electric utility company, including being on their outage notification list if they maintain one. This will help operators better implement response procedures in the event of a predicted or actual grid failure or outage. For instance, with an expected extended grid failure, the operator may want to shutdown less critical operations to save fuel. Also consider that your utility may prioritize your infrastructure for power restoration based on the relationships established ahead of the disaster and the importance that your organization has shown to COOP.
- **Audits** – Ensure the O&M Plan is being followed properly by implementing quality standards such as ISO 9000. This should include delineating the regular audits needed

to ensure that the O&M Plan's Planning, Organization, Equipment, Training, and Exercises (POETE) supports the desired resilience level.

The O&M Plan might reference another document in some cases, such as the contract with a vendor, instead of directly listing the required activities. This is particularly true for a Level 1 Resilience organization, which may have a less formal O&M Plan than specified above but should still have one.

The O&M Plan should also cover any requirements from federal, state, and local laws, regulations, and ordinances on the planning, organization, equipment, training, and exercises (POETE) elements. Occupational Safety and Health Administration Publication 3122 provides guidance on emergency response requirements and 29 CFR 1910.38 provides guidance on Emergency Action Plans. National Incident Management System (NIMS), National Preparedness Guidelines, and the National Planning Frameworks provide guidance on prevention, protection, mitigation, response, and recovery capabilities as well as the capability development process.

2.5. Telecommunications

During power outages, telecommunications from some providers may be accidentally or intentionally disrupted during or shortly after the event causing the outage. As the telecommunications sector and electric distribution industry become more interdependent due to shared use of infrastructure such as utility poles, telecommunications services may face an increased prevalence of service losses contemporaneously with power outages. Therefore, it is recommended that telecommunications providers follow industry-accepted best practices, including both those suggested by the FCC's Communications Security, Reliability, and Interoperability Council (CSRIC)[31] and the resilient power best practices in this document.

Further, during prolonged power outages, telecommunications systems that did not store sufficient fuel on site may not continue to operate because of fuel delivery disruptions. Given these potential problems, the O&M Plan should address telecommunications sustainment where applicable including in the Training and Exercises section and in the Parts, Tools and Supplies O&M section. This should include periodic exercises to communicate with partners, employees, and contractors when the primary method of telecommunications has failed or has been compromised.

In addition to telecommunications being integrated throughout the O&M Plan, the document should also have an annex that specifically addresses telecommunications and the actions that need to be taken to sustain communications throughout the objective design period for all-hazard emergency power operations. This annex should be consistent with your organization's risk management plan and the supported operations and address the following:

- The primary telecommunications equipment used daily.
- Backup or only occasionally used telecommunications equipment and how often these need to be tested.
- The design period of operation, which should meet or exceed the minimum continuity period for the emergency power operations supported.
- Non-cellular mobile communications coverage map.
- Relationships with vendors and outside service providers.

Given the criticality of communications for resilient power and for other purposes, it is recommended that organizations deploy multiple telecommunications capabilities as described below and referenced in Table 4. Generally, a power resiliency implementation that follows these best practices should not require guaranteed immediate communications between two specific parties, but when this is required per your risk management plan, the PACE model should be deployed. PACE stands for Primary, Alternate, Contingency, and Emergency with each of the four methods of communications being separate and independent from the other three methods.

- Level 1 – Two independent services with land mobile radio (LMR) having standalone capabilities if deployed. Cellular and wireline should include priority services if permitted by the service provider.
- Level 2 – Level 1 plus one additional independent service (three services total) with at least one voice service being encryption capable.
- Level 3 – Level 2 with at least one service being an *all-hazards* resilient service. The all-hazards service should be hardened and follow the recommendations in this document and implement the network resiliency recommendations under "*Communications and Cyber Resiliency | CISA"*, including those in the document "Ten Keys to Obtaining a Resilient Local Access Network." The capabilities should also include handling sensitive but unclassified (SBU) data and voice (e.g., Law Enforcement Sensitive) and preferably classified data. The overall communications systems should have no known single point of failure.
- Level 4 – Level 3 plus one additional independent service (four services total) with at least one service being an *all-hazards wireless* backup service or an *all-hazards private wide area network* (generally using fiber in at least the core part of the network). The capabilities should include handling protected critical infrastructure information (PCII) or equivalent, such as classified data and classified voice. Hardened satellite communications or hardened high frequency (HF) radio should be available for backup communications including for use during/after EMP events.

The above telecommunications sites should also meet the hardening requirements specified in the *ANSI APCO Public Safety Grade Site Hardening Requirements*[32] (June 2019) where feasible. For critical infrastructure stakeholders that self-provision backup telecommunications services, it is recommended that they follow the relevant CSRIC best practices, including those best practices that involve security-by-design, to ensure secure, reliable, and resilient communications in the absence of commercial power.[33]

Service providers often share facilities so hardening one site can help many end users with a single investment.

The common mode failure between telecommunications providers should be as minimal as possible and is the reason for the services to be independent and geographically separated from each other (e.g., diverse facilities that use different fiber cables and are not close to each other). This often requires using multiple service providers. A facility could also partner with a neighboring facility that uses an independent and geographically separated communications service particularly where there is a reliable, hardened connection between the two facilities.

Table 4. Potential Telecommunications Capabilities

Category	Telecommunications Capabilities
Wireline Primary	• **Internet/Data** – An Internet-based connection can enable both data and Voice over Internet Protocol (VoIP) communications. • **Analog Telecom Service** – Plain Old Telephone Service (POTS) is the traditional phone communications and can offer a third communications path if the Internet and cellular connections have failed. • **Private** – A private network is typically used to either improve security or reduce costs. It generally consists of fiber but may be built or augmented using copper or wireless (e.g., microwave). It might be connected to the Internet through a gateway.
Wireless Primary	• **Cellular** – This wide area network reaches most homes and businesses but may be dependent upon some of the same data connections as used for Internet access. • **Land Mobile Radio (LMR)** – This primarily voice and low speed data local, metropolitan, or statewide network is used in many public safety related industries such as police, fire, emergency medical services, but also often with utility companies.
Wireless Backup	• **Satellite** – These communications have been used mostly for limited voice usage in remote and maritime areas but is expected to be increasingly used for voice and data (typically need line-of-sight to the sky). For a hardened solution, Geosynchronous Earth Orbit (GEO) and Medium Earth Orbit (MEO) satellite services are typically preferred since Low Earth Orbit (LEO) satellite communication systems are more risk prone to high-altitude nuclear explosions (see *Catalog of Earth Satellite Orbits (nasa.gov)*[34]). • **HF Radio** – Due to its operating band of 3 MHz – 30 MHz, which is much lower than the frequencies used by modern wireless technologies such as cellular (starts at 698 MHz), HF can be used for long distance communications without relying upon other wired or wireless infrastructure although most types of HF can be disrupted for hours due to a HEMP or GMD event.

If deploying HF, it is recommended that the organization join the SHAred RESources (SHARES) Program, administered by DHS CISA. More than 2,400 HF radio stations, representing over 400 Federal, State, County, 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. SHARES promotes interoperability between HF radio systems and provides awareness of applicable regulatory, procedural, and technical issues. Further information on SHARES may be obtained at https://www.dhs.gov/shares or by contacting the SHARES Program Office at SHARES Customer Service Request. Coordinating with amateur radio emergency communications users (also known as "HAM" radio operators and radio clubs) can also be useful. Note: Solar Photovoltaic (PV) inverters or Light Emitting Diode (LED) lighting power supplies could emit significant broadband radio noise in the HF radio spectrum. Without occasional testing of the HF backup communications, this interference problem might not be noticed until the HF radio system is needed.

If using a wireless phone or a landline phone, CISA provides priority telecommunications services (see Priority Telecommunications Services | CISA) 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 help ensure key Federal, State, Local, Territorial, and Tribal

governments, and first responder and industry organizations have communications capabilities available to support emergency response incidents. The First Responder Network Authority (FirstNet) cellular service can provide public safety agencies with priority services and more secure communications (see https://www.firstnet.com/signup/eligibility for eligibility).

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 cellular phones during network congestion.
- Is an add-on feature to your cellular phone.
- Can be used in conjunction with GETS to provide priority access over both wireless-to-wireless calls and wireless-to-wireline calls.

TSP provides priority installation and repair of critical communications circuits:

- 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.

3. CYBERSECURITY AND PHYSICAL SECURITY

Target Audience:

- Executives: *Browse*
- Power Management/Engineering, Continuity & Planning: *Read all*
- Cybersecurity: *Read all*
- Physical Security: *Read all*
- Procurement: *Read Supply Chain Security*

It is critical to implement cybersecurity and physical security mitigations for all resilient power solutions, whether it's using a backup diesel generator, a renewable energy hybrid system (REHS), or something else. Typically, the same security mitigations applied to other IT and industrial control systems (ICSes) should also apply to the power system. At all times, critical infrastructure is at risk, but when the grid is down or immediately prior to the grid maliciously being taken down, the risk of the backup power system being targeted increases for several reasons:

- An attack that successfully takes down the backup power after grid power is lost will likely cause the critical equipment to stop functioning (after the local UPS storage is exhausted).
- Ransomware demands with threats to shutdown backup power as well as terrorist and destructive hacker attacks may be more likely since the grid is not functioning properly, and the damage inflicted will likely increase.
- Physical theft is much more likely during a power outage. For example, during Hurricane Maria, the VP of the Puerto Rico Telecommunications Alliance stated, "the fuel trucks are being hijacked and scant fuel we have is being stolen from the emergency power plants."[35]

Therefore, integrating cybersecurity and physical security defenses is an important step toward maintaining resilience for both critical infrastructure and its source(s) of power (although the timeframe best practices are not directly applicable to this chapter). For instance, CISA's *Cybersecurity and Physical Security Convergence Guide* [36]states "the adoption and integration of Internet of Things (IoT) and Industrial Internet of Things (IIoT) devices have led to an increasingly interconnected mesh of cyber-physical systems (CPS), which expands the attack surface and blurs the once clear functions of cybersecurity and physical security." Further, CISA's Convergence Guide states "when security leaders operate in these siloes, they lack a holistic view of security threats targeting their enterprise."

3.1. Cybersecurity

Below is a cybersecurity *Problem Background* description from a resilient power perspective followed by the *Cybersecurity Best Practices*, *Supply Chain Security*, and then *Resources Including Assessment Tools*.

Cybersecurity: "The process of protecting information by preventing, detecting, and responding to attacks."
– NIST Cybersecurity Framework

Problem Background

According to the Wall Street Journal in August 2018, "the threat to the U.S. electric grids is so *serious that in June a group of presidential advisers said the country needs to prepare for a 'catastrophic power outage' possibly caused by a cyberattack."*[37] There are numerous examples of cyberattacks including a DHS report in July 2018 stating that hackers working for the Russian government were inside control rooms of U.S. electric utilities where they could have triggered blackouts. A pipeline provider was shut down for two days by a ransomware attack that halted operations while staff shut down, then restored systems.[38] There have been almost 12 million control system cyber incidents with more than 1,500 deaths and more than $90 Billion in direct damage globally (per Joe Weiss, who served as the Task Force Lead for review of information security impacts on IEEE standards).[39]

After a sophisticated attack on the U.S. electric grid, additional cyberattacks could be extended into microgrids or even enterprise power systems supporting critical infrastructure. Further, an attack could occur by disrupting the grid to an important site while a cyberattack keeps the backup power from operating. Once a cyberattack is successful and the adversary is inside the power control system, it may also be possible that attack can be extended to partner networks. Therefore, it is important to ensure that all critical infrastructure sites implement strong cybersecurity measures, particularly at sites requiring high resilience levels.

The types of potential attacks are discussed in many documents, including the *DHS Study on Mobile Device Security*[40] and the Emergency Communications Division's (ECD's) interactive graphic shown in the *CISA Public Safety Communications and Cyber Resiliency Toolkit*[41] including the DHS ECD *OEC NG911 Cybersecurity Primer*.[42] However, most of the leading types of attacks that critical infrastructure stakeholders need to be concerned with are discussed below in *Table 5. Leading Types of Cybersecurity Attacks*.

Table 5. Leading Types of Cybersecurity Attacks

User Devices	Network Infrastructure and Connections
• **Data breaches**: Data on device is accessed, manipulated, or stolen. • **Malware**: Malicious software is downloaded (e.g., viruses, worms, Trojan horses, spyware). • **Ransomware**: Malware that blocks the usage of a computer system or the data residing in it for the purpose of extorting a ransom. • **Phishing**: Generic social engineering is employed (e.g., emails) to solicit personal engineering. • **Spear-phishing**: Phishing targeted at a specific individual. • **Insider Threats**: Employees or other authorized personnel steal, corrupt, or destroy data, or operate equipment in an unauthorized manner. • **Spoofing**: Unauthorized device masquerades as an authorized device.	• **Denial-of-Service (DoS)**: Attackers overload network resources with requests for access, straining the network's operability and capacity. • **Distributed Denial-of-Service (DdoS)**: A distributed DoS where the attack comes from many devices distributed over the network. • **Man-in-the-middle**: Wireless link between the user device and the tower is compromised allowing attackers to steal data or monitor conversations. • **Signaling System 7 (SS7) / Diameter**: A global standard signaling protocol network used by all major phone carriers that can be misused to intercept phone traffic. • **Jamming**: A third party uses a radio frequency (RF) transmitter to interfere with existing wireless signals preventing RF receivers from properly decoding the communications. This is also a form of *Electromagnetic Interference (EMI)*. • **RF Weapon (RFW)**: Use of a high-power transmitter that directs IEMI to damage or disable electronic equipment or systems (all electronics are vulnerable to powerful RF Weapons – see *Electromagnetic Interference (EMI)*).

Some of the specific cybersecurity threat areas with an enterprise's power system are the power system controller, battery management, solar power management, and remote powering of generators. However, a cyberattack against the user device or the network could also impact the power system. Infiltrating the network typically will cause the most damage, but a successful attack on a user device may enable access to the network or at least access to a substantial amount of data in the network. Although the network attacks are technical, most of the user device attacks are based upon weak user security. Sometimes, this is due to unscrupulous employees as occurs with an insider threats attack, but generally it is due to carelessness or lack of training.

Cybersecurity Best Practices

To mitigate risks against cyberattacks including the ones discussed under the *Problem Background* above, it is recommended that the power system be part of the critical infrastructure's overall cybersecurity plan. Likewise, ICS cybersecurity should be part of the power system planning and requirements documents since for example, *Supply Chain Security* requirements could influence the power system procurement or O&M Plan.

To improve cybersecurity risk management in critical infrastructure regardless of size, cybersecurity risk, or cybersecurity sophistication, it is recommended that organizations follow the National Institute of Standards and Technology's (NIST's) *Framework for Improving Critical Infrastructure Cybersecurity*[43] (*NIST Cybersecurity Framework)*. It applies the principles and best practices of risk management to improve security and resilience. It focuses on both using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of

the organization's risk management processes. The five NIST Cybersecurity Framework Core Functions are defined in *Table 24* in *Appendix B*.

It is recommended that all critical infrastructure organizations at least follow the NIST Cybersecurity Framework "*Tier 3: Repeatable*" process, which includes having an approved risk management policy with regular updates of the organizational cybersecurity practices. The most resilient facilities and sites will also want to implement "*Tier 4: Adaptive*" and the applicable requirements from the NERC CIP security standards CIP-002, CIP-003, and CIP-007. The IEC 62443 Standards are also a noteworthy set of standards that can be followed and are compatible with the *NIST Cybersecurity Framework*. The higher the resilience level, the better the cybersecurity controls should be to protect against the cyberattacks listed in *Table 5. Leading Types of Cybersecurity Attacks* and against cyberattacks that are not listed.

In addition to implementing the above best practices, it is recommended that the cybersecurity mitigations shown in Table 6 be implemented based upon a cybersecurity risk and vulnerability analysis. If the backup power ICS network is separated from any outside connections (also known as "air gapped"), which is preferred from a cybersecurity perspective, some of the below mitigations are not needed. However, insider threats remain an issue and malicious software can still be introduced into the network whenever an external device is connected to the standalone network (e.g., universal serial bus (USB) drive, new software, maintenance computer).

Table 6. Recommended Cybersecurity Mitigations (applicable to all resiliency levels)

Mitigations	Specifics and Rationale
Implement Zero Trust Security Model	• Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location or based on asset ownership (enterprise or personally owned). • This is increasingly important with a mobile workforce, an increased use of wireless (e.g., 5G cellular), Internet of Things (IoT), and the high number of compromised passwords. • Consider further reducing or preventing lateral movement and privilege escalation during a compromise. • Per Brandon Wales, [Executive Director] of CISA stated in 2021, "zero trust architectures are going to be critical for helping [agencies]."[44].

Mitigations	Specifics and Rationale
Minimize Account Privileges (part of Zero Trust Security)	• Reduce or eliminate account privileges when an employee leaves the organization, or an asset, port, or service is no longer needed. • Reduce both insider threats and the risk from hackers gaining access to insider accounts. • Remove network access permissions of non-compliant assets that do not meet the organization's security requirements. • Minimize and secure all network connections to the ICS (even calibration tools are vulnerable to cyberattacks if they can connect to a network). • Implement geofencing at least for the ICS network, typically including not allowing assets that are outside the country or at least within a non-friendly country to have access to the network. • Do not allow remote persistent vendor or employee connection to the ICS network. • Require two-person authorization for the most critical network or security activity including downloading highly sensitive or proprietary data, actions that could take down a critical network, and deleting cybersecurity event logs. • The power system's cybersecurity risk is substantially reduced when in island mode.
Identify Assets	• Automatically identify assets at risk to cybersecurity attacks including compromised supply chains (backdoors, counterfeits etc.).
Provide Manual Override	• Install a manual override located within the physical security perimeter to startup the backup power systems.
Monitor Network Traffic	• Monitor the network traffic crossing the boundary of critical networks, including ICS networks.
Log Cybersecurity Events	• Log events in a centralized system with automatic monitoring and alerting. • Ensure log file integrity such as by using blockchain.
Implement Strong Identity and Access Management	• Ensure good password security controls, including enforcing strong passwords and blocking the use of leaked passwords available on the dark web. • Implement multi-factor authentication as a part of endpoint management.
Train Employees and Conduct Exercises	• Provide training to all employees (e.g., do not click on unknown, suspicious links) at least annually. • Conduct exercises and perform tests (fake phishing emails, etc.) to ensure that the training is adequate. • The training and exercises should cover preventing cyberattacks and responding properly.
Deploy End-to-End Encryption	• Use end-to-end encryption for all communications paths, particularly for sensitive data.
Patch and Upgrade Software	• Follow recommendations from vendors to patch and upgrade software. • Do not use end-of-life or unsupported software.

Mitigations	Specifics and Rationale
Deploy Artificial Intelligence (AI)	• Use AI to detect, predict, and mitigate advanced attacks and zero-day exploits by identifying anomalous/suspect traffic, questionable sensor data, and connections (this goes beyond just checking for signature-based malware). • Consider disallowing or closing a connection if there is an exploit detected such as a suspicious device/user or a faulty sensor.
Backup Data	• Periodically backup and store data in a separate location with offline backups beyond the reach of malicious actors. • This creates insurance against data loss.
Protect Against EM	• Follow Chapter *4 ELECTROMAGNETIC (EM) SECURITY* to reduce threats from RF Weapons as well as from lightning, HEMP, and GMD. • Do not use wireless sensors unless well protected from EM and cyberattacks.
Create Incident Response and Continuity Plans	• Implement and exercise a Cybersecurity Incident Response Plan and a Continuity Plan that includes the C-suite and the physical security team. • Report any cyber incidents deemed "significant" to CISA within 72 hours or within 24 hours of making a cyber ransom payment (per the Fiscal Year 2022 appropriations bill).
Develop Unified Security Policies	• Converge the cybersecurity and physical security functions to create unified security policies. • The unified policies should include many of the above mitigations such as identifying assets, training personnel, conducting exercises, creating an incident response plan, and developing response and continuity plans. • Identify the interactions between the physical and cyber assets including the interdependencies to adequately plan for, protect against, and respond to threats/incidents. • The facility's ICS policies should be applied to the power system.
Conduct Assessments	• Internal assessments should occur annually at least starting with Level 2 Resiliency (Level 2 extends Level 1's cost-effective practices). • For Level 3 Resiliency, an external Red Team risk and vulnerability assessment should occasionally occur (at least every 2-3 years for Level 4) in place of an internal assessment.

The above guidance is based upon:

- NIST Special Publication (SP)800-207 *Zero Trust Architecture | NIST*[45]
- *Zero Trust Maturity Model | CISA*[46]
- CISA's *Recommended Cybersecurity Practices for Industrial Control Systems*[47]
- CISA's *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies*[48]
- *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach (NIST Special Publication 800-160, Volume 2)*[49]
- *Framework for Improving Critical Infrastructure Cybersecurity* (previously mentioned)
- RPWG inputs and widely recognized cybersecurity best practices.

It is recommended that critical infrastructure organizations become a member and participate in the appropriate sector- and geographically based Information Sharing and Analysis Organization. Also consider networking with local National Guard cybersecurity personnel and utilizing the CISA Protective Security Advisor (PSA) Program, which can help conduct voluntary, non-regulatory security surveys and assessments on critical infrastructure assets and facilities within their respective regions (see *Protective Security Advisor Program (cisa.gov)*). Security plans should also incorporate potential threats due to quantum computing such as migrating to post-quantum cryptographic algorithms, which should be approved by NIST by the end of 2022.[50]

Supply Chain Security

It is highly recommended that organizations implement the above cybersecurity recommendations as the first part of reducing supply chain risks, including implementing Table 6. *Recommended Cybersecurity Mitigations*. Mitigations such as zero-trust security can help ensure that your vendor's cybersecurity vulnerabilities do not become your organization's vulnerabilities. Access should not be provided to your computer systems/network and data to any organization without verifying that your vendor's cybersecurity will be sufficient to protect your data and systems.

A supply chain attack can concurrently impact numerous critical infrastructure sites potentially eliminating service overlaps and redundancies.

It is also suggested that your organization follow NISTIR 8276 *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry* (February 2021) and Defending Against Software Supply Chain Attacks.[51] Cybersecurity professionals should review all procurements impacting cybersecurity, establish a cyber supply chain risk management program and include the supply chain software-related security issues and recommendations in the organization's cybersecurity plan. This includes **creating a software bill-of-materials and performing a cybersecurity assessment of the supply chain**, particularly for Level 2-4 resiliency sites. Passive equipment that cannot be programmed are of minimal concern from a cybersecurity perspective and do not need to meet most of the supply chain cybersecurity best practices.

For Level 2-4, best practices dictate that control equipment, telecommunications equipment, and any other programmable equipment that is critical typically should not be purchased from companies with close ties to adversaries as defined by the federal government or by the site's security organization. These adversaries often include China, Russia, Cuba, Iran, North Korea, and Venezuela.[52] Challenges arise if the device is labeled by a different vendor or integrator. To identify the manufacturer of a Network Interface Controller, see the *Joint Staff White Paper on Supply Chain Vendor Identification – Noninvasive Network Interface Controller*[53] written by Federal Energy Regulatory Commission (FERC) and NERC.

Level 2 resilience organizations may make an exception to the above power-related supply chain best practices if their power control system is standalone and is neither connected to the Internet nor to the enterprise's network. Nevertheless, this best practice is still applicable to their telecommunications equipment. Level 3 and 4 Resiliency organizations should generally follow the above best practices even if not connected to the Internet since latent defects could be inserted into the equipment and malware could trigger malicious code within the product.

For **federal agencies and DoD contractors and vendors**, it is recommended that the below are followed:

- **Civilian Agencies**: NIST 800-171 Rev. 2 "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations."[54]
- **Defense Industrial Base**: *Cybersecurity Maturity Model Certification (CMMC)*.[55]

As part of resilient power supply chain management, all **Level 1-4** critical infrastructure entities should follow Section 889, which is part of the Fiscal Year 2019 National Defense Authorization Act.[56] This includes not procuring certain telecommunications equipment (including video surveillance equipment) or services produced by the following covered entities and their subsidiaries and affiliates without a waiver:

- Huawei Technologies Company
- ZTE Corporation
- Hytera Communications Corporation
- Hangzhou Hikvision Digital Technology Company
- Dahua Technology Company

The Secure Equipment Act of 2021 strengthens Section 889 mentioned above by stating that that the FCC will not review or issue "new equipment licenses to companies on the FCC's 'Covered Equipment or Services List'[57] that pose a national security threat."

The Secure Equipment Act prevents new equipment licenses to companies posing a nation security threat.

Lastly, to help prevent hardware-related supply chain disruptions, ensure that your organization maintains enough power system spare parts and consumable maintenance items onsite per the "Parts, Tools, and Supplies" under Section *2.4 Operations and Maintenance (O&M) Plan*.

Resources Including Assessment Tools

Federal agencies should follow NIST's NISTIR 8170 1 *The Cybersecurity Framework Implementation Guidance for Federal Agencies*. "This report illustrates eight example approaches through which federal agencies can leverage the Cybersecurity Framework to address common cybersecurity-related responsibilities."[58] It is also recommended that critical infrastructure operations and many public and private sector organizations follow NIST's NISTIR 8170 Cybersecurity Framework Implementation Guidance or an equivalent document.

All Level 2 resilience and higher organizations should assess their cybersecurity vulnerabilities using different personnel from the ones responsible for implementing the cybersecurity protections. To help with this, CISA offers the "*Cybersecurity Vulnerability Assessments through the Control Systems Security Program (CSSP).*" "This program provides onsite support to critical infrastructure asset owners by assisting them in performing a security self-assessment of their enterprise and control system networks against industry accepted standards, policies, and procedures." For more information about this program and other CISA cybersecurity resources, please see https://www.dhs.gov/xlibrary/assets/pso-safeguarding-and-securing-cyberspace.pdf. Contact CSSP@dhs.gov to request onsite assistance.

High impact cyberattacks should be reported to https://www.us-cert.gov/forms/report. Organizations should also consider implementing MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Framework®, which is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.

Other cybersecurity resources can be found in the document "Cyber Resiliency Resources for Public Safety" under *Communications and Cyber Resiliency | CISA*.[59] Although the resource list was written for public safety, it is applicable to all critical infrastructure sites. Another resource is DOE's *Cybersecurity Capability Maturity Model (C2M2)*, which addresses the implementation and management of cybersecurity practices associated with information technology (IT) and operations technology or ICS assets and the environments in which they operate.[60]

3.2. Physical Security

Physical security for backup power and fuel supplies should be incorporated in the critical infrastructure facility or site physical security plan and be consistent with the cybersecurity policies. Depending upon the organization's structure, this may involve the facility manager, the chief facility engineer, loss prevention managers, security contractors, risk management specialists, local/state/federal law enforcement if applicable, and cybersecurity policy experts. The security plan should include security measures that are appropriate for long-term outages as well as short-term ones.

Vandalism and theft can become major issues if there is a long-term power outage. Fuel and generators can become prized objects during power outages and history has shown that desperate people will sometimes use creative and even illegal means to obtain fuel and portable generators, particularly when they cannot be obtained via the open market.

Because the power section of the security plan is highly dependent upon the overall security precautions, the nearby population (e.g., size, military versus civilian), and the geographical characteristics of the site and its surroundings, the physical security plan needs to specify what is best for that specific site based upon the risk management plan. At secure sites or if the generator and fuel supplies are inside the facility, no special precautions may be needed (although flooding could still be an issue). Extra security precautions might also not be required where the threat and required resiliency are both low. InfraGard (https://www.infragard.org/) and your state fusion center can provide advice about the risks.

The below considerations should be covered in the physical security plan, which should also be consistent with the cybersecurity plan:

- **Resilience level** – The higher the resilience level per Section 1.4, the greater the need for physical security.
- **Threats** – Conduct a threat assessment working with local enforcement agencies to review the probability of damage or theft due to natural or manmade threats. Threats include naturally occurring events (e.g., hurricanes, solar weather), vandalism (e.g., breaking windows, setting fires), theft, terrorism (e.g., explosives), state actor related (e.g., EMP, cybersecurity), and insider threats.
- **Existing security** – This includes various protections such as fences, locks, and security guards. Natural barriers such as being in a remote area or on an island can also help although being next to public land might require additional precautions.
- **Vulnerabilities** – Assess the vulnerabilities of the assets to the threats, considering the existing security measures already in place or already planned. Note normal operational vulnerability and changes in vulnerability during a widespread or long-term power outage. For instance, higher fuel prices may increase the threat to fuel supplies making large aboveground fuel tanks and fuel deliveries more vulnerable.

Based upon the above and the organization's resources, the critical infrastructure facility manager should select the most appropriate protection measures, including the following:

- **Site Location** – When selecting a site for the critical infrastructure, the security risks should include implementing the precautions discussed below and the IEMI protections covered in *Section 4.4 Electromagnetic Interference (EMI).*
    - Includes Level 3 Resilient facilities/sites having a secure perimeter to protect against IEMI and to reduce the risk of physical attacks.
    - Choosing the best location can also reduce risks associated with the below bullets.
- **Restricted Access Policies** – Establish restricted access policies to resilient power and fuel storage areas so that only authorized personnel have access. Best practices include double authentication (e.g., having a badge to get into the facility/site and a key to enter the backup generation area) for Level 2 resilience and higher. Restrict asset visibility both physically and online by ensuring that resilient power infrastructure cannot be seen from outside the facility and that facility details are not on the Internet.
- **Physical Security and RF Barriers** – Install fencing and gate access (particularly for Level 2-4 resilience) or put the generator in a locked, shielded metal container (the fuel should also be locked up). A barrier together with installing the generator equipment in a shielded metal container can help reduce the threat against both IEMI and drones (also called Unmanned Aerial Vehicles [UAVs]). Additional security measures to mitigate RF attacks including from drones are covered under *Section 4.4 Electromagnetic Interference (EMI)* (most pertinent to Level 3-4 resilience).
- **Monitoring Systems** – Use lighting as well as intrusion detection and monitoring systems to better secure the backup/emergency power components and supplies. Remove landscaping or other items that restrict monitoring by these systems.
- **Protection Against Natural Elements** – Protect the components against wind, flying debris, and water. When determining the maximum and minimum weather conditions (e.g., temperature, wind, ice, rain, snow) to protect against, assume that a record weather event is occurring when the backup power system is most needed. Carefully consider that weather extremes may be combined (i.e., extreme heat and flooding, extreme cold and wind).
- **Flooding** -- This is a particular concern in many parts of the country due to the loss of life and damage that flooding has caused. The following are best practices:
    - Elevate all electrical components and critical infrastructure above the 500-year base flood elevation as encouraged by Facilities Standards (P100) Overview | GSA.[61] This includes generators, service panels, outlets, etc.
    - For Level 2 resilience sites, it is suggested that the electrical components be above the 1000-year base flood elevation. Note: a 1000-year flooding time period represents a 5% chance of flooding over a 50-year period so Level 3 and 4 facilities should elevate the electrical components higher than this.
    - When determining the minimum elevation, account for flooding models that do not incorporate all observed and expected changes in land use or changes in historical weather patterns (the above only partially accounts for this).

- Water protection should also be extended to protecting against burst pipes, and dams or other manmade water barriers being damaged.
- It is often preferable to be in an area that is not expected to flood rather than raising the equipment. This can help reduce vulnerabilities and save costs. The *FEMA Flood Map Service Center | Welcome!*[62] Site provides a search by address feature for mapping flood hazard information and FEMA's National Flood Hazard Layer (NFHL) Viewer (arcgis.com)[63] provides an ArcGIS map.

In addition to following the International Building Code standards, it is recommended that CISA's "The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard"[64] be followed. It defines the criteria and processes that those responsible for the security of a facility should use to determine its facility security level.

Further, the ANSI/APCO *Public Safety Grade Site Hardening Requirements*[65] technical standard should be consulted. Threats discussed in the document include seismic events, wildfires, flooding, wind, ice storms, grid events, and geographical specific events. It covers when and how to use fencing, gates, and signs to improve physical security. General recommendations include burying or encasing fuel tanks in concrete materials and limiting access to the onsite generator.

For any critical infrastructure organization considering a nuclear SMR reactor in its future plans, the May 2014 NRC document *Physical Security Best Practices for the Protection of Risk-Significant Radioactive Material (NUREG-2166)*[66] should be reviewed. This NRC document may also help Level 3 and 4 Resiliency site managers and even Level 2 site managers improve overall site physical security.

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.

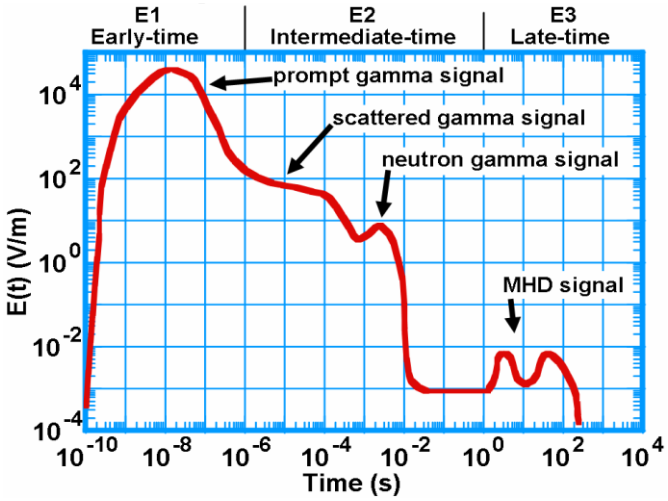

Figure 4. Generic HEMP waveform (ref. Meta-R-324)

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.

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.

"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)

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.

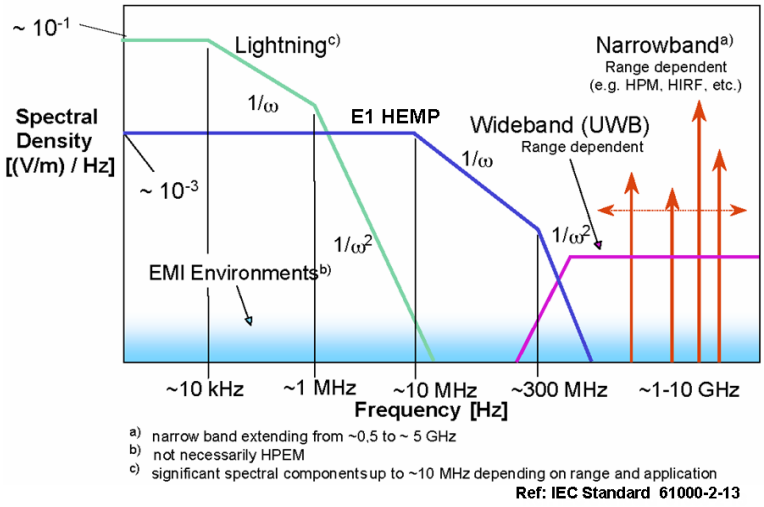

Figure 5. Frequency ranges of lightning, EMP, and IEMI

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.

5. GENERATORS AND FUEL

Target Audience:

- Power Management/Engineering: *Read all*
- Continuity & Planning: *Browse/Read*

This chapter covers the types of primary independent power generation systems that most critical infrastructure organizations will use. More specifically, it discusses generators running on liquid fuel (i.e., diesel, gasoline) or gas (i.e., natural gas, propane) and is broken up into the following sections:

- Section *5.1 Diesel and Gas Generator Overview*
- Section *5.2 Diesel versus Natural Gas/Propane Comparison*
- Section *5.3 Fuel and Generator Maintenance Procedures*
- Section *5.4 Diesel and Natural Gas/Propane Fuel* Deliveries
- Section *5.5 Emergency Generator Deliveries and Mobile Power*

Per the National Communications System's February 2009 "*Long-Term Outage (LTO) Study (p. ES-3)*", "standard diesel or natural gas-fueled generation systems will not meet the requirements necessary to sustain operations during an LTO once the supply chain is extended to a critical length, and equipment that was sized for STOs [short-term outages] begins to break down." Thus, the optimal solution may be to **procure multiple smaller generation sources rather than buy one large generator, particularly if the site's power load can be prioritized and segmented**. In this case, it is recommended that each generation source be capable of meeting the most critical power load and with the combined generation power capable of meeting the entire non-segmented load that needs to be backed up.

The above concept can also be thought of using the N+1 concept. "N" is the minimum number of generators needed to meet the most critical power load and the "+1" generator is used if one of the "N" generators fails or if additional generator capacity is needed to power loads outside of the most critical ones. N+2 is like N+1 but has two redundant generators in case two generators fail.

Implementing different types of generators (e.g., natural gas and diesel) is strongly recommended for Level 3 and Level 4 resilience to improve fuel diversity. The control electronics can adapt to the different engine response times and successfully load share.

Note: The material below does <u>not</u> provide low level design and installation guidelines, such as how to install a generator or the ventilation required. It is recommended that other documents be reviewed for those guidelines, such as (i) IEEE Standard 446-1995 *IEEE Recommended Practice for Emergency and Standby Power Systems for Industrial and Commercial Applications*, (ii) *NFPA 37 – Installation and Use of Stationary Combustion Engines and Gas Turbines*, and (iii) *NFPA 110 – Standard for Emergency and Standby Power Systems*.

5.1. Diesel and Gas Generator Overview

Generators convert mechanical energy generated by the engine into electricity using an alternator. There are four types of generators per ISO 8528-1 "Reciprocating internal

combustion engine driven alternating current generating sets – Part 1: Application, ratings and performance" that can be used for backup/emergency power as well as some that can be for continuous power by non-utility entities. These are summarized in Table 11. The generator ratings assume that proper maintenance is performed although the number of continuous hours of operation can be extended on some units with certain accessories such as advanced oil management systems.

Table 11. ISO 8528 Generator Ratings[82]

Rating	Definition Summary	Comments
Emergency Standby Power	• Up to an average of **200 hours** of operation per year. • Permissible average power output over 24 hours of operation shall not exceed 70% of the power rating.	• Due to the limited number of operational hours, it is generally more suitable for Level 1 and 2 resilience than for higher levels of resilience. • Considered acceptable for Level 2 since 200 hours is sufficient to run for one week. • Manufacturer maintenance intervals must be respected.
Limited Time Running Power	• Up to **500 hours** of operation per year.	• This can be used for peak shaving to save power costs and it can help turnover the fuel to ensure that the quality of the fuel is maintained. • Suitable for Level 1 and 2 resilience. • Check with manufacturer if generator could run continuously per your requirements (e.g., 30 days on rare occasions) to meet Level 3 resilience requirements (how often the air filter must be changed is dependent upon local conditions).
Prime Running Power	• **Unlimited** number of operating hours per year. • Permissible average power output over 24 hours of operation shall not exceed 70% of the power rating.	• Suitable for Levels 3 and 4 resilience as well as lower levels of resilience. • Diesel generators suitable for continuous operations as well as most natural gas generators are significantly more reliable than standby generators.[83]
Continuous Operating Power	• **Unlimited** number of operating hours per year. • Typically has a high load factor.	• Operating a generator at light loads for extended periods of time reduces the efficiency of the power system and creates maintenance issues due to wet stacking (operating under 50% rated capacity).[84]

Generators are becoming more and more important to ensure the nation's continuity when the electric power grid is disrupted. Diesel is the most common type of generator for backup/emergency power purposes followed by natural gas.

Diesel Generators

The global diesel generator market size is expected to increase at a CAGR of 4% from $16 B as of 2018 to $21 B by the end of 2025. Diesel is the most popular independent power generation option deployed largely because of several major advantages:

- **Low cost –** Diesel generators tend to be the least expensive at least for larger loads.

- **High efficiency** – Its efficiency is better than with gasoline and much better than with natural gas/propane.
- **Energy density and ease of storage** – Diesel has a much higher energy density than natural gas or propane making it much easier to store and taking up much less space.
- **Wide availability of fuel** – Diesel is widely available and can be delivered cost effectively without the need for a pipeline.
- **24/7 Readiness** – As long as fuel is available, the generator can be run at any time of the day or night unlike some alternative generation sources such as solar or wind.

Diesel generators also have several disadvantages including environmental, fuel storage and maintenance issues. The disadvantages and the advantages are listed in the below subsection *Diesel versus Natural Gas/Propane Comparison*.

Natural Gas and Propane Generator Market

Figure 7. Natural Gas Distribution

Natural gas (see Figure 7) is the second most common type of independent power generation that is used behind diesel with just over 25% of the market, but its market is growing faster than the diesel market. The global natural gas generator market is projected to reach USD 10.87 B by 2025, registering a CAGR of 10.7% from 2019, according to Grand View Research, Inc.[85] Its primary advantages over diesel is that it is more environmentally friendly (particularly renewable natural gas -- see Renewable Natural Gas | US EPA[86]), and minimal gas needs to be stored onsite depending upon the overall solution (see *Diesel versus Natural Gas/Propane Comparison* section below for more details).

Low power generators, which provide under 350 kW of power, and are very popular for residential and commercial power backup operation. Medium power generators provide 350 kW – 1 MW of power and are largely used for commercial and industrial applications. High power generators with over 1 MW of power are installed in large manufacturing facilities, data centers, and remote locations.

Historically, natural gas backup generators have had a difficult time meeting a 10 second startup requirement that many companies have for a backup system, and they have had a shorter lifespan than diesel. However, with many natural gas generators now able to meet the 10 second startup requirement and with a longer life span, the diesel advantages in these areas have been reduced. Further, environmental factors have become more important, which benefits natural gas. A comparison of these two types of generators is shown below in *Table 12 and Table 13* although the comments are general by nature and may vary depending upon the individual site's requirements.

For smaller power needs up to 150 – 200 kW, generators can be purchased that can use natural gas or propane. For larger generators or ones that run during non-emergency, the cost of transport and storage is often too high to use propane gas, but propane can be a good backup to natural gas. Propane can match the combustion properties of natural gas although because it has a higher boiling point than natural gas, propane can be delivered via truck and kept in tanks on site. A conversion kit may be necessary to use propane instead of natural gas depending upon the make and model of the generator.

Dual-Fuel and Other Generators

There are also some interesting **dual-fuel or multi-fuel** generator options that can run on either diesel or natural gas with some also able to be run on other fuels such as propane, or gasoline. These can provide additional power resiliency against power outages. However, these dual-fuel generators are declining in numbers due to cost and additional environmental regulations. If a dual-fuel generator is used, the fuel switching capabilities should be rigorously tested.

A better resilient power solution to dual-fuel generators may be to install two smaller generators, one of which runs on diesel and the other on natural gas/propane. Each generator should be sized to meet the requirements of the most critical equipment and operations with the two generators together able to meet the overall emergency or backup power needs. This requires segmenting the load, but it adds resiliency and efficiency in fuel usage and does not have a single point of failure that just having one dual-fuel generator would have. It also makes replacement of a generator easier.

The portion of the fixed generator market outside of diesel and natural gas is small. For portable and very small generators, **gasoline** is the most popular fuel – it was a $1.9 B market in 2017 per *MarketsandMarkets.*[87] Gasoline is not discussed in detail below because diesel is safer, easier to store, and doesn't deteriorate as quickly as gasoline, but gasoline may fill a role with some resilient power plans.

Fuel cells, which use chemical energy of hydrogen or another fuel to produce electricity are discussed further under *Section 8.3 Fuel Cells.*

Methanol may also have potential in geographical areas where it is commonly used. Its primary backup power application is for it to be used as a backup fuel for natural gas generators. Stirling engines can use methanol and with minor modifications, natural gas turbines can use both methanol and natural gas. Methanol can be stored on site as a liquid in most environments (its boiling point is 148 degrees) so that it has a much higher energy density than propane and likewise takes up much less space. Similar to propane, it is clean burning and requires a lot less care in storage than most diesel or fuel oils. Unfortunately, because methanol is typically not readily available, it is generally not practical to use when resilient power is needed. It also has less than half the energy density as diesel. Due to these negatives, it is not covered further in this document although it could have potential in some areas in the future.

Liquefied Natural Gas (LNG) is around 600 times smaller than in its natural gaseous state and is typically used to make the transportation of natural gas much more cost effective, particularly prior to being loaded onto a tanker. However, there are companies that can transport LNG via land often to a remote site that isn't connected to either the electrical grid or to a natural gas pipeline, but these companies can also transport it for use in emergency situations.

Compressed Natural Gas (CNG) is becoming more prevalent with an expected global CAGR of 6%.[88] It is formed by compressing natural gas to less than 1% of its normal volume. Mobile compression enables natural gas to be sourced from virtually any nearby pipeline. It is generally less expensive than LNG since it does not need to be supercooled and it can be stored much longer. On the other hand, the energy density is much lower than with LNG although the total storage space required may or may not be less depending upon the amount stored since LNG requires a more sophisticated storage solution.

Multi-fuel Microturbines can use diesel, natural gas, and other types of fuels such as propane and biogas. These generation sources have few moving parts, excellent energy efficiency,

reduced emissions, and can run for a long time between maintenance intervals. With these characteristics, its market share is growing particularly in markets where the generator is routinely used (e.g., demand response programs, off-grid).

5.2. Diesel versus Natural Gas/Propane Comparison

The tables below compare diesel versus natural gas because they are by far the two most common energy sources. Propane is considered, but as a backup fuel source to natural gas. Propane could be used as the primary energy source for generators less than 150 – 200 kW, but it is generally not used for these purposes since diesel is much easier to transport and store per megawatt-hour (MWh) generated. Small, portable generators typically use gasoline. Table 12 below considers the costs between these two generator types. Table 13 discusses non-cost related pros and cons of each approach.

Table 12. Costs of Diesel Generators Compared to Natural Gas/Propane Generators

Evaluation Criteria (cost)	Diesel Generators	Natural Gas/Propane Generators
Upfront Costs Above 150 kW (See Legend Note below for color/font description)	• *Rating: Good* • In this market segment, the cost of emergency/standby diesel units is typically 40 to 50% less than natural gas units.[89] • On the other hand, liquid fuel handling system for large diesel generators cost more than the natural gas handling system, particularly as more fuel must be stored to support longer outages. • Tier 4 generators, which the EPA allows to be run during non-emergencies, add significant costs.	• *Rating: Moderate* • Costs have decreased, but upfront costs are still generally higher than with diesel. • Above 150 kW, natural gas generators use diesel-derivative engines (rather than typically using automobile derived engines) that are more specialized and have a lower power density. • At higher power output capabilities, often 400 kW, natural gas generators may require load management systems to add loads sequentially.[90]
Upfront Costs Below 150 kW	• *Rating: Moderate* • Diesel generators tend to cost more than natural gas ones at lower power levels. • The above statement assumes that no new gas pipeline needs to be run to the site.	• *Rating: Good* • Natural gas generators below 150 kW are generally priced at or below diesel units. • If any significant pipeline needs to be run for a natural gas generator, that can substantially increase costs (in which case this cell would be orange due to the likely high cost).
Operating Costs	• *Rating: Moderate* • Target is 50%-70% generation utilization to meet the load demands. Running at low load can send unburned fuel and soot into the exhaust or fuel must be burned off and wasted.	• *Rating: Good* • Reduced maintenance costs. • Generally, reduced fuel costs versus diesel although this is dependent upon commodity prices. • Minimal expense to modify system so that it can be run in non-emergency mode helping to pay for generator in a demand-response/interruptible electric

Evaluation Criteria (cost)	Diesel Generators	Natural Gas/Propane Generators
	• Need to store the diesel fuel, which takes up valuable space usually near the facility being supplied. • Diesel fuel maintenance increases operating costs – see Section 5.3. Only more expensive and complex Tier 4 diesel generators can be run in non-emergency mode to reduce peak demand costs.	rate program that exists in many markets. • If utility rates are particularly high, a natural gas generator can be used to reduce peak demand rates. See Chapter 6 POWER TRANSFER SYSTEMS AND MICROGRIDS for more details.

Legend Note: A green background (Rating: Good) is the highest rating for that evaluation criteria followed by a yellow background (Rating: Moderate).

Table 13. Non-cost Related Issues of Diesel versus Natural Gas/Propane Generators

Non-cost Criteria	Diesel Generators	Natural Gas/Propane Generators
Reliability (See Legend Note below for color/font description)	• *Rating: Moderate* • Considered reliable when the fuel and the generator are well maintained. • Most reliability issues are due to poor maintenance with 80% due to poor quality fuel[91], e.g., water, microbes, and sediment can enter the diesel fuel. • Enables quick adjustments to load changes. • Is often less reliable than natural gas if the diesel maintenance procedures are not rigorously followed.[92] • Reliability has decreased since ultra-low diesel fuel requirements were implemented in 2010.[93]	• *Rating: Moderate* • Reliability has increased significantly over the past decade. • Per NREL "natural gas generators are less likely than diesel generators to fail during a power outage" although this assumes that the generators and fuel are not optimally maintained.[94] • There is a systemic risk of a gas pipeline malfunctioning during a power outage. • Natural gas supplier takes care of the gas quality. • Natural gas generators can be run much more often than just being used for backup services, which helps to ensure that they are working properly when an emergency comes.
Fuel Supply	• *Rating: Moderate* • Enables guaranteed supply of fuel while onsite fuel is available. • Can be delivered almost anywhere although trucks and drivers that must deliver the diesel are dependent upon roadways. • Diesel may not be available for lower priority sites during power outages due to greater demand and crimped supply lines. • Winterized diesel may be needed at cold temperatures to prevent it from gelling. • *Rating: Moderate*	• *Rating: Poor* • Although they are monitored remoted via a Supervisory Control and Data Acquisition (SCADA) system, even the fear of a natural gas pipeline breaking can lead to shutting down the pipeline. • Propane typically can be used as a backup fuel for generators under 150 kW – 200 kW although availability of propane and other alternative fuels are often very limited. • Some natural gas turbines can burn liquid fuels (e.g., diesel, butane, Kerosene), but this significantly

Non-cost Criteria	Diesel Generators	Natural Gas/Propane Generators
	• *Rating: Moderate* • Safety codes (e.g., for hospitals) may require fuel to be stored onsite, which makes diesel the only option in many cases.[95] • Storage volumes are substantially less than if using propane. • Many types of diesel generators are often available for emergency delivery except for Tier 4 generators.	increases the cost of the natural gas system. • Fuel supply reliability significantly increases if the natural gas pipeline compression system is powered by natural gas and not the electrical grid. (An electric powered pipeline compressor will often have a backup generator, but fuel supplies can run out.) • Enterprise natural gas deliveries often have priority over utility companies.
Environmental	• *Rating: Moderate* • Emits more emissions that are especially dirty during startup (carbon monoxide poisoning is a major issue). • Tends to be louder. • On the positive side, diesel is less likely to explode than natural gas and safer than gasoline.	• *Rating: Good* • If catalytic converters are included, the generator produces less nitrogen oxides and carbon monoxide as well as no measurable particulate matter. • It is quieter and emits much less carbon dioxide.

Legend Note: See the legend note in Table 12. A dark orange background (Rating: Poor) indicates that the evaluation criteria rating is worse than a yellow background.

Diesel Versus Natural Gas/Propane Comparison

To choose the best generation source(s) between diesel and natural gas/propane, see the best practices shown below in Table 14.

Table 14. Diesel and Natural Gas/Propane Best Practices

Resiliency	Best Practices	Rationale
Level 1	• Use diesel or natural gas/propane typically with at least three (3) days of fuel stored onsite (specific amount stored should be based upon your risk management plan). • Install generators per NFPA 110 per NFPA 37 "Standard for the Installation and Use of Stationary Combustion Engines and Gas Turbines." • If there is minimal onsite natural gas/propane storage, combine with a second type of power generation source, such as a renewable (e.g., solar power) with an energy storage system (ESS). • May strictly rely upon natural gas/propane without substantial onsite fuel storage when the pipeline provider implements the following (the below are important to reduce systemic risks since gas pipelines can feed many, many sites): o Has sufficient fuel or energy storage for their pipeline compression equipment (e.g., pipeline power is provided by natural gas generators) to meet your requirements. o Protect the pipeline electronics from HEMP, cyberattacks, and other risks per this document or per recognized industry standard.	• The Level 1 all-hazards resilience requirement includes three days of guaranteed fuel. • Pipelines often rely upon the electric grid for power and have less than three days of backup power availability. A backup generator for pipeline compressor stations that can use natural gas is the best resiliency solution for backup power. • Supply disruption mitigations could include cross-connectivity of gas supply pipelines, shock-resistant pipeline or pumping LNG into a pipeline.
Level 2	• Implement above best practices with enough onsite fuel storage to meet Level 2 resilience. • If both a diesel and a natural gas generator are deployed, less onsite fuel is needed although sufficient onsite fuel should be maintained per your site's risk management plan. • Above without onsite natural gas fuel storage but with the pipeline and the source protected to Level 2 resilience or equivalent (e.g., seven days of backup power to equipment), and with either (i) a local gas source or (ii) two independent natural gas supply lines fed into the local gas distribution system.	• Being able to use both natural gas and diesel is very beneficial against long-term outages. • A gas source that is nearby can substantially reduce risks versus using a long pipeline where the source is hundreds or thousands of miles away and supplies gas to many areas.
Levels 3-4	• Implement above best practices with enough onsite fuel storage to meet the desired resilience level. • Being able to use multiple fuel types is preferred and can reduce the amount of onsite fuel required. • Relying upon off-site natural gas is not recommended except under niche circumstances where the source and delivery resilience is extremely high.	• Being able to use diesel or natural gas/propane enables power generation even if one of the fuel sources is disrupted.

Another Best Practice: Use Multiple Smaller Generators

These best practices recommend a minimum of one backup/emergency generation source for Level 1 resilience and at least two generation sources or N+1 for Level 2. If the critical infrastructure requires hundreds of kWs of backup/emergency power or more, it is often preferred that two smaller generation sources be deployed for Level 1 and at least three for Level 2 (with two smaller generation sources being used to meet the full load). The advantages are as follows:

- **Improved Resilience** – Provides extra redundancy and optionality:
    - There is extra redundancy since most sites could either use an Energy Storage System (ESS) together with a single generator or reduce the load and run just one smaller generator if required.
    - It is typically easier to obtain a small emergency generator if a unit fails than a large one – see Section *5.5 Emergency Generator Deliveries and Mobile Power*.
    - Can more readily leave a generator offline and maintain or fix it.
    - Easier implementation of fuel diversity.
    - May be able to more cost effectively deploy a renewable energy hybrid system (REHS) and use the ESS and the renewable system to meet peak power demands when combined with a smaller generator.
- **Lower Upfront Costs** – For Level 2 and higher, can usually install fewer kWs of generation capacity, which typically lowers costs. May also be able to reduce Level 1 costs when requiring a moderately high amount of power (e.g., 1 MW or more) since the power generation cost per kW tends to be "U-shaped" so that two smaller (e.g., 500 kW) generators may cost less than one larger (e.g., 1 MW) generator.
- **Reduced Fuel Usage During Power Outages** – The average fuel efficiency may increase since a generator can often be run closer to its optimal power output.

The above advantages are most notable when the load varies significantly throughout the day or when there is an alternative generation source (e.g., an ESS or solar PV system that can augment a smaller generator). If the total number of generated kWs cannot be reduced, and there is no upfront nor O&M cost savings per kW by purchasing smaller generators, then at least some of the above will not be applicable.

Table 15 below provides an example of using multiple smaller generators where only 750 kW of backup generation capacity is purchased instead of 1 MW resulting in lower costs and improved resilience. The example assumes that the load varies significantly depending upon the time of day. These concepts are also discussed in *Table 18. Potential Microgrid Benefits Versus Traditional Power Backup Capabilities.*

Table 15. Example Showing Benefits of Using Smaller Generation Sources

Power Needed	Generation Sources	Comments
Assume Level 2 or 3 Resilience	• Two (2) 500 kW generators • One 500 kW / 500 kWh UPS	• One 500 kW generator is running when on backup/emergency power regardless of the load. • The UPS is only used for the brief period after power is lost and before the generator starts up.

Power Needed	Generation Sources	Comments
Business Day: 300 kW (average) **Nightshift: 100 kW** (average) **Peak: 450 kW**	• Three (3) 250 kW generators • One 500 kW / 500 kWh UPS/ESS	• Lowers the cost since only 750 kW of generation power is purchased instead of 1 MW. • The UPS/ESS is combined with the first generator to meet both the 300-kW average load and the 450-kW peak load while the UPS/ESS is sufficiently charged per the power management plan. ○ This solution can reduce operating costs and increase resiliency since it can provide power even if both generators were offline. ○ Upfront costs will increase if a more expensive ESS needs to be purchased. • During the nightshift, a generator could be operated at 40% capacity (or higher when charging the UPS/ESS) instead of at 20% capacity with the 500-kW generator, which can improve reliability and reduce fuel usage. • The UPS/ESS can be recharged when the load is significantly less than 250 kW or by starting the second generator.

5.3. Fuel and Generator Maintenance Procedures

Generators are notorious for failing due to poor maintenance. Per some studies, 80% of emergency generator engine failures are fuel related.[96] For instance, "during Superstorm Sandy, 50% of hospitals' emergency generators failed due to maintenance and fuel issues."[97] Because of this, the below subsections are very important:

- *Diesel Fuel Storage* – A good storage container in a dry, cool, and dark place can make the fuel last much longer. Consider ceramic tanks which cost more but do not rust.
- *Diesel Fuel Maintenance* – Filters (including a fuel polishing system) and additives can significantly extend the life of the fuel although sometimes the fuel needs to be either used or sent to a special facility to be maintained.
- *Diesel Fuel Testing*– Because of the variability in storage containers, storage location, and the weather, fuel testing often needs to occur to determine how to best maintain the fuel.
- *Diesel and Natural Gas/Propane Generator Maintenance (excludes fuel maintenance)* – Following these procedures helps ensure that the generator(s) will start when needed.

An example of one major fuel quality issue is that diesel components react with oxygen from the air to form fine sediment and gum, which can then block fuel filters and lead to fuel starvation and the engine stopping. The gums and sediments do not burn in the engine very well and can lead to carbon and soot deposits on injectors and other combustion surfaces.[98] In this case, a well-designed storage container, proper fuel maintenance, and testing can all be used to minimize this issue. Good storage can minimize the issue, testing can find the problem, and maintenance including frequent filter changes can keep the engine running well. The optimal time interval between filter changes can be determined by inspecting the filters or the filters can be changed based upon the manufacturer's recommendations.

Records should be maintained for each diesel generator regardless of the resilience level desired. These records should consist of all maintenance activities, failures, errors, causes and corrective actions of any problems, and test data.

For more details about maintenance standards and guidelines, the following document is a good resource: *MIL-STD-3004-1, DoD Standard Practice Quality Assurance for Bulk Fuels, Lubricants and Related Products.* Level 4 resilient generators may need additional design, maintenance, and test methods applied such as those specified in IEEE Std 387-2017 *IEEE Standard for Criteria for Diesel Generator Units Applied as Standby Power Supplies for Nuclear Power Generating Stations*.

Diesel Fuel Storage

The size of the diesel fuel storage container is the first fuel maintenance related decision that needs to be made. To calculate the number of gallons of fuel needed, the power manager or engineer should estimate the average load per hour during a multi-day power outage and the generator efficiency over each of these hourly estimates. The amount of fuel used per hour can then be calculated and the overall usage over a 24-hour period can be determined. Lastly, the storage required can easily be calculated by multiplying the estimated fuel used in a 24-hour period by the number of days that guaranteed power is required. An estimate of the storage required is also shown in FEMA's June 2017 *Power Outage Incident Annex to the Response and Recovery Federal Interagency Operational Plans* under Figure 3 *Daily Fuel Consumption by Critical Facilities*.

Once the minimum fuel storage size is known, the next major decision often is whether to store the container aboveground or underground (in many places, underground storage is not feasible in which case the container must be stored aboveground). The advantages of each storage location are described below:

- **Underground:** Buried or mostly buried tanks are prone to water leakage at the fuel supply cover assembly and from corrosion if the tank is made from metal (consider fiber glass or ceramic or protect the metal for resilient fuel storage). Although condensation is less of an issue with underground tanks than aboveground ones, they will have a difference in temperature between the bottom and top of the tank, which will lead to condensation forming on the tank walls and dropping to the tank bottom. Overtime, this water will accumulate and provide an environment for fungal and microbial growth.[99] Lastly, because it is very difficult to inspect underground tanks, there needs to be automated measurements to ensure that there is no leakage.
- **Aboveground:** The lack of ground insulation and the change in temperature and the amount of sunshine will cause the fuel inside the tank to expand and then contract daily. This contraction can lead to condensation forming on the walls of the tank and then settling to the bottom providing a growth medium. This can cause fuel in aboveground tanks to have a shorter shelf life than underground tanks. Further, fuel is often easier to steal in aboveground tanks than underground tanks requiring additional security. Lastly, in extremely cold climates, kerosene will need to be blended into the diesel fuel to prevent "freezing" during the winter.

The location of the tank should ensure to the extent feasible that the diesel fuel is stored in a dry, cool location without water, humidity, or oxygen being able to enter the storage container although some will enter when the tank exchanges air for fuel. Tanks should also have a well-defined low point where water will collect and be drained. Further, the storage container should

ensure that the diesel fuel will not contact zinc, copper or metal alloys containing them. These metals will quickly react with diesel fuel to form unstable compounds. Even dust with traces of these elements can be an issue.

With good maintenance procedures such as keeping the tank full, use of desiccant vent caps and following those procedures listed in the below subsections, even diesel fuel in aboveground tanks can be expected to stay in a useable condition for 12 months or longer.

Diesel Fuel Maintenance

To properly maintain diesel fuel, it is recommended that an industry or government standard be followed, such as *MIL-STD-3004-1 (latest version), DoD Standard Practice Quality Assurance for Bulk Fuels, Lubricants and Related Products*. Because of the time required for fuel quality issues to occur assuming proper storage is implemented, *MIL-STD-3004-1* states that a "product is considered under long-term storage conditions when held for a period longer than six months without an exchange of at least two-thirds of the tank contents." MIL-STD-3004D states (p. 64) "**product stored without an inventory exchange** received into existing inventories **of at least two-thirds** of the tank content from a different Defense Fuel Support Point (DFSP)/commercial supplier with product that meets quality surveillance requirements **within 6 months is considered long-term storage**."

When feasible, long-term diesel storage should be avoided and at least 2/3rds of the fuel should be used and replaced within six months (or possibly longer than six months in a dry, cool environment or if using high-quality diesel in a good underground storage tank). But as a minimum, at least use the fuel within one to five years and replace it with fresh fuel. Testing the fuel can determine the specific timeframe that should be allotted before the fuel is used.

Turning the fuel over is important because various elements of the fuel deteriorate over time so that eventually rehabilitation is required before usage. If rehabilitation is not feasible, the fuel needs to be replaced. Alternatively, fuel that is approaching but still meets a minimum specification might be moved to another location where it can be quickly consumed (if using MIL-STD-3004-1, the fuel should still meet the Intra-Governmental Receipt Limit). Note that testing, which is also a key aspect of maintaining quality fuel, is covered in the next subsection.

Some maintenance should be performed on a routine basis regardless of whether the fuel is stored long-term. Per MIL-STD-3004-1, these procedures should include the following:

- **Buy Quality Fuel** – Obtain assurances from the supplier that all components are fully refined to promote stability.
- **Check for Water in Tank** – Water checks should be made daily on issue tanks or weekly on static tanks or each time a tank is gauged, whichever occurs first. When water is found, it should be drained as soon as possible.
- **Drain Water** – Bulk fuel tanks should be drained of water after each product receipt, as well as a minimum of weekly thereafter and prior to each issue. Floating roof tanks should be checked more frequently during periods of heavy rain or melting snow. Underground fuel tanks should be checked more frequently when the water table is high and during periods of excessive rain or melting snow.

- **Keep Tanks Full** – Tanks should be kept full to reduce the space for water to condense. Maintaining tanks that are partially empty increases the water build-up and promotes corrosion in the top half of the tank.
- **Filter Fuel** – Establish a system for filtering the contents of the main storage tank through a recirculating filter system to reduce the potential for problems by removing sediment and gums. This can be made automatic. The filters should be checked and changed at regular intervals. When the filter change interval reaches a certain frequency then the fuel should be changed.
- **Clean Tank** – The tank should be emptied and cleaned at least once every 10 years, or more frequently if there is a major contamination.
- **Avoid Biodiesel** – Do not use biodiesel or biodiesel blends if possible. Biodiesel and blends have a shorter storage life than petroleum derived diesel and have lower energy content per gallon which may reduce maximum engine power output.

A **fuel polishing unit** can keep the fuel from being contaminated and can fulfill some of the above steps to ensure that the fuel is always ready to use. It uses multiple stages to effectively filter and remove contaminants including water and microbial growth. The polishing unit can be cost effectively programmed to run on a regular cycle without human intervention eliminating the need for chemical stabilizers. Polishing the stored fuel as seldom as once a month provides for a very highly extended shelf life of the stored product.

When a polishing unit is not used and it is infeasible to cycle through the fuel in a timely fashion, the following additives may be needed to improve **diesel** fuel storage life:

- **Fuel stabilizers or antioxidants** are recommended for long-term fuel storage to stop the oxidation processes from taking place and reduce the formation of sediment and gum.
- **Fungicides/biocides** stop fungus and bacteria from growing in the fuel to prolong the life of the fuel and should be used on a maintenance basis to prevent more costly problems. Care must be taken in handling these since they are poisons. A large dose can be used to kill the fungus although this can lead to a build-up of dead matter which will block filters and cause the fuel to oxidize. Thus, when there is fungus, it should be killed, and the tank emptied and drained.
- **Metal deactivators** stop copper, zinc, and other reactive metals from reacting with the fuel and should be used if this is an issue.
- **Water controllers** chemically bond water, which will collect at the bottom of a tank that isn't drained, helps prevent the tank from becoming a breeding ground for microbes. The water can then be burned off as steam when the generator is running.

Diesel Fuel Testing

As mentioned under the *Diesel Fuel Maintenance* subsection above, testing is required if less than 2/3rds of the existing diesel is used and replaced within 6 months or if there is a known issue that requires more frequent testing (e.g., water leaking into the tank, purchased fuel that was previously stored, container is in excessive humidity and heat). As with the *Fuel Maintenance* subsection, it is recommended that an industry or governmental standard be followed, such as *MIL-STD-3004-1 (latest version), DoD Standard Practice Quality Assurance for Bulk Fuels, Lubricants and Related Products.*

Per MIL-STD-3004-1 the rate of product deterioration cannot be accurately predicted because storage locations differ in temperature and environment and the products stored at each location are produced differently from refinery to refinery. Therefore, each product in long-term storage or of questionable quality should be sampled and tested more frequently when deterioration is first detected. **These tests should be in accordance with the B-2 test requirements listed in *MIL-STD-3004-1 Table XV.***

In addition to the above, a monitoring program should be established whereby samples are taken at regular intervals to monitor the condition of the fuel. The samples can be visually examined at the site for evidence of haziness, sediment, darkening or sent to a laboratory for testing.

Diesel and Natural Gas/Propane Generator Maintenance (excludes fuel maintenance)

Frequent maintenance is particularly important for emergency generators since many of them are not rated to operate more than 200 hours per year[100] with others not rated to operate more than 240 hours or 10 days of continuous operations. Indeed, per FEMA, "the failure rate of backup generators will increase to approximately 15 percent after 24 hours of continuous use."[101]

The failure rate of generators and the limited ability of emergency generators to continue to operate under long-term outages are the two primary reasons these best practices recommend using two smaller generators versus one larger one if feasible. With two smaller generators, one can takeover while the other one is serviced. Further, if one fails to operate properly, there will be another generator capable of running the most critical operations assuming that the load can be subdivided adequately. To compare diesel generator resilience versus natural gas/propane generator resilience, see *Table 13. Non-cost Related Issues of Diesel versus Natural Gas/Propane Generators*.

To help ensure that the backup diesel or natural gas/propane generator will operate when needed, **the generator maintenance manual should be followed**. Some of the typical maintenance activities that are recommended are shown below in Table 16:

Table 16. Diesel and Natural Gas/Propane Generator Maintenance Activities

Activity Timeline	Best Practices (applicable to all resilience levels unless indicated otherwise)
Weekly	• Level 4: Run generator to ensure that there are no issues. • Visually check the unit, circuit breaker is closed (unless this automatically creates an alert), generator will automatically start, and no fluids are leaking. • Drain water traps.

Activity Timeline	Best Practices (applicable to all resilience levels unless indicated otherwise)
Monthly	• Level 1: Exercise generator for a minimum of 30 minutes using a load that either (1) maintains the minimum exhaust gas temperatures as recommended by the manufacturer, or (2) at not less than 30% of the generator's standby nameplate kW rating. These tests are per National Fire Prevention Association (NFPA) 110 *Standard for Emergency and Standby Power Systems*. • Level 3: Operate the generator under load for long enough to fully heat up the generator at not less than 50% capacity for 30 minutes and at not less than 75% capacity for one hour for a total test duration of not less than 1.5 hours per NFPA 110's Annual Requirements. • Check engine coolant and oil. • Ensure the battery is charged.
Quarterly	• Check the battery charging system and that the battery is within its expected life timeframe. • Closely check the entire generator system and ensure that there are no loose or corroded wires, no rodents are living there, and everything functions properly. • Check inventory of maintenance equipment (such as filters), repair parts, and instructional manuals / procedures (including manual switchover and grid disconnect procedures) to ensure personnel / equipment readiness.
Bi-Annually	• Inspect the enclosure, drive belts, coolant heater, exhaust system, air induction piping and connections, the DC electrical system, and the AC wiring and accessories.[102] • Examine the battery electrolyte level, specific gravity, cables, and connections. • Check for coolant, oil, or fuel leaks, including their connectors and hoses. • Examine and clean the air cleaner units.
Annually	• Change all the filters and spark plugs. • Clean the crankcase breather and test the cooling system and flush it when needed (needs to be flushed more often with more generator usage). • Check the coolant concentration. • Operate the generator under load for long enough to fully heat up the generator at not less than 50% capacity for 30 minutes and at not less than 75% capacity for one hour for a total test duration of not less than 1.5 hours per NFPA 110. • Per the O&M Plan or at least annually, verify that electricity is only provided to the critical equipment tiers per the O&M Plan and that applicable equipment can be put into energy conservation mode (e.g., thermostats are adjusted appropriately, lighting is reduced).
Special Weather Events	• Ensure generation system is prepared for special weather events, such as using low temperature oils before a very cold weather event. • Fill fuel tanks, including adding additives to liquid fuels as needed for extra cold temperatures (see *Diesel Fuel Maintenance* subsection above). • Can require additional starting aids to be 100% operational such as a jacket water heater, battery charger and generator starting batteries.[103]

In addition to the above specific maintenance activities, high-level generator process related maintenance items activities per the EPA include:[104]

- Test the generator under load every time after it is serviced.

- Perform additional maintenance requirements for a generator that is planned to be used for 10 days or longer.
- Level 3 resilience should include preparing and executing a test plan to operate the critical loads or comparable test loads for extended periods.
- Record all maintenance activities to assess performance and operating costs to inform predictive maintenance requirements and future buying decisions.
- When changing the oil, consider sending a sample to be tested for the presence of metals. Metals could indicate engine wear, which may indicate that other repairs are needed.
- Consider service requirements when selecting the generator location for ease of service access and replacement.
- See *Appendix A REGULATORY AND UTILITY POWER GENERATION ENVIRONMENT* for details on some EPA regulations regarding operating generators.

5.4. Diesel and Natural Gas/Propane Fuel Deliveries

Under Section *1.4 Definition of Resilience Levels,* a Level 1 resilience site should have guaranteed power under all hazards defined in your risk management plan to meet the site's requirements by implementing one of the following:

- Onsite Fuel Storage – Store the amount of fuel needed onsite to meet the all-hazards requirement (e.g., 3 days for Level 1). The power manager may need to scale back operations to the most critical infrastructure to extend the fuel supply and meet this requirement, particularly at higher resilience levels.
- Microgrid – Typically working with onsite storage, implement an island-mode capable microgrid that the site manager can tap into for additional power (e.g., renewables, neighbor's fuel supply) to help meet resiliency requirements and prioritize the power to the most critical resources.
- Nearby Fuel Storage – Store fuel nearby with a delivery mechanism that is extremely reliable under all hazards.

Guaranteeing fuel delivery under all hazards is very difficult since most private fuel contractors are only prepared for conditions that have previously occurred and not for an extended outage. This is particularly true under worst-case or near worst-case scenarios when the outage is across multiple regions where there is no functional power grid, communications are substantially disrupted, the roads are unpassable, and gas stations are out of fuel or unable to pump it.

To exceed the minimum all-hazards requirements, commercial contractual fuel deliveries can be used to provide the fuel under commercially reasonable conditions and sometimes under best-efforts conditions. Because most states can commandeer commercial fuel during an emergency, the critical infrastructure power manager should ensure that his/her site is prioritized appropriately so that the fuel will not be commandeered and the fuel that will be delivered is also not confiscated. There are some commercial agreements with no single point of failure (including fuel being available that is outside of the area) that may be very reliable for up to 30 days, but most supply agreements are not rigorously developed enough to meet

delivery requirements under all hazards. Nevertheless, even a poor contract is better than planning to buy fuel from the spot market after a disaster / power outage.

Almost all non-military sites rely upon commercial fuel deliveries using either as needed purchases or a contract with delivery terms based upon commercially reasonable efforts. Since these deliveries often are not adequate, federal, and state/local governments also play a critical role to provide fuel and spare generators in longer-term outages as described below in Table 17.

Table 17. Fuel and Generator Delivery Responsibilities

Agency	General Responsibilities	Implementation Process
Industry	• Provide fuel to whomever pays for it. • Delivery reliability can be based upon the contract.	• The implementation varies by company and by contract in some cases.
FEMA	• Responsible for supporting state and local agencies with emergency fuel and generators during Presidentially declared emergencies (per the Stafford Act). • Cannot support federal agencies unless it is through a state/local partnership.	• Uses commercial fuel contracts to provide fuel during Presidentially declared emergencies. • Obtains assistance from the Defense Logistics Agency (DLA) when required. • Can make one time buys from federal agencies.
DOE	• Primary responsibility for ESF #12. • DOE's ESF #12 responsibility is "*to facilitate the restoration of damaged energy systems and components when activated by the Secretary of Homeland Security for incidents requiring a coordinated Federal response.* • The Office of Fossil Energy and Carbon Management manages the U.S. Strategic Petroleum Reserve, Northeast Home Heating Oil Reserve, and the Northeast Gasoline Supply Reserve.	• As part of its ESF #12 responsibilities, DOE works closely with industry partners across both the electricity and oil & natural gas subsectors on preparedness and response activities. • During an incident, DOE holds regular calls with industry partners for situational awareness and to discuss any unmet needs that may require federal assistance. • Decisions to release diesel fuel from the Northeast Gasoline Supply Reserve are made under the authorities of the Energy Policy and Conservation Act.
GSA	• Provides fuel to GSA maintained facilities through inter agency agreements. • GSA does not offer generator refueling as a service to federal entities that own or directly lease their own buildings.	• Fuel is provided through GSA's Public Building Service. • Buys fuel from commercial vendors and from DLA (who typically obtains it from industry).
Defense Logistics Agency (DLA)	• Provide fuel and generators for the entire federal government. ○ For non-military federal agencies, provides fuel and related logistics support through a direct delivery program via commercial vendors. ○ Provides fuel to GSA and FEMA in accordance with ESF#7 and in accordance with 41 C.F.R. § 101-26.602 "*Fuels and packaged petroleum products obtained from or through the Defense Logistics Agency*."	• Sells diesel, gasoline, marine and aviation fuels. Also sells electricity and natural gas where states permit competition. Does not sell propane. • Maintains a database of fuel deliveries (see https://www.dla.mil/Energy/Business/ContractInformationSystem/ for DLA database). • Primarily relies upon local commercial contracts for commercial specification fuel

Agency	General Responsibilities	Implementation Process
	• Can only sell to state or local agencies that meet the "public interest" requirement of 10 U.S.C. 2922e(d). ○ When there is no emergency, this typically means having a closely aligned, formal partnership with a federal agency (e.g., support a military service mission, jointly fight forest fires). ○ During emergencies, 'in the public interest' could apply after local, state, and FEMA resources are exhausted or unavailable.	products (gasoline, diesel, heating fuel) delivered to Federal and DoD sites. • Military bases maintain limited quantities of commercial specification gasoline, diesel, and heating oil to support day-to-day operations only. • Large quantities of military specification aviation or marine fuels are usually available. However, the use of aviation fuel can cause problems in many commercial generators due to its high sulfur content (see generator manufacturer's technical recommendations).
State/Local Government	• Write laws and regulations supporting emergency response/recovery within the state/local jurisdiction. • Help ensure emergency equipment and supplies are delivered to the highest priority customers to minimize the impact to the state/local area.	• Implementation is typically through commercial vendors and contracts. • Some areas may confiscate fuel from commercial supplies, particularly if not needed directly by that organization, to provide to critical infrastructure or high priority stakeholders (e.g., providing fuel to public safety).

General Fuel Delivery Requirements

For most residential and commercial entities, procuring fuel on an ad hoc basis, such as from a local fuel delivery service or from a gasoline station, is sufficient. But for critical infrastructure and operations, a service level agreement (SLA) should be signed that requires at least a commercially reasonable effort to be applied to fuel deliveries. Multiple vendors should also be identified in case the primary one fails to deliver. See the Riggins *Superstorm Sandy Petroleum Shortage After-Action Report*[105] for some of the fuel delivery issues that can occur.

To meet the all-hazards fuel delivery requirement, the critical infrastructure operator could require a best-efforts contract from a vendor with a good performance record. It could also review the procedures that must be followed and the equipment that is used (e.g., the truck's fuel nozzles are compatible with the site's fueling system, the truck can use its own fuel to power itself). This includes signing off on any changes made to the procedures and testing the procedures with the vendor. The fuel delivery process should not rely upon any of the following:

- A single person or vehicle
- Driving on a road that may not be passable during all potential events
- Hoping that the fuel will not be diverted to a higher priority customer
- Guessing the amount of fuel remaining in the fuel tank – remote monitoring should be performed if the fuel tank is not onsite
- A fuel delivery system that doesn't meet the best practices in this document including those listed in the *ELECTROMAGNETIC (EM) SECURITY* chapter.
- Relying upon a local fuel source versus using a regional or nationwide fuel delivery system.

Due to the many requirements to ensure delivery during an all-hazards event, typically the fuel should be stored onsite.

Adjustments in the fuel delivery plan may be needed based upon the potential difficulty in reaching the site during an emergency, the environment, and other factors. For instance, an island (e.g., Puerto Rico) is generally much more difficult to reach than most areas within CONUS. This difficult-to-reach case has a higher risk of a longer-term outage than most areas within CONUS, so additional fuel might be stored onsite assuming that fuel can be physically secured. Solutions could also include extending the fuel supply using a microgrid together with alternative technologies such as a renewable (see *RENEWABLE ENERGY* section) or possibly deploying nuclear within the next several years in a campus environment (see the *NUCLEAR SMALL MODULAR REACTORS (SMRs)* chapter). Improving energy efficiency also reduces the amount of fuel needed and should be an important part of any Resilient Power Plan.

Emergency Fuel Deliveries Provided by The Federal Government

A non-federal entity should only rely upon the federal government for fuel deliveries. However, as described in *Table 17. Fuel and Generator Delivery Responsibilities*, federal fuel deliveries can be a secondary part of the overall resilient power strategy even without an agreement. For long-term, widespread power outages, it is likely that ESF #12 will be activated, which can allow federal agencies to help with fuel deliveries during an emergency. Per FEMA's June 2017 *Power Outage Incident Annex to the Response and Recovery Federal Interagency Operational Plans*, ESF #12 is an integral part of the larger Department of Energy (DOE) responsibility of maintaining continuous and reliable energy supplies for the United States through preventive measures and restoration and recovery actions."[106]

The premise for FEMA's Power Outage Annex is that a power outage affects multiple FEMA Regions or states and leaves millions of customers without power for an extended period. Some areas are likely to get power restored in a few weeks, but the overall outage will last much longer in other areas. Therefore, federal support to local, state, tribal, territorial, and insular area governments in a long-term power outage should utilize limited resources to achieve the most positive impact for the largest number of people (p. 15).

- Resources will maintain infrastructure in areas where power is expected to be restored in two weeks or less. This will reduce the cascading impacts of power loss, maintain, or facilitate quicker restoration of essential services, and prepare regions to accept survivors self-evacuating from areas suffering long-duration outages.
- In tandem with these activities, emergency resources and services will be selectively delivered to areas with the longest projected duration of power loss that have a high population density or a significant number of survivors.

Fuel may also be sourced by other federal entities besides FEMA, but this fuel is typically delivered through FEMA or in consultation with FEMA if it is provided to a non-Federal entity.

For federal sites, fuel deliveries are handled by non-FEMA agencies as shown in Table 17 above. In particular, "DLA Energy Direct Delivery Fuels provides worldwide acquisition and integrated materiel management of commercial fuels delivered directly to military and federal civilian customers"[107], which includes diesel fuel. DLA Energy also supports FEMA during disasters as needed.

There have been suggestions for a national coordination system (e.g., EIS Council calls for a software-based National Recovery Coordination System[108]). This would include delivery guidance for fuel as well as for generators and other essential equipment or supplies that would be needed during a long-term power outage. However, because state governments have the primary responsibility for emergency fuel planning, no federal coordination system exists at this time although DOE has provided funds for state governments to develop such fuel plans.

Natural Gas/Propane Fuel Delivery

Natural gas/propane should not be the cornerstone of a resilient power strategy unless there is a guaranteed natural gas/propane fuel supply. However, natural gas might be part of a system that includes generation sources with onsite fuel or equivalent (e.g., diesel, propane). For instance, as previously stated in the *Dual-Fuel and Other Generators* subsection, a natural gas/propane generator could be paired with a diesel generator, either of which could meet the minimum required critical loads, to provide excellent power resiliency. It could also use propane as a backup fuel source.

Natural gas is typically only delivered via pipelines, which are beyond the direct control of most enterprises. But there are some controls that an enterprise may have over the reliability of the natural gas/propane deliveries:

- Either use an uninterruptible delivery contract so that gas companies will not curtail deliveries to your critical infrastructure site or ensure that your enterprise is high on the priority list.
- Use a highly reliable connection from the gas company to the generator perhaps via multiple delivery pipelines.
- Make the resilience of the natural gas/propane delivery system a key evaluation factor when choosing the vendor.

Some of the characteristics that are desired when choosing a natural gas or propane delivery vendor are (i) their reliance upon the grid, (ii) the degree to which they implement the recommendations in *CYBERSECURITY AND PHYSICAL SECURITY,* (iii) the SCADA resiliency and the readiness to use a backup communications mechanism; (iv) the gas storage capabilities, and (v) the vendor's past record. If a federal agency or department needs natural gas/propane, it can also ask DLA to help it if there is competition in the area as mentioned in Table 17 in the previous subsection.

5.5. Emergency Generator Deliveries and Mobile Power

As discussed under *Chapter 2 BEST PRACTICES* above, systems that meet Level 2 resilience or higher generally should be able to continue to provide power to the most critical systems even when a generator malfunctions or is unavailable because it is being repaired or maintained. The likelihood of two generators malfunctioning is minimal if the previously suggested fuel and generator maintenance procedures are followed and there is not a systemic risk between the two such as flooding. However, Level 4 sites typically should be able to maintain backup power even if two generators fail.

The delivery of an emergency generator or mobile power truck/van may be needed on occasion to help meet the above resilience levels, but this should only be a core part of a critical infrastructure's resilient power strategy if it is assured that a generator or mobile power can be

delivered (e.g., a mobile generator is kept onsite). If the generator is offsite and not nearby and under the control of the critical infrastructure owner/operator with delivery being able to be guaranteed, any of the following negative generator events could happen (does not include fuel issues, which were previously discussed):

- **Unavailable Generators** – The site will likely be in competition with many other enterprises for obtaining a generator. This is particularly true for larger generators or as generators are loaned out and as they begin to breakdown from extended use and need to be replaced.
- **Impassable roads** – Many major events often cause at least some roads to be closed or for the road to be so congested that either deliveries cannot be made in a reasonable period or the delivering entity prioritizes its deliveries.
- **Driver or transport vehicle cannot be dispatched** – There are many reasons that a vehicle might not be able to make it to the site beyond issues with roads. This includes disrupted communications to the driver or to the enterprise, vehicle problems, or the driver being sick or simply deciding to stay home.
- **Generator cannot be quickly connected** – If a generator or a mobile power source can be delivered, the enterprise should use a standard generator interface so that a generator can be plugged in quickly without requiring a lot of time to install. Cabling should be pre-installed to avoid delays due to procurement and installation by a licensed electrician.
- **Generator malfunctions** – The risk of a loaner generator malfunctioning could be high if a rigid maintenance program is not implemented.

If there is no contract or internal capability for a generator or mobile power (e.g., a generator on wheels) to be delivered when needed, the most likely source for a spare generator is from a commercial entity. If no companies can deliver a spare generator or mobile power during declared disasters and emergencies under the Stafford Act and for non-Stafford Act incidents, then contact your local or state emergency manager who may then contact or coordinate with either FEMA or GSA. **FEMA is typically the best contact for state sponsored requirements with GSA being the best contact for federal departments and agencies**.

When FEMA is contacted by the state or territorial Emergency Management Agency (EMA) after neither industry nor the local and state entities can supply the necessary spare generators or mobile power, FEMA will work with its partners to attempt to supply the generators including using its limited stockpile of generators. Because resources will likely become very scarce during a large-scale incident, planners should know their peak and average loads, and then ensure that their critical facilities are on a critical facility register and appropriately prioritized. Typically, the higher the resilience level of the site, the higher priority that site will have, but the larger the generator needed and the bigger the disaster, the more time FEMA will usually require to obtain and deliver the generator and then properly set it up.

FEMA and GSA are the two lead and coordinating agencies per **ESF #7**, which "provides centralized management of supply chain functions in support of local, state, tribal, territorial, insular area, and Federal governments for an actual or potential incident."[109] After GSA or FEMA is contacted, they will work with the other party (GSA or FEMA) as well as the DoD and commercial enterprises as needed to provide emergency generators based upon availability, need, and delivery capabilities. Note: Per ESF #7, DoD "supports the hauling, installing, operations, and maintenance of DHS/FEMA generators for critical public facilities and provides generator lease and purchase support as require."

Recommended Preparation to Receive an Emergency Generator

ESF #3 empowers the United States Army Corps of Engineers (USACE) to coordinate and organize the capabilities and resources of the Federal Government to assist FEMA. USACE facilitates the delivery of services, technical assistance, engineering expertise, construction management, and other support to prepare for, respond to, and/or recover from a disaster or an incident requiring a coordinated Federal response.

It can require many hours, possibly days, to deploy adequately trained assessment, repair, and maintenance teams to all impacted critical public facilities. USACE provides a free web-based self-assessment tool that permits facilities to input, store, and update standby power data prior to a disaster, which expedites the process if additional generator power from FEMA's temporary power assets is ever required for a facility. By some estimates, it can reduce the time to establishing additional standby power by up to 30%.[110]

USACE can help provide assessments of power needs (sizing, etc.) and help an owner/operator install the required hook ups prior to an outage so that getting back up power up and running quickly is expedited after a generator is moved to the site. Without the hook up installed prior to an emergency, it can be very time consuming to schedule technicians to assess and set up a hook up, which is generally the critical path to obtaining and installing an emergency generator. Further, the organization should have a contract in place to quickly obtain a generator delivered during a disaster, particularly if the owner/operator does not want to keep a generator onsite.

REMINDER: **Establish good working relationships and preparedness networking prior to a disaster with personnel in supporting agencies such as FEMA, GSA, USACE, National Guard, Local and State Emergency Management Offices and the Governor's Office.**

6. POWER TRANSFER SYSTEMS AND MICROGRIDS

Target Audience:

- Power Management/Engineering: *Read all*
- Continuity & Planning: *Browse/Read*

When grid power is lost, critical infrastructure and operations should automatically transfer power to the site's resilient emergency power system. There should also be either a redundant automated power switch (at least for Level 3 and Level 4) or a manual power transfer system backing up the automated method as discussed in *Section 6.1* below. Automating the power transfer reduces both the power outage time and the dependency upon limited trained personnel who may or may not be available during a major event.

Because of the increased resilience, at least an "island-mode" capable microgrid (a microgrid that can operate disconnected from the grid) should be implemented for Level 4 resilience and strongly considered for Level 3 sites. The *Microgrid Definition and Purpose* is explained in *Section 6.2* below with the *Microgrid Benefits and Issues* discussed in *Section 6.3*.

6.1. Power Transfer System

An automatic power transfer system transfers the load from the primary power source to an alternate power source without human intervention. Typically, this involves transferring power from the grid to an emergency or backup generator when the grid fails. There are three types of power transfers considered in this document:

- **Automatic Switchover** – Recommended for all power resilience levels.
- **Manual Switchover** – This is needed as a backup power transfer method in case the automated switchover fails. The manual switchover method should be well documented with step-by-step instructions including pictures where applicable so that the switchover does not rely upon one or two people who are the only ones familiar with the process. For manual segmentation of the loads, there should be pictures showing the breaker positions and which buttons to press. These procedures should be placed in an obvious location in case the chief engineer and their backups are not available.
- **Microgrid with multiple potential generation sources** – An island-mode capable microgrid that can isolate from external sources should strongly be considered for Level 3 resilience and implemented for Level 4 resilience. Note: If there is an impending major GMD/EMP event or warning, on-site power generation resources should not be started until the facility microgrid has been isolated from the utility (island mode).

All the above options include a transfer switch, an AC panel with circuit breakers, control logic and remote monitoring, and a user interface. Since the "microgrid with multiple generation sources" includes a lot more than just an automatic transfer system, it is further discussed in Section 6.2 below. All equipment, including the automatic transfer switch and the AC panel, should be protected per *Chapter 4 ELECTROMAGNETIC (EM) SECURITY*. For Level 3, there should be a means to bypass and isolate the ATS (or any component) for repair or replacement without deenergizing critical power to the mission.

An **automatic transfer switch** (ATS) includes control logic, a user interface, and a manual backup in addition to the transfer switch. Robustness is the most important aspect of the system to

ensure that it will automatically switch power to the alternate power system when needed and will not accidentally switch power due to common electrical surges. It also should not generate transients on the AC powerline connecting sensitive microprocessor-based equipment.

The backup mechanism for the ATS should ensure that the enterprise's power system remains in island mode if the ATS is damaged, upset, or hacked until either the primary transfer switch can be repaired/replaced, or the high-level cause of the failure is known. In particular, the trained operator should ensure that power variations (e.g., harmonics) from the grid did not destroy the transfer switch and do not become an ongoing issue. For instance, EMP E3 or GMD could cause harmonics in the distribution system and a redundant ATS (suggested at least for Level 3 and Level 4 resilience) could inherit the same problem that caused the primary ATS to fail if it switches over to grid power too quickly. A manual switchover back to using grid power too quickly could also be an issue unless that power is being passed along to something that can handle the harmonics without passing them along. The ATS should be tested under load when the generator is tested under load as discussed under *Table 16. Diesel and Natural Gas/Propane Generator Maintenance Activities.*

If the **AC panel** circuit breaker tripping function is part of the ATS, the basic control interface between the AC panel and the rest of the system should be determined during the system architecture and design stage. For instance, if a circuit breaker is manually closed, should system report an alarm, and should it notify the ATS so that it can act as needed?

The **control logic** should support the automatic startup of the alternate power system when needed, take actions to prevent an overload condition, and record every automated and manual action that is taken. Further, the required alarms (e.g., switchover, environmental, voltages) should be defined in the O&M Plan using the following alerting process as a minimum:

- A local sound alert should occur when a major event is triggered (e.g., circuit breaker is tripped).
- An electronic alert should be sent immediately to the primary person responsible and trained to resolve the issue, often using multiple transmission mechanisms.
- An electronic alert to the backup person, which should be sent either simultaneously with the alert to the primary person or within a short period of time if the primary person doesn't respond.

Some controllers can manage multiple loads so that if the primary power is disrupted, the user has a programmable choice of which loads will be connected to the alternate power, which is recommended for all resilience levels. This can reduce generator costs, substantially extend the fuel supply, and improve resiliency. If the control equipment fails, the operators should have a fully documented and rehearsed manual recovery plan.

Reducing critical load power requirements can:
- **Save expenses.**
- **Extend the fuel supply.**
- **Improve resiliency.**

The **remote monitoring capabilities** can enable operators to observe engine and alternator data, control system status, power-transfer status, power-transfer connection status, and load levels without leaving the control room or possibly without leaving the office if the automatic transfer system is connected to the network (or the serial connection is directly connected to their office). If there is a connection to the network, the guidelines in the *Cybersecurity* section below should be followed.

There are three types of **user interfaces**: discrete controls (switches, indicator lights), remote control, and touch screen. Most enterprise systems typically have discrete controls and remote-control capabilities with some systems using a combination of all three user interfaces. The discrete controls and touchscreen can provide needed information when in the equipment operating area. The remote control includes the remote monitoring capabilities discussed above.

In a very limited number of cases, sites may be connected to multiple utility generation sources that can supply power to a critical infrastructure site. In these cases, the power transfer system architecture and design need to be worked out with those in charge of the generation sources since those two generation sources may not be synchronized. For the site to rely upon these dual generation sources in place of a backup or emergency generator, the electrical distribution should also implement route diversity such that one event is unlikely to cause both distribution paths to be broken. For instance, if trees could fall on both distribution lines, then either at least one of the power lines should be buried or the at-risk trees that could fall should be cut back appropriately.

6.2. Microgrid Definition and Purpose

The microgrid market is growing very quickly largely due to both the increased resiliency that microgrids add and the benefits discussed in the next section.[111] About 3.2 GW of microgrids were added in 2019 with 16 GW expected to added annually by 2027, according to a forecast by Navigant Research.[112]

> ***"For many sites, microgrids offer many benefits including enhanced reliability, reduced life cycle costs, improvements in power quality and efficiency, demand reduction, reduction in fossil fuel emissions by using renewable and nuclear generation, and installation flexibility for both urban and rural applications."***
> **Dr. George H. Baker,** Microgrids — A Watershed Moment (2020)

Implementing at least the island-mode microgrid resiliency aspects (excludes being able to export to the grid while the site is producing its own power), is highly recommended for Level 3 and Level 4 resilience and should be considered for Level 2 resilience and even Level 1 campus type environments. Microgrids should implement all the guidelines in *Table 3. Resilient Power Best Practices*. The U.S. Department of Energy (DOE) Microgrid Exchange Group defines a microgrid as the following:[113]

> *A microgrid is a group of interconnected loads and distributed energy resources within clearly defined electrical boundaries that acts as a single controllable entity with respect to the grid. A microgrid can connect and disconnect from the grid to enable it to operate in both grid-connected or island-mode.*

When renewables are used, the site will typically want to implement a microgrid so that it can take advantage of the renewable power while connected to the grid. However, if implementing multiple generators, the site may prefer to implement all the aspects of a microgrid except being connected to the grid while running onsite engine-generators. The island-mode capability is critical to reliably provide power to equipment and facilities when the grid has failed. From a safety perspective, island mode is required when the site is generating power and there is a grid power outage to prevent repairmen working on restoring the grid from being injured. The distributed energy resources in a microgrid keep the critical infrastructure from being

dependent upon any one backup generation source. For added resiliency or to reduce costs, sometimes multiple microgrids are combined into an archipelago.

The above microgrid definition has the key resiliency criteria that the energy resources are interconnected, which can be used to optimize reliability, efficiency, and cost. By acting as a single controllable entity, even if the primary energy system goes down and a backup component malfunctions (e.g., generator fails), the system should be designed so that the backup system can continue to provide power to at least the critical equipment and facilities.

A typical power backup system is shown in Figure 8. More recently, microgrids have been used to augment the grid via the architecture shown in Figure 9, particularly when the power system occasionally generates excess electricity or in areas with substantial variability in electricity prices based upon supply/demand. This augmentation of the grid can be financially lucrative and help pay for the backup system.

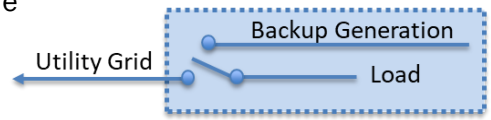

Figure 8. Basic backup power system includes island mode

Diesel generators typically have been the primary backup mechanism for larger sites that need over 150 kW, but microgrids better enable natural gas/propane generators to be a backup solution since multiple generators can be combined to meet the required demand. Further, natural gas/propane generators can be used to augment the grid. Diesel generators can also be used in a smart microgrid, but they must be a more expensive Tier 4 generator to be run to augment the grid as discussed in *Table 11. ISO 8528 Generator Ratings*, which the EPA allows to be run during non-emergencies.

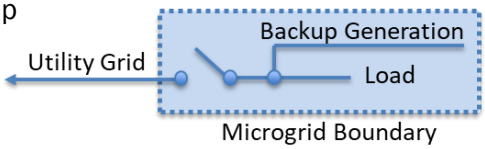

Figure 9. Smart microgrid system enables grid augmentation

Renewables are often implemented to save fuel costs and for environmental reasons, but renewables combined with a battery energy storage system (BESS) can significantly improve resiliency in a microgrid by extending the fuel supplies during a long-term power outage. During a power outage, the renewables can at least intermittently provide power and enable operations after fuel supplies are depleted and more fuel cannot be delivered. Note: In this document, it will be assumed that a BESS does not provide uninterruptible power for sensitive equipment such as computers unless explicitly stated otherwise (e.g., the term UPS is used).

Figure 10 below shows a conceptual microgrid architecture (specific microgrid implementations vary greatly). The amount of onsite fuel storage is dictated by the resilience requirements. The recommended Backup Generation System may consist of one or more diesel or natural gas/propane generators that typically have onsite fuel storage (see *Diesel versus Natural Gas/Propane Comparison*). The specific architecture shown in the figure assumes that the BESS is too slow for some sensitive equipment so local energy storage (LES) UPSes are used where needed (e.g., ensure that a server doesn't briefly lose power).

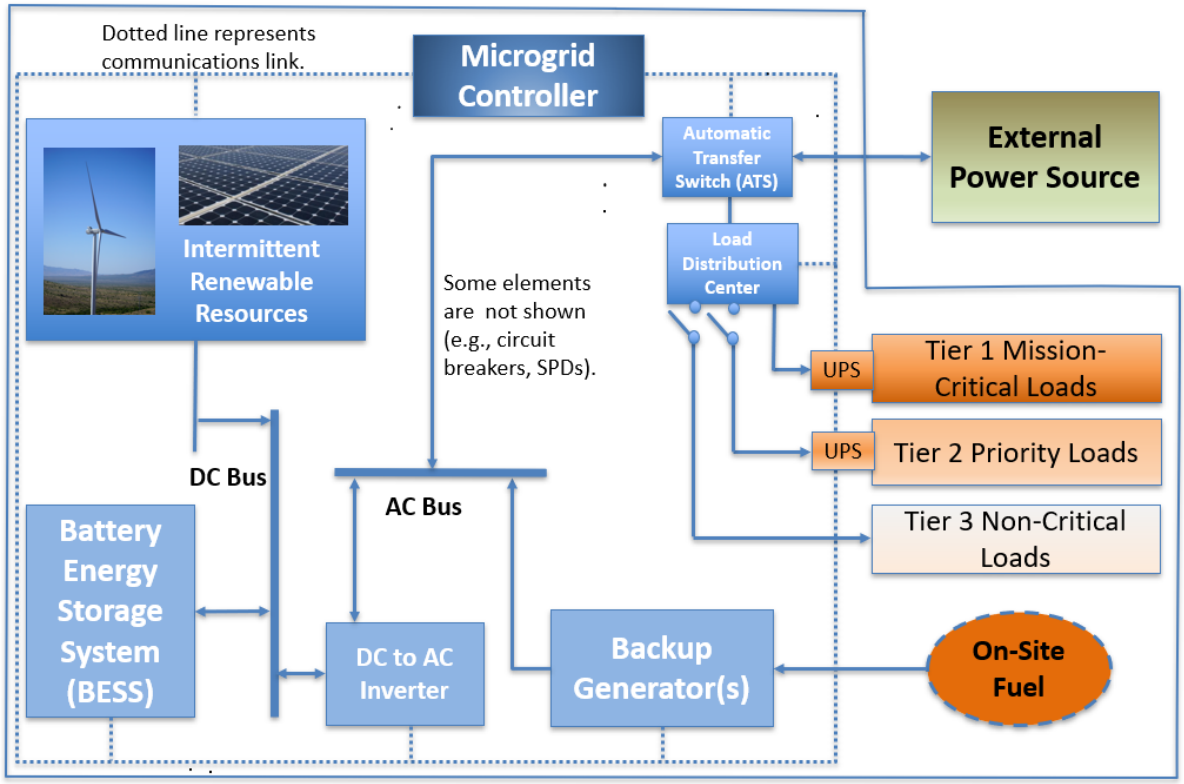

Figure 10. Conceptual microgrid architecture consists of a REHS and load segmentation[114]

In the Figure 10 above, the BESS includes the charge controller. Since the BESS' response is not fast enough to provide uninterruptible power to sensitive equipment (e.g., servers), a local UPS is provided where needed. The loads are defined as the following:

- Tier 1 Mission-Critical: The most critical loads within the microgrid with at least Level 2 resilience required.
- Tier 2 Priority: Loads that should be powered if doing so does not threaten the ability to provide power to Tier 1 Mission-Critical loads.
- Tier 3 Non-Critical: Level 0 or Level 1 resilience loads that are only maintained when there is either grid power or there is sufficient backup power and fuel to support these Tier 3 loads without threatening Tier 1 and Tier 2 resilience.

6.3. Microgrid Benefits and Issues

To improve power resiliency, Level 3 and Level 4 resilience sites are strongly encouraged to implement an island-mode capable microgrid particularly if procuring significant new backup power equipment. Level 2 resilience sites and Level 1 sites on campus-type environments with multiple facilities should also consider microgrids in their plans. A reduced total cost of ownership (TCO) can be an added reason in many situations to implement a microgrid although upfront costs along with the associated complexity are two primary reasons that microgrids have still not been implemented even in situations where there are two or more generation sources onsite.

The benefits and issues are discussed below, but the specific outcomes are highly dependent upon the microgrid implementation. For instance, if it is desired to sell electricity to the utility, the *Smart microgrid system enables grid augmentation* design in the previous section needs to be implemented where the microgrid is fully synchronized to the electric grid. This may be desirable because either the utility pricing varies significantly by the time of day or the site has excess electricity available, which may occur with renewables. On the other hand, this adds cost and complexity. Implementing the *Basic backup power system* shown above is simpler, allows the site to go into island mode, but that setup won't enable the site to sell excess electricity to the utility.

Microgrid Benefits

In this subsection, the critical infrastructure site benefits of a microgrid are broken down into the capabilities offered by a microgrid and the advantages of those capabilities, which typically include improved resiliency. Given the dependency of the outcome on the specific implementation, the *Potential Microgrid Benefits Versus Traditional Power Backup Capabilities* table assumes that the necessary microgrid control components are implemented. External benefits are also noted when the added capabilities increase the resiliency of the grid.

Table 18. Potential Microgrid Benefits Versus Traditional Power Backup Capabilities

Capability	Advantages	Specific Benefits (dependent upon specific implementation)
Distributed Energy Resources	Per the microgrid definition, there must be more than one energy resource, and these must be distributed.	
	Improved Resiliency and Lower TCO	• **More Redundancy** – Typically leads to at least some power generation redundancy for the most critical resources. • **Fewer Generators** – Power generation resources can be shared between facilities potentially reducing the number of generators required for N+1 redundancy. • **Reduced Maintenance Costs** – With a centralized fuel storage system, there are fewer storage containers where maintenance must be performed on the fuel or other components. Generator efficiency can also be improved reducing potential maintenance issues. • **Increased Reliability and Reduced Fuel Usage** – Can better match the generation resources with the load both to improve generator efficiency and reduce maintenance. This will increase reliability and reduce fuel usage as discussed in *Table 11* under *Diesel and Gas Generator Overview.*
Load Shedding	Enables the most critical load(s) to be separated from less critical loads since the loads are interconnected under a single control solution.	
	Improved Resiliency and Lower TCO	• **Improved Resiliency to Long-Term Power Outages** – Pooling resources can ensure that fuel and generation capacity is diverted to the most critical loads. • **Increased Reliability and Reduced Fuel Usage** – Can switch off unneeded loads to reduce generation resources and fuel usage and thereby reduce fuel usage and improve generator resiliency.
Fuel Type Diversification	Can more often justify adding multiple types of generation resources with a microgrid since it often brings an economy of scale and more total generation power.	

Capability	Advantages	Specific Benefits (dependent upon specific implementation)
	Improved Resiliency and Lower TCO	• **Greater Fuel Supply Diversity** – There is more opportunity to use natural gas/propane or other generation resources (e.g., solar) and better diversify the supply chain. • **Usage of Renewables** – Can best take advantage of renewables during a power outage.
Capability of Using Generation Systems During Non-Emergencies	May be able to procure better non-emergency generation resources given the increased usage although generators providing the below services will need to be permitted to run during non-emergencies (see *Table 11. ISO 8528 Generator Ratings*)	
	Improved Resiliency and Lower TCO	• **Reduced Electricity Costs** – Generators that are allowed to be run during normal grid operation can produce electricity at any time to save money. The backup generation system is no longer just an insurance policy. • **Improved Resiliency** – Using a generator than can run during normal operations can improve resiliency since generators that are regularly run under load tend to be more reliable than generators that only operate when being tested. • **Reduced Maintenance Costs** – Eliminates most diesel fuel maintenance activities by using the fuel before long-term storage maintenance procedures should be followed per the *Diesel Fuel Maintenance* subsection. • **Assured Testing** – Helps ensure frequent testing of the generator system in an operational environment to help verify that it will operate properly when needed.
Savings or Revenue via Demand Response and Related Programs	Using non-emergency power generation, take advantage of utility pricing programs to reduce the power system's TCO (some of the below are only applicable to a net-export capable microgrid).	
	Lower TCO and External	• **Selling Electricity to A Utility –** With a microgrid leveraging the design shown in "*Figure 9. Smart microgrid system enables grid augmentation*", electricity could be sold into the grid when the cost to produce or store and sell the electricity is less than the price being paid per kWh. • **Utilize Demand Reduction Incentives** – These include participating in a demand-response program and peak-shaving, which can help stabilize the grid and offer improved resiliency through distributed energy resources (DERs). • **Incentives** – Financial incentives may also be available from the state, locality, or utility to build a microgrid to increase power resiliency (incentives are rapidly evolving so check the federal, state, and local programs). • **Exploit Advanced Ancillary Services**—With a smart microgrid, energy storage devices can be used to participate in the ancillary services markets that require near real-time operation.

There are numerous examples of the success of microgrids during natural and manmade disasters. For instance, during Hurricane Sandy, the NYU, and Co-Op City microgrid operations were very reliable. Perhaps better known are the numerous examples of microgrids that helped many businesses and people during the "California Public Safety Power Shutoff Due to High Winds" incident.

Microgrid Issues

The potential issues with implementing a microgrid include the following:

- **Need Multiple Energy Resources** – If a facility only needs Level 1 resilience and there are no plans or needs for a renewable solution, then one generator may suffice and a microgrid would not be needed.
- **Upfront costs** – The upfront investment can range substantially depending upon the size and the complexity of the project. Simple microgrids are typically very affordable and large campuses with a complex microgrid design may require a significant budget. Energy-as-a-Service (EaaS) can mitigate the upfront costs whereby customers pay for an energy service without having to make any upfront capital investment.
- **Complexity** – The complexity can range from two generation sources to many generation sources connected to a myriad of loads in multiple facilities. In addition to the technical complexity, if there is not a single facilities manager or engineer (or equivalent) overseeing the resilient power plans of all the facilities involved, it can be difficult to reach agreement between multiple facility managers/engineers.
- **Legacy Architectures** – Microgrids are still relatively new for most owners/operators requiring them to spend time to understand how they might deploy a microgrid and find funding to change the site's existing architecture.
- **Impact on The Grid** – Net export capable microgrids can help stabilize the grid as discussed under *Microgrid Benefits* above. However, they can also have a negative impact on the grid if many microgrids and small independent power systems all have the same vulnerability or have rapid power swings in either transmitting electricity into the grid or needing electricity from the grid at the same time. These rapid power swings are particularly likely if there are a lot of sites using the same type of renewable energy source. They can also increase the cyberattack vectors.

Despite the above challenges, sites with two or more generation sources should consider deploying an island-mode capable microgrid, particularly if a site needs Level 3 or Level 4 resilience or the site is updating its backup power design. More specifically, all Level 4 sites should strongly consider deploying an island-mode capable microgrid with resiliency built-in versus improving resiliency later.

Alternating Current (AC) versus Direct Current (DC)

Traditionally, most microgrids use an AC-based microgrid but more microgrids are being built with either a DC-based system or a hybrid AC/DC system. The primary growth drivers of DC-based and hybrid microgrids are that most renewables and BESSes are native DC energy sources and there has been a rapid increase in DC loads ranging from electronic devices to rapid charge stations for electric vehicles. For the system to be considered hybrid, both AC and DC energy sources and loads need to be part of the system.

In the above *Figure 10. Conceptual microgrid architecture,* although the renewables are connected to the battery storage via a DC bus, there are no DC loads, so the system is considered AC-based. AC-based microgrids have the following advantages over DC-based microgrids:

- **Interoperability, Lower Initial Cost, and Reduced Complexity at Most Sites** – Because most equipment is designed to be used in an AC-based system and most sites already

are built around an AC system, AC-based microgrids tend to cost less upfront and be simpler than DC-based systems although DC-based systems are becoming less expensive. For instance, generators typically output AC requiring an inverter to convert the AC to DC in a DC-based system.

- Grid Interconnection – The microgrid must be able to interconnect with and follow the grid's AC-based connection rules and regulations. This is simpler and cheaper if the microgrid is AC-based than if it is DC-based.

Assuming that there are significant DC energy sources beyond BESSes, DC microgrids may have the following advantages over AC microgrids depending upon the architecture:

- Improved Resiliency – With the addition of DC-based Distributed Energy Resources (DERs) and significant DC loads, a DC-based microgrid eliminates the need for DC to AC and AC to DC inverters within the microgrid. This eliminates a major vulnerability issue. Conducted HEMP is also not an issue if the lines are interlaced.
- Better Energy Performance – When a DC DER is providing power to a DC load, the elimination of the inverters discussed in the previous bullet improves energy efficiency since an inverter can reduce the available power by up to 5% (with an efficient modern inverter) with further power loss if converting back from AC to DC.
- Simplified Power Sharing within Microgrids – Since frequency synchronization is not an issue, power from DC-based systems may be shared more easily and resiliently with other sites or facilities than with AC-based systems.

Overall, AC-based microgrids dominate the 2021 market primarily because of the importance of interoperability and since most equipment is designed for AC systems as mentioned above. AC-based microgrids include implementations where a DC-based energy source (e.g., solar) is coupled to a BESS via a DC bus but is then converted to AC before being transmitted to the loads as shown in *Figure 10. Conceptual microgrid architecture*. It is therefore useful to distinguish between microgrids deploying DC-coupled power from solar panels to a BESS from that of DC-coupled systems supplying DC-distribution networks.

DC-based microgrids tend to work best when there is substantial power coming from DC-based DERs going to DC loads, such as might occur at a data center or multiple electric-vehicle charging stations with a substantial nearby renewable power generation source. When there is a mixture of significant DC-based and AC-based DERs and loads, a hybrid AC/DC microgrid might be the best solution, particularly with a new buildout where the DC loads can be easily separated from the AC loads. An energy router can manage the electricity across both the AC and DC buses to maximize the energy efficiency.

7. ENERGY STORAGE

Target Audience:

- Power Management/Engineering: *Read all*
- Continuity & Planning: *Browse/Read*

Traditionally, the energy storage market has consisted of using a network-based or a device-level uninterruptible power supply (UPS) to enable computers and other equipment requiring electricity to continue to operate during short power outages. The primary benefits of the UPS are the following:

- Protect equipment against brief power outages and voltage fluctuations.
- Enable continuous operations until primary power returns or a backup generator is operational.
- Automatically and gracefully shut down equipment during long power outages and provide users with enough time to save their work.
- Monitor the status of the power supply and provide alarms on certain error conditions.

More recently, the use of battery energy storage systems (BESSes) with slower response times are increasingly being used to store energy for later use within a microgrid to improve resiliency and to reduce electricity costs or to sell electricity to a utility company typically during peak demand. As discussed below in the *Energy Storage* section below and as shown previously in *Figure 10. Conceptual microgrid architecture*, a BESS together with a significant onsite renewable energy supply can meaningfully improve resiliency particularly if the fuel storage capacity is the same under both instances.

The above concepts together with an overview of the market, technologies and recommendations are discussed below in the following sections:

- *Section 7.1 Energy Storage*
- *Section 7.2 Centralized Versus Local Energy Storage (LES)*
- *Section 7.3 UPS Guidance*
- *Section 7.4 Battery Energy Storage Systems (BESSes)*

Note that fuel cells are sometimes considered an energy generation source but are discussed in this chapter since they are more often used to store energy.

7.1. Energy Storage System (ESS)

The ESS market consists primarily of the UPS and the BESS. UPSes have historically been most of the ESS market but the BESS market is growing much more quickly and will likely be big as the UPS market within the next several years.[115] Energy storage is expected to help provide the following for critical infrastructure sites:

- **Uninterrupted Power** – Batteries can provide a near-instant backup system, which can help ensure that there is no down time due to a power failure or voltage fluctuation. Most standard battery supplies have a hold-up time of 20 ms, but a UPS can generally transfer power between 0 ms and 12 ms.[116] Per the *ELECTROMAGNETIC (EM)*

SECURITY chapter, it is recommended that an online (preferred) or a high-quality interactive UPS be considered to best protect against voltage fluctuations, including EM threats/hazards.

- **Reduced Backup Generation Costs Using A BESS** – A BESS is most often used to store renewable power to save electricity costs during peak demand pricing. As discussed in Section 6 *POWER TRANSFER SYSTEMS AND MICROGRIDS*, a BESS can reduce peak demand or transmit electricity into the grid when the price is high. A FERC ruling in February 2018 requires that the minimum size for the ancillary services bidding does not exceed 100 kW, which can help a critical infrastructure site selling power from a BESS to a utility. See NERC's 2021 *Reliability Guideline Performance, Modeling, and Simulations of BPS-Connected Battery Energy Storage Systems and Hybrid Power Plants*[117] for grid interconnection details. In some geographical areas, a BESS is also eligible for government incentives typically when combined with a renewable system.
- **Improved Resiliency** – Both a UPS and a BESS enable electricity to continue to be provided when grid power is lost. To improve resiliency, a BESS should typically be used in combination with a generator since the number of kWh stored by a BESS can usually only provide hours of power to a site and solar/wind power are intermittent sources of energy. It is often combined with a UPS because the deployed BESS is not fast enough for sensitive electronic equipment. A BESS can provide power during peak demand reducing the size of the generator needed or eliminating the need for a redundant generator and making the one that is used more efficient overall as discussed in *Section 8.5 Intermittent Renewable Energy Hybrid System (REHS)* Guidance.

A properly sized renewable system that includes a BESS combined with a generator can help enable Level 2 or higher resiliency.

The benefit of a BESS is often the greatest where there is a high use of non-dispatchable electricity sources (a non-dispatchable generation source cannot vary output to follow demand, e.g., solar, wind). For example, California, which has substantial solar production swings that have become difficult to manage, has adopted use rates for residential customers and most states have adopted peak demand charges for industry. This flexible pricing enables customers to significantly reduce their electricity costs by using a BESS during peak demand or to sell electricity into the grid during peak pricing.

High peak demand electricity pricing is typically key to deploying a BESS from a business case perspective and can help justify significant additional resiliency at little or no extra cost. Indeed, ResearchAndMarkets states that "the reduction in the energy bills for the customers relying on the utility grid for electricity is expected to drive the growth of the [on-grid BESS] segment."[118] This is discussed further in *Chapter 8 RENEWABLE ENERGY.*

7.2. Centralized Versus Local Energy Storage (LES)

To ensure continuous power, a UPS or BESS/UPS combination solution should be considered and used in most new implementations as discussed below:

The battery backup architecture should be based upon short-term and long-term resiliency considerations in addition to cost.

- **Local Energy Storage (LES)** – Generally consists of low power UPSes with 2-10 electrical outlets that are

used to ensure continuous power to sensitive electronics and equipment for short disruptions in power.

- **Centralized UPS system** – A networked UPS system that provides backup power to the facility particularly to sensitive devices and equipment.
- **BESS with LES** – Use a BESS for most equipment where very short outages are acceptable. Use a UPS when very short power disruptions cannot be tolerated, such as with sensitive electronics.

Each of the above are discussed below with the various types of UPS devices discussed in the next section. The optimal solution is dependent upon the existing energy delivery architecture, the facility requirements, and the reliability of the grid. If a piece or set of equipment is particularly critical and must operate with no downtime, then either that equipment or the redundant equipment should probably be on a different UPS. Non battery storage solutions are also possible but running a spare generator to provide continuous power at a critical site is rare for new deployments and is generally not recommended even for very large projects over 100 MWh.

Local Energy Storage (LES)

For small new deployments such as in a leased small office building, the **LES solution** is typically preferred. This enables uninterrupted power to be provided to the required equipment using inexpensive, mass-produced energy storage usually without any significant labor involved or changes to the building. A UPS can backup sensitive equipment while lights with batteries can ensure that lighting is not lost (smoke alarms, etc. can also be backed up this way).

However, even for larger deployments, LES may be the preferred solution when there is no need for a BESS that might be used with renewables or to provide significant power to non-sensitive equipment such as elevators. Indeed, in 2015 Microsoft found the following LES advantages with one of its data centers versus traditional large, centralized energy storage systems[119]:

- **Significantly lower cost** – Microsoft estimated local energy storage is "up to a 5x cost reduction over traditional facility UPS (using lead-acid batteries), achieved by extreme simplification of the datacenter power delivery solution and moving the energy storage function to a high-volume commodity supply chain." Although this was for a new facility and included savings such as reduced floor space[120], which will likely be less than for an existing facility, the savings could still be substantial.
- **Better energy efficiency –** Microsoft achieved a 15% improvement in its data center power usage efficiency. Per Microsoft, "moving the energy storage local to the server eliminates up to 9 percent of the losses associated [with] conventional UPS systems. The LES topology and lithium-ion batteries require only 2 percent charge overhead versus conventional UPS systems (which require up to 8 percent charge overhead and 1 percent operating overhead)." Perhaps more importantly though, if the battery system supports far less electrical items (e.g., laptops, refrigerators), that could further substantially improve efficiency.
- **Improved robustness** – If a large battery backup system fails, the entire data site will lose power. With LES, if an energy storage unit fails, only the piece of equipment or the rack that it is being backing up will fail and these are generally hot swappable within Microsoft's data centers. Since each piece of equipment and each rack within a data center has a backup, the overall system performance will be minimally impacted. Note

that this improved robustness requires that either the facility energy manager or the users be diligent about using the necessary LES and occasionally checking the systems.

Centralized UPS

A **centralized UPS** system is the traditional energy storage system for most larger facilities. It enables the Energy Manager to have complete control although today a local UPS can be networked. If a centralized energy storage system is used, it needs to be robust enough so that no one failure brings down the backup power to any of the mission critical services that are provided. There are three possible solutions to implementing a centralized backup system:

- **Backup everything** – A centralized battery backup power system can provide power to everything inside a facility (except perhaps to a few high-power items) so that no user input or knowledge of the backup system is required. This is logically the simplest solution and is the easiest to implement in an existing facility but is also requires a larger UPS, generation system and fuel supply to provide backup power to all the equipment.
- **Duplicate branch circuits** – To save money on energy storage, the energy manager can provide a different color electrical outlet (e.g., red) for equipment that need 24/7 continuous power. This requires duplicating both the number of power lines and outlets and educating the user since there will be minimal savings if many staff use always-on power for almost everything.
- **Run custom branch circuits** – Routing power from a centralized energy storage system to just the critical components can be complicated, so this method is typically only used when all the critical equipment and workspaces are in an isolated area.

Battery Energy Storage System (BESS) with Local Energy Storage (LES)

From a cost and robustness perspective, a combination of localized and centralized power backup systems may be best. A combined centralized BESS together with LES for many components can be the best solution in two situations:

- **Renewables are used** – The renewables can charge the BESS to reduce peak electricity costs and to provide increased long-term power outage resiliency.
- **BESS backup of high-power systems** – A high quality and mass-produced LES UPS can provide backup power without harmful voltage or EMP transients to any sensitive equipment. A centralized BESS can then be deployed for high-power systems that can tolerate voltage transients or brief power outages. The BESS can also support smaller systems where the BESS can meet the requirements and provide backup power more inexpensively than a LES considering any manpower savings and expected resiliency benefits or costs.

This solution is similar to the LES system except that a BESS is used to backup high-power systems that do not require continuous power but cannot wait for a backup generator to come online, such as an elevator. If the elevator (except perhaps for the lights) briefly loses power and quickly regains power (typically in less than a second), no damage will occur. A centralized UPS could also be used but those are generally more expensive than a BESS which may take hundreds of ms before providing backup power. A small amount of the strategically placed emergency lighting can be handled via battery backup to ensure that it's not totally dark even for hundreds of ms and that there is redundant backup lighting power.

7.3. UPS Guidance

The three most common UPS design approaches are as follows[121] (general critical infrastructure guidance is provided in parentheses):

- **Standby (not recommended)** – A low cost, high efficiency common design for desktop and laptop computers. Unfortunately, this type of UPS has a low amount of power filtering and the inverter only starts when power is lost and is only recommended to be used with non-critical equipment.
- **Line interactive (recommended for small loads)** – This is the most common design used for a small UPS with small businesses, Web, and departmental servers. In this design, the inverter is always on and connected to the output, providing additional filtering and reduced switching transients when compared with the standby UPS topology. Its high reliability, filtering capabilities, high efficiency, small size, and moderately low cost make this the dominant type of UPS in the 0.5-5 kVA power range. Therefore, a high-quality line interactive UPS is recommended for critical equipment.
- **Double conversion online (recommended)** – "In 2019, online systems accounted for over 65% of the global UPS market share."[122] It is the most common design for a large UPS above 10 kVA. The battery is always online providing power so there is zero transfer time when grid power is lost. The grid or onsite generation source recharges the battery. It has nearly ideal output electrical performance and is therefore recommended for all critical infrastructures. However, its constant use does increase power usage and decrease reliability of the components. The power draw can also be non-linear, which can cause problems on the input side.

To choose the best UPS, there are four critical factors:

- **Equipment protection** – As discussed above, the double conversion online UPS provides the best protection against voltage spikes, but a high-quality interactive UPS is also good. Equipment with sensitive electronics is particularly vulnerable, including modern switched-mode power supplies (SMPSes).
- **Transfer time** – There is no transfer time with a double conversion online UPS. A high-quality line interactive unit will take 2-4 ms to transfer power to the battery source. This meets the specifications for all common modern equipment but may not protect against some transients (see *Chapter 4 ELECTROMAGNETIC (EM) SECURITY*) depending upon the UPS' filtering capabilities.
- **Upfront cost** – The upfront cost is dependent upon the number of kVA needed as well as the design. The battery life of the UPS should be long enough for backup power sources to come online.
- **Reliability and power drain** – An interactive or standby UPS are better in this category than an online double conversion UPS.

7.4. Battery Energy Storage Systems (BESSes)

This section covers the following topics:

- *Lithium-ion Versus Lead Acid Batteries*
- Lithium Iron Phosphate (LFP), Solid-State Lithium Metal, and Other Battery Technologies

Lithium-ion Versus Lead Acid Batteries

The primary advantages and disadvantages of a lithium-ion based UPS or BESS versus a lead acid one is covered below in Table 19 including the solution typically best for each evaluation criteria:

Table 19. Comparison of Lithium-ion versus Lead Acid Batteries

Evaluation Criteria	Best Solution	Rationale for Best Solution
Upfront Costs	Lead Acid	• Lead acid batteries cost significantly less than lithium-ion batteries. • The price of lithium-ion batteries is expected to decrease in the future versus lead acid (e.g., DOE expects lithium-ion batteries to be similar in cost on average in 2025 in a BESS).[123] • Note: There are several factors impacting the cost.
Lifetime Expectancy	Lithium-ion	• Estimates vary from lithium-ion lasting 2x-3x times longer than lead acid batteries[124] to four times as long with daily use.[125]
Charging/Discharging	Lithium-ion	• A lithium-ion battery can hold a charge approximately four times longer than a lead acid battery[126] and charge at least four times quicker.
Footprint and Physical Location	Lithium-ion	• Lithium-ion batteries are about 70% smaller and 60% lighter than lead acid.[127] • Lithium-ion can often be deployed in warmer temperatures than lead acid without degradation, which can reduce cooling costs by as much as 70%.[128]

From a safety perspective, both battery types require extra safety considerations when used in volume (e.g., in a centralized energy storage system). Lithium-ion requires temperature control and battery monitoring to prevent fires.[129] Lead acid batteries are hazardous and need proper venting. For environmental purposes, both should be recycled although it is legal to dispose of lithium-ion batteries in landfills in moderation. It is generally recommended that most BESSes, which are typically deployed with renewables, use lithium-ion batteries.

For a **UPS,** a lead acid battery is generally the preferred solution to provide uninterruptible power to critical equipment given its upfront cost advantages over a lithium-ion battery and since the charging/discharging cycle is a minimal issue for a UPS. Lead acid use in the stationary energy storage market is expected to grow by almost 9% CAGR from 2020 to 2024.[130]

However, a **lithium-ion UPS** is now preferred in some applications and is particularly advantageous in the following cases:

- New installations or major updates where a reduced or less temperature regulated footprint can reduce costs.
- Environments where it is difficult or time consuming to swap out batteries.

In addition to the above, some vendors state that the TCO of a lithium-ion UPS is already significantly lower than for a lead acid UPS even in general operating environments[131] although

the TCO will vary depending upon both the specific usage and market conditions. As the cost per storage watt continues to decrease and the number of lithium-ion based product offerings increases, it is expected **that the lithium-ion based UPS market share will continue to increase.**

Lithium Iron Phosphate (LFP), Solid-State Lithium Metal, and Other Battery Technologies

Lithium Iron Phosphate (LFP) is a newer type of battery with the following technical advantages over traditional lithium-ion batteries:

- Can be less expensive since it does not use cobalt or nickel,
- Is stable/safer at high temperatures,
- Can be charged many more times to give it a lifetime up to 20 years.[132]

Because of the above advantages, Tesla noted in its third-quarter 2021 earnings report that, despite the hit to range due to the lower energy density, its standard range vehicles will shift to an LFP battery chemistry. In January 2022 during the fourth-quarter 2021 conference call, Elon Musk said that he expects Tesla to transition all of its stationary ESS products to LFP battery chemistry.

LFP's primary disadvantages are that (1) the specific energy density is lower than standard lithium-ion batteries (or Lithium Nickel Manganese Cobalt) so it is not targeted toward portable devices such as mobile phones, and (2) the upfront costs are higher as of late 2021 than for standard lithium-ion batteries although the lifetime costs may be lower when needing an extended life BESS.

A **solid-state lithium metal** battery uses both solid electrodes and solid electrolytes. A lot of publicity has been given to this type of battery due to its improved energy density and safety characteristics versus lithium-ion. These solid-state lithium metal batteries have the following advantages over lithium-ion batteries:

- Increased energy density
- Improved safety (the design of the solid-state batteries makes it much more difficult to catch on fire)
- Longer life expectancy
- Faster charge times.

In addition to the above, solid-state battery costs may become the least expensive fixed energy storage battery technology longer term primarily due to the much higher energy density versus lithium-ion batteries[133], but also due to their safer design and increased life expectancy. Unfortunately, there are manufacturing issues that remain before these batteries are mass produced for electric vehicles and for fixed energy storage.

Another potential BESS technology uses **vanadium** instead of lithium. The primary advantage of vanadium-based batteries is that these can last over 20 years with no degradation from heavy cycling giving users a potential superior levelized cost of storage over lithium when used over a long period of time. The batteries are bulky but can be packed closely together since they have no risk of thermal runaway. It is recommended that critical infrastructure consider using vanadium for energy storage when the batteries are used very often (e.g., daily) since that

application takes advantage of the technology's strengths. The market is very small as of the end of 2020 but is predicted to grow to $4.7 B by 2028 per the vanadium battery company Invinity Energy Systems.[134]

Lastly, as electric vehicles (EVs) including small and large trucks become more prolific with improved energy storage and as more of these vehicles include AC outlets to power equipment, these EVs can be used to power equipment and augment existing energy storage. Indeed, this is advertised as a major feature of the 2022 Ford F-150 Lightning, which offers 19.2 kW of power.

7.5. Other Energy Storage System (ESS) Technologies

There are also numerous non-battery ESS technologies being researched and deployed including the below:

- **Pumped-Storage Hydropower** – This is commonly used by some utilities where there are two bodies of water at different elevations. Water is pumped from a lower-level water source to a higher-level storage area and then the system uses the height differential to generate electricity as shown in Figure 11. This technology accounts for 95% of the grid energy storage[135] and can be EM protected.

  Excluding utilities, Pumped-Storage Hydropower is most applicable to larger campuses. Some campuses may deploy renewable energy generation that can intermittently produce significant excess power, but the power is much more valuable financially or from a resiliency perspective if it is stored and used during peak demand periods or when the power is out. In these cases, the excess generated power could be used to pump water to an elevated reservoir for storage until additional power is required at which time the water can flow downward through a turbine to generate electricity.

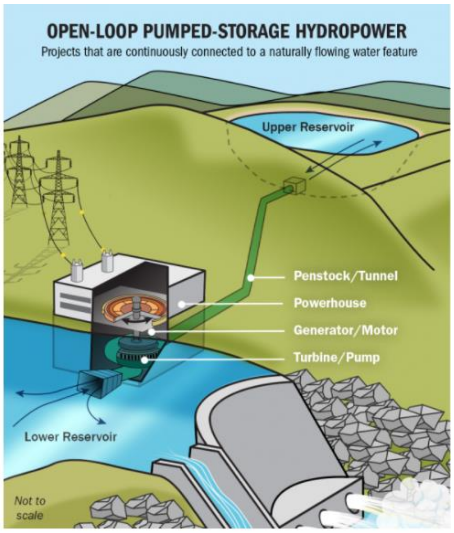

Figure 11. Open-loop Pumped-Storage Hydropower (courtesy of DOE)

- **Mechanical ESS (e.g., Flywheels)** – Uses kinetic (e.g., rotating) or gravitational energy that can be called upon to produce electric energy.
- **Compressed Air ESS** – Converts excess power to compressed air energy, which can be stored efficiently and later used to produce electricity. Typically, this is stored in a large area, such as a cavern, mostly limiting its use to utilities.
- **Ultracapacitors or Supercapacitors** – This is an electrical energy storage solution and enables much faster charging and discharging than battery solutions with long lifetimes and high efficiency. A sample usage is starting a hybrid engine where the engine needs a lot of cranking amps and might often be started and stopped but high energy density is not required.

At this point, the above are niche solutions within the non-utility enterprise fixed energy storage market but some of the above technologies could be useful under certain circumstances (fuel

cells using hydrogen can be considered an energy storage technology but that topic is covered in *Section 8.3*).

8. RENEWABLE ENERGY

Target Audience: Power Management/Engineering, Continuity & Planning: Browse, read if considering.

As shown in Figure 12[136], renewables are an important part of the country's electricity generation with a 20% market share in 2020 per Electricity in the U.S. – U.S. Energy Information Administration (EIA).[137] Further, the EIA expects renewables to double its market share to 42% by 2050 with solar surpassing wind power by 2040.[138] Renewables are discussed in this document since they can help improve power resiliency partially because the renewable fuel supply is not dependent upon pipelines nor the transportation system. Renewables can also reduce facility energy demand and operating costs during normal operating conditions.

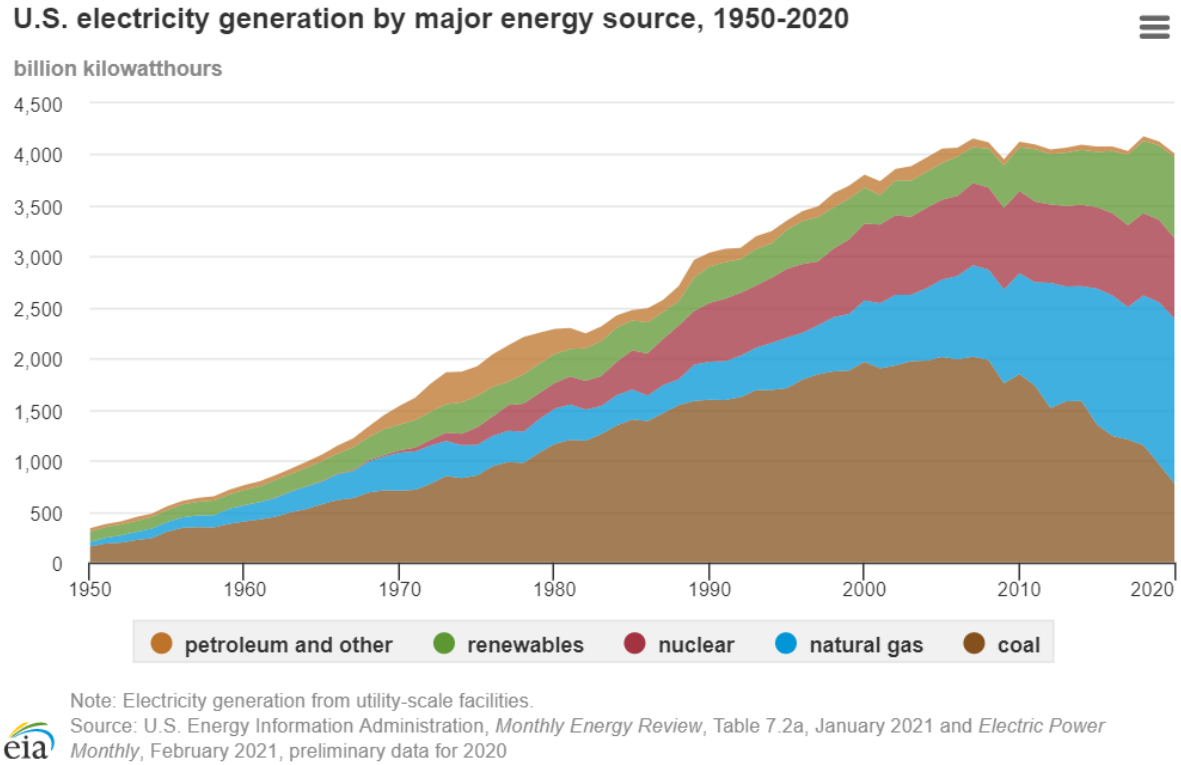

Figure 12. Natural gas and renewables have increased significantly since 2000

The renewable market consists of many different technologies of which the most important to a resilient power strategy are discussed in the following sections:

- *Section 8.1 Renewable Energy Overview*
- *Section 8.2 Solar Power*
- *Section 8.3 Fuel Cells*
- *Section 8.4 Wind Power and Other Renewable Energy Sources*
- *Section 8.5 Intermittent Renewable Energy Hybrid System (REHS) Guidance*
- *Section 8.6 Renewable Energy Hybrid System (REHS) Sample Use Cases*

Note that this chapter uses the term renewable energy instead of clean energy both because "clean energy" is a matter of degree and nuclear energy, which is one of the largest and cleanest forms of energy, is covered separately in *Chapter 9 NUCLEAR SMALL MODULAR REACTORS (SMRs).* From a clean energy and cost perspective, improved energy efficiency should also be considered.

8.1. Renewable Energy Overview

Per the EIA, the largest renewable energy source is from wind with a 7% market share in 2019 as shown in Figure 13.[139] Wind power recently passed hydropower as the largest renewable energy source in the U.S. The primary supply of wind power comes from large wind turbines, which are more cost effective per generated kWh than smaller turbines. These turbines are typically located in wind farms in unpopulated and windy areas such as in West Texas where the noise and potentially negative aesthetic of the wind turbines is not a major issue. Because of the constraints in placing these wind turbines in urban areas or near buildings, wind turbines tend to be partially used for backup power in more niche applications and are therefore covered in *Section 8.4 Wind Power and Other Renewable Energy Sources*.

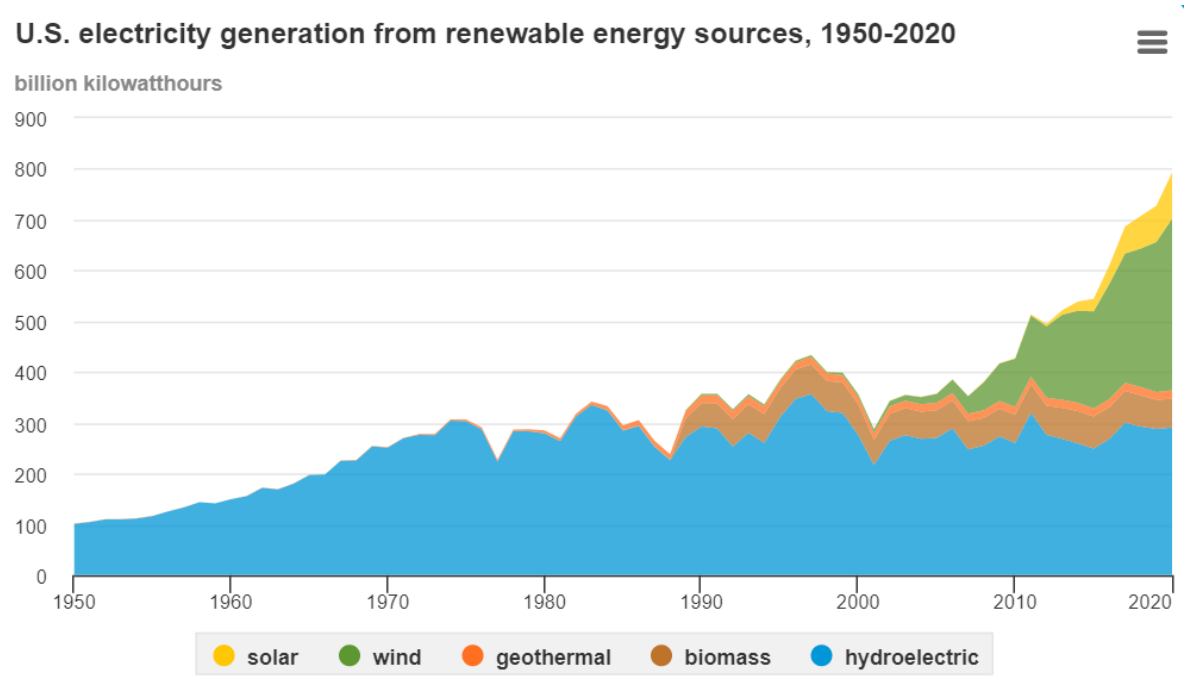

Figure 13. Wind and solar power have substantially increased since the early 2000s

Hydropower is the next largest deployed renewable energy technology after wind. It had a 6.6% share of the utility electricity market and 38% of the utility-scale renewable electricity market in 2019, numbers that have decreased over time.[140] Hydropower can be an excellent source of resilient power. It has been mostly controlled by utility and government entities, but new technologies and regulations are expanding its reach as discussed in *Section 8.4 Wind Power and Other Renewable Energy Sources*.

Solar represented about 2% of annual electricity generation in 2019 per the EIA. Partially because solar often has the best onsite renewable energy potential, costs have substantially decreased, and there are significant subsidies, its market share is rapidly growing accounting for 40% of all new 2019 electric generating capacity in the U.S. This is its highest solar power market share gain in absolute terms ever with 13.3 GW installed and more than any other source of electricity.[141] Most of the solar market is photovoltaic (PV), which is covered below in *Section 8.2 Solar Power*. Solar PV panels have the significant advantage of being able to be installed on rooftops and are generally permitted by zoning laws. On the other hand, solar thermal or Concentrating Solar Power (CSP) has less than 10% of the solar market and is typically implemented as a utility-scale solution or possibly on large campuses and is therefore not covered until *Section 8.4 Wind Power and Other Renewable Energy Sources*.

Fuel cells can be considered an energy storage technology, but because they require fuel and may need minutes to startup, they are included in this chapter under *Section 8.3 Fuel Cells*. The fuel cell market is not nearly as large as the wind or solar markets, but the fuel cell market is growing quickly and can be used for backup power or for 24/7 power generation.

Role of Renewables in Resilient Power

Renewables use an enduring energy source that can augment power generation to reduce or eliminate fuel needs and provide at least intermittent power. Because of the intermittent nature of most renewables, they are generally used in combination with an energy storage system and a backup generation source to create a renewable energy hybrid system (REHS) that can provide power at any time.

Renewables, particularly when used in a REHS, can substantially improve power resilience, and prolong backup power.

However, there are some exceptions where renewables combined with a sufficient energy storage system are used as the primary souce of backup generation power typically for Level 1 resilience although this is based upon your risk management plan:

- In areas where the renewable energy source is extremely reliable (e.g., fuel cells, sunshine occurs almost everyday).
- When little power is required for the critical infrastructure and it is very expensive or unreliable to connect to the grid.
- In localities that either heavily subsidize both renewables and energy storage or where there are regulations requiring or strongly encouraging renewables together with high levels of energy storage.

If Level 2 resilience is needed, it is generally a best practice that each site or facility has more than one backup generation source. Also, it should be noted that even for Level 1 resilience, the cost of an energy storage system (ESS) to meet the backup power requirements (e.g., 3 days of continuous operation) can be expensive if supporting a significant load.

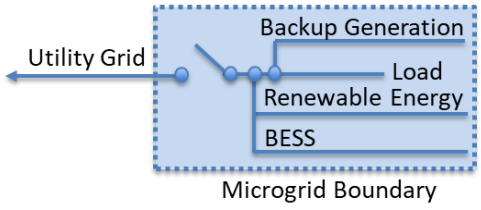

Figure 14. A REHS microgrid has multiple sources of onsite power

Given that most use cases do not meet the above situations, it is generally suggested that renewables be integrated into a REHS and connected to the grid as shown in *Figure 14*. Per the National

Renewable Energy Laboratory (NREL), a REHS can sustain longer outages for a given amount of diesel fuel by reducing the runtime (and, therefore, fuel consumption) of the diesel generator, thus increasing the energy resiliency of the site. A REHS can also extend the scale of backup power available by extending backup power to loads that otherwise would not be powered.

Because of the intermittent nature of sunshine and wind, renewables have traditionally been integrated into sites such that they supply 20% or less of the annual energy needs.[142] But with good energy management and load shedding, the backup power supplied by renewable energy could be substantially increased and it might also enable limited operations even if all the fuel is depleted during a long-term outage.

Renewables can often provide this improved resilient power at little or even no increase in the overall TCO (includes the complete lifecycle of a capital purchase) by reducing the critical infrastructure site's electricity costs, particularly if resiliency is added in the design phase. Furthermore, these REHS can be operated for economic gain when the grid is functional by offsetting bulk energy purchases, reducing peak demand charges, performing energy arbitrage, and providing ancillary services."[143] Advantages and issues of a REHS system are further discussed in the sections below, which also include a more detailed discussion of the potential costs and savings.

8.2. Solar Power

Solar power has widespread appeal due to its environmental friendliness, its low cost of operations (just needs maintenance and sunshine assuming that the operator owns the property), and federal, state, and local incentives. This section and the next one describes solar power's potential to improve resilient power and its overall business value.

To best rely upon the solar power system as a **primary** backup generation system, the solar power and the energy storage system need to reliably provide power to at least operate the critical infrastructure for the minimum specified time regardless of the weather, location, time of day, and season of the year. To supply backup power for days or weeks without external deliveries of fuel, it is typically more cost effective and resilient to use solar in a Renewable Energy Hybrid System (REHS) with the generator backing up the solar power system including the ESS.

Solar generally should be combined with a 24/7 generation source and an ESS into a REHS.

When solar power is incorporated into a REHS, it can:

- Extend the backup generator's fuel supplies during a power outage.
- Supply at least intermittent power if the fuel supplies are depleted.
- Provide an additional generation source in case the primary backup generation source malfunctions.
- Generate power during normal grid-tied operations, thus improving the economics of the REHS (although only an ESS needs to be added to the solar system in this case).

The above assumes that in addition to the solar system and the ESS, the system includes at least one other power generation source as shown in *Figure 10. Conceptual microgrid architecture* in *Section 6.2 Microgrid Definition and Purpose*. If necessary, it is recommended that load shedding occur to ensure that the most-critical loads can continue to operate. With commercial solar power generation costs predicted to continue to decrease, it is expected that

solar will be used by more and more enterprises even in areas with just a moderate amount of solar irradiance. This together with lower ESS prices will encourage more critical infrastructure enterprises to use a REHS for backup power.

Although solar power is very cost effective in many parts of the country, it does have the following issues, which can be partially or mostly mitigated when combined with a generator or another 24/7 generation source (i.e., it's part of a REHS):

- **Inconsistent/Intermittent Solar Power** – The amount of sunlight that arrives at the Earth's surface is inconsistent/intermittent or snow/ice can cover the panel. Therefore, to improve power resiliency, energy storage is required, and in most cases a 24/7 generation source is needed.
- **Large Surface Collection Area** – Per the EIA, "the amount of sunlight reaching a square foot of the Earth's surface is relatively small, so a large surface area is necessary to absorb or collect sufficient energy."[144] Another generation source can reduce the collection area required. This is further discussed in the subsection *Solar Photovoltaic (PV) Power* directly below.
- **Costs** – The total cost of ownership (TCO) can be high if deploying a solar system with a ESS as the only source for backup power since the ESS may need to store days or even weeks of energy to meet the power resiliency requirements, driving up capital costs. Further, if using a BESS, it won't be able to be fully utilized to reduce peak power costs if it needs to stay sufficiently charged in case grid power is lost. Although the upfront costs can still be high, the costs can be mitigated through third party financing or fixed-price contracts.
- **Damage –** Panels can be easily scratched, damaged, or broken from falling objects such as tree branches and hail.

Due to the above**, a REHS that includes a 24/7 generation source is recommended** in most cases to substantially improve resilient power and reduce costs.

The potential components and processes that are typically included in a REHS, which is shown earlier in *Figure 10. Conceptual microgrid architecture,* are the following:

- Solar Power Collection System
- Various power interconnection and control equipment
- Design, Installation, and Maintenance
- 24/7 Backup Generation System (e.g., diesel generator)
- Energy Storage System (ESS)

The first three bullets are discussed in the subsection directly below. The last two bullets above have been previously discussed. Specific use cases are discussed in Section 8.6 *Renewable Energy Hybrid System (REHS) Sample Use Cases*.

Solar Photovoltaic (PV) Power

Several years ago, solar panels were a large part of the overall cost of a solar installation, but solar panels now represent less than 15% of the total upfront cost. As these costs have decreased, it has become more cost effective to use more expensive but more efficient solar

panels particularly in areas with minimal space such as a rooftop where watts per square foot is very important.

The solar panels are joined into arrays either on the roof or in free standing structures (i.e., carports) typically using mounting racks. Combiner boxes add the output of several solar strings together in a larger solar system (not a small residential one) to reduce wiring costs and connect to an inverter or battery controller. These boxes can include features such as monitoring equipment, disconnect switches, and a remote rapid shutdown.

Although the cost of electricity is generally more important from a value perspective than the amount of sunshine in an area, the Global Horizontal Irradiance (GHI) can influence the economic viability of a solar project and the number of panels needed for a solar PV project. As shown in Figure 15, most parts of the country have a GHI number over 4 kWh/m^2/day with southern sunny areas having the highest GHI. The GHI is based upon the total amount of shortwave radiation received from the sun by a surface horizontal to the ground over a period of a year and is used to determine the output from solar PV systems. The specific potential is dependent upon the latitude, altitude, panel orientation and tilt, and local shading conditions.

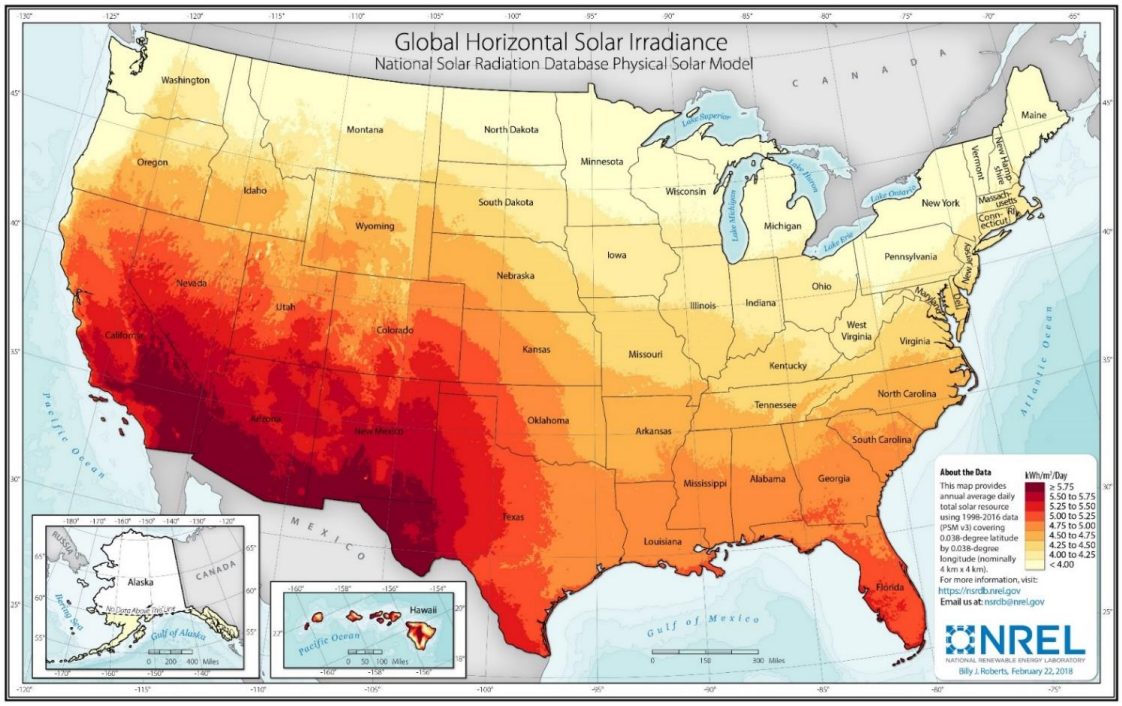

Figure 15. U.S. solar irradiance is strongest in the southwest

For optimal resiliency, both the power demand and supply throughout the year should be considered. Typically, most organizations will want to overbuild the solar collection system and use a smaller ESS to reduce the TCO, but this may not be an option in some areas of the country where there could be many days in a row with little or no sunshine and the ESS is needed for power resiliency. Physical space or utility interconnection policies could also limit the number of solar panels that can be installed.

When deciding whether to install solar panels, one of the first potential decisions is determining how much space should be set aside for the solar panels. Various space considerations include the following:

- **Roof Space** – How much space is available on the rooftop and is there a leasing fee to use that space? Although there is insufficient space for enough solar panels to fully supply the building with electricity on most high-rise building rooftops, there may be enough space on a low-rise building. Regardless, the system can extend the fuel supplies and might power the critical systems for at least for part of the day. A ballpark estimate of the rooftop space available can be made using Google Maps as defined in the article *How to Calculate a Building's Rooftop Area*.[145]
- **Ground Space** – What space might be made available for solar panels and what is the opportunity cost? Where do regulations permit solar panels to be installed? Is there added value to a ground-mounted system, such as one that provides protection to cars from sun and snow (e.g., a carport)?
- **Maintenance** – What are the maintenance costs of the target solar panel locations to fix something broken? What is the cost to remove snow or dirt from the solar panels when required? If the facility is being leased, will the owner pay for any of the installation and maintenance costs?

In addition to the above costs from the solar panels, mounting racks, installation, power inverters, and combiner boxes, there are also costs from circuit breakers and interconnections, power meter, smart charge controller, and battery system, which have been previously discussed including those in *Section 6.2 Microgrid Definition and Purpose*.

Solar Power Resiliency Best Practices

Although solar is inherently dependent upon sunshine, which is variable from day-to-day, there are many best practices that can be implemented to improve its resiliency including those shown in Table 20.

Table 20. Solar Power Resiliency Best Practices

Best Practice	Specific Suggestions
REHS Microgrid	• Implement a hardened microgrid as discussed in Sections 6.2 and 6.3, which has island-mode capabilities and enables the enterprise to sell excess electricity generation into the grid. • More specifically, a REHS microgrid with an ESS and a 24/7 generator should be implemented: ○ Enables renewable power operation independent of the grid. ○ Facilitates use of a smaller solar panel collection system and a smaller ESS since there is a 24/7 generation source. ○ The ESS can be used to reduce peak energy costs (it doesn't need to remain fully charged to provide backup power since there is a 24/7 generation source).
Load Shedding	• Attempt to enable enough load shedding so that the solar power system can at least power the most critical loads during peak sunshine hours. • To best enable the most critical loads to be separated from less critical loads, see Section 6.3 *Microgrid Benefits and Issues* .

Best Practice	Specific Suggestions
Redundancy	• Consider adding redundant components (e.g., second inverter) depending upon the importance of a solar power system to improve power resiliency and the added costs of redundancy.
Cybersecurity	• Anything connected to the Internet or even to an intranet can be a cybersecurity risk including power inverters, etc. • Implement the best practices listed in the Cybersecurity and the Supply Chain Security sections.
Physical Security	• Solar panels on high-rise rooftops typically have built-in security, but additional security may be needed if in accessible areas or where the panels could be easily vandalized. • Implement the best practices listed in the Physical Security section.
EM Security	• Note: The RPWG does not know of any solar power systems to have been tested against HEMP except for standalone silicon-based PV panels, which were successfully tested.[146] • Implement the best practices listed in the *ELECTROMAGNETIC (EM) SECURITY* chapter, including using shielded cables, EMP-rated surge protection devices (SPDs), and low impedance grounding.
Environmental Resiliency	• If feasible, install solar panels so that potential harm by winds or flying debris is minimized. • If the area is susceptible to large hailstorms, the panels should be protected beyond the built-in protection of typical solar panels. • During power outages, there should be a process to remove any snow or ice that accumulates on the solar panels.

8.3. Fuel Cells

Per the Army's *Electric Power Generation and Distribution* publication, "fuel cells chemically convert fuel to electricity through a non-combustion process. Fuel cells are similar to batteries because they produce electricity through a chemical reaction. However, battery chemical energy is self-contained, whereas fuel cells need an external fuel source to sustain the chemical reaction."[147] As such, fuel cells are considered a renewable in this document since they use hydrogen to operate, and hydrogen is renewable (although the hydrogen might be made using fossil fuels).

Per Grand View Research, "stationary fuel cells dominate the fuel cell market in terms of shipped units and accounting for a [global] revenue share of USD 6.9 billion in 2019" with a 15.5% CAGR from 2020-2027.[148] The most common use case is implementing a hydrogen gas-based backup generation system for small loads of 10-25 kW or less, which is the primary use case in the first subsection below.

Because of the space required for hydrogen gas, several other use cases that do not involve the delivery of hydrogen gas are being implemented. In these cases, the sites make their own hydrogen gas using natural gas, ammonia, liquefied hydrogen, or other potential fuel containing hydrogen. These other use cases are covered in the second subsection below.

There are several types of fuel cells and various manufacturers. Thus, those chief engineers or power managers that are interested in fuel cells should contact multiple fuel cell vendors and determine which technology and offering might be best for their facility or site.

Pressurized Hydrogen Gas Delivery System

Hydrogen gas-based fuel cells, where pressurized hydrogen is delivered, are typically best for loads of 10 kW or less, or at least no more than 25 kW due to the storage space required for hydrogen gas. This use case has the following potential advantages:

- **Low Maintenance**– The maintainability doesn't require the fuel and generator maintenance that diesel or gasoline need although the fuel cells may need to be purged at startup or shutdown.
- **Robust Reliability** – Hydrogen can be stored for a long time without degradation making it a particularly good option for those organizations that cannot easily perform the maintenance needed when using a diesel generator.
- **Clean Energy** – Fuel cells are considered a clean form of energy similarly to batteries although this is typically partially offset by the generation process used to create the hydrogen. As a "clean" energy, tax credits or incentives may be available.
- **Compact Footprint** – With small loads, hydrogen generally requires less overall space than a generator when also considering the space required for the fuel and the surrounding area required for ventilation and safety purposes.
- **Quiet** – Fuel cells create very little noise unlike most generators.

In remote cases requiring either a very reliable backup power solution or where the generator may be frequently run, the TCO for fuel cells is often lower than for traditional generation solutions. This may include but is not limited to sites where a technician must be deployed to maintain the equipment, such as at a remote communications site. For instance, Altergy states that its fuel cells technology for a 5 kW, 8-hour backup power application solution is significantly less expensive than a Tier 4 generator for remote telecommunications equipment over a several year period.[149]

As an example of the potential reliability, "Plug Power's GenSure fuel cells have been third party tested at 99.6% reliability." Further, Southern Linc, which has an average LTE site load of 1.6kW, is using fuel cells to meet a specification of 7 days of onsite power.[150] Bulk refueling is quick and hydrogen cylinders can be quickly exchanged, which is typically only required after a multi-hour or multi-day power outage. Given the high reliability, a critical infrastructure owner/operator may be able to use fuel cells to meet Level 2 resilience guidelines without needing a second power generation source.

The primary disadvantages to this use case with hydrogen gas being delivered are the following:

- **Upfront Costs** – Despite the huge power density advantage of fuel cells, the upfront costs are significantly higher than for traditional backup generation costs although the cost to produce fuel cells is quickly falling.
- **Delivery System** – Although hydrogen containers can be easily delivered, hydrogen delivery typically costs much more than other types of delivery systems (e.g., delivery of electricity to charge a battery, diesel fuel which has a much higher energy density than hydrogen). Further, there are many more companies that will deliver diesel or gasoline

than will deliver hydrogen, which can be a disadvantage for fuel cells during a long-term power outage.

- **Size of System** – Because of the space required to store hydrogen gas, it is typically limited to loads of 25 kW or less.
- **Firefighting System** – Because fuel cells are far less common than systems based upon diesel, natural gas, or gasoline, many areas are not prepared to fight fires that involve fuel cells. Therefore, the firefighting department needs to be part of the implementation.

Because of the above delivery issues, it is recommended that infrastructure sites store the fuel onsite if it is needed for all hazards. For Level 3 Resilient sites, it is recommended that at least one more power generation source be available onsite both to back up the fuel cell and to better ensure enough fuel is available.

On-Site Hydrogen Conversion

Because of the space required for hydrogen and the difficulty of hydrogen delivery in many parts of the country, alternative methods are being used or commercialized instead of delivering hydrogen via gas containers although the fire department should still be notified if implementing any type of a hydrogen system. The primary near-term target market for these solutions is where the site is off-grid or frequently needs backup power for significant periods of time (e.g., a Tier 4 generator would be needed if using diesel). However, they are also being used where a higher level of power resiliency is needed. Some of the most common or promising on-site hydrogen conversion solutions include the following:

- **Solid Oxide Fuel Cell (SOFC) –** The global SOFC market size was valued at USD 403.3 million in 2019 Per Grand View Research and is expected to grow at a CAGR of 30.0% from 2020 to 2027. SOFCs can run on fuels such as natural gas or ammonia, which are plentiful in most parts of the country.[151]
- **Natural Gas to Hydrogen** – Some systems can ingest natural gas and automatically convert the natural gas to hydrogen and then run off the hydrogen. For an increased level of resilient power, natural gas can be stored by liquefying it, which can later be converted back to a gas. Natural gas is much cheaper to liquefy than hydrogen since the liquefying temperature for natural gas is 165 °F warmer than it is for hydrogen (-260 °F versus -425 °F).
- **Ammonia to Hydrogen** –Ammonia is the second most widely used inorganic chemical in the world and is cheaper than diesel. With one atom of nitrogen and three atoms of hydrogen, the system releases the hydrogen from the ammonia into a storage tank, which is then used to generate power. A single 12-ton tank of ammonia can fuel a wireless base station 24 hours a day, 365 days a year.[152]
- **Liquefied Hydrogen** – The primary fuel cell application for liquefied hydrogen is to increase tanker load by 5X over pressurized shipments. Unfortunately, it is expensive and uses about 35% of the total energy content to liquefy the hydrogen to -425 °F so it's more practical only when the hydrogen must be shipped over long distances.[153]

Each of the above could be excellent in providing resiliency against a long-term power outage. There are also fuel cell technologies that are being commercialized such as molten carbonate. The bottom line is that fuel cells are mostly deployed when small loads are required (10 kW or less). However, as the upfront costs and TCO for fuel cells continue to decrease, and as

environmental regulations increase, fuel cells are starting to provide power beyond small applications.

8.4. Wind Power and Other Renewable Energy Sources

Although the above renewables are the most popular for onsite enterprise power generation, wind power and other renewable energy sources (e.g., hydropower) may be preferred in some situations, particularly with ongoing technical improvements being made with many of these power sources. These are covered below.

Wind Power

Wind power is most often used by utilities since it is generally most cost effective to use large turbines that are integrated into wind farms. These large, integrated turbines have an economy of scale advantage with respect to the setup and maintenance costs versus smaller or standalone turbines. Wind farms are almost always located in rural settings due to zoning and space challenges within urban areas as shown in Figure 16.

Figure 16. Traditional Wind Farm (courtesy of DOE)

For critical infrastructure, wind power has been mostly used in two situations: (1) to power small loads in remote areas, and (2) on large campuses. More recently, microturbines have been developed that are compact and can be safely mounted on a rooftop or on the ground near a building. These can provide tens or hundreds of kWs of power per microturbine. For instance, the wind generator shown in Figure 17 can provide up to 100 kW of power with a 17-mph wind and 225 square feet of roof or ground space.[154] However, installing wind turbines in a retrofit application on an existing building can be challenging due to additional structural and wind loads.

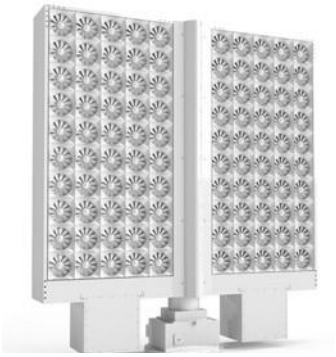

Figure 17. Compact Wind Turbine (courtesy of American Wind, Inc.)

To determine the feasibility of a wind project, it is recommended that a temporary anemometer be installed to collect at least a year's worth of wind speed data, particularly for large-scale turbines (> 100 kW). For small turbines, wind measurements are still very helpful although the energy manager may prefer to consult a local wind chart or one from DOE although even the wind speed map shown in Figure 18 could help. To best analyze whether the location is appropriate, any potential zoning regulations, safety, aesthetics, environment, and noise issues should be understood and mitigated as required. Transmission line vulnerabilities should also be considered, with long transmission lines avoided if wind power is a key part of the resilient power plans.

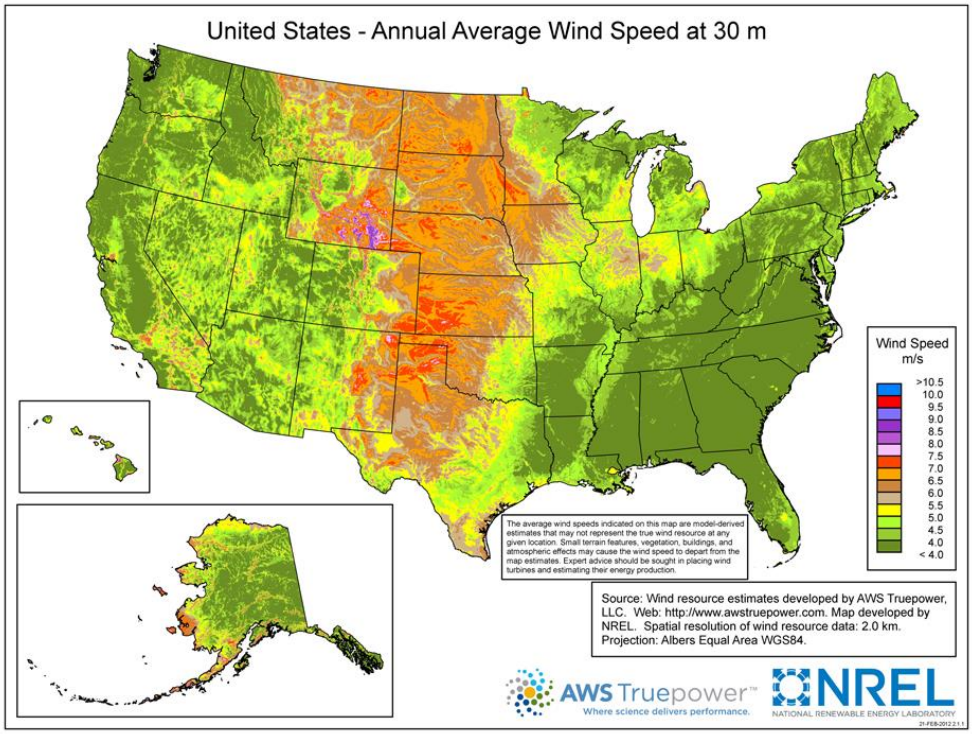

Figure 18. Wind speeds indicate that the Plains states are excellent for wind power

The business case should include upfront and operational costs and savings, but also resiliency improvements, environmental impacts (positive and negative), and end-of-life costs. The more important that wind power is to the site's resilient power strategy, the more precautions should be taken to improve resiliency such as winterizing the turbines (there are several different methods to winterize turbine blades). Turbines can be very resilient such as shown after Hurricane Sandy[155] although they must be built for resilience and they should be part of a REHS due to the intermittency of the wind.

Other Renewables

There are many other renewable or clean energy power projects that have been deployed or are being researched with some of the leading candidates discussed below:

- **Small and Micro Hydropower** – Demand for small and micro low-head (small vertical drop) hydropower is increasing due to (1) technology improvements, (2) regulatory rule changes, (3) increased need for onsite 24/7 power (although 24/7 hydropower is dependent upon the water supply/storage), and (4) desire for sustainable, clean electricity generation. Hydropower is most applicable to sites that are near a large or moderate stream of water where generated electricity can be reliably transmitted to an enterprise. The hydropower plant is often in a rural setting but it can be in an urban or suburban environment when there are sufficient resources to minimize the impact from the hydropower station on the environment. (Note that pumped storage hydropower is briefly discussed in the *Other Energy Storage System (ESS) Technologies* subsection above *in Section 7.5.*)

- **Concentrating Thermal-Solar Power (CSP)** – Generates electricity by using energy from sunlight to convert water to steam to power a turbine. With thermal energy storage, the energy can be dispatchable around the clock. CSP is typically limited to large scale, standalone power plants but can be feasible in some large campuses. The space required varies significantly based upon the location, but it averages about 10 acres per MW assuming 6-8 hours of sunlight per day. Thus, 5 acres of land could generate an average of 3-5 MWh per day when it's sunny.[156] CSP is best suited towards the desert southwest of the US, where consistently high levels of direct beam solar radiation are present year-round. The present utility-based cost is about $.098/kWh with DOE's Solar Energy Technologies Office having a goal to reach $0.05 per kilowatt-hour by 2030 for baseload plants with at least 12 hours of thermal energy storage.[157]
- **Geothermal** – This can be reliable and very cost competitive in certain geographical areas, but the facility should have a direct connection to the geothermal power generation source to use it as a 24/7 resilient power generation source. It had 0.5% market share in 2019 per the EIA.
- **Biopower** – The main biomass feedstocks for power are paper mill residue, lumber mill scrap, and municipal waste. Some of these are not renewables but most are. In the near future, agricultural residues such as corn stover (the stalks, leaves, and husks of the plant) and wheat straw will also be used.[158] Biopower had a 1% market share in 2019 per EIA but most of this was either with large operations or fuel related (e.g., ethanol) and was not used for backup or emergency power purposes. Biomass is also used for heating purposes.
- **Methane Capture** – Obtained from activities such as coal mining or trash disposal, methane can be an excellent source of energy and may be a good solution in some critical infrastructure environments, but its production can often be disrupted during a major event.

There are many cases where one or more of the above should be considered and the power manager is encouraged to follow-up on the above if it may be applicable to his/her facility. Further, some of the above may even qualify as the primary source of power when the grid is down such as a weatherized hydropower plant powered by a reliable source of water.

8.5. Intermittent Renewable Energy Hybrid System (REHS) Guidance

Critical infrastructure stakeholders desiring Level 3 resilience should strongly consider **deploying a REHS microgrid with intermittent renewable power,** which consists of a 24/7 generation source, an energy storage system (ESS), and renewable power (deployment of a microgrid is also encouraged for Level 2 resilience). Intermittent renewable power (e.g., solar, wind) should only be used as the sole backup power generation solution if needing Level 1 resilience and the solution guarantees backup power for the timeframe needed (e.g., three days). Renewables that are 24/7 (e.g., fuel cells, hydropower with storage or a reliable source of water) can be used as the sole backup power generation source but since these use cases are like using a generator, these non-intermittent renewables are not included in this section.

This section provides very high-level characteristics that need to be understood to calculate the amount of value that an intermittent REHS may provide to a site and briefly discusses how to determine the best REHS solution briefly covering the following topics:

- *REHS Versus Generator Only Solution*

- *Sizing The Energy Storage System*

REHS Versus Generator Only Solution

The best REHS use cases combine the major REHS benefits including improved power resiliency, lowered lifecycle costs, and a reduced environmental impact. When of these factors are all realized up, it's usually a straightforward business decision to decide to implement a REHS.

However, if one or more of the above factors is a disadvantage such as the REHS increases the lifecycle costs but also improves resiliency and offers a better user experience and environmental impact, it is recommended that the person or team making this decision attempt to estimate the financial impacts of all the factors as described in Table 21 below.

Table 21. An Intermittent REHS Compared to a Standby Generator Solution

Factor	REHS Solution	Generator Only Solution
Capital	• Includes renewable and energy storage costs. • Regulatory benefits could include grants, tax credits, or tax deductions, which could significantly reduce capital costs. • Costs may be partially offset by (1) using a less expensive smaller generator(s) or sometimes even eliminating a generator; (2) reducing the size of the fuel storage container,	• Most solutions implement 1-2 generators with a UPS system.
Operating Budget: Recurring Costs and Savings	Savings: • Reduces electricity purchased (by the amount of MWs internally produced or stored multiplied by the market pricing of that power when it is used). • Similar O&M costs to having a Generator Only Solution but may be able to use a smaller generator and less fuel. O&M Costs: • Equipment, components, installation, and maintenance of both the system and the surrounding area (e.g., ensure trees do not shade the solar panels). • Optimization effort to maximize the use of the energy storage and the renewables system while taking power resiliency into account. • Upfront, recurring, or opportunity cost of using the land or space where the renewable is located (if applicable). • To estimate O&M expenses, see *Asset Performance Suite (APS) – SunSpec Alliance*.[159] The costs can vary significantly depending upon the system implemented.	• Typically, all electricity is purchased. • O&M costs include storing and maintaining the fuel and the generator(s). • Generation system needs to be periodically tested. • May be able to reduce electricity costs by using a Type 4 diesel or natural gas/propane generator during periods of peak electricity pricing but capital costs would increase.

Factor	REHS Solution	Generator Only Solution
Power Resiliency	• The energy storage system can provide reliable power short-term until the stored energy is depleted. • The renewable plus energy storage system should be capable of powering the most critical loads at least for a minimum period during long-term outages.	• Typically, reliability obtained from using 1-2 generators until the fuel runs out.
User Experience and Environmental Impact	• Environmental benefits to various stakeholders, including the employees and the community. • May have a negative cosmetic or environmental impact if the choice of siting is very limited, such as a noisy wind turbine built near a building, or solar panels on the ground that replace cosmetically pleasing geography. On the other hand, these could also have positive benefits depending upon the type of renewable and its location (e.g., solar panels providing shade for parked cars).	• Generators are typically noisy and cause more pollution than a REHS.

Legend Note: The green background and italicized font is generally the preferred solution for that factor.

To better calculate each site's costs and benefits using the factors listed in Table 21, the resilient power team first needs to understand the site's existing power generation needs and costs including the costs of the generator only solution. Additionally, the team needs to determine the following if it is desired to perform an objective cost comparison between a REHS and a generator only backup power solution:

- **Optimal size of the REHS system**
  - To calculate the size of the generation system including the fuel container needed, use the worst-case conditions so that the system can meet the minimum emergency backup requirements during the troughs, typically around January for solar power as shown in Figure 19,
  - Use one of the renewable cost-benefit tools on the market to help determine a potential project's economic viability and to optimize the system such as *Reopt Lite | Reopt Energy Integration & Optimization | NREL*.[160]
  - See *Sizing The Energy Storage System* below to optimize the size of the energy storage system.
  - A wind turbine might add further resiliency since often during months or days when the generated solar power is weakest is also when the wind is stronger.
- **Resiliency costs of power outages**
  - To convert the value of power resiliency into a cost number, multiply the expected impact on customers or society per power outage event type by chances that event type will occur.
  - Per NREL, "the most effective method of determining VoLL [value of lost load] is through customer surveys, which attempt to capture the direct costs that customers experience as a result" of lost service.[161]
  - Include indirect costs that are not captured above. This may include reputational damage and the value of lives lost.
  - For example, if an area loses cellular communications, the direct costs to the cellular service provider might only be a small amount of the revenue that is

lost. But there is reputational damage and someone who needed to use the service could have been delayed getting to a hospital causing them to lose their life. It is recommended that these indirect costs be estimated. On the other hand, someone might also be inconvenienced or be less productive since they cannot use apps requiring wireless service during the outage, but those inconvenience costs can be captured under the reputational damage.

- **Environmental impact**
  - Estimate the value of the items listed in Table 21.
  - The general environmental benefits may be estimated by using an environmental calculator.

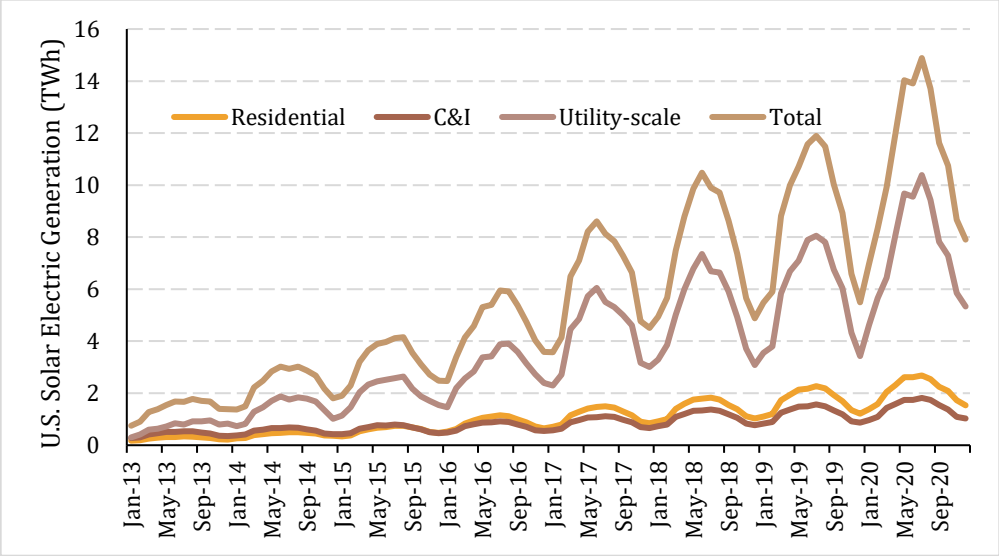

Figure 19. U.S. monthly solar production shows strong seasonal dependency

Sizing The Energy Storage System (ESS)

Once the decision is made to implement a REHS with both renewable power and an energy storage system, the size of the energy storage system (typically using a BESS) needs to be determined. To determine the size of the energy storage system (ESS) needed, it should be realized that even a small ESS has significant resiliency benefits if it can meet the critical load demands and can enable the renewable power to be used in island mode.

The next step is to size the ESS by calculating the advantages and disadvantages of a larger ESS. The main disadvantage with implementing a larger ESS is the high upfront costs although space, electricity losses, and maintenance are also potential issues as discussed in the *ENERGY STORAGE* chapter.

The primary advantages with implementing a larger ESS (or other type of energy storage system) are site dependent and includes the following:

- **Improves power resiliency**

- Backs up the primary power generation source when the renewable is not generating sufficient power (until the ESS is depleted).
- Reduces fuel usage since less fuel is needed during emergencies with a larger ESS. This is particularly beneficial during extended outages if the renewable system is big enough to power the critical load and charge a ESS simultaneously.
- The duration of previous power outages should be reviewed to better determine the improved resiliency versus the size of the ESS.
- All the above are very dependent upon the site, the architecture, and how critical the infrastructure's operations are during a power outage.

- Reduces peak demand charges
  - Per NREL[162], as of 2017, sites with higher demand charges were most likely to financially benefit from having an ESS.
  - With demand charges typically increasing much faster than kWh electricity costs and with battery costs per kW and kWh decreasing since 2017, installing a ESS would likely benefit significantly more commercial entities in 2021 than in 2017.
  - These charges are highly dependent upon the utility charges at that location, which are often controlled by the state.
  - See *Local Utility Market Analysis* under *Appendix A* for the rationale behind these charges.
- Lowers electricity kWh costs
  - Use stored energy during higher electricity pricing rather than selling the renewable power into the grid when electricity prices are often low.
  - The savings are dependent upon the commercial rates being paid.
- May enable receipt of government or clean energy incentives
  - May obtain either significant incentives from federal, state, or local governments or income from a renewable energy certificate marketplace.
  - This is dependent upon the location and whether the critical infrastructure is government or privately owned, and the type of business that it is.
- May reduce non-ESS capital costs:
  - Reduces generator costs when a smaller generator system can be purchased since the larger ESS could help provide power during peak demand at the site. Further, it could make the backup generator(s) more efficient since it could be sized closer to the average critical load.
  - May be able to downsize the UPS system (both the kW and kWh) since the ESS can quickly provide power. See *Section 7.3 UPS Guidance* for more details.

In addition to the above, an ESS will help:

- Enable the renewable system to be used in island mode. Without this, the renewable system typically will not improve power resiliency.

- Prevents inefficient generator start-ups when grid power is lost for just a short period of time (milliseconds to seconds or minutes), which wastes fuel and causes unnecessary wear on the generator.
- Minimize downtime for equipment not on a UPS when the utility grid goes down.
- Reduces noise and emissions by using renewables plus energy storage instead of a generator.

Thus, a larger ESS offers many benefits to an extent that a small ESS cannot offer, but it also costs a lot more than a small ESS. Further, the small ESS can still enable the renewables to be used in island mode, which is the most critical resiliency feature typically provided by the ESS. Therefore, it is a resiliency best practice that an ESS (or network UPS) be used with renewables although the size of the ESS is dependent upon the site's needs and the environment in which it operates.

8.6. Renewable Energy Hybrid System (REHS) Sample Use Cases

This subsection's goal is to help the reader better appreciate what has been previously discussed in this chapter including the potential benefits and costs from improved power resiliency when implementing a REHS microgrid. Using previously discussed cost related information in this chapter, the site's resilient power team can determine the TCO of a REHS and compare this against deploying a traditional backup generator system. Neither system is EMP hardened (see the best practices in *Table 20. Solar Power Resiliency Best Practices*).

Use Case 1: NREL 2018 New York City (NYC) Solar-based REHS

In this example from NREL[163], using 2018 solar costs, the renewable and energy storage systems of a hypothetical NYC hospital sized for maximum economic gain in a microgrid included the following:

- **Existing Power**: 500 kW of diesel generators and 250 gallons of fuel storage.
- **Existing Load**: Typical load of 500 kW. Critical load is 30% of the typical load (modeled using DOE's commercial reference building hospital model). During a power outage, only the critical load is run although the PV and battery are optimized to minimize the lifecycle costs of electricity to the site (which are based upon the typical load).
- **Solar PV**: Total cost is $3,101,670 consisting of 1287-kW DC solar system with a PV installed cost of $2.41/W. Note: It would require a very large rooftop with available space of approximately 130,000 square feet (per 2021 NREL estimates) to house enough solar panels to generate 1287 kW.
- **BESS**: Total cost is $992,500 for a 214 kW, 1557 kWh battery that costs $1000/kW or $214,000, plus $500/kWh or $778,500. It was assumed that all solar generated power was used internally or stored and could not be sold.
- **PV and BESS O&M**: Total PV O&M cost = $25,740/year or 1287 kW * $20/kW/year. No annual BESS O&M is assumed, but a battery replacement is included in year 10 at a cost of $460/kW plus $230/kWh, or $456,550.
- **Capital Cost**: $5,588,420 includes the cost of the PV ($3,101,670) and BESS ($992,500) or $4,094,170 plus the microgrid related costs of $1,494,250, which is

about 27% of the total capital costs. The microgrid costs include the cost of the microgrid controls, communications, and critical communications.

- **Total Lifecycle Cost Savings**: The REHS reduces total lifecycle costs versus the generator only solution over the project lifecycle of 25 years by an estimated net present value (NPV) of **$1,737,800** (prior to resiliency benefits). This was determined using the Reopt Energy Integration & Optimization Home | NREL[164] model to minimize the lifecycle cost of electricity, along with the economic assumptions in the NREL paper including a 3.1% discount rate, 0.1% inflation rate, and a 1.52% electricity escalation rate. It also includes an Investment Credit of 30% of the solar and storage capital costs or $1,228,251.
- **Estimated Resiliency Benefit**: $781,200
  - The estimated resiliency benefit is highly dependent upon the specific critical infrastructure site and the methodology used.
  - The Value of Lost Load (VoLL) in this use case was estimated to be $100/kWh, which was selected to fall in the middle of the range of VoLL values of a paper by Thomas Schroder and Wilhelm Kuckshinrichs.[165]
  - The solar and storage system extended the amount of time that the site could survive an outage by 2.1 days (from 0.9 days with diesel-only to 3.0 days) with a 90% probability as shown in Figure 20.

To determine the value of power resiliency or VoLL, the potential cost to customers of losing service from your critical infrastructure must be understood.

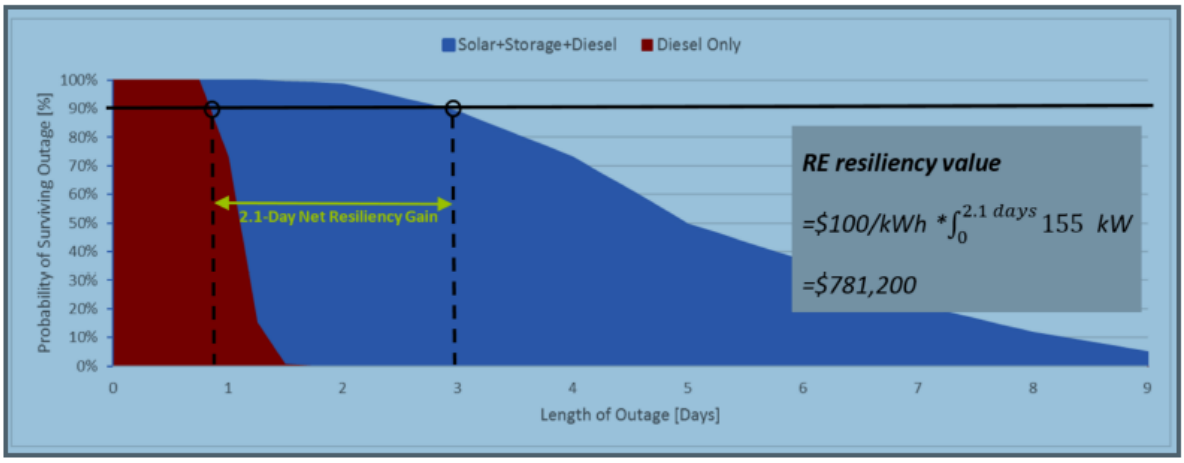

Figure 20. REHS triples outage survivability versus using only a diesel generator (NREL[166])

Overall, the above use case makes some assumptions that may or may not be true in other situations:

- Your site may have lower (or higher) electricity costs than New York City, which has above average electricity costs per the EIA. This will decrease (or increase) your site's electricity savings.

- The inflation rate is much higher than 0.1% today, which decreases the NPV of future savings (although this often leads to higher electricity escalation rates as well, which increases future savings).
- The discount rate may be higher (or lower) for your organization, which increases (or decreases) borrowing costs.
- The investment tax credit may be different for your site, particularly since some sites (e.g., Federal) are not eligible for it.
- The BESS maintenance costs are not included.

On the other hand, PV and battery costs have dropped significantly since these calculations were made. As of the second quarter of 2021, NREL estimates that the "all in" costs (including installation, inverters, etc.) are $1.60/W for PV[167], $420/kWh + $840/kW for a battery[168], and $16/kW/year for PV O&M costs. Thus, the costs would be $2,059,200 for the PV system and $833,700 for the BESS in 2021 for a total of $2,892,900 versus $4,094,170 in 2018 for an additional savings of $1.2M.

Conclusion: The NPV was estimated to be about $1.74 million and over $2.5M if including the resiliency benefits of $781,200 over the 25-year project lifespan. This was despite the use case occurring in 2018 in a northeastern city with below average solar irradiance and assumed that the utility would not pay to purchase excess power. The use case included tax credits, a low discount rate, retail rates in an above average electricity-pricing environment and was based upon estimated costs and benefits.

Use Case 2: Pacific Northwest Fire Department Solar-Based REHS

This second use case, courtesy of muGrid Analytics, uses 2020 costs and benefits for a critical infrastructure fire department in the Pacific Northwest that also supports a communications tower on the exterior of the building. As shown in Figure 21, the number of days that backup power could be maintained without external fuel supplies increased by 68% by adding a solar power system and a BESS to the existing propane generator.

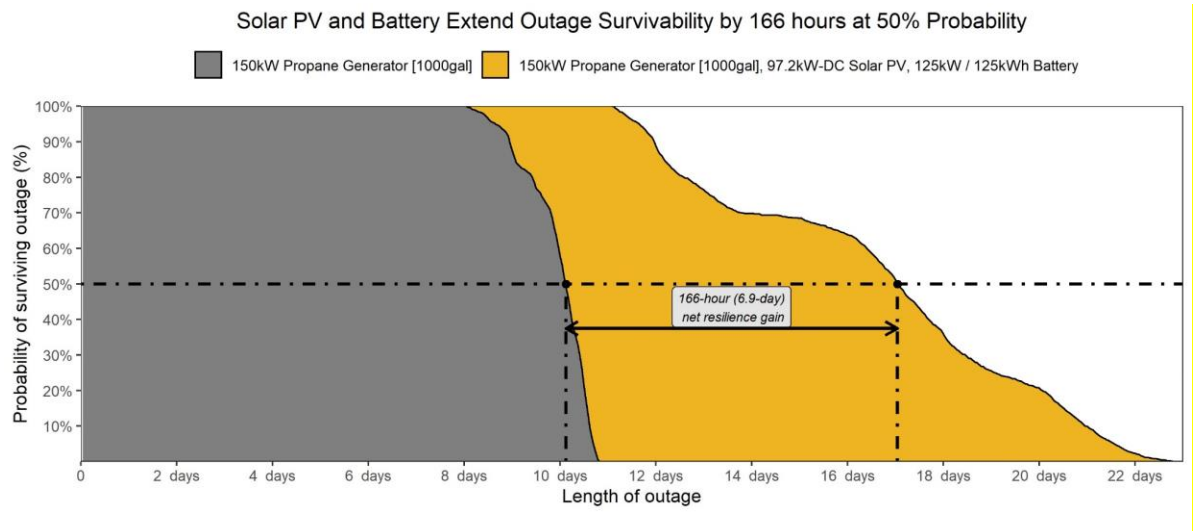

Figure 21. Site's resiliency increases to Level 2 with a REHS (courtesy of muGrid Analytics)

It now meets 14 days of fuel supply with 70% confidence without any fuel deliveries and meets a much higher level of confidence when considering potential fuel deliveries. Perhaps more importantly, it also adds another power generation source enabling it to meet Level 2 resilience as defined in this document and it could continue to provide some power for a long period of time even without any fuel deliveries.

The microgrid REHS included the following:

- **Existing Load**: 41 kW peak, 15 kW average (load based upon actual load profile measured every 15 minutes over a year). The critical load goes up to 52 kW peak during resilience operations. The critical load is bigger than the normal operational load because the communications tower is on its own meter during normal operations, but the fire station's backup power supports the tower during grid outages.
- **Propane Generator**: 150 kW propane generator, 1000-gallon propane tank
- **Solar**: 97.2 kW DC Solar PV; 122.3 MWh per year (335 kW/day). Using NREL 2021 standard cost estimates of $1.60/W, the solar capital cost is estimated to be $150,000.
- **Solar Irradiance**: 14.4% capacity factor
- **BESS**: 125 kW / 125 kWh. Using NREL 2021 standard cost estimates of $840/kW and $420/kWh, the BESS capital cost is estimated at $160,000.
- **Microgrid O&M**: $5,000 per year (estimate for first year). This includes annualized expenses like servicing, software control subscriptions, monitoring, and insurance. Expected equipment replacements or augmentation is not included here but is included in the NPV calculation below.
- **Capital Cost (added PV/BESS only)**: Estimated **$310,000**
- **Incentives**: Incentives are not included in this analysis because the site is a not a tax paying entity. Tax credits and depreciation benefits would apply to projects owned by tax-paying entities. Other federal, state, and local incentives or grant funding may be available, but were not included in this analysis.
- **1st Year Electricity Savings**: $54,000 savings during the first year resulting from avoided energy purchases and reduced demand charges based upon a $30 peak demand charge. This amount will change in future years based on the utility escalation rate (3%), the PV degradation rate (0.7%), and other factors.
- **Net Present Value (NPV)**: The NPV of the system is **-$6,500 u**sing a 25-year project lifespan, with appropriate equipment maintenance and replacement as needed, and using a discount rate of 3.9% and a utility escalation rate of 3%.
    - This financial calculation includes all planned O&M expenses, both annual expenses and one-time equipment replacement and augmentation over the 25-year project life.
    - A third-party investor or a private company could have received tax benefits from this project increasing the NPV of the system to be as high as $26,500 assuming a discount rate of 3.9% (this tends to be low for an investor).
    - With or without the tax benefits, this project was considered very worthwhile since the resiliency benefits far exceed the NPV.
- **Resiliency Benefit**:

- The solar and storage system extended the amount of time that the site could survive an outage by 7.1 days (from 10.1 days with generator-only to 17.2 days) with a 50% probability or by 2.8 days (from 8.5 days with generator-only to 11.3 days) with a 98% probability, where the probability is based on the time to first failure of the microgrid for outages uniformly distributed throughout the year.
- Since this fire station and communications tower have been designated as critical facilities, the value of resilience is high. This fire station is in a geographically isolated community which may be cut off from outside help in case of a natural disaster or other emergency.
- Site now meets Level 2 resilience since it has two sources of power with a reliable 24/7 propane generator and a solar plus storage system.

Time to first microgrid system failure was simulated for outages beginning at each hour during a year to assess the resilience performance sensitivity to time of day and seasonality using Typical Meteorological Year weather files. Adding solar plus storage to the existing generator enables the system to support the site requirements for two weeks or longer at most times throughout the year. Time to first failure is defined as the point at which the generator fuel tank is empty and the solar plus storage is not able to meet the load. Performance degrades slightly during the winter months (November through January) when the solar resource is lower.

The critical load includes 100% of the normal load at the fire station plus additional loads from the communications tower mounted on the building that are normally separately metered. If 40% of the site's normal load was considered critical (a 60% reduction in load), that would increase the site's resilience to Level 3 with nearly 100% confidence as shown in Figure 22 but even powering 60% of the load might be considered Level 3 resilience given the long-term resiliency of the REHS.

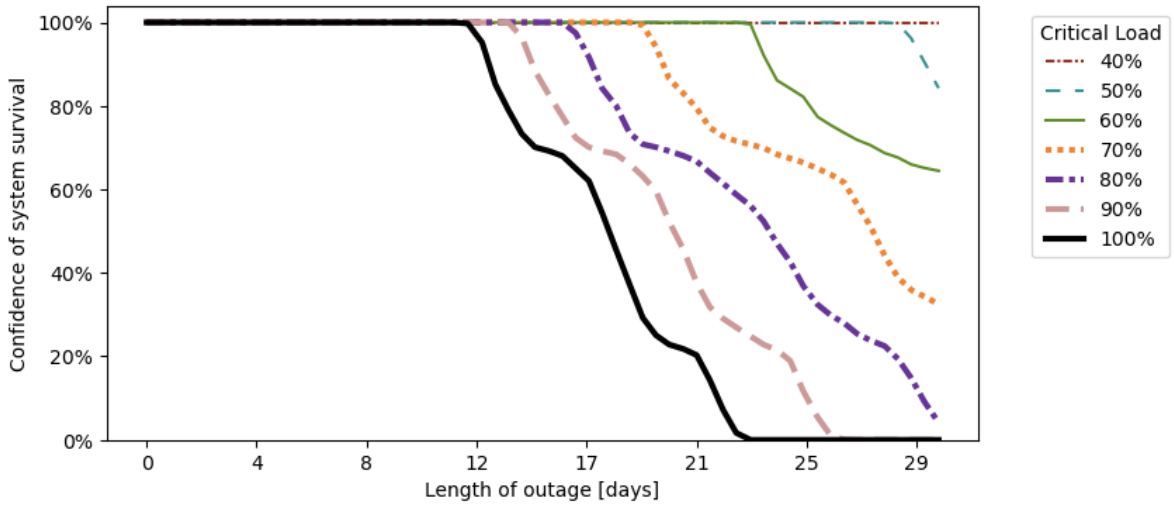

Figure 22. Decreasing the critical load increases resiliency (courtesy of muGrid Analytics)

Conclusion: The decision makers estimated that the value of the added resiliency was worth significantly more than the -$6,500 NPV over the 25-year project lifespan. Thus, this use case, which is based upon an actual implementation, is economically viable with a positive ROI even without grant money, tax credits, or the environmental benefits. The project also shows the helpfulness in being able to reduce the critical load when needed.

9. NUCLEAR SMALL MODULAR REACTORS (SMRs)

Target Audience:

- Power Management/Engineering
- Continuity & Planning: Browse, read if considering

Because SMRs have excellent resiliency and can operate for years without refueling, they could be critical during long-term outages.

Given SMR's excellent potential resiliency while acknowledging the significant investment and planning that will be required to deploy an SMR, this section is provided for educational purposes and for future planning. In addition to SMR's substantial potential contributions to power resiliency, SMRs may be very advantageous in remote locations that are not connected to the main U.S. electrical grid and where delivery of supplies is difficult or expensive. SMRs also have the potential for mainstream power production given their benefits listed in Section 9.3 including their capability to be factory produced in a controlled environment, rather than stick-built at a site using various designs and different labor teams.

The 4th generation (Gen IV) Small Modular Reactor (SMR) technology, its potential advantages over previous generations, and some procurement opportunities are further discussed below. Although the technologies are still in the research, development, and early demonstration phases within the U.S. (some have been deployed outside the U.S.), many companies are investing in Gen IV SMRs with operational SMRs expected from multiple vendors by 2030. Thus, more than one Gen IV technology may be of interest to critical infrastructure stakeholders.

If a dispatchable SMR or microreactor is used, it might be reliable enough to replace a primary power system. However, it would likely need to be combined with an energy storage system (ESS) to handle short-term rises in power usage and to store excess generated power when the supply is greater than the load. A backup power source would also be needed for when the SMR needed to be moved offline, perhaps for maintenance. Some of these companies are listed in *Appendix E NUCLEAR SMR VENDOR OFFERINGS*.

9.1. General SMR Background

The International Atomic Energy Agency defines SMRs as "advanced reactors that produce electricity of up to 300 Megawatts of Electrical Output (MWe) per module. These reactors have advanced engineered features, are deployable either as a single or multi-module plant and are designed to be built in tightly-controlled, "nuclear qualified" factories and shipped to utilities for installation as demand arises."[169] Per DOE, "more than 50 U.S. companies are working on designs that are smaller, scalable, versatile and even mobile—providing far greater access to nuclear power than ever before."[170] "The global small modular reactor market was valued at $3.5 Billion in 2020, and is projected to reach $18.8 Billion by 2030, growing at a CAGR of 15.8%."[171]

The U.S. government is also encouraging nuclear power. The November 2021 "Infrastructure Investment and Jobs Act" (also known as the Bipartisan Infrastructure Deal) allocates $6B to prevent premature retirement of existing zero-carbon nuclear plants.[172] This is in addition to the funding being provided to Gen IV SMR technology.

With nuclear power total costs, including end-of-life, being less than half of diesel's costs at $2.25 per gallon at 75% capacity, SMRs can be an excellent choice for remote locations without a stable grid.
Source: Study on The Use Mobile Nuclear Power Plants for Ground Operations by the DoD Deputy Chief of Staff (Oct 2018)

Although nuclear provides almost 20% of the total U.S. electricity supply and over 50% of its clean energy at an average cost of only 3.2 cents/kWh[173], it has not been a source of onsite power (except at nuclear power plants). This is primarily due to the complexity of building and operating a nuclear reactor and the minimum size needed to make it economical.

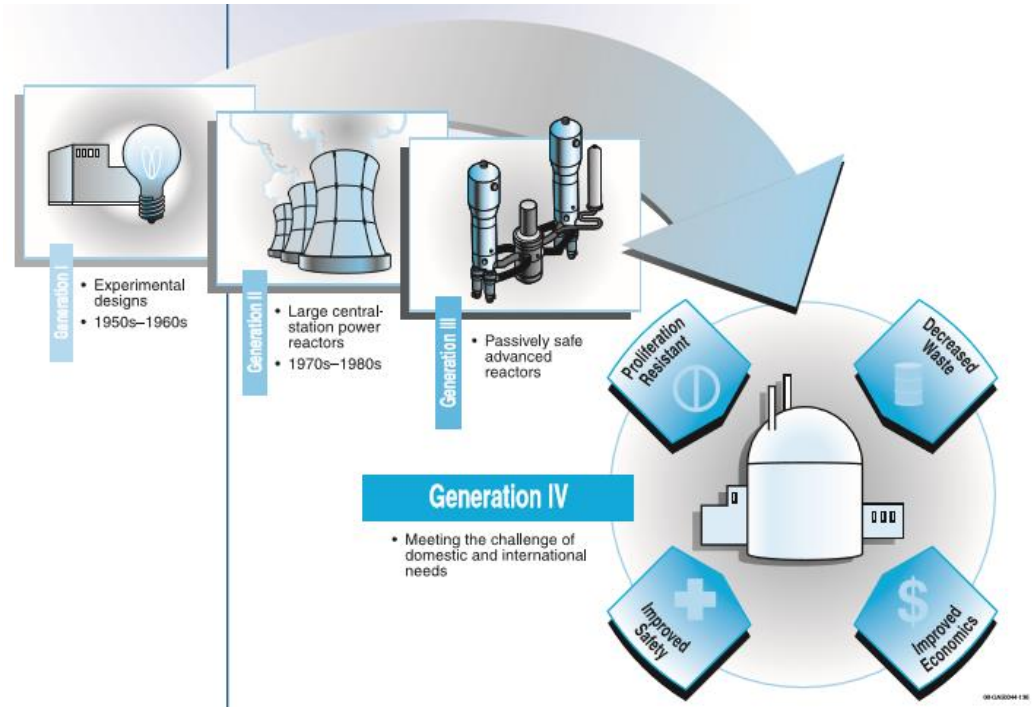

Figure 23. Migration to Gen IV Nuclear Reactors (courtesy of Idaho National Laboratory)

Generation (Gen) IV SMR power plants, as shown in Figure 23, build upon Gen III that are cooled by the laws of physics or natural circulation. Gen II reactors, which have a history of being extremely safe compared to other power generation methods, require dedicated electrical sources to power pumps to circulate emergency cooling water for reactor cooling purposes, which is a safety risk as evidenced by the Fukushima Daiichi nuclear accident. But Gen III plants either do not require any cooling pumps or need much less powerful pumps (they use natural circulation sometimes combined with compressed gas). For instance, the Westinghouse Generation III+ AP1000 passive safety system that is being implemented in the Vogtle Units 3 and 4 in Georgia with a total generating capacity of over 2.4 GW do not require "pumps, diesels, chillers or other active machinery."[174]

9.2. SMR Technical Details and Benefits

Gen IV SMRs offer four potential benefits versus traditional nuclear reactors: lower costs, reduced safety risks, higher resiliency, and additional environmental benefits. Costs are briefly discussed in the first two paragraphs below with a discussion of the other benefits following in the remaining part of this section.

EIA estimates that advanced nuclear will have the lowest costs using a LACE model.

The U.S. Energy Information Administration (EIA) estimated that the Levelized Cost of Electricity (LCOE) (unweighted) for new advanced reactor resources entering service in 2026 will be $63.10/MWhr (in 2020 dollars). (The decommission, waste, and O&M costs are included.) However, more importantly to commercial deployments, the EIA estimates that advanced nuclear will have the **lowest** levelized avoided cost of electricity (**LACE**) for a dispatchable generation source (a dispatchable can vary output to follow demand). LACE is generally more important than LCOE because it "accounts for the differences in the grid services that each technology provides, and recognizes that intermittent resources, such as wind or solar, have substantially different duty cycles than the baseload, intermediate, and peaking duty cycles of conventional generators."[175]

Further, because most SMRs can be produced at a manufacturing plant versus almost entirely onsite, there is a strong possibility of significant future cost cuts. Also, there is a strong movement in the world toward carbon pricing, which would reduce nuclear power's LACE versus alternative technologies, particularly if the carbon pricing replaces large subsidies that are provided to other technologies but typically haven't been allocated to nuclear power.

SMRs do not require safety pumps and have added other improvements to make the plants significantly more reliable, safer, and simpler than the older Gen II power plants. For example, SMRs are designed to be either EMP hardened or at least very resilient to EMP although testing is required to confirm this. They can also use an enduring fuel that can last for years. SMRs are also expected to "reduce or eliminate many of the types of contamination issues by reducing the number of systems, structures, and components that can become radioactive as a result of operations; shrinking the volume of systems exposed to primary cooling systems; and selecting materials that are easy to decontaminate."[176]

Table 22. Fuel Type Versus Energy Density

Fuel Type	Energy Density (MJ/kg)[177]
Coal	29
Diesel	42.6
Gasoline	43.4
LNG	48.6
4% Uranium 235	701,988

SMRs may be an excellent way for some large enterprises to achieve highly resilient emergency power either by constructing one on-site or working with a utility or a partner to construct one nearby with route diversity for the power distribution. SMRs can enable an enterprise to go from a "bolt-on stovepipe resilience" where the off-site fuel deliveries may or may not be successful to "baked-in reliability" with a long-term internally stored energy supply where the same power system is used on a bad day as on a good day. This is possible because of the tremendous

energy density of uranium (see Table 22). Plus, the modern nuclear power plant designs can automatically reduce fuel consumption based upon changes in demand.

In a nutshell, advanced reactors (non-light water designs) and SMRs, such as the one shown in Figure 24, offer many benefits over current large light water reactors:

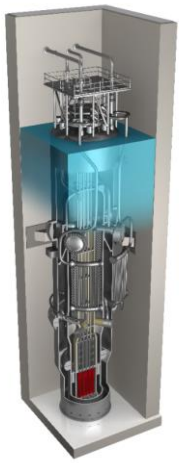

Figure 24. NuScale Power Module
(courtesy of NuScale)

- **Improved power resiliency** with the added cost of resiliency baked into the day-to-day energy production including:
    - Fuel security with multiple years of fuel that can be stored on-site
    - Island mode capable
    - Reduced EMP susceptibility when deployed with hardened passive safety systems, underground construction (optional), and fewer electrical components
    - Black-start capable with a battery or enterprise generator backup system
    - Not susceptible to climate stresses such as the freezing/icing of solar panels or high wind damage to wind turbines.
- **Enhanced safety** particularly versus Gen II reactors, including:
    - Small and efficient cores with passive reactor designs that limit source-terms, which could have the potential to release radiation if there is an accident.
    - Incorporates passive cooling (i.e., cooling pumps are not required) so that high powered generators are not needed.
    - Operates without the need for safety-related backup electrical systems.
    - Underground construction for enhanced security features and seismic performance,
    - Uses a variety of coolants such as water, molten salt, high temperature gas and liquid metal that can improve safety and efficiency.
    - Implements modern control systems and human-machine interfaces that simplify operations and improve safety.
    - Most designs are resistant to proliferation since they use low enriched uranium (LEU) (similarly to existing nuclear reactors) or high assay LEU (HALEU) fuels that are more proliferation resistant.
- **Smaller footprint and site flexibility** offers:
    - More placement optionality with some SMRs such as Molten Salt Reactors (MSRs) being able to be located away from bodies of water.
    - Could enable the SMRs to be located near the loads, such as large campuses and military bases, perhaps as energy-as-a-service.
    - Can also help with delivering reliable electricity off campus so that people can come into work.

- **Modularity and scalability** can enable some units to operate while others are serviced. The simpler design also provides improved quality and regulatory compliance, which can reduce costs and improve safety.
- **Faster deployment** since the SMR is manufactured off-site in parallel with site preparation.
- **Extremely clean form of energy** including:
    - Carbon free and always-on with existing nuclear power plants already considered to have the lowest average lifecycle CO2 emissions per GWh per the United Nations Economic Commission for Europe (UNECE).[178]
    - Many of the SMR technologies generate less waste/GWh versus existing reactors and some SMRs are being designed to reuse/recycle nuclear waste (see below for a further discussion of waste).
    - UNECE ranked nuclear as third in total lifecycle impacts, just behind smaller-scale hydro plants and almost on par with tower-type concentrated solar plants.[179] SMRs are expected to significantly improve this already high score.
- **Rapid ramp up and ramp down** of power with some designs capable of being varied over hours or even minutes, which enables better support of variable demand and integration with renewables if needed.
- **Lower cost** potential based on the following developments:
    - "Mass production" with SMRs being made in one location and shipped globally.
    - New technologies are being implemented to make SMRs even simpler, which are expected to further reduce capital and operational costs.
    - Some designs produce substantially less waste reducing the cost of storing the waste and lowering uranium usage.
    - Costs decrease when building multiple reactors that use the same design with the same basic construction crew.

Some designs use Tri-structural Isotropic (TRISO), which is an intrinsically safe and proliferation resistant uranium fuel. Each TRISO particle starts with a uranium oxycarbide (UCO) kernel, which is then encapsulated by three layers of pyrolytic carbon and silicon carbide that prevent the release of radioactive fission products. The TRISO particles are fabricated into billiard ball-sized graphite spheres called pebbles.

TRISO Fuel Enhances Safety

- **Intrinsically safe.**
- **No possible Chernobyl, Fukushima, or Three Mile Island scenarios.**

Thus, even if the TRISO encapsulated particles are released from the graphite pebbles, they will not make the surrounding area radioactive. This elimination of contamination together with a reduction of contamination in other parts of the modern nuclear power plant design not only addresses the biggest safety concern while also helping environmentally, which could significantly reduce decommissioning costs.

Lastly, many SMRs and advanced reactors are being designed to significantly reduce nuclear waste or can even reuse spent nuclear fuel from other plants, which provides strong

environmental benefits. For instance, technologies such as Fast Breeder Reactor (FBR) plants are being used today outside the U.S. to make nuclear a form of renewable energy by recycling uranium from nuclear power plants. Using updated FBR technology could not only provide GWs of electricity but could eliminate most of the leftover uranium nuclear "waste", including eliminating most of the long-lived radioactive isotopes, which has been a primary nuclear waste concern. For more details on the above, see the DOE sponsored paper *Small Modular Reactors: Adding to Resilience at Federal Facilities*.[180]

SMRs Can Reduce Waste:

- **Improved efficiency generates less waste per GWh.**
- **Some technologies can reuse/recycle existing nuclear waste.**

Microreactors

A sub-category of SMRs are microreactors, which DOE's Office of Nuclear Energy defines as "plug-and-play reactors able to produce 1-20 megawatts of thermal energy used directly as heat or converted to electric power."[181] Key microreactor benefits include the following:

Microreactors are expected to be deployed on large campuses, starting with those that already generate their own power.

- **Fail-safe design** – With passive safety systems, proliferation secure fuel, and the likely use of inherently safe fuel, systems are expected to be safely operated near commercial or governmental structures.
- **Self-regulating** – Fail-safe design and simple maintenance requirements allow the microreactor to self-regulate with minimal specialized staff, using the latest in digital controls and artificial intelligence (AI).
- **Factory fabricated** – Enables much quicker construction and potentially lower costs with "mass production" where all components are fully assembled in a factory including rapid on-site installation potentially in under a week.
- **Transportable** – Their small size makes them easy to transport by truck, ship, airplane, or railcar.

Because of how small microreactors are in size and power output, their ability to run continuously, and their low refueling requirements, they could change the power landscape for many critical infrastructure sites. These could be extremely valuable during long-term power outages given their resilient designs and since they could operate up to or even beyond 10 years without refueling with minimal O&M downtime per reactor.

Further, it might be feasible in the future for a mobile microreactor to be powered down in less than a week, moved to an area with a long-term power outage, and then powered up within a day or so. American microreactor developers are currently focused on gas and heat pipe-cooled designs that could debut as early as the mid-2020s.[182]

9.3. SMR Procurement Opportunities and Activities

There is increasing momentum worldwide to install nuclear reactors to produce safe, clean, and resilient baseload electrical power with national governments playing a leading role. From a critical infrastructure resilient power perspective, these SMRs, particularly the microreactors, could play a vital role at larger Level 3 and 4 resilience sites and at Level 1 and 2 remote sites that presently operate mostly using diesel generators. In the U.S., DOE and DoD are the lead

agencies with support from Congress being critical to provide funds and a level playing field to help commercialize the SMR and microreactor markets.

DOE has significantly increased its investment in research and development of new reactor technologies over the past few years. In October 2020, the Office of Nuclear Energy provided cost share awards to (1) TerraPower and GE Hitachi for a 345 MW Natrium reactor which uses molten sodium metal as a coolant and (2) X-energy for an 80 MW reactor using helium in a packaging of meltdown proof pebbles. Both reactors are expected to be simpler, safer, and more economical than traditional reactors and could be operational by 2027.[183] In total, DOE is funding over a dozen SMR and microreactor technologies. See *Appendix E NUCLEAR SMR VENDOR OFFERINGS* for more details.

In addition to the above DOE efforts, DoD has also significantly increased its SMR efforts. In March 2021, DoD awarded contracts to BWX Technologies (BWXT) and X-energy, both of whom were part of DoD's initial design award in March 2020, to develop a reactor of 1- to 5-megawatt output that can last at least three years at full power. In addition, the reactors must be designed to operate within three days of delivery and be safely removed in as few as seven days if needed.[184] It followed this up in June 2022 with a prototype award to BWXT to deliver a 1-5 MWe microreactor to Idaho National Laboratory in 2024 for testing. The microreactor will be powered by TRISO fuel, which is intrinsically safe and proliferation resistant.[185]

A second effort by the DoD consists of conducting a pilot program to demonstrate the efficacy of a microreactor in the 2-10 MWe range as identified in the 2019 National Defense Authorization Act. As part of this, the Air Force announced in October 2021 that it had selected Eielson Air Force Base in Alaska to pilot an NRC licensed, commercially owned microreactor up to 5 MWe as soon as 2027. These microreactors could be used to significantly improve resilient power for critical functions.[186]

For federal entities, see Appendix A of the DOE resource document *Small Modular Reactors: Adding to Resilience at Federal Facilities.*[187] Appendix A, which is the Executive Summary of a previous report titled "*Purchasing Power Produced by Small Modular Reactors: Federal Agency Options*" includes a discussion of how a federal entity can setup an agreement with a local utility to build a local highly resilient SMR. Alternatively, a facility on a DoD base may be able to partner with its DoD host to obtain this resilient power. For more details regarding the technology and vendors, see *Appendix E NUCLEAR SMR VENDOR OFFERINGS*.

Appendix A. REGULATORY AND UTILITY POWER GENERATION ENVIRONMENT

The recommended initial step to improve power resilience for most larger enterprises and those that need to be Level 2 resilience or higher is to assess the energy and regulatory environment in which it operates. To help understand these environments, the critical infrastructure energy manager needs to understand *Existing Laws and Regulations* and conduct a *Local Utility Market Analysis* below.

After understanding the local pricing market, laws, and regulations, an energy or facilities manager/engineer can better determine how often they may need to rely upon their site's own power generation or energy storage capabilities.

Existing Laws and Regulations

Typically, most enterprises will use a third party that has strong regulatory expertise to help design its resilient power system, so this section focuses on just providing a high-level overview of the general regulatory entities and includes a few particularly pertinent regulations that are targeted at enterprises.

The Federal Energy Regulatory Commission (**FERC**) is the most important national entity regulating energy utilities. It is an independent federal agency responsible for regulating rates and services for electric transmission in interstate commerce and electric wholesale power sales in interstate commerce. FERC's authority does not apply to the ERCOT markets; however, its authority does cover "reliability of the bulk-power system, through oversight of the development/approval of and compliance with mandatory reliability standards" in all states including Texas.[188]

FERC can play a role in allowing an enterprise to sell power into the grid, which could impact the enterprise's power generation and energy storage decisions. For instance, with the 2018 passage of *Final Rule on Electric Storage Participation in Regional Markets*, it is expected that battery storage systems will play a larger role in frequency regulation. This ruling will "remove barriers to the participation of electric storage resources in the capacity, energy and ancillary services markets operated by Regional Transmission Organizations and Independent System Operators."[189] The goal is not only to help improve overall reliability and lower electric costs, but also provide a cost incentive for enterprises to deploy significant storage resources and sell electricity into the grid when it is needed for short periods of time, which could reduce the total cost of ownership (TCO) to deploy an enterprise power storage system.

FERC exercises its authority through the North American Electric Reliability Corporation (**NERC**), a not-for-profit international regulatory authority whose mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid. NERC develops and enforces reliability standards; annually assesses seasonal and long-term reliability; monitors the bulk power system through system awareness; and educates, trains, and certifies industry personnel. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC's authority does not cover distribution and has limited applicability to ERCOT in Texas. NERC is the electric reliability organization for North America, subject to oversight by the FERC and governmental authorities in Canada. NERC's jurisdiction includes users, owners, and operators of the bulk power system, which serves more than 360 million people.

The **EPA** is another agency that affects resilient power decisions. Per the EPA, standby emergency generators are allowed to operate on an unlimited basis for emergency power or up to 100 hours per year "*for the following purposes:*

- *maintenance and testing,*
- *emergency demand response for Emergency Alert Level 2 situations,*
- *responding to situations when there is at least a 5% or more change in voltage, and*
- *operating for up to 50 hours to head off potential voltage collapse, or line overloads, that could result in local or regional power disruption*."[190]

The EPA defines a bulk storage fuel container as having a capacity of 55 gallons or more.[191] To prevent leakage, it stipulates the type of material that the container is made of, its piping, overflow protection, and other items that are the responsibility of the vendor. The National Fire Protection Association (NFPA) also provides codes and standards that cover the storage of fuel.

The Federal Motor Carrier Safety Administration (FMCSA) includes rules that cover the transportation of fuel. For instance, it requires a special type of commercial motor vehicle called a "tank vehicle" if it transports more than 119 gallons in an individual rated capacity and an aggregate rated capacity of 1,000 gallons.[192]

The above discusses some federal regulators and a few significant laws and regulations. Additionally, there are many state, local and even other federal regulations applicable to resilient power that an enterprise may need to consider. For instance, Illinois limits "the aggregate total gallons of fuel stored at one facility to 12,000 Gallons."[193] Further, "in dense urban areas, like New York City, there are significant barriers to generators, such as stringent codes and noise and environmental concerns."[194] Each State has a public utility/service commission that typically regulates electricity rates and could approve requests for rate recovery for resilient power investments.

Local Utility Market Analysis

Understanding the local electric market, including potential financial and power resiliency impacts to the enterprise, may be important if the enterprise is considering (1) building spare generating power capacity to sell to utility companies, or (2) partnering with a utility or third party as part of the enterprise resiliency strategy. An example of when an enterprise might rely more heavily upon a local utility could occur if the power plant was nearby with multiple generation sources, onsite fuel or equivalent, and with very resilient power distribution to the enterprise so that the overall power resiliency was very high. These capabilities could be sufficient to provide a resilient power system to meet Level 1 best practices or help meet Level 2 best practices if combined with an onsite generator.

Excluding the laws and regulations that were described in the section above, the local utility market can be broken down into three major categories:

- **Online power generation** – The power being generated to meet user needs including:
    - **Operating reserve power** – This reserve generation market falls into the following categories: frequency regulation, spinning, non-spinning, and replacement reserves.

- **Black Start Resources** – Resources used to restart a grid segment without assistance from external power following a large area outage. The purpose of black start resources is to avoid or promptly recover from a "Black Sky" event where all utility resources are offline across a large geographical area.

- **Transmission** – Moves large amounts of power generally over substantial distances and directly serves very large electrical loads.
- **Distribution –** The final stage of electricity distribution to the final customer. "Traditionally distribution distances are under 20 miles and voltages are less than 69.5 kV (kilovolt) (more commonly 13.5 kV). However, voltages up to 115 kV are used in some locations. Distribution has substations just like transmission, only smaller."[195]

The local implementation is important to understand since this can significantly impact the resiliency of the power being delivered to the enterprise by the utility. For instance, if the utility's power generation is very close to the enterprise, then there is probably a much lower likelihood of a power disruption due to downed power lines and the enterprise may be able to rely more heavily on the utility as part of its resilient power system. The power plant generation also needs to be understood. If it uses natural gas, which is increasing popular as shown in Figure 25 below from the U.S. Energy Information Administration (EIA), that plant will need to rely upon an external source of fuel, which could impact reliability. With proper planning, there might be a nearby highly resilient commercial utility generation system with black start capabilities (able to start without external power) along with transmission route diversity to the enterprise.

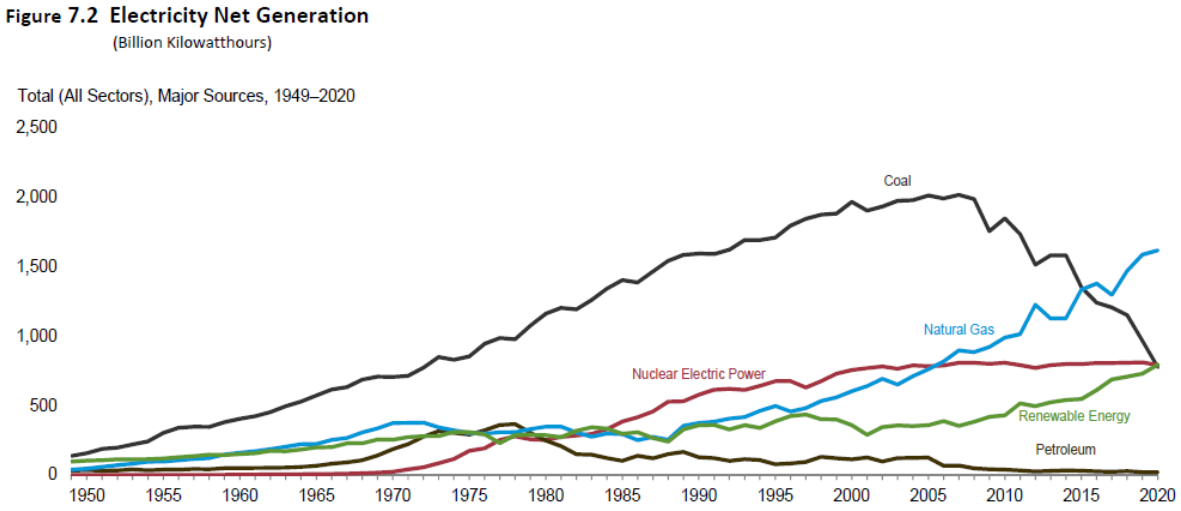

Figure 25. Sources of U.S. Electricity (source: Monthly Energy Review, EIA, Aug 2021)

Operating reserve power, described in Table 23 below, helps provide overall grid reliability, stability, and capability to meet peak power needs. Understanding this concept can help the enterprise energy manager better understand electricity pricing and the wholesale market including selling electricity to the utility company. It might also help the energy manager better understand the rationale behind a demand response program where the enterprise cuts back its demand in response to short-term increased market prices for electricity.

Table 23. Types of Operating Reserve Bulk Power Electricity Generation (normal operation)

Category	Response Time	Description
• **Frequency Regulation**	• Response starts within seconds or milliseconds (ms) with completion within 20 minutes	• Regulates the alternating current (AC) frequency within tight tolerance bounds in order to synchronize generation assets for electrical grid operation. • Mainly provided by ramping up or down generating assets[196] although battery storage systems are starting to play a role partially due to the FERC 2018 *Electric Storage Participation* rule previously discussed. • Typically, frequency regulation is roughly 1% of the overall grid generation capacity.
• **Spinning**	• Within 10 minutes, but starts coming online immediately	• "Unloaded generation that is synchronized and ready to serve additional demand."[197]
• **Non-Spinning**	• Within 10 minutes, but there is a delay as generator starts-up off-line	• "That generating reserve not connected to the system but capable of serving demand within a specified time. • Interruptible load that can be removed from the system in a specified time."[198]

An event such as a large generator failing or rapid cloud coverage over multiple large solar farms could require the above operating reserve power categories to be activated. When a large generator stops working, fires damage major transmission lines, or solar farms stop generating power, not only is the output power impacted, but the generators providing the remaining power may slow down due to the increased load. When this occurs, additional assets will kick-in to increase the frequency and the power output.

Due to the above, a large electricity customer will often have both an energy charge based upon the number of kilowatt-hours (kWh) used over the billing period and a separate charge for the peak kWh used. The peak kWh charge helps pay for electricity generation equipment that must be brought online for the peak usage periods and to help encourage larger customers to use less electricity during these periods or even generate additional electricity and sell it to the utility. For instance, microgrids can help enterprises reduce the effects of this pricing increase by leveraging internal power generation sources to reduce demand charges and increase grid reliability.

Appendix B. NIST CYBERSECURITY FRAMEWORK CORE FUNCTIONS

The five *NIST Cybersecurity Framework* Core Functions mentioned in Section *3.1 Cybersecurity* are shown in *Table 24*. The Identify, Protect, Detect, Respond, and Recover Functions are not intended to form a serial path or lead to a static end state. Rather, the Functions should be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk.

Table 24. NIST Cybersecurity Framework Core Functions

Function	Specifics	Categories
Identify	Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.	• Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy • Supply Chain Risk Assessment
Protect	Develop and implement appropriate safeguards to ensure delivery of critical services.	• Identity Management and Access Control • Awareness and Training • Data Security • Information Protection Processes and Procedures • Maintenance • Protective Technology
Detect	Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.	• Anomalies and Events • Security Continuous Monitoring • Detection Processes
Respond	Develop and implement appropriate activities to perform regarding a detected cybersecurity incident.	• Response Planning • Communications • Analysis • Mitigation • Improvements
Recover	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.	• Recovery Planning • Improvements • Communications

Appendix C. ADDITIONAL E3 HEMP AND GMD DETAILS

Chapter 4 ELECTROMAGNETIC (EM) SECURITY provides background information and mitigation best practices for EMP/HEMP and GMD, both of which could cause severe widespread power outages. To keep the material in Chapter 4 from being too technical and to help make it more targeted toward the audience of this document, the following material was moved into this appendix:

- *E3 HEMP and GMD Technical Characteristics* – Engineers should read this appendix subsection if they support critical infrastructure deploying long lines containing metal (more than 10 km), such as might occur in an archipelago.
- *E3 HEMP and GMD Impacts* – In those situations where either long lines need to be protected or where the reader is interested in why the mitigations in *Section 4.3 E3 HEMP and GMD* are recommended, this subsection should be read.
- *SREMP* – Source Region EMP (SREMP) mitigations might be necessary for some of the most critical infrastructure requiring a very high level of resiliency.

E3 HEMP and GMD Technical Characteristics

E3 HEMP and GMD space weather impacts are a result of very low frequency geomagnetic field fluctuations of less than 1 Hz that reach deep within the Earth's surface (see Figure 4 in the *E1 HEMP Technical Overview* subsection in Chapter 4). Depending on the 3-D electrical conductivity variations of the Earth (magneteulliric [MT]) beneath and surrounding a specific location, which can vary by orders of magnitude,[199] E3 and GMD can induce significant quasi-DC or very low frequency currents in long electric transmission lines, pipelines, rail lines, communication lines, and any long lines made of conducting material (see the technical specifications in Section *4.3*). The direct threat to a site's power system is that harmonics from a E3/GMD event could propagate into the distribution grid and damage the critical infrastructure's power system.

The intensity of the GMD impact from space weather increases with higher geomagnetic latitude which increases the risk of more intense induced ground electric fields. Similarly, the more resistive the ground (crust and mantle) is in the area, or the greater the lateral conductivity contrast is between one area and another, the higher the induced electric field levels. The 3-D variations in geoelectric conductivity structure is a primary factor in determining the induced E3/GMD electric field strength, so even equipment connected to long conductors in lower geomagnetic latitudes can be at significant risk if those areas have poor Earth conductivity.

References: See *Geomagnetic Storms and the US Power Grid*[200] presentation for a simulation of potential GMD impacts on the grid. See Geoelectric 3D-1D Comparison | NOAA / NWS Space Weather Prediction Center[201] for a comparison of ground electric fields using idealized 1-D ground conductivity models vs. real-world 3-D conductivity data.

E3 HEMP and GMD Impacts

E3 HEMP and GMD both induce large quasi-DC currents that can cause significant damage, including the following:

- Damage the electrical grid. This may be applicable to microgrids when there are multiple microgrids electrically networked together grouped into an **archipelago** interconnected by long power cables (more than 10 km at a minimum).
- Destabilize or damage a facility's backup power system due to AC harmonics from the electrical grid. UPSes and DC power supplies are vulnerable to damage from E3/GMD-caused harmonic waveforms.
- Induce damaging voltages on long telecommunications and data transmission lines containing conducting material.

Because E3 and GMD can damage high-voltage transformers (GMD has caused this in the past), any critical infrastructure stakeholder implementing an archipelago interconnected by long lines (over 10 km) should ensure high-voltage transformers (if used) are EMP protected by working with the applicable utility company and following DOE recommendations.

In addition to the grid related problems discussed above, the **AC voltage harmonics** generated by system transformers can propagate into the distribution grid and create harmonic voltage distortion at lower system voltages. These harmonics are known to disrupt facility UPSes and may damage them (more testing is needed). Harmonics might also prevent an enterprise site's backup power system from coming online (more testing is needed) and could damage some types of DC power supplies (rectifier units are particularly vulnerable to damage[202]). Also, there is evidence that large GW-class bulk power generators could also be susceptible to damage from line harmonics.[203]

The induced currents are lower in metal-based **telecommunications** lines (e.g., copper, fiber with metal in it) than in power lines as the resistance per unit length of these telecommunications cables is much higher than for power transmission cables. Although modern cables have voltage regulation on both ends and protective current limiters, substantial damage might be caused to a telecommunications network. For example, with a 5-ohm conductor and grounding system, a 100 km telecom line, and a peak E3 field of 25 V/km, there could be a current of 500 A, which could cause substantial damage.

Because of the above potential impacts, the best practices to mitigate these impacts are provided in *Section 4.3 E3 HEMP and GMD.*

SREMP

SREMP is an EM field that can be in the 100s of kV/m and extends to about 4 km from a nuclear near-surface burst. Long lines traversing the source region can conduct high currents to connected systems that are tens of miles distant from the nuclear burst. The low altitude causes SREMP to have significantly less area-of-coverage and typically much less overall impact than HEMP.

Nevertheless, there are time-urgent Level 4 resilience facilities that should implement SREMP mitigations partially because SREMP can impact hardened deeply buried systems. But since there are very few of those facilities and the management of those facilities typically have access to EMP experts, details of SREMP environments and protection are not covered in this document. The reader is referred to Glasstone 1977 NW Effects for more background on these threats.

Appendix D. REMOTE HOSPITAL SOLAR-BASED REHS USE CASE

This hospital use case, courtesy of muGrid Analytics, uses 2021 costs and benefits for a critical infrastructure hospital in the Pacific Northwest. This care facility sits just outside an anticipated tsunami danger zone and serves patients from a wide area which includes the tsunami zone as well as underserved, largely inaccessible rural areas. In the event of a tsunami, it is likely that the single grid feeder would be damaged leaving the hospital to island itself as it serves this remote community during a crisis. Although this use case is focused on a hospital including its communications and IT equipment, the lessons learned are applicable to many different types of critical infrastructure.

The hospital has been identified as critical infrastructure at a very high level and was already required by law to have onsite backup generators. As shown in Figure 26, the number of days that backup power could be maintained without external fuel supplies by adding a solar power system and a BESS to the existing generators more than doubled if needing nearly 100% confidence and almost doubled if just needing 50% confidence.

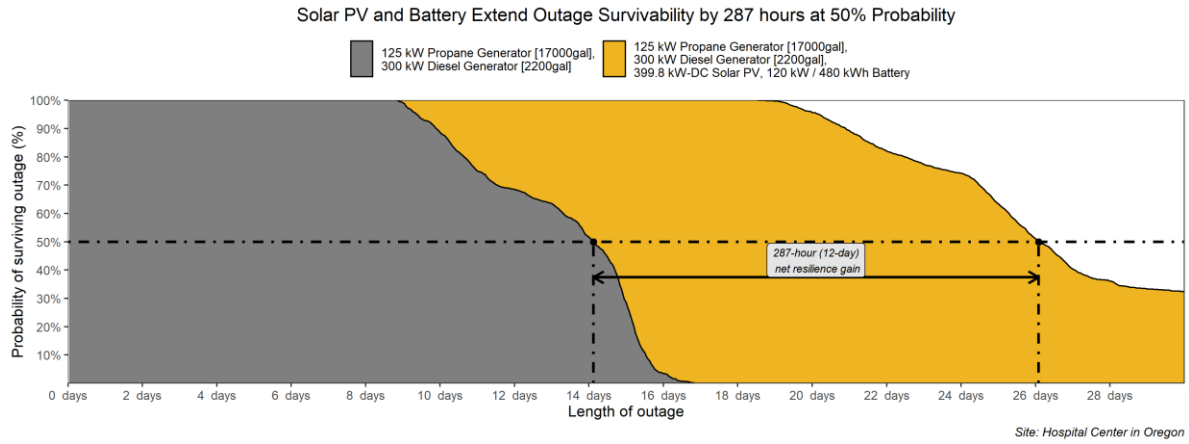

Figure 26. Site's power resiliency doubles with a REHS (courtesy of muGrid Analytics)

The microgrid REHS included the following:

- **Existing Power**: 300 kW diesel generator, 2200-gallon diesel fuel container; 175kW propane generator, 17,000-gallon propane tank.
- **Existing/Critical Load**: 340 kW peak, 300 kW average (load based upon actual load profile measured every 15 minutes over a year). The load is not segmented so the critical load is the same as the regular load.
- **Solar**: 399.8 kW DC Solar PV; 522.8 MWh produced per year. Using NREL 2021 standard cost estimates of $1.60/W, the solar capital cost is estimated at $640,000.
- **Solar Irradiance**: 15.1% capacity factor.
- **BESS**: 120 kW / 480 kWh BESS. Using NREL 2021 standard cost estimates of $840/kW and $420/kWh, the BESS capital cost is estimated at $300,000.
- **Microgrid O&M**: $9,000 per year (estimated for year 1). This includes annualized expenses like maintenance, software control subscriptions, monitoring, and insurance. It does not include expected equipment replacements or augmentation over the 25-year

project life. Equipment replacement is, however, included in the net present value (NPV) below.

- **Capital Cost (added PV/BESS only)**: Estimated $940,000
- **Incentives**: Incentives are not included in this analysis because the site is a not a tax paying entity. Tax credits and depreciation benefits would apply to projects owned by tax-paying entities. Other federal, state, and local incentives or grant funding may be available, but were not included in this analysis.
- **1st Year Electricity Savings**: $54,000 resulting from avoided energy purchases and reduced demand charges. This amount will change in future years based on the utility escalation rate (3%), the PV degradation rate (0.7%), and other factors.
- **NPV**: Excluding the resiliency benefits, the system's NPV is **-$85,000 u**sing a 25-year project lifespan.
    - Uses a discount rate of 3.9% and a utility escalation rate of 3%.
    - Includes all planned O&M expenses, both annual expenses and one-time equipment replacement, and augmentation over the 25-year project life.
    - A third-party investor or a private company could have received tax benefits from this project making the NPV positive and as high as $68,000 assuming a discount rate of 3.9% (this tends to be low for an investor).
    - With or without the tax benefits, this project was considered very worthwhile since the resiliency benefits far exceed the NPV.
- **Resiliency Benefit**:
    - The solar and storage system extended the amount of time that the site could survive an outage with 98% confidence to 19.5 days from 9.0 days with a generator-only solution.
    - The backup power operations improved 12.1 days from 14.1 days with a generator-only solution to 26.0 days with 50% confidence as shown in Figure 26.
    - The site considers itself at Level 3 resilience given that the REHS could provide approximately 20 days of power under all hazards and is very likely to provide 30 days between the fuel that is onsite and the likelihood that fuel could be delivered sometime within the first few weeks of power outage.
    - If the site were able to shed 20% of its normal loads as shown in Figure 27, the "all hazards" available fuel would effectively meet a requirement to have 30 of fuel stored onsite as defined in this document.

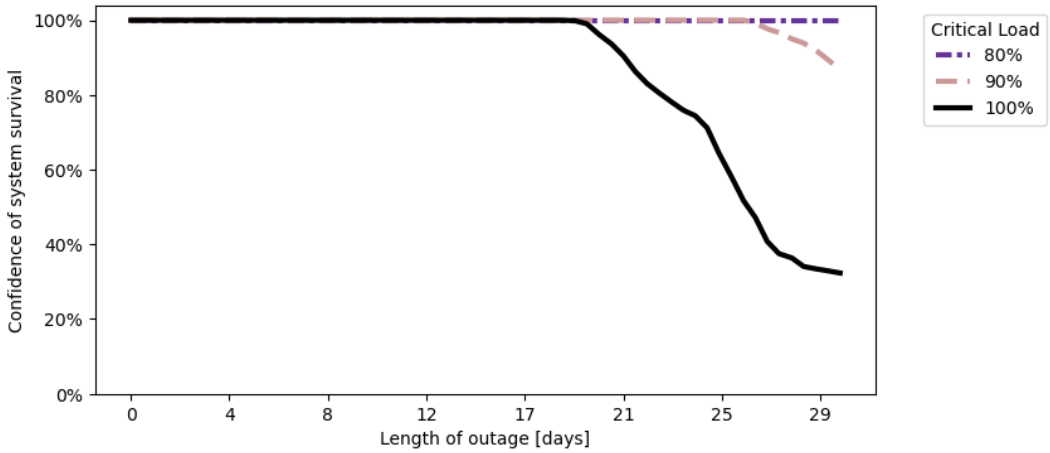

Figure 27. A small load reduction leads to Level 3 resilience (courtesy of muGrid Analytics)

Time to first microgrid system failure was simulated for outages occurring at every hour of the year to assess the resilience performance sensitivity to time of day and seasonality, using Typical Meteorological Year weather files. Time to first failure is defined as the point at which the generator fuel tanks are empty, and the solar plus storage is not able to meet the load. The existing generators provide longer duration, higher confidence in the winter than in the summer, as the summer load is higher due to HVAC demands although this is partially offset by the solar system providing more power during the summer.

Conclusion: Since this hospital has been designated as a critical facility for community support in case of an emergency, the decision makers believe that the improved power resiliency is worth significantly more than the $85,000 negative NPV over the 25-year project lifespan. Therefore, this use case, which is based upon an actual implementation, is economically viable even without grant money, tax credits, or the environmental benefits. With those benefits, it could become viable without the resiliency benefits.

Appendix E. NUCLEAR SMR VENDOR OFFERINGS

Per the World Nuclear Association, nuclear generation is expected to increase by 60% from 2018 to 2040.[204] The U.S. Nuclear Regulatory Commission (NRC) is tracking a number of water-cooled SMRs and advanced reactor technology designs, most of which offer the benefits and features listed in *Section 9.2 SMR Technical Details and Benefits*. Figure 28 identifies proposed new non-water coolant reactor designs, i.e., cooled by liquid metal sodium or lead, helium gas or molten liquid salt. Progress on these advanced design reactors has picked up in the last few years with several reactor vendors beginning pre-application discussions and one microreactor currently under formal review (Oklo's Aurora reactor).

The NRC is engaged with three SMR vendors proposing proven Light Water Reactor (LWR) technology who are seeking to develop projects before 2030. In 2020, NuScale received a Standard Design Approval for a 50 MWe LWR module design. It intends to seek approval for an uprate to 77 MWe per module for application to the UAMPS project in Idaho.

General Electric-Hitachi (GEH) BWRX-300 LWR SMR is pursuing NRC approval of several technical reports that could support a future construction permit authorization by the NRC. Holtec International is having pre-application discussions on technical reports to support its SMR-160 reactor design. The NRC is also working with the international community on nuclear regulatory and safety and providing regulatory assistance "particularly related to large light water and small modular reactor technology."[205]

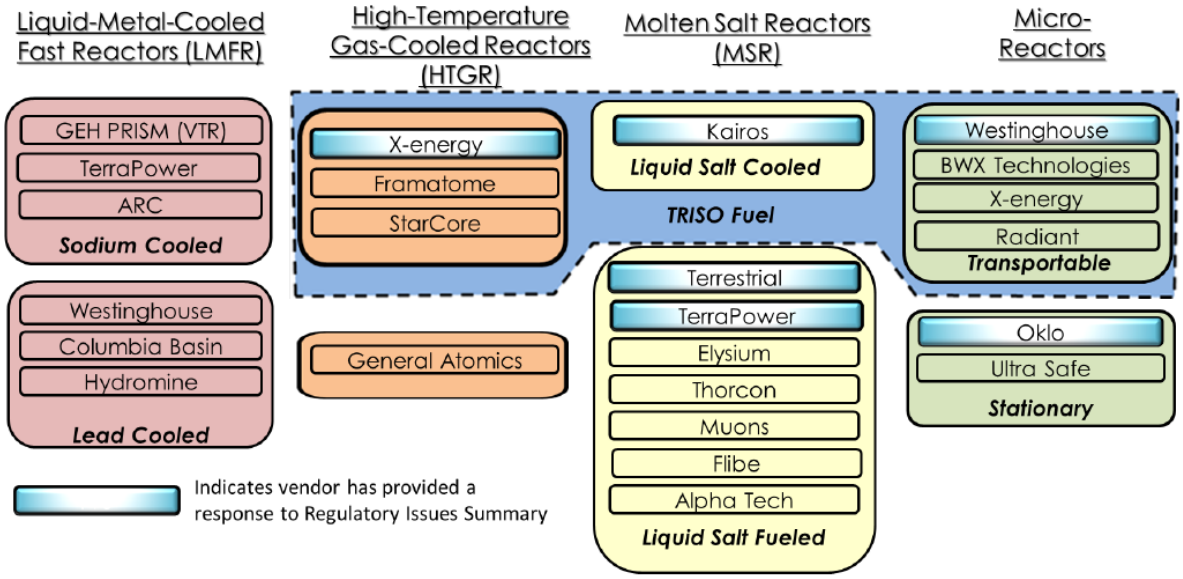

Figure 28. Broad landscape of non-LWR advanced reactor designs[206] (NRC)

The U.S. Department of Energy (DOE) plans to invest $3.2 billion over seven years in various reactor technologies. In October 2020, DOE announced the first of two Advanced Reactor Demonstration Program (ARDP) recipients as part of a multi-year program to develop and demonstrate advanced reactor concepts. The first award was $160 million in 1st year funding through a DOE cost-sharing (50/50) program to deploy two advanced reactors by 2027.[13] DOE selected TerraPower's Natrium reactor and X-energy's X-100 reactor with each receiving $80 million in initial funding. In December 2020, DOE issued additional cost-sharing awards to support five additional reactor designs for future demonstration, including: Holtec

International's SMR-160 reactor; the BWXT Advanced Nuclear Reactor (BANR) microreactor; Westinghouse's eVinci™ micro reactor; and two experimental test reactors, the Hermes Reduced-Scale Test Reactor by Kairos Power and the Molten Chloride Reactor Experiment (MCRE) by Southern Company.

More specifically, some of the SMR vendors closer to deployment are listed below in Table 25 (much of the below and above is courtesy of IP3 International and Allied Nuclear Partners). See *Section 9.2 SMR Technical Details and Benefits* for most of the features and benefits of SMRs and their general leadership from a levelized avoided cost of electricity (LACE) perspective.

Table 25. Sample SMR Vendors, Highlights, Costs, and Status

Vendor	Technical Highlights	Cost Information	Current Status
BWRX-300™ GEH (U.S.)	• Light water cooled, boiling water reactor. • 300 MWe • Significant reductions in capital costs, including 50% less concrete per MWe. • Significant reductions in operating, staff, maintenance cost, and security requirements.[12]	• Targeting $2,250/kW for NOAK (nth of a kind) implementations. [1207] • LCOE $44–$51/MWh[19]	• GE Hitachi Nuclear Energy is working with Ontario Power Generation to deploy a Small Modular Reactor (SMR) as early as 2028.[208]. • First licensing topical reports submitted to NRC. • Partners include Dominion Energy, Exelon, HGNE and MIT.
NuScale™ (U.S.)	• Light water cooled, pressurized water reactor • NRC approved 50 MWe modules, uprate to 77 • 77 MWe per reactor module, in 4, 6, 8 or 12-pack plant • Island mode capable. • A full 12-module plant is expected to require only 35 acres (with a buffer zone around the plant).	• 12-module plant deployment estimate is $2,850/kW[209] versus the global nuclear reactor cost of $5,587 per kW.[210] • LCOE $51–$54/MWh[19] • Operating and maintenance costs are expected to be lower than those of the top quartile of the current U.S. nuclear fleet."[211]	• In July 2022, the NRC voted to approve the design certification of NuScale's SMR.[212] • The first 77 MWe power plant is planned for delivery in 2027 and operational in 2029 with remaining modules coming online for full plant operation by 2030. • Can construct in as little as three years. • Has collaborative projects in nine countries including the U.S.[213]

Vendor	Technical Highlights	Cost Information	Current Status
X-100™ X-Energy[214] (U.S.)	• High temperature helium gas-cooled reactor (HTGR), with meltdown-proof design using TRISO fuel (*see SMR Technical Details and Benefits* for details regarding TRISO). • 80 MWe or 320 MWe (x4) with the "four-pack" plant fitting on 13 acres. • X-energy is also developing the X-1, a 1 MWe microreactor.	• Anticipated deployment cost share = $1.2B (DOE), $0.8B (Energy Northwest) and $0.3B (X-energy)[16] • Expected X-100 LCOE ~$50 per MWhr[16] • Safety benefits from using TRISO could reduce costs.	• Preliminary design of X-energy's TRISO-X Fuel Fabrication Facility was completed in November 2021.[215] • Final design and limited production for military microreactor demonstration is expected to start by late 2022.
Natrium™ TerraPower-GEH (U.S.)	• Sodium Cooled Fast Reactor (SFR) with an integrated molten salt Energy Storage System (ESS). • 345 MWe, with output up to 500 MWe during peak demand for 5.5 hours.[216] • Natrium consumes more of its fuel than traditional light water reactors producing about 80% less waste.[217] • Developing a Molten Chloride Fast Reactor (MCFR) using liquid salt as both fuel and coolant in the reactor core.	• No published cost data has been made publicly available, although the target capital cost for a commercial Natrium plant is $1 billion, according to TerraPower.[17]	• In June 2021, TerraPower reported its 345 MWe demonstration plant will be in Wyoming. • Targets a prototype TWR reactor in the mid-2020s with commercial production beginning in the late 2020s.
BWX Technologies (BWXT)	• Developing a transportable 50 MWth BWXT Advanced Nuclear Reactor (BANR) using TRISO fuel. • This fast reactor will achieve higher uranium loading and improved fuel utilization.	• Targets cutting lifecycle costs in half versus a traditional reactor.	• Sole manufacturer of naval nuclear reactors for U.S. submarines and aircraft carriers.[218] • Restarting TRISO manufacturing. • Under a DoD contract, it plans to ship a 1-5 MWe transportable microreactor in 2024 to the Idaho National Laboratory for testing.[219]

Other SMR and Advance Reactor Design offerings include the following:

- **ARC Energy**'s ARC-100 uses an inherently safe Sodium Cooled Fast Reactor of 100 MWe and has been selected by New Brunswick Power in Canada with a targeted completion date in the late 2020s.[220]

- **Elysium** is developing a Molten Chloride Salt Fast Reactor designed to produce variable output optionality from 50 -200 MWe, or scale to upwards of 400 MWe or even 1200 MWe. The fast reactor can recycle nuclear waste.[221]
- **Holtec International's** SMR-160 reactor has an expected output of 160 MWe with an outlet temperature of 316°C. The SMR-160 relies on traditional LWR technology and standard commercially available fuel that would extend refueling to every 42 months.
- **Kairos Power's** 140 MWe high efficiency reactor uses TRISO fuel and can be refueled while operating. Kairos is planning a reduced scale 50 MWe test reactor "Hermes" for initial demonstration in Oak Ridge, TN and is expected to be operational in 2026, partially funded by a $303 million DOE grant in 2020.[222] Its cost targets are competitive with natural gas in the U.S. electricity market.[223]
- **Moltex's** reactor is a 300 – 500 MWe inherently safe Molten Salt Reactor that can be fueled online and recycle spent fuel with plans to make it cheaper than coal or gas. It has completed the Vendor Design Review Phase 1 by the Canadian Nuclear Safety Commission (CNSC) and plans to build its first operational reactor with New Brunswick Power in the early 2030s.
- **Oklo** submitted an initial application to the NRC in March 2020 to build its first Aurora reactor that could generate 1.5 MW of power. It could run for 20 years on a single core of "high-assay, low-enriched uranium" or HALEU (uranium enriched anywhere from 5% to 20%) enabling it to provide more power in a very small, portable form factor.
- **Radiant**. Founded by former SpaceX engineers, Radiant is developing a portable 1 MWe High Temperature Gas Cooled microreactor designed to fit in a single shipping container and be operational within three days of delivery. Full scale demonstration is planned by 2026.[224]
- **Terrestrial Energy** uses an Integral Molten Salt Reactor (IMSR®) technology to generate 195 MWs per unit. It plans to commission its first power plant in 2028 working with Ontario Power Generation in Canada.[225]
- **Ultra Safe Nuclear's** Micro Modular Reactor (MMR) uses TRISO fuel pellets and has an estimated power output of 5 MWe or 15 Megawatts Thermal (MWth) for thermal heat applications. The MMR is currently under licensing review by the CNSC and plans to demonstrate the MMR at the Chalk River site in Ontario, Canada to produce electricity or heat.[226]
- **Westinghouse's** eVinci™ microreactor is transportable and can be installed on-site in less than 30 days. The 15 MW thermal reactor utilizes TRISO fuel and a specialized heat pipe design to flexibly operate in a grid or in remote locations. Westinghouse is targeting a prototype reactor by 2024 with full commercial deployment targeted for the mid-to-late 2020s.[227]

Appendix F. ACKNOWLEDGEMENTS

This *Resilient Power Best Practices for Critical Facilities and Sites* would not have been possible without the support of many federal, state, and local government departments and agencies, non-profits, and private industry. An initial rough draft of the document was originally created by CISA working with the federal interagency Continuity Communications Managers Group (CCMG). With the creation of CISA, it was decided that it would be within scope and very beneficial for the agency to provide much better resilient power best practices to critical communications infrastructure than were available. However, CISA needed the vast knowledge and hands-on experience of other departments and agencies, non-profits, and the private industry to make this a high-quality document and to gain buy-in. The support from the critical infrastructure and the nation's continuity community has far surpassed expectations.

CISA would like to thank and acknowledge those who attended at least four (4) RPWG meetings or significantly contributed outside of these meetings.

Participant	Department/Agency/Office/Title (optional)
Franklin Allgauer II	CISA National Risk Management Center (NRMC)
George H. Baker, Ph.D.	Executive Office of the President (EOP) National Security Council (NSC) (retired January 2021)
Chris Beck, Ph.D.	Electric Infrastructure Security (EIS) Council (nonprofit), Chief Scientist
Dan Bennett	Department of Energy (DOE) National Renewable Energy Laboratory (NREL)
Kathy Blasco	CISA Integrated Operations Division (IOD) Emergency Response Operations
Kevin Briggs	CISA IOD Senior Advisor for Telecommunications, Program Sponsor
Ryan Broughton	Bravo Team Solutions, LLC (Emergency Management Consulting)
Malgorzata Brzakalska	National Cancer Institute (NCI), Emergency Planner
Chris Cannizzaro, PhD	EOP NSC
Timothy A. Carty	EMP Shield, Founder
Stephen Cauffman	CISA Infrastructure Security Division (ISD)
Bethany Cecere*	NRC Office of Nuclear Security and Incident Response
Michael L. Cohen, Ph.D.	MITRE/Homeland Security Systems Engineering and Development Institute (HSSEDI)
Dana Davidson	DoD Defense Logistics Agency (DLA)
Paul Detitta	General Services Administration (GSA) Continuity Policy Lead
Plamen Doynov, Ph.D.	EMP Shield Chief Technology Officer (CTO)
Robert (Beau) Finley	Federal Communications Commission (FCC)
Amanda Mosle Friedman	IP3 International
Scott Gromer	Mesa Natural Gas Solutions, Chief Executive Officer (CEO)
Michael Hainzl, CBCP*	Power Solutions Manager, Generac Power Systems
Bill Harris	InfraGard National Disaster Resilience Council Vice Chairman (nonprofit)
Barry Herman	Office of Science and Technology Policy (OSTP)
Thomas Herrity*	NRC Nuclear Security and Incident Response
RDML Mike Hewitt	CEO, IP3 Corp.

Participant	Department/Agency/Office/Title (optional)
Georgette Holmes	CISA NRMC
Eliza Hotchkiss	DOE NREL
Mark Jones	Jacobs, Senior Technical Advisor, CISA IOD Emergency Response Operations Support, Primary Author and Editor
Donald Junta	United States Department of Agriculture (USDA) Rural Utilities Service – Electric
Tom Kendzia*	NRC Office of Nuclear Security and Incident Response
Michael Kilmartin	CISA IOD OPRC Business Continuity & Emergency Preparedness
Jesse Kirchmeier	Wyoming Department of Transportation (DOT) Emergency Response Planner
Brig Gen Robert Korte	Jacobs, CISA IOD Support
Frank Koza, P.E.*	EIS Council (nonprofit)
Bob Kravinsky	DoD Energy Resilience
Mary Lasky	InfraGard National Disaster Resilience Council Chairwoman (nonprofit)
James Lawton	CISA IOD Continuity Program Manager (PM), Program Sponsor
Jim LeBlanc	Chair Louisiana Grid Coalition (nonprofit)
Jody Little	Southwest Research Institute (nonprofit)
Arthur Lord	DoD OUSD (Policy) for Homeland Defense and Global Security
Jules LoRusso	FEMA Hazard Mitigation (reservist), Roush Industries, Inc. (part time)
Brig Gen Michael J. Lovell	Executive Director, Joint Base San Antonio's EM Defense Initiative (EDI)
Mark Macalester	CISA IOD Liaison to NORTHCOM
Sarah Mahmood	DHS Science and Technology (S&T) Directorate
Gabriel Martinez	CISA Emergency Communications Division Senior Electronics Engineer
Gabriel Mata	FEMA National Continuity Programs
Robert McFadden	City of Phoenix Water Facility Supervisor-Electrical/Instrumentation
Sara Mroz*	Executive Office of the President, NSC Resiliency, NRC
Henry Newton, P.E.	NDRC Member and Founding President of New Orleans InfraGard
Dave Nolan	CISA Emergency Communications Division (ECD) PM
John O'Connor	CISA IOD National Coordinating Center for Communications (NCC) Director
Edward J Ohlert	CISA IOD SHARES Program Support
John Organek, P.E.	EIS Council, Director, Program Planning and Operational Architecture
Tom Patterson	Executive Director, National Cyber Moonshot Inc.
Ben Pisarcik	GSA, Public Building Service, Office of Design and Construction
Tom Pitotti	FEMA, Chief, Engineering Branch, Facilities Management Div.
Tom Poteet	Mesa Natural Gas
Mojo Raheem	Health and Human Services (HHS) Preparedness and Response
Maj Gen (ret.) Luke Reiner	Wyoming DOT, Director of Transportation
Bill Rhodes	DOE National Nuclear Security Administration (NNSA) Support
Richard Rodriguez	University of Texas at San Antonio, National Security Collaboration Center

Participant	Department/Agency/Office/Title (optional)
Dale Rowley	Maine Waldo County Emergency Management
Bill Ryan	CISA IOD Emergency Response Operations Branch, Program Sponsor
Vince Saporita	Saporita Consulting
Amy Simpkins	muGrid Analytics CEO
Travis Simpkins, Ph.D.	muGrid Analytics Chief Technology Officer (CTO)
LtCol Eddie (Thumper) Stamper	USAF, Mission Coordinator, Joint Base San Antonio (JBSA)-Electromagnetic Defense Initiative
David C. Stoudt, Ph.D.	Booz Allen Hamilton, Engineering Fellow for Directed Energy
John Twitchell, P.E.	EIS Council (nonprofit)
Tommy Waller	The Center for Security Policy (nonprofit)
David Walter, P.E.	DOE Solar Energy Technologies Office
Kevin Walz	Jacobs, CISA IOD Support
Troy Warshel	DoD Office of the Deputy Assistant Secretary of Defense for Energy
Mike Wendling	CISA ECD
Sunny Wescott	CISA ISD-IOD Meteorologist
Matthew West	Elgin Texas Independent School District, Director of Safety and Risk Management
Greg White, Ph.D.	UTSA, Director of the Center for Infrastructure Assurance and Security
Larry Willis	CISA NRMC
David Winks	AcquSight, Managing Director
Lauren Wisniewski	Environmental Protection Agency (EPA), Water Security Division
Warren Youngblood	CISA IOD Business Continuity and Emergency Preparedness office

* Note: (1) NRC members did not participate in the Nuclear Small Modular Reactor (SMR) chapter to ensure their independence from any material advocating for or against nuclear usage. (2) P.E. = Professional Engineer, (3) CBCP = Certified Business Continuity Professional

Although it is difficult to select just a few entities for appreciation given the many contributions from the above entities, we first want to express our gratitude to the U.S. Department of Energy for its many detailed comments and guidance throughout the development of the report. We also want to extend a particular thank you to our federal and state partners such as the DoD and Wyoming DOT, as well as the nonprofit organizations EIS Council, Center for Security Policy, and InfraGard for their numerous contributions.

Also, a sincere thank you is extended to CISA's Integrated Operations Division (IOD) including Kevin Briggs, Bill Ryan, and John O'Connor for sponsoring this project. And a special thank you to James Lawton of IOD, who not only sponsored the project, but who enthusiastically and quickly helped remove roadblocks and resolve many issues. Lastly, we want to remember the contributions of Bill Harris of InfraGard who lost the fight to a brutal pandemic in April 2021. He enthusiastically provided an amazing amount of input and was always on the lookout for how the document might be improved.

Appendix G. ACRONYMS

A	Amperes
AC	Alternating Current
AI	Artificial Intelligence
ATS	Automatic Transfer Switch
B	Billion
BESS	Battery Energy Storage System
BWXT	BWX Technologies
C2M2	Cybersecurity Capability Maturity Model
CAGR	Compound Annual Growth Rate
CBCP	Certified Business Continuity Professional
CCMG	Continuity Communications Managers Group
CISA	Cybersecurity and Infrastructure Security Agency
CMMC	Cybersecurity Maturity Model Certification
CNG	Compressed Natural Gas
COG	Continuity of Government
CERT	Community Emergency Response Team
COOP	Continuity of Operations
COTS	Commercial Off The Shelf
CSP	Concentrating solar-thermal power
CSRIC	Communications Security, Reliability, and Interoperability Council (CSRIC)
dB	Decibels
DC	Direct Current
DER	Distributed Energy Resource
DHS	Department of Homeland Security
DLA	Defense Logistics Agency
DOD	Department of Defense
DOE	Department of Energy
DOT	Department of Transportation
EaaS	Energy-as-a-Service
ECD	Emergency Communications Division (within CISA)
EIA	US Energy Information Administration

EIS	Electric Infrastructure Security
EM	Electromagnetic
EMA	Emergency Management Agency
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EMP	Electromagnetic Pulse
EO	Executive Order
EPA	Environmental Protection Agency
EPRI	Electric Power Research Institute
ERCOT	Electric Reliability Council of Texas
ESF	Emergency Support Function
ESS	Energy Storage System
EV	Electric Vehicle
FBR	Fast Breeder Reactor
FCC	Federal Communications Commission
FERC	Federal Energy Regulatory Commission
FEMA	Federal Emergency Management Agency
FirstNet	First Responder Network Authority
FMCSA	Federal Motor Carrier Safety Administration
FMEA	Failure Modes and Effects Analysis
FOUO	For Official Use Only
GEO	Geosynchronous Earth Orbit
Gen	Generation
GETS	Government Emergency Telecommunications Service
GHI	Global Horizontal Irradiance
GMD	Geomagnetic Disturbance
GSA	General Services Administration
GWe	Gigawatts of Electrical Output
GWh	Gigawatt Hours
HALEU	High Assay Low Enriched Uranium
HEMP	High-Altitude Electromagnetic Pulse
HF	High Frequency
HHS	Department of Health and Human Resources

HVAC	Heating, Ventilation, and Air Conditioning
ICS	Industrial Control System
IEC	International Electrotechnical Commission
IEMI	Intentional Electromagnetic Interference
IOD	Integrated Operations Division (within CISA)
ISAC	Information Sharing and Analysis Centers
ISD	Infrastructure Security Division (within CISA)
IT	Information Technology
INL	Idaho National Laboratory
km	kilometer
kV	Kilovolt
kW	Kilowatt
kWh	Kilowatt-hour
LACE	Levelized Avoided Cost of Electricity
LCOE	Levelized Cost of Electricity
LEO	Low Earth Orbit
LES	Local Energy Storage
LEU	Low Enriched Uranium
LED	Light Emitting Diode
LMR	Land Mobile Radio
LNG	Liquefied Natural Gas
LTO	Long-Term Outage
LWR	Light Water Reactor
M	Meter
MEO	Medium Earth Orbit
MSR	Molten Salt Reactor
MT	Magneteulliric
MTBF	Mean Time Between Failures
MW	Megawatt
MWh	Megawatt-hours
MWe	Megawatts of Electrical Output
MWth	Megawatts Thermal
NCC	National Coordinating Center for Communications

NCS	National Communications System
NDRC	National Disaster Resilience Council (InfraGard)
NEF	National Essential Function
NRC	Nuclear Regulatory Commission
NYC	New York City
NERC	North American Electric Corporation
NFPA	National Fire Protection Agency
NIAC	National Infrastructure Advisory Council
NIMS	National Incident Management System
NIST	National Institute for Standards and Technology
NPV	Net Present Value
NRC	Nuclear Regulatory Commission
NRF	National Response Framework
ns	Nanoseconds
NSC	National Security Council
NS/EP	National Security/Emergency Security
NREL	National Renewable Energy Laboratory
O&M	Operations and Maintenance
PNT	Position, Navigation and Timing
POETE	Planning, Organization, Equipment, Training, and Exercises
POTS	Plain Old Telephone System (wireline)
PPD	Presidential Policy Directive
P.E.	Professional Engineer
PV	Photovoltaic
R&D	Research and Development
REHS	Renewable Energy Hybrid System
RF	Radio Frequency
RFP	Request for Proposal
RFQ	Request for Quotation
RPWG	Resilient Power Working Group
SBU	Sensitive But Unclassified
SCADA	Supervisory Control and Data Acquisition
SHARES	SHAred RESources

SMR	Small Modular Nuclear
SOFC	Solid Oxide Fuel Cell
SP	Special Publication
SPD	Surge Protection Device
SREMP	Source Region Electromagnetic Pulse
SRMA	Sector Risk Management Agency
SGEMP	System Generated Electromagnetic Pulse
STO	Short-Term Outage
TCO	Total Cost of Ownership
TRISO	Tri-structural Isotropic
TSP	Telecommunications Service Priority
UAV	Unmanned Aerial Vehicles
UCO	Oxycarbide
UNECE	United Nations Economic Commission for Europe
USACE	United State Army Corps of Engineers
UPS	Uninterruptible Power Supply
U.S.	United States
UTSA	University of Texas at San Antonio
USB	Universal Serial Bus
V	Volts
VLRA	Valve Regulated Lead Acid
WPS	Wireless Priority Service

Appendix H. REFERENCES

1 FEMA, Glossary, https://training.fema.gov/programs/emischool/el361toolkit/glossary.htm (11/17/2021)

2 FEMA, Continuity Resource Toolkit, https://www.fema.gov/emergency-managers/national-preparedness/continuity/toolkit, (11/17/2021)

3 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

4 CISA, Resilient Power Working Group website, https://www.cisa.gov/resilient-power-working-group (11/17/2021)

5 National Security Telecommunications Advisory Committee (NSTAC) Report to the President on Telecommunications and Electric Power Interdependencies: The Implications of Long-Term Outages on the Implications of Long-Term Outages, December 2006

6 Kristina Hamachi LaCommare , Joseph H. Eto, Laurel N. Dunn, and Michael D. Sohn, Improving the Estimated Cost of Sustained Power Interruptions to Electricity Customers (June 2018), DOE Lawrence Berkeley National Laboratory, https://eta-publications.lbl.gov/sites/default/files/copi_26sept2018.pdf

7 116th Congress, S.4049, https://www.congress.gov/116/bills/s4049/BILLS-116s4049es.pdf

8 IBID, pages 1-2

9 FEMA, Power Outage Incident Annex to the Response and Recovery Federal Interagency Operational Plans, Managing the Cascading Impacts from a Long-Term Power Outage (June 2017)

10 Patrick Svitek, Texas puts final estimate of winter storm death toll at 246 (1/2/2022), The Texas Tribune, https://www.texastribune.org/2022/01/02/texas-winter-storm-final-death-toll-246/

11 Yevgeniy Sverdlik, Most Texas Data Centers Weathered the Storm, But Things Did Not Go Smoothly (3/8/2021), Data Center Knowledge, https://www.datacenterknowledge.com/uptime/most-texas-data-centers-weathered-storm-things-did-not-go-smoothly

12 Jeremy Rogalski, City: 20% of back-up water generators failed during winter storm | khou.com (5/16/21)

13 Yevgeniy Sverdlik, Most Texas Data Centers Weathered the Storm, But Things Did Not Go Smoothly (3/8/2021), Data Center Knowledge, https://www.datacenterknowledge.com/uptime/most-texas-data-centers-weathered-storm-things-did-not-go-smoothly

14 FCC, 2017 Atlantic Hurricane Season Impact on Communications Report and Recommendations Public Safety Docket No. 17-344, A Report of the Public Safety and Homeland Security Bureau Federal Communications Commission August 201 (p. 17), https://docs.fcc.gov/public/attachments/DOC-353805A1.pdf

15 Mary Lasky, et al, Powering Through: Building Critical Infrastructure Resilience (11/12/2020)

16 Ajit Pai, Commissioner Pai Statement on Superstorm Sandy | Federal Communications Commission (fcc.gov) (2/5/2013)

17 John Wohlstetter, Katrina: The Sounds of Communications Silence | Discovery Institute

18 History.com Editors, The Great Northeast Blackout - HISTORY (updated 11/9/2021)

19 NERC, August 2003 Northeast Blackout, https://www.nerc.com/pa/rrm/ea/Pages/Blackout-August-2003.aspx

20 Dr. Sten Odenwald, The Day the Sun Brought Darkness | NASA (5/13/2009)

21 Evan Halper and Marc Lifsher, *Attack on California Electric Grid Called 'Terrorism' (govtech.com)* (2/14/2014), McClatchy News

22 Bill Whitaker, 60 Minutes, *Vulnerable U.S. electric grid facing threats from Russia and domestic terrorists - 60 Minutes - CBS News* (8/28/2022)

23 DOE Office of Electricity, Addressing Security and Reliability Concerns of Large Power Transformers (7/11/18), https://www.energy.gov/oe/activities/addressing-security-and-reliability-concerns-large-power-transformers

24 Jerry Emanuelson, An Introduction to Nuclear Electromagnetic Pulse (7/11/2018), Future Science, http://www.futurescience.com/emp.html

25 CISA, National Critical Function Set, https://www.cisa.gov/national-critical-functions-set (11/22/2021)

26 FEMA, Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) Guide, https://www.fema.gov/sites/default/files/2020-04/CPG201Final20180525.pdf

27 CISA, National Critical Functions Set, https://www.cisa.gov/national-critical-functions-set (12/15/2021)

28 Jack Baylis, et al., Water Sector Resilience Final Report and Recommendations (June 2016), National Infrastructure Advisory Council, https://www.cisa.gov/publication/niac-water-sector-resilience-final-report

29 29148-2018 ISO/IEC/IEEE International Standard - Systems and software engineering -- Life cycle processes -- Requirements engineering

[30] FEMA, How to Build a Kit for Emergencies (6/12/2020), https://www.fema.gov/press-release/20210318/how-build-kit-emergencies

[31] CSRIC Best Practice 12-10-0492, Network Operators, Property Managers, and Public Safety should provide back-up power (e.g., some combination of batteries, generator, fuel cells) at cell sites and remote equipment locations, consistent with the site-specific constraints, criticality of the site, the expected load and reliability of primary power, https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data

[32] https://www.apcointl.org/services/standards/find-standards/

[33] CSRIC Best Practices, https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t; CSRIC V, Working Group 6, Secure Hardware and Software: Security-By-Design Final Report (March 2016), https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG6_Final_091416.docx

[34] Holli Riebeek, Catalog of Earth Satellite Orbits (9/4/2009), NASA, https://earthobservatory.nasa.gov/features/OrbitsCatalog

[35] Seth Fiegerman, It's been 9 days. Puerto Rico has almost no cell service (cnn.com) (9/29/2017)

[36] CISA, Cybersecurity and Physical Security Convergence, https://www.cisa.gov/publication/cybersecurity-and-physical-security-convergence (5/10/2022)

[37] Staying wary of cyber attacks shows vision (8/22/2018), Altoona Mirror, http://www.altoonamirror.com/opinion/editorials/2018/08/staying-wary-of-cyber-attacks-shows-vision/

[38] CISA, Alert AA20-049A Ransomware Impacting Pipeline Operation, https://www.us-cert.gov/ncas/alerts/aa20-049a?mod=article_inline

[39] Joe Weiss,Q&A: Joe Weiss of Applied Control Solutions on Control Systems and Cybersecurity (threatconnect.com) (8/2/2021) https://www.cerias.purdue.edu/news_and_events/events/security_seminar/details/index/64bqh1s3sul9mikcpufrihevrf

[40] DHS Science and Technology Directorate, Study on Mobile Security (April 2017), https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf

[41] CISA, https://www.cisa.gov/publication/communications-resiliency (12/9/2021)

[42] CISA, https://www.911.gov/pdf/OEC_NG911_Cybersecurity_Primer_May_2018.pdf (12/9/2021)

[43] Matthew P. Barrett, NIST, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (4/16/2018), https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11

[44] Grace Dille, Wales, CISA, *Federal Officials Urge Widespread Migration to Zero Trust Model – MeriTalk* (1/13/21)

[45] Scott Rose (NIST), Oliver Borchert (NIST), Stu Mitchell (Stu2Labs), Sean Connelly (CISA), NIST SP 800-207, Zero Trust Architecture (August 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[46] CISA, Zero Trust Maturity Model v1.0 (June 2021), https://www.cisa.gov/publication/zero-trust-maturity-model

[47] CISA, Recommended Cybersecurity Practices for Industrial Control Systems, https://www.cisa.gov/sites/default/files/publications/Cybersecurity_Best_Practices_for_Industrial_Control_Systems.pdf (12/7/2021)

[48] Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, CISA Industrial Control Systems Cyber Emergency Response Team (September 2016), https://us-cert.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

[49] Ron Ross et al., Developing Cyber-Resilient Systems: A Systems Security Engineering Approach (December 2021), NIST/MITRE, https://csrc.nist.gov/publications/detail/sp/800-160/vol-2-rev-1/final

[50] Alan Grau, PQShield, When it comes to securing systems against quantum computers, there is no one-size-fits-all solution (11/15/2021), (In)Secure Magazine, https://www.helpnetsecurity.com/2021/11/15/securing-systems-against-quantum-computers/

[51] CISA and NIST, Defending Against Software Supply Chain Attacks (April 2021) https://www.cisa.gov/publication/software-supply-chain-attacks

[52] Robert Walton, DOE lists China, 5 other 'foreign adversaries' as it asks how to enforce Trump's grid security order (7/10/2020), UtilityDive, https://www.utilitydive.com/news/doe-lists-china-5-other-foreign-adversaries-as-it-asks-how-to-enforce-tr/581369/

[53] FERC and NERC, Joint Staff White Paper on Supply Chain Vendor Identification - Noninvasive Network Interface Controller (7/31/2020), https://www.nerc.com/pa/comp/CAOneStopShop/Joint%20Staff%20White%20Paper%20on%20Supply%20Chain_07312020.pdf

[54] NIST, SP 800-171 Rev. 2 “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

[55] Acquisition & Sustainment, Office of The Undersecretary of Defense, CMMC 2.0, https://www.acq.osd.mil/cmmc/ (12/13/2021)

[56] One Hundred Fifteenth Congress of the United States of America, H.R. 5515, Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment, (1/3/2018)

[57] List of Equipment and Services Covered By Section 2 of The Secure Networks Act | Federal Communications Commission (fcc.gov)

[58] Matt Barrett Jeff Marron Victoria Yan Pillitteri Jon Boyens Stephen Quinn Greg Witte Larry Feldman, NISTIR 8170 Approaches for Federal Agencies to Use the Cybersecurity Framework, NIST, https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8170.pdf

[59] CISA, Cyber Resiliency Resources for Public Safety, https://www.cisa.gov/publication/communications-resiliency

[60] DOE, Cybersecurity Capability Maturity Model (C2M2) (July 2021), https://c2m2.doe.gov/C2M2%20Version%202.0%20July%202021.pdf

[61] GSA, P100 Facilities Standards for The Public Buildings Service (October 2021), https://www.gsa.gov/real-estate/design-construction/engineering-and-architecture/facilities-standards-p100-overview

[62] https://msc.fema.gov/portal/home (12/13/2021)

[63] FEMA's National Flood Hazard Layer (NFHL) Viewer (arcgis.com), https://hazards-fema.maps.arcgis.com/apps/webappviewer/index.html (12/13/2021)

[64] Interagency Security Committee, The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard, 2nd Edition (November 2016), https://www.cisa.gov/sites/default/files/publications/isc-risk-management-process-2016-508.pdf

[65] ANSI/APCO, ANS 2.106.1-2019 *Public Safety Grade Site Hardening Requirements* (2019), *https://www.apcointl.org/standards/standards-to-download/*

[66] NRC, *Physical Security Best Practices for the Protection of Risk-Significant Radioactive Material (NUREG-2166) (May 2014).* https://www.nrc.gov/docs/ML1415/ML14150A382.pdf

[67] 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

[68] 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

[69] Glasstone, USG Book, Nuclear Weapon Effects, 1977

[70] IEC, IEC/TS 61000-2-10, Electromagnetic compatibility (EMC) – Part 2-10: Environment – Description of HEMP environment – Conducted disturbance. Basic EMC publication, Edition 1.0 (1998-11)

[71] Dan Brouillette (Secretary of Energy), Physical Characteristics of HEMP Waveform Benchmarks for Use in Assessing Susceptibilities of the Power Grid, Electrical Infrastructures, and Other Critical Infrastructure to HEMP Insults, For National Security Council Records (1/11/2021), https://www.energy.gov/sites/prod/files/2021/01/f82/FINAL%20HEMP%20MEMO_1.12.21_508.pdf

[72] ANSI/APCO, ANS 2.106.1-2019 *Public Safety Grade Site Hardening Requirements* (2019), *https://www.apcointl.org/standards/standards-to-download/*

[73] ANSI/APCO, ANS 2.106.1-2019 *Public Safety Grade Site Hardening Requirements* (2019), *https://www.*apcointl*.org/standards/standards-to-download/*

[74] NFPA, Standard for the Installation of Lightning Systems (2020), https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=780

[75] UL, Standard for Surge Protection Devices (1/8/2021), https://standardscatalog.ul.com/ProductDetail.aspx?productId=UL1449

[76] Serge Stroobandt, World Atlas of Ground Conductivity (7/22/2020), https://hamwaves.com/ground/en/index.html

[77] Pete Riley, On the probability of occurrence of extreme space weather events (February 2014), Space Weather, https://science.nasa.gov/science-news/science-at-nasa/2014/23jul_superstorm/

[78] IEEE 519-2014 - IEEE Recommended Practice and Requirements for Harmonic Control in Electric Power Systems (6/11/2014), https://standards.ieee.org/standard/519-2014.html

[79] TSWG and Deto Publication, The Threat of Radio Frequency Weapons to Critical Infrastructure Facilities, DoD (Aug 2005), https://apps.dtic.mil/dtic/tr/fulltext/u2/a593293.pdf

[80] CISA, Radio Frequency Interference Best Practice Guidebook (2020), https://www.cisa.gov/publication/communications-resiliency

[81] Boeing, CHAMP – Lights Out (10/22/2012), http://www.boeing.com/features/2012/10/bds-champ-10-22-12.page

[82] Caterpillar, Understanding Generator Set Ratings (6/29/20), https://www.cat.com/en_US/by-industry/electric-power-generation/Articles/White-papers/understanding-generator-set-ratings.html

[83] Sean Ericson and Dan Olis, A Comparison of Fuel Choice for Backup Generators (p. 8) (March 2019), Joint Institute for Strategic Energy Analysis, DOE National Renewable Energy Laboratory (NREL)

[84] Army and Navy, Electric Power Generation and Distribution (July 2018) p. 2-1, https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN10584_ATP%203-34x45%20FINAL%20WEB.pdf

[85] Grand View Research, Natural Gas Generator Market Size, Share & Trends Analysis Report By Rating (Low Rating, Medium Rating, High Rating), By Application (Industrial, Residential, Commercial), And Segment Forecasts, 2019 – 2025 (Dec 2019), https://www.grandviewresearch.com/industry-analysis/natural-gas-generator-market

[86] EPA, Renewable Natural Gas, https://www.epa.gov/lmop/renewable-natural-gas (12/14/2021)

[87] MarketsandMarkets, Portable Generator Market Worth 2.28 Billion USD by 2022 (1/11/2018), https://www.prnewswire.com/news-releases/portable-generator-market-worth-228-billion-usd-by-2022-668796063.html

[88] Technavio, Compressed Natural Gas (CNG) Market 2020-2024 | Increase in the Number of CNG Vehicles to Boost Growth | Technavio (3/13/2020), https://www.businesswire.com/news/home/20200313005221/en/

[89] Generac Power Systems, Total Cost of Ownership Diesel vs. Natural Gas Generators, White Paper, http://gensetservices.com/wp-content/uploads/2017/11/TCO-_diesel_vs_natural_gas_generators.pdf

[90] Fernando Carou, Minimum Backup Power Guidelines for MURBs (p. 11), City of Toronto (Oct 2016)

[91] The Importance of Fuel Maintenance for Emergency Standby Generators, Authorized Services of New England (ASNE), http://www.asne.com/the-importance-of-fuel-maintenance-for-emergency-standby-generators/

[92] IBID

[93] Mike Hainzl, Generac Power Systems, Standby Power Generation Fuel Security – Diesel vs. Natural Gas (2017), https://www.generac.com/industrial/download?pdf=Generac-Industrial-Power-Whitepaper-Standby-Power-Generation-Fuel.pdf

[94] Sean Ericson and Dan Olis, A Comparison of Fuel Choice for Backup Generators, NREL (March 2019)

[95] Mark Costis, Generator Fuel: Is Natural Gas or Diesel Better?, Generx Generators (12/15/2016), https://generxgenerators.com/2016/12/15/natural-gas-vs-diesel-generators/

[96] Authorized Services of New England (ASNE), The Importance of Fuel Maintenance for Standby Generators, http://www.asne.com/the-importance-of-fuel-maintenance-for-emergency-standby-generators/ (2/3/2020)

[97] Dr. Stockton et al, E-PRO Handbook II Volume 1\Fuel, CIS Council (March 2017), p. 96

[98] BP, Fuel News: Long Term Storage of Diesel, https://www.bp.com/content/dam/bp-country/en_au/media/fuel-news/long-term-storage-diesel.pdf (2/4/2020)

[99] Authorized Services of New England (ASNE), The Importance of Fuel Maintenance for Standby Generators, http://www.asne.com/the-importance-of-fuel-maintenance-for-emergency-standby-generators/ (2/3/2020)

[100] EPA, Power Resilience Guide for Water and Wastewater Utilities (June 2019) (p. 3-1), https://www.epa.gov/sites/production/files/2016-03/documents/160212-powerresilienceguide508.pdf

[101] FEMA, Power Outage Incident Annex to the Response and Recovery Federal Interagency Operational Plans, Managing the Cascading Impacts from a Long-Term Power Outage (June 2017)

[102] Woodstock Power Company, Natural Gas Generator Maintenance: How To Be Prepared, https://woodstockpower.com/blog/natural-gas-generator-maintenance-how-to-be-prepared/ (2/10/2020)

[103] Generac, Preventative Maintenance Fact Sheet, https://www.generac.com/Industrial/GeneracIndustrialPower/media/library/Downloads/Generator-Maintenance-Fact-Sheet.pdf (9/21/2021)

[104] EPA, Power Resilience Guide for Water and Wastewater Utilities (June 2019) (p. 3-9), https://www.epa.gov/sites/production/files/2016-03/documents/160212-powerresilienceguide508.pdf

[105] Riggins, Superstorm Sandy Petroleum Shortage After-Action Report, https://rigginsoil.com/wp-content/uploads/2013/02/Sandy-After-Action-Report.pdf (12/19/2012)

[106] FEMA, Emergency Support Function #12 – Energy Annex (January 2008), https://www.fema.gov/pdf/emergency/nrf/nrf-esf-12.pdf

[107] DLA Energy, Direct Delivery Fuels: Commercial Specification Fuels (4/16/20), https://www.dla.mil/Energy/Offers/Products/DirectDeliveryFuels/

[108] EIS Council, Electric Protection Infrastructure Initiative (EPRO) Black Sky Systems Engineering Process, p. 10 (no date is provided)

[109] FEMA, Emergency Support Function #7 – Logistics Annex (June 2016), https://www.fema.gov/media-library-data/1470149740861a43de89d07026b4be5790cb20b84872c/ESF_7_Logistics_20160705_508.pdf

[110] FEMA, Healthcare Facilities and Power Outages Guidance for State, Local, Tribal, Territorial, and Private Sector Partners (August 2019), https://www.fema.gov/media-library-data/1566392446802-cb3f4603ff821158811d3f55f370238e/Healthcare_Facilities_and_Power_Outages.pdf

[111] George H. Baker, Microgrids — A Watershed Moment, INCOSE June 2020 Volume 23/ Issue 2

[112] Microgrid Knowledge, Microgrid Drivers and Obstructions: What's Moving the Dial on the Market?, https://microgridknowledge.com/microgrid-drivers-schneider/

[113] Berkeley Lab (8/10/2018), https://building-microgrid.lbl.gov/microgrid-definitions

[114] Figure courtesy of CISA and The Resilient Power Working Group (RPWG) including Mesa Natural Gas Solutions and muGrid Analytics, Sept 2020

[115] Preeti Wadhwani, Saloni Gankar, UPS Market Size & Share 2020-2026 | Forecast Report, (May 2020), Global Market Insights, https://www.gminsights.com/industry-analysis/ups-market

[116] Sunpower Electronics, https://www.sunpower-uk.com/glossary/what-is-transfer-time/ (8/28/2018)

[117] NERC, Reliability Guideline: Performance, Modeling, and Simulations of BPS-Connected Battery Energy Storage Systems and Hybrid Power Plants (March 2021), https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Reliability_Guideline_BESS_Hybrid_Performance_Modeling_Studies_.pdf

[118] MarketsAndResearch, Worldwide Battery Energy Storage System Industry to 2025 - COVID-19 Impact Analysis, Markets Insider (10/16/2020), https://markets.businessinsider.com/news/stocks/worldwide-battery-energy-storage-system-industry-to-2025-covid-19-impact-analysis-1029687653#

[119] Shaun Harris, Microsoft Reinvents Datacenter Power Backup with New Open Compute Project Specification (3/10/2015), Microsoft Global Datacenters, https://blogs.technet.microsoft.com/msdatacenters/2015/03/10/microsoft-reinvents-datacenter-power-backup-with-new-open-compute-project-specification/

[120] Yevgenly Sverdlik, How Microsoft got rid of the big Data Center UPS (3/12/2015), Data Center knowledge, https://www.datacenterknowledge.com/archives/2015/03/12/how-microsoft-got-rid-of-the-big-data-center-ups

[121] Neil Rasmussen, The Different Types of UPS Systems (White Paper 1, Revision 7), Schneider Electric, https://www.datacenterexperts.com/resources/white-papers/datacenter-power/133-the-different-types-of-ups-systems.html#:~:text=For%20example%2C%20it%20is%20widely%20believed%20that%20there,different%20types%20of%20UPS%20topologies%20are%20properly%20identified. (11/24/2020)

[122] Preeti Wadhwani, Saloni Gankar, UPS Market Size & Share 2020-2026 | Forecast Report, (May 2020), Global Market Insights, https://www.gminsights.com/industry-analysis/ups-market

[123] K Mongird, V Fotedar, V Viswanathan, V Koritarov, P Balducci, B Hadjerioua, J Alam, Energy Storage Technology and Cost Characterization Report (Table ES.1) (July 2019), DOE Pacific Northwest National Laboratory, https://www.energy.gov/sites/prod/files/2019/07/f65/Storage%20Cost%20and%20Performance%20Characterization%20Report_Final.pdf

[124] Voices of The Industry, Lithium-Ion Batteries Offer New Option for Data Center Backup Power

[125] K Mongird, V Fotedar, V Viswanathan, V Koritarov, P Balducci, B Hadjerioua, J Alam, Energy Storage Technology and Cost Characterization Report (Table ES.1) (July 2019), DOE Pacific Northwest National Laboratory

[126] Voices of The Industry, Lithium-Ion Batteries Offer New Option for Data Center Backup Power

[127] Victor Avelar and Martin Zacho, Battery Technology for Single Phase UPS Systems: VRLA vs. Li-ion (2017) White Paper 266 Rev 1, Scheider Electric

[128] Voices of The Industry, Lithium-Ion Batteries Offer New Option for Data Center Backup Power

[129] Smart Energy International, APS completes investigation following 2019 battery storage fire disaster (7/30/2020), Renewable Energy World, https://www.renewableenergyworld.com/2020/07/30/aps-completes-investigation-following-2019-battery-storage-fire-disaster/

[130] Technavio Research, The Global Stationary Lead-Acid (SLA) Battery Market will grow by $ 4.86 bn during 2020-2024, Business Wire (9/9/2020), https://www.businesswire.com/news/home/20200908005710/en/COVID-19-Stationary-Lead-Acid-Battery-Market-2020-2024-Increased-Investment-in-Green-Telecom-to-boost-Market-Growth-Technavio

[131] CleanTechnicay, Kokam Launching New Battery System For Global UPS Market, (8/31/2020), https://cleantechnica.com/2020/08/31/kokam-launching-new-battery-system-for-global-ups-market/

[132] Anton Beck, Lithium Iron Phosphate Vs. Lithium-Ion: Differences and Advantages (epectec.com) (9/20/2019)

[133] Steve Goldberg, How a Failed Car Company Gave Rise to a Revolutionary New Battery Inc (Aug 2018), Inc, https://www.inc.com/magazine/201808/steve-goldberg/fisker-automotive-solid-state-battery.html

[134] Invinity Energy Systems, redT and Avalon have merged as Invinity Energy Systems, a leading Vanadium Flow Battery company (4/16/2020), https://invinity.com/creating-leading-vanadium-flow-battery-company/

[135] DOE Office of Energy Efficiency and Renewable Energy, Pumped-Storage Hydropower | Department of Energy (12/22/2020)

[136] Electricity in the U.S. - U.S. Energy Information Administration (EIA)

[137] EIA, Electricity explained: Electricity in the United States, https://www.eia.gov/energyexplained/electricity/electricity-in-the-us.php (12/15/2021)

[138] EIA projects renewables share of U.S. electricity generation mix will double by 2050 - Today in Energy - U.S. Energy Information Administration (EIA) (2/8/2021)

[139] Electricity in the U.S. - U.S. Energy Information Administration (EIA)

[140] Hydropower explained - U.S. Energy Information Administration (EIA) (12/28/2020)

[141] Solar Energy Industries Association (SEIA), Solar Accounts for 40% of U.S. Electric Generating Capacity Additions in 2019, Adds 13.3 GW | SEIA (3/17/2020)

[142] Broekhoven, et al, Lincoln Laboratory, Microgrid Study: Energy Security for DoD Installations (June 18, 2012), MIT, p. 9

[143] Kate Anderson et al, Quantifying and Monetizing Renewable Energy Resiliency (3/23/2018), NREL

[144] Solar Explained, EIA, https://www.eia.gov/energyexplained/index.php?page=solar_home

[145] Appendix F – How to Calculate a Building's Rooftop Area, Housing and Urban Development (HUD), https://www.hudexchange.info/resources/documents/Appendix-F-Rooftop-Calculation-Tool.pdf

[146] Tyler Bowman, Matt Halligan, Ross Guttromson, Radiated High-Altitude Electromagnetic Pulse Testing of Photovoltaic Panels, Sandia National Laboratories, published by IEEE (2020)

[147] Department of the Army, Department of the Navy US Marine Corps, Electric Power Generation and Distribution (July 2018), https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN10584_ATP%203-34x45%20FINAL%20WEB.pdf

[148] Grand View Research, Fuel Cell Market Size & Share | Industry Report, 2020-2027 (grandviewresearch.com) (3/25/2021)

[149] Altergy website, https://www.altergy.com/products/freedom-power-technology/ (3/25/2021)

[150] CASE STUDY: Southern Linc, https://www.plugpower.com/wp-content/uploads/2020/07/2017_PlugPowerCaseStudy_SouthernLinc_F.pdf (4/6/2021)

[151] Global Solid Oxide Fuel Cell Market Trends Report, 2020-2027 (grandviewresearch.com) (5/26/2021)

[152] A5™ Off Grid Power Solution | GenCell (gencellenergy.com) (5/26/2021)

[153] Peter Kelly-Detwiler, A Key To The 'Hydrogen Economy' Is Carbon-Free Ammonia (forbes.com) (5/26/2021)

[154] Robert Yost, President & CEO, Achieving Max Power at 17 MPH, American Wind Inc.

[155] E. Hotchkiss, I. Metzger, J. Salasovich, and P. Schwabe, Alternative Energy Generation Opportunities in Critical Infrastructure (Nov 2013), NREL

[156] Sean Ong, Clinton Campbell, Paul Denholm, Robert Margolis, and Garvin Heath, NREL, Land-Use Requirements for Solar Power Plants in the United States (June 2013), https://www.nrel.gov/docs/fy13osti/56290.pdf

[157] DOE Solar Energy Technologies Office, Concentrating Solar-Thermal Power | Department of Energy (3/25/21)

[158] Biomass Energy Basics | NREL (12/28/20)

[159] SunSpec Alliance, https://sunspec.org/asset-performance-suite-aps/ (12/15/2021)

[160] NREL, REopt: Renewable Energy Integration and Optimization, https://reopt.nrel.gov/ (12/15/2021)

[161] Kate Anderson, et al, Quantifying and Monetizing Renewable Energy Resiliency (3/23/2018), p. 2, NREL

[162] NREL, Identifying Potential Markets for Behind-the-Meter Battery Energy Storage: A Survey of U.S. Demand Charges (August 2017) https://www.nrel.gov/docs/fy17osti/68963.pdf

[163] Kate Anderson, et al, Quantifying and Monetizing Renewable Energy Resiliency (3/23/2018), p 9, NREL. Use case includes clarifications provided via email from Kate Anderson to Mark Jones on 6/18/21.

[164] NREL, REopt: Renewable Energy Integration and Optimization, https://reopt.nrel.gov/ (12/15/2021)

[165] Value of Lost Load: An Efficient Economic Indicator for Power Supply Security? A Literature Review (see Figure 2 Willingness to Pay data) (12/24/2015). https://www.frontiersin.org/articles/10.3389/fenrg.2015.00055/full

[166] Kate Anderson, et al, Quantifying and Monetizing Renewable Energy Resiliency (3/23/2018), p 9, NREL

[167] ATB | NREL, see the assumptions for the 2020 Annual Technology Baseline and Standard Scenarios (6/22/2021)

[168] U.S. Energy Storage Monitor: Q3 2019 Report | Wood Mackenzie (Sept 2019)

[169] International Atomic Energy Agency, https://www.iaea.org/topics/small-modular-reactors (2/24/2020)

[170] DOE Office of Nuclear Energy, The BIG potential for nuclear micro-reactors (5/15/2019), https://www.energy.gov/ne/articles/big-potential-nuclear-micro-reactors

[171] Allied Market Research, Small Modular Reactor Market Statistics Analysis – 2030, https://www.alliedmarketresearch.com/small-modular-reactor-market-A14492 (12/15/2021)

[172] World nuclear news, Nuclear-supporting infrastructure bill becomes US law : Nuclear Policies - World Nuclear News (world-nuclear-news.org) (November 16, 2021)

[173] Dr. Peter B. Lyons, Hearing of the U.S. Senate Committee on Environment and Public Works, Preserving and Expanding Clean, Reliable Nuclear Power: U.S. Commercial Nuclear Reactor Performance Trends and Safety Initiatives (11/13/2019) https://www.epw.senate.gov/public/_cache/files/0/b/0b363e13-8875-4764-bd7f-29ae008166ae/7B09FA44A23AEBAACEC9C6C45AE9B2BD.lyons-testimony-11.13.2019.pdf

[174] Westinghouse, AP1000 Nuclear Power Plant – Passive Safety Systems, http://www.westinghousenuclear.com/new-plants/ap1000-pwr/safety/passive-safety-systems (2/24/2020)

[175] U.S. Energy Information Administration (EIA), Levelized Costs of New Generation Resources in the Annual Energy Outlook 2021. (9/23/2021)

[176] Juan A. Vitali, Joseph G. Lamothe, Charles J. Toomey Jr., Virgil O. Peoples, Kerry A. Mccabe, DoD Deputy Chief of Staff G-4, Study on The Use of Mobile Nuclear Power Plants for Ground Operations (10/26/2018)

[177] Fuels - Higher and Lower Calorific Values (engineeringtoolbox.com) (8/30/2021)

[178] United Nations Economic Commission for Europe (UNECE), Life Cycle Assessment of Electricity Generation Options (October 2021)

[179] IBID

[180] Kutakrock and Scully Capital, Small Modular Reactors: Adding to Resilience at Federal Facilities (December 2017), https://www.energy.gov/sites/prod/files/2018/01/f47/Small%20Modular%20Reactors%20-%20Adding%20to%20Resilience%20at%20Federal%20Facilities%20.pdf

[181] Office of Nuclear Energy, What is a Nuclear Microreactor? (10/23/2018), https://www.energy.gov/ne/articles/what-nuclear-microreactor

[182] DOE Office of Nuclear Energy, The Ultimate Fast Facts Guide to Nuclear Energy (1/16/2019) https://www.energy.gov/ne/downloads/ultimate-fast-facts-guide-nuclear-energy

[183] Adrian Cho, Science, Department of Energy picks two advanced nuclear reactors for demonstration projects (10/16/20), https://www.sciencemag.org/news/2020/10/department-energy-picks-two-advanced-nuclear-reactors-demonstration-projects

[184] Aaron Mehta, Portable nuclear reactor project moves forward at Pentagon (defensenews.com) (3/23/2021)

[185] BWXT, BWXT to Build First Advanced Microreactor in United States (6/9/2022)

[186] US Air Force confirms site for first microreactor: New Nuclear - World Nuclear News (world-nuclear-news.org) (10/26/2021)

[187] Kutakrock and Scully Capital sponsored by DOE, Small Modular Reactors: Adding to Resilience at Federal Facilities (Dec 2017), https://www.energy.gov/sites/prod/files/2018/01/f47/Small%20Modular%20Reactors%20-%20Adding%20to%20Resilience%20at%20Federal%20Facilities%20.pdf

[188] Lawrence R. Greenfield, An Overview of the Federal Energy Regulatory Commission and Federal Regulation of Public Utilities (p. 12) (June 2018), FERC, https://www.ferc.gov/sites/default/files/2020-07/ferc101.pdf

[189] FERC, FERC Issues Final Rule on Electric Storage Participation in Regional Markets (2/15/2018), Docket Nos. RM16-23, https://www.ferc.gov/media/news-releases/2018/2018-1/02-15-18-E-1.asp#.W4mf585Kipo

[190] EPA, Fact Sheet: Final Amendments to The Emission Standards for Reciprocating Internal Combustion Engines (1/15/2013), https://www.epa.gov/stationary-engines/fact-sheet-final-amendments-emission-standards

[191] EPA, Spill Prevention, Control and Countermeasure Plan (SPCC) Program Bulk Storage Container Inspection Fact Sheet (Dec 2019), https://www.epa.gov/sites/production/files/2014-05/documents/bulk_storage_container_integrity-testing-factsheet.pdf

[192] FMCSA, Part 383.5 Definitions (Dec 2019), https://www.fmcsa.dot.gov/regulations/title49/section/383.5

[193] Office of The Illinois State Fire Marshall, Above Ground Tanks Frequently Asked Questions (12/5/2019), https://www2.illinois.gov/sites/sfm/About/Divisions/Fire-Prevention-and-Building-Safety/AST/Pages/FAQs.aspx#h14

[194] Kate Anderson, Nicholas D. Laws, Spencer Marr, Lars Lisell, Tony Jimenez, Tria Case, Xiangkun Li, Dag Lohmann and Dylan Cutler, Quantifying and Monetizing Renewable Energy Resiliency (3/23/2018), NREL

[195] Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack (April 2008), http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf

[196] Frequency Regulation, Energy Storage Association (ESA), http://energystorage.org/energy-storage/technology-applications/frequency-regulation (8/21/18)

[197] NERC, Glossary of Terms Used in NERC Reliability Standards (updated 10/8/20)

[198] IBID

[199] Research Findings for Geomagnetic Disturbance Research Work Plan Summary Report (August 2020), EPRI

[200] Metatech, Geomagnetic Storms and the US Power Grid (4/26/2011), https://www.swpc.noaa.gov/sites/default/files/images/u33/finalBoulderPresentation042611%20%281%29.pdf

[201] NOAA, Geoelectric 3-D-1D Comparison, *https://www.swpc.noaa.gov/products/geoelectric-3d-1d-comparison* (12/15/2021)

[202] Edward Savage#1, William Radasky#2, and Michael Madrid, AC Harmonics Effects on Small External Power Supplies (Wall Warts), Metatech Corporation (no date is provided)

[203] L. Marti,A Rezaei-Zare; Generator Thermal Stress during a Geomagnetic Disturbance; IEEE 978-1-4799-1303-9, 2013.

[204] World Energy Needs and Nuclear Power | Energy Needs | Nuclear Energy meeting Energy Needs - World Nuclear Association (world-nuclear.org) (11/5/21)

[205] U.S. NRC, International Strategy 2021-2025,https://www.nrc.gov/docs/ML2123/ML21236A120.pdf

[206] Wendy Reed, NRC's Preparations for Advanced Reactor Licensing (10/15/2021), NRC

[207] GE Hitachi website (08/25/20), https://nuclear.gepower.com/build-a-plant/products/nuclear-power-plants-overview/bwrx-300

[208] Ontario Power Generation, OPG advances clean energy generation project (12/2/2021), https://www.opg.com/innovating-for-tomorrow/small-modular-nuclear-reactors/media_release/opg-advances-clean-energy-generation-project/

[209] NuScale, A Cost Competitive Nuclear Power Solution, Cost Competitive Nuclear Technology | NuScale Power (9/23/21)

[210] Neutron Bytes, Vogtle 3 & 4 Nuclear Reactors are a "Go" for Completion (12/26/2016), https://neutronbytes.com/2017/12/26/vogtle-3-4-nuclear-reactors-are-a-go-for-completion/

[211] NuScale, A Cost Competitive Nuclear Power Solution, Cost Competitive Nuclear Technology | NuScale Power (9/23/21)

[212] John Hopkins, NuScale Power, From the CEO's Desk, NUCLEUS Fall 2022 | NuScale Power (Fall 2022)

[213] Current Projects | NuScale Power (10/27/2021)

[214] Information approved for release by X-energy's Harlan Bowers on February 6, 2020

[215] Centrus Energy Corp, X-energy Completes Preliminary Design of TRISO-X Fuel Fabrication Facility, Signs Contract with Centrus Energy for Next Phase of Work (prnewswire.com) (11/2/2021)

[216] Kate Duffy, Bill Gates and Warren Buffett are building a $1 billion 'next-generation' nuclear reactor in Wyoming (msn.com) (6/3/2021), Business Insider

[217] Isabella Isaacs Thomas, How the next generation of nuclear reactors could be smaller, greener and safer (2/12/2020), PBS, https://www.pbs.org/newshour/science/how-the-next-generation-of-nuclear-reactors-could-be-smaller-greener-and-safer

[218] Gateway for Accelerated in Nuclear Innovation in Nuclear (GAIN), Advanced Nuclear Directory (7/1/2021), Gateway for Accelerated Innovation in Nuclear - Industry (inl.gov)
[219] BusinessWire, BWXT to Build First Advanced Microreactor in United States (yahoo.com) (6/9/2022)
[220] Carbon Free Energy | ARC Clean Energy (arcenergy.co) (9/23/2021)
[221] Gateway for Accelerated in Nuclear Innovation in Nuclear (GAIN), Advanced Nuclear Directory (7/1/2021), Gateway for Accelerated Innovation in Nuclear - Industry (inl.gov)
[222] DOE Office of Nuclear Energy, 5 Advanced Reactor Designs to Watch in 2030 | Department of Energy (03/17/21)
[223] Kairos Power, Homepage - Kairos Power (12/12/2021)
[224] Gateway for Accelerated in Nuclear Innovation in Nuclear (GAIN), Advanced Nuclear Directory (7/1/2021), Gateway for Accelerated Innovation in Nuclear - Industry (inl.gov)
[225] Gateway for Accelerated in Nuclear Innovation in Nuclear (GAIN), Advanced Nuclear Directory (7/1/2021), Gateway for Accelerated Innovation in Nuclear - Industry (inl.gov)
[226] Gateway for Accelerated in Nuclear Innovation in Nuclear (GAIN), Advanced Nuclear Directory (7/1/2021), Gateway for Accelerated Innovation in Nuclear - Industry (inl.gov)
[227] 5 Advanced Reactor Designs to Watch in 2030 | Department of Energy (3/17/2021)