Distributed Energy Resource Visual Emulator: Phase 1

Shane McFly, Jordan Peterson, Ryan Cryar, and Tami Reynolds

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-5R00-84079
Revised February 2023

Distributed Energy Resource Visual Emulator: Phase 1

Shane McFly, Jordan Peterson, Ryan Cryar, and Tami Reynolds

National Renewable Energy Laboratory

Suggested Citation
McFly, Shane, Jordan Peterson, Ryan Cryar, and Tami Reynolds. 2023. *Distributed Energy Resource Visual Emulator: Phase 1*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5R00-84079. https://www.nrel.gov/docs/fy22osti/84079.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-5R00-84079
Revised February 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 U.S. Department of Energy Federal Energy Management Program. The views expressed herein do not necessarily represent the views of the DOE or the U.S. Government.

Errata

This report, originally published in January 2023, has been revised in February 2023 to include the name of the Distributed Energy Resource Visual Emulator.

Acknowledgments

The authors gratefully acknowledge Jason Koman, program manager at the U.S. Department of Energy Federal Energy Management Program, for his support in developing and enhancing the Distributed Energy Resource Cybersecurity Framework.

List of Acronyms

ADMS	Advanced Distribution Management System
ARIES	Advanced Research on Integrated Energy Systems
DER-CF	Distributed Energy Resource Cybersecurity Framework
JSON	JavaScript Object Notation
NREL	National Renewable Energy Laboratory
OCPP	Open Charge Point Protocol
TLS	Transport Layer Security

Table of Contents

List of Figures

1 Introduction

As with any critical energy infrastructure, distributed energy resource systems feature complex, data-driven communication networks that require careful system coordination and constant vigilance to ensure grid assets are secure. Because distributed energy resources are an important component of the decarbonization strategy, agencies need to secure energy data that could impact issues of national security if compromised.

To help federal energy managers assess, monitor, and manage cybersecurity while achieving decarbonization, the National Renewable Energy Laboratory's (NREL's) Distributed Energy Resource Cybersecurity Framework (DER-CF) offers a comprehensive, web-based assessment tool focusing on cyber governance or policies, technical management, and physical security. The DER-CF presents users with a series of pertinent cybersecurity questions, the answers to which are used to generate a site-specific report and recommendations.

Discussions among NREL researchers, DER-CF users, and other partners have shown that the DER-CF's site-specific reports and recommendations can overwhelm planners as they process the data into action plans; the sheer amount of data collected by the DER-CF and similar cybersecurity risk management tools can result in a sense of information overload. Without a contextualized frame of reference, categorizing this information by sections of the system or prioritizing various controls can be a guessing game. A comprehensive visual presentation of the wealth of information would enable decision makers to direct their efforts and budgets to action items with the largest and most immediate impact on improving the compliance of the system at large.

This paper outlines a plan to integrate the DER-CF with another key asset—NREL's Advanced Research on Integrated Energy Systems (ARIES) Cyber Range—to visualize cybersecurity resilience and compliance and to enhance the usability and accessibility of the DER-CF for federal facility energy managers and planners. This integration will result in a visualization environment to interpret and interact with compliance data.The new resource is called the Distributed Energy Resource Visual Emulator (DER-VE). Its development will include regular conversations with stakeholders to assess the effectiveness of these efforts, refine the visualization capability, and ensure its value to our partners.

The cyber range will be a useful contribution to the DER-CF as well as other possible tools discussed in this paper. It generates emulated, multilayer grid environments that allow researchers to visualize and evaluate the interdependencies of power systems and network communication flows and to safely explore vulnerabilities and mitigation effectiveness. This unique capability is helping researchers better understand how to improve the security, resilience, and black-start recovery of today's critical energy infrastructure.

NREL is establishing a niche in cybersecurity research for renewable energy systems, including redefining how cyber-physical threats are identified. With the development of the DER-VE, a revolutionary emulation platform for evaluating a wide variety of energy systems, researchers at NREL are making cybersecurity evaluation more visual, more tangible, more scalable, and more meaningful. Integrating the DER-CF and other tools with the cyber range will be transformative, allowing interactive visualizations of current and future cybersecurity scenarios for each site.

2 Cyber Range Emulation and Visualization

The ARIES Cyber Range allows researchers and partners to study energy systems' interaction with and dependence on digital communication devices and networks. NREL's unique energy systems modeling and co-simulation capabilities are the differentiating factors in realizing proven cybersecurity protocols for increasingly renewable and distributed energy systems. To match the complexity of modern, multilayer grids, the cyber range is designed to evaluate multi-owner power systems and visualize interdependencies with digital communication devices and networks.

The cyber range provides the ability to virtualize, emulate, and visualize energy systems subjected to energy disruption scenarios, with the fidelity needed to represent future energy and telecommunication systems—from individual devices to regional grids.

The cyber range enables powerful, interactive research, administration, and management front ends; adds a powerful visualization and demonstration capability; and provides a library of emulation tools, including component models, configuration scripts, and prebuilt prototype research environments. This world-class capability is designed to answer research questions at scale using virtual and physical assets by leveraging simulation, emulation, and power hardware-in-the-loop. Through the cyber range, NREL can emulate physical and communications-related aspects of distributed energy resources at scale to provide system-level security evaluation for bulk power renewables and distributed energy systems.

2.1 Visual Representation Details

The cyber range uses a custom, NREL-designed application to provide 3D, real-time presentations of system data for an interactive, at-a-glance understanding of an experiment. It also uses data visualization dashboards and can be customized to use open-source or enterprise security information and event management systems for a deep view of an entire energy system. This allows the experiment user to visualize simulated attacks for live visual verification that their tests are running correctly. Alongside system emulation, visualizations can provide insight into broader elements, such as the state of compliance with respect to established security plans and processes.

2.2 Representation of Policy Compliance

The cyber range allows the user to view a system wide illustration of compliance levels. The cyber range can create an emulated environment to demonstrate possible vulnerabilities associated with varying degrees of compliance. With minimal system information, the cyber range can illustrate generic compliance templates, reflecting low-, medium-, or high-compliance scenarios. With additional system information, a custom emulation can be generated.

The ARIES Cyber Range provides a detailed view of a system's compliance state through advanced emulation and power-communications co-simulation, the ability to connect to physical hardware in the lab, and the ability to visually demonstrate a system's performance with its 3D, multilayer visualization tool.

3 Phase 1 Project Objective

Phase 1 is the development and implementation of the plans created in Phase 0. There are three parts to this phase, which will be conducted in parallel. The first piece of Phase 1 is the DER-CF portal integration development. For this piece, a new page will be created in the DER-CF administrator portal for the internal creation of assets and capabilities for users to define their systems in review. The second piece of this phase is the static visualization development. Using the systems defined by the user and the questions answered in the DER-CF application, a static 2D visualization of the systems compliance is generated. The visualization will include color highlighting for levels of compliance as they apply to system components. The third piece of this phase is to design a compliance server within the ARIES Cyber Range that will facilitate the creation of representative or reference virtual architectures based on the user's system definition through the DER-CF application. This server will take in data from the DER-CF application along with asset information provided by the cyber range to orchestrate an interactive virtual environment with 3D visualization.

4 Technical Approach

4.1 Phase 0

Phase 0 of this project was concluded at the end of Fiscal Year 2021. This phase was primarily the planning phase of the DER-CF administrator portal, static visualization tool, and future integration of the ARIES Cyber Range. For full details on this phase, see https://www.nrel.gov/docs/fy22osti/82545.pdf.

4.2 Phase 1

Phase 1 has two primary deliverables: The first is the development of a working visualization of system compliance using the DER-CF, and the second is a plan for the design of a server application that takes input data from the DER-CF and creates a personal emulated environment of the user's system or a selected reference architect.

Major components that were developed in this phase are the DER-CF output, compliance visualization, data model, and compliance server design. The following subsections describe these components in greater detail. The expected flow of information for the Phase 1 use case is as follows: The user logs into the DER-CF application and defines the system assets and capabilities related to the evaluation. The user then answers the application questions as normal. Once these questions have been answered, the user can generate a visualization of their compliance using a custom or reference architecture. In Phase 2, this information will then be packaged and sent to the compliance server in the ARIES Cyber Range to generate an interactive virtual environment of their system or selected reference architecture.

4.2.1 DER-CF Output

There are two core sections of the DER-CF that form the framework for the final visualization output: the administrator core and the user core. These portions allow both NREL researchers and users to interact with the information, making the application dynamic. The administrator part of the application is where NREL researchers can modify the data within the application, which includes the assessment. It is within this part of the application that we are building out the ability for our researchers to identify two parts for a user to select: system assets and asset capabilities. Assets are system components of a facility, such as a wind turbine, and asset capabilities are security or communication protocol features that each asset possesses, such as Modbus or Transport Layer Security (TLS).

Asset capabilities are defined by the researcher and include configuration options that are also defined by the researcher. As such, TLS can be using version 1.2 or 1.3, which can change the state of compliance for the asset. Similarly, electric vehicle infrastructure relies on Open Charge Point Protocol (OCPP), which, depending on the version used, can also change the asset's compliance.

The compliance metric for each asset is computed by attaching questions from the assessment to the asset capabilities that are being defined. The corresponding configuration is then searched through the question list, and all the answers are aggregated for each asset. We then normalize the data by dividing the total score for the asset by the number of available answers, which then allows our color scale to be activated based on that normalized score.

The user core selects the assets and capabilities that are applicable to their facility based on the information (assets and capabilities) that is defined in the admin core. When the user has selected the capabilities for the assets, they will be presented with the configuration options for each capability that has been defined. These configurations directly map to the questions answered and allow the user to tailor their experience to what they have in their facilities. When all the assets, asset capabilities, and capability configurations have been defined, the user can transition to the visualization.

4.2.2 Visualization

The visualization is the static picture that is generated upon user request via the dashboard. The visualization is developed using open-source 3D models developed outside of NREL. The Three.js framework is then used to place the 3D models within the visualization and to assign their color based on their determined compliance state.

The visualization placement is based on the user selection for how the assets connect to each other from the user selection core page. These placements align with the connections between the elements but may not exactly represent the real-world system topology. The model prioritizes the connectivity between the elements rather than their exact geographical proximity.

The assets are represented from publicly available 3D object files, such as the wind turbine shown in Figure 1.

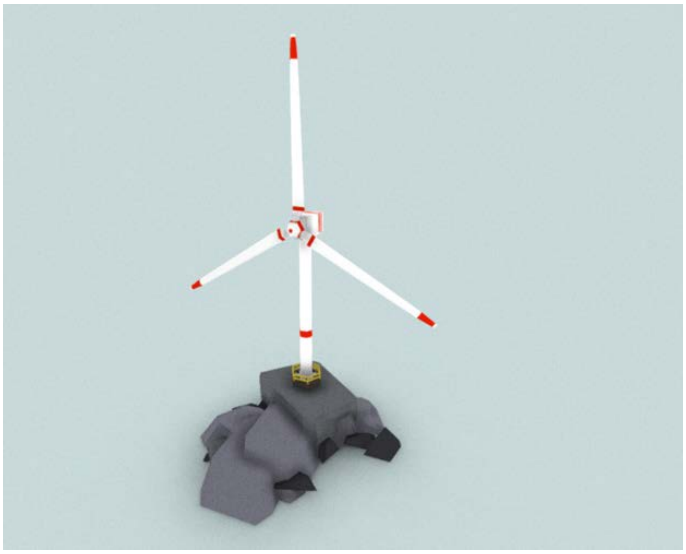

Figure 1. Example 3D asset

This object has been publicly listed as free to use and free to use in enterprise. This approach to adding objects from open-access 3D object libraries will allow us to model facilities at scale without having to design each asset ourselves if the asset already exists. These objects are loaded under a glTF loader and can be dynamically placed from a few lines of code.

These loaders are also publicly available from Three.js and serve as a dynamic and easy way to import 3D asset models into the scene and move them around. These visualized assets will have two parts: a circle that shows the compliance color above it and a connection line (if a

connection has been selected) to each asset that shows the connection. These will represent the compliance and connection states to the user, who can then click and drag their facility to view it more easily.

4.2.3 Data Model

A standard information schema needs to be defined for the compliance server that will be implemented and interfaced with DER-CF application in phase 2.

The server requires both compliance information and topology information to orchestrate a representative or custom Phenix research environment. All this information is organized in a single JavaScript Object Notation (JSON) file. An example is shown in Figure 2.

```
{
    "Systemname":"My System",
    "systemObjectTopology": [
        {
            "systemObjectName": "AMI 1",
            "uuid": 2345232,
            "interfaces" : [
                {
                    "interfaceName":"eth0",
                    "linksTo": 411431
                }
            ], "Services": [
                {
                "serviceName": "ssh",
                "port": 22,
                "config": {
                    "passwordAuth": "on",
                    "password": 12354,
                    "username": "root"
                    },
                "compliance": "red",
                "compliance_reason":"password authentication on with insecure password."
                },
                {
                    "serviceName": "http",
                    "port": "80",
                    "config": {},
                    "compliance":"red",
                    "compliance_reason": "use of http proctocol which is an insecure protocol."
                }
            ],
            "Overall_Compliance": "red"
        }
    ]
}
```

Figure 2. Example compliance and topology JSON file

The top-level object contains an identifier for the topology that has been modeled and a topology object listing each system within the topology. Each system within the topology has a name, universally unique identifier, interfaces, and services field. The name helps identify the system listed in a human-readable way. The universally unique identifier is used to map network connections between systems. The interfaces list each active interface on the system. Finally, the

services object lists each service running on the system. Each service running on the system has an identifier, port, and configuration field.

With this information gathered from the user about their topology, the server will be able to parse the JSON file and generate a representative or custom environment to best fit the provided topology.

The user might not want to—or, in some cases, cannot—provide the system details shown in Figure 2. In this case, the DER-CF application will provide a selection of representative architectures to better approximate the user's topology. This is handled by manually crafted JSON files to describe the representative architecture.

The data model also needs to provide compliance metrics to the server to correctly orchestrate the ARIES Cyber Range visualization to match the user's system compliance. The overall compliance of the system can be gathered from the "Overall_Compliance" field following the "Services" field. Within the "Services" object, there is a "compliance" and "compliance_reason" field. The compliance and overall compliance fields provide information needed by the visualization to draw the system/service in the correct compliance state. If the user wants to understand why a given service is in the compliance state shown, the "compliance_reason" field will provide a description.

4.2.4 Server Design

The server plays the intermediary between the cyber range and the DER-CF connection. As seen in Figure 3, the information that is generated in the DER-CF compliance metric will be sent to the cyber range front-end. That connection then passes the information to the server that lives within the cyber range's ecosystem. The server acts as a parser to set up the virtual machines and containers that the cyber range uses to visualize all system components.

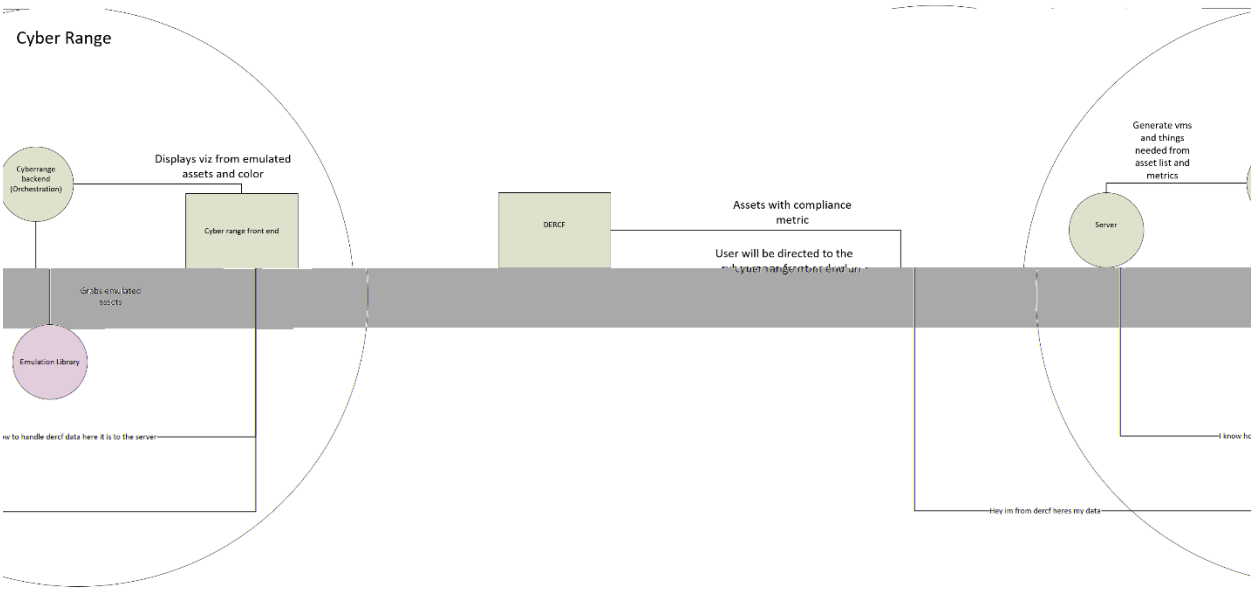

Figure 3. DER-CF to cyber range connection

As described in the server process flowchart, Figure 4, the server parses the compliance and topology information and reaches out to the emulation library maintained by NREL researchers to set up any emulated components in the experiment. The returned emulated components are then set up in the orchestration process, which creates the connections among all the components. All this information is then sent back to the front end of the cyber range application, which then displays all the information along with the compliance metric.

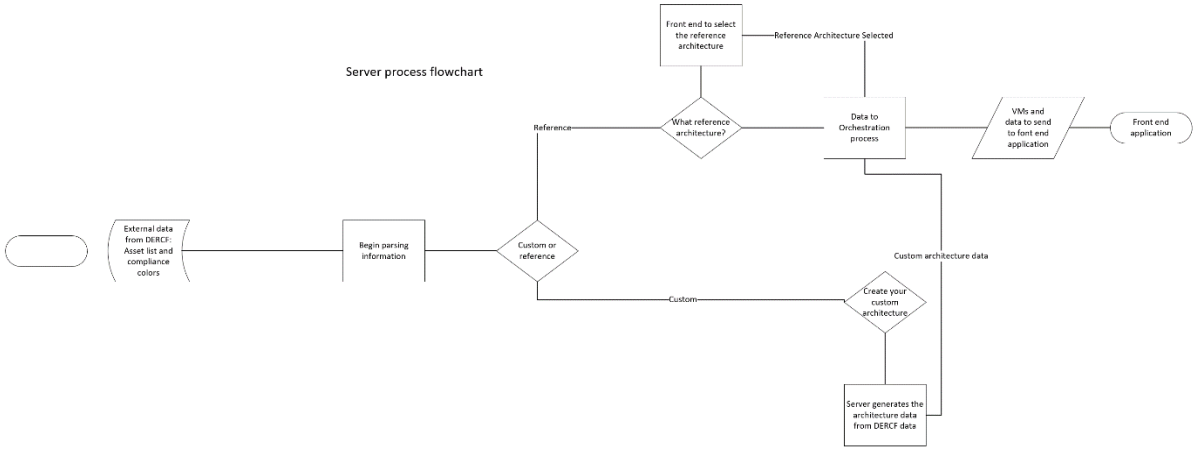

Figure 4. Server process flowchart

4.2.5 Partner Engagement

The U.S. Department of Agriculture Forest Service has been a long-term partner in the development and research of the DER-CF. In turn, they have been able to increase their cybersecurity posture of the advanced metering infrastructure through assessments within the DER-CF. With the integration work, they have supplied lists of meters and their configurations so that they could be the first to view their compliance visualization, and we had a use case to develop the integration.

The integration team has begun conversations with the National Aeronautics and Space Administration, the National Institute of Standards and Technology, and the U.S. Department of Defense (Navy) as potential stakeholder in this project and about providing feedback in phases 2, 3, and 4.

5 Next Steps

5.1 Phase 2

One main objective of Phase 2 is the development and deployment of the compliance server designed in Phase 1. Following the design, the compliance server will be custom programmed and hosted within the ARIES Cyber Range. The core functionality of this server is to take information provided by the DER-CF to build a representative emulation of the user's described system or a selected reference architecture. For example, one reference architecture would be a generalized organization of a solar array site's assets. It would include virtual components relevant to this use case, such as smart inverters, a few advanced metering infrastructure elements, battery charge controllers, and others. Each component would be networked together to represent a realistic topology. The architecture would also include any details related to services running on any of the components. The deployment of a predefined architecture like this can be quickly automated; however, the trade-off is that the virtualized system of components will not specifically match the user's site(s) they are evaluating. If opting for a custom representation of the user's system, key aspects of this emulated system will be influenced by the user's level of compliance. These include the defined services and their evaluated compliances per the DER-CF.

For the virtual environments to be automatically deployed, certain assets need to be developed or integrated into this new system. These assets include orchestration scripts for reference architectures and orchestration scripts for custom architectures. Other assets stored in the emulation library include virtual machines and configuration files for all interactive elements within the virtual environment. With these assets defined, generalized reference architectures will be created. Through these reference architectures, a templated environment of assets can be orchestrated in an automated fashion. Compliance information can then be mapped to these architectures. When the system is completed, a demonstration will be held to show the integration of the DER-CF with the cyber range.

A second objective of Phase 2 is broadening stakeholder engagement. Continuing conversations with the U.S. Department of Agriculture Forest Service, the National Aeronautics and Space Administration, the National Institute of Standards and Technology, and the U.S. Department of Defense (Navy) will help influence the functionality and usability of the service NREL is developing.

5.2 Phase 3

Phase 3 involves a significant increase in effort and scope. To increase the utility of this integrated capability, we propose that Phase 3 centers around the creation of a generalized reference architecture for federal systems. The idea would be to create a useful model for understanding compliance without the added expense and effort required to create a model of a specific system or architecture. This reference system would contain familiar elements in a relevant configuration in which a representative of a federal facility could apply aspects of their system. This would give them the opportunity to rapidly make changes and determine the effects of new policies on the general state of compliance of their system.

This capability would increase compliance awareness and lead to faster acquisition of authority to operate. Additionally, the potential would exist to create targeted training vignettes geared toward specific learning outcomes and increase the overall comprehension of compliance awareness and the authority-to-operate procedure.

Additional use cases for this architecture will include training vignettes targeting learning outcomes in the field of digital forensics and incidence response. The system could also be leveraged to provide cybersecurity training that extends offerings by Idaho National Laboratory to include distributed energy resources, fast-charging stations, renewable energy devices, and other future grid developments. The system could even be used to create and host research or training exercises (e.g., Liberty Eclipse) or to develop or augment existing cyber defense exercise (e.g., CyberForce Competition).

The process of designing and creating this architecture will require stakeholder feedback to ensure that the resulting system is sufficiently relevant to their use cases. Again, stakeholders would be needed to provide guidance on desirable learning outcomes in the creation of the training scenarios and to offer feedback and suggestions on the completed system.

5.3 Phase 4

Once the generalized reference architecture has been created in Phase 3, the system can then be scaled to include other NREL resources. Leveraging the resources of ARIES at NREL, the architecture can be extended to include high-performance computing, the Advanced Distribution Management System (ADMS) test bed, specific devices as hardware-in-the-loop, photovoltaic arrays, wind turbines, or the many resources at NREL's Flatirons Campus.

Through this integration, stakeholders can determine the effects of new technological solutions on their compliance stance and use real-world data to drive decision making. Leveraging this capability will allow them to greatly de-risk their posture as they look to integrate their systems into the future energy infrastructure and maintain compliance through their transition to the net-zero economy.