



Cyber100 Compass User Guide

Chelsea Quilling, Laura Leddy, and Maurice Martin

National Renewable Energy Laboratory

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

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

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5R00-86529
September 2023



Cyber100 Compass User Guide

Chelsea Quilling, Laura Leddy, and Maurice Martin

National Renewable Energy Laboratory

Suggested Citation

Quilling, Chelsea, Laura Leddy, and Maurice Martin. 2023. *Cyber100 Compass User Guide*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5R00-86529. <https://www.nrel.gov/docs/fy23osti/86529.pdf>.

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

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

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5R00-86529
September 2023

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

NOTICE

This work was authored 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 U.S. Department of Energy Office of Electricity and the U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response. The views expressed herein do not necessarily represent the views of the DOE or the U.S. Government.

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

U.S. Department of Energy (DOE) reports produced after 1991 and a growing number of pre-1991 documents are available free via www.osti.gov.

Cover Photos by Dennis Schroeder: (clockwise, left to right) NREL 51934, NREL 45897, NREL 42160, NREL 45891, NREL 48097, NREL 46526.

NREL prints on paper that contains recycled content.

List of Acronyms

CESA	Clean Energy States Alliance
DER	distributed energy resource
DHS	U.S. Department of Homeland Security
DOE	U.S. Department of Energy
EIA	U.S. Energy Information Administration
FEMP	Federal Energy Management Program
ICE	Interruption Cost Estimate
IEEE	Institute of Electrical and Electronics Engineers
INL	Idaho National Laboratory
IT	information technology
NIST	National Institute of Standards and Technology
NREL	National Renewable Energy Laboratory
OSHA	Occupational Safety and Health Administration
OT	operational technology
SME	subject matter expert

Executive Summary

The continuing deployment of high levels of renewable energy will require a significant reengineering of the electric grid. This transition brings many benefits but also many potentially costly cybersecurity risks. The ability to model and anticipate the cybersecurity impacts from this transition prior to implementation could save system planners considerable time, money, and effort during their clean energy transitions.

Nearly half of all states in the United States have 100% clean energy goals, with target dates ranging from 2030 to 2050, and more than 200 U.S. cities and counties have committed to attain 100% renewable energy. Achieving these goals will mean extensive changes to the grid, with more wind, solar, and other distributed energy resources playing a larger role in generation and regulation. Future energy systems will become a system of systems, where the operating entities for the different renewable resources represent the constituent systems.

The National Renewable Energy Laboratory (NREL) developed Cyber100 Compass for cyber risk assessment at the system-of-systems level for system planners who are trying to reach high levels of renewable resources. Two offices of the U.S. Department of Energy—the Office of Electricity and the Office of Cybersecurity, Energy Security, and Emergency Response—funded NREL to develop this framework, which will enable system planners to understand and mitigate cybersecurity risks for electric systems transitioning to high levels of renewable energy, including 100% renewable electricity.

Greater cybersecurity risks to electrical systems are anticipated and are the subject of continuing research. As deployment increases, utilities and other system planners could unintentionally build in systemic cyber vulnerabilities that would be difficult to address after implementation. The principle of security-by-design, widely accepted at the device level, must also apply to the system-of-systems level. Cyber100 Compass can help system planners apply the principle of security-by-design at scale. Investing in an upfront understanding of system-of-systems risks from high-renewable energy will result in a more resilient system at a lower long-term cost.

This document provides an overview of Cyber100 Compass and serves as a guide to users who are interested in understanding the cybersecurity risks facing their clean energy transition.

Table of Contents

1	Introduction	1
2	Background	2
2.1	Relevant Research.....	3
2.2	Value Added.....	3
3	Conceptual Model	4
4	Core Concepts	6
4.1	Front End.....	6
4.1.1	Risk Tolerance	6
4.1.2	Events	7
4.1.3	Conditions	8
4.1.4	Advanced Settings: Simulation Settings	10
4.2	Back End	11
4.2.1	Baseline Risk.....	11
4.2.2	Conditional Probability	12
4.2.3	Distribution of Impact	12
5	Cyber100 Compass Outputs	13
5.1	Application Considerations	13
6	Summary	14
	Glossary	15
	References	16
	Bibliography	18
	Appendix A. Cyber100 Compass Use Case	20
	Appendix B. Back-End Calculations	24

List of Figures

Figure 1. A series of transitions leading to a high-renewable grid	3
Figure 2. Conceptual drawing of a high-renewable energy mix as a system of systems	4
Figure 3. Decision point: Is the risk acceptable?	5
Figure 4. Example of a risk tolerance curve	6
Figure 5. Cyber100 Compass event input example—harm to equipment	8
Figure 6. Cyber100 Compass condition input example—degrees of centrality	9
Figure A-1. Risk tolerance curve	21
Figure B-1. Flowchart of the Monte Carlo event simulation procedure implemented in Cyber100 Compass	27

List of Tables

Table A-1. 21	
Table B-1. Demonstration of How Cyber100 Compass Turns User-Provided Upper Bounds on Loss Values Into Confidence Intervals for Loss Values.....	24
Table B-2. Equations for Calculating the Mean and Standard Deviation of the Lognormal Distributions Used to Model Loss Values	26

1 Introduction

Cyber100 Compass is a unique risk assessment framework that will enable system planners to understand and mitigate cybersecurity risk for energy systems transitioning to high levels of renewable generation, including 100% renewable electricity. The idea for Cyber100 Compass was developed by the National Renewable Energy Laboratory (NREL) based on past work on high-renewable grids and a series of discussions with the U.S. Department of Energy.

Cyber100 Compass is a desktop application designed with a user-friendly interface. The tool gathers information from users, conducts probabilistic back-end calculations, and outputs data and visualizations to help users understand and analyze their cybersecurity risks based on the unique features of their future energy systems. Cyber100 Compass takes input values for different conditions and produces a risk score of the resulting system. By trying different configurations, system planners can compare the resultant risks against their own risk tolerance and decide which system-of-system controls to implement as they transition toward 100% renewable energy.

This document provides an overview of Cyber100 Compass, the motivation behind developing this tool, and how Cyber100 Compass calculates cybersecurity risk as energy systems transition to higher percentages of renewable energy. In addition, this document provides guidance on how to use the application for maximum benefit.

Cyber100 Compass is intended to be used by individuals and organizations that have (1) a need to understand the risks associated with the future renewable energy systems and (2) can influence the development of those systems. These include utility systems planners and municipalities. To collect data for the assessment, system planners will coordinate with internal and external stakeholders, then input that data into the Cyber100 Compass application, and present the output to utility decision makers and other stakeholders. For examples of how Cyber100 Compass can be used, see Appendix A: Use Case.

2 Background

As of 2022, renewable energy accounts for approximately 21% of the total utility-scale electricity generation in the United States (EIA 2022). This number is likely to increase in the coming years because of policy and market forces. The prices of renewable generation technologies have continued to decrease, and a wide range of jurisdictions have established some sort of renewable portfolio standard or clean energy standard. Currently, 22 states plus the District of Columbia and Puerto Rico have 100% clean energy goals, with target dates ranging from 2030 to 2050 (CESA 2023).

The continuing deployment of high levels of renewable energy could entail a significant reengineering of the grid. Future renewable grids will incorporate more distributed energy resources (DERs)—small energy generation, storage, and combined head and power technologies, including renewable energy technologies (FEMP 2023). DERs will likely be managed by sophisticated control algorithms operating over communication networks reaching almost—or perhaps all the way—to the grid edge to maintain grid stability and reliability. If not implemented correctly, the rapid integration of grid-connected devices and their associated communication networks could provide new cyberattack vectors for threat actors to exploit (INL 2017). Because DERs are typically connected at the local electric distribution level, portions of the emerging distribution grid also fall outside the jurisdiction of federal regulations, such as the North American Electric Reliability Corporation’s Critical Infrastructure Protection—but cyberattacks on distribution elements can reverberate across the bulk electric system as well (Christensen et.al. 2019).

Historically, utilities have been the primary entity managing the electric grids in the United States, but that is changing. An increased focus on renewable energy integration means that many different generation facilities, storage facilities, and responsive loads could be simultaneously managed by multiple operating entities in the future. Besides the utility, these operating entities might include owners of large-scale solar, wind, or storage facilities; aggregators of many small-scale generation units, such as rooftop solar; building management systems; operators of electric vehicle charging stations, etc. Although the current grid is sometimes referred to as a system of systems, the new renewable grid will embody this idea to a much greater degree and on a much larger scale. In this scenario, the individual operating entities will be the systems, each with their own operational infrastructures, control loops, and business objectives. The system of systems will encompass the collective behavior of the grid as these constituent systems are brought together in purposeful, coordinated operation.

How will the restructuring of the grid into a system of systems change the cyberattack surface of the grid? How would a cyberattack on any constituent system impact the broader grid? How will different types of communications between constituent systems—for example, between a utility and an aggregator of solar power—change cyber risk? Without answers to these and similar questions, the cyber risk associated with electric grids deploying high levels of renewable generation remains largely unknown. As deployment increases, utilities and other system planners could unintentionally build in systemic cyber vulnerabilities that would be difficult to address after the fact. The principle of security-by-design, widely accepted at the device level, must also apply at each level up to the system-of-systems level. Although there is no single pathway for mitigating cybersecurity vulnerabilities, building security into the clean energy grid

of the future is a key priority of the U.S. Department of Energy’s Office of Cybersecurity, Energy Security, and Emergency Response.

2.1 Relevant Research

Research has already begun to explore some aspects of grids with high shares of renewable energy. In March 2021, the National Renewable Energy Laboratory (NREL) completed the LA100 study, an integrated engineering-economic analysis of the Los Angeles Department of Water and Power grid projected to the year 2045 with 100% renewable energy (Cochran et.al. 2021.H). However, the cybersecurity implications of grids with high shares of renewable energy were not explored in LA100 nor by any other publicly available effort to date.

2.2 Value Added

Cybersecurity standards, guidance, and risk assessment tools have been created for the grid at many levels, from devices to organizations. However, risk assessment tools have not yet been developed at the emerging system-of-systems level. This is partly due to the newness of this domain but also because of variable conditions inherent in such a system of systems. Because the transition to high levels of renewable energy will require significant reengineering of the grid, system planners need a framework to help them assess and mitigate the cybersecurity risks at each stage of their transition.

Cyber100 Compass is the first-of-its-kind risk quantification framework intended to be used each time significant quantities of renewable energy are added to an existing electric system. Figure 1 illustrates a series of transitions, each of which might trigger the use of Cyber100 Compass.

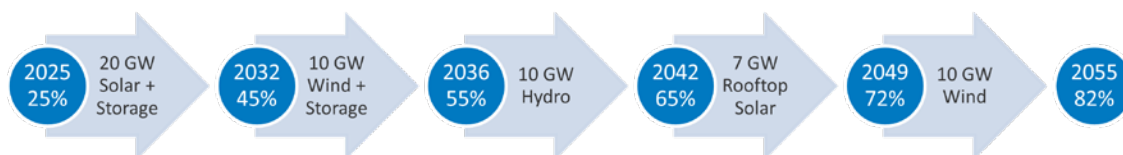


Figure 1. A series of transitions leading to a high-renewable grid

Cyber100 Compass will allow system planners to better understand the risks associated with each proposed transition and how various security controls will impact those risks. In this way, system planners can experiment with various approaches to security prior to executing significant changes to their energy systems, allowing them to practice security-by-design on a system-of-systems scale.

3 Conceptual Model

Cyber100 Compass is designed to accommodate a conceptual model in which high-renewable energy systems are a collection of heterogeneous generation technologies controlled by multiple operating entities.

Figure 2 shows an example of a hypothetical grid with high levels of renewable generation and storage; each circle represents a constituent system within the system of systems. The lines between the circles represent communication pathways. Power connections are not shown. Note that, for this hypothetical grid, there are multiple suppliers of solar, wind, and bulk storage. The utility, which is not shown in Figure 2, could assume one or more of these roles.

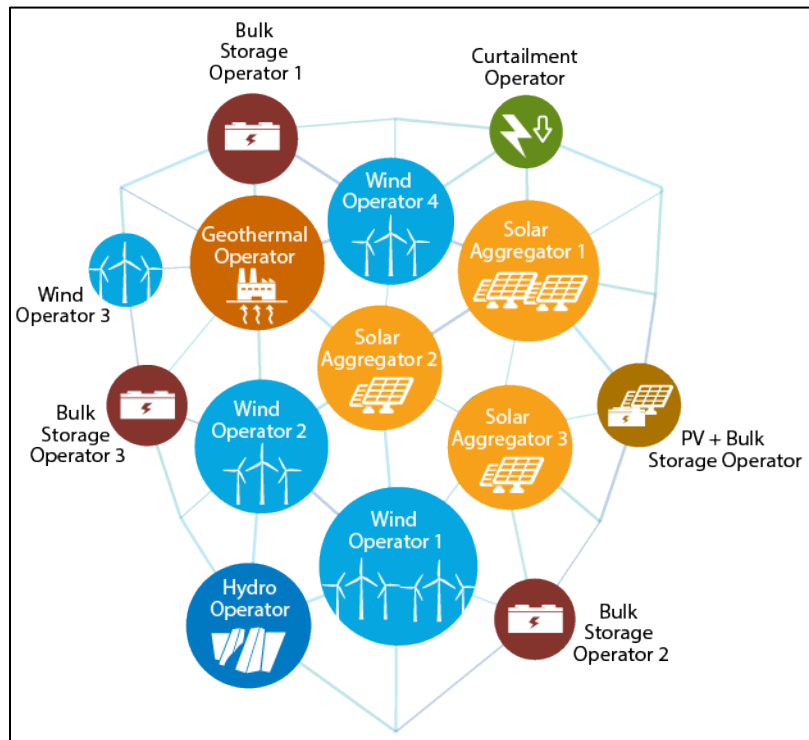


Figure 2. Conceptual drawing of a high-renewable energy mix as a system of systems

This conceptual model offers users a novel method of quantifying and visualizing the cybersecurity risks of their future energy systems to share with investors, executive leadership, industry, and other stakeholders to improve decision making during the energy transition. Figure 3 represents the iterative process system planners would use to bring their anticipated cyber risk to acceptable levels.

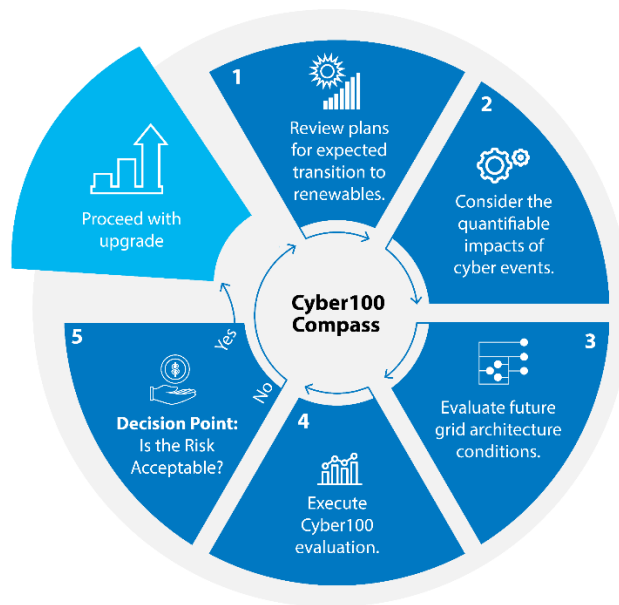


Figure 3. Decision flow from Cyber100 Compass

The results generated by Cyber100 Compass are intended to direct users to the strengths and vulnerabilities of their energy transition plans and to help decision makers focus on high-impact areas for cyber defense investments and risk mitigation strategies.

4 Core Concepts

Cyber100 Compass uses probabilistic methods to estimate cybersecurity risks based on the unique characteristics of a user’s energy system as well as their organization’s risk tolerance. This section introduces the core concepts present in Cyber100 Compass on the front end (what the user sees and interacts with) and the back end (the tool’s structure, data, and logic).

4.1 Front End

Several Cyber100 Compass components require user input to generate the calculations used to estimate a user’s cybersecurity risks.

4.1.1 Risk Tolerance

Risk tolerance describes an organization’s willingness to accept certain levels of risk based on the financial losses that could occur from a cyberattack. Risk tolerance inputs in Cyber100 Compass help users quantify the potential losses their organization might be willing accept from certain kinds of cyberattack. Risk tolerance defines the losses from a given cyber event based on the probability of occurrence. Risk tolerance values, combined with values derived from event inputs and condition questions, which are explained later in this section, will warn users if their system development plans are leading them toward unacceptable levels of risk.

The risk tolerance inputs are entered in a specific format, through the creation of a *risk tolerance curve*. The risk tolerance curve, a widely used concept in decision sciences (Geer et.al. 2016, 66) visualizes losses based on the probability of occurrence, with larger losses less likely than smaller losses. Figure 4 shows an example of a risk tolerance curve.

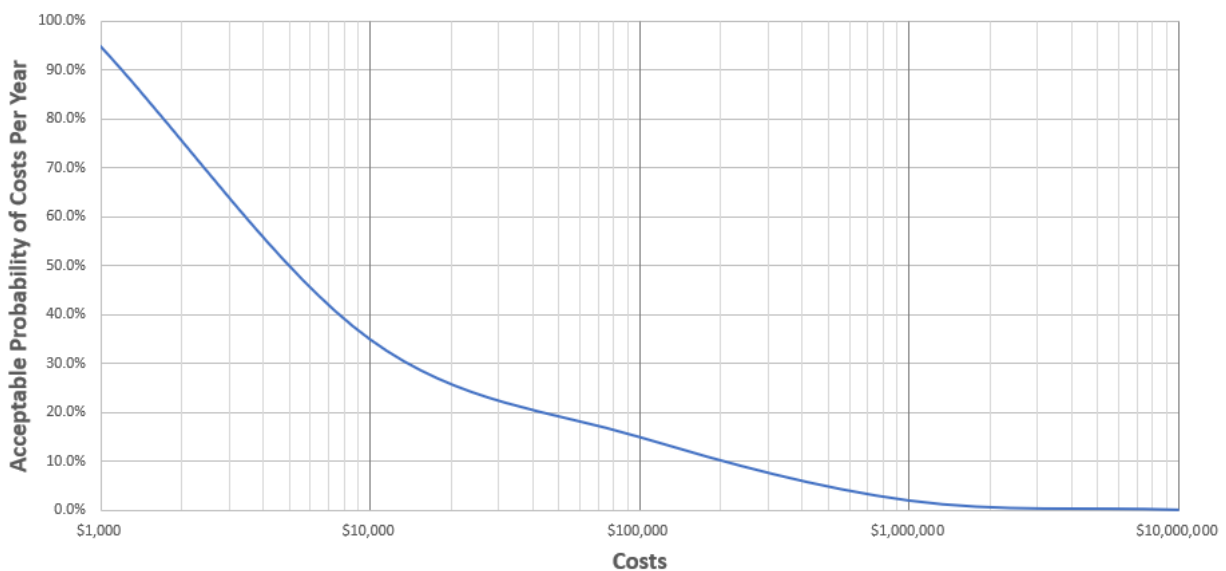


Figure 4. Example of a risk tolerance curve

An even deeper dive into risk tolerance curves and probabilistic risk assessment can be found in Chapter 3 of the book *How to Measure Anything in Cybersecurity Risk* (Geer et al. 2016).

4.1.2 Events

Event inputs allow users to quantify the value they place on avoiding certain types of adverse events that could be caused by a successful cyberattack. In the resilience space, these values are often called “avoided costs” (NREL 2022).

4.1.2.1 Avoided Cost

Avoided cost is the estimated cost that would result from a possible cyberattack, which users hope to avoid. For instance, if a utility knows from experience that an outage of its entire system lasting 12 hours would result in financial damages of \$100,000, then the value of avoiding that event is \$100,000. If the utility can take action to prevent the outage, then those actions result in an avoided cost of \$100,000.

When calculating the avoided cost, Cyber100 Compass asks users to include all possible expenses that might arise from the attack. At a minimum, these include the loss of revenue from business that cannot be transacted due to the attack as well as the cost of recovery efforts; however, there are many other possible costs to consider. For instance, utilities could include the economic impact of a cyber-induced outage on their customers. Cyber100 Compass allows for considerable flexibility in calculating avoided costs for different cyber events. The tool suggests some cost factors users might consider, but deciding which costs to include is ultimately up to the user.

4.1.2.2 Event Categories

Cyber100 Compass asks users to generate avoided cost values for events spread across the following five categories:

- Power outage
- Harm to equipment
- Harm to employees
- Harm to community
- Denial of communication.

These events could impact systems and networks that control physical devices and processes—for instance, a command on an electric utility operational technology (OT) network might open a circuit breaker and cause an outage. Cyber100 Compass considers only cyber events that impact OT systems and networks.

Attacks focused on information technology (IT) systems are out of scope for Cyber100 Compass. IT systems store, transmit, and process information, but they do not control physical devices. An example of an IT system would be one designed to process financial records. In some cases, attacks might begin on IT systems and pivot to OT systems through some touchpoint. In these scenarios, Cyber100 Compass is concerned with only the OT impacts of such attacks. The decision to exclude IT system impacts reflects the unique nature of OT systems in relation to the security, safety, and reliability of the electric grid.

4.1.2.3 Sources of Information

For some types of events, users might partially base valuations on similar past events with a non-cyber origin. For instance, when placing a value on avoiding an outage, a utility can look at data

from outages caused by weather, equipment failure, etc. The utility does not need to have experienced an outage due to cyberattack—much of the value is determined by the nature of the event, not the cause; however, the cause of the attack might influence how the utility estimates the cost of recovery.

4.1.2.4 Assessment Scales

Each event is divided into three impact levels: low, moderate, and high. The impact levels represent a simplified assessment scale inspired by the National Institute of Standards and Technology (NIST) Special Publication 800-30, Appendix H, Table H-3 (NIST 2012b). Cyber100 Compass leveraged this assessment scale to guide users in estimating the avoidance costs they must input across the five event categories. Figure 5 shows an example of an event input—in this case, in the category of harm to equipment—that users are asked to complete.

Impact Scale from NIST SP 800-30	Compass Interpretation	Maximum Avoided Cost
Low <i>...minor damage to organizational assets...</i>	<p>Criteria: Even though equipment is damaged, the grid can continue to deliver power to all customers by shifting functions to other equipment still in operation. Little or no service interruption.</p> <p>Example: A transformer is rendered inoperable, but the system stays online (with only minor interruptions) by rerouting power and operating other transformers closer to their rated limit.</p>	<input type="text" value="\$"/>
Moderate <i>...significant damage to organizational assets...</i>	<p>Criteria: The damaged equipment can be replaced with spares that system operators already have on hand. Service is interrupted only for the time required to make this replacement.</p> <p>Example: A transformer is rendered inoperable, taking part of the grid offline. Workers install a spare transformer within 24 hours, restoring the system to full capacity.</p>	<input type="text" value="\$"/>
High <i>...major damage to organizational assets...</i>	<p>Criteria: System operators do not have spare equipment of the correct kind or in sufficient numbers to replace the damaged equipment. Parts of the system remain offline until replacement equipment is ordered and delivered.</p> <p>Example: A large substation transformer is rendered inoperable. Obtaining a replacement will take several months, during which time system operators must implement rolling blackouts.</p>	<input type="text" value="\$"/>

Figure 5. Cyber100 Compass event input example—harm to equipment

The maximum avoided cost describes the highest dollar amount a user estimates the organization could lose at each impact level for each type of event. Each of the five event categories requires users to input the maximum avoided costs at low-, moderate-, and high-impact levels. Once users complete all the inputs across all five event categories, they may proceed to the next part of the tool—conditions.

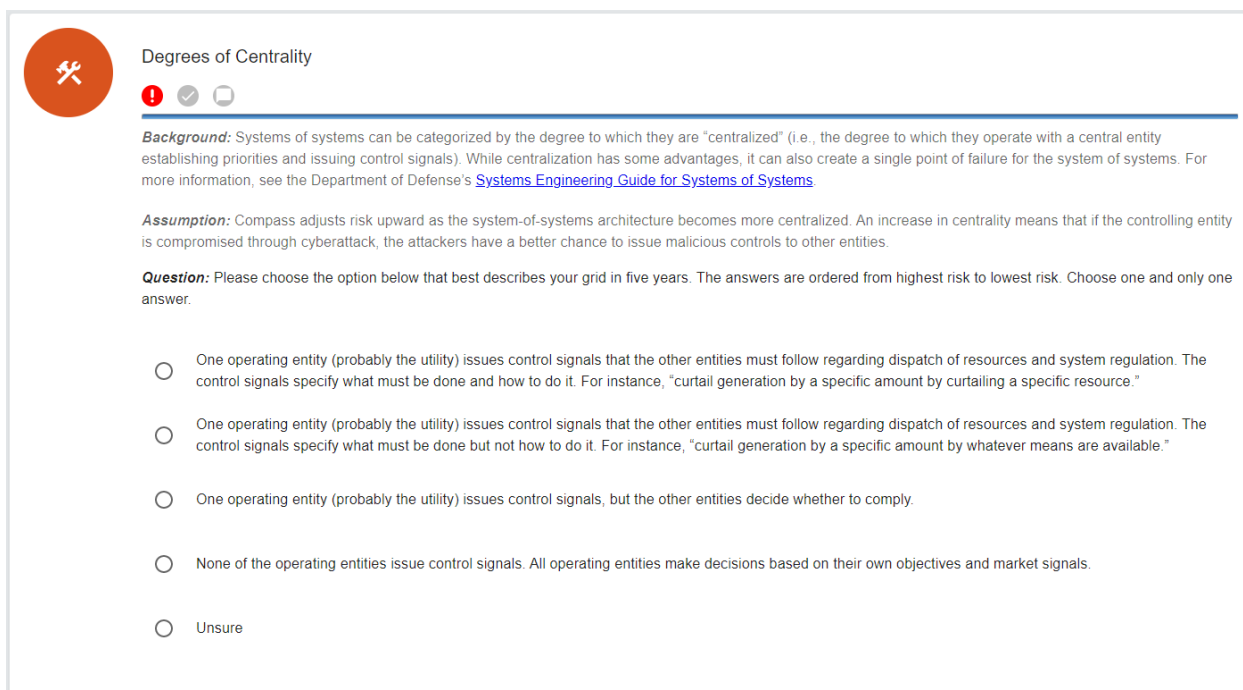
4.1.3 Conditions

For Cyber100 Compass purposes, the “conditions” describe any constraints, resources, requirements, controls, or other factors that modify the cybersecurity risks of a system’s energy transformation plans. Conditions are presented as a series of questions posed to users about their energy transition plans. These questions allow users to describe aspects of their current and future energy systems that will impact cybersecurity risk.

The conditions in Cyber100 Compass are similar to NIST’s definition of a “predisposing condition” (NIST 2023):

A condition that exists within an organization, a mission/business process, enterprise architecture, or information system including its environment of operation, which contributes to (i.e., increases or decreases) the likelihood that one or more threat events, once initiated, will result in undesirable consequences or adverse impact to organizational operations and assets, individuals, other organizations, or the Nation.

Cyber100 Compass extends this idea from the present into the future. Many of the condition questions ask users what they expect to be true about their electric system within the next 5 years. Figure 6 provides an example of condition inputs.



Degrees of Centrality

Background: Systems of systems can be categorized by the degree to which they are “centralized” (i.e., the degree to which they operate with a central entity establishing priorities and issuing control signals). While centralization has some advantages, it can also create a single point of failure for the system of systems. For more information, see the Department of Defense’s [Systems Engineering Guide for Systems of Systems](#).

Assumption: Compass adjusts risk upward as the system-of-systems architecture becomes more centralized. An increase in centrality means that if the controlling entity is compromised through cyberattack, the attackers have a better chance to issue malicious controls to other entities.

Question: Please choose the option below that best describes your grid in five years. The answers are ordered from highest risk to lowest risk. Choose one and only one answer.

- One operating entity (probably the utility) issues control signals that the other entities must follow regarding dispatch of resources and system regulation. The control signals specify what must be done and how to do it. For instance, “curtail generation by a specific amount by curtailing a specific resource.”
- One operating entity (probably the utility) issues control signals that the other entities must follow regarding dispatch of resources and system regulation. The control signals specify what must be done but not how to do it. For instance, “curtail generation by a specific amount by whatever means are available.”
- One operating entity (probably the utility) issues control signals, but the other entities decide whether to comply.
- None of the operating entities issue control signals. All operating entities make decisions based on their own objectives and market signals.
- Unsure

Figure 6. Cyber100 Compass condition input example—degrees of centrality

These questions are meant to elicit information; they are not meant to be—and they should not be interpreted as—policy recommendations. Further, Cyber100 Compass is not primarily focused on the physical controls for security. The purpose of Cyber100 Compass is to assess the risk of cyberattacks producing physical impacts on energy systems, not physical security breaches that have cybersecurity impacts.

Condition questions are spread across the following five categories:

1. Changes to grid topology
2. Changes to system-of-systems architecture
3. Communications
4. Security controls
5. Regulatory environment.

Each answered condition question refines the user’s risk estimate specific to the system under consideration. These refinements improve the probabilistic calculations that quantify the cybersecurity risks for the assessed future energy system.

Because Cyber100 Compass users are asked about future aspects of their grids, there is inevitably some amount of uncertainty. Users of Cyber100 Compass are not expected to have perfect knowledge regarding their energy systems within the 5-year time span identified in most questions. If a question asks for one and only one answer, Cyber100 Compass gives users the opportunity to select “unsure”; however, users are encouraged to use this option as infrequently as possible. Selecting more decisive answers—based on business plans, information from third parties, trends, the user’s own foresight, and other sources—produces results that are more specific to their future system. The more questions that are decisively answered, the better Cyber100 Compass can estimate risk and calculate expected losses from cybersecurity events.

4.1.3.1 Sources of Information

Users might find it helpful to refer to the following information sources as they progress through the questions:

- Utility personnel, which could include the chief security officer, the chief technology officer, the chief information officer, system planners, control engineers, power engineering teams, communication engineers, the chief financial officer, the corporate governance team, the government affairs office, etc.
- System planning data, which could include design documents, power purchase agreements, capacity expansion models, projections of load growth, etc.
- Persons involved in the development and implementation of interconnection agreements
- Current or future third-party operating entities
- State public utility commissions
- State, regional, or national service organizations, for example, the National Rural Electric Cooperative Association or one of its state-level associations.

4.1.4 Advanced Settings: Simulation Settings

There is naturally a high degree of uncertainty related to the cybersecurity risks of the future grid. Cyber100 Compass handles this uncertainty and the presence of potential random variables by using Monte Carlo simulations to better understand the impact of cybersecurity risks. A Monte Carlo simulation is a mathematical process of repeatedly simulating the outcome of an uncertain event or process and then analyzing the outcomes in aggregate to draw inferences about the uncertain event or process (Shonkwiler and Mendivil 2009). Monte Carlo simulations help Cyber100 Compass users improve loss estimates, given the potential for many unknown random variables when estimating future cybersecurity risks. The advanced settings of Cyber100 Compass provide users the opportunity to set the number of Monte Carlo simulations used to predict the probabilities of a variety of monetary losses resulting from cybersecurity events within a single year.

4.1.4.1 Reproducibility and Random Seeds

The results of a Monte Carlo simulation depend on stochasticity, or randomness, and generally involve the use of a random number generator or draws from probability distributions. Due to

this stochasticity, the numerical results from a Monte Carlo simulation will be slightly different each time the simulation is executed unless a random seed is used to begin the simulation.

A random seed tells the simulation code to use the same process to generate the random numbers every time the simulation is executed, meaning the same random numbers will be generated and the results will be reproducible. Cyber100 Compass sets a random seed by default and provides this value to users; the seed value can also be set or changed by users. This serves two purposes: The first is reproducibility of simulation results, and the second is to allow users to iteratively adjust the conditions being applied and view the impact on the simulation results. By setting the random seed before changing the conditions, all changes in the simulation results are due to the updated conditions rather than stochasticity.

Within a single simulation, representing 1 year, the cyber events that occur and the levels of severity or impact for each event are determined stochastically. The simulation settings, including the number of Monte Carlo simulations, and the random seed can be determined by the user under the “advanced settings” of Cyber100 Compass.

4.2 Back End

On the back end, Cyber100 Compass is data driven and uses object-oriented programming. All events, conditions, and cybersecurity controls are specified using input data sets. Events, conditions, and risk tolerance are defined as generic “objects,” which are populated with information from input data sets. Cyber100 Compass back-end computations include three key components: baseline risk, conditional probability, and distribution of impact.

The values of these three components were solicited from a select group of subject matter experts (SMEs) with deep expertise in system planning, cybersecurity, interconnection agreements, and related topics. The inputs from multiple SMEs were combined to arrive at the values required for Cyber100 Compass back-end computations.

4.2.1 Baseline Risk

Baseline risk describes the cybersecurity risks to a user’s electric system before any conditions are applied. Cyber100 Compass drew from NIST Special Publication 800-30 to develop the approach to determining baseline risk in Cyber100 Compass (NIST 2012b). For each type of event, the SMEs selected a rating for three factors from NIST 800-30:

- **C = adversary capability.** For a particular event (e.g., outage), what is the cyberattacker’s level of expertise, resources, and opportunities to support the attack? (Table D-3)
- **T = adversary targeting.** For a particular event, to what degree is the cyberattacker specifically interested in disrupting the electric system or (more specifically) a particular system operator? (Table D-5)
- **V = vulnerability severity.** How vulnerable is the electric system operator to cyberattack? (Table F-2)

Each rating is given an assigned value, which is multiplied to obtain the baseline probability.

4.2.2 Conditional Probability

As mentioned previously, conditions—including technical controls, policies, architecture, and topologies that users select—can either increase or decrease risk. These increases or decreases in risk are expressed as conditional probabilities.

To arrive at the conditional probabilities, SMEs applied adjustment factors to each baseline probability for each possible answer to a condition question. For instance, in a condition question about communication protocols, the continued use of older communication protocols that lack security features is likely to increase risk; switching to modern, secure communication protocols decreases risk. The SMEs determined how much these conditions should increase or decrease the baseline and chose an adjustment factor accordingly. These adjustment factors determined the conditional probabilities.

Because conditions are selected by the user, it is likely that some will increase risk and others will decrease it. Cyber100 Compass tracks this, arriving at amalgams—or combinations—of the baseline probabilities plus all conditional probabilities. These amalgams are used to calculate the application's Cyber100 Compass output.

4.2.3 Distribution of Impact

Another way that SMEs contributed to Cyber100 Compass back end was by determining the distribution of impact for different events. Starting with the assumption that an event has occurred, the SMEs determined the relative probability that the event will be low impact, moderate impact, or high impact according to the same criteria used by users when determining the maximum avoided costs.

Cyber100 Compass uses this distribution of impact during Monte Carlo simulations to determine the range (low, moderate, or high) of each event that happens during the simulation. The exact value within the range is then determined by supplying a random value to a function. See Appendix B for details.

5 Cyber100 Compass Outputs

Upon completion of all portions of the user inputs, the user will run Cyber100 Compass and generate a series of visualizations that show how the user's system risk compares with their risk tolerance. These visualizations, in an easily digestible format, can be shared with decision makers and stakeholders to inform future plans and investment decisions.

If the expected financial losses from different cyberattack events exceed the risk a system is willing to tolerate, planners might reconsider and/or adjust upgrade plans by changing the power or control elements or by applying additional cybersecurity mitigations. The utility could then rerun Cyber100 Compass with the revised plan to see if the expected loss would be more acceptable. Cyber100 Compass is intended to be used at multiple stages of a system's energy transition. As such, users have the option to download the information input into Cyber100 Compass as a CSV file for later use.

5.1 Application Considerations

Cyber100 Compass is a desktop application compatible with 64-bit machines running Windows 10 or higher or macOS.

The back-end server of Cyber100 Compass is hard-coded to launch on Port 4000. Cyber100 Compass users will see an error on the front end if there's another application or service running on Port 4000. If that is the case, users will need to close anything running on Port 4000 and relaunch the application to view their results and visualizations.

Note that in the advanced settings of Cyber100 Compass, users may upload any CSV file; however, this could result in an error if the file is not specifically formatted for Cyber100 Compass. It is therefore recommended that users use only CSV files produced by Cyber100 Compass and avoid uploading other files.

6 Summary

Cyber100 Compass is a novel risk management tool that provides systems planners with actionable and quantifiable risk assessments for their clean energy transition and future energy systems. Cyber100 Compass will enable system planners to explore the consequences of different kinds of cyberattack scenarios without putting any assets or resources at risk. With Cyber100 Compass' assessment, systems planners will be able to make more informed decisions to ensure that the next evolution of their energy system is designed with security in mind. System planners can repeat the risk assessment process at each phase of their renewable energy transition.

Glossary

Term	Definition
Baseline risk	Cybersecurity risks present within a user's electric system before any conditions are applied
Conditions	Any constraints, resources, requirements, controls, or other factors that modify the cybersecurity risks of a system's energy transformation plans. In Cyber100 Compass, conditions are presented as a series of questions posed to users about their energy transition plans.
Conditional probabilities	Increases or decreases in risk expressed as probabilities that are applied to adjust the baseline risk based on user's answers to conditions questions
Events	Cyber incidents that have physical impacts on operational technology systems and networks, for example, a power outage, damage to equipment, or the loss of communication leading to the loss of generation
Maximum avoided cost	A monetary value provided by Cyber100 Compass users within the events page of the tool. This value describes the highest dollar amount a user estimates the organization could lose from a cyber event in a given year given certain limiting factors. Maximum avoided costs are provided by users at low-, moderate-, and high-impact levels for each kind of Cyber100 Compass cyber event.
Monte Carlo simulation	A mathematical process of repeatedly simulating the outcome of an uncertain event or process and then analyzing the outcomes in aggregate to draw inferences about the uncertain event or process
Random seed	A model parameter within a Monte Carlo simulation that ensures the same series of pseudo-random numbers are used every time a Monte Carlo simulation is executed. This ensures that the results will be reproducible.
Risk tolerance	An organization's willingness to accept certain levels of risk based on the financial losses that could occur from cyberattack

References

- Bertsekas, D., and Tsitsiklis, J. N. 2008. *Introduction to Probability* (Vol. 1). Athena Scientific.
- Christensen, Dane, Maurice Martin, Erdenebat Gantumur, and Brandon Mendrick. 2019. “Risk Assessment at the Edge: Applying NERC CIP to Aggregated Grid-Edge Resources.” *The Electricity Journal* 32 (2): 50–57. <https://doi.org/10.1016/j.tej.2019.01.018>.
- Clean Energy States Alliance (CESA). 2023. “Table of 100% Clean Energy States.” Accessed May 26, 2023. <https://www.cesa.org/projects/100-clean-energy-collaborative/guide/table-of-100-clean-energy-states/>.
- Cochran, Jaquelin, and Paul Denholm, eds. 2021. *The Los Angeles 100% Renewable Energy Study*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-6A20-79444. <https://maps.nrel.gov/la100/>.
- Federal Energy Management Program (FEMP). 2023. “Distributed Energy Resources for Resilience.” Accessed May 11, 2023. <https://www.energy.gov/femp/distributed-energy-resources-resilience>.
- Geer, Daniel E. Jr, Douglas W. Hubbard, Stuart McClure, and Richard Seiersen. 2016. “Chapter 3.” In *How to Measure Anything in Cybersecurity Risk*. Wiley.
- Idaho National Laboratory (INL). 2017. *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector: Mission Support Center Analysis Report*. Idaho Falls, ID: Idaho National Laboratory Mission Support Center. <https://doi.org/10.2172/1337873>.
- Murphy, K. P. 2012. *Machine Learning: A Probabilistic Perspective*. Cambridge, MA: MIT Press.
- National Institute of Standards and Technology (NIST). 2012a. “1.3.6.6.9 Lognormal Distribution.” In *NIST/SEMATECH e-Handbook of Statistical Methods*. Accessed May 25, 2023. <http://www.itl.nist.gov/div898/handbook/eda/section3/eda3669.htm>.
- . 2012b. *NIST Special Publication 800-30, Revision 1: Guide for Conducting Risk Assessments*. Gaithersburg, MD. Last updated April 23, 2021. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>.
- . 2023. “Glossary.” Computer Security Resource Center. Accessed May 11, 2023. https://csrc.nist.gov/glossary/term/predisposing_condition.
- National Renewable Energy Laboratory (NREL). 2022. “Valuing Resilience in Electricity Systems.” Golden, CO. Accessed May 26, 2023. <https://www.nrel.gov/docs/fy19osti/74673.pdf>.
- Shonkwiler, Ronald W., and Franklin Mendivil. 2009. *Explorations in Monte Carlo Methods*. Dordrecht, Netherlands: Springer.

U.S. Energy Information Administration (EIA). 2022. “How Much of U.S. Energy Consumption and Electricity Generation Comes from Renewable Energy Sources?” Frequently Asked Questions (FAQs). Updated April 28, 2022. <https://www.eia.gov/tools/faqs/faq.php?id=92&t=4>.

Bibliography

- Bartol, Nadya. 2015. *Cyber Supply Chain Risk Management for Utilities—Roadmap for Implementation*. Washington, D.C.: Utilities Telecom Council. <https://utc.org/wp-content/uploads/2018/02/SupplyChain2015-2.pdf>
- Carter, Cedric, Christine Lai, Nicholas Jacobs, Shamina Hossain-McKenzie, Patricia Cordeiro, Ifeoma Onunkwo, and Jay Tillay Johnson. 2017. “Cyber Security Primer for DER Vendors Aggregators and Grid Operators.” Albuquerque, NM: Sandia National Laboratories. SAND-2017-13113. <https://doi.org/10.2172/1761987>.
- Goff, Ed, Cliff Glantz, and Rebecca Massello. 2014. “Cybersecurity Procurement Language for Energy Delivery Systems.” In *Proceedings of the 9th Annual Cyber and Information Security Research Conference (CISR '14)*, 77–79. New York, NY: Association for Computing Machinery. <https://doi.org/10.1145/2602087.2602097>.
- Institute of Electrical and Electronics Engineers (IEEE). 2012. IEEE Std 1366-2012 (Revision of IEEE Std 1366-2003)—IEEE Guide for Electric Power Distribution Reliability Indices. New York, NY. <https://doi.org/10.1109/IEEESTD.2012.6209381>.
- Interruption Cost Estimate (ICE) Calculator. 2023. U.S. Department of Energy Office of Electricity, Lawrence Berkeley National Laboratory, and Nexant. Accessed June 8, 2023. <https://icecalculator.com/home>.
- Johnson, Jay. 2017. *Roadmap for Photovoltaic Cyber Security*. Albuquerque, NM: Sandia National Laboratories. SAND2017-13262, 1782667, 668568. <https://doi.org/10.2172/1782667>.
- Kniesner, Thomas J., and W. Kip Viscusi. 2019. “The Value of a Statistical Life.” *Oxford Research Encyclopedia of Economics and Finance*. Vanderbilt Law Research Paper No. 19-15. <https://doi.org/10.2139/ssrn.3379967>.
- Narang, David, Peter Schwartz, Steve Widergren, Sigifredo Gonzalez, S. Alam, Theodore Bohn, Yaosuo Xue et al. 2021. *GMLC Survey of Distributed Energy Resource Interconnection and Interoperability Standards*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5D00-77497, 1823018, MainId:27433. <https://doi.org/10.2172/1823018>.
- National Institute of Standards and Technology (NIST). 2020. *NIST Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations*. Gaithersburg, MD. <https://doi.org/10.6028/NIST.SP.800-53r5>.
- National Renewable Energy Laboratory (NREL). 2023. “Customer Damage Function Calculator.” Accessed June 8, 2023. <https://cdfc.nrel.gov>.
- Occupational Safety and Health Administration (OSHA). 2023. “Estimated Costs of Occupational Injuries and Illnesses and Estimated Impact on a Company’s Profitability Worksheet.” U.S. Department of Labor. Accessed June 8, 2023. <https://www.osha.gov/safetypays/estimator>.

Onunkwo, Ifeoma. 2020. *Recommendations for Data-in-Transit Requirements for Securing DER Communications*. Albuquerque, NM: Sandia National Laboratories. SAND2020-12704. <https://doi.org/10.2172/1813646>.

Reaves, Bradley, and Thomas Morris. 2012. “Analysis and Mitigation of Vulnerabilities in Short-Range Wireless Communications for Industrial Control Systems.” *International Journal of Critical Infrastructure Protection* 5 (3): 154–74. <https://doi.org/10.1016/j.ijcip.2012.10.001>.

Shea, Daniel. 2020. *Cybersecurity and the Electric Grid: The State Role in Protecting Critical Infrastructure*. Washington, D.C.: National Conference of State Legislatures. Accessed June 8, 2023. <https://www.ncsl.org/energy/cybersecurity-and-the-electric-grid-the-state-role-in-protecting-critical-infrastructure>.

Stouffer, Keith, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, and Adam Hahn. 2015. *NIST Special Publication 800-82, Revision 2: Guide to Industrial Control Systems (ICS) Security*. Gaithersburg, MD: National Institute of Standards and Technology. <http://dx.doi.org/10.6028/NIST.SP.800-82r2>.

Sundararajan, Aditya, Aniket Chavan, Danish Saleem, and Arif I. Sarwat. 2018. “A Survey of Protocol-Level Challenges and Solutions for Distributed Energy Resource Cyber-Physical Security.” *Energies* 11 (9): 2360. <https://doi.org/10.3390/en11092360>.

Sunspec Alliance. 2018. “Cybersecurity Webinar: Securing California Rule 21 Networks.” December 13, 2018. <https://sunspec.org/cybersecurity-webinar-securing-california-rule-21-networks/>.

U.S. Department of Energy (DOE). 2022. *Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid*. Washington, D.C.: Office of Cybersecurity, Energy Security, and Emergency Response and Office of Energy Efficiency and Renewable Energy. <https://www.energy.gov/sites/default/files/2022-10/Cybersecurity%20Considerations%20for%20Distributed%20Energy%20Resources%20on%20the%20U.S.%20Electric%20Grid.pdf>

U.S. Department of Homeland Security (DHS). 2009. *Cyber Security Procurement Language for Control Systems*. Washington, D.C.: DHS Control Systems Security Program, National Cyber Security Division. https://www.cisa.gov/sites/default/files/2023-01/Procurement_Language_Rev4_100809_S508C.pdf.

Wang, Weikang, Kaiqi Sun, Chujie Zeng, Chang Chen, Wei Qiu, Shutang You, and Yilu Liu. 2021. “Information and Communication Infrastructures in Modern Wide-Area Systems.” In *Wide Area Power Systems Stability, Protection, and Security*, edited by Hassan Haes Alhelou, Almoataz Y. Abdelaziz, and Pierluigi Siano, 71–104. Power Systems. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-54275-7_3.

Appendix A. Cyber100 Compass Use Case

The following hypothetical use case provides an example of how an organization could use Cyber100 Compass to model cybersecurity risks as it integrates large amounts of distributed energy resources. This hypothetical use case is not intended to be comprehensive nor cover every event or condition that an organization might encounter; it is designed to illustrate how Cyber100 Compass could be used.

The situation: System A is a large, investor-owned utility serving more than 1 million customers and operating over a large geographic region in the state. The system has ambitious renewable energy transition targets (80%–90% renewable electricity and more than 65 GW of annual renewable energy capacity by 2050), with a target of achieving 40% overall renewable energy and an additional 30 GW of renewable energy capacity deployed by 2030. System A seeks to add numerous new options, including the following, some of which the utility will own and operate, but most will be owned and operated by third-party entities. System upgrades include:

- New large-scale solar and wind facilities
- Electric vehicle charging stations.

The problem: Given the large number of customers supported by System A, the board of directors are increasingly concerned about how their plans to restructure the grid into a system of systems (where the constituent systems are operating entities of the different renewable resources) will change the cyberattack surface of their future energy system.

The solution: System A's board of directors have tasked an employee, Gary, to use a new tool from the National Renewable Energy Laboratory—Cyber100 Compass—to understand and assess the cyber risks and mitigation strategies for their evolving energy system. Using Cyber100 Compass will enable System A staff to quantify the cybersecurity risks, and it will allow Gary to present those risks to the System A Board members, executive leadership, and external stakeholders so that decisions and corrective actions can be made prior to the transition.

Risk Tolerance

The utility has already evaluated the risk of cyberattacks associated with System A's information technology (IT) systems. The IT networks are regularly hit with phishing, ransomware, and similar attacks, and the utility has a good sense of how much System A spends on average each year to recover from these IT events. As the utility transitions to more distributed resources and increases automation on their energy system; however, the utility suspects that they are increasingly vulnerable to cyberattacks that could cause physical impacts, such as outages, harm to equipment, harm to employees, harm to the community, and denial of communications. These types of cyberattacks have not yet entered the utility's risk calculations.

Gary starts with the utility leadership (the board of directors and the senior executives). Gary and the chief risk officer begin a conversation with the operational technology (OT) security team, system planners, and other senior executives about risks from cyberattacks that cause physical impacts. The goal of this conversation is to determine which total annual costs are acceptable across a spectrum of cyberattack probabilities. As total costs increase, the acceptable probability of experiencing those costs decreases.

To formalize the decision, System A places a series of scenarios before all the stakeholders (including the senior executives). Each scenario includes a question. For instance:

Scenario 1: More than \$1,000

A cyberattack on OT systems results in physical impacts to the grid. The total cost to the organization, including lost revenue, recovery, etc., is more than \$1,000.

For this scenario, what is the acceptable probability that a cyberattack costing more than \$1,000 will occur in any given year? Please write the probability as a percentage between 0 and 100.

Scenario 2 is identical except that the cyberattack would cost System A more than \$10,000. Scenario 3 introduces a cyberattack costing more than \$100,000, and so on. The answers are summarized in Table A-1.

Table A-1. Example of Risk Tolerance Inputs

Total Costs From Attacks	More than \$1,000	More than \$10,000	More than \$100,000	More than \$1,000,000	More than \$10,000,000
Acceptable probability of cyberattacks costing this amount in any given year	95%	35%	15%	2%	0.1%

This enables System A to generate the risk tolerance curve shown in Figure A-1.

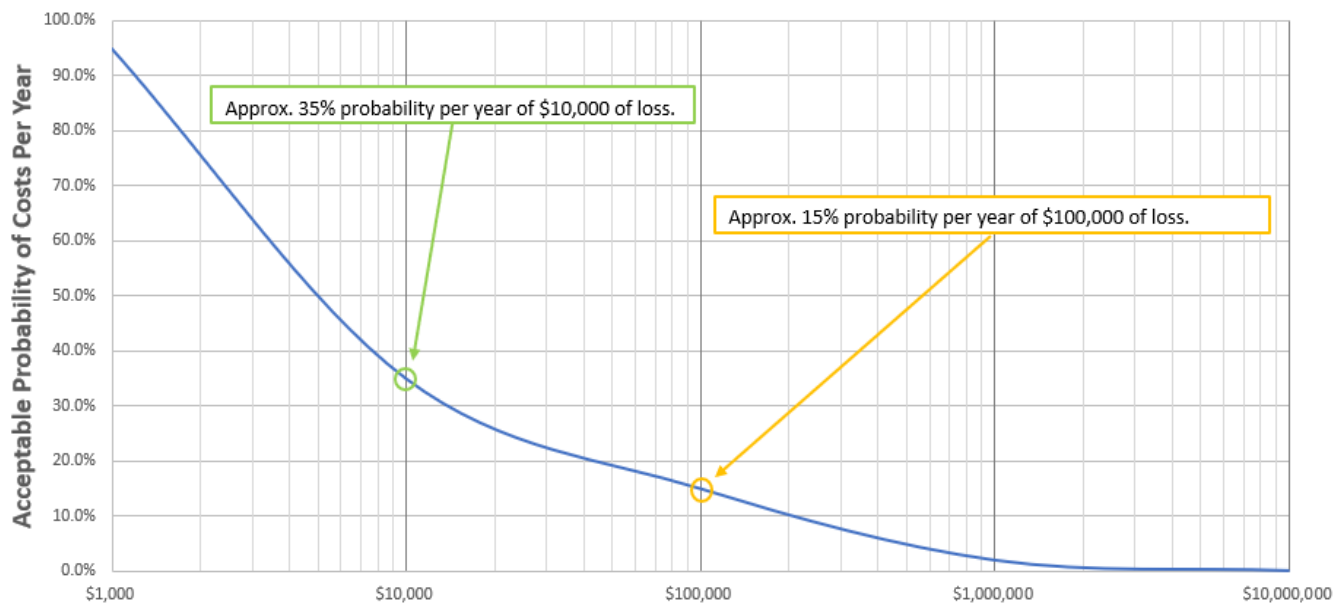


Figure A-1. Example Risk tolerance curve

The risk tolerance curve provides a probabilistic risk assessment that helps organizations quantify risk. For more information on risk tolerance curves and probabilistic risk assessment, see Chapter 3 of *How to Measure Anything in Cybersecurity Risk* (Greer et al. 2016).

Cyber100 Compass will use the values in this section (together with the input values in the next section) to create System A's expected loss curve.

Events

The next step is for System A to provide inputs into the events section. These inputs allow users to tell Cyber100 Compass the value placed on avoiding certain types of events that could be caused by a successful cyberattack. In the resilience space, these values are often called "avoided costs." System A is asked to provide the maximum avoided costs for events given certain constraints that define three levels of impact: low, moderate, and high.

To gather these maximum avoided costs, Gary meets with System A's finance and risk management committee. This committee was convened by the board of directors to manage overall risks in its clean energy transition and to oversee large capital investments, including those for new operating entities. Together, Gary helps the committee members identify the maximum avoided costs of the financial impacts that could occur based on the description of the cyber events and their levels of impact as described in Cyber100 Compass.

Conditions

The next step is for System A to select conditions that it expects to apply to its energy systems in the future and which will have an impact on cybersecurity.

For Cyber100 Compass purposes, conditions describe any constraints, resources, requirements, controls, or other factors that modify the cybersecurity risks of System A's energy transformation plans. To gather the necessary input information for Cyber100 Compass, Gary must meet with stakeholders internal System A stakeholders as well as external stakeholders.

For example, to gather information related to the regulatory environment, Gary sets up meetings with System A's government relations office to understand state-level policies that could be valuable resources for System A in case of a cyberattack. Several policy practices that are implemented in other states could come to System A's state in the future. Gary will discuss these future possibilities with the corporate governance team, which can then leverage their relationships with state legislators to discuss any potential critical infrastructure cybersecurity policies that might occur within the next 5 years.

Running Cyber100 Compass

Gary has now consulted with the appropriate stakeholders, gathered information on System A's current and future conditions, and input this information. Depending on the number of Monte Carlo simulations selected, running Cyber100 Compass takes at most a few minutes. Cyber100 Compass generates a report and visualizations that capture the risk calculations made based on Gary's inputs. Gary collects the reports and creates a cover page summarizing the findings for senior executive decision makers. Cyber100 Compass can be run multiple times to test various future scenarios and to adjust inputs as conversations with stakeholders evolve.

Conclusions

Cyber100 Compass has given Gary and System A an actionable and quantifiable risk assessment for their future energy system. System A is now able to make more informed and better decisions to ensure that the next stage of its energy system's evolution is designed with security in mind.

System A expects to use Cyber100 Compass again in approximately 5 years to quantify the risks involved with the following stage of upgrades (the next 5-year increment). At that time, System A expects that a new version of Cyber100 Compass will be available to provide even better risk insights.

Appendix B. Back-End Calculations

Part of the user input required by Cyber100 Compass is a maximum avoided cost value from each event and at each severity level. These user-generated maximum avoided costs are used to create the upper bounds of a 90% confidence interval on the loss values, which, in turn, are used to calculate the probability distribution parameters for the losses. For any event, suppose a user provides the upper bound costs UB_L , UB_M , and UB_H for the low-, moderate-, and high-severity losses, respectively. The lower bounds for these losses are generated by Cyber100 Compass. For low-severity losses, the lower bound is set as 1% of the user-provided low-severity upper bound. For moderate-severity losses, the lower bound is set to the low-severity upper bound. For high-severity losses, the lower bound is set to the moderate-severity upper bound. This process is demonstrated in Table B.1.

Table B-1. Demonstration of How Cyber100 Compass Turns User-Provided Upper Bounds on Loss Values Into Confidence Intervals for Loss Values

Severity Level	User-Provided Upper Bound	Cyber100 Compass-Generated Lower Bound	Cyber100 Compass-Generated Loss Interval
Low	UB_L	$0.01UB_L$	$[0.01UB_L, UB_L]$
Moderate	UB_M	UB_L	$[UB_L, UB_M]$
High	UB_H	UB_M	$[UB_M, UB_H]$

Monte Carlo Simulation

A Monte Carlo simulation is the process of repeatedly simulating the outcome of an uncertain event or process and then analyzing the outcomes in aggregate to draw inferences about the uncertain event or process (Shonkwiler and Mendivil 2009).

Reproducibility and Random Seeds

The results of a Monte Carlo simulation depend on stochasticity, or randomness, and generally involve the use of a random number generator or random draws from probability distributions. Due to this stochasticity, numerical results from a Monte Carlo simulation will be slightly different every time the simulation is executed unless a random seed is used to begin the simulation. A random seed tells the simulation code to use the same process to generate the random numbers every time the simulation is executed, meaning that Cyber100 Compass will generate the same random numbers and the results will be reproducible.

Cyber100 Compass sets a random seed by default and provides this value to users; the seed value can also be set or changed by users. This serves two purposes: The first is reproducibility of the simulation results, and the second is to allow users to iteratively adjust the conditions being applied and view the impact on the simulation results. By setting the random seed before changing conditions, all changes in the simulation results are due to the updated conditions rather than stochasticity.

Number of Rounds

There are no concrete rules for how many rounds to execute in a Monte Carlo simulation. Generally, more rounds will provide results that are more stable (vary less from one simulation

to another) and more representative of the underlying uncertain process. The upper limit of rounds that can be run tends to be determined by the computational time and resources available. Within Cyber100 Compass, 100 rounds are executed by default, and users can change this number if needed. The developers settled on 100 rounds after performing timed tests of the simulation and assessing the change in the overall simulation results as the number of rounds increased.

Probability Distributions

The procedure for determining the event occurrence, severity, and loss value involves several random draws from probability distributions. Event occurrence is modeled with a Bernoulli distribution (Bertsekas and Tsitsiklis 2008):

$$f_o(x; p_o) = \begin{cases} p_o & x = 1 \\ 1 - p_o & x = 0 \end{cases}$$

In this equation, f_o is the probability mass function of the Bernoulli distribution, and p_o is the probability that the event will occur. This probability mass function means that when the random draw, x , from this distribution is equal to 1, the event occurs, and in a single simulated year (one round of the simulation), the event occurs with probability p_o . The outcome of the random draw from a Bernoulli distribution can be thought of as a coin toss with unequal probabilities for the two sides of the coin.

Once an event occurs, a multinoulli, or categorical distribution, models the event severity level (low, moderate, or high) (Murphy 2012):

$$f_v(x = s | (p_L, p_M, p_H)) = p_s, \quad s = (L, M, H)$$

In this equation, f_v is the probability mass function of the multinoulli or categorical distribution; and p_L , p_M , and p_H are the probabilities that the event will be of low, moderate, or high severity, respectively. These probabilities must always sum to 1:

$$p_L + p_M + p_H = 1$$

This probability mass function means that once an event occurs, the random draw, x , from this distribution determines the event severity. The event is of low severity when $x = L$, which happens with probability p_L ; the event is of moderate severity when $x = M$, which happens with probability p_M ; and the event is of high severity when $x = H$, which happens with probability p_H . The outcome of the random draw from a categorical distribution can be thought of as drawing one of three differently colored items from a bag, with unequal probabilities of drawing each item.

After determining the event severity, the actual loss value from the event occurrence is simulated as a random draw from the lognormal distribution (NIST 2012a):

$$f_{loss}(x) = \frac{1}{x\sigma\sqrt{2\pi}} e^{-\frac{(\ln x - \mu)^2}{2\sigma^2}}$$

In this equation, f_{loss} is the probability density¹ function of the lognormal distribution, μ is the mean of the distribution, and σ is the standard deviation. The value of μ and σ are calculated by Cyber100 Compass from the user-provided upper bounds on loss values, which are used to generate 90% confidence intervals on loss values, as described. The equations for μ and σ at each severity level are given in Table B-1 (Geer et al. 2016).

Table B-2. Equations for Calculating the Mean and Standard Deviation of the Lognormal Distributions Used to Model Loss Values

Severity Level	Mean	Standard Deviation
Low	$\mu_L = \frac{\ln(0.01UB_L) + \ln UB_L}{2}$	$\sigma_L = \frac{\ln UB_L - \ln(0.01UB_L)}{3.28971}$
Moderate	$\mu_M = \frac{\ln UB_L + \ln UB_M}{2}$	$\sigma_M = \frac{\ln UB_M - \ln UB_L}{3.28971}$
High	$\mu_H = \frac{\ln UB_M + \ln UB_H}{2}$	$\sigma_H = \frac{\ln UB_H - \ln UB_M}{3.28971}$

Simulation Procedure

Each round of the Monte Carlo simulation represents 1 calendar year. Within a round, each event modeled in Cyber100 Compass is tested once to determine if it occurs; if the event does occur, then the severity level and corresponding loss value is determined. If the event does not occur, that event is not tested again until the next round of the simulation. Each event in Cyber100 Compass can thus occur at most once during one simulation round (representing 1 calendar year), at a single level of severity. Figure B.1 illustrates the overall simulation procedure.

¹ This is a probability *density* function because the lognormal distribution is continuous. The Bernoulli and multinoulli distributions are discrete— x can only take on certain predefined values—so they are represented with probability *mass* functions.

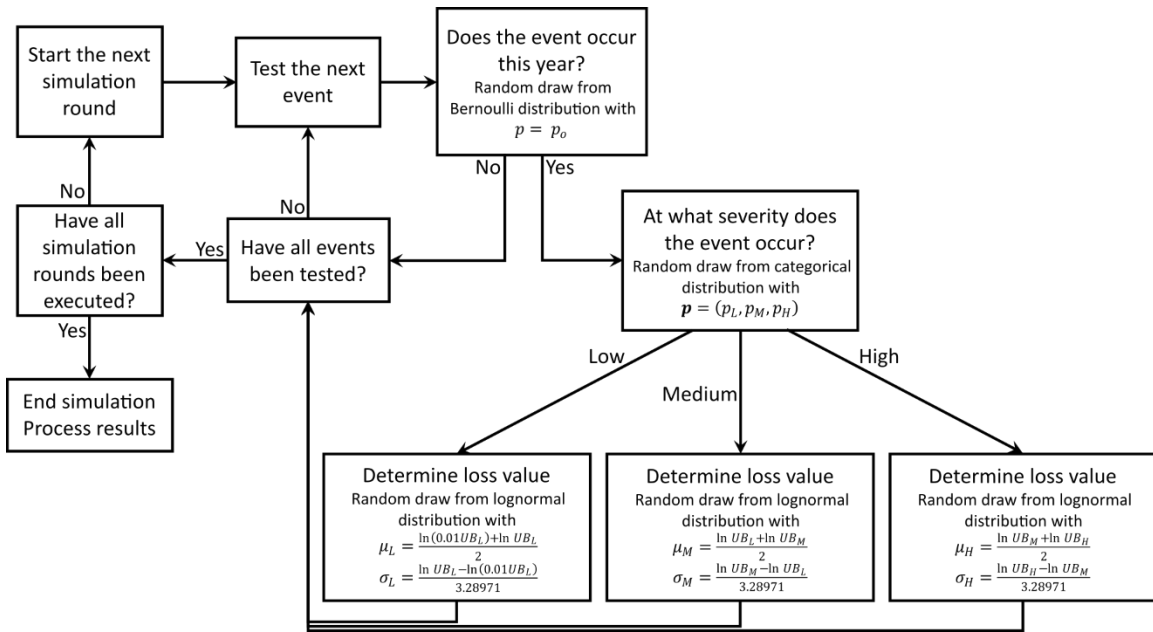


Figure B-1. Flowchart of the Monte Carlo event simulation procedure implemented in Cyber100 Compass