Energy Resilience Assessment Methodology

Kate Anderson, Eliza Hotchkiss, Lissa Myers, and Sherry Stout

National Renewable Energy Laboratory

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-7A40-74983
October 2019

Energy Resilience Assessment Methodology

Kate Anderson, Eliza Hotchkiss, Lissa Myers, and Sherry Stout

National Renewable Energy Laboratory

Suggested Citation
Anderson, Kate, Eliza Hotchkiss, Lissa Myers, and Sherry Stout. 2019. *Energy Resilience Assessment Methodology*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-7A40-74983. https://www.nrel.gov/docs/fy20osti/74983.pdf.

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-7A40-74983
October 2019

National Renewable Energy Laboratory
15013 Denver West Parkway
Golden, CO 80401
303-275-3000 • www.nrel.gov

Acknowledgments

This methodology was developed and validated in collaboration with the U.S. Air Force Civil Engineer Center. The authors gratefully acknowledge Michael Rits, Lt. Col. Josh Aldred, and Christian Rasmussen for their sponsorship and support of this work. Additionally, the authors thank Alison Holm and Greg Guibert for their insightful review.

Executive Summary

With increasing utility grid outages in the United States, there is growing interest in assessing risk and developing mitigations to reduce the impact of grid outages and other power disruptions. The U.S. Department of Energy's National Renewable Energy Laboratory worked with military bases and stakeholders in their local community to develop a replicable energy resilience assessment methodology for sites, bases, and campuses to assess energy risks and develop prioritized solutions to increase site resilience. This includes steps to assess the baseline resilience of the site, identify and score hazards and vulnerabilities, analyze risks based on hazard likelihood and vulnerability probability and consequence, identify and prioritize mitigation actions based on cost, difficulty, and risk reduction, and then develop an action plan and implement solutions (Figure ES-1). The method focuses on risks to a site's primary missions, infrastructure, and population, as well as risks to infrastructure and population in the surrounding community that may impact the site.

Figure ES-1. Resilience assessment methodology

The energy resilience assessment methodology presented here can help sites to identify potential hazards and vulnerabilities and develop a comprehensive suite of mitigation actions to increase site energy resilience. By considering the interdependencies between energy, water, transportation, and communication systems, it also allows sites to understand the potential impacts of energy resilience on other critical systems. While developed for military bases, this methodology can also be used more broadly by other sites and campuses.

Table of Contents

List of Figures

List of Tables

1 Introduction

There is growing interest in assessing risk and developing mitigations to reduce the impact of utility grid outages. Energy lays at the core of our society, powering our buildings, transportation, water, and communication systems. As our dependence on energy increases, the complexity of the system and the inherent vulnerabilities within the system are also increasing. This makes energy resilience planning more important than ever.

Energy resilience focuses on preparing for, absorbing, adapting to, and recovering from low-probability, high-consequence disruptive events. Compared to reliability events that may affect small areas for a short time, resilience events typically result in longer outage durations and larger geographic areas of impact. An energy resilient site can continue to power critical operations (including the water, transportation, and communication systems that depend on energy) during natural disasters or human-caused incidents and recover rapidly after any disruption.

The U.S. Department of Energy's National Renewable Energy Laboratory has developed processes such as the Resilience Roadmap[1] and Technical Resilience Navigator to guide federal, state, and local entities through a resilience planning process. This report focuses more narrowly on one part of the broader planning process: a replicable energy resilience assessment methodology for the identification and scoring of hazards and vulnerabilities, analysis of risk, and prioritization of mitigation actions. This methodology was developed for military bases and stakeholders in their surrounding communities but may be more broadly useful to site and campus energy managers and resilience planners tasked with assessing energy risks and developing prioritized solutions to increase the energy resilience of their site.

The methodology includes steps to assess baseline resilience; identify and score hazards and vulnerabilities; analyze risks based on hazard likelihood, vulnerability probability, and consequence; identify and prioritize mitigation actions based on cost, difficulty, and risk reduction; develop an action plan; and implement solutions (Figure 1). The method focuses on risks to a site's primary missions, infrastructure, and population, as well as risks to infrastructure and population in the surrounding community that may impact the site.

[1] https://www.nrel.gov/resilience-planning-roadmap/

Figure 1. Resilience assessment methodology

Each step of the methodology is described in more detail in the following sections.

2 Assess Baseline

Understanding the existing conditions in terms of environmental location, capacity of the organization, and other factors helps determine the ability to respond and adapt under different operational conditions if a disruption were to occur (e.g., a seven-day power outage) is an important first step in the methodology. Baseline assessments are intended to identify the assets (property, people, information, missions) that need to be protected. The baseline assessment includes data collection and a literature review of emergency plans, maps, geographic data, utility information, and historical data relating to disasters, extreme temperatures, and grid outages. It often also includes workshops or interviews with site staff. Typical data collected in this stage are shown in Table 1.

Table 1. Typical Baseline Data

Process-Based Information	Operational Data	Geospatial Data	Historical Data
Emergency management plan	Energy consumption per building (if available) or meter and tariff	Map of electrical and natural gas infrastructure	Grid outages
Continuity of operations or contingency response plan	Water consumption per building or meter	Map of water and sewage infrastructure	Disruption to utilities or services
Memorandums of understanding between site and community	Fuel consumption by fixed (electrical) equipment and mobile equipment	Map of site and facilities	After-action reports
Community and site development plans	List of critical facilities and missions	Map of communications networks	Weather-related events and sequences of events
Ordinances and codes	List of backup generators and locations	Map of critical infrastructure	Assessments of local environmental risks and hazards

3 Identify Hazards and Vulnerabilities

The next step in the methodology is intended to uncover the potential hazards to the site that expose existing vulnerabilities in the infrastructure, processes and systems required to perform work at the site.

3.1 Hazards

Hazards and threats expose a vulnerability or damage, destroy, or disrupt an asset. The terms hazards and threats may be used interchangeably although some sources consider threats a sub-category of hazards that are specifically human-caused incidents. This paper uses the broader concept of hazards to include human-related threats. Hazards are not within the site's control. They can include wildfires, hurricanes, storm surges, or cyberattacks. Known or predicted, hazards must be identified to understand the potential impacts to the site and, eventually, the mitigation efforts to consider. Hazards are identified through literature reviews and stakeholder interviews with site staff and county emergency operations staff. Helpful resources include hazard assessments available from the county or state, NASA, the National Oceanic and Atmospheric Administration's Regional Integrated Science and Assessment program, and the American Society of Civil Engineers (such as its ASCE 7 Hazard tool,[2] which maps hazards based on location and criticality of facilities and creates a report noting maximum expected extreme weather or geohazards including wind, ice, snow, rain, flood, and tsunami levels that can be expected at the specified location). There are numerous resources publicly available; many of these are listed in Appendix A.

Additionally, engagement with local communities is necessary to determine the availability of existing hazard assessments or other informative resources. For example, states often have reports that identify hazards related to water quality, river systems, floodplain management, legal status of streams, and geology, such as landslide areas and earthquakes. Likewise, site staff can provide professional judgement on hazards other than natural hazards that should be considered. Hazards can be natural, technological, or adversarial in nature. sample of hazards are presented in Table 2. This is not a comprehensive list, but it serves as example areas to consider.

Table 2. Sample Categories of Hazards to Assess

Natural Hazards	Technological Hazards	Adversarial Hazards
Hurricanes	Power equipment failure	Bad actor
Flooding	Failure of water line	Act of terror
Earthquakes	Communication network interruption	Cyberattack
Severe winter storms	Pumping system failure on water lines	Political upheaval
Wildfire	Pumping system failure on wastewater lines	War

[2] https://asce7hazardtool.online/

3.2 Vulnerabilities

Vulnerabilities are weaknesses within infrastructure, systems, or processes that can be modified and mitigated to either prevent a disruption from occurring or lessen the consequences of a disruption. Vulnerabilities are identified through stakeholder interviews with site and surrounding community staff, as well as through review of existing planning documents. Examples of different types of vulnerabilities ranging from process to physical or natural vulnerabilities are listed in Table 3. Each assessment will determine its own location specific vulnerabilities.

Table 3. Sample Types of Vulnerabilities

Type of Vulnerabilities	Examples
Physical	Lack of backup systems and supplies or single points of failure in transportation routes, electrical lines, food supplies, water supplies, wastewater systems, communications networks on-site or in community, and infrastructure supporting site.
Natural	Location prone to flooding, fire, and so on.
Process	Lack of emergency planning. Lack of coordination and communication between site and supporting service providers.
Hardware, software, or media	Lack of cybersecurity defenses, malware, and potential for stolen data.
Emanation	Sensitive materials not protected from radiation.
Communication	Single lines of communication, dependence on digital networks, and lack of redundant systems.
Human	Inability to access site during an emergency. Overworked or exhausted employees.

A resilience assessment evaluates the potential vulnerability of an asset against a broad range of identified hazards. The intent of this step is to learn about and understand the resources and systems necessary for staff to complete their work, critical missions required to continue uninterrupted, and the consequences to the organization if those resources or systems were compromised. Table 4 provides examples of the types of systems that could be included in determining vulnerabilities.

Table 4. Resources and Systems Included in the Assessment

Resource	System
Water	Water treatment
	Water distribution
	Wastewater treatment
	Wastewater distribution
	Potable and nonpotable water supply
Facilities	Critical buildings, warehouses, or hangars
	Specialized equipment
	Specialized activities and operations
	Site security (perimeter fencing, guard stations)
Transportation	Roads
	Bridges
	Control towers
	Vehicle fleet
	Air fleet
	Marine fleet
	Fueling operations
	Fuel storage
Power	Electric feeders
	Substations
	Transformers
	Switching capability
	Backup generators
	Generator fuel storage
Communications	Communications network
	Phone lines
	Wireless fiber
	High-performance computers
Waste	Hazardous waste storage
	Waste disposal site
Capabilities	Site workforce
	Fire fighting
	Emergency medical service
	Linemen
	Clearing/cleanup/excavation

Stakeholder workshops or interviews are a critical component of this resilience assessment methodology. As infrastructure, process, and system creators, owners, operators, users, and stewards, stakeholders have a wealth of information to inform the assessment that may not be found in written documents. Further, interviews present an opportunity for dialogue that often teases out nuances or failure points that cannot be obtained otherwise. This includes providing historic and anecdotal information about vulnerabilities as well as hazards.

Stakeholders include members internal to the organization as well as those outside the organization. Internal stakeholders include staff that can identify key operations and missions, as well as staff that provide funding or services and manage systems and operations. This may include site leadership, mission owners, facility and fleet operators, utility managers, long-range planners, emergency and response management personnel, geographic information system and data managers. External stakeholders such as utilities, community development and land-use planners, stormwater managers, hazard mitigation planners, and emergency managers are often essential stakeholders to engage in the resilience assessment. Table 5 summarizes the types of individuals that could be engaged in interviews. A sample of interview questions are summarized in Appendix B.

Table 5. Stakeholders to Interview

Type of Stakeholder	Examples
Site Leadership, Support, and Energy Management	Installation leadership Mission owners Site electrical engineer Site energy manager Water program manager Wastewater treatment plant manager Generator testing and maintenance staff Communications staff Site emergency management personnel Geographic information system staff Air emissions officers Real property managers Transportation managers (ground and flight crew)
Utilities	Electric Water Gas Communications
Community Leaders	County Emergency Management Office County Chamber of Commerce

In addition to stakeholder workshops and interviews, data collection activities should include a review of relevant documents and studies. Examples of documents that can inform the identification and scoring of hazards and vulnerabilities include development plans, master plans, natural hazard studies, contingency response plans, after action reports following disasters

or disruptions, grid outage reports on historical outages, emergency operation plans, fire station functionality reports, and utility disaster response plans.

4 Score Hazards and Vulnerabilities

The next step is to score identified hazards and vulnerabilities to assess the dynamics of risk to a site. Risk is a function of the likelihood of a hazard, the probability of a vulnerability occurring given a hazard, and the consequence of the vulnerability.

> Risk = Likelihood of Hazard x Probability of Vulnerability x Consequence of Vulnerability

By decreasing the probability or consequence of a vulnerability in relation to an impending hazard, an overall reduction in risk can be achieved. The scoring can range from very qualitative and subjective to more detailed and quantitative. The less detailed approach would involve assigning terms such as "low, medium, high" scores for hazards. A more detailed approach would involve specific probabilities for hazards and detailed cost-based consequences for vulnerabilities. However, assessment teams should be mindful of the cost-benefit of using specific probabilities and cost-based consequences. The additional time and level of effort required to obtain detailed information could derail the process and does not necessarily generate more valuable results.

4.1 Hazards

Having identified hazards and vulnerabilities, the next step is to determine the likelihood of the hazards occurring in a specific area or within a specific political context. Utilizing the comprehensive list of potential hazards and their likelihood scores, the assessment team identifies which hazards are related to, or have the potential to impact, each vulnerability. According to the United Nations Office for Disaster Risk Reduction, risk analysis is forward-looking, so it can be understood as the likelihood (or probability) of loss of assets or life, injury, or destruction in a given period of time.[3] For the natural hazards, the scores are assigned using a combination of documented natural hazards, climate projections, and professional judgement based on likelihood of occurrence assessed from the quality and consistency of data and the degree of agreement among different sources. For the human-caused threats, scores are assigned based on current understanding of conditions from information collected during stakeholder interviews. It should be noted that the human-caused threats are more likely to be dynamic and change on a more regular basis than the natural hazards. As a result, more resilient sites will be those that undertake an analysis of human-caused threats on a regular basis. One approach to scoring hazards is based on probabilistic modeling, as outlined in Table 6.

[3] United Nations Office for Disaster Risk Reduction, *Global Assessment Report on Disaster Risk Reduction 2015.* https://www.unisdr.org/we/inform/publications/42809.

Table 6. Sample Probabilistic Scoring for Hazards

Score	Qualitative Description	Threshold (percentage likelihood of occurrence)
1	Rare; almost certain not to occur	0%–10%
2	Very low probability of occurrence; an event has the potential to occur but is still very rare	11%–20%
3	Slightly elevated level of occurrence; low probability, but not impossible	21%–30%
4	Possible, but more likely not to occur	31%–40%
5	May occur; 50/50 chance of occurring or not occurring	41%–50%
6	More likely to occur than not	51%–60%
7	Fairly likely to occur	61%–70%
8	Very likely probability	71%–80%
9	High probability of occurrence; has happened historically, but intermittently	81%–90%
10	Almost certain to occur; historic and frequent occurrences	91%–100%

4.2 Vulnerabilities

Vulnerability consequence scores are assigned using professional judgement, again drawing from the stakeholder interviews and document review. Site personnel determine the extent to which each of these hazards could negatively impact the site. This is done through a scoring system of ranking consequences or impact from low (score = 1) to high (score = 10) based on the degree to which an affected unit—a process, system, facility, or staff member—would suffer or fail as a result of a hazard occurring. When thinking about vulnerabilities, it is helpful to consider the characteristics of resilience. For example, the Air Force uses the following characteristics to assess resilience:

- Robustness: the level to which assets are hardened against disruptions
- Recoverability: the extent to which assets can bounce back from disruption
- Resourcefulness: the flexibility of the system to adapt to new conditions
- Responsiveness: the ability of the system to self-heal or automatically respond to disruption
- Redundancy: the characteristic of the system to have multiple pathways to achieve the mission.

In scoring each vulnerability, multiple areas of impact should be considered. Areas of impact include internal operations (e.g., the percentage of the business, the community, critical facilities/systems/equipment), number of staff or community members, percentage of land area, capital and operating costs, health and safety of workers and community members, environmental effects, and reliance on surrounding community to continue daily operations. Table 7 presents example criteria utilized to assign the vulnerability scores. These qualitative descriptions and thresholds are simply a guide for assigning a score.

Table 7. Sample Vulnerability Scores with Qualitative Descriptions

Score	Qualitative Description	Threshold (percentage impact to the organization)
1	Lowest magnitude of consequence to the organization. The organization would experience little to no effect or an in-place backup system would minimize impacts and ensure continuity of operations.	0%–10%
2	Very slightly elevated consequence to the organization. The organization would experience mild effects but could quickly resolve the failure. Few buildings or staff directly affected.	11%–20%
3	Slightly elevated consequence to the organization. The organization may need to temporarily transition operations to backup systems to resolve failure. Limited financial impacts may become apparent.	21%–30%
4	The organization would be somewhat affected and would expect limited financial consequences.	31%–40%
5	Medium magnitude of consequence. The organization would be somewhat affected. Specific systems or functions would be substantially delayed, but not all. Financial impacts would be expected to change budgeting plans or require reallocation of funds.	41%–50%
6	Prioritization of critical mission functionality would impact an increasing number of staff members and facilities.	51%–60%
7	Noncritical facilities and job functions are greatly reduced to almost fully prioritize more critical missions. Most buildings directly affected.	61%–70%
8	Noncritical facilities are fully shut down. Health and safety impacts to personnel concerns are increased, and only critical personnel are on-site.	71%–80%
9	All buildings are affected, and only emergency centers are occupied. Significant financial impacts would exist.	81%–90%
10	Highest magnitude of consequence. The organization would be significantly affected. Impacts would hinder almost every staff member's work and have serious implications for the ability to meet mission objectives. All buildings directly affected. Extreme financial impacts would exist.	91%–100%

Vulnerability probability scores represent the likelihood that a vulnerability will occur, given a realized hazard. Similar to hazard and vulnerability consequence, the vulnerability probability can be scored on a 1–10 scale, with 1 representing low likelihood and 10 representing high likelihood. Alternately, a more simplified binary 0/1 scale can be used, where 0 indicates that a particular hazard does not result a given vulnerability, and 1 indicates it does.

5 Analyze Risks

To evaluate the relationship between hazards and vulnerabilities, a risk matrix is used. The vulnerability score is the function of the probability of that vulnerability and the consequence of that vulnerability. The vulnerability score is then multiplied by the hazard likelihood scores to create a risk score for each specific hazard-vulnerability combination. Table 8 shows how the vulnerability consequence and probability scores are combined with the hazard likelihood scores to calculate risk scores. Table 9 presents an example of how the scores are combined for each vulnerability-hazard combination. Developing a risk matrix provides a structure for combining scores in a meaningful way that enables analysis and ranking of the risks to prioritize mitigation actions for the highest risks.

Table 8. Risk Score Matrix

Vulnerability Score	Hazard Scores									
	10	9	8	7	6	5	4	3	2	1
10	100	90	80	70	60	50	40	30	20	10
9	90	81	72	63	56	45	36	27	18	9
8	80	72	64	56	48	40	32	24	16	8
7	70	63	12	16	20	24	28	32	36	70
6	60	54	48	42	36	30	24	18	12	6
5	50	45	40	35	30	25	20	15	10	5
4	40	36	32	28	24	20	16	12	8	4
3	30	27	24	27	18	15	12	9	6	3
2	20	18	16	14	12	10	8	6	4	2
1	10	9	8	7	6	5	4	3	2	1

Table 9. Example Risk Score Calculations

Vulnerability	Consequence Score	Probability Score	Hazard	Likelihood Score	Consequence x Probability x Likelihood	Risk Score
Lack of backup power at specific facilities	10	1	Higher storm surge because of hurricanes	9	10 x 1 x 9	90
Lack of redundant water supply	7	1	Decreased annual rainfall	5	7 x 1 x 5	35
Lack of formal agreements for emergency response and clear roles with surrounding community	4	1	Increased number of days with freezing temperatures	2	4 x 1 x 2	8

6 Identify and Prioritize Mitigation Strategies

After understanding the risks, the assessment team identifies mitigation options that reduce the exposure or consequence of each vulnerability to respective hazards. It may be useful to think about the characteristics of resilience when developing mitigations and identify a set of actions that improve resilience across multiple characteristics (Table 10).

Table 10. Example Mitigations by Resilience Characteristics

Source: Adapted from Air Force Civil Engineer Center

Characteristic	Qualities	Examples
Robustness Are systems physically secure and hardened against disruptions?	• Physically secure • Cybersecure • Hardened infrastructure • Performance monitoring	• Maintenance schedule and checklist • Active performance monitoring • Critical assets elevated above the floodplain • Critical equipment or facilities physically secured and enclosed to protect from elements or bad actor • Critical assets cyber-secured, including removing unnecessary software and services, disabling unneeded communications and data ports, using robust passwords, and regularly patching software • Resilient building and infrastructure design (drainage, underground lines, elevation of infrastructure) • Temporary or permanent relocation of critical missions
Redundancy Are there single points of failure?	• Eliminate single points of failure	• Backup power (i.e., generators or microgrid) • Modular assets • Redundant electric, water, wastewater, transportation, and communication systems and sources • Mesh or loop networks to route power from multiple directions • Mission capability duplicated at other sites • Critical staff have backups
Resourcefulness Do we have diverse and flexible options?	• Available power generation • Energy storage • Community coordination	• Diversified generation sources, including generators, renewable energy, and storage • Diversified fuel sources for generators • Diversified water, wastewater, transportation and communication sources • On-site generation • Load shedding • Uninterruptable power supply • Community planning and resource integration • Mutual aid agreements • Supply chains diversified
Response Are systems automated and self-healing?	• Automated • Self-healing • Forecasting/ hazard assessment • Performance indicators • Training and exercises	• Maintenance staff training and exercise • Data collection and predictive analytics • Fault tolerance (controlled cooldown for safe recovery) • Inclement weather response plans • Smart control systems • Documented procedures • Training and exercises for outage scenarios
Recovery Can systems bounce back from disruption?	• Standardized components • Spare parts inventory • Damage assessment • Prioritization of repowering	• Spare parts inventory, preferably using commercial off-the-shelf parts • Utility coordination and agreements • Development of staff support programs to institutionalize resilience and build capacity

Each mitigation strategy is then evaluated based on its potential to reduce the risks to the site, its difficulty, and its cost. The risk reduction score is based on a potential percentage of reduction. In the absence of more granular, site-specific information, low to high reduction scores are assigned where low = 20%, low-medium = 35% medium = 50%, medium-high = 65%, and high = 80% risk reduction. The cost and difficulty of each mitigation are estimated on a low to high (1 to 10) scale. The site can then use the scores to prioritize mitigation actions based on their cost, difficulty of implementation, and ability to reduce risk, enabling identification of the highest return actions. Table 11 provides an example of scored mitigation actions. The same information can be graphically displayed as shown in Figure 2, where cost is shown on the Y axis, difficulty on the X axis, and risk reduction by the size of the bubble. Sites might prioritize actions shown by the largest bubbles (indicating highest risk reduction) near the lower left corner of the plot (indicating lower difficulty and cost).

Table 11. Example Mitigations Scored by Difficult, Cost, and Risk Reduction

Mitigation Action	Difficulty	Cost	Risk Reduction
Add backup power to critical loads	4	4	High (80%)
Improve water infrastructure by adding backup line and storage	3	3	Low (20%)
Develop memorandum of understanding with county to establish clear contingency plans	4	1	Med (50%)

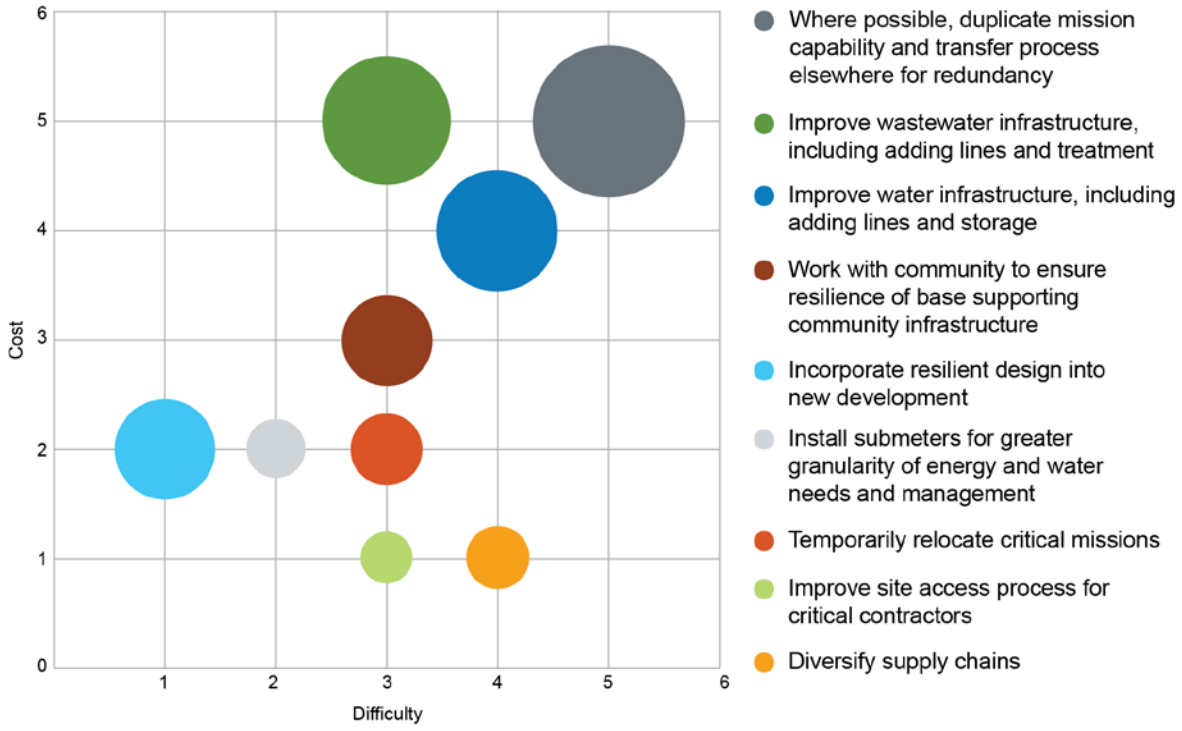

Figure 2. Mitigation actions prioritized based on cost, difficulty, and risk reduction, where risk reduction corresponds to the size of the bubble

7 Create an Action Plan and Implement Solutions

The final steps are to create an action plan, implement solutions and measure the results. The action plan should include the prioritized list of mitigation strategies, next steps, a timeline, and a budget, along with the entity or person responsible for carrying out the activity. The next steps for selected mitigation actions may include a feasibility study (e.g., carry out a detailed study on implementation, costs, and return on investment for creating a microgrid to power critical loads in specific facilities). Revisiting the vulnerability assessment and action plan on a regular basis will help refine the assessment and identify where improvements can be or have been made, as well as begin to measure the success of different mitigation strategies to inform future assessments. Table 12 shows an example action plan format, which could be as simple as an Excel spreadsheet or a table that is updated on a regular basis with status information on implementation.

Table 12. Example Action Plan

Mitigation Action	Next Steps	Responsible Party	Timeline to Start	Timeline to Implement	Potential Costs	Priority
Implement microgrid	Feasibility study	Ms. Smith	6/1/19	12/31/20	$2,000,000	1
Develop memorandum of understanding with community	Draft memorandum of understanding	Mr. Johnson	6/1/19	9/30/19	0	2
Conduct outage scenario exercise	Draft exercise scenario	Ms. Wells	6/1/19	7/31/19	0	3

8 Conclusions

The energy resilience assessment methodology presented here can help sites identify potential hazards and vulnerabilities and develop a comprehensive suite of mitigation actions to increase site energy resilience. By considering the interdependencies between energy, water, transportation, and communication systems, it also allows sites to understand the potential impacts of energy resilience on other critical systems. Stakeholder engagement, on-site champions, and decision maker buy-in are critical to the success of this methodology, and it is most successful when integrated with other planning processes to build off existing efforts. Undertaking resilience planning will require commitment and resources, but if applied in a cyclical and iterative process, integrating lessons that are learned and evaluating the process along the way, the investment will build institutional capacity and increase site resilience.

Appendix A. Publicly Available U.S. Hazard Data

American Society of Civil Engineers. *ASCE 7 Hazard Tool*. https://asce7hazardtool.online/.

NASA. "Sea Level Change Portal: Understanding Sea Level." https://sealevel.nasa.gov/understanding-sea-level/projections/empirical-projections.

National Climate Assessment. "Full Report." https://nca2014.globalchange.gov/node/1961.

National Oceanic and Atmospheric Administration, National Centers for Environmental Information. "Storm Events Database." https://www.ncdc.noaa.gov/stormevents/.

National Oceanic and Atmospheric Administration. "Sea Level Rise Viewer." https://coast.noaa.gov/slr/.

National Oceanic and Atmospheric Administration Climate.Gov. "U.S. Hazards Outlooks – Maps." https://www.climate.gov/maps-data/dataset/us-hazards-outlooks-maps.

National Weather Service Climate Prediction Center. "U.S. Hazards Assessment." http://www.cpc.ncep.noaa.gov/products/expert_assessment/threats.shtml.

U.S. Climate Resilience Toolkit. "Steps to Resilience." https://toolkit.climate.gov/steps-to-resilience/explore-hazards.

U.S. Department of Energy. "Climate Change and the U.S. Energy Sector: Regional Vulnerabilities and Resilience Solutions." https://www.energy.gov/sites/prod/files/2015/10/f27/Regional_Climate_Vulnerabilities_and_Resilience_Solutions_0.pdf.

Appendix B. Interview Questions

The following questions are example interview questions to elicit input from site staff on hazards and vulnerabilities resulting from a seven-day power outage.

Mission Owners:

1. What operations are most dependent on consistent power supply? What would happen if power supply was limited or not available for seven days? Day 1? Day 2? Day 3?... Day 7?
2. Which functions are mobile versus stuck in place? Are there missions/functions that can tolerate some outage duration, and be brought on sequentially? Are missions/functions schedulable? Are there times of day that missions/functions must operate?
3. What costs are incurred when the grid goes down?
4. What type of equipment, facilities, or buildings are critical/dependent on continuous supply of power and where are they located (location on-site and elevation)?
5. Are there missions/functions that can tolerate some outage duration, and be brought on sequentially? Are missions/functions schedulable? Are there times of day that missions/functions must operate?
6. What impact would a seven-day utility outage have on other resources you depend on, such as water, food, transportation, and communications?
7. Do you have backup generation capabilities or energy storage? How much fuel is stored on-site, and how long would they provide backup power?
8. Is the quality of power supply important?
9. Are there future or planned capital projects that will change power needs?
10. Are there plans in place to automatically/manually shed load in specific buildings/missions in the event of a power outage?
11. Are there personnel plans in place outlining which individuals must report for duty or leave the site in certain events?
12. Are there personnel plans for maintaining energy systems during outages?
13. Describe past outage events: what were their durations, what happened, were any lessons learned?
14. What are the primary vulnerabilities or points of failure?
15. Are there programs in place to support staff mental health?
16. What additional mitigation strategies would you suggest to reduce the impact of a seven-day power outage?

Energy Manager:

1. Can you provide the following data?
    a. One year of 15-minute load data for each building (if available) or the site
    b. One year of 15-minute load data for critical loads (if not, monthly kWh and peak kW, estimated hours of operation)

   c. List of critical buildings (low, medium, high), including which should be included in microgrid design, which should be shut off first if needed (important enough to be included in microgrid, but first to go if system conditions require immediate load shed)
   d. Location, size, elevation, and age of backup generators
   e. Water load
   f. Fuel load
   g. Any projected changes to electricity, fuel, or water use
   h. Utility rate tariffs
   i. Demand response or peak shaving capabilities
   j. Historical outage information or power quality issues
   k. Value of lost load (costs incurred when grid goes down)
   l. Site sustainability reports
   m. Interconnection policies
   n. Electrical one-line diagram of distribution system with power generation and energy storage resources, main distribution switchgear, voltage feeders, and transformers
   o. Diagrams of thermal and water systems.
2. What operations are most dependent on consistent power supply? What would happen if power supply was limited or not available for seven days? Day 1? Day 2? Day 3?... Day 7?
3. What type of equipment, facilities, or buildings are critical/dependent on continuous supply of power and where are they located (location on-site and elevation)?
4. Which functions are mobile versus stuck in place? Are there missions/functions that can tolerate some outage duration, and be brought on sequentially? Are missions/functions schedulable? Are there times of day that missions/functions must operate?
5. What impact would a seven-day utility outage have on other resources like water, food, transportation, and communications?
6. How does power get to the site and distributed around the site?
7. Do you have backup generation capabilities and what fuel source? Where is the fuel sourced? Are there any modifications to systems or equipment required to use them? How long would these fuel sources provide backup power? Are they regularly maintained and tested?
8. Is the quality of power supply important?
9. Do you store any power supply on-site? Are there temperature-related storage requirements?
10. Are there future or planned capital projects that will change power needs?
11. Is there switching capability to shed loads or partition feeders?
12. Do you have a spare parts strategy?
13. Are there plans in place to automatically/manually shed load in specific buildings/missions in the event of a power outage?

14. Are there personnel plans in place outlining which individuals must report for duty or leave the site in certain events?
15. Are there personnel plans for maintaining energy systems during outages?
16. Describe past outage events; durations, what happened, were any lessons learned?
17. What are the primary vulnerabilities or points of failure?
18. What additional mitigation strategies would you suggest to reduce the impact of a seven-day power outage?

Utilities (Electric, Gas, Water, Wastewater):

1. Can you provide electrical one-line diagrams that shows the site electrical distribution system with power generation and energy storage resources, main distribution switchgear, voltage, feeders, and transformers?
2. Can you provide diagrams that shows the site water and wastewater infrastructure?
3. Can you provide diagrams that shows the site gas infrastructure?
4. What is the typical electric, gas, water and wastewater consumption/load? What is the cost or rate tariff?
5. Where is power/gas/water generated? How does it get to the site? Is any generated on-site? Where is wastewater treated?
6. What backup systems are in place in the event of a power outage?
7. What frequency and duration of outages has the site experienced historically?
8. Describe past outage events; what were their durations, what happened, were any lessons learned?
9. What emergency response plans does the utility have in place to respond to a power outage? Can you share existing emergency response plans?
10. What are the primary vulnerabilities or points of failure?
11. Is there switching capability to shed loads or partition feeders?
12. Are there plans in place to automatically/manually shed load in specific buildings/missions in the event of a power outage?
13. Do you have a spare parts strategy?
14. What additional mitigation strategies would you suggest to reduce the impact of a seven-day power outage?
15. Are there any renewable energy, microgrid, or other investments the site could make that would also benefit the utility?
16. What utility rate tariff is the site on? (Include energy, demand, power factor, or other penalties as applicable.)
17. Are demand response or peak shaving programs available?
18. Does the utility offer incentives for implementing renewable energy or energy efficiency projects?
19. What are the net metering and interconnection limits?

Emergency Management:

1. What are the site's critical missions and facilities?
2. What impact would a seven-day utility outage have on these missions/facilities?
3. What impact would a seven-day utility outage have on other resources like water, food, transportation, and communications?
4. What emergency response plans does the site have in place to respond to a seven-day power outage? Can you share existing emergency response plans?
5. Do you have backup generation capabilities at critical facilities, and how long would on-site fuel sources provide backup power?
6. Are there personnel plans for maintaining energy systems during an outage? Are their plans outlining which individuals must report for duty or leave the site in certain events?
7. Describe past outage events; what were their durations, what happened, were any lessons learned?
8. What are the primary vulnerabilities or points of failure?
9. What additional mitigation strategies would you suggest to reduce the impact of a seven-day power outage?

Power Production (Generator Testing and Maintenance):

1. What type of equipment, facilities, or buildings are critical/dependent on continuous supply of power and where are they located (location on-site and elevation)?
2. Do you have backup generation capabilities and what fuel source? Where is the fuel sourced? Are there any modifications to systems or equipment required to use them? How long would these fuel sources provide backup power? Are they dual fuel? Are they regularly maintained and tested?
3. Is the quality of power supply important?
4. Do you store any power supply on-site? Are there temperature-related storage requirements?
5. Is there switching capability to shed loads or partition feeders?
6. Do you have a spare parts strategy?
7. Are there plans in place to automatically/manually shed load in specific buildings/missions in the event of a power outage?
8. Are there personnel plans for maintaining energy systems during outages?
9. Describe past outage events; what were their durations, what happened, were any lessons learned?
10. What are the primary vulnerabilities or points of failure?
11. What additional mitigation strategies would you suggest to reduce the impact of a seven-day power outage?

Communications and Information Assurance:

1. What operations are most dependent on consistent power supply? What would happen if power supply was limited or not available for seven days? Day 1? Day 2? Day 3?... Day 7?
2. What type of communications equipment or facilities are critical/dependent on continuous supply of power and where are they located (location on-site and elevation)?
3. Do you have backup generation capabilities at critical facilities, and how long would on-site fuel sources provide backup power?
4. Is the quality of the power supply important?
5. Are there emergency response plans for maintaining communications during a power outage?
6. Describe past outage events; what were their durations, what happened, were any lessons learned?
7. What are the primary vulnerabilities or points of failure?
8. What additional mitigation strategies would you suggest to reduce the impact of a seven-day power outage?

Air Emissions:

1. Do emissions restrictions impose any limits on the use of diesel/natural gas generators for backup power during a seven-day electrical outage?

Security:

1. What are the primary threats to the site? How likely do you consider a physical attack, cyberattack, or other human-caused attack?