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.