Resilient Energy Platform

POWER SECTOR RESILIENCE PLANNING GUIDEBOOK

A Self-Guided Reference for Practitioners

Sherry Stout, Nathan Lee, Sadie Cox, and James Elsworth

U.S. Department of Energy's National Renewable Energy Laboratory

Jennifer Leisch

United States Agency for International Development

www.resilient-energy.org | www.nrel.gov/usaid-partnership

USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

NOTICE

This work was authored, in part, by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by the United States Agency for International Development (USAID) under Contract No. Contract No. IAG-17-2050. The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government or any agency thereof, including the United States Agency for International Development.

This guidebook is largely a compilation of content from previously published sources developed at the National Renewable Energy Laboratory (NREL). Some of the text is taken directly from the two main sources cited below. This guidebook seeks to utilize this content and repurpose it in a format useful for power sector resilience planners internationally and for conducting power sector resilience planning workshops.

1. Anderson, Kate, Josh Aldred, Michael Elchinger, Christine Gamble, Nick Grue, Nicholas Gilroy, Eliza Hotchkiss, Michael Ingram, Lissa Myers, Michael Rits, Sherry Stout, and Julie Tran. "Using GIS Visualization and Temporal Dynamism to Enhance Resilience Assessments." Forthcoming.
2. Hotchkiss, Eliza, Alex Dane, and Connie Komomua. NREL. "Resilience Roadmap: A Collaborative Approach to Multi-Jurisdictional Planning." https://www.nrel.gov/resilience-planning-roadmap/.

Table of Contents

Introduction to Planning a Resilient Power Sector

Planning for Power Sector Resilience

The provision of reliable, secure, and affordable electricity is essential to power economic growth and development. The power system is at risk from an array of natural, human-caused, and technological threats, which can cause everything from power interruption to chronic under-supply of energy. It is critical for policy-makers, planners, and system operators to safeguard their power systems from these threats by proactively planning for future needs and investing in resilient power systems.

Aim and Audience of this Guidebook

This guidebook is a reference for power sector resilience planning that introduces policymakers, power sector investors, planners, system operators, and other energy-sector stakeholders to the key concepts and steps involved in power sector resilience planning. Users can then apply this knowledge in the development of strategic, country-specific processes and identify actions that increase power sector resilience.

Use of this Guidebook

As a manual for power sector resilience planning, this guidebook can be used as a stand-alone resource or shared with participants at stakeholder workshops to facilitate discussions and complete key steps of a resilience planning process.

This guidebook is organized into chapters that guide the user through the resilience planning process. Each chapter focuses on a specific topic and presents the concepts in a brief planning guide, activities to support planning for that topic, and presentation slides that can be used either as a reference for background material or to conduct training workshops. Together, these resources facilitate the step-by-step process of identifying threats to the power system and their associated impacts, assessing potential vulnerabilities, evaluating risk, and developing strategies to increase resilience, as shown below:

In addition to these topical chapters, this guidebook contains resources for readers to learn more about key terms and concepts related to resilience, research natural threats that may impact their systems, explore case studies related to power sector resilience, and learn from existing resilience action plans.

Resilient Energy Platform

Planning a Resilient Power Sector

Ensuring reliable, secure, safe, and affordable electricity

What is power sector resilience?

The provision of reliable, secure, and affordable electricity is essential to power economic growth and development. The power system is at risk from an array of natural, technological, and man-made threats that can cause everything from power interruption to chronic undersupply. It is critical for policymakers, planners, and system operators to safeguard their systems and plan for and invest in the improved resilience of the power sector in their countries.

Through holistic resilience planning, actors can anticipate, prepare for, and adapt to the threats and stresses on the power system. Resilience planning identifies the threats, impacts, and vulnerabilities to the power system, and devises strategies to mitigate them.

What is Power Sector Resilience?

The ability to anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruptions to the power sector through adaptable and holistic planning and technical solutions.[1]

What are threats to the power system?

Power sector vulnerabilities—weaknesses within infrastructure, systems, or operations—are susceptible to natural, technological, and human-caused threats. Impacts from these threats include potential fuel supply shortages for transportation and energy generation, physical infrastructure damage, shifts in energy demand, and disruption of electricity supply to the end user.[2] These disruptions, in turn, adversely affect critical services and facilities (e.g., hospital services, water treatment, and communications networks). As such, it is vital to understand threats to the power system and their associated impacts.

Natural threats include long-term climatic changes, such as variations in precipitation patterns and changes in air and water temperatures, as well as severe weather events, such as storms, flooding, and storm surges. For example, warmer water and drought may impact the availability of cooling water for thermal generation and increase competition between hydroelectric generation facilities and other users. Altered precipitation patterns and more intense storms can impact hydropower output and biomass resource availability. Changes in wind direction, speed, and availability can alter wind power generation and damage transmission and distribution lines. Flooding and extreme weather events, such as hurricanes, severe storms, and wildfires, can damage generation, transmission, and distribution infrastructure.[3,4] This damage can cause both short- and long-term outages as seen in the United States after hurricanes Irma and Maria.

Technological threats are often unpredicted equipment and infrastructure failures. For example, dam failure, nuclear power station accidents, generation station fires, and power outages caused by faulty system equipment or aging infrastructure are all considered technological threats. These threats can be stand alone or tied to human-caused or natural threats. For example, the Three Mile Island nuclear incident was an isolated technology failure whereas the Fukushima nuclear incident was directly tied to a 15-meter tsunami caused by the Great East Japan earthquake.[5,6] Aging or undersized electricity transmission and distribution infrastructure are also common threats that can cause the failure and interruption of electricity.

Human-caused threats fit into two categories: accidents and malicious events. Accidents involve unintentional actions that damage systems, such as a driver running into a transmission pole and causing an outage. Malicious events are the result of deliberate, harmful, human actions, such as physical terrorism or cyberattacks on power infrastructure and control systems. Physical attacks could injure workers and destroy energy infrastructure, such as fuel pipelines or transmission lines. Cyberattacks can impact system operations or take confidential information—targeting power control systems, generators, or critical data infrastructure.[7]

Severe weather can cause flooding, landslides, and other threats to power system infrastructure and affect energy resource availability. Renewable energy generation can enhance resilience because of its modular nature and lack of fuel requirements.[4] *Photo from iStock 155353280*

How do I improve power sector resilience?

Improving power sector resilience requires systematically identifying and addressing vulnerabilities through proactive resilience planning. Power sector resilience planning can be done at many geographic scales and should be included within the existing power sector planning processes in place, such as integrated resource planning or power development planing.[7,8]

Planning for power sector resilience

Planning for power sector resilience requires engaging stakeholders in a common vision for a resilient system, gathering needed system data and information, assessing vulnerabilities, and developing strategies and enabling policies to improve the resilience of the sector. To perform a vulnerability assessment, planners initially gather data about critical loads, threats, energy resources, energy system infrastructure, and other relevant areas. The Resilience Roadmap (www.nrel.gov/resilience-planning-roadmap) and the Renewable Energy Data Explorer (www.re-explorer.org) provide data lists (e.g., relevant polices and plans, electricity generation characteristics, transportation systems profiles, energy costs, and

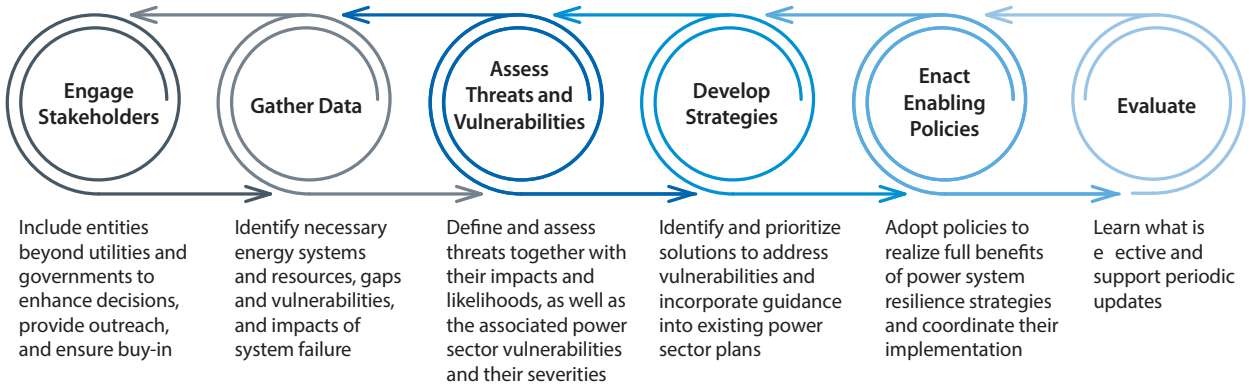


Fig. 1. Planning for power sector resilience can happen at different geographic scales (local, national, or regional) and should be incorporated into existing power sector planning and policies to ensure effectiveness.

government and community operations) and aggregated spatial data (e.g., energy resource availability and location of energy infrastructure) that can support resilience planning.

After gathering data, planners conduct a vulnerability assessment that considers the risks (calculated as the product of the likelihood of the threat and the severity of the vulnerability) and exposure (how power systems may respond to threats) posed by certain threats that a system faces.[9]

After assessing vulnerabilities, planners identify and prioritize solutions to improve power sector resilience. These solutions can then be integrated into existing power sector plans and policies.[10]

Solutions may include options such as spatial diversification of generation and transmission, development of microgrids for critical systems, introducing redundancy to the most vulnerable systems, and demand side management and efficiency. Any of these solutions should be completed within an appropriate policy framework that values and enables resilience through infrastructure development and operational planning. It is also vital to identify financing that enables implementation of these solutions. The effectiveness of actions and policies should be evaluated regularly, as the resilience process is iterative.[10]

Resilient Energy Platform

The Resilient Energy Platform provides expertly curated resources, training, tools, and technical assistance to enhance power sector resilience. Find out more at www.resilient-energy.org.

References

[1] Hotchkiss, Eliza, Alex Dane, and Connie Komomua. "Resilience Roadmap." National Renewable Energy Laboratory (NREL), 2018. https://www.nrel.gov/resilience-planning-roadmap/.

[2] DOE. "Climate Change and the Electricity Sector: Guide for Climate Change Resilience Planning." Washington, D.C.: U.S. Department of Energy (DOE), 2016. https://www.energy.gov/sites/prod/files/2016/10/f33/Climate%20Change%20and%20the%20Electricity%20Sector%20Guide%20for%20Climate%20Change%20Resilience%20Planning%20September%202016_0.pdf.

[3] Hellmuth, Molly, Pamela Cookson, and Joanne Potter. "Addressing Climate Vulnerability for Power System Resilience and Energy Security: A Focus on Hydropower Resources." Technical Report. RALI Series: Promoting Solutions for Low Emission Development. Washington, D.C.: Resources to Advance LEDS Implementation (RALI) from U.S. Agency for International Development (USAID) and ICF International, Inc., 2017. https://www.climatelinks.org/resources/addressing-climate-vulnerability-power-system-resilience-and-energy-security-focus.

[4] Miara, Ariel, Jordan E. Macknick, Charles J. Vörösmarty, Vincent C. Tidwell, Robin Newmark, and Balazs Fekete. "Climate and Water Resource Change Impacts and Adaptation Potential for US Power Supply." Nature Climate Change 7, no. 11 (November 2017): 793–98. https://doi.org/10.1038/nclimate3417.

[5] NRC. "Backgrounder: Three Mile Island Accident." U.S. Nuclear Regulatory Commission (NRC). 2018. https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/3mile-isle.html.

[6] World Nuclear Association. "Fukushima Accident." 2018. http://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/fukushima-accident.aspx.

[7] NIST. "Community Resilience Planning Guide." National Institute of Standards and Technology (NIST), 2018. https://www.nist.gov/topics/community-resilience/community-resilience-planning-guide.

[8] Cox, Sadie, Eliza Hotchkiss, Dan Bilello, Andrea Watson, Alison Holm, and Jennifer Leisch. "Bridging Climate Change Resilience and Mitigation in the Electricity Sector Through Renewable Energy and Energy Efficiency: Emerging Climate Change and Development Topics for Energy Sector Transformation." Technical Report. Golden, CO: National Renewable Energy Laboratory (NREL), 2017. https://www.nrel.gov/docs/fy18osti/67040.pdf.

[9] GIZ. "The Vulnerability Sourcebook: Concept and Guidelines for Standardised Vulnerability Assessments." Bonn: Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH, 2014. https://www.adelphi.de/en/publication/vulnerability-sourcebook-concept-and-guidelines-standardised-vulnerability-assessments.

[10] Cox, S., Gagnon, P., Stout, S., Zinaman, O., Watson, A., and Hotchkiss, E. 2016. "Distributed Generation to Support Development-Focused Climate Action. EC-LEDS (Enhancing Capacity for Low Emission Development Strategies)." Technical Report. Golden, CO: NREL. www.nrel.gov/docs/fy16osti/66597.pdf.

Written by Nathan Lee and Sherry Stout, National Renewable Energy Laboratory

www.resilient-energy.org | www.nrel.gov/usaid-partnership

Jennifer E. Leisch, Ph.D.
USAID-NREL Partnership Manager
U.S. Agency for International Development
Tel: +1-303-913-0103 | Email: jleisch@usaid.gov

Sadie Cox
Senior Researcher
National Renewable Energy Laboratory
Tel: +1-303-384-7391 | Email: sadie.cox@nrel.gov

This work was authored, in part, by the National Renewable Energy Laboratory (NREL), operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by the United States Agency for International Development (USAID) under Contract No. IAG-17-2050. The views expressed in this report do not necessarily represent the views of the DOE or the U.S. Government, or any agency thereof, including USAID.

NREL/TP-7A40-73618 | June 2019
NREL prints on paper that contains recycled content.

The Resilient Energy Platform provides expertly curated resources, training, tools, and technical assistance to enhance power sector resilience. The Resilient Energy Platform is supported by the U.S. Agency for International Development.

The USAID-NREL Partnership addresses critical challenges to scaling up advanced energy systems through global tools and technical assistance, including the Renewable Energy Data Explorer, Greening the Grid, the International Jobs and Economic Development Impacts tool, and the Resilient Energy Platform. More information can be found at: **www.nrel.gov/usaid-partnership**.

USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

REexplorer MAPPING OUR ENERGY FUTURE

Greening the Grid

I-JEDI

Resilient Energy Platform

THREATS

Guide to Threats

Introduction

The identification of threats to the power sector is a key step in planning for a resilient power system. A threat is anything that can, either intentionally or accidentally, damage, destroy, or disrupt the power sector. Threats can be natural, technological, or human caused. Threats are not typically within the control of power system planners and operators. They can include wildfires, hurricanes, storm surges, cyberattacks, and more. Threats can affect many components of the power sector—from generation to transmission and distribution to operations, workforce, and finance. For more information and examples of types of threats, refer to the presentation at the end of this section.

This section introduces the key steps in identifying threats to the power sector:

1. Assessing existing conditions
2. Identifying threats
3. Scoring the likelihoods of threats

Threats—anything that can damage, destroy, or disrupt the power sector. Threats can be natural, technological, or human caused. Threats are not typically within the control of power system planners and operators. They can include wildfires, hurricanes, storm surges, cyberattacks, and more.

1. Assess Existing Conditions

An understanding of the existing conditions of the power sector in terms of location, operational practices, political threats, and other factors helps determine the ability of the power sector to respond and adapt under different operational conditions if a disruption were to occur[1]. This step is conducted to identify these conditions and highlight the assets that need to be protected under various planning scenarios. The assessment begins with stakeholder interviews, literature reviews, and data collection of resources, including (but not limited to):

- Integrated resource plans
- Emergency plans
- Maps and geographic data
- Utility information
- Historical data related to disasters, extreme temperatures, and grid outages
- Other available, relevant resources.

2. Identify Threats

Developing an understanding of the potential threats to a power system is important to enhancing resilience. Threats are identified for current and future power system conditions because the likelihood of different threats may change over the planning horizon. The following sections present an approach to identifying and defining threats to the power system.

Known or predicted threats must be identified to understand the potential impacts to the power sector and their likelihood of occurring. This information will be used later in this guidebook to evaluate risk, as part of the vulnerability assessment, and factor into the potential resilience efforts to consider in later steps. Threats are identified through literature reviews, climate data, and stakeholder interviews with power sector staff from organizations that include ministries of energy and environment, grid operators, utilities, meteorological services, emergency managers, and natural resource offices.

Table 1. Three Categories of Threats[1]

Natural	Technological	Human Caused
Cyclones	Infrastructure failure (because of aging, material defects, etc.)	Accidents
Floods		Terrorism
Earthquakes	Poor workmanship or design	Cyberattacks
Drought	Unpredictable loads	Political upheaval
Wildfire	Water-line disruption impacting power sector	
Wildlife interactions		
Solar flares		

Additionally, resilience assessment teams should work with national environmental offices and local communities to determine the availability of existing threat assessments[1]. National planning resources can be used to identify threats related to water quality, river systems, floodplain management, and geology, such as landslide areas and earthquakes[1]. Power sector staff (e.g., grid operators, utilities staff, and ministries of energy) can provide professional judgment on likelihoods and impacts of technological and human-caused threats.

Threats are typically categorized into three types: natural, technological, or human caused. Table 1 provides examples of threats in each category.

3. Score Threat Likelihoods

The next step in the process is to score the likelihood that each threat may occur. Later in the process, these scores will be combined with vulnerability scores to evaluate the overall risk to the power sector (refer to the *Guide to Vulnerabilities* and the *Guide to Risk Assessments* for further information).

The scores for each category of threat are assigned through the review of information from data collection and stakeholder interviews.

- **Natural threat likelihood scores**—assigned using a combination of documented natural threats and climate projections based on likelihood of occurrence assessed from the quality and consistency of data and the degree of agreement between different sources[1].
- **Technological and human-caused threat likelihood scores**—assigned based on current understanding of conditions from information collected during stakeholder interviews[1].

One approach to scoring threats is based on likelihood modeling, as outlined in Table 2.

Technological and human-caused threat scores are more likely to be dynamic and change on a regular basis than the natural threat scores. As a result, these scores are constantly shifting, and more resilient power sectors will be those that undertake an analysis of threats on a regular basis[1].

Table 2. Scores and Descriptions for Scoring Threat Likelihoods

Threat Likelihood Scores		Threshold Descriptions
Categorical	**Numerical**	
High	9	Almost certain to occur. Historic and frequent occurrences.
Medium-High	**7**	More likely to occur than not.
Medium	5	May occur.
Low-Medium	3	Slightly elevated level of occurrence. Possible, but more likely not to occur.
Low	1	Very low probability of occurrence. An event has the potential to occur but is still very rare.

Activity: Identifying Threats

Goal of this Activity

In this activity, you will identify potential threats that your power sector may face and assign each a likelihood score.

Introduction

The output of this activity will be a list of five power system threats and a likelihood score for each. These threats will help to identify impacts and vulnerabilities in the next two steps of the process. Threat likelihood scores will later be combined with a vulnerability severity score to calculate risk.

> **Threats**—anything that can damage, destroy, or disrupt the power system. Threats can be natural, technological, or caused by human activity. Threats are not typically within the control of power system planners and operators. They can include wildfires, hurricanes, storm surges, cyberattacks, and more[1].

Exercise 1: Identifying Threats

Potential threats must be identified to understand the potential impacts to communities and, eventually, the potential mitigation efforts to consider. An all-threats approach offers a holistic way to incorporate the many needs of various stakeholders and utilize limited resources during resilience planning. An all-threats approach would account for the following:

- **Natural threats** resulting from acts of nature (e.g., severe weather, floods, earthquakes, hurricanes, solar flares, etc.) as well as wildlife interactions with the power system (e.g., squirrels, snakes, or birds causing short circuits on distribution lines).
- **Technological threats** resulting from accidents or failures of systems and structures (e.g., a bridge collapse or grid outage).
- **Human-caused threats** resulting from accidents (e.g., cutting an underground line) or the threats or intentional actions of an adversary (e.g., cyberattacks or acts of terror).

Additional threats may include longer-term system stresses caused by population change or changing economic conditions.

To guide this activity and identify threats, consider the following questions:

Discussion Questions

1. What natural threats may exist for your power sector and how frequently do they occur?
2. Which power sector infrastructure systems have been impacted by past threats or system stresses?
   - Natural threats?
   - Technological threats?
   - Human-caused threats?
3. Has critical power sector infrastructure ever gone off-line or experienced reduced operability?
   - What was the threat that caused this?
   - How many hours, days, or weeks was the infrastructure off-line or not operational?
4. In the future, which threats and shocks are likely to increase (at the city, national, or multinational scale)?
   - Natural threats?
   - Technological threats?
   - Human-caused threats?
5. What are the top five threats that should be considered for a power sector vulnerability assessment?
   - Record these in the table on the next page.

Likelihood Scores

After identifying your top five threats, score the likelihood that each threat may occur. Refer to the *Guide to Threats* section for more information, and use the qualitative scoring scale provided below:

Threat Likelihood Scores		Threshold Descriptions
Categorical	**Numerical**	
High	9	Almost certain to occur. Historic and frequent occurrences.
Medium-High	**7**	More likely to occur than not.
Medium	5	May occur.
Low-Medium	3	Slightly elevated level of occurrence. Possible, but more likely not to occur.
Low	1	Very low probability of occurrence. An event has the potential to occur but is still very rare.

Activity: Identifying Threats

In the table below, record the top five threats that should be considered for a power sector vulnerability assessment. This activity is for exercise purposes only (in a comprehensive resilience assessment, far more than five threats should be considered).

Threats	Likelihood Scores
1.	
2.	
3.	
4.	
5.	

Threats Introduction

Power Sector Resilience Planning Guidebook

The following slides are intended to provide additional background information and examples of power system threats. They can serve simply as a reference or can be used in local power sector resilience assessment workshops. For questions or more information on the slides, use the "Ask An Expert" feature on the Resilient Energy Platform website.

Outline

Power Sector Threats:

1. Natural Threats
2. Technological Threats
3. Human-Caused Threats

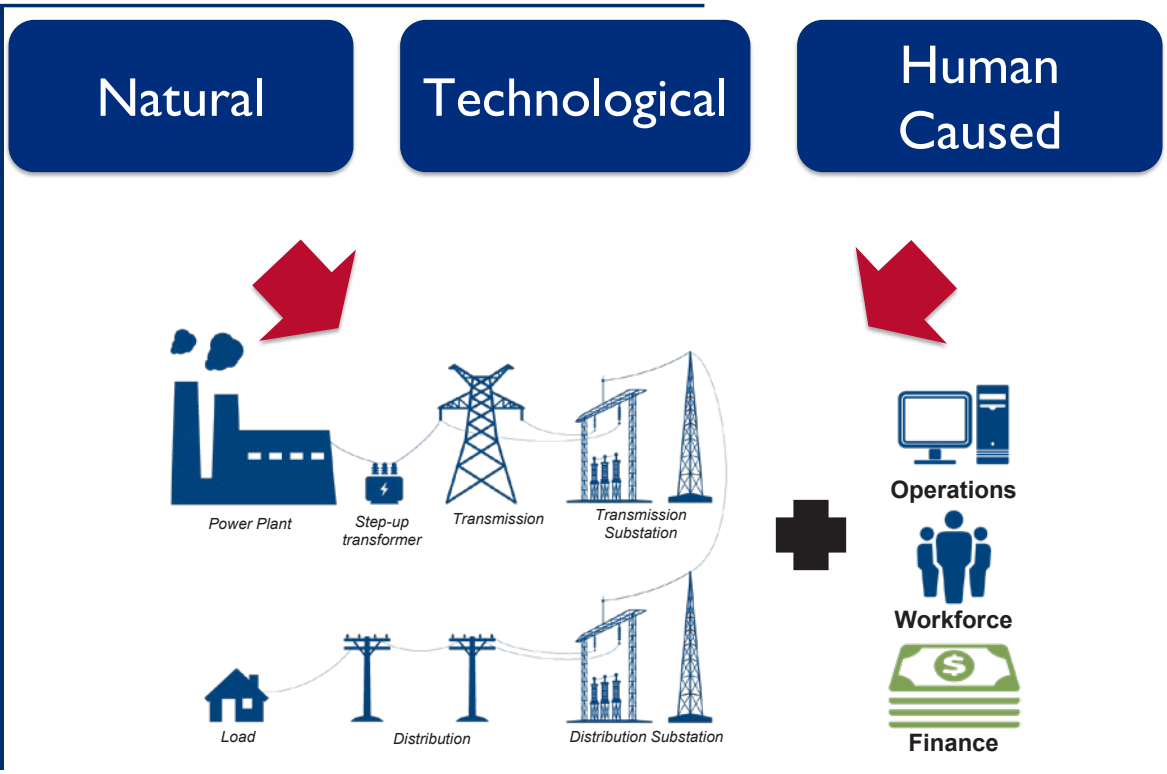
Definitions

Threat*: Anything that can damage, destroy or disrupt the power sector. Threats can be natural, technological, or human-caused. Threats are typically not within the control of power system planners and operators and can include wildfires, hurricanes, storm surges, system malfunctions, and cyber attacks. This term is often used interchangeably with *hazard*.

Hazard: Often used interchangeably with *threat*.

*Many different definitions exist for the terms threats, hazards, impacts, vulnerabilities, and resilience that encompass different factors. We propose these "working definitions" for the purposes of this guidebook. We invite readers to explore other definitions in the future.

Overview of Power Sector Threats



Natural Threats

Natural Threats May Include:

- Cyclones (typhoons and hurricanes)
- Extreme precipitation
- Extreme heat and cold
- High Winds
- Drought
- Landslides
- Earthquakes
- Volcanic Eruptions
- Sinkholes
- Space Weather Events (such as solar flares)
- Wildlife Interactions
- Lightning
- Flooding
- Others

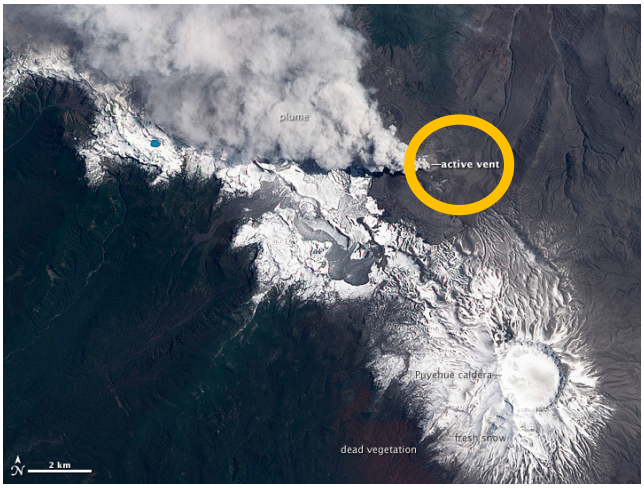


Figure. Nasa. Satellite: Aqua. Eruption of Puyehue-Cordón Caulle Volcano from June 2011, Chile from:https://eoimages.gsfc.nasa.gov/images/imagerecords/76000/76810/puyehue_ali_2011357.jpg

Natural Threats Vary Widely and are Location Specific

Example: projected increases (green) and decreases (red) in hydropower generation. Due to climate impacts on river flows, South Africa, Brazil, Afghanistan, Tajikistan, and Venezuela are forecast to have large reductions in hydropower potential.

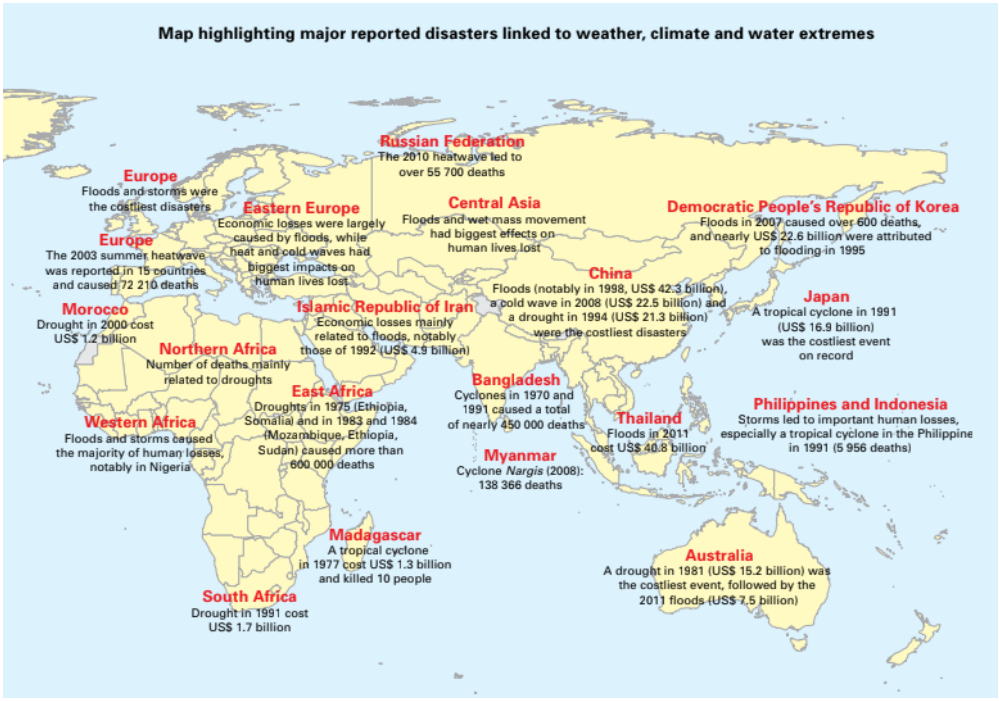
Source: Hamududu and Killingtveit, 2010.

Natural Threats Vary Widely and are Location Specific

Example: In one given year, climate shifts can have vastly different effects—from flooding in East Africa to drought in Indonesia.

Source: Tan, Chun Knee, 2010, https://ourworld.unu.edu/en/indonesia-drought-kenya-flooding

Economic Impacts of Natural Threats



Source: World Meteorological Organization, 2015 ATLAS OF MORTALITY AND ECONOMIC LOSSES FROM WEATHER, CLIMATE AND WATER EXTREMES (1970–2012)

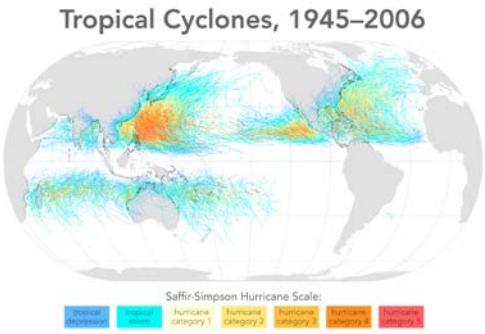
Natural Threats: Hurricanes/Typhoons/Cyclones

Climate Forecasts Vary:

- Hurricane/typhoon/cyclone intensity increases of 2–11% by 2100.
- Hurricane/typhoon/cyclone frequency decreases of 6–34% by 2100.
- Substantial increases in the frequency of the most intense cyclones
- Increases of the order of 20% in the precipitation rate within 100 km of the storm center.
- Large variation by basin
- Detection and attribution difficult

Source: Kuntson, et. al., 2010, Tropical Cyclones and Climate Change, Nature Geoscience

Figure. NASA https://earthobservatory.nasa.gov/images/82372/typhoon-haiyan-approaches-vietnam



Source: Citynoise at English Wikipedia, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=18049077

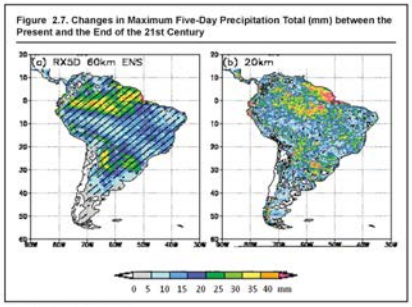
Natural Threats: Extreme Precipitation

Climate Forecasts:

- Atmospheric water-holding increases roughly exponentially with temperature.
- Observations confirm theory.
- Greenhouse gas increases have contributed to observed heavy precipitation event intensification

Source: Seung-Ki Min, et. al., 2011, Human contribution to more-intense precipitation extremes, *Nature*

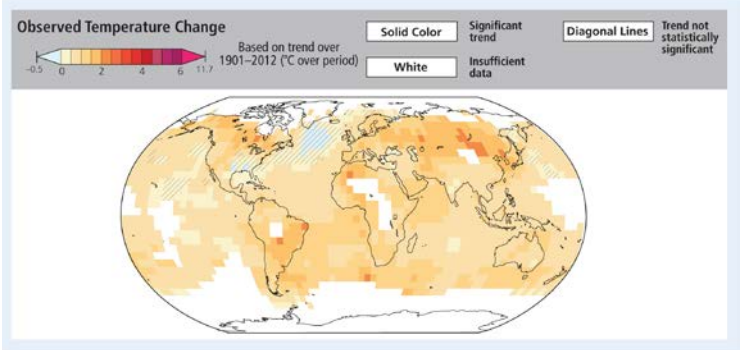
Mekong River flooding threat to distribution infrastructure in Vientiane, Lao PDR
Photo: Sherry Stout, NREL

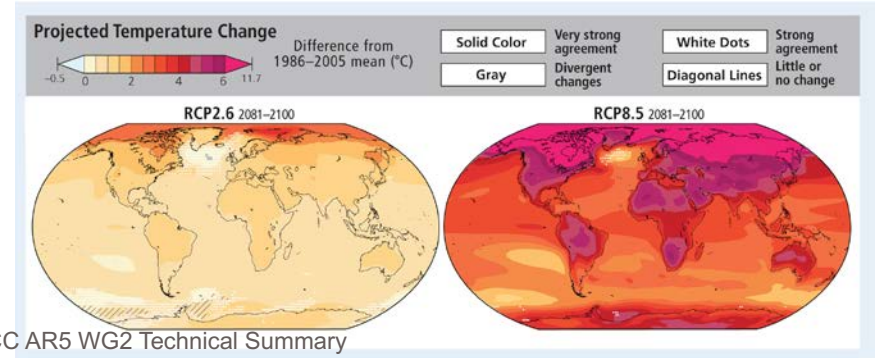


Source: Vergara, Walter; Scholz, Sebastian M.. 2011. Assessment of the Risk of Amazon Dieback. A World Bank study. World Bank. © World Bank. https://openknowledge.worldbank.org/handle/10986/2531 License: CC BY 3.0 IGO.

Natural Threats: Extreme Heat

Observed and Projected Global Average Temperature Change





Source: IPCC AR5 WG2 Technical Summary

Natural Threats: Drought

- Increased precipitation may not mean fewer droughts
- Increases in temperature mean more severe droughts are possible
- In presently dry regions, drought frequency will *likely* increase by the end of the 21st century*
- Drought can impact the frequency and intensity of secondary hazards such as wildfire and wind

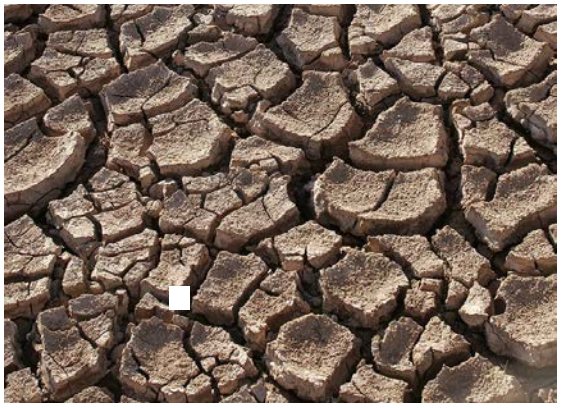


Figure. Drought. Tomas Castelazo, www.tomascastelazo.com / Wikimedia Commons

**Representative Concentration Pathway 8.5 IPCC AR5 WG2 Technical Summary*

Natural Threats: Wildlife Interactions

- Wildlife such as squirrels, birds, snakes, and others can pose a threat to power sector infrastructure.
  - This may be in the form of interactions with transmission and distribution lines or nesting in substations.

Squirrels have caused hundreds of times the number of power outages as humans.[1]
Photo: "Brave Squirrel II" by judy h is licensed under CC BY-NC-SA 2.0

1. https://cybersquirrel1.com/

Technological Threats

Technological and Human-caused Threats

Technological and human-caused threats involve unknown technological issues and human behavior and are therefore difficult to predict.

Image: Electricity Theft In India
Photo: Braden Gunem, https://www.nature.com/articles/nenergy201644#rightslink

Technological Threats

Technological threats are non-natural threats that directly affect technology and infrastructure.

Examples:

- Defects in materials
- Poor workmanship or design
- Fires from system faults
- Technology failures
- Unpredictable load shifts
- Aging infrastructure

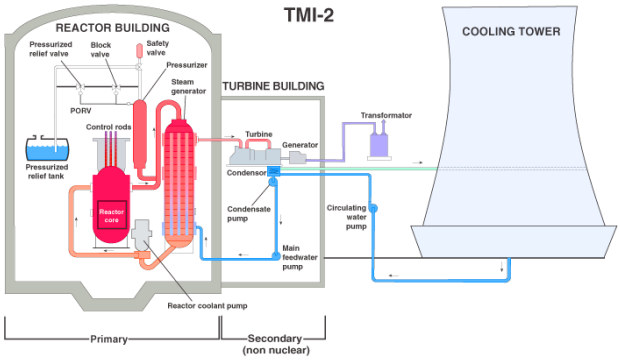
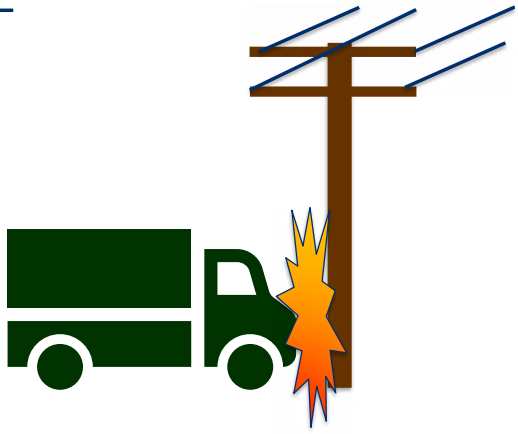


Figure. Three Mile Island Plant. http://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/three-mile-island-accident.aspx

Human-Caused Threats

Human-Caused Threats: Accidents

- There are different types of human threats.
- Accidents are unintentional acts that can impact the power system. Common accidents include:
  - Accidental cutting of power lines
  - Vehicles hitting power poles and ground based electrical equipment
  - Electrical workers causing equipment failures
  - Informal electrical connections
- Do accidents occur in your power sector?
  - We are sure they do!



Human-Caused Threats: Incompetence

- Due to a number of reasons, a lack of knowledge or experience of those working in the power sector can also be a threat to the system.

Examples:

- Lack of adequate worker training
- Incompetence in system management
- Lack of emergency plans

Human-Caused Threats: Bad Actors

Bad actors may arise for any number of reasons:

- Some are simply disgruntled power customers that seek to damage power company equipment.
- Others may be part of a more organized group seeking political action against the state or individual companies.

Actions may include:

- Intentional cutting of lines or destroying of equipment
- Arson
- Cyber attacks
- Acts of terror

Figures from top. D. Schroeder 2017. NREL. Figure # 18981.; https://pixabay.com/en/burglar-thief-criminal-crime-man-308858/

Key Takeaways

Threats are not typically within the control of system planners and operators and can include:

- Natural Threats
  - Cyclones
  - Extreme precipitation
  - Extreme heat or cold
  - Wildlife interactions
  - Many others
- Technological Threats
  - Defects in materials
  - Poor workmanship or design
  - Many others
- Human-Caused Threats from:
  - Accidents
  - Bad Actors

Figure. Siemens. Siemens platform managing North America's largest transmission grid (PJM Regional Transmission Organization Control Room). *Photo: PJM Interconnection*
https://w3.siemens.com/smartgrid/global/en/projects/pages/pjm.aspx

IMPACTS

Guide to Impacts

Introduction

Impacts describe the effects that threats have on power system infrastructure, systems, or processes. The identification of impacts associated with each threat is an important step in assessing vulnerabilities. Every threat could impact the power system in multiple ways. For example, strong winds from tornadoes could cause transmission poles and lines to fall—resulting in power outages, additional costs for repairs, and financial loss due to decreased generation requirements. For more information on impacts, refer to the presentation at the end of this section.

To identify power system impacts:

- Identify impacts to the power sector
- Identify impacts to the end user

Key Terms

Before identifying impacts, it is helpful to clarify a few key terms in relation to power sector resilience.

Threats—anything that can expose a vulnerability and, either intentionally or accidentally, can damage, destroy, or disrupt the power system. Threats can be natural, technological, or human caused. Threats are not typically within the operator's control. They can include wildfires, hurricanes, storm surges, cyberattacks, and more. For additional information on threats, refer to the *Threats* section of this guidebook.

Impacts—the extent to which a threat affects power sector infrastructure, systems, or processes (e.g., a tornadoes causes wind damage to transmission lines).

1. Identifying Impacts on the Power Sector

Threats can impact the power sector in many ways and are not limited to physical effects on infrastructure. Different types of impacts include:

- **Effect on delivery of power**—the percentage of service disrupted, effects on power quality, etc., due to impacts on generation, transmission, or distribution.
- **Effect on capital and operating costs**—additional costs incurred during a power disruption and costs to resume or maintain the reliable operation of the power system.

2. Identify the Impacts on the End User

Threats also impact the various end users of the power system in different ways. These impacts include health and safety impacts to the population and environmental effects, such as the release of toxic materials, effects on biodiversity, changes to an area's ecosystem, impacts on historic sites, and others. End users include the general population, communications industry, transportation, government infrastructure, and medical services.

Activity: Power System Impacts

Goal of this Activity

In this activity, you will identify the impacts associated with threats to your power sector.

Introduction

Impacts describe the effects that threats have on power system infrastructure, systems, or processes. The identification of impacts associated with each threat is an important step in assessing vulnerabilities. Every threat could impact the power system in multiple ways. For example, strong winds from tornadoes could cause transmission poles and lines to fall—resulting in power outages, additional costs for repairs, and financial loss due to decreased generation requirements.

The output of this activity will provide an initial list of the impacts associated with the top five threats identified earlier.

Key Terms

Before identifying impacts, it is helpful to clarify a few key terms in relation to power sector resilience.

Threats—anything that can expose a vulnerability and, either intentionally or accidentally, can damage, destroy, or disrupt the power system. Threats can be natural, human caused, or technological. Threats are not typically within the operator's control. They can include wildfires, hurricanes, storm surges, cyberattacks, and more. For additional information on threats, refer to the *Threats* section of this guidebook.

Impacts—the extent to which a threat affects power sector infrastructure, systems, or processes (e.g., a tornadoes causes wind damage to transmission lines).

Exercise: 1
Identifying Impacts

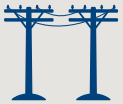
For your top five threats from the *Identifying Threats* activity, consider the impacts of each threat. Fill in each row of the table below, listing the impacts of each threat on the various components of the power system.

Discussion Questions

To guide the discussion, consider the following questions:

1. Has critical power sector infrastructure ever gone off-line or experienced reduced operability?
    - How many hours, days, or weeks was the infrastructure off-line or inoperable?
2. What was the impact (at the city, national, or multinational scale) of losing this power sector infrastructure?
    - Impact on power sector?
    - Impact on local, city, and regional government operations?
    - Impact on society?
    - Impact on national government operations?

Exercise 1: Identify the potential impacts that each of the top five threats may have on the power sector

	Generation 	Transmission 	Distribution 	Customer 	Operations 	Workforce 	Financial 	Other
Example *Earthquakes*	*Reduced generation capacity*	*Fallen transmission poles*	*Fallen distribution poles or cut lines*	*Loss of power*	*Need to compensate for load imbalance*	*Unable to access damaged infrastructure due to debris blocking access roads*	*Cost of rebuilding transmission infrastructure, loss of revenue, assets, production*	
Threat 1								
Threat 2								
Threat 3								
Threat 4								
Threat 5								

Exercise 2: Identify the potential end-user impacts of the top five threats in Exercise 1

Use this chart to identify potential impacts of the top five threats. Fill in the chart below, noting how the threats at left impact the power sector dependent systems at the bottom of the chart.

	Population 	Communications 	Transportation 	Government Operations 	Medical Service 	Other
Example *Strong Winds*	*Loss of power and economic activity*	*Disruption in communications for emergency services*	*Increased traffic and accidents due to traffic light outage*	*Lack of access to vital computer systems for governance*	*Lack of power in critical infrastructure*	
Threat 1						
Threat 2						
Threat 3						
Threat 4						
Threat 5						

Impacts Introduction

Power Sector Resilience Planning Guidebook

The following slides are intended to provide additional background information and examples of types of power system impacts. They can serve simply as a reference or can be used in local power sector resilience assessment workshops. For questions or more information on the slides, use the "Ask An Expert" feature on the Resilient Energy Platform website.

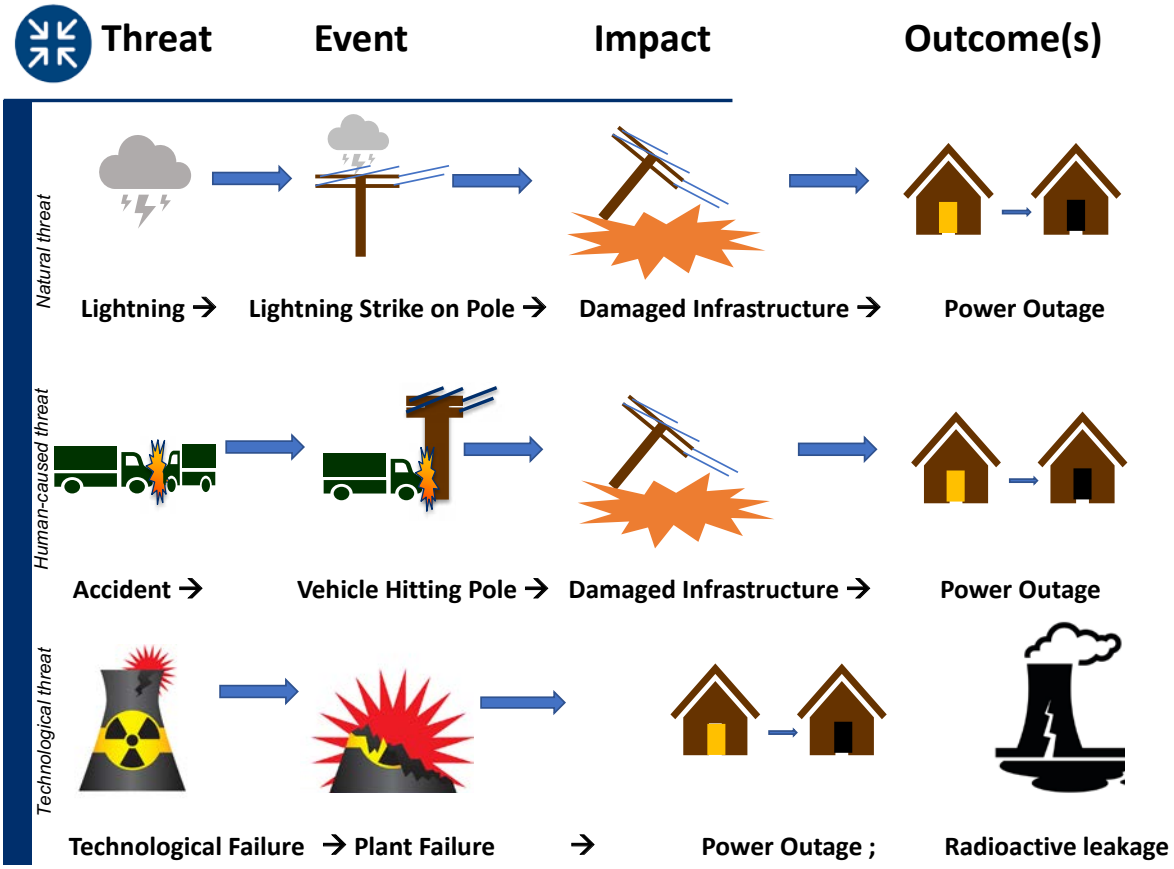
What Are The Impacts of Threats?

Impacts describe the extent to which threats affect power sector infrastructure, systems or processes, such as a cyclone that causes wind damage to transmission lines.

Types of Impacts

Threats can impact the power sector in many ways. Impacts are not limited to physical effect on infrastructure:

- **Effect on delivery of power**: the percentage of service disrupted, effects on power quality, etc.
- **Effect on capital and operating costs**: additional costs for the reliable operation of the power system
- **Extent of health and safety impacts to the population**: metrics of health and safety for the population
- **Extent of environmental effects**: metrics of the release of toxic materials, effects on biodiversity, changes to area's ecosystem, impacts on historic sites, and others



VULNERABILITIES

Guide to Vulnerabilities

Introduction

Identifying and scoring power sector vulnerabilities are vital components of the power sector resilience planning process. These processes evaluate the degree to which a power system or power system components, such as generators or transmission lines, may be adversely affected (e.g., damaged, destroyed, or disrupted operation) by a broad range of potential threats and their impacts. The purpose of this step is to learn about power system objectives, understand the key resources and systems necessary for staff to complete their work, and understand what would happen if those resources or systems were compromised. The next step of the power sector resilience planning process is a risk assessment, which is based on the likelihood of threats occurring and the severity of potential vulnerabilities. For more information on vulnerabilities to the power sector, refer to the presentation at the end of this section of the guidebook.

Key Terms

Vulnerabilities—weaknesses within infrastructure, processes, and systems, or the degree of susceptibility to various threats. Different measures can be taken to reduce vulnerability or improve adaptive capacity to threats to the power sector.

Threats—anything that can expose a vulnerability and damage, destroy, or disrupt the power system. Threats can be natural, technological, or human caused. Threats are not typically within the power system operator's control. They can include wildfires, hurricanes, storm surges, and cyberattacks.

The identification of vulnerabilities is a key step in the power sector resilience planning process—following the identification of threats and their associated impacts. Table 3 describes the types of infrastructure, processes, and systems that may be evaluated in a power sector vulnerability assessment.

This document introduces the key steps in identifying power system vulnerabilities:

1. Assessing existing conditions
2. Identifying vulnerabilities
3. Scoring vulnerabilities

Table 3. Key Power System Infrastructure, Processes, and Systems Included in Vulnerability Assessments

Key Power System Infrastructure, Processes, and Systems
Asset security (perimeter fencing, guard stations)
Critical transportation routes for fuel and supplies
Fuel storage
Electric feeders
Substations
Transformers
Switching capability
Reserve capacity
Generation stations
Transmission and distribution networks
Power sector workforce
Critical customers and demands
Others, depending on context

1. Assess Existing Conditions

An understanding of the existing conditions of the power system in terms of location of assets, operational practices, political threats, and other factors, helps determine the ability of the power sector to respond and adapt under different operational conditions if a disruption were to occur[1]. This step is conducted to identify these factors and highlight the assets that need to be protected under various planning scenarios. An existing-conditions assessment begins with stakeholder interviews, data collection, and literature reviews of resources that include:

- Integrated resource plans
- Emergency plans
- Maps and geographic data
- Utility information
- Historical data relating to disasters, extreme temperatures, and grid outages
- Other available, relevant resources.

2. Identify Vulnerabilities

In the planning process, vulnerabilities are often identified together with threats and impacts. Understanding existing conditions, as well as potential threats and vulnerabilities, along the planning horizon for infrastructure, processes, and systems is important to enhancing resilience.

Many different types of vulnerabilities exist and need to be considered. Vulnerabilities may occur within the infrastructure (e.g., generation, transmission, distribution, customers, and others) or system processes (e.g., operations, workforce, planning, financial, and others) as illustrated in Table 4. Infrastructure vulnerabilities are often easy to address but tend to be expensive, while process vulnerabilities tend to be difficult to address but usually require relatively inexpensive fixes. Other location-specific vulnerabilities must also be identified to ensure a comprehensive list of potential vulnerabilities.

Table 4. Examples of Vulnerabilities

Examples of Vulnerabilities
Lack of backup systems and supplies or single points of failure in transportation route, electrical line, water supply, or fiber-optic cable.
Location prone to flooding, fire, etc.
Lack of cybersecurity defenses
Poorly resourced or under-trained workforce
Location-specific vulnerabilities identified by the resilience assessment team

Stakeholder interviews conducted by the resilience assessment team are a critical component of identifying vulnerabilities. Stakeholders have information that will inform—and may improve—the assessment and which may not be found in existing documents. This includes historical and anecdotal information about potential vulnerabilities.

Stakeholders include staff that can identify key operations and assets as well as those who provide funding or services and manage systems and operations. Stakeholders may also include staff in different agencies, including grid operators, utilities, the ministries of energy or environment, independent power producers, and more. For information on forming resilience assessment teams and engaging stakeholders, refer to Step 1 of NREL's Resilience Planning Roadmap (https://www.nrel.gov/resilience-planning-roadmap/).

3. Score Vulnerabilities

The next step in the process is to score the severity of the identified vulnerabilities. These scores will be combined with the threat likelihood scores (see the *Threats* section of this guidebook) to determine the total risk to the power system. Vulnerability severity scores are assigned using professional judgment—with information from the stakeholder interviews, data collection, and literature review of Steps 1 and 2, *Assess Existing Vulnerability Conditions* and *Identify Vulnerabilities,* respectively.

A review of documents and studies (e.g., development plans, community development 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, utility disaster response plans, and others) can aid in the scoring of vulnerabilities. Often, studies are conducted by outside experts (e.g., experts on earthquakes or cyclones), providing resources and insight that would be beyond the capabilities of most assessment teams.

The assessment team determines the severity score of each vulnerability (the magnitude or extent to which each vulnerability could negatively impact the power sector if it were to occur) through a scoring system of ranking the severity (magnitude of consequence) on the power system from low to high. Table 5 shows the qualitative and quantitative scores and associated threshold descriptions used to assign vulnerability scores. Threshold descriptions are provided as guides that can help in assigning scores. The score represents the degree to which an affected process, system, or population could be adversely affected as a result of a disruptive event (e.g., flooding, a

large storm, or attack). In scoring each vulnerability, the following categories are considered:

- **Effect on delivery of power**—the percentage of service disrupted, effects on power quality, etc.
- **Effect on capital and operating costs**—additional costs for the reliable operation of the power system
- **Extent of health and safety impacts to the population**—number of people and severity of potential impact on the health and safety of the population
- **Extent of environmental effects**—metrics of the release of toxic materials, effects on biodiversity, changes to an area's ecosystem, impacts on historical sites, and others.

Table 5. Qualitative and Quantitative Vulnerability Severity Scores and Threshold Descriptions

Vulnerability Severity Score		Threshold Descriptions
Categorical	**Numerical**	
High	9	Highest magnitude of consequence. Entire power system would be impacted. Extreme financial impacts would exist.
Medium-High	**7**	Significant consequences to the organization. Majority of population served would be impacted. Staff tasks would be switched to emergency/critical operations. Significant financial impacts would exist.
Medium	5	Medium magnitude of consequence. The organization would be somewhat affected. Specific systems or functions would be substantially interrupted, but not all. Financial impacts would be expected to change budgeting plans or require reallocation of funds.
Low-Medium	3	Slightly elevated consequence to the organization. The power sector may need to temporarily transition operations to backup systems to resolve failure. Limited financial impacts may become apparent.
Low	1	Lowest magnitude (or severity) of consequence to the organization. The power sector would experience little to no affect or an in-place backup system would resolve the failure.

Activity: Developing Vulnerability Statements and Assigning Vulnerability Severity Scores

Goal of this Activity

In this activity, you will identify potential vulnerabilities that your power sector may face from possible threats, form vulnerability statements, and assign a severity score to each.

Introduction

The output of this activity will provide a foundation for understanding the vulnerabilities that your power sector may face at different planning scales of concern, such as city, national, or regional/multinational.

Exercise 1: Developing Vulnerability Statements

Use the table below to identify the vulnerabilities associated with the top five threats identified in prior activities. The vulnerability statement answers the "why" question or "why might this threat impact the power sector?" For each of the threats and associated impacts in the table below, begin by asking the question, "why does this threat impact the power sector?" Reaching the final vulnerability of the power sector may require asking this question multiple times. The vulnerability statement should not propose a solution—instead, it offers an objective statement of what makes the power system vulnerable. Developing these statements likely requires discussions with colleagues because there is no simple formula.

Key Terms

Before identifying vulnerabilities, it is helpful to clarify a few key terms in relation to power sector resilience.

Vulnerabilities—weaknesses within infrastructure, processes, and systems, or the degree of susceptibility to various threats. Different measures can be taken to reduce vulnerability or improve adaptive capacity to threats to the power sector. Vulnerabilities are typically identified through stakeholder interviews, technical analyses, and/or literature reviews[1].

Threats—anything that can expose a vulnerability and damage, destroy, or disrupt the power system. Threats can be natural, human caused, or technological. Threats are not typically within the power system operator's control. They can include wildfires, hurricanes, storm surges, and cyberattacks. For additional information on threats, refer to the *Threats* section of this guidebook[1].

Impacts—the extent to which a threat affects power sector infrastructure and processes (e.g., a typhoon causes wind damage to transmission lines which disrupts power to customers for a specific duration).

Exercise 2. Vulnerability Severity Scores

After drafting all five vulnerability statements in the table below, we can assess the severity of each vulnerability on the power sector and assign a severity score. As described in the *Guide to Vulnerabilities* section, assign each vulnerability statement a severity score based on how problematic the exposure of this vulnerability could be. Assign one of the following scores to each of the five vulnerabilities listed below:

High | Medium-High | Medium | Low-Medium | Low

Refer to the Guide to Vulnerabilities section for a description of the thresholds for this scoring system.

Threats	Impacts		Vulnerability Statements	Severity Scores
Example *Lightning strike*	*Damaged poles, power outage*	***Why?*** →	*Lack of lightning protection on transmission and distribution equipment increases the likelihood of a lightning strike damaging transmission poles, leading to a power outage.*	*Medium*
Threat 1		***Why?*** →		
Threat 2		***Why?*** →		
Threat 3		***Why?*** →		
Threat 4		***Why?*** →		
Threat 5		***Why?*** →		

Vulnerabilities Introduction

Power Sector Resilience Planning Guidebook

The following slides are intended to provide additional background information and examples of power system vulnerabilities. They can serve simply as a reference or can be used in local power sector resilience assessment workshops. For questions or more information on the slides, use the "Ask An Expert" feature on the Resilient Energy Platform website.

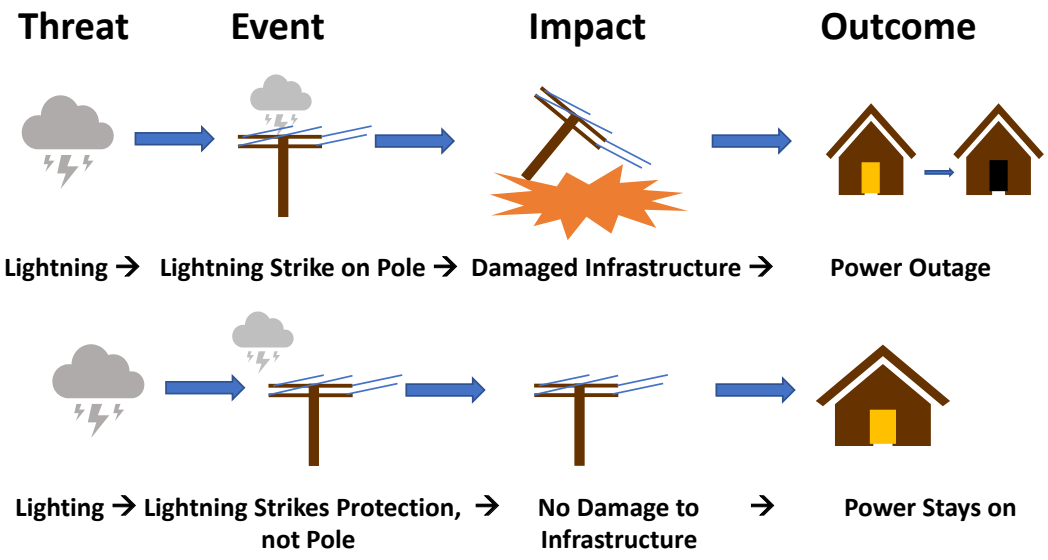
Key Messages

- Power sector vulnerabilities usually fit into two categories:
  - Infrastructure
  - Process (and systems)
- Both types of vulnerabilities need to be considered when assessing resilience options for the power sector.
- Infrastructure vulnerabilities are often easy to address but tend to be very expensive.
  - Power system hardening
  - Large infrastructure development
- Process vulnerabilities tend to be difficult to address but usually require relatively inexpensive fixes.
  - Trainings
  - Development of codes and standards

What Are Vulnerabilities?

Vulnerabilities are weaknesses within infrastructure, processes, and or systems or the degree of susceptibility to various threats. Different measures can be taken to reduce vulnerability or improve adaptive capacity to threats to the power sector.

Threats & Impacts Expose Vulnerabilities



Vulnerability: Lack of Lightning Protection on Transmission and Distribution Equipment

Power Sector Vulnerabilities

Infrastructure

- Generation
- Transmission
- Distribution
- Customer

System/ Process

- Operations
- Workforce
- Planning
- Financial

Power Sector Vulnerabilities

Vulnerabilities can also be categorized following the threats that may expose them.

Types of threats	Vulnerability examples
Physical	Lack of backup systems and supplies or single points of failure in transportation route, electrical line, water supply, or fiber optic cable.
Natural	Location prone to flooding, fire, etc.
Technological (Hardware, Software or Media)	Lack of cyber security defenses
Human	Poorly resourced or under-trained workforce
Others	Location-specific vulnerabilities identified by the resilience assessment team

Infrastructure Vulnerabilities

Generation

- Aging infrastructure is more vulnerable to impacts from threats
- Insufficient cooling water supply
- Fuel supply uncertainties
  - Water for hydro
  - Coal, gas, biomass

Photo: US Army Corps of Engineers.

- Undersized capacity for future needs
- Restricted supply chain for parts and fuels

Transmission

- Infrastructure design susceptible to failure
- Aging infrastructure
- Undersized power systems
- Transmission bottlenecks
- Lack of redundant lines
- Restricted supply chain for parts and fuels
- Exposed transmission & distribution lines in high wind & high threat environments

345 kV

Source: iStock

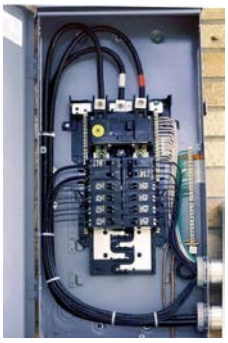
Distribution

- Infrastructure design susceptible to failure
- Infrastructure design susceptible to interference from people and wildlife
- Vegetation interactions with distribution network, such as tree limbs contacting power lines
- Aging infrastructure
- Undersized power systems for rapid population growth
- Other infrastructure can negatively impact power system
- Lack of redundant power for critical loads
- Restricted supply chain for parts and fuels
- Poles not buried to adequate depth
- Workforce capacity lacking in installation requirements for resilience

Photos courtesy Michael Coddington, NREL

Customer (Demand)

- Interference from non-compliant equipment
- Unauthorized self-generation
- Unpredictable loads
- Informal/unauthorized connections (e.g., electricity theft/piracy)



Photos courtesy Michael Coddington and Sherry Stout, NREL

Process Vulnerabilities

System Operations

- Limited operational flexibility
- Limited generation forecasting
- Lack of UPS/backup power on operation centers
- Lack of cyber and physical security measures
- Lack of granular data on infrastructure and energy consumption/needs
- Lag time in communications between system components

Figure. Siemens. Siemens platform managing North America's largest transmission grid (PJM Regional Transmission Organization Control Room). *Photo: PJM Interconnection*
https://w3.siemens.com/smartgrid/global/en/projects/pages/pjm.aspx

Workforce and Human Resources

- Restricted supply chain across all operations
- Under-resourced/trained workforce
- Access time for workforce during emergency operations

Figure: *"NOLA stoplight repair" by opacity is licensed under CC BY-NC-ND 2.0*

Planning

- Resilient design not included in broader planning (IRPP-Integrated Resource and Resilience Planning)
- Inaccurate predictions for load growth
  - Generation needs
  - Destruction needs
- Lack of updated codes/standards
- Lack of short, mid, and long term plans for infrastructure upgrades
- Lack of coordination with other government agencies
- Lack of coordination and communication between power sector stakeholders
- Lack of granular data on infrastructure and energy consumption/needs
- Lack of formal agreements for emergency response with surrounding countries

Figure. Dennis Schroeder. NREL. 2010. NREL members and AIST (Advanced Industrial Science and Technology) members meet at SolarTAC in Aurora at the site of a concentrated solar PV system being tested by the joint partnership. Image #. 19109

Financial

- Insufficient capital for system upgrades
- Difficulty in securing financing for infrastructure projects
- Lack of funding for workforce development
- Low rates of customer bill collection
- Heavy energy subsidies that are not recovered through rates

Discussion and Key Takeaways

- What vulnerabilities do you think of when you consider your power sector?

- Multiple vulnerabilities can impact the power sector. These usually fall into two categories:
  - Infrastructure
  - Process

- Infrastructure vulnerabilities relate to the built environment.
  - Easier to fix, but more $$

- Process vulnerabilities relate to human interactions with the power sector.
  - Less $$, more difficult

RISK ASSESSMENTS

Guide to Risk Assessments

Introduction

Risk is defined as the potential for loss, damage, or destruction of key resources or power system assets resulting from exposure to a threat. Risk is evaluated as the product of the threat likelihood and vulnerability severity scores. Analyzing risk is a key step in vulnerability assessments and allows for the prioritization of vulnerability mitigation actions. This document presents the steps involved in analyzing risks:

- Assess risks
- Score risks
- Evaluate risks
- Identify levels of risk acceptance

Risk—the potential for loss, damage, or destruction of key resources or power system assets resulting from exposure to a *threat*. Risk is evaluated as the product of the *threat likelihood score* and the *vulnerability severity score*.

1. Assess Risks

Not all threats directly influence each vulnerability. As such, the first step involves determining which threats and vulnerabilities are associated. The matrix shown in Figure 2 is one way to do this.

2. Score Risks

There are many different methodologies for scoring risk. The method highlighted here is based on that developed by Anderson et al, 2018, and uses risk matrices to score and prioritize risks. Risk matrices show the relationships between threats and vulnerabilities. The severity score for each vulnerability is multiplied by the threat likelihood score to create a risk score for each specific threat-vulnerability combination. Risk scores are scaled from one to 100, with higher scores corresponding to higher risks. This requires assigning quantitative values to the qualitative thresholds previously presented in

		VULNERABILITIES								
		Infrastructure design susceptible to failure	Aging infrastructure	Undersized power systems	Lack of redundant generation for at least 30% of load	Lack of operational flexibility	Lack of capital for system upgrades	Lack of properly trained workforce	Lack of coordination with other government agencies	No formal disaster or emergency plans in IRRP
THREATS	More frequent flooding	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Increased annual average temperature	Yes	Yes	Yes	No	Yes	No	No	No	No
	Increased intensity of typhoon winds	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Increased number of days with thunderstorms/lightning	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Typhoons	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Increased landslides	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
	Increase in magnitude of hottest annual temperature	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes
	Increased change of drought/low water levels	No	No	No	No	Yes	Yes	No	Yes	Yes
	Increased number of days with 95°F (35°C) or higher per year	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
	Increased number of days with heavy rainfall	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Increased precipitation on days with precipitation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Infrastructure failure	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Figure 2. Example matrix linking threats to vulnerabilities

the threat and vulnerability sections of this guidebook. The risk is calculated as:

Risk score = Threat likelihood score X Vulnerability severity score

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. No risk score is assigned where threats are not associated with a vulnerability, and the matrix is blank at this intersection. The final risk score is shown in the matrix and used to prioritize the vulnerabilities (Figure 3).

3. Evaluate Risks

The heat map (Figure 3) portrays high-risk scores as red cells (top left) and low-risk scores as orange or yellow values (bottom right). Blank cells indicate a lack of connection between that combination of a threat and vulnerability. This format helps in displaying the relative importance of different risks and provides insight into potential causes of—and vulnerabilities to—disruptive events. This can also enable decision makers to identify tailored resilience solutions for certain vulnerability-threat combinations. For example, a decision maker could weigh specific vulnerabilities against the likelihood of different threats and be well-positioned to direct resources to priority areas.

			THREATS												
			Extreme Precipitation	Extreme Temperatures	Flooding	Landslides	Wildfire Interactions	Wind	Human Actions: Bad Actors	Human Actions: Accidents	Technological Design	Technological Materials	Technological Workmanship	Drought	Lightning
			Threat Likelihood Score												
			9	7	7	7	5	5	5	5	5	5	5	5	1
VULNERABILITIES	Power system rules, regulations, and technical standards do not meet current and changing environmental conditions	Vulnerability Severity Score 9	81		63	63			45		45	45			
	Corruption leads to code violations	9	81			63	45	45	45			45	45		
	Dam construction does not follow design specifications	9	81	63		63	45	45	45	45	45	45	45		
	Installation does not follow design specifications	9			63	63	45		45	45	45		45		
	Lack of compliance with codes in design	9	81	63	63	63	45	45			45	45	45		
	System operations are not flexible enough to respond to changes in demand and supply	7	63	49	49			35			35			35	7
	Demand forecasting is not responsive to changing load conditions	7	63	49							35			35	
	Heavy power sector reliance on hydro generation	7		49	49						35			35	
	Inadequate domestic generation capacity requires costly energy imports	7		49	49	49	35	35	35	35	35	35	35	35	

Figure 3. Example risk matrix

4. Identify levels of risk acceptance

A comprehensive risk evaluation will likely yield far more threat-vulnerability pairs than can be addressed. In this case, the next step of the assessment involves using experience and professional judgment to form a plan for how many and on which of these pairs to focus. Making these decisions serves to identify what threshold of risk is tolerable and possible, and which threat-vulnerability pairs are critical and feasible to address.

In this decision-making process, some factors to consider are:

- Which vulnerabilities are affected by the largest number of risks?
- Whether priority will be given to the high-frequency risks or the highest-impact risks.
- What level of risk is the power sector capable of realizing—financially, technologically, and logistically?

After the decision makers have identified these levels of risk acceptance and focused their list of priorities, they should be sure to re-engage relevant stakeholders for feedback, amendments, and approval.

Activity: Country Risk Assessment

Goal of this Activity

In this activity, you will assess risks to your power sector by linking and scoring the vulnerabilities and threats you determined in previous activities.

Introduction

The output of this activity will provide a foundation for identifying and prioritizing resilience solutions in the coming steps of the process. Risk is the product of both the vulnerability and the likelihood of the threat that can expose it.

Not all threats directly influence each vulnerability. The first step in assessing risk involves determining which threats and vulnerabilities are linked. Risk scores are then calculated for all linked threats and vulnerabilities. The scores are often placed in a risk-matrix heat map, as shown in the *Guide to Risk Assessments*, which highlights the highest-risk vulnerability-threat pairs. This matrix can use either quantitative or qualitative scores. For a quantitative analysis, calculate risk using the formula:

$$\textit{Risk Score} = \textit{Threat Likelihood Score} \times \textit{Vulnerability Severity Score}$$

Key Terms

Before assessing risk, it is helpful to clarify a few key terms in relation to power sector resilience.

Vulnerabilities—weaknesses within infrastructure, systems, or processes that can be modified and mitigated to either prevent a disruption from occurring or lessen the impact of a disruption. Vulnerabilities are identified through stakeholder interviews with technical base and country staff that are familiar with system operations and maintenance as well as through review of planning documents[1].

Threats—anything that can expose a vulnerability, either intentionally or accidentally, and can damage, destroy, or disrupt the power system. Threats can be natural, human caused, or technological. Threats are not typically within the control of power system planners and operators. They can include wildfires, hurricanes, storm surges, and cyberattaks. For additional information on threats, refer to the *Guide to Threats* section of this guidebook.

Risk—the potential for loss, damage, or destruction of key resources or power system assets resulting from exposure to a *threat*. Risk scores are the product of the *threat likelihood score* and the *vulnerability severity score*.

Exercise 1: Assessing Risk

This is an example of how risk scores are calculated for demonstration and educational purposes. In an actual risk assessment, we will use a more sophisticated, computer-based spreadsheet to score and assess risk.

1. List your top five vulnerabilities in the left column of the table in order from highest severity to lowest severity, as you determined in *Activity: Developing Vulnerability Statements and Assigning Vulnerability Severity Scores*.
2. List your top five threats in the top row, from most likely to least likely, as determined in *Activity: Identifying Threats*.
3. If a vulnerability in any given row is linked with a hazard in any column, write *"yes"* or *"no"* next to "Linked."
4. In the boxes for the linked vulnerability-threat pairs, assign each pair a risk score equal to threat likelihood score x vulnerability severity score.

	Threat 1: _____ _____ **Likelihood Score:**____	**Threat 2:** _____ _____ **Likelihood Score:**____	**Threat 3:** _____ _____ **Likelihood Score:**____	**Threat 4:** _____ _____ **Likelihood Score:**____	**Threat 5:** _____ _____ **Likelihood Score:**____
Vulnerability 1: ___ _____ **Severity Score:**___	Linked Yes/No	Linked ____	Linked ____	Linked ____	Linked ____
Vulnerability 2: ___ _____ **Severity Score:**___	Linked ____	Linked ____	Linked ____	Linked ____	Linked ____
Vulnerability 3: ___ _____ **Severity Score:**___	Linked ____	Linked ____	Linked ____	Linked ____	Linked ____
Vulnerability 4: ___ _____ **Severity Score:**___	Linked ____	Linked ____	Linked ____	Linked ____	Linked ____
Vulnerability 5: ___ _____ **Severity Score:**___	Linked ____	Linked ____	Linked ____	Linked ____	Linked ____

Risk Introduction

Power Sector Resilience Planning Guidebook

The following slides are intended to provide additional background information on how to assess and evaluate risks to the power system. They can serve simply as a reference or can be used in local power sector resilience assessment workshops. For questions or more information on the slides, use the "Ask An Expert" feature on the Resilient Energy Platform website.

What is Risk?

Risk is the potential for loss, damage, or destruction of key resources or power system assets resulting from exposure to a threat. Risk scores are the product of the threat likelihood score and the vulnerability severity score.

Risk Score = Threat Likelihood Score x Vulnerability Severity Score

Assessing the Risk Score

- Not all threats directly influence each vulnerability. The first step in assessing risk involves determining which threats and vulnerabilities are linked. Some vulnerabilities may be linked to multiple threats.
- The risk scores are then calculated for all linked threats and vulnerabilities.
- The scores are often shown in a risk-matrix heat map, as shown here, which highlights the highest-risk vulnerability-threat pairs with qualitative scores. However, this matrix can also show quantitative scores.

Vulnerability Severity Score					
High	Medium	Medium-to-high	Medium-to-high	High	High
Medium-to-high	Medium	Medium	Medium-to-high	Medium-to-high	High
Medium	Low-to-medium	Medium	Medium	Medium-to-high	Medium-to-high
Low-to-medium	Low-to-medium	Low-to-medium	Medium	Medium	Medium-to-high
Low	Low	Low-to-medium	Low-to-medium	Medium	Medium
	Low	Low-to-medium	Medium	Medium-to-high	High

Threat Likelihood Score

Evaluating Risks

- The risk-matrix heat map is helpful for showing the relative importance of different risks.
- Displaying in this format facilitates understanding of the interactions between threats and vulnerabilities, identifies potential solutions, and helps prioritize resilience planning efforts.

VULNERABILITIES	Vulnerability Severity Score	THREATS: More frequent flooding	Increased annual average temperature	Increased intensity to typhoon winds	Increased number of days with thunderstorms/lightning	Typhoons	Increased landslides
	Threat Likelihood Score	9	9	8	7	5	3
Infrastructure design susceptible to failure	9	81	81	72	63	45	27
Aging transmission infrastructure	8	72	72	64	56	40	24
Undersized power systems	7	63	63	56	49	35	21
Lack of redundant generation for at least 30% of load	5	45		40	35	25	15
Lack of operational flexibility	2	18	18	16	14	10	6

Hypothetical example of a national resilience planning process risk assessment, based on a risk matrix developed by Anderson et al, 2018.

RESILIENCE SOLUTIONS

Guide to Resilience Solutions

Introduction

Power sector resilience solutions often include some combination of resource or technological diversity, redundancy, decentralization, transparency, collaboration, flexibility, and foresight considerations[1]. A mix of solutions should be considered because no single intervention will address all potential vulnerabilities. Additionally, every power system is unique, and any solutions will have to be tailored to fit with specific power system characteristics.

Solutions may fall into different categories of power sector interventions:

- **Long-term planning** in the form of comprehensive community plans, threat mitigation plans, watershed plans, and others.
- **Regulations and policies,** such as zoning, subdivision codes, floodplain regulations, and building codes.
- **Programs** like capacity building, land acquisition, and low-income housing.
- **Capital projects,** such as capital improvement, decentralized backup energy generation for critical facilities, passive stormwater management system designs, etc.

Key Term

Power sector resilience—the ability of the power sector to anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruptions through adaptable and holistic planning and technical solutions.[1]

Renewable energy solutions, especially as distributed generation sources, can play a valuable role in power sector resilience through redundancy and energy diversification.

Planning for resilience solutions should always be part of an integrated and existing planning process, include stakeholder engagement (including nonutility entities), be linked to implementation and financing mechanisms, and should be periodically revisited. This process should involve a prioritization of resilience actions that can be based on such factors as priority threats, cost, difficulty, or number and priority of enhanced systems. Some examples of power system resilience solutions are shown in Table 6.

The first two activities in this section provide an approach to identify and prioritize technical solutions to support power sector resilience. The exercises are high level and can be tailored to, and elaborated on, to thoroughly assess possible solutions. For more detailed background and examples of resilience solutions, refer to the slides at the end of this section.

Power sector resilience solutions will fit within a broader planning process. Figure 4 provides one such example and can be tailored to meet the needs of individual countries and jurisdictions. The *Activity: Developing A Resilience Planning Process* provides a high-level activity that can inform a more thorough power sector resilience planning process.

Table 6: Examples of Resilience Solutions and their Impact on Power System Resilience

Example Resilience Solution	Impact on Power System Resilience
Spatial and Generation Diversification	Reduces the vulnerability of the energy supply system and the probability of an event to damage the larger system of critical locations, which increases system resilience.
Microgrids	A microgrid capable of islanding may ensure customers have access to power during long-term power outages that impact central grid systems occurring after major events. Microgrids can also be used in demand-response programs to reduce peak loads.
Redundancy	Including additional resources beyond those that are required for daily operations increases a power system's resilience because these resources can be relied on during other infrastructure failures or fuel shortages.
Policy	An enabling policy landscape helps to accelerate the adoption of power system resilience solutions. Restrictive policies can stifle resilience efforts.
Others: Supply chain assurance, critical load panels in emergency facilities, passive survivability, load shedding, energy storage.	

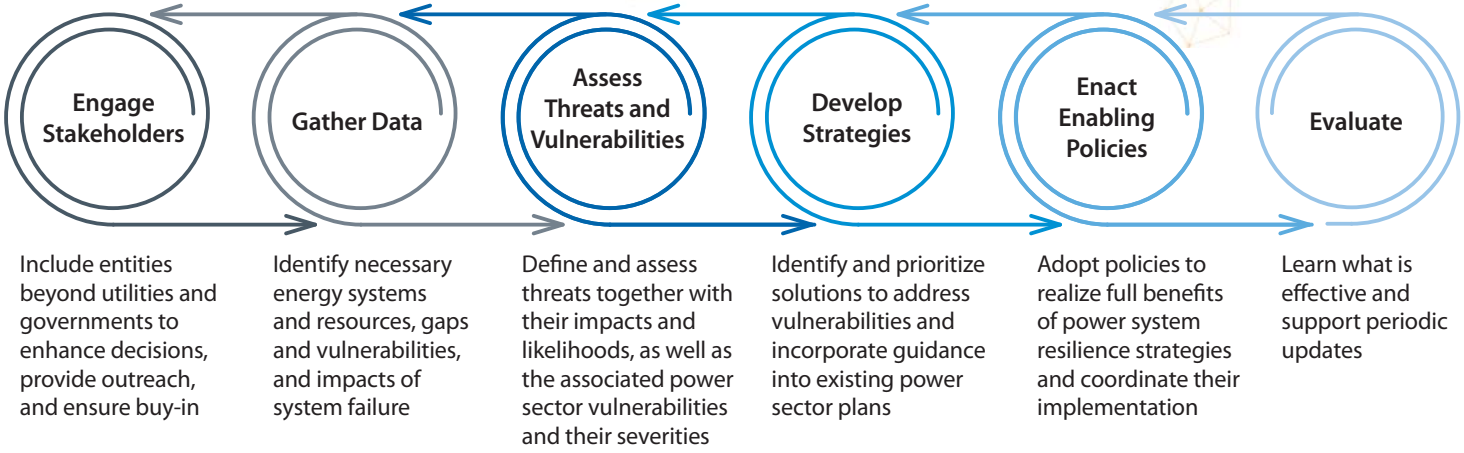


Figure 4. Planning for power sector resilience

Activity: Identify Resilience Solutions

Goal of this Activity

In this activity, you will identify potential solutions to enhance power sector resilience based on your knowledge of the threats, vulnerabilities, and risks developed in previous activities.

Introduction

The output of this activity is a preliminary set of solutions that support power sector resilience in the face of vulnerabilities that have the highest risks. Resilience solutions often include some combination of resource and technology diversity, redundancy, decentralization, transparency, collaboration, flexibility, and foresight considerations[1]. Many different solutions should be considered because no single intervention will address all potential vulnerabilities. Additionally, every power system is unique, and solutions must be tailored to specific circumstances and contexts.

These solutions will be prioritized in the next activity by their impact and effectiveness.

Solutions may fall into different categories of power sector interventions:

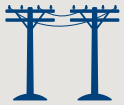
- **Long-term planning** in the form of comprehensive community plans, threat mitigation plans, watershed plans, and others.
- **Regulations and policies,** such as zoning, subdivision codes, floodplain regulations, and building codes.
- **Programs** like capacity building, land acquisition, and low-income housing.
- **Capital projects,** such as capital improvement, decentralized backup energy generation for critical facilities, passive stormwater management system designs, etc.

To guide the discussion, consider the following questions and complete the exercise on identifying resilience solutions. These can be completed in a group workshop or by individual organizations.

Discussion Questions

- Which solutions or interventions may address the top five risks to your power system?
- Which solutions might support a greater ability to maintain the operability of shared power system-wide infrastructure (or operations) during system stress or shock?
- Which solutions could provide a cobenefit across the power system and/or provide a downstream benefit for other infrastructure users or operations?
- Which solutions support a site-specific, critical operation, or load solution versus a broader system or regional resilience?
- Are there any site-specific, critical operation, or load solutions that could be scaled throughout the system for broader power system resilience?
- Have you considered solutions that support not only operability of the power system but also economic resilience, readiness for climatic changes, operational flexibility, and other resilience considerations?
- Have all the strategy categories listed above been considered?

Exercise: Which solutions for power sector resilience can help address your top five vulnerabilities? Which power sector systems do these solutions support?

	Generation 	Transmission 	Distribution 	Customer 	Operations 	Workforce 	Financial 	Other
Risk Pair 1: **V:** **T:**								
Risk Pair 2: **V:** **T:**								
Risk Pair 3: **V:** **T:**								
Risk Pair 4: **V:** **T:**								
Risk Pair 5: **V:** **T:**								

Activity: Resilience Solution Prioritization

Goal of this Activity

In this activity, you will prioritize power sector resilience solutions, identified in previous activities, by their impact and effectiveness. Prioritizing these solutions will lay the foundation for future collaboration on targeted planning, policy programs, and/or projects for all participants. This may enable participants to develop strategies for solutions under their authority.

Introduction

The last step in the workshop process is to prioritize the solutions developed. Resilience solutions often include some combination of diversity, redundancy, decentralization, transparency, collaboration, flexibility, and foresight considerations. However, there may be many different implementation solutions that must be considered, which focus on diverse concerns, and fall into different power sector systems. Prioritizing these solutions by their impact and effectiveness for power sector resilience helps participating jurisdictions and governmental entities build consensus; become informed about related activities, interdependencies, and vulnerabilities; and advance with implementation of the highest-priority resilience solutions.

Prioritization also lays the groundwork for future collaboration on targeted planning, policy, programs, or projects. This may allow participants to move forward with solutions that fall within their statutory and/or financing authority. Other solutions will rely on regional collaboration across jurisdictions or vertically among local, state, and federal agencies[1].

Prioritization begins with identifying relevant solutions and their relationships. These can then be prioritized by cost, complexity, and the relative impact and effectiveness in increasing power sector resilience. Impact refers to the extent that the strategy may have long-term, sustained changes in power sector resilience. Effectiveness relates to the level to which the solution will improve power sector resilience. There is no single way to evaluate impact and effectiveness, and all power sectors will have to determine an acceptable approach. Although some solutions may be complex in terms of implementation, they could have a positive impact and should not be ruled out based solely on complexity.

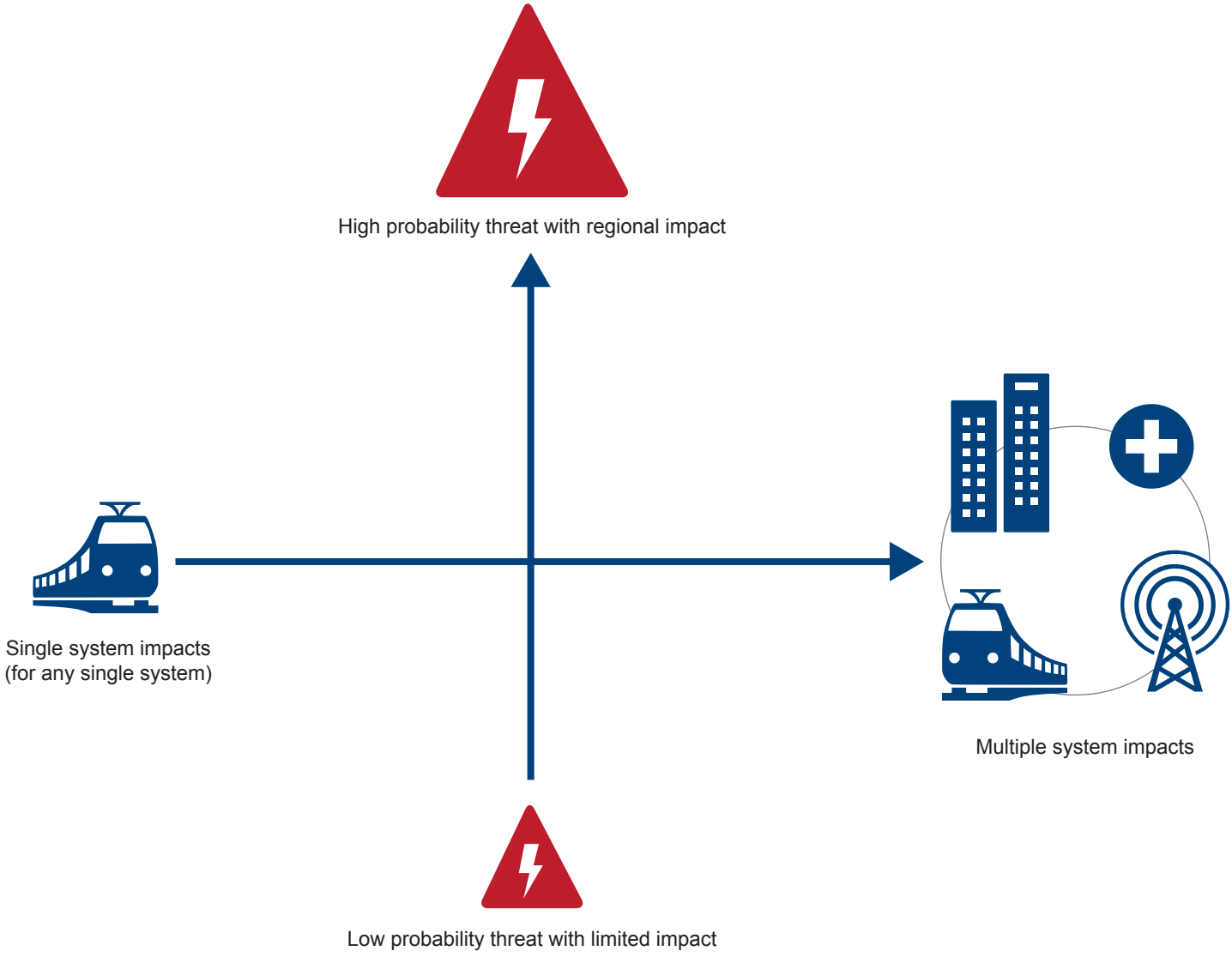
To guide the discussion, consider the following questions and complete the exercises on prioritizing solutions for power sector resilience. These can be completed as part of a group workshop or by individual organizations.

Discussion Questions

1. Which power sector solutions have been identified (at city, national, or regional/multinational scales)?
2. Do these solutions fall into Long-Term Planning, Regulations & Policies, Programs, or Capital Projects categories?
3. Are there any relationships between these solutions? If so, how are they related?
4. Which strategies support a specific site or critical infrastructure operation versus broader power sector resilience?
5. Where should the focus be placed on the implementation of these identified solutions?

Exercise 1: Where should focus be placed on the implementation of identified solutions?

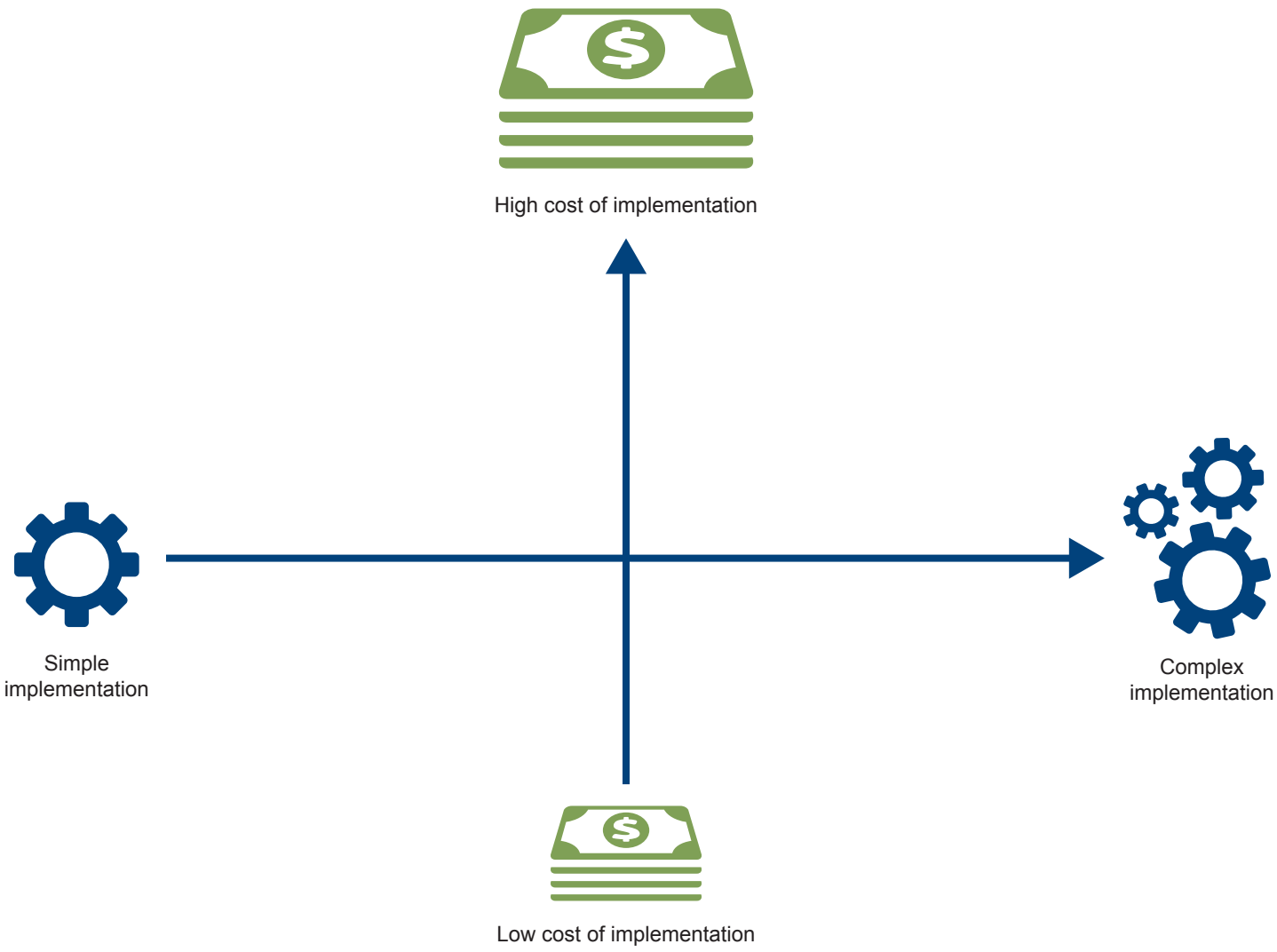
Use the chart below to map priority risks by likelihood and scale of hazard against the scope of the impact. Use this chart to select risks to prioritize for resilience action.



Note: This is a training exercise. For a comprehensive power system resilience assessment, a full cost-benefit analysis is necessary. These exercises are based on those created for NREL's resilience roadmap: https://www.nrel.gov/resilience-planning-roadmap/

Exercise 2: How challenging and costly will your resilience solutions be?

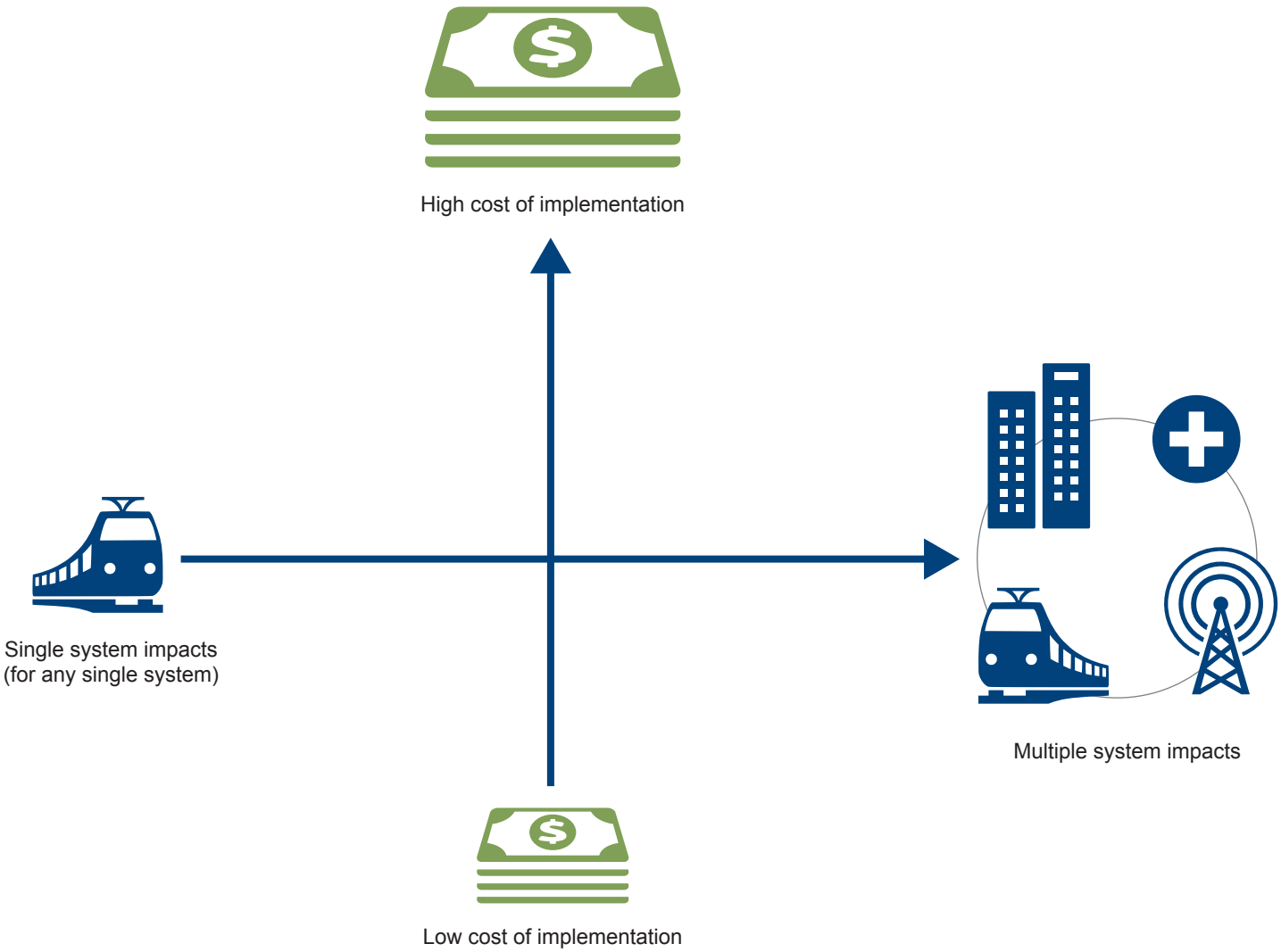
Use the chart below to map the relative cost of your possible resilience actions against the complexity of implementation. This will define the overall difficulty of implementation. This will help you choose solutions that comply with financial and capacity constraints.



Note: This is a training exercise. For a comprehensive power system resilience assessment, a full cost-benefit analysis is necessary. These exercises are based on those created for NREL's resilience roadmap: https://www.nrel.gov/resilience-planning-roadmap/

Exercise 3: How many systems will have added resilience based on your solutions?

Use the chart below to map the relative cost of your possible resilience actions against the number of system vulnerabilities addressed. This will define the overall impact of the solutions. Use this to prioritize solutions that reduce the greatest number of vulnerabilities relative to cost of implementation.



Note: This is a training exercise. For a comprehensive power system resilience assessment, a full cost-benefit analysis is necessary. These exercises are based on those created for NREL's resilience roadmap: https://www.nrel.gov/resilience-planning-roadmap/

Exercise 4:

Using the charts above, list your top five resilience solutions based on cost and vulnerabilities addressed.

Resilience Solution	Lead Organization	Supporting Organization	Policy or Regulatory Considerations	Cost Implications	Timeline	Vulnerabilities Addressed
1.						
2.						
3.						
4.						
5.						

Activity: Developing a Resilience Planning Process

Goal of this Activity

In this activity, you will develop a country-specific plan to assess power system vulnerabilities and develop a resilience strategy.

Introduction

The output of this activity will provide a framework for the resilience planning process in your country. It will identify key stakeholders, data, and a country-specific process for improving power sector resilience. The process below may be modified and customized to suit the needs of a specific country or jurisdiction following the main steps of the power sector resilience planning process shown in Figure 5.

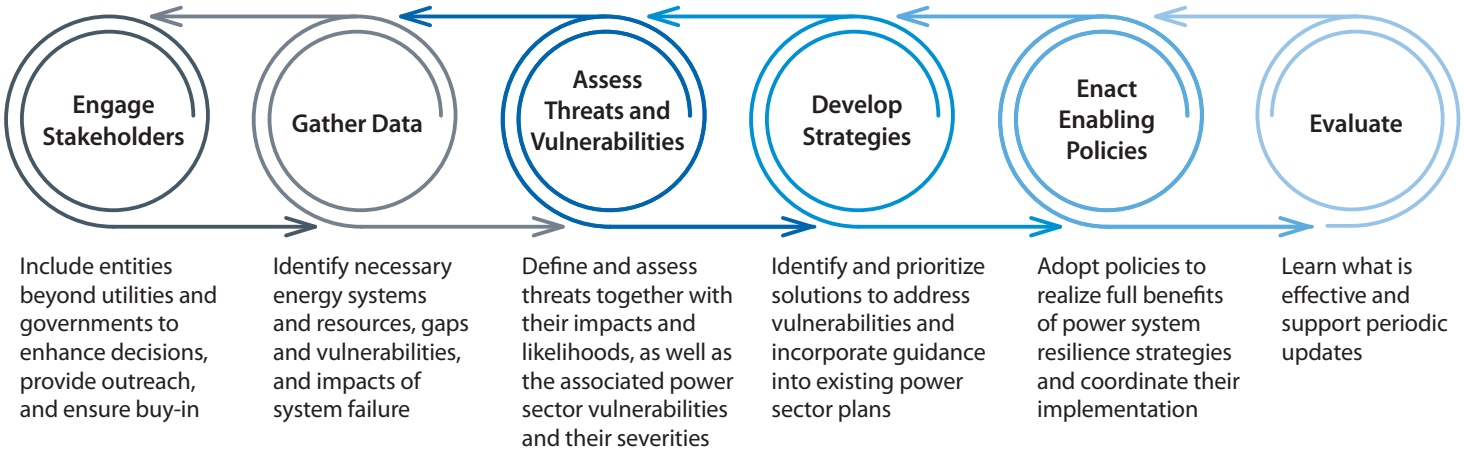


Figure 5. Planning for power sector resilience

Exercise 1: Resilience Planning

Work as a group to develop a resilience planning process of your own. Fill in the key details for each of the first five steps of the planning process.

Engage Stakeholders	**Who Leads the Resilience Planning Process?**	**Policy or Decision needed?**	**Primary Stakeholders**	**Secondary Stakeholders**

Gather Data	**Existing Climate, Threat, and Power System Data**	**Data Sources**	**Data Gaps and Needs**	**Planning Horizon**

Assess Threats and Vulnerabilities	**Who Leads?**	**Supporting Organizations?**	**Tools and Resources Needed?**	**Planning Horizon**

Develop Solutions	**Who Leads?**	**Part of Existing Planning Process?**	**Other?**	**Planning Horizon**

Enact Enabling Policies (and technical solutions)	**Key Agencies/Ministries**	**Budget Considerations**	**Political Will**	**Planning Horizon**

Power Sector Resilience Solutions

Power Sector Resilience Planning Guidebook

The following slides are intended to provide additional background information on the entire power sector resilience planning process, including examples of solutions and how to prioritize them. They can serve simply as a reference or can be used in local power sector resilience assessment workshops. For questions or more information on the slides, use the "Ask An Expert" feature on the Resilient Energy Platform website.

Key Messages

- Resilience is more than just reliability
- Resilience planning should be part of integrated planning
- There are multiple ways to prioritize resilience action:
  - Priority threats
  - Cost
  - Difficulty
  - Number/priority of enhanced systems
  - Cascading Impacts
  - Ancillary benefits
- Benefits to power system resilience:
  - Ability to reliably meet growing electricity demands
  - Decreased dependence on imported fuels, diversification of resources
  - Less economic loss/impact from threats
  - Improved infrastructure for fuel supply and electricity transmission
  - Increased safety and decreased mortality rates

What Do We Mean by Resilience?

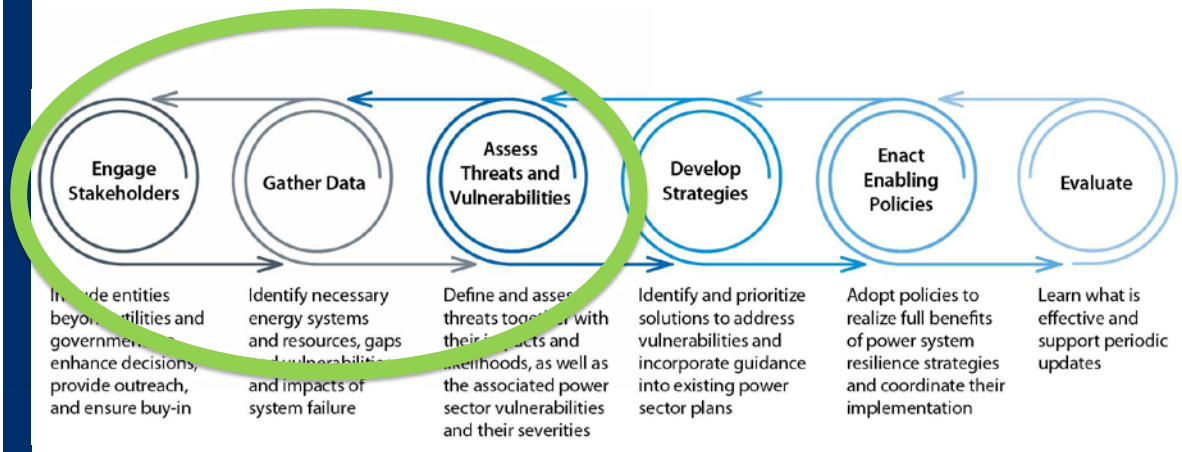
Power sector resilience refers to the ability of the power sector to anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruptions.[1]

- Utilities often speak about resilience in terms of **reliability**.
- In reality, **resilience encompasses more topics:**
  - Economic resilience
  - Readiness for climatic changes
  - Operational flexibility
  - Ability to shift resources should also be considered

Photo: US Army Corps of Engineers.

1. NREL's Resilience Roadmap: https://www.nrel.gov/resilience-planning-roadmap/

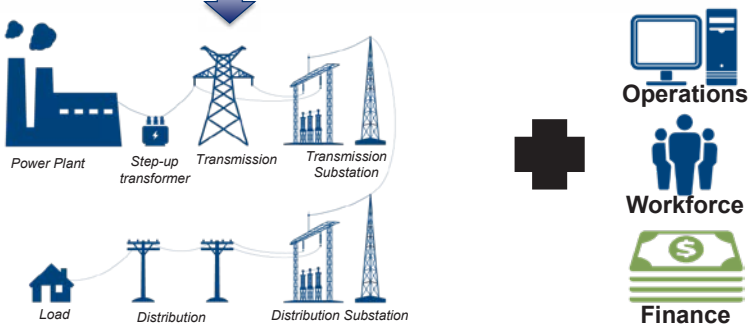
Resilience Planning Process Review



Power Sector Threats to Consider

Threats to power systems include:

- Climate threats
- Price volatility of generation fuel
- Variability of renewable energy resources
- Technology failures (such as dam collapses)
- Human actions including accidents and attacks



Community impacts related to power-supply vulnerabilities include:

- Critical facility outages
- Health impacts of power outages
- Social and financial impacts of power outages

Economic Impacts of Power Outages

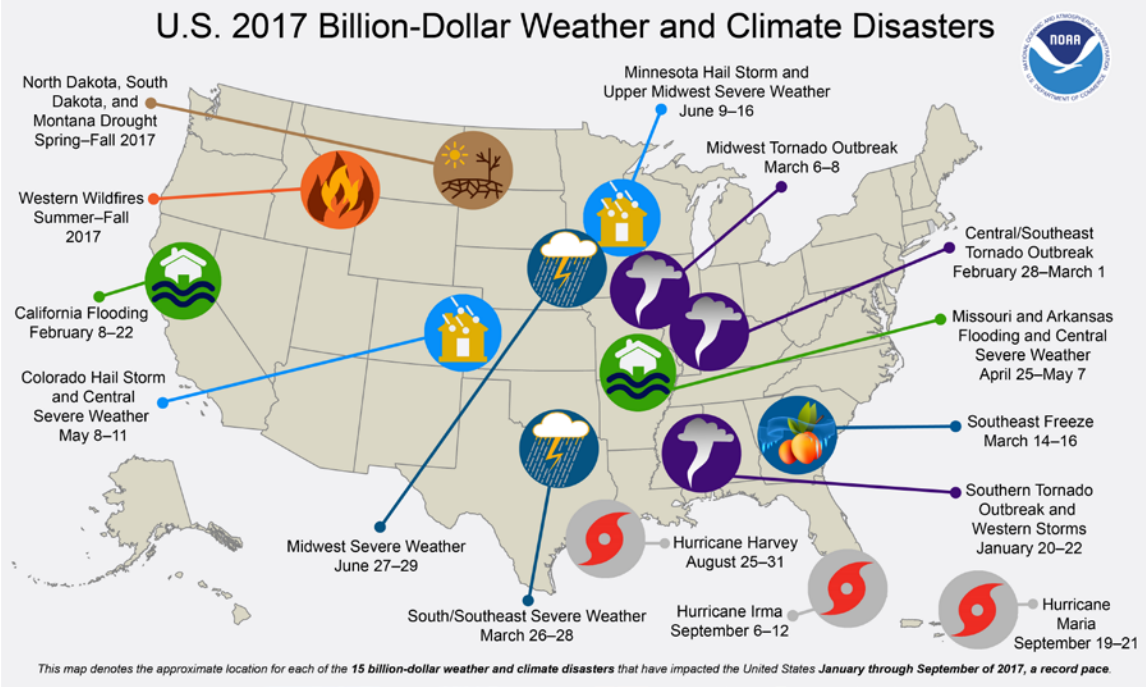
Cost estimates from storm-related outages to the U.S. economy are estimated at between $20 billion and $55 billion annually.

Industries most impacted by outages:

- **Digital economy** (telecommunications, data storage and retrieval services, the financial industry, etc.)
- **Continuous process manufacturing** (e.g. paper, chemicals, petroleum, rubber and plastic, etc.)
- **Essential services** (e.g. hospitals, utilities and transportation facilities such as railroads and mass transit, water and wastewater treatment, gas utilities and pipelines, etc.)

Source: ttp://woodpoles.org/portals/2/documents/CRS_Outages.pdf

Economic Impacts of Power Outages



Source: NOAA NCEI, https://www.climate.gov/news-features/blogs/beyond-data/2017-us-billion-dollar-weather-and-climate-disasters-historic-year

Economic Impacts of Power Outages

Example: Pakistan

- **Pakistan** ranks 115th out of 137 countries for grid reliability
- **50 million** Pakistanis lack access to reliable electricity

Cost estimates from storm-related outages to the Pakistani economy are estimated at $18 billion annually, 7% of their GDP.

Zhang, 2019, In the Dark: How Much Do Power Sector Distortions Cost South Asia
The World Bank

Resilience Planning Process

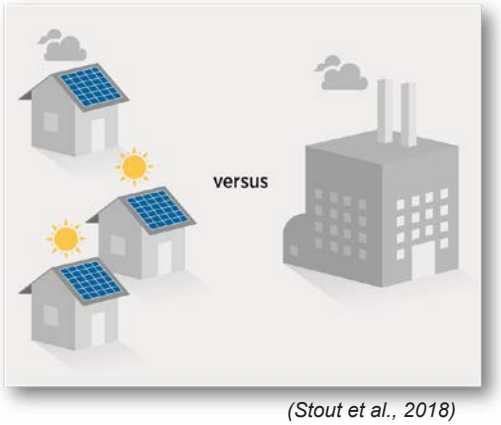
Example Resilience Solutions

- Supply chain assurance
- Spatial diversification
- Generation mix diversification
- Islandable energy systems for critical loads (microgrids)
- Critical load panels in emergency facilities
- Passive survivability
- Load shedding
- Energy storage
- Hardening infrastructure
- Underground distribution lines
- Fortifying transmission lines
- Raising substations

Figures: Dennis Schroeder, NREL

Resilience Solution: Spatial and Generation Diversification

- The modular (or sectional) nature of renewable energy technologies, such as wind turbines and solar photovoltaics (PV) allows:
  - Greater spatial diversification of energy supplies compared to conventional power generation systems
  - Increased diversification of energy mix compared to single fuel conventional power plants
- Increased diversification reduces the vulnerability of the energy supply system and the probability of an event to damage the larger system or critical locations, which increases overall energy system resilience



(Stout et al., 2018)

Resilience Solution: Microgrids

- Distributed generation (DG) based microgrids **capable of islanding** can disconnect from the central grid during an outage event to allow energy to be diverted to critical loads.
  - Allows utilities flexibility in restoring generation stations, responding to critical outages, and shutting down systems before an anticipated major event (like storms) to prevent damage.
- Islanded DG systems ensure consumers have access to power during long-term power outages that severely impact central grid systems, which can occur after major events.
- Additional Benefit: microgrids can participate in demand response programs to reduce electric loads during times of peak demand.

Resilience Solution: Microgrids

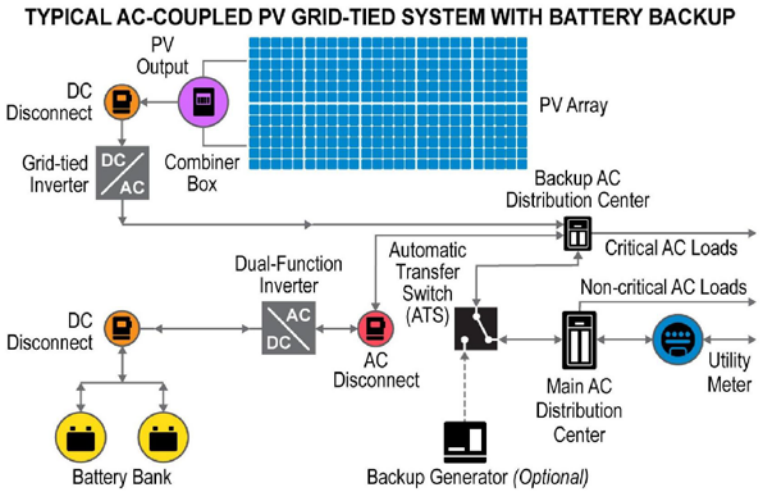


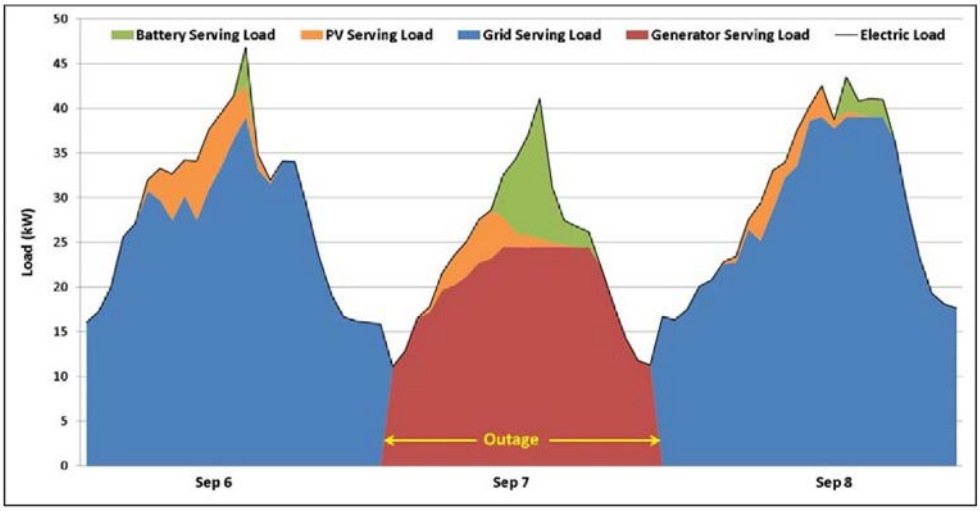
Figure.
https://nysolarmap.com/media/1655/dghubresiliencyretrofitfactsheet_8_8_16.pdf

Resilience Solution: Redundancy

Redundancy is the inclusion of additional resources beyond those that are required for daily operations that can be relied upon in case of failure in other components.

- The increased stress on infrastructure systems can increase the likelihood of failure of one or more parts of a system.
- Redundancy is essential for resilience. Renewable DG can add redundancy while stretching fuel supplies for conventional generators
- Communities served by only one power line or generating station have limited resilience. Increasing supplies, routes, or incorporating redundancy to overall systems will reduce the risks of those systems.

Resilience Solution: Redundancy



(Anderson et al. 2016)

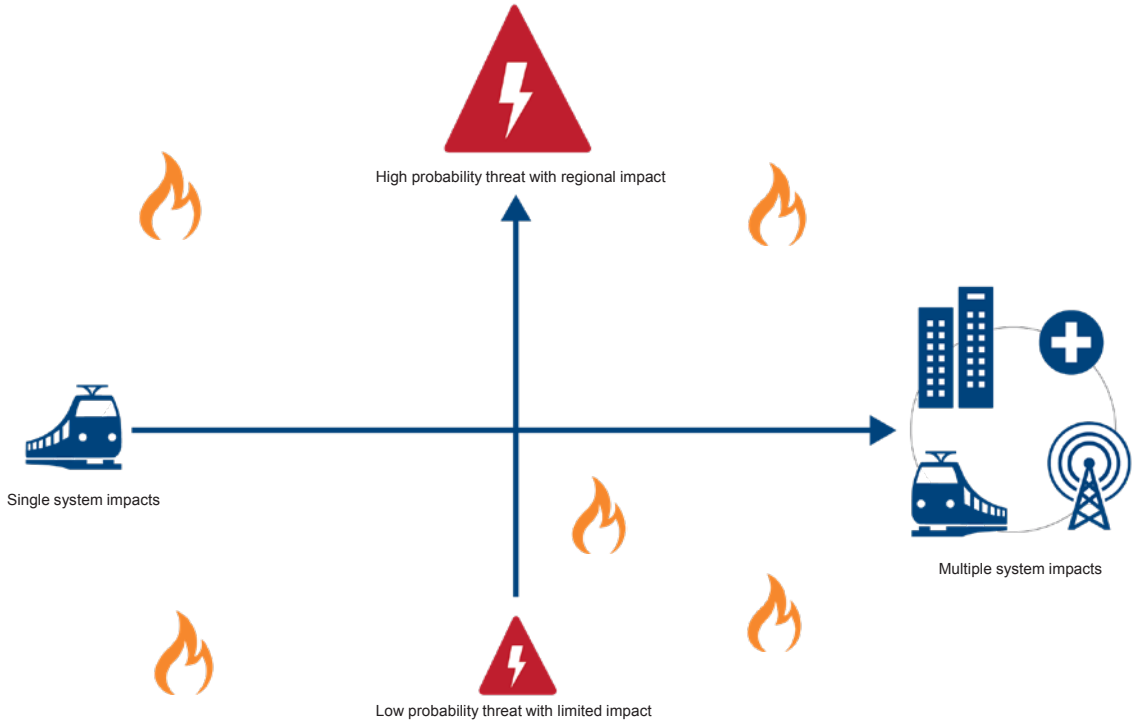
Resilience Solution: Policy

- In 2012 the U.S. state of New Jersey had the second most installed solar PV of any U.S. state.
- When Hurricane Sandy hit, only a few of those systems provided power during the 12 day ensuing power outage.
- Why?
  - Lack of resilience enabling policy, interconnection agreements, and island controls!

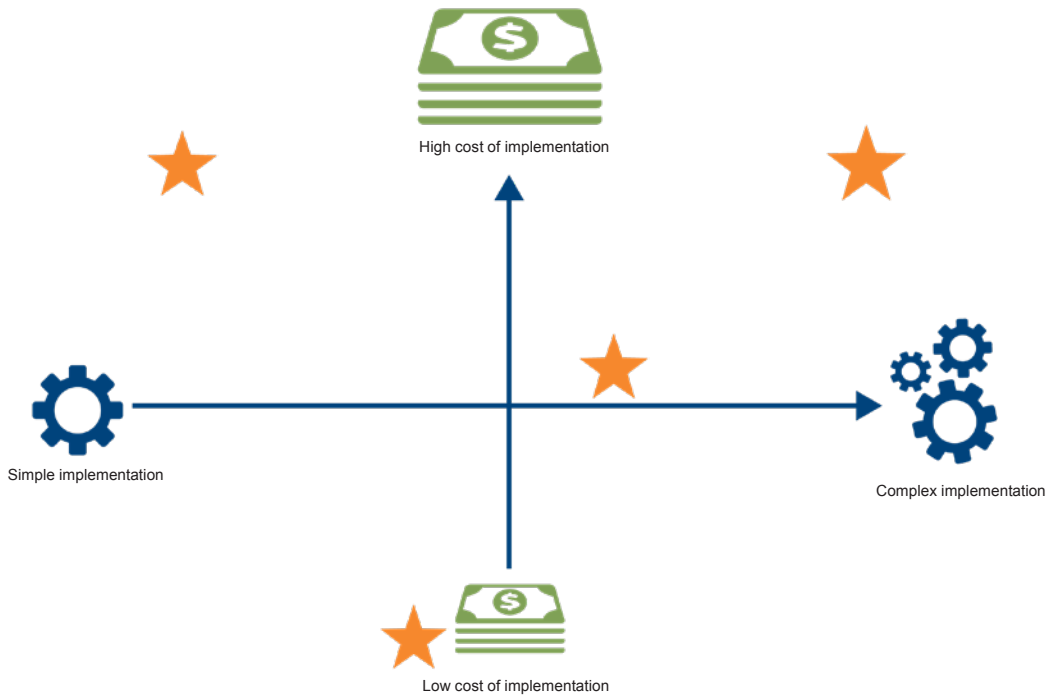
Figure. https://en.wikipedia.org/wiki/File:Map_of_the_USA_highlighting_New_Jersey.png

Resilience Planning Process

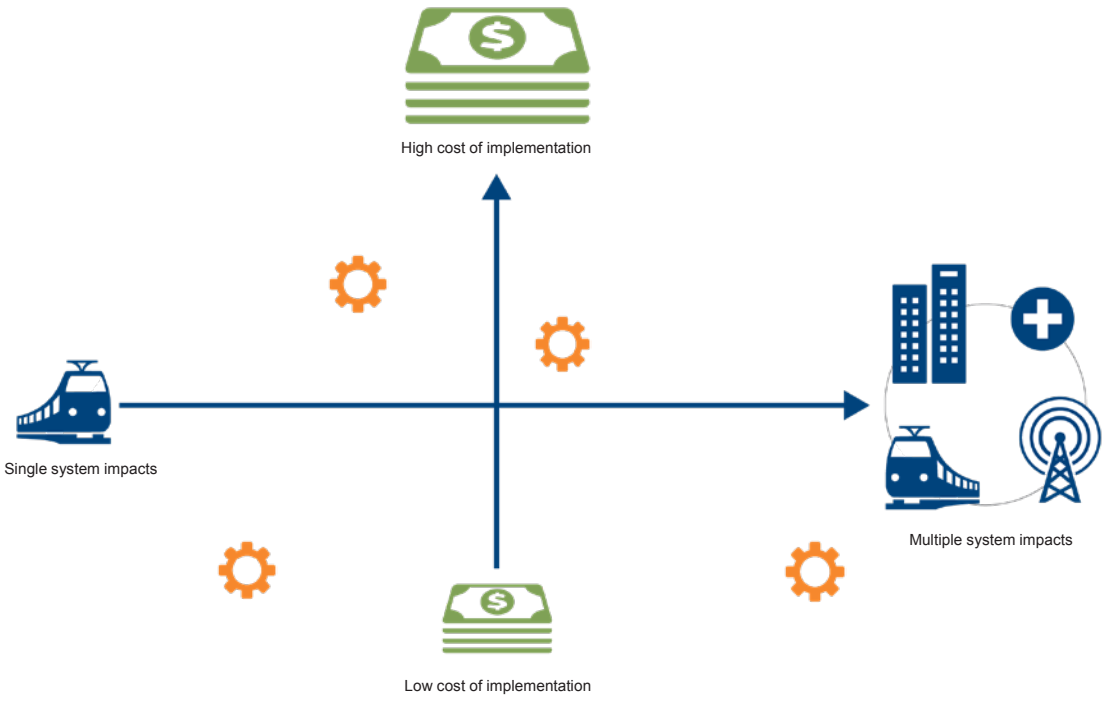
Resilience Planning: Options Evaluation by Priority Vulnerabilities



Resilience Planning: Options Evaluation by Cost and Complexity



Resilience Planning: Options Evaluation by Cost and Priority Systems



Effective Resilience Planning:

Power sector resilience planning should:

- Be incorporated into existing planning processes
- Include engagement with non-utility entities for incorporation into broader community resilience and adaptation planning
- Be part of a process that is revisited and updated periodically
- Be incorporated into an action plan for implementation and financing will need to be identified to support project implementation

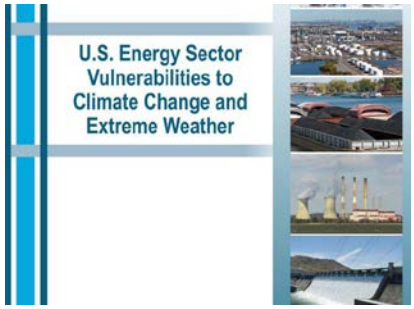
Early Actions for Resilience

Update resilience enabling policies

Are energy systems allowed to island? How much fuel must you store?

Set resilience goals

Ability to fully re-power within 3 days of major weather event, 10% DG + storage by 2025, all substations above projected flood height by 2020



Define current and projected threats

How many floods do you have now? How many floods will you have in 2050?

Define critical facilities and services

Figure. https://www.energy.gov/downloads/us-energy-sector-vulnerabilities-climate-change-and-extreme-weather

Key Takeaways

- **Redundancy and diversification are key** to increasing power sector resilience.
  - Renewable energy can play a valuable role in power sector resilience through redundancy and energy diversification.
- **Policy matters!** Don't forget to incorporate good policy design into technical adaptation strategies
- **Include resilience planning as part of larger integrated planning processes.**
- **Resilience planning is iterative**. Plans have to evolve as contexts and threats change

Useful Links

- Resilience Roadmap https://www.nrel.gov/resilience-planning-roadmap/
- Reopt Model https://reopt.nrel.gov/
- New York Solar Smart DG Hub Resilient Solar Project: https://www.nrel.gov/docs/fy16osti/66617.pdf
- Distributed Solar PV for Electricity System Resiliency: Policy and Regulatory Considerations https://www.nrel.gov/docs/fy15osti/62631.pdf
- Microgrid-Ready Solar PV - Planning for Resiliency https://www.nrel.gov/docs/fy18osti/70122.pdf
- Distributed Generation to Support Development Focused Climate Action https://www.nrel.gov/docs/fy16osti/66597.pdf
- NY Solar Smart Glossary https://nysolarmap.com/media/1457/dg_hub_glossary.pdf

References

1. Anderson, Kate, Josh Aldred, Michael Elchinger, Christine Gamble, Nick Grue, Nicholas Gilroy, Eliza Hotchkiss, Michael Ingram, Lissa Myers, Michael Rits, Sherry Stout, and Julie Tran. "Using GIS Visualization and Temporal Dynamism to Enhance Resilience Assessments." Forthcoming.
2. Eliza Hotchkiss, Alex Dane, and Connie Komomua. NREL. "Resilience Roadmap: A Collaborative Approach to Multi-Jurisdictional Planning." https://www.nrel.gov/resilience-planning-roadmap/.
3. Stout, S., E. Hotchkiss, N. Lee, A. Holm, and M. Day. 2018. *Distributed Energy Planning for Climate Resilience*. American Planning Association – National Planning Conference 2018. New Orleans, Louisiana, USA. April 21-24, 2018.

Image citations

4. CENAPRED, 2001. Diagnóstico de Peligros e Identię cación de Riesgos de Desastres en México, atlas nacional de riesgos de la república mexicana, Secretaría de Gobernación, Centro Nacional de Prevención de Desastres, Sistema Nacional de Protección Civil, México, pp. 106-141.
5. Ebinger, Jane O. and Walter Vegara. 2010. *Climate Impacts on Energy Systems: Key Issues for Energy Sector Adoption*. Washington, D.C.: World Bank Publications.
6. Hamududu, B. and Å. Killingtveit. 2010. *Estimating effects of climate change on global hydropower production*. Norwegian University of Science and Technology. Hydropower 2010—6th International Conference on Hydropower. Tromsø, Norway. February 1–3, 2010.
7. Vergara, W. and S. M. Scholj (Eds.). 2011. *Risk assessment of Amazon Dieback*. Washington, D.C.: World Bank Publications.

Vulnerability Assessment and Resilience Resources

Distributed Generation to Support Development-Focused Climate Action

U.S. Department of Energy's National Renewable Energy Laboratory (NREL) and USAID, 2016

Description: This paper explores the role of distributed generation, with a high renewable energy contribution, in supporting low-emission, climate-resilient development. The paper presents potential impacts on development (via energy access), greenhouse gas emission mitigation, and climate resilience directly associated with distributed generation, as well as specific actions that may enhance or increase the likelihood of climate and development benefits. This paper also seeks to provide practical and timely insights to support distributed generation policymaking and planning within the context of common climate and development goals as the global distributed generation landscape rapidly evolves. Country-specific distributed generation policy and program examples, as well as analytical tools that can inform efforts internationally, are also highlighted throughout the paper.

https://www.nrel.gov/docs/fy16osti/66597.pdf

Bridging Climate Change Resilience and Mitigation in the Electricity Sector Through Renewable Energy and Energy Efficiency

NREL and USAID, 2016

Description: Reliable, safe, and secure electricity is essential for economic and social development and a necessary input for many sectors of the economy. However, electricity generation and associated processes make up a significant portion of global greenhouse gas (GHG) emissions contributing to climate change. Furthermore, electricity systems are vulnerable to climate change impacts—both short-term events and changes over the longer term. Energy efficiency and renewable energy technical solutions described in this paper can bridge action across climate change mitigation and resilience through reducing GHG emissions and supporting electric power sector adaptation to increasing climate risk. Integrated planning approaches, also highlighted in this paper, play an integral role in bringing together mitigation and resilience action under broader frameworks.

https://www.nrel.gov/docs/fy18osti/67040.pdf

Vulnerability Assessment Methodologies: A Review of the Literature

USAID, 2014

Description: This resource is not energy-infrastructure specific but has methodologies and best practices that can be applied to power system vulnerability assessments. This literature review provides an overview of the tools and methods used to measure vulnerability, because it pertains to development interventions focused on economic strengthening, at the population level as well as the household and individual level.

https://www.fhi360.org/sites/default/files/media/documents/Vulnerability%20Assessment%20Literature%20Review.pdf

Climate Change and the Electricity Sector: Guide for Climate Change Resilience Planning

U.S. Department of Energy, 2016

Description: This guide provides a broad framework for assessing the vulnerability of electric utility assets and operations to climate change and extreme weather, and developing appropriate resilience solutions. Vulnerability assessments help utilities determine where and under what conditions their systems may be vulnerable to rising temperatures and sea levels, changing precipitation patterns,

or more frequent and severe episodes of extreme weather. Resilience plans, which are informed by the findings of the vulnerability assessments, identify solutions and prioritize climate resilience actions and investments. By completing the key steps in this guide (Figure ES.1), utilities will develop planning-level documents that identify specific actions for managing or mitigating climate change risks.

https://www.energy.gov/sites/prod/files/2016/10/f33/Climate%20Change%20and%20the%20Electricity%20Sector%20Guide%20for%20Climate%20Change%20Resilience%20Planning%20September%202016_0.pdf

Climate Change Vulnerability Mapping for Southeast Asia

Economy and Environment Program for Southeast Asia (EEPSEA), 2009

Description: This paper provides information about the subnational areas (regions, districts, provinces) most vulnerable to climate change impacts in Southeast Asia. This assessment was carried out by overlaying climate hazard maps, sensitivity maps, and adaptive capacity maps following the vulnerability assessment framework of the United Nations' Intergovernmental Panel on Climate Change (IPCC). The study used data on the spatial distribution of various climate-related hazards in 530 subnational areas of Indonesia, Thailand, Vietnam, Lao PDR, Cambodia, Malaysia, and the Philippines.

https://www.idrc.ca/sites/default/files/sp/Documents%20EN/climate-change-vulnerability-mapping-sa.pdf

Guidelines for Climate Proofing Investment in the Energy Sector

Asian Development Bank (ADB), 2013

Description: This publication is the third in a series of technical notes covering various sectors, as a companion to an earlier report, *Climate Risk and Adaptation in the Electric Power Sector*, which highlights the climate change risks faced by the sector and the nature of the possible adaptation options. This technical note aims to provide guidance to project teams as they integrate climate change adaptation and risk management into each step of project processing, design, and implementation. The technical note encompasses lessons learned and good practices identified through several completed and ongoing ADB energy projects. The aim is that it improves—and simplifies—the work of development professionals in their efforts to enhance the climate resilience of energy sector projects.

https://www.adb.org/sites/default/files/institutional-document/33896/files/guidelines-climate-proofing-investment-energy-sector.pdf

Climate Vulnerability Assessment: An Annex to the USAID Climate-Resilient Development Framework

USAID, 2016

Description: This annex is an introduction to climate vulnerability assessments (VAs), one of the first inputs when designing evidence-based climate adaptation measures, including projects tailored for a country or region. It includes key definitions, a conceptual framework to increase the consistency of such assessments, sample questions for VAs at the country, sector, and local levels, and an overview of methods and outputs. It is aimed at those who are designing and managing VAs. The VA process described is part of USAID's five-step Climate-Resilient Development Framework, which helps decision makers and development practitioners understand and address climate variability and change within development programs.

https://www.climatelinks.org/resources/climate-vulnerability-assessment-annex-usaid-climate-resilient-development-framework

Glossary of Terms

Adaptive Capacity
The ability of a system to successfully adjust to various external factors.

Adversarial actor
An individual, organization, or nation that acts maliciously with the intent to damage, disrupt, or destroy the power system or components of the system. Also referred to as *bad actor* or *malicious actor*.

Critical infrastructure
Assets, systems and networks that are essential for the functioning of society and the economy. Damage to this infrastructure, or disruption of the services they provide, may harm the security, economic activity, and/or public health and safety. Infrastructure may be physical or virtual, and publicly or privately owned, such as power systems, roadways, waterways, or other systems (e.g., buildings and water treatment facilities).

Critical loads
Loads for which power supply must always be maintained and cannot be interrupted to ensure the functioning of society and the economy, such as hospitals, critical communications, emergency services, water and wastewater treatment, and military installations.

Distribution network
The final system (structures, wires, insulators, and associated hardware) in the delivery of electric power to customers (load). Distribution systems consist of subtransmission-level voltage lines, typically below 69 kilovolts (kV).

Energy profile
Information on the energy consumption patterns and generation assets of the power system in addition to utility service provider agreements and long-term regional forecasts for meeting demands given socioeconomic projections.

Exposure
The infrastructure, operations, workforce, and/or finance systems that are present where hazards may occur. Exposure is not a sufficient determinant of risk because systems may be exposed but not vulnerable.

Fault
Any abnormal flow of electric current in a power system that disrupts the steady state of the system. This may occur from, for example, a failure of system insulation materials or contact of the system with a conducting object, resulting in a short circuit. There are many possible causes, including, lightning, heavy winds, vehicles colliding with structures, squirrels shorting lines, lines breaking due to excessive loading, and others.

Flexibility (operational)
The ability of a power system to respond to changes in electricity demand and supply. High flexibility implies that a system can respond quickly to changes in net load.

Hazard
Anything that can damage, destroy, or disrupt the power sector. This term is often used interchangeably with *threat*.

Human-caused threat
A threat that results from an accident (e.g., accidentally cutting underground lines) or an action from a bad actor (e.g., cyber, acts of terror). Refer to the definition of *threat*.

Impact
The extent to which a hazard affects power sector infrastructure and processes (e.g., a typhoon causes wind damage to transmission lines). This term is often used interchangeably with *consequence* or *outcome*.

Infrastructure
This term refers to the physical and virtual structures, facilities, and systems of a power system. It includes generation, transmission and distribution, and transportation systems in addition to the assets that support these systems.

Load
This term refers to end-use devices or customers that receive power from the electric system. It also refers to the aggregate electric power consumed by all users connected to the power system.

Natural threats
Threats that result from acts of nature (e.g., severe weather, floods, earthquakes, hurricanes, solar flares, and others) as well as wildlife interactions with the power system (e.g., squirrels, snakes, or birds causing short circuits on distribution lines). Refer to the definition of *threat*.

Planning horizon
The length of time into the future (start and end year) that is considered for a particular planning activity. For example, a planning horizon of 15 years, starting in the year 2015, would go until the year 2030.

Redundancy
The inclusion of additional resources beyond those that are required for daily operation and which can be relied upon to continue system operations in case of failure of other components.

Reliability
A measure of whether a power system can provide regular, consistent power, typically defined by System Average Interruption Duration Index (SAIDI), Customer Average Interruption Duration Index (CAIDI), and System Average Interruption Frequency Index (SAIFI).

Resilience
The ability of the power sector to anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruptions through adaptable and holistic planning and technical solutions.

Risk
The potential for loss, damage, or destruction of key resources or power system assets resulting from exposure to a *threat*. Risk is evaluated as the product of the *threat* likelihood and *vulnerability* severity scores.

Spatial diversification
The practice of separating power system infrastructure over different geographical areas to avoid *exposure* to *threats*. The modular nature of renewable energy technologies, such as wind turbines and photovoltaics, permits spatial diversification.

Stress
A pressure or tension that is exerted on the power system that could have adverse effects on continued operations (e.g., changes in population or economic conditions in a region).

Technological threats
Unpredicted equipment and infrastructure failures (e.g., a bridge collapse or grid outage). Refer to the definition of *threat*.

Threat
Anything that can damage, destroy, or disrupt the power sector. Threats can be natural, human caused, or technological. Threats are not typically within the control of power system planners and operators. They may consist of wildfires, hurricanes, storm surges, cyberattacks, and others. This term is often used interchangeably with *hazard*.

Transmission network
A system of structures, wires, insulators, and associated hardware that carry electric energy from one point to another in an electric power system. The system is operated at high voltages (above 69 kV) and can transmit large quantities of electricity over long distances.

Uncertainty
A situation in which the current state of knowledge involves imperfect or unknown information; the consequences, extent, or magnitude of conditions or events is unpredictable; or the credible probabilities of possible outcomes are not available.

Vulnerability
Weaknesses within infrastructure, processes, or systems, or the degree of susceptibility to various threats. Different measures can be taken to reduce vulnerability or improve adaptive capacity to threats to the power sector. Vulnerabilities are typically identified through stakeholder interviews, technical analyses, and/or literature reviews.

Vulnerability assessment
A process that begins with data gathering, consideration of risks and exposure, and the identification of *threats*, *impacts*, and *vulnerabilities* in a power system followed by the prioritization of vulnerabilities according to *risk*.

Photo credits: front page photo by Dennis Schroeder, NREL 46142; page 4: iStock 458541345; page 20: iStock 881926684; page 27: iStock 1065674238; page 42: iStock 531920932; page 50: iStock 870562604

www.resilient-energy.org | www.nrel.gov/usaid-partnership

Jennifer E. Leisch, Ph.D.
USAID-NREL Partnership Manager
U.S. Agency for International Development
Tel: +1-303-913-0103 | Email: jleisch@usaid.gov

Sadie Cox
Senior Researcher
National Renewable Energy Laboratory
Tel: +1-303-384-7391 | Email: sadie.cox@nrel.gov

This work was authored, in part, by the National Renewable Energy Laboratory (NREL), operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by the United States Agency for International Development (USAID) under Contract No. IAG-17-2050. The views expressed in this report do not necessarily represent the views of the DOE or the U.S. Government, or any agency thereof, including USAID.

NREL/TP-7A40-73489 | June 2019
NREL prints on paper that contains recycled content.

The Resilient Energy Platform provides expertly curated resources, training, tools, and technical assistance to enhance power sector resilience. The Resilient Energy Platform is supported by the U.S. Agency for International Development.

The USAID-NREL Partnership addresses critical challenges to scaling up advanced energy systems through global tools and technical assistance, including the Renewable Energy Data Explorer, Greening the Grid, the International Jobs and Economic Development Impacts tool, and the Resilient Energy Platform. More information can be found at: **www.nrel.gov/usaid-partnership**.

USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

REexplorer MAPPING OUR ENERGY FUTURE

Greening the Grid

I-JEDI

Resilient Energy Platform