Cite as: Daniel A. Eisenberg and David L. Alderson, 2024, "Operational Energy Vulnerability and Resilience," in Alan Howard, Daniel Nussbaum, Brenda Shaffer, *Operational Energy*, DeGruyter, Berlin.

6 Operational Energy Vulnerability and Resilience

Daniel A. Eisenberg and David L. Alderson

OE systems are vulnerable and can be seriously disrupted by accidents, failures, extreme weather, or deliberate attack. Determining where such vulnerabilities lie is an important task for the military. So is developing strategies that use new technologies to make OE systems more resilient and able to adapt and complete missions if such systems are compromised.

This chapter focuses on the concepts of *vulnerability* and *resilience* as they pertain to OE systems. It describes how to think about vulnerability and resilience for OE systems, provides key analysis techniques to identify vulnerabilities, and presents a framework to compare different resilience strategies. In the contingent case study, these methods are applied to the case of the US Virgin Islands and their local energy systems in response to the 2017 hurricane season.

Vulnerability is a broad concept that encompasses several commonly used analysis techniques, namely reliability, risk, and adversarial analysis. This chapter covers the distinctions between these techniques, including their treatment of uncertainty when modeling and identifying OE system vulnerabilities. What is rarely discussed is that these techniques tend to identify different vulnerabilities in the same system, which can create difficulties in determining an appropriate management approach.

Toward this end, this chapter provides four distinct ways in which resilience is viewed to describe the way that a system responds to stress, resilience outcomes to aim for, and examples of strategies to achieve them. All resilience outcomes are beneficial for OE systems; however, it may be difficult to achieve them. In addition, strategies to achieve each outcome can be in conflict.

6.1 Background on Vulnerability and Resilience in OE Systems

OE systems like power grids, fuel pipelines, and supply chains are generally large, complicated, diverse, and difficult to fully comprehend, even for experts. This chapter begins with a brief overview of systems concepts to help orient thinking about OE systems and their vulnerability and resilience.

The first step to taking a systems perspective is to define an OE system, i. e., define all the infrastructure, organizations, environmental factors, etc. that are "in" the system and everything "outside" the system. When it comes to OE (and other critical infrastructure), there are two common ways analysts and designers approach this task:

https://doi.org/10.1515/9783110798104-008

1. A list of assets (not recommended)
   The basic idea is to list all the relevant OE assets in inventory at the installation or command, then use some rack-and-stack scheme to prioritize the most important ones. Examples of OE assets include things like fuel storage tanks, fuel delivery trucks, electric generators, solar panels, or microgrids.
2. An interconnected *network* that works to achieve a particular function (recommended)
   The emphasis here is not so much on the assets but the functions that they provide. One of the most powerful ways to relate assets to functions is to consider how they are managed as a *network.* Examples of OE systems often represented as networks include power grids or fuel storage and distribution pipelines.

Although obtaining an inventory of the things to be managed or protected is perhaps a necessary first step, it turns out that simple lists tend to be poor tools for identifying what matters most and what to do about it. Lists tend to focus on assets in isolation, without consideration for the interactions or dependencies between them which are often critical to mission success.

Instead, it is important to recognize that *assets* are commonly organized into *systems* that work to provide a *function* which enables a *capability* and ultimately supports a *mission.*

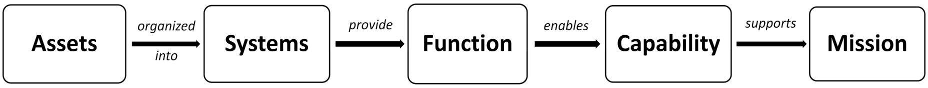


Figure 6.1: A conceptual view for the relationship between assets, function, and mission success.

Even the smallest building block of an OE system (such as circuits and logic gates in electronic hardware) can be and often are represented by a simple network to show their input-output relationships and functions. Like these building blocks of OE systems, larger infrastructure (e. g., transformers, generators, pumps, pipes, etc.) are not isolated from each other. They are always interconnected into networks that work together to provide a function (e. g., electricity, fuel distribution). Importantly, the vulnerability and resilience of an OE system depends on how it functions as a network; using a network perspective enables military planners to test and measure how the loss of an asset or sub-system impacts the overall functioning of a system.

Consider the following analogy: a traditional *kill-chain analysis* identifies the structure of an attack and reveals the ways in which an interruption at any stage in the "chain" can interrupt the entire process. In a similar manner, the breakdown of a key element in an energy system can lead to a failure in the OE mission. Viewing OE systems only as a list of assets ignores these "kill chain" relationships.

In this view of systems, vulnerability and resilience are interdependent concepts. The purpose of vulnerability analysis techniques is to reveal what events and conditions (e.g., where in the OE kill chain) may prevent systems from being able to carry out critical functions. Resilience strategies, in turn, aim to develop mechanisms to adapt to failures when they occur or help to avoid them altogether. Thus, the goal of vulnerability analysis is to identify issues in OE systems that need to be managed with resilience strategies.

Unfortunately, it is not easy to identify the way in which the loss of one or more components in a system will lead to its failure. Similarly, it is difficult to recognize effective mitigations that achieve resilience outcomes to survive and adapt to change. This is in part because the connections between components can quickly become very complicated. Even when all dependencies are known, it can be challenging to find a single point of failure. A second reason is that in many cases, the behavior of these systems is governed by decision-makers (either human or automated) that adjust in the presence of a disruption. Thus, identifying failure modes requires consideration not only of how the system is currently operating, but how it could adjust its operation in response to disruption. A third reason identifying failure modes is hard is that typically not all system dependencies are identified, rather the system often contains a multitude of hidden dependencies that only reveal themselves at the most inopportune times – when the system fails.

An all-too-common experience when an OE system fails to provide a critical function is the discovery of vulnerabilities that could have been managed ahead of time. A transformer fails, a pump shuts down, a powerline disconnects, a backup generator does not turn on. In retrospect, these assets may not have been viewed as critical to the mission, even though the entire system function depended on them. These types of vulnerabilities are called “hidden in plain sight,” that is, things that are obvious in retrospect but hard to see before the failure event. Thus, people often identify with perfect hindsight the resilience actions that could have been taken given knowledge of these vulnerabilities.

The overall goal of this chapter is to help officers learn how they can uncover potential problems and fix them before they risk the success of missions. Vulnerability and resilience analysis techniques provide a basis to identify issues “hidden in plain sight” and potential alternatives to manage them.

6.2 Vulnerability Analysis for OE Systems

OE systems are *vulnerable* if they are susceptible to events or conditions that can lead to loss of a critical function. All systems are vulnerable to something – the question is: what? As discussed in Chapter 4, OE systems must be concerned with both deliberate sources of harm (e. g., vandalism, sabotage, attack) and non-deliberate sources of harm (e. g., accidents, failures, natural disasters). But the list of potential threats to OE systems is long.

Several authors in the academic literature have tried to tackle this question to enable vulnerability analysis of infrastructure and OE systems. Vulnerability is defined across these works as:

- the manifestation of inherent states of a system that can be exploited;[297]
- the susceptibility and/or inability to cope and deal with a particular threat;[298]
- the conditional probability that damages occur given a specific threat or attack;[299]
- the uncertainty about and severity of the consequences of an activity given an initiating event;[300]
- the degree that a system can be affected by a particular risk;[301]
- the degree a system can withstand specified loads.[302]

Linking perspectives together, this examination of system vulnerability may consider one or both of the following: (1) analysis of the likelihood a system will experience an undesired event or condition (via system exploitation, susceptibility, probability of damage, etc.), and (2) analysis of the magnitude of damages experienced (via severity of consequences, the degree of consequences, degree to withstand loads, etc.). Given this view, vulnerability analysis is broad enough to encompass any technique that combines these analyses together.

For OE systems, vulnerability analysis relies on several methods to determine the susceptibility of systems to loss of function, namely reliability, risk, and adversarial analysis. Vulnerability analysis is the process of integrating knowledge from those methods into a comprehensive view of how systems may fail. Hence, vulnerability analysis informs management decisions that can improve the resilience of OE systems, where reliability, risk, and adversarial methods on their own are too narrow to produce such recommendations. The goal of vulnerability analysis is to compare and prioritize differ-

[297] Yacov Y. Haimes, "On the Definition of Vulnerabilities in Measuring Risks to Infrastructures," *Risk Analysis: An International Journal*, vol. 26, no. 2, 2006, pages 293–296.

[298] Barry Charles Ezell, "Infrastructure Vulnerability Assessment Model (I-VAM)," *Risk Analysis: An International Journal*, vol. 27, no. 3, 2007, pages 571–583.

[299] Henry H. Willis, "Guiding Resource Allocations Based on Terrorism Risk," *Risk Analysis: An International Journal*, vol. 27, no. 3, 2007, pages 597–606.

[300] Terje Aven, "On Some Recent Definitions and Analysis Frameworks for Risk, Vulnerability, and Resilience," *Risk Analysis: An International Journal*, vol. 31, no. 4, 2011, pages 515–522.

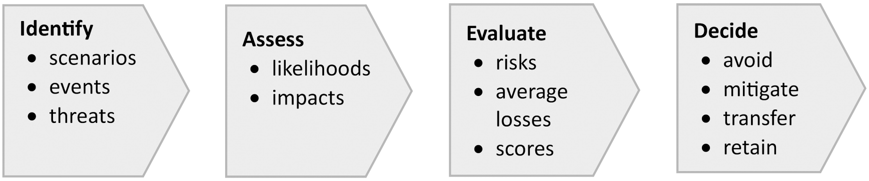
[301] Society for Risk Analysis, "Society for Risk Analysis Glossary" (https://sra.org/sites/default/files/pdf/SRA\%20Glossary\%20-\%20FINAL.pdf).

[302] Society for Risk Analysis, "Society for Risk Analysis Glossary" (https://sra.org/sites/default/files/pdf/SRA\%20Glossary\%20-\%20FINAL.pdf).

ent (and potentially conflicting) ways reliability, risk, and adversarial analysis indicate OE systems may fail.

Some may object to this framing as methods like risk analysis have significant development and application across OE systems. For example, one may argue that a comprehensive risk management program should be enough to support OE system resilience.

However, risk analysis is in fact a subset of vulnerability analysis because it creates a particular view of why OE systems fail to function. Specifically, reliability, risk, and adversarial analyses approach OE systems with different perspectives on what events or conditions can cause failure, which consequences matter, and how they should be measured. Accordingly, each analysis applied to the same OE system will produce different results. This chapter will discuss not only how methods like reliability, risk, and adversarial analyses differ in application, but also how they differ in outcomes – characteristically, they identify different system vulnerabilities.



Traditional Risk Analysis

Step 1: Identify and list the scenarios, events, and/or threats of concern.

Step 2: For each entity identified in Step 1, estimate the likelihood the event will happen, as well as the potential impacts (e. g., consequences, damage, lives lost) if it does occur.

Step 3: Evaluate the risk (as some combined measure that combines likelihood and impact). A simple form of this is to evaluate the expected (or average) case and/or to assign a risk score.

Step 4: Decide whether to avoid the risk (don’t proceed with the action), mitigate the risk (by altering the course of action), transfer the risk (for example, by buying insurance), or retain the risk (proceed as is).

6.3 Reliability, Risk, and Adversarial Analysis

6.3.1 The Basics

A key distinction between reliability, risk, and adversarial analysis is their treatment of uncertainty.[303] An important distinction between different sources of uncertainty is whether they are *non-deliberate* or *deliberate.*

Non-deliberate sources produce random events, sometimes referred to as "Mother Nature" uncertainty. The tools of probability and statistics appropriately study random events. The last decade has seen incredible growth in the use of advanced analytic tools (often based on statistics and probability) to identify patterns, predict potential failures, and even advise courses of action. These increasingly rely on techniques such as machine learning and artificial intelligence. It is important to recognize that these techniques rely on past data, and their ability to predict is often dependent on the quality of such data.

Statistics, Probability, and Possibility

Statistics is the study of methods for organizing and summarizing data and for drawing conclusions based on information contained in it – that is, characterizing things that *have happened.*

Probability is the study of randomness and uncertainty. It includes mathematical methods for quantifying the likelihoods associated with the various outcomes of an experiment – that is, characterizing the things that *might happen.*

Possibility is the study of what could happen, irrespective of whether it is likely or even realistic. Mathematical methods for studying possibility fall into discrete and combinatorial techniques that test multiple scenarios using specified settings (e. g., turning assets on or off) – that is, characterizing things that *could happen.*

In contrast, there is also uncertainty that comes from *deliberate* sources, such as adversaries. For example, in a game of chess a player does not know what the other player will do, but the player can assume that the adversary will behave in a manner that is deliberate and motivated by a desire to win (or to have the other player lose). The field of *game theory* is devoted to making the best possible decisions in the face of this type of uncertainty. Here, a slightly different look at uncertainty is applied, distinguishing between the *probable* and the *possible.* Things that are *probable* can be characterized using probability, typically based on experience or analysis designed to discover the

[303] Adversarial, reliability, and risk analyses are entire fields of study that cannot be adequately covered in a single book chapter. For interested readers, several related texts go into more detail on applying these techniques: Adversarial: Alan. R Washburn, *Two-Person Zero-Sum Games*, New York: Springer, 2014; Reliability: Kailash C. Kapur and Michael Pecht, *Reliability Engineering*, Hoboken, NJ: John Wiley & Sons, 2014; Risk: Terje Aven, *Risk Analysis*, Chichester: John Wiley & Sons, 2015.

frequency with which the event might occur. In contrast, things that are possible could happen but might seem strange, absurd, or unbelievable.

Importantly, officers should not treat adversarial behavior as random, in chess or in war. If there are significant concerns that adversaries intend to disrupt or harm a system, these potential disrupters should not be treated like random events (e.g., weather). Whereas random events might be appropriately represented by an average case, deliberate events are more likely to yield the worst case.

Accordingly, each analysis method considers uncertainty in a distinct way that, in turn, reveals different events and conditions that lead to system failure.

Reliability analysis considers uncertainty regarding the availability and functioning of assets within the system given estimates of the quality of these assets to perform their intended function (e.g., the failure rate of a transformer under normal operating conditions). Reliability methods are the most dependent on statistics and generally employ probability distributions to estimate asset quality and failure rate. Reliability methods also ignore the magnitude of the impacts caused when assets fail. This in turn focuses attention on system design that can meet minimum criteria for how well it will function under anticipated circumstances and prioritizes decisions for redundant, backup, or fail-safe systems. This is in contrast to other analysis techniques that aim to attenuate failure consequences when a failure eventually does occur.

Risk analysis considers uncertainty regarding the likelihood and magnitude of events that put assets in abnormal or extreme operating conditions (e.g., the return period on a storm that can flood the transformer's substation). Risk methods are the most reliant on probability to estimate threat likelihoods and consequences. Importantly, risk analysis often assigns probabilities to possible events that may lack sufficient statistical data, e.g., terrorist attacks, solar storms, extreme floods, etc. Hence, risk analysis prioritizes decisions that minimize the impacts of the most common (i.e., expected) events and consequences, and lowers the importance of decisions for events with rare or low impacts.

Adversarial Analysis considers uncertainty regarding the possibility that some assets may fail in detrimental combinations. The goal is to estimate the quantity of key assets that can be removed from service simultaneously and measure their impacts on system function (e.g., identifying the single, pair, or otherwise combination of worst transformers to lose). Adversarial analysis is most reliant on combinatorial methods to test possibilities by asking "what if" a particular combination of assets is not available, not when, why, or how this lack of availability may occur. The result is adversarial analysis will identify and recommend managing vulnerabilities that will cause the greatest disruption to system function and consequences irrespective of how likely the onset of such an event is.

6.3.2 The Details

This section provides more detail on each analysis method and an example of how each leads to different conclusions on vulnerability.

6.3.2.1 Reliability Analysis

Reliability deals with estimating the future performance of an OE system based on the quality of its assets. The key question reliability analysis is trying to answer is whether the OE system will be dependable in the future. It therefore focuses attention on the design and management of the system itself, including factors such as age, materials, environmental exposure, and maintenance history. Assessors use this information to estimate asset and system quality and to predict potential asset or system failure. An OE system is considered *reliable* if it is expected to perform its functional purpose to a defined quality within a particular future time horizon. Conversely, an OE system is *unreliable* if it will not perform its function within the established time frame and is expected to fail to meet required quality.

Failure in reliability is generally modeled as a binary state – either working (on) or not working (off). However, there are many different levels of failure that OE system operators may identify that define a spectrum of failure modes that are either desirable or undesirable. For example, having a fuse in a circuit overheat and turn off power may be a much more desirable failure state than burning out the wiring. Hence, failure for an OE system is a complex topic that requires a strong functional knowledge of the system's purpose, design, and existing mitigations.

Fault tolerance is the ability of an asset or system to function reliably despite stresses, and it is often measured as a probability of failure over a given amount of time into the future. This measure produces an estimate of asset or system *failure rate*, which is the fundamental measure dictating reliability-based decisions. Assets that have a low failure rate in the near or far future are assumed to be more reliable than assets with a higher failure rate. Reliability analysis is often reported as a *mean time to failure* (MTTF) or a related measure for this reason. MTTF and related measures are primarily used to inform preventive maintenance to keep systems operational. It is often prudent to be proactive and replace a component that is likely to fail before it actually does and causes an operational disruption.

There are also numerous techniques to transform asset-based measures like MTTF into system-wide measures to understand system reliability. For example, a *fault tree* is a tool that relates failure rates and related metrics of multiple assets together to determine when and how an asset failure may lead to system failure. Such analyses are often used to identify places where a system needs to be hardened or to have redundancy added.

6.3.2.2 Risk Analysis

Risk analysis deals with determining which threats to OE system assets and function are more or less important. The key question risk analysis is trying to answer is which threats should be expected to impact the OE system and how consequential these threats will be. Accordingly, risk analysis follows a well-established process that involves defining threats, measuring their likelihood and consequences, and then prioritizing threats based on these measures. An OE system is assumed to be low risk if there are no likely threats that can cause major disruption or damage. Conversely, an OE system is at higher risk if threats are identified that are likely to happen and cause significant impacts.

Threats to OE systems come in all shapes and sizes (see Chapter 4 for greater detail) but are generally categorized based on how they originate and challenge system performance. For example, the Homeland Security National Risk Categorization method developed by the Rand Corporation (see Table 6.1) defines twenty-eight different threats that can impact national critical infrastructure (including OE systems) and organizes them into seven different categories, including: terrorist threats, cyber threats, illegal activities, natural hazards, health hazards, infrastructure hazards, and other. A key step in risk analysis is defining which threats matter most to the OE system. For example, some natural hazards such as tsunamis that may be irrelevant to study for OE systems located inland, and vice versa.

Table 6.1: List of Threats Considered in the Homeland Security National Risk Categorization Framework by the Rand Corporation. Source: Henry H. Willis, Mary Tighe, Andrew Lauland, Lisa Ecola, Shoshana R. Shelton, Meagan L. Smith, John G. Rivers, Kristin J. Leuschner, Terry Marsh, and Daniel M. Gerstein, “Homeland Security National Risk Characterization: Risk Assessment Methodology,” RAND Corporation, 2018.

Terrorist Threats
Attack on leadership
Attack targeting critical infrastructure
Biological weapon attack
Chemical weapon attack
Nuclear attack
Radiological attack
Small arms/explosive attack on populations
Cyber Threats
Cyber attack on critical infrastructure networks
Cyber attack that steals sensitive government data
Cyber attack on government networks
Illegal Activities
Counterfeit goods
Human trafficking
Illegal migration
Mass migration
Transnational drug trafficking
Natural Hazards
Drought
Earthquake
Flooding
Hurricane
Space weather
Tsunami
Volcano
Wildfire
Health Hazards
Agricultural plant disease outbreak
Foreign animal disease outbreak
Transnational communicable disease
Infrastructure Hazards
Technical failure or industrial accident of critical infrastructure cause by human error or age

Once threats are determined, risk analysis requires measures of threat likelihood and consequences to identify system vulnerabilities. Threat likelihoods are generally estimates using statistical methods to relate the size and severity of a threat to its frequency or tendency to occur. For natural hazards, this is often based on historical records of past events, such as the *return period*[304] on a storm or the frequency of earthquakes of different magnitude. For terrorist threats, this may include intelligence estimates of an actor's capability and intent to act, which are then converted into numerical measures of likelihood.

Consequences are generally measured as the impact on the functioning of a system should assets be lost due to a threat. For example, the consequences of a flood on a pipeline system would be estimated given some flood event (either modeled or based on historical data), determining which assets are flooded, which of those assets will stop functioning, and in turn, how much loss of system function results.

The final step in traditional risk analysis is to combine these two measures and compare different threats. Generally, this includes the use of a table to compare threat likelihood and consequences and characterizing risks as high, medium, and low priority. Ideally, this process produces a nuanced view of the risk of each asset in the OE system and potential mitigations. This process means risk analysis will highlight threats that have a large, expected impact on system function, i. e., have high likelihood and consequence. In contrast, risk analysis will understate threats with high likelihood, but have little consequence on system function (e. g., normal rain), or events with enormous consequences, but are very rare (e. g., 1000-year flood). When risk analysis is conducted in this way, it is also referred to a *probabilistic risk analysis* (PRA). PRA is the most common form of risk analysis used across OE systems.

6.3.2.3 Adversarial Analysis

Adversarial analysis deals with finding the "worst-case" failures that challenge an OE system's function irrespective of why they occur. It focuses attention on identifying "bottlenecks" within the OE system, where the loss of few components can lead to a large loss in system function – i. e., locations in the system that would be "easy" for an adversary to interdict (stop, block, destroy, etc.) function with minimal effort.[305] A system is considered easy to interdict if few asset failures lead to a large reduction in system function. Conversely, a system is considered difficult to interdict if many failures are required to produce a reduction in system function.

[304] A return period, also known as a recurrence interval or repeat interval, is an average time or an estimated average time between events.

[305] David L. Alderson, Gerald G. Brown, W. Matthew Carlyle, and Louis Anthony Cox, "Sometimes There Is No 'Most-Vital' Arc: Assessing and Improving the Operational Resilience of Systems," *Military Operations Research*, vol. 18, no. 1, 2013, pages 21–37.

The reason this approach is called adversarial analysis is from its original mathematical development combining optimization and game theory techniques.[306] These techniques, referred to as two-player, zero-sum games, model how an intelligent adversary would inflict damage or disruption on a system – i. e., an adversary would choose to inflict the most damage with the least cost possible. However, this modeling approach is fundamental to finding the worst-case failures a system can experience irrespective of why they may occur (because of an intelligent adversary, or just by bad luck). More broadly, adversarial analysis uses a class of optimization techniques called "interdiction models" to study adversarial decisions and identify worst-case disruptions.

Adversarial analysis is dictated by a few key elements of an interdiction model. An interdiction model can be formulated as a mathematical optimization problem in which the notional "attacker" must choose between a limited set of actions that balance the preferences for disrupting the system with the constraints on the actions they can take.[307] A key metric to assess the actions available to an attacker is referred to as the attack "budget" which reflects the greatest disruption to an OE system that can be triggered by a given number of assets that fail. The most common forms of these models consider actions as binary decisions that turn assets on or off, and all decisions are assumed to occur simultaneously. For example, an adversarial analysis with a budget of three would find the combination of three assets that if turned off simultaneously would cause the greatest disruption to OE system function.

In practice, vulnerability analysis with adversarial modeling is conducted as follows: for different attack budgets (generally increasing from 1, 2, 3, …), identify which assets an adversary should attack with each budget to maximally disrupt the system, and measure how much impact that has on system function.[308] The results of such an analysis are not so simple – the assets that cause the worst-case disruption for a budget of two might be very different than the assets for a budget of three. The reason for this is straightforward: *the importance of a system asset depends on the other assets also available.* For example, consider a bridge that provides transport over a river. How important is this bridge? If there is a second bridge over the river, then the loss of either one in isolation might not cause a big problem. However, losing both bridges together (and interdicting any possible transport over the river) might be catastrophic for the mission.

[306] Gerald Brown, Matthew Carlyle, Javier Salmerón, and Kevin Wood, "Defending Critical Infrastructure," *Interfaces*, vol. 36, no. 6, 2006, pages 530–544.

[307] David L. Alderson, Gerald G. Brown, and W. Matthew Carlyle, "Assessing and Improving Operational Resilience of Critical Infrastructures and Other Systems," *Tutorials in Operations Research: Bridging Data and Decision*, October 27, 2014 (https://doi.org/10.1287/educ.2014.0131).

[308] David L. Alderson, Gerald G. Brown, W. Matthew Carlyle, "Operational Models of Infrastructure Resilience," *Risk Analysis*, vol. 35, no. 4, 2015, pages 562–586.

The goal of this type of vulnerability analysis is to identify the components that, if lost together, would disrupt the system in the worst possible way and/or cause mission failure. Framing this problem from an adversarial perspective often reveals interdependencies and insights not easily obtained using other forms of system analysis.

Application of adversarial analysis across a diversity of critical infrastructure systems has consistently revealed two important implications. First, although it is common to design systems so that the loss of any single component does not compromise system function (this is known as "N-1 security"[309]), few systems are designed to withstand multiple, simultaneous failures (e. g., attacker budget greater than 2). Thus, it is important that designers and operators of OE systems "think beyond the first failure." Second, because the importance of a system component often depends on other components, in many cases it is not possible to rank components from most important to least important.[310] When prioritizing OE infrastructure, planners need to "think systems" and not get overly fixated on prioritized asset lists.

6.3.3 Example for How Reliability, Risk, and Adversarial Analyses Produce Different Results

Figure 6.2 demonstrates how these three analysis techniques differ in practice. In this OE example, a simple fuel network is located on the coast of a major body of water. Deliveries of fuel arrive at coastal pumping stations and are pumped uphill to a local terminal from which fuel is distributed to a community or military installation. The system also has a redundant pumping station and pipelines connecting the coast and the terminal. The pumping stations and terminal are relatively new (less than five years in operation), but the pipeline has been around for a long time (over thirty years).

As analytical assumptions for the reliability, risk, and adversarial methods, it is assumed that planners care about operations for the next year (for reliability analysis), have identified sea level rise, coast storms, and tsunamis as key threats (for risk analysis), and defined the attack budget as a single asset (for adversarial analysis).

These simple assumptions lead to widely different analysis results. Considering the system's history, construction, maintenance record, etc., reliability analysis may indicate the pipelines are the biggest vulnerability. They might be made of old materials and

[309] Electric power systems in the United States are required to be N-1 secure by regulation. However, there are no requirements for these systems to be N-2 secure.

[310] David L. Alderson, Gerald G. Brown, W. Matthew Carlyle, and Louis Anthony Cox, "Sometimes There Is No 'Most-Vital' Arc: Assessing and Improving the Operational Resilience of Systems," *Military Operations Research*, vol. 18, no. 1, 2013, pages 21–37.

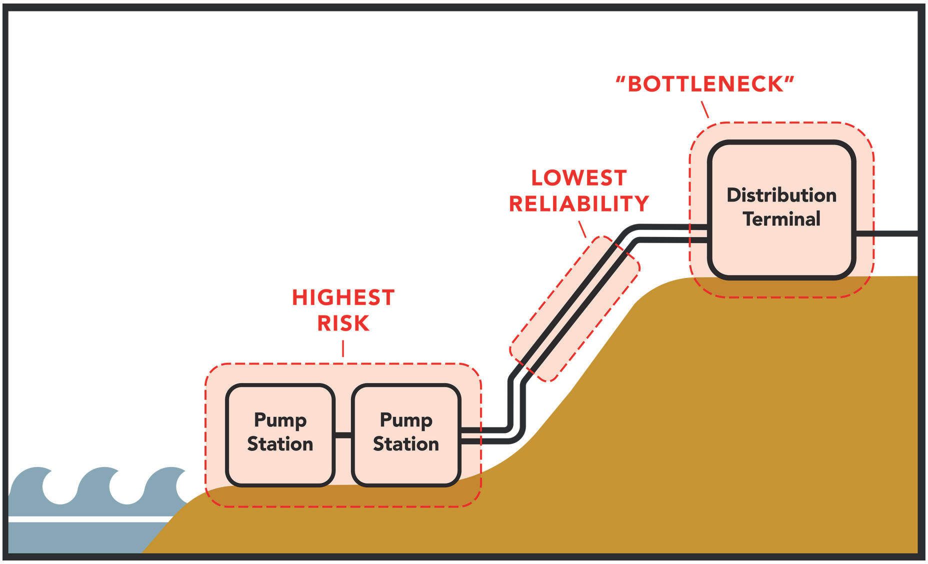


Figure 6.2: Reliability, risk, and adversarial analysis techniques can lead to different results in terms of what is a critical vulnerability.

likely to not function even with proper maintenance and management. In contrast, risk analysis may indicate the pumping stations are the most vulnerable due to their proximity to the coast and low-lying position. Sea level rise, coastal storms, and tsunami threats are most likely to impact pumping and the resulting consequences are sufficient to warrant concern. Finally, adversarial analysis may indicate the distribution terminal as the most vulnerable asset. The system possesses redundant pumping and pipelines, but only one terminal. Hence, the terminal serves as a bottleneck in that, if the terminal is lost for any reason, it will cause worst-case disruptions for fuel access.

6.4 Resilience Strategies for OE Systems

Whereas vulnerability analysis identifies key assets and systems to consider for protection and mitigation efforts, *resilience* involves ways in which to try to adapt and improve systems to avoid losses. A vulnerability analyst should expect reliability, risk, and adversarial analyses to point in different directions. Resilience theory and methods provide a suite of techniques to manage these inherent issues. Overall, it is up to decision-makers to decide how to use limited budgets and time to address vulnerabilities and improve resilience.

Resilience has become a popular term in the last decade for how to think about systems and the way that they deal with stress. The use (and overuse) of this term has resulted in considerable confusion about what it means for a system to be resilient and what we can do to make our systems resilient in the presence of potentially disruptive events.

To make sense of resilience, it helps to first consider its opposite, namely what it means to be *brittle.* Here there is considerable agreement. Something is *brittle* if it has hardness and rigidity but is prone to cracking and breaking when placed under stress. Whereas all systems have some inherent vulnerability, not all systems are inherently brittle. OE systems will experience stress, but soldiers do not want these systems to fail when this happens.

The use and interpretation of what it means to be resilient has evolved over the last few centuries. As far back as the 1800s, resilience was introduced as a mathematically technical concept in material science to characterize if and how a material deforms under stress. Much later, in the 1970s, resilience was used in ecology to describe the ability of an ecosystem to absorb changes and persist. More recently, resilience has also been used in the context of human psychology – alongside other concepts such as character, grit, and hardiness – in describing the factors that contribute to human well-being.

Over the last fifteen years, the concept of resilience has also become prominent in discussions of national security. One of the first mentions of resilience in this context was in the 2007 *National Strategy for Homeland Security* which recognized: “We will not be able to deter all terrorist threats, and it is impossible to deter or prevent natural catastrophes. We can, however, mitigate the Nation’s vulnerability to acts of terrorism, other man-made threats, and natural disasters by ensuring the structural and operational resilience of our critical infrastructure and key resources.”[311] It also offered important guidance: “We must now focus on the resilience of the system as a whole – an approach that centers on investments that make the system better able to absorb the impact of an event without losing the capacity to function.”[312]

In military operations, the notion of resilience is often closely tied with *mission assurance*, as defined in DOD Directive 3020.40 as “A process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan. It is a summation of the activities and measures taken to ensure that required capabilities and all

[311] Homeland Security Council, *National Strategy for Homeland Security, 2007*, October 2007, page 27 (https://www.ojp.gov/ncjrs/virtual-library/abstracts/national-strategy-homeland-security-2007).

[312] Homeland Security Council, *National Strategy for Homeland Security, 2007*, October 2007, page 28 (https://www.ojp.gov/ncjrs/virtual-library/abstracts/national-strategy-homeland-security-2007).

supporting infrastructures are available […] to mobilize, deploy, support, and sustain military operations throughout the continuum of operations."[313]

Origins of resilience – the verb *resile*

Surprisingly, the approach to resilience stems all the way back to its original use and meaning in Latin, as a *verb* related to action.[314] Resilience was originally the verb *resilio* meaning to leap or bounce. Later, this entered early French as the verb *resilire*, meaning to desist, retract, or renege on one's position. The earliest use of resilience in the English language was in the 1500s as the verb *to resile*, with a similar definition to its partner in French. We highlight this form of the word because it is helpful for distinguishing resilience from other similar concepts, such as risk.

Resilience and risk both have noun and verb forms, but they are grammatically and logically different. For example, it is grammatically correct to have one risk, but it makes no sense to have one resilience. Similarly, a system can risk something (e. g., hurricanes) because it is a linking verb, but a system cannot resile something – a system either resiles or does not. This is why risk must always involve the definition of external threats, where resilience is meant to adapt systems to anything.

6.5 Resilience Outcomes: What Should Systems Do (Rather than Fail)

A closer look across the many domains where the term resilience is commonly used reveals several distinct notions. There are four distinct notions of resilience originally identified by Woods[315] and expanded for vulnerability analysis of networked systems by Sharkey et al.:[316]

- **Resilience as robustness.**
  This involves managing a stressful event with limited-to-no impact on normal activities. It also involves the design and operation of systems that continue to function in the presence of stress. This notion of resilience as robustness is also known as *survivable design* or *fault tolerance.*
  An OE system does not exhibit resilience as robustness if it cannot maintain predefined operational thresholds during perturbations.
- **Resilience as rebound.**
  This involves returning system performance to normal (or an acceptable level)

[313] Department of Defense, "DOD Policy and Responsibilities for Critical Infrastructure, DOD Directive 3020.40," January 14, 2010 (https://policy.defense.gov/Portals/11/Documents/hdasa/newsletters/302040p.pdf).

[314] David E. Alexander, "Resilience and Disaster Risk Reduction: An Etymological Journey," *Natural Hazards and Earth System Sciences*, vol. 13, no. 11, 2013, pages 2707–2716.

[315] David D. Woods, "Four Concepts for Resilience and the Implications for the Future of Resilience Engineering," *Reliability Engineering & System Safety*, 141, 2015, pages 5–9.

[316] Thomas C. Sharkey, Sarah G. Nurre Pinkley, Daniel A. Eisenberg, and David L. Alderson, "In Search of Network Resilience: An Optimization-Based View," *Networks*, 2020, pages 1–30 (https://doi.org/10.1002/net.21996).

after a stressful event. Also called "bouncing back."

An OE system does not exhibit resilience as rebound if it cannot resume functioning after a stressful event.

- **Resilience as extensibility.**

  This involves extending system performance or capabilities by reconfiguring and/or prolonging the use of constrained resources to accommodate new operations and survive stressful events. Extensibility is a dynamic capability that reflects how well a system can "stretch" to handle stress or unanticipated events.

  Unlike robustness and rebound, which emphasize the continuation and restoration of existing network function, extensibility focuses on creating new system function to exceed predefined operational thresholds or change functional requirements.

  An OE system does not exhibit resilience as extensibility if its function is so tightly constrained that minor perturbations in resource allocation or functional requirements lead to extreme and cascading losses. Moreover, a system that is unable to redistribute limited resources, adjust operational thresholds, or serve multiple purposes will likely experience brittle failure when unanticipated events require its operations to change.
- **Resilience as adaptability.**

  This involves managing tradeoffs within continuously evolving contexts, often over long timescales, through *adaptive capacity.*

  Adaptive capacity is a system's readiness or potential to adjust a system's operations – its processes, behaviors, relationships – to fit changing situations. Sometimes this is also called *sustained adaptability* because it tends to focus attention on how a system survives over the long term.

  Unlike robustness, rebound, and extensibility, which are concerned with the impacts of stress on a network in a single event (or several events closely related in time), sustained adaptability is less concerned with the outcome of a single event, and more concerned with how a system survives many stressful events over its life cycle, considering tradeoffs between robustness, rebound, and extensibility.

  A system might not exhibit resilience as adaptability in at least two ways: (1) not being able to manage short-term tradeoffs sufficiently to maintain, restore, or extend a system's structure or function, and (2) not being able to manage long-term tradeoffs to balance these adaptive capacities into the future.

Figure 6.3 summarizes each of these notions in terms of the way in which a system is prepared to respond to a stressful event. These four concepts are *resilience outcomes* as they orient resilience activities toward achieving a particular goal for system response. Robustness is really about the system holding onto its existing configuration. Rebound is typically about having the system return as quickly as possible to its previous configuration. A key difference with extensibility and adaptability is that they require the system to *reorganize* itself in order to extend and adapt.

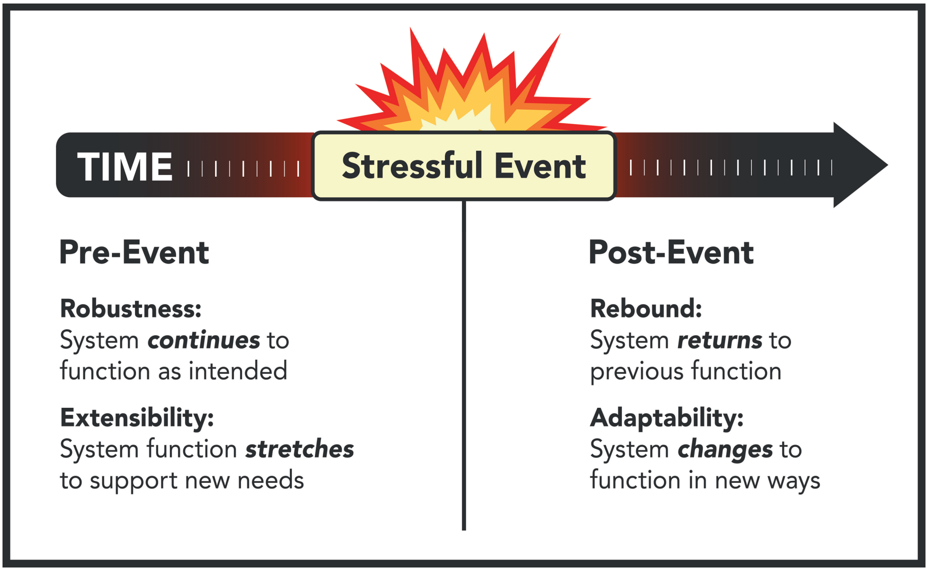

TIME
Stressful Event
Pre-Event
Robustness:
System *continues* to function as intended
Extensibility:
System function *stretches* to support new needs
Post-Event
Rebound:
System *returns* to previous function
Adaptability:
System *changes* to function in new ways

Figure 6.3: A conceptual view of four different notions of resilience.

Each concept of resilience is associated with particular strategies to achieve the intended outcome. For example, strategies to improve robustness of an OE system (e.g., via hardening or protecting existing infrastructure) can conflict with strategies for extensibility by making systems more difficult to reconfigure and extend operations. Similarly, strategies to rebound systems quickly may hinder capacities to adapt systems to have a new structure and function. As a result, there are tradeoffs between one resilience strategy and another. In the contingent case study, we explore vulnerability analysis techniques and tradeoffs between resilience strategies and outcomes through recent events involving energy systems in the US Virgin Islands.

6.6 A Final Thought: Efficiency vs Resilience

Over the last several decades, it has become increasingly fashionable to *optimize* systems – both for OE and in other contexts – in their design and operation. In common parlance, “optimized” is used synonymously with “efficient,” suggesting that a system is inherently improved if it is faster, better, and/or cheaper. But a highly efficient system typically has little waste and/or slack, making it also brittle and fragile.

As a result, there is a grand challenge in the design and operation of OE systems to make them more efficient in using limited resources while still being able to respond and adapt to surprises (as illustrated by the Colonial Pipeline case in chapter 5). The goal in optimizing (a system or plan) should *not* be to eliminate all slack, but to have the right amounts of slack in the right places and at the right times. In practice, optimization should be about assessing tradeoffs between objectives, such as whether we want efficiency or resilience. It is important not to make lean, brittle OE systems. Assessing and improving resilience in OE systems remains a major challenge, both technologically and organizationally, but one that remains critical to the continued success of military operations. And there remain lots of opportunity for contributions from a variety of disciplines.

Tradeoffs exist for all OE systems. There is no one-size-fits-all solution for making OE systems more resilient. There are many ways that OE systems can fail, and there are many ways such failure can be mitigated. Perhaps more important than understanding any single strategy for resilience is understanding the tradeoffs between them. Vulnerability and resilience methods help us recognize these tradeoffs when adapting and improving systems.

6.7 Topics for Discussion and Research

- What are key vulnerability analysis techniques for OE systems? How do they consider uncertainty? How can they lead to different conclusions on how OE systems are vulnerable?
- Describe four different resilience strategies. How do they differ?
- Describe an OE system familiar to you. List all assets in ranked priority based on a chosen vulnerability analysis. Define real or fictitious situations that might lead to a change in vulnerabilities and associated priorities. How might we think of this system in a networked way and prioritize assets without using a list?
- For a given OE system, conduct a vulnerability analysis and define associated resilience strategies. Can you identify tradeoffs in how some resilience strategies either improve or exacerbate system vulnerabilities? Can you identify tradeoffs between resilience strategies and preferred outcomes?

6.8 Case Study: The US Virgin Islands – the Hurricanes of 2017

This case study illustrates concepts for vulnerability analysis and resilience strategies through examination of how US Virgin Islands (USVI) energy systems responded to the 2017 hurricane season.

The USVI Territory comprises three main islands – St. Croix, St. John, and St. Thomas – and several smaller surrounding islands. The islands are among the Leeward Islands of the Lesser Antilles approximately 40 miles east of Puerto Rico and more than 1100 miles from Miami, Florida. The United States acquired these islands in 1917, as part of a strategy to protect the approaches to the Panama Canal during World War I.[317]

In September 2017, Hurricane Irma and Hurricane Maria, both category-5 storms, struck the USVI within a two-week period. These storms devastated critical infrastructure systems, including energy, water, telecommunications, and transportation. Five years after the storms, the territory still had not recovered fully, despite receiving billions of dollars of US emergency federal funding. In the recovery plans, much of the emphasis focused on "bouncing back" to the way things were prior to the storms. However, it was logical that it was better to design systems that can adapt to a future filled with evolving challenges likely from weather and climate, and uncertain changes in technology, and economics.

Yet the story of infrastructure vulnerability and resilience in the USVI dates back long before the 2017 storms. The USVI's energy infrastructure, like many other USVI government services, had been plagued by problems for decades prior to the hurricanes.

The islands' rising energy demand during the twentieth century, highly affected the development of its energy infrastructure. In the mid-1950s, the USVI economy deliberately shifted from agriculture to tourism and manufacturing, and during this period the (permanent and temporary) population of the USVI increased dramatically. The number of tourists increased from approximately 16,000 in 1949 to more than 1.1 million in 1969, while the resident population grew from approximately 26,000 in 1950, to 62,000 in 1970 and 102,000 in 1990.[318]

USVI energy infrastructure includes fuel delivery systems and electric power systems. The islands of St. Thomas and St. John share a single power system, with generation coming from a single power plant in St. Thomas. St. Croix has its own independent power grid, powered by a single power plant. Both power plants burn fossil fuels, historically imported diesel fuel oil and more recently liquefied propane gas (LPG). The Virgin Islands Water and Power Authority (WAPA) owns, operates, and maintains the electric power infrastructure. WAPA is an autonomous government public utility that serves approximately 55,000 customers throughout the Territory.

Historically, power systems in the USVI relied on diesel fuel for power generation because they had a reliable source, a local petroleum refinery. The Hess Oil Virgin Islands Corporation opened a refinery in Limetree Bay, St. Croix in 1966, and it became one of the ten largest refineries in the world. Hovensa LLC, a joint venture between Hess Cor-

[317] Isaac Dookhan, *A History of the Virgin Islands of the United States*, Kingston, Jamaica: Canoe Press, 1994.

[318] Isaac Dookhan, *A History of the Virgin Islands of the United States*, Kingston, Jamaica: Canoe Press, 1994.

poration and Petroleos de Venezuela, took over operation of the refinery in 1998. In the late 2000s, the refinery began to lose money due to reduced demand caused by a global economic slowdown and increased refining capacity in emerging markets.[319]

By 2011, due to loss of revenue,[320] the Hovensa refinery stopped providing diesel fuel to WAPA and in 2012, closed down. The loss of this local source of diesel increased the length and cost of the fuel supply chain to the power system. Although WAPA has transitioned to using LPG as its primary fuel source for electric power generation to increase generator efficiency, save money, and reduce pollution and carbon emissions, the cost of fuel remains high.

Even during normal operations, a lack of generation reliability creates challenges for WAPA to provide stable power. However, during severe weather incidents, transmission and distribution infrastructure often fail. Hurricanes Irma and Maria caused significant damage to electric power infrastructure across the USVI. Nearly 100 percent of WAPA customers lost electricity. The storms damaged the electrical transmission and distribution networks in the territory: with 60 percent of such networks being affected on St. Croix, 80 percent on St. Thomas, and 90 percent on St. John. According to FEMA, WAPA did not restore electricity to 100 percent of eligible customers across the territory until January 2018.[321]

Recovery efforts included a variety of investments intended to increase system resilience. This case study demonstrates the four different notions of resilience in action.

6.8.1 Vulnerability Analysis of the USVI Energy System

- Reliability: the centralized system is highly unreliable based on national standards for power systems. This is compounded with very high electricity rates that many customers are unable to pay.
- Risk: the system is clearly at risk of major storms that bring wind and flood damage to the power system. Risk mitigation would entail hardening parts of the system exposed to hurricane-force winds, flying debris, and flooding.

[319] Associated Press (Business Staff), “Major Oil Refinery to Close in US Virgin Islands,” January 18, 2012 (https://www.cleveland.com/business/2012/01/major_oil_refinery_to_close_in.html).

[320] Associated Press (Business Staff), “Major Oil Refinery to Close in US Virgin Islands,” January 18, 2012 (https://www.cleveland.com/business/2012/01/major_oil_refinery_to_close_in.html).

[321] David L. Alderson, Brendan B. Bunn, Daniel A. Eisenberg, Alan R. Howard, Daniel A. Nussbaum, and Jack Templeton, “Interdependent Infrastructure Resilience in the US Virgin Islands: Preliminary Assessment,” Naval Postgraduate School Technical Report, NPS-OR-18 – 005, December 2018 (https://faculty.nps.edu/dlalders/usvi/NPS-OR-18-005.pdf).

– Adversarial: there is little redundancy in the power system, where individual feeder power lines spread like branches and are subject to outage. This means each power line and all associated communities on that power line has at least one single point of failure. However, these branches are mostly independent, meaning that a failure in one branch often does not affect the others. Another issue is the size and management of generators. The oversizing of generators creates issues when trying to restart systems after a blackout (i. e., blackstart). Together, this means loss of generating assets and/or key substation equipment may be more impactful for the entire power system than bottlenecks that exist on each individual line.

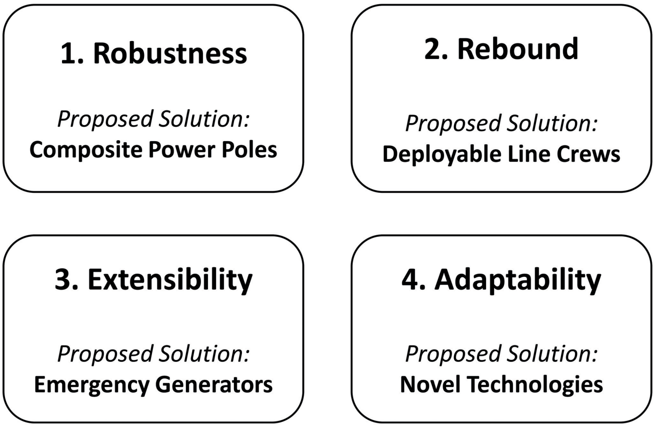


Figure 6.4: Four strategies for creating a resilient energy system in the US Virgin Islands.

Four different resilience strategies for the USVI energy system:

1. Resilience as Robustness: composite power pole
   Power poles made from composite materials are considerably stronger than wooden poles and are capable of withstanding sustained winds up to 200 miles per hour. Installation of composite power poles provides robustness to help mitigate hurricane risk.
2. Resilience as Rebound: deployable line crews
   Being able to deploy trained personnel and equipment in the immediate aftermath of a storm helps manage unreliability with faster recovery times and emergency response.
3. Resilience as Extensibility: emergency generators
   Having the ability to put emergency generators into service on short notice helps mitigate against unreliability by providing additional backup assets to respond to

blackouts. Doing so also helps manage against adversarial attack by decentralizing generating resources.

4. Resilience as Adaptability: redesign of the electric grid to include renewable generation
   Reconfiguring the overall energy system helps mitigate against adversarial vulnerabilities by distributing generation resources and producing power from additional sources. It also helps mitigate hurricane risk by removing some of the most vulnerable infrastructure to hurricanes (e. g., the 240/120 V lines connecting a house to the distribution feeder).

Each of these strategies targets different aspects of resilience, and they can be used in combination as part of a broader resilience portfolio. However, there are tradeoffs and conflicts between these resilience strategies:

- Composite power poles actually *make it more difficult to recover* systems. The poles are so strong that they cannot be cut with a chainsaw or normal means available to onsite workers. In general, it is not possible to repair a broken power pole; it must be replaced, requiring significant cost and time to do so.
- Once in service, emergency backup generators are often used longer and/or more frequently than intended. This overuse can degrade their ability to provide service and can *render them unreliable* when needed for the next big emergency. Moreover, they add more assets to the system that will need regular management, potentially diverting limited resources and degrading the reliability of other assets in the system.
- Having readily deployable line crews is expensive and can create a burden on the local economy. Similar to backup generators, they are likely to be used in non-emergency situations and for non-energy-related purposes and/or may reduce staffing for other purposes due to limited budgets.
- Renewable energy sources in the USVI are only affordable to wealthy users and create incentive for *more* power use. They are more difficult to distribute across communities in need. Should solar panels become unavailable, residential power requirements may be larger than planned by the utility in an emergency, increasing response burden.

6.8.2 Case Conclusions

The lesson in this case is that resilience strategies need to be considered in combination, as part of a broader portfolio. It also illustrates that analysts should look at vulnerability and resilience of system as a whole.

Importantly, the case shows the tradeoffs between resilience strategies and how they can conflict with one another. For example, the USVI system has been vulnerable to major hurricanes for decades and experienced several storms prior to 2017 (and since). Hardening the power grid to withstand hurricane-force winds (i. e., making power poles more robust to storms) comes with the tradeoff that composite power poles are much more difficult and costly to replace (which reduces the ability of the system to rebound). Similarly, the USVI energy system was unreliable prior to the storms and remains unreliable today. Managing reliability would greatly improve the resilience of the system. Another key way to manage power outages is through greater use of backup generators and novel technologies like distributed generation and microgrids. These novel systems add complexity to the existing grid making it more difficult to maintain in lieu of benefits they may bring to respond to regular and extreme blackouts.

6.8.3 Topics for Discussion and Research

- Revisit a small OE system like that of the USVI, e. g., a military installation or other island location. Define vulnerabilities and resilience strategies. How do they differ to the USVI? How are they the same? Why might they differ or be the same?
- What OE challenges (and opportunities) exist for small island territories that don’t exist for the mainland?
- The US DOD has expressed concern regarding climate change and how it potentially affects island territories disproportionately. How do concerns about a changing climate affect resilience strategy in the USVI? Of other island military installations?