# 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. |