Resilience and Cybersecurity for Distribution Systems with Distributed Energy Resources

Baza Rodrigue SOMDA

Thesis submitted to the faculty of the Virginia Polytechnic Institute and State University

in partial fulfillment of the requirements for the degree of

Master of Science

In

Electrical Engineering

Chen-Ching Liu, Chair

Ali Mehrizi-Sani

Vassilis Kekatos

April 26, 2023

Blacksburg, Virginia

Keywords: Microgrid, Resilience, Cyber-Physical Systems, Digital Twins

Resilience and Cybersecurity for Distribution Systems with Distributed Energy Resources

Baza Rodrigue SOMDA

ABSTRACT

Heightened awareness of the impact of climate change has led to rapidly increasing penetration of renewable energy resources in electric energy distribution systems. Those distributed energy resources (DERs), mostly inverter-based, can act as resiliency sources for the grid but also introduce new control and stability challenges. In this thesis, a cyber-physical system (CPS) testbed is proposed combining a real-time electro-magnetic transient power system simulation and a practical model for communication network simulation. By regularly updating the CPS testbed with real-world SCADA information, a digital twin is effectively created. The digital twin allows the testing of novel microgrid control and cybersecurity strategies. Simulations using the Virginia Tech Electric Service (VTES) as a test case demonstrate the capability of adequately controlled resources, including solar PV, energy storage, and a synchronous generator, to enhance resilience by providing energy to critical loads. The DERs comply with IEEE disturbance ride-through requirements and switching transients are maintained within acceptable limits. A comprehensive DER-based resiliency plan is developed and validated for the Virginia Tech smart grid.

Resilience and Cybersecurity for Distribution Systems with Distributed Energy Resources

Baza Rodrigue SOMDA

GENERAL AUDIENCE ABSTRACT

In the last two decades, the increased occurrence of major power outages in the United States underscores the critical need to improve the reliability and resilience of the power grid. Massive investments have been made to install information and communications technology enabling near real-time monitoring and control of the smart grid. Simultaneously, heightened awareness of the impact of climate change led to rapidly increasing penetration of renewable energy resources at the distribution system level. Those distributed energy resources, mostly inverter-based, can act as resiliency sources for the grid but also introduce new control and stability challenges. In this work, a comprehensive testbed is proposed for the real-time simulation of both the power systems and communication networks. This method allows the testing of novel microgrid control and cybersecurity strategies. The testbed is used to develop and validate a resiliency plan for the Virginia Tech Electric Service using distributed energy resources.

Dedication

To my parents, Zieme Somda and Jeanne Soulama, for their unyielding support.

Acknowledgments

I would like to express my gratitude to my academic advisor Dr. Chen-Ching Liu for his constant support and motivation. His patience and encouragement always helped me get through difficult times.

I also appreciate and thank Dr. Virgilio A. Centeno for his guidance during my first year as a Master's student as well as Dr. Jaime De La Ree Lopez and Dr. Vassilis Kekatos for their challenging courses that deepened my interest in the field of power systems. Additionally, I would like to thank Dr. Ali Mehrizi-Sani for opportunities to demonstrate my RTDS work and obtain suggestions from knowledgeable visitors.

My fellow colleagues and friends at Power and Energy Center have been a family to me during these past few years. A very special thanks to Markus, Akshay, Ardavan, Vic, Chensen and Nitasha who gracefully shared their experiences with me and helped me find my way. I would also like to thank my siblings, Stephanie and Yann, as well as my girlfriend, Genervive, for their support.

Finally, I would like to acknowledge the Commonwealth Cyber Initiative (CCI), State of Virginia, for the support of this research through the project *"Learning the Attackers' Behavior for Defense of Smart Power Infrastructures."*

Table of Contents

Table of Figures

Chapter 1: Introduction

1.1 Motivation

The concept of reliability in distribution systems is well defined. It refers to the ability of a distribution system to reduce the occurrence and duration of power outages, and when they occur, to quickly take restorative actions that recover service to customers. Resiliency, however, is a relatively new requirement. In the case of distribution systems, resiliency is the ability to restore and maintain service to critical loads during and following a catastrophic event [1]. Low-probability high-impact events such as storms, floods, and earthquakes can cause cascading events that result in the loss of critical service. These critical services include water purification plants, gas plants for heating, hospitals; their loss can lead to significant safety hazards. Such an event occurred in Winter 2021 in Texas and caused numerous deaths due to freezing conditions [2]. These events can lead to severe economic losses. It is estimated that catastrophic events cause between 18 and 33 billion dollars of loss to the U.S. economy each year. Moreover, their impact is only expected to grow with the changing climate.

Due to their expansive nature, distribution systems are particularly affected by extreme weather events. In these situations, traditional restoration methods cannot be deployed because of the unavailability of power grid facilities caused by severe damages. It is thus imperative to improve the resilience of the power distribution networks. The resiliency of

a distribution system can be improved by using islanded microgrids (MG) and distributed energy resources to serve critical loads during extended outages. These DERs include synchronous generators, renewable energy sources (RES), and battery energy storage systems (BESS).

Traditional power systems are centralized in planning and operation. Electric energy generated in large-scale power plants is transported through a high voltage transmission system. The voltages are then gradually reduced in the sub-transmission and distribution system before the energy is delivered to the end users. With the increased awareness of climate change and its impact and the push for renewable energy integration, the centralized nature is rapidly changing. A large number of distributed energy resources are now being installed at the distribution level. To improve the reliability and resilience of the power system, major investments are made in the areas of monitoring and control. These investments resulted in the installation of information and communications technology (ICT) in the system [3]. ICT devices enable near-real time remote monitoring and control of the power system, referred to as a "smart grid." Unfortunately, the reliance on ICT devices opens the door for possible cyber insecurity. A power system with an extensive information and communication network is essentially a cyber-physical system. Attacks in the communication infrastructure (cyber layer) can lead to severe consequences causing damages in the physical system. This has been publicized for the first time in a real system during the cyber-attacks on Ukrainian distribution utilities in 2015 [4]. It is therefore crucial to develop defense mechanisms against coordinated cyber-attacks on the power system. Co-simulation environments integrating both the physical and cyber layers are needed for cyber-physical security analysis and resilience

planning. The goal of this thesis is to develop a digital twin of a distribution system that can be used for resiliency planning, DER integration studies, and analysis of cyber-vulnerability and mitigation.

1.2 Literature review

Widespread outages due to catastrophic events are characterized by numerous faults that affect multiple grid components and disable distribution substations for an extended period [5]. Based on these characteristics, possible approaches for the enhancement of distribution system resilience are proposed in references [1, 5, 6, 7]. The most common suggestions include the reinforcement or" hardening" of vulnerable components, regular maintenance of the facilities and components, and deployment of smart grid techniques. A smart and resilient grid is characterized by a high level of remote monitoring and automation, and the availability of distributed energy resources and microgrids as resiliency sources.

The benefits and challenges of using those microgrids as resiliency sources are highlighted in [8]. Microgrids can be used to sustain critical loads during an extended outage and accelerate the distribution restoration process by acting as black-start resources. The critical load restoration problem is to determine a sequence of switching events to pick up as many critical loads as possible while respecting operational, topological, and power flow constraints. More challenges are related to the low inertia of microgrids. Cold-load pickup, transformer energization, and other switching operations

cause transients that can potentially cause system instability.

Multiple strategies for critical load restoration using microgrids and distributed generators are proposed in the literature. Reference [9] introduces a graph-theoretic critical load restoration algorithm using a spanning tree search technique. This method ensures an optimal solution with minimum switching operations and restores as much load as possible without violating operational constraints. Reference [10] uses a mixed-integer linear programming formulation to solve the restoration problem while ensuring an equitable service time for the restored loads and minimizing the risk of post-restoration failures. In a recent study [11], the authors propose a generalized framework that supports both conventional restoration and microgrid-assisted restoration. Reference [12] proposes a two-stage approach that combines a graph-theoretic method to find possible post-restoration topologies and a mixed-integer semi-definite program formulation to maximize the critical loads to be restored. The loads are weighted based on their priority. Reference [13] proposes a two-objective chance-constrained method that accounts for the intermittence of renewable energy sources and load uncertainty. While these strategies are interesting, they are incomplete as they normally do not consider system dynamics and parallel operation of multiple microgrids or distributed generators.

In references [14, 15], the authors formulate critical load restoration as a multi-objective optimization problem that maximizes the number of critical loads restored weighted by priority level and minimizes the number of non-critical loads to energize while respecting topological, operational, and dynamic constraints. The formulation allows distributed generators to be operated in parallel. This is an improvement, but only synchronous

generators are modeled. Inverter-based resources have fast dynamics and therefore require further investigation.

The usage of microgrids and distributed generators for restoration and islanded operation also introduces control challenges that are not normally addressed by these strategies. The challenges include DER synchronization, frequency and voltage control, power sharing, and grid re-connection [16]. There is abundant ongoing research on microgrid control in grid-connected and islanded modes [17, 18, 19, 20]. In the context of critical load restoration, reference [21] implements a two-level microgrid control scheme. The primary control is based on droop characteristics and the secondary control is ensured by a feedback control-based microgrid controller. This control scheme ensures proper power dispatch and frequency/voltage regulation of the microgrid in a resiliency mode. However, all distributed energy sources are modeled as synchronous generators. Reference [22] demonstrates that the interaction between fast grid forming inverters and slow synchronous machines can cause instabilities. It is therefore important to include inverter-based resources in dynamic simulations.

Multiple real time co-simulation testbeds have been presented in the literature. Liu et al. present the modeling and real time simulation of a cyber-power system [23]. Their setup integrates a real time simulation of the IEEE 14-bus test feeder in RTDS and a corresponding network simulation using NS-3. The states of the system are collected using physical and simulated phasor measurement units (PMU) and control actions are performed using the information. The consequences of denial-of-service (DoS) and man-in-the-middle (MITM) attacks on the physical system are observed. Similarly, Chen et al. observed the behavior of transient stability of bus voltages under cyber-attacks [24]. The

physical system is modeled in RTDS, and the OPNET network simulator is used for the communication system.

1.3 Contributions

In this thesis, a comprehensive restoration procedure is proposed for the Virginia Tech Smart Grid composed of grid-forming and grid-following inverter-based resources as well as a synchronous generator. A complete sequence of actions is provided to restore critical loads using DGs during a catastrophic outage and reconnect to the grid when it becomes available. The contributions of this work are:

- A detailed model of the Virginia Tech Smart Grid for real-time dynamic simulation is created.
- A communication network of the Virginia Tech Electric Service is modeled in the NS-3 network simulator.
- Coordinated Direct Switching and Denial-of-Service cyberattacks are simulated to demonstrate their ability to cause extended outages.
- The DER control strategy is designed to handle both grid-connected and resiliency operation modes. It enables control of the sequence of events upon islanding, including the grid-forming operation of a battery energy storage system, synchronization, and coordination with a synchronous generator, connection with a grid-following PV inverter, and critical load pickup.
- Electro-magnetic transient simulations are conducted to evaluate the ability to regulate system frequency and voltage in steady-state operation and during

switching events.

1.4 Thesis organization

The remainder of this thesis is organized as follows:

- Chapter 2 gives a summary of distribution system resilience.
- Chapter 3 explores the design and architecture of the VT digital twin testbed.
- Chapter 4 provides the simulation cases and their results.
- The conclusion and future work are discussed in chapter 5.

Chapter 2: Concept of distribution system resilience

2.1 Reliability vs resilience

2.1.1 Concepts

Traditionally, distribution systems have been designed and operated according to the reliability principles of security and adequacy. Adequacy is the ability of the system to provide sufficient generation resources to meet the electrical demand of customers. Security is the system's ability to withstand sudden disturbances such as feeder short circuits or equipment failures. The reliability of the distribution system can thus be defined as its ability to avoid outages, and when they do occur, to quickly restore service. For that reason, the reliability of a distribution system is typically measured by the frequency and duration of power outages. The two most common reliability metrics are the System Average Interruption Duration Index (SAIDI) and the System Average Interruption Frequency Index (SAIFI). Temporary duration outages (less than 3 to 5 minutes) may not be included in the calculation of these indices. Typical outages involve single faults that occur on the power system infrastructure. The simple, localized events, coupled with the increasing presence of distribution automation devices, such as remote-controlled switches, make the damage assessment and restoration processes relatively straightforward. Therefore, current distribution systems are usually highly reliable based on these metrics[1].

Catastrophic outages are usually caused by natural disasters. These events result in multiple faults in the system, the loss of power generation units, and substantial damage to inter-dependent infrastructures (communication, transportation networks). The unavailability of generation units and the loss of remote-control capabilities greatly affect the repair and restoration process and can result in sustained outages. It is thus crucial to prepare the system for those low-probability, high-impact events. Resilience can be defined as the distribution system's ability to withstand and recover from rare and extreme events by sustaining electricity service to critical loads.

2.1.2 System performance curve

The conceptual system performance curve (Figure 1) is proposed in [25]. The curve outlines the response of a system to an extreme event. The resilience level of the system is qualitatively illustrated as a function of time. The main features required for an effective response to a disaster event are demonstrated. The event occurs at time t_e. Before the event, the system needs to be robust and resistant enough to absorb the initial shock. Immediately following the event, the system performance level, in terms of the MW served, is significantly degraded (R_0 to R_{pe}). Preventive methods and emergency strategies implemented before the event can help minimize its impact by limiting the loss of MW served ($R_0 - R_{pe}$). The system then enters the restorative or recovery state (t_r to t_{pr}). In this state, distribution restoration strategies are implemented to restore service using the available generation capacity. Availability of restorative generation capacity is thus a crucial requirement. In the post-restoration state (t_{pr} to t_{ir}), the system

performance level of the system R_{pr} is most likely lower than the pre-event level. This is due to potential damage to the grid infrastructure, including transmission, distribution and substation facilities. The availability and proper dispatch of repair field crew allow for a complete recovery at t_{pir}. The transition times between the states are also important parameters to consider. Based on the system performance curve, the resilience of the distribution system can be improved by:

- Reducing the initial degradation during the event ($R_0 - R_{pe}$).
- Ensuring a "slow and controlled" degradation (increase $[t_{pe} - t_e]$).
- Reducing the restoration time ($t_{pr} - t_r$).
- Improving the post-restoration resiliency level.
- Reducing the infrastructure recovery time ($t_{pir} - t_{pr}$).

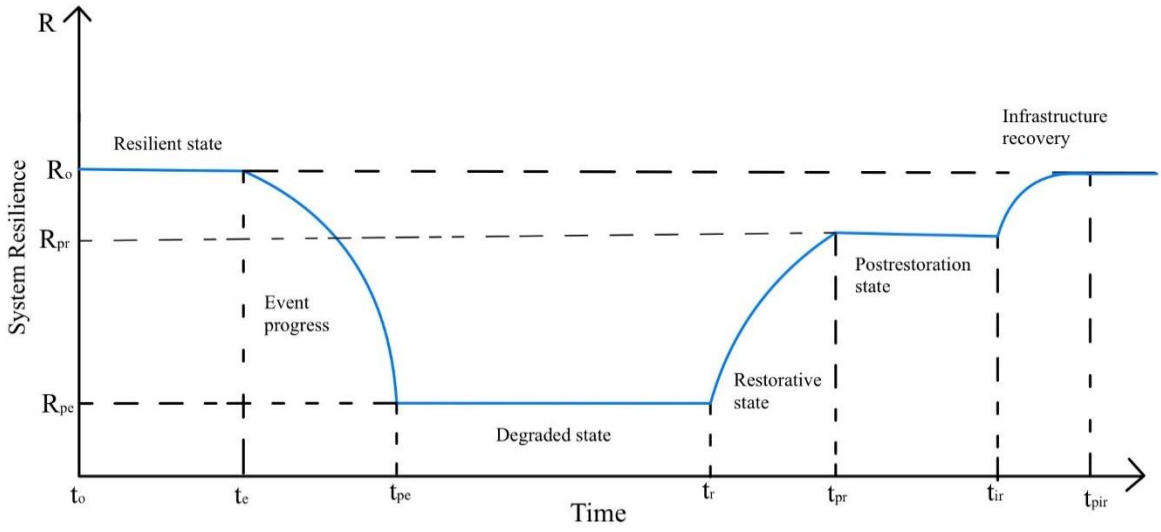


Figure 1: System performance curve associated with an extreme event.

2.2 Measures for resilience enhancement

Based on the conceptual resilience curve, measures are identified that can be adopted to improve the resilience of distribution systems.

2.2.1 Improvement of preparedness methods

Preparedness methods aim at reducing the magnitude and speed of the initial state degradation due to extreme events. Careful study and implementation of these methods can help achieve a relatively slow and controlled degradation and ultimately reduce the infrastructure recovery time after the event.

A. Extreme event impact prediction tools

Damage and outage forecasting tools can provide guidance for resilience programs. These tools are statistical or simulation-based models that rely on weather forecast parameters, environmental data, power system information and disaster scenarios to predict damages and outage duration [26]. They can also provide suggestions for hardening regarding vulnerable sections (or components) and restoration strategies. The impact prediction models can be made flexible and adaptable by learning from damage assessment performed following past disasters.

Unfortunately, difficulties in obtaining valid real-time data make their usage for short-term forecasting challenging. Additionally, statistical methods are very case-dependent because of their reliance on localized data and specific events. The large amount of

trusted information required to build realistic and accurate models prevents their use for predictions. In addition to accurate forecasting, models are needed for a realistic cost-benefit analysis of suggested hardening investments.

B. Construction programs

Hardening refers to the action of physically changing the infrastructure to reduce its susceptibility to damages caused by extreme conditions. Distribution system resilience can be improved by enhancing current designs and adopting more rigorous construction standards. This is a necessary part of the general approach to system resilience [27]. Multiple hardening suggestions have been made and some of the best practices have been identified. For example, structural reinforcements such as adding guy wires, applying hydrophobic coating to conductors, and using steel poles are effective ways to "harden" overhead lines. The elevation of substations and vulnerable components is an important part of flooding protection in susceptible zones. Another popular suggestion is the replacement of overhead distribution lines with underground cables, which are less vulnerable to weather-related damages. This is referred to as "undergrounding."

The main issue with these hardening measures, especially undergrounding, is their prohibitive cost. For example, for the same distance and voltage level, the construction of underground lines can be four (4) to fourteen (14) times more expensive than overhead lines [26]. In addition, the topic of undergrounding, despite seeming like an intuitive solution, can be controversial. In fact, while underground lines can reduce outage frequency, the difficulty in reaching them often leads to longer repair times. It is therefore

crucial to adopt a selective approach to hardening. These measures can be implemented on specific components after a cost-benefit analysis that accounts for failure probability, proximity to critical loads, estimated repair time, and other relevant metrics. The identification of those components or sections can be the output of aforementioned prediction tools, or optimization models based on past performance of the components.

C.Maintenance programs

The proactive identification of devices with a high chance of failure or close to their expected lifetime is an important part of resilience enhancement. Regular inspection and maintenance schedules help identify and replace those vulnerable components [5]. Modern maintenance approaches also ensure that expensive assets safely reach or even exceed their design life. Those practices include online temperature monitoring, thermal imaging, partial discharge monitoring and the installation of intelligent protective devices [26]. Functional abnormalities can be detected and corrected at an early stage. Keeping a safe clearance between trees and overhead lines reduces the chance of contact during storms. Tree trimming remains the primary vegetation management method near distribution lines.

2.2.2 Improvement of restoration methods

A. Distribution automation

Distribution automation is enabled by the adoption of smart grid techniques. The smart grid infrastructure improves the observability, controllability, and operational flexibility of the distribution system. The improved monitoring and control capabilities allow distribution operators to efficiently coordinate the response to disasters as they happen. The Smart Grid Investment Grant (SGIG) by the U.S. Department of Energy supported the installation of many remotely controlled switches (RCS) in the distribution system. These automated switches enhance the topological flexibility of the system. They allow operators to perform feeder reconfiguration actions in a timely manner, reducing the restoration time and the number of affected customers [5]. The advanced metering infrastructure (AMI) is also an important element of a resilient distribution system. Smart meters have a “last gasp” feature allowing them to automatically report outages. Operators can thus have real-time outage information without relying on customer “trouble calls.” They can also check the success of the restoration actions. The deployment of smart grid devices led to the development of integrated distribution management systems (IDMS). IDMS applications rely on typical SCADA, distribution management as well as the outage management systems. One of those applications is fault location, isolation, and service restoration (FLISR). By integrating automated devices, FLISR enables the implementation of restoration strategies with minimal manual effort.

There are a few challenges related to distribution automation. The expansive nature of distribution systems makes the complete adoption of RCS impractical due to their cost. Methods have been proposed that maximize system restoration capability with an optimal number of remote-controlled switches [27]. The quality and availability of communication networks during extreme events is another challenge faced by utilities deploying advanced distribution automation. Most systems rely on centralized restoration methods that require high communication bandwidths. In these cases, the central controller becomes a single- point of failure. Resilient distribution systems must adopt decentralized service restoration strategies. Decentralized methods based on multi-agent coordination have been proposed [28]. Finally, because of their reliance on information and communications technology, distribution systems are cyber-physical systems in nature. Several cybersecurity vulnerabilities have been identified in smart distribution systems [29]. Cyberattacks can have disastrous consequences on the physical grid. Resilient distribution systems of the future must adopt improved cybersecurity strategies.

B. Deployment of microgrids

After a disaster causes a power outage, the main objective of distribution operators is to quickly restore service to critical loads and minimize the impact to customers. Generation availability is a major issue when dealing with restoration during and after extreme events. The deployment of distributed energy resources (DERs) managed as part of microgrids is a promising solution to the unavailability problem. A microgrid is a group of distributed energy resources and loads located within clear electrical boundaries. From

the point of view of a utility grid, the microgrid acts as a single controllable entity. It is important to distinguish microgrids from a typical emergency power supply system (EPSS). A conventional EPSS generally serves a single building and cannot be operated in parallel with the utility system [9]. Their generators may have a high downtime, making their operation inefficient.

A microgrid can operate in a grid-connected mode in normal conditions or in an islanded mode during an outage. As such, microgrids help serve critical loads during extreme outages. Microgrids can have the added advantage of distributed and diverse generation resources. The distributed nature of DERs reduces the probability of damage (unavailability) during extreme events. As explained in [30], microgrid sources can be hardened and placed at adequate locations to reduce their chance of failure. Additionally, damages due to natural disasters tend to be unevenly distributed. It is possible to encounter zones with little damage right next to heavily damaged areas. The chances that most DERs are impacted are therefore relatively low.

Microgrids typically contain multiple types of DERs. They can be renewable sources such as photovoltaic (PV) and/or wind turbines, diesel generators and battery energy storage systems (BESS). Diesel generators rely on “lifelines” such fuel supply to operate continuously during extreme events. However, transportation networks may be affected by disasters, potentially interrupting supply lines. Integrating a mix of DERs can therefore reduce the distribution system’s dependence on other critical infrastructures. Through the added redundancy and decentralization, microgrids improve the overall readiness of the distribution infrastructure.

With the combination of controllable loads and grid-connected operation, ancillary services can be developed to improve microgrid generation efficiency and offset operation costs. For example, microgrid owners can be compensated by shedding internal load or selling power to the utility during peak hours and producing reactive power to support feeder voltage control. Nevertheless, the integration of microgrids creates operational and regulatory challenges that will be explored further in the next section.

2.3 Microgrids as a resiliency source

A. Metric for resiliency enhancement due to microgrids

Because of the multi-dimensional nature of the concept of resilience, it is difficult to quantify resilience enhancements. Multiple metrics have been proposed, often focusing on specific aspects of resilience. Some of those metrics are based on "the degree of robustness to the initial shock, the duration of the post-event recovery or the functionality achieved during the event" [2]. In this work, a resilience criterion proposed in [11] is adopted to quantify the resilience enhancement due to microgrid-based restoration strategies. In their work, Gao et al. specify the system performance function ($F(t)$) described in Figure 1 as the total amount of electric energy delivered to critical loads weighted by their priority at time t.

From the system performance curve, it is observed that the main contribution of microgrids occurs during the restorative and post-restoration states (t_r to t_{ir}). t_{ir} is typically unknown. However, based on historical data or forecasting tools, it is possible

to generate an estimated outage duration T^O. It is thus assumed that utility power restoration and infrastructure recovery start at $t_{ir} = t_r + T^O$. The resilience (R) is computed as the integral of the system performance function over the restoration period. From its definition, the system performance function can be written as:

$$F(t) = \sum_{c \in C} W_c \cdot P_c(t), \quad t \in [t_r, t_r + T^O]$$

Where c is a critical load belonging to the set $\boldsymbol{C}$ of critical loads restored by a microgrid. The priority of critical load c is represented by the weight W_c and its active power demand at time t is $P_c(t)$. The system resilience can therefore be specified as:

$$R = \int_{t_r}^{t_r + T^O} F(t)dt$$

$$= \int_{t_r}^{t_r + T^O} \sum_{c \in C} W_c \cdot P_c(t)dt$$

$$R = \sum_{c \in C} W_c \cdot \int_{t_r}^{t_r + T^O} P_c(t)dt$$

Due to limited reserves (fuel reserves for diesel generators or state of charge for battery energy storage systems), the microgrid may not be available for the entire outage duration. The maximum duration for which the microgrid can serve the critical load c is specified as T_c^R. When the intermittence of renewable energy resources and the uncertainty of load demands are considered, T_c^R becomes a random variable. When

restored by a microgrid, i.e., for $t \in [t_r, t_r + T_c^R]$, the active power demand by critical c is equal to its nominal active power demand $P_c^N(t)$. If the reserves are exhausted before utility power restoration, i.e., $t \in [\, t_r + T_c^R, T^O \,]$, the critical load can no longer be served and $P_c(t) = 0$. The resilience equation can therefore be rewritten as follows:

$$R = \sum_{c \in C} W_c \cdot \int_{t_r}^{t_r + T_c^R} P_c^N(t)\, dt$$

$$R = \sum_{c \in C} W_c \cdot P_c^N \cdot T_c^R$$

The resilience criterion can thus be defined as the weighted sum of the energy supplied by a microgrid to critical loads during the restoration and post-restorative states. This criterion can be used in the planning stage to compare different microgrid-based restoration strategies or evaluate the resilience improvement that can be achieved by adding new DERs into an existing system.

B. Critical load restoration

Microgrids can support critical load restoration by acting as a local resource or a community resource. When working as a local resource, a microgrid is used to supply energy to the critical loads within its own boundaries. The microgrid is a community resource when it also provides excess energy to the essential loads of a nearby distribution feeder or microgrid (wheeling). Multiple studies have explored the formation of microgrids in a disaster scenario [31]. In a long-term resiliency plan, optimally sized

and located DERs can be used to transform an existing distribution system into a microgrid for the duration of the extreme event. For example, individual inverter-based DERs (e.g., BESS) can operate in a grid-following mode in normal conditions and switch to a grid-forming mode to support critical loads when an outage occurs. Optimal paths can be determined in advance, hardened, and fitted with RCSs to minimize the risk of damage and facilitate feeder reconfiguration. Microgrids can also be formed dynamically in response to the damage sustained during a disaster. In this case, algorithms are devised for real-time network reconfiguration of microgrids. These algorithms propose graph-theoretic, multi-agent or master-slave approaches to generate microgrids using an optimal number of switching (reduction of restoration time) and ensuring energy adequacy (improvement of availability). This approach, sometimes called self-healing, can be used to improve the survivability of a microgrid created in the long-term resiliency plan. Dynamic microgrid formation typically results in the creation of multiple autonomous microgrids. In cases where the microgrids are in close proximity, resiliency may be further improved by forming clusters: this is referred to as networked microgrid formation. Networking (power sharing) ensures system stability, generation availability and cost-effective operation. It is important to note that new regulatory frameworks that facilitate wheeling need to be established to allow the usage of microgrids as community resources.

C. Black start resource

In the event of a large-scale outage, some generation units have the capability to start-up independently and begin the restoration process. These plants, usually hydroelectric or combustion turbine units, are called black start units. Large fossil generating units typically do not have a black start capability. Microgrids can act as black start resources by providing the power necessary to energize a transmission line and start the auxiliary units for a non-black start generation plant [9]. These auxiliary units include air handlers, pulverizers, conveyors, and pumps. The energization of long transmission lines requires the ability to absorb large amounts of reactive power. Because of their relatively low rating, microgrids have a limited capability to absorb reactive power. Therefore, microgrids are more suitable to assist the start-up of a nearby non-black start unit.

2.4 Operational issues due to microgrid integration

The usage of microgrids as a resiliency source poses several challenges that may affect the operational reliability of the restored portions of the system.

- **Uncertainty of generation, demand, and reserves:** For environmental reasons, the bulk of the generation units within microgrids is expected to be based on renewable energy resources. Wind and photovoltaic power are highly intermittent, making those resources non-dispatchable. In addition, power consumption patterns are variable and difficult to predict. This problem is compounded by the cold load pickup phenomenon during the restoration process. Furthermore,

thermal distributed generators rely on fuel reserves (and supply) for continuous operation. Fuel reserves may be depleted at the time of a disaster or supply routes may be interrupted, resulting in an increase of the restoration time. While a Battery Energy Storage System (BESS) does not rely on external "lifelines," improper management of their state of charge (SOC) may result in sub-optimal usefulness during an extreme event.

- **Frequency and voltage regulation in an islanded operation:** In a grid-connected mode, a microgrid operates in parallel with a large distribution system. The utility system acts as a strong voltage source with a large rotational inertia, which dampens the overall system dynamics. In an islanded mode, however, the microgrid must rely on its distributed generators for frequency and voltage regulation. The relatively small size of the generators and the high penetration of "low-inertia" inverter-based resources limit the microgrid's ability to prevent large frequency and voltage swings during disturbances. These disturbances include switching events (e.g., load pickup/shedding, line energization) and temporary faults. Energizing a relatively heavy load in a microgrid may cause the unintentional tripping of under-frequency or under-voltage protection relays. To study these issues, dynamic simulations of microgrids are needed. Electromagnetic transient (EMT) simulations using accurate unbalanced system dynamic models (the distribution system is unbalanced) are typically conducted. The simulations are used to evaluate the impact of switching operations on the system's transients and electro-mechanical dynamics. Based on the results of the

simulation, a restoration plan with an optimal sequence of switching events can be constructed.

- **In-rush currents and reactive power management:** The energization of transformers and lightly loaded lines (especially underground cables) causes transient current surges called in-rush currents. In-rush currents can be large enough to cause significant frequency and voltage deviations. The transformer energization in-rush can be managed by adopting a soft energization process which involves slowly ramping the voltage to its nominal value. In the case of lightly loaded cables and long transmission lines, relatively large amounts of reactive power can also be generated. The low power rating of distributed generators limits their capacity to absorb reactive power, which may cause voltage swells and instabilities. These problems are particularly significant when using microgrids as black-start resources. Solutions may include the decomposition of the black start process into multiple stages. Dynamics simulations can be used to determine the appropriate sequence of operations.
- **Grid interconnection and coordination of DGs:** To avoid the possibility of cascading failures, IEEE standard 1547-2018 assigns disturbance ride-through performance requirements for DGs interconnected with the grid. In addition, the parallel operation of multiples DGs in an islanded mode requires coordinated controls. The varying line impedance between the DGs can lead to a mismatch in their terminal voltage and cause circulating currents. Robust and adaptive microgrid control strategies are needed to ensure the proper operation of microgrids in both grid-connected and islanded modes.

- **Protection coordination:** The deployment of microgrids raises protection challenges. Because of the bidirectional current flow in multi-generator microgrids, typical overcurrent protection schemes do not work as intended. Furthermore, inverter-based resources produce a limited level of fault current (1.1~1.5 pu). Those fault currents are difficult to distinguish from normal overload currents. Due to their ability to operate in grid-connected and islanded modes, protection schemes for microgrids must be capable of functioning effectively at different fault current levels. Multiple adaptive, differential or traveling wave protection schemes have been proposed in the literature [32].

Chapter 3: Virginia tech digital twin and resiliency plan

3.1 The VTES distribution system

The Virginia Tech Electric Service (VTES) distribution system (Figure 2) serves a peak load of about 60 MW across the Virginia Tech Main Campus and customers in the town of Blacksburg. The campus electrical network is composed of 3 substations, 26 feeders and 31 nodes. There is currently no specific resiliency plan for the system. To reach Virginia Tech's climate action goal of 100% renewable electricity by 2030, the installation of distributed energy resources is required. The deployment of these DERs represents an opportunity for VTES to develop and implement a microgrid-based resiliency plan. The proposed DERs for this study are as follows:

- A 10 MW battery energy storage system
- A 2 MW photovoltaic plant
- A 5 MW conventional synchronous generator.

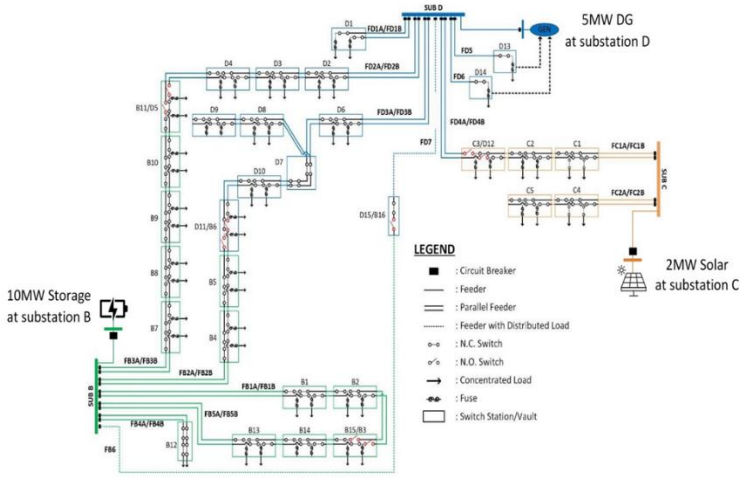


Figure 2: One-line diagram of the VTES system with planned DERs

3.2 The Virginia Tech digital twin

3.2.1 Motivation for building a digital twin (DT)

Cyber physical electric power distribution systems are often exposed to multiple threats. Extreme weather events are a leading cause of power outages. It is estimated that over 80% of outages between 2003 and 2012 were due to weather [33] and the majority of them affected distribution systems. In addition, physical attacks on the distribution system are causing damages. According to the U.S. Department of Energy electric disturbance event report, at least 101 incidents of vandalism, intentional attacks or threats occurred between January and August 2022 [34]. Finally, the ubiquity of ICT devices in the grid has caused an expansion of the attack surface of CPSs. Cyber-attacks and cyber-security breaches have become a serious threat for the power grids. Resilience enhancement of distribution systems is thus essential to prevent disruptions of the electricity service. Due to their limited generation and energy storage resources to enhance resilience, small utilities and campus distribution systems can be vulnerable to these events. To meet these challenges, the DT acts as a comprehensive testbed for resilience planning, cybersecurity testing, and short-term decision support. Operating a distribution system in an islanded mode as a microgrid requires the integration of control, protection, and cyber-security technologies. Managing the complex interactions among these systems has been challenging and the large-scale integration of inverter-based resources (IBRs) has not been explored in depth. For instance, fault currents are reduced by IBRs which requires a rethinking of the protection strategy that traditionally relies on high fault currents to detect and trigger protective devices. A technically sound and

feasible methodology validated via detailed modeling and simulation is critical before renewable energy and storage technologies can be deployed. Analytical studies typically rely on a static model of the distribution system to analyze the impact of planned design and implementation. Such models may not be accurate, as these are created using limited data that does not reflect the real-time variations of the distribution system. Through a collaborative research effort between VTES and Virginia Tech's Power and Energy Center (PEC), a data link has been established to allow online data to be transferred from VTES's grid assets to PEC's cyber-power laboratory (Figure 3).

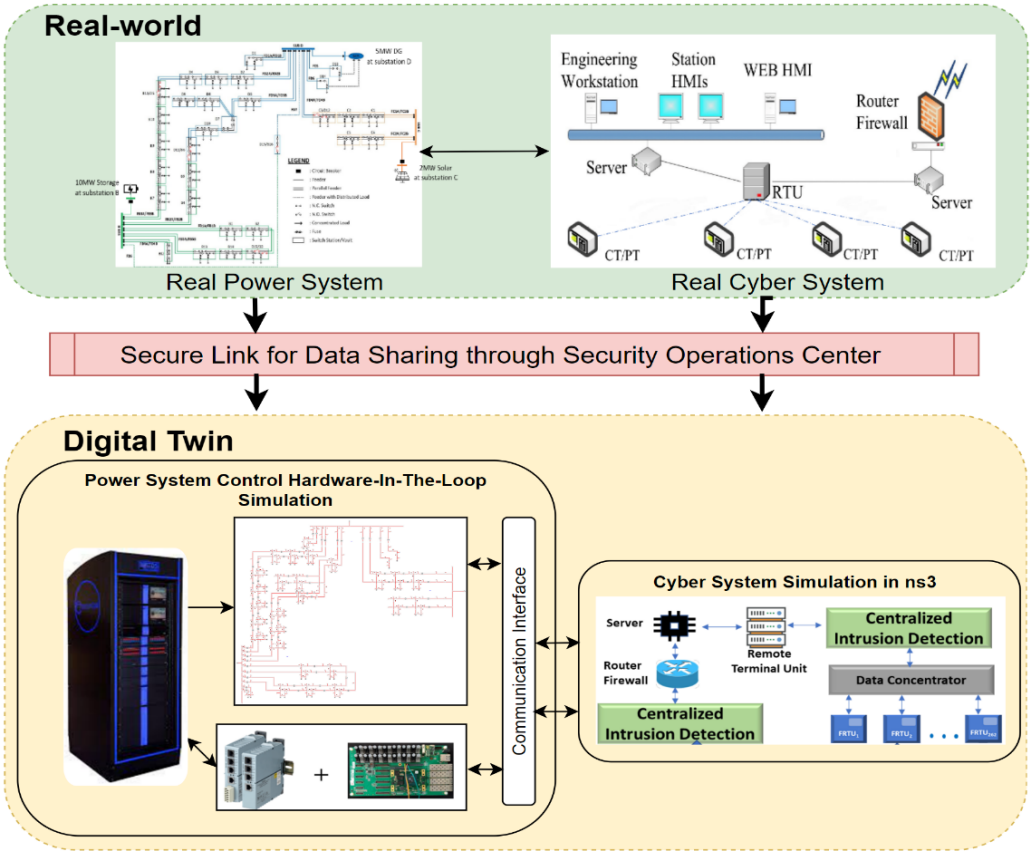


Figure 3: Architecture of VT digital twin

3.2.2 Virginia Tech digital twin

A typical digital twin consists of five main components: the physical system, the virtual system, a connection, real-time data, and services. At Virginia Tech, the physical part is the VTES campus electricity infrastructure, a 60 MW distribution system serving the university campus and part of the City of Blacksburg. The DT is modeled in a real-time digital simulator (RTDS). The virtual system is a cyber-physical system (CPS) co-simulation of the distribution system and communication networks as shown in Figure 3. A detailed Electromagnetic Transient (EMT) model of VTES has been constructed within the RTDS. The model is created using information about the generation resources, network topology, line parameters, and loading of the system. Power flow analysis is used for the validation of the model. The RTDS allows the study of the transient behavior of the VTES system when subjected to disturbances, especially when inverter-based resources are incorporated. A cyber network of VTES is modeled using the NS-3 network simulator. Due to its open-source nature as well as its modularity, NS-3 can readily be used for other digital twin projects. The secure data link implemented at the Power and Energy Center (PEC) enables access to the real-time data collected by sensors and measurement devices installed in the physical system. The cyber-security of the data link is a major issue due to the confidentiality and sensitivity of the transferred data. In collaboration with the Virginia Tech Office of Export and Secure Research Compliance (OESRC), several security measures have been implemented for the datalink. For instance, a secure room is designated with a one-directional communication link from the VTES operating center. Additionally, mandatory cybersecurity training is required for all personnel (student, faculty, or staff) with access to the digital twin

3.3 Detailed description of the cyber-power simulation testbed

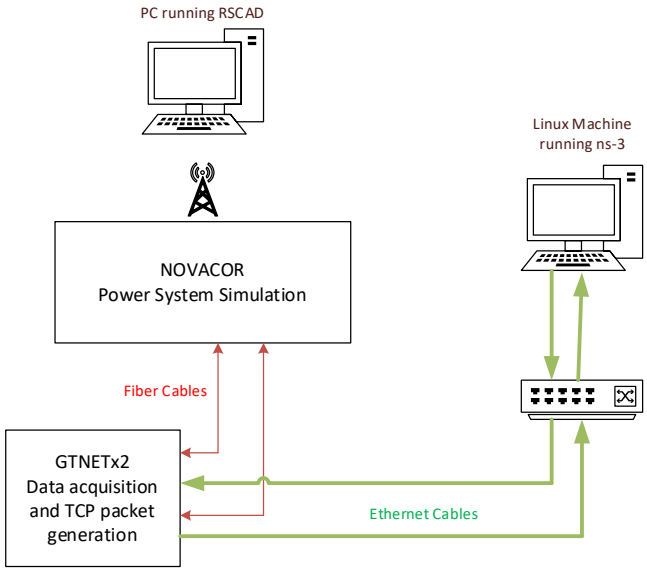


Figure 4: Diagram of the cyber-power simulation testbed

3.3.1 Components of the testbed

The proposed testbed is composed of the following components (Figure 4):

- A laptop running the RSCAD graphical user interface for power and control system modeling.
- The RTDS hardware (NOVACOR chassis) that runs the real-time power system simulation.
- The GTNETx2 chassis serves as a communication interface between the power system simulation and the network simulation.
- An Ethernet network switch is used to create a local area network containing all the devices within the testbed.
- A Linux machine running the NS-3 network simulator.

Each of these components will be described in detail in the following sections.

3.3.2 Physical power system layer

The physical power system is simulated using the Real Time Digital Simulator (RTDS) (Figure 2). RTDS is a tool widely used for real time electromagnetic transient (EMT) simulations of the power system. In EMT simulations a network solution algorithm is performed at each time-step to compute all the node voltages and branch currents of the power system. The system is simulated in discrete time with a fixed 50 μS time-step when no switching devices are included. Switching devices (e.g., power electronics converters) can be modeled and simulated with a time-step as low as 500 nanoseconds using the substep environment. The large number of points computed within a cycle (~16 milliseconds) allows the simulation to appropriately approximate the continuous time power system. The RTDS hardware available at the Virginia Tech Power and Energy Center (PEC) is composed of three (3) racks (or chassis) interconnected by a Global Bus Hub (GBH) through fiber optic cables. This hardware allows us to simulate systems with a maximum of two hundred and thirty-four (234) single-phase buses (78 three-phase buses) in a cross-rack simulation. The RSCAD graphical user interface provided with RTDS can be used to model and simulate the dynamics of both power and control systems components. RSCAD, running on a Windows laptop, gives the user the option to use the standard dynamic models included or create user-defined models.

i. Synchronous generator model

The synchronous generator is modeled using standard RTDS dynamic models for synchronous machines, excitation system, governor/turbine and power system stabilizer (Figure 5). The standard dynamic models are described in detail in the RSCAD power systems components user manual.

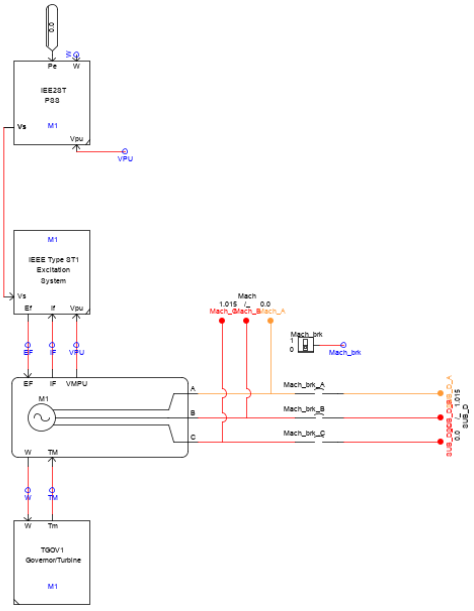


Figure 5: RSCAD model of synchronous machine with attached control components

ii. BESS model

The battery cells are modeled using standard RSCAD Li-Ion battery models (Figure 6). Average value models of DC/AC inverters are used for interfacing the BESS with the rest of the grid. The inverter control loops are adapted from reference [35].

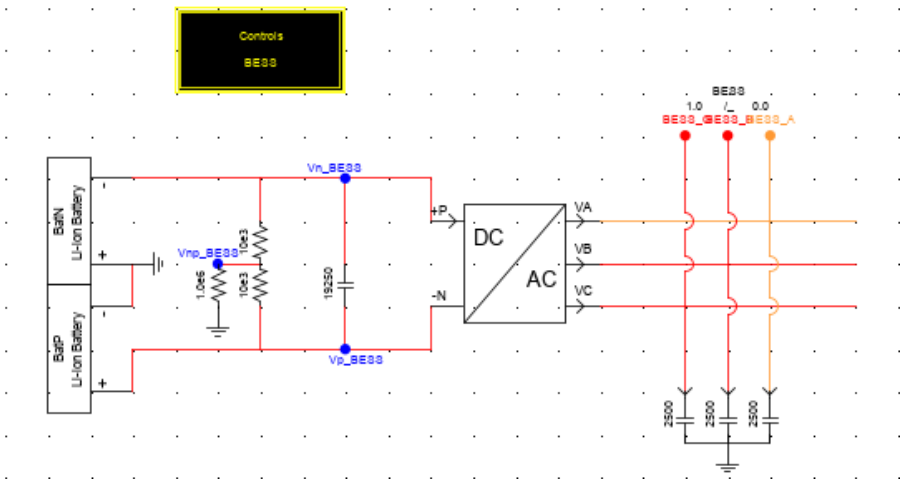


Figure 6: RSCAD model of BESS and Average Value Model DC/AC inverter

The BESS inverter can operate in a grid-connected mode using a Phase Locked Loop (Figure 7) to obtain the reference frequency and voltage angle by measuring the grid side voltage. In this grid following control mode, the user can control the real and reactive power (P/Q) injected by the BESS (using a closed-loop current controller shown in Figure 8).

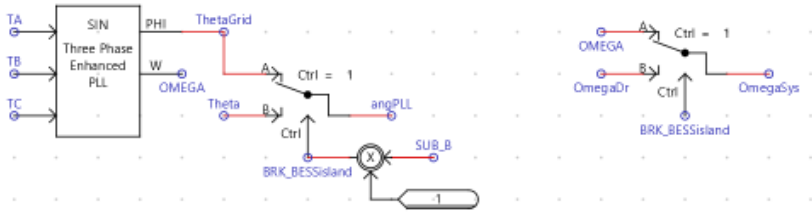


Figure 7: Model of Phased-Locked-Loop (PLL) with the option to switch to islanded mode (BESS only)

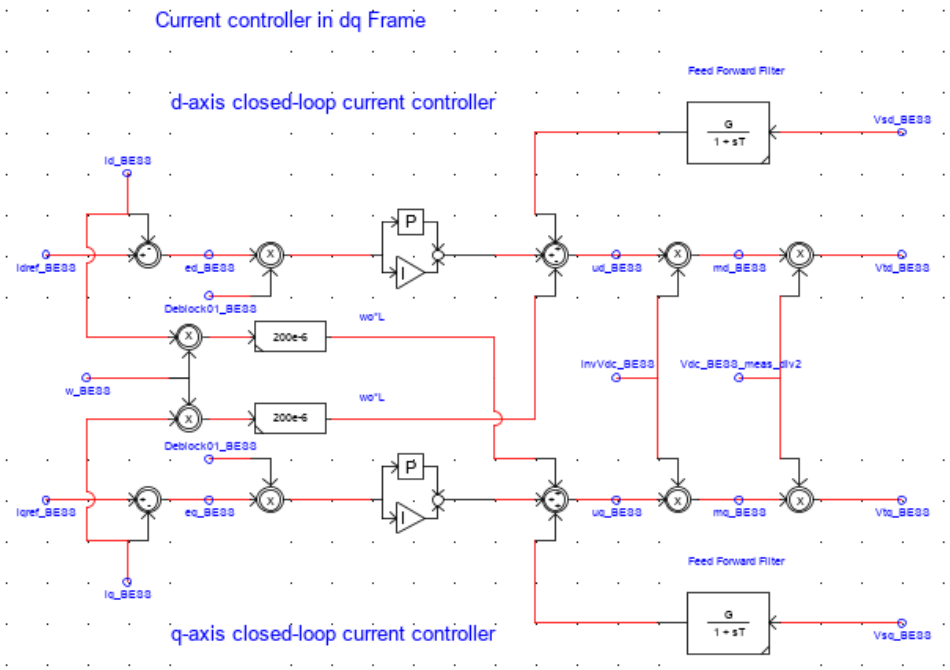


Figure 8: DQ frame inner current control loop for BESS in grid-following mode

When operating in an islanded mode, the inverter switches to the grid-forming control mode by using conventional P-ω/Q-V droop characteristics (Figure 9). In this mode, the user can directly control the reference voltage and frequency of the inverter.

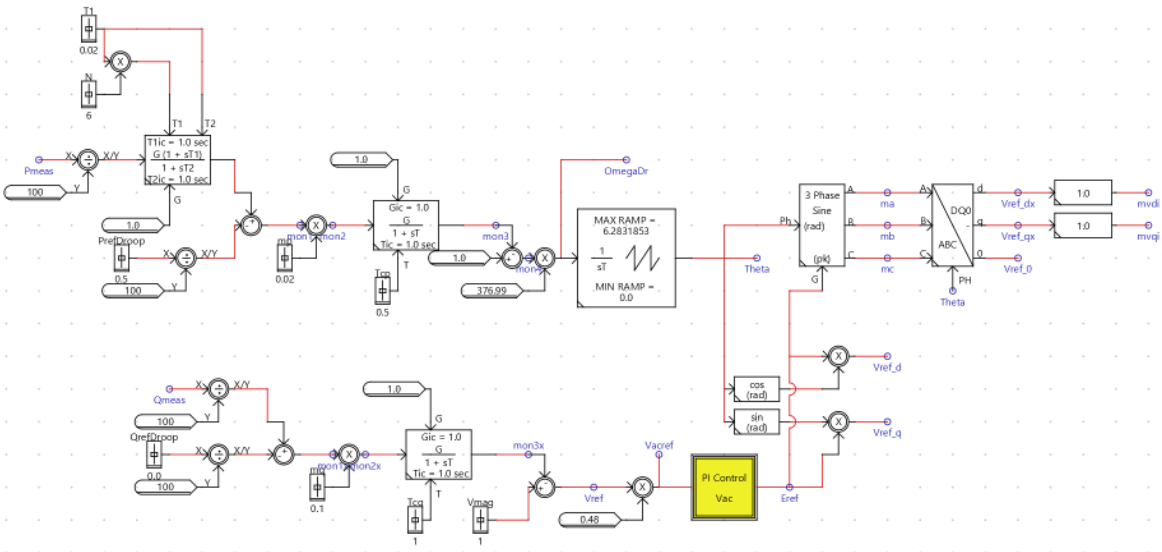


Figure 9: P-ω and Q-V droop control diagram for BESS in Grid-forming mode

iii. PV plant model

The PV plant is modeled using standard RSCAD solar panel dynamic models (Figure 10). These models offer the option to use Maximum Power Point Tracking. The solar plant can therefore inject the maximum power available at a given temperature and insolation level. Because of the intermittent solar resource, it is desirable to always extract as much power as possible. Grid forming control, which requires available reserves, is therefore not implemented in this case. The solar plant only operates in a grid following mode using a PLL and closed-loop current controller (Figure 11).

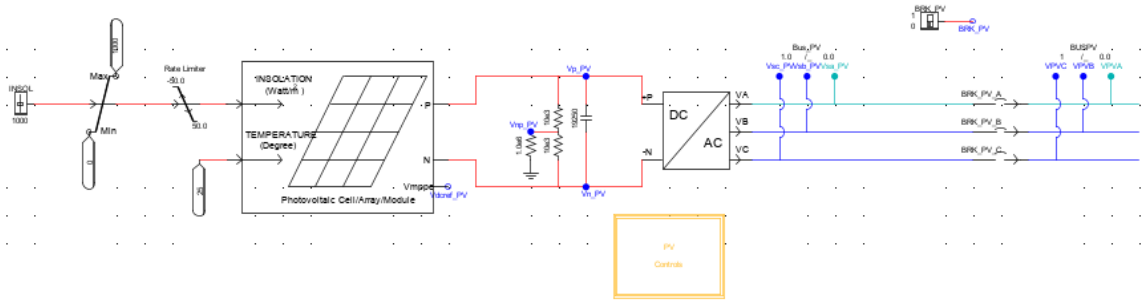


Figure 10: RSCAD model of PV plant and AVM DC/AC inverter

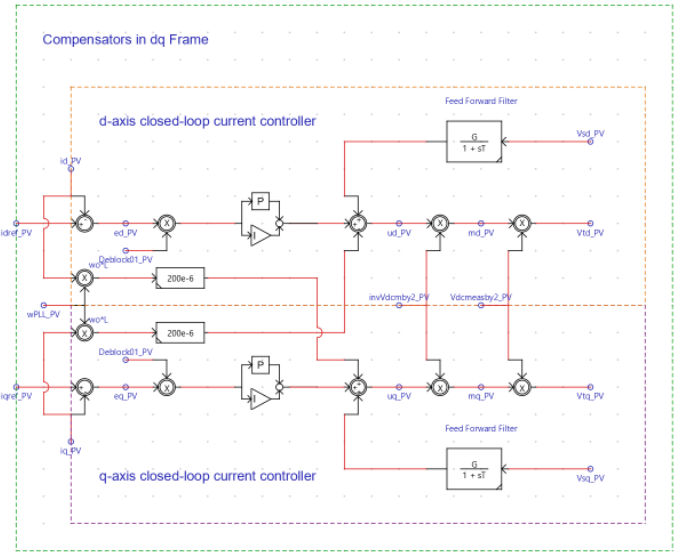


Figure 11: DQ frame current control loop for grid-following PV inverter

3.3.3 Communication interface (GTNET)

The RTDS hardware is equipped with a GTNETx2 card that acts as communication interface for external devices. The GTNETx2 card is a bi-directional protocol converter. Data from the RTDS can be enveloped into packets and transferred to the LAN where the destination devices can receive them (IP addresses need to be specified). In the other direction, the GTNETx2 card extracts data from packets sent by external devices and sends the payload to the appropriate RTDS processors. The GTNETx2 is connected to the RTDS through fiber optic cables and to the LAN network switch via Ethernet cables. GTNETx2 supports multiple protocols including, but not limited to, IEC-61850, DNP3, PMU, MODBUS, and Socket (SKT). The UDP Socket communication is used in this work. Each GTNETx2 chassis can simultaneously simulate two network protocols or communication channels, thus allowing for bi-directional transfers with low congestion risks. Figure 12 shows the configuration panels of the GTNET modules. IP addresses, a subnet mask, and a gateway address are assigned to all the communicating devices (e.g., automated switches). These addresses match the ones assigned to the devices within the NS-3 simulation.

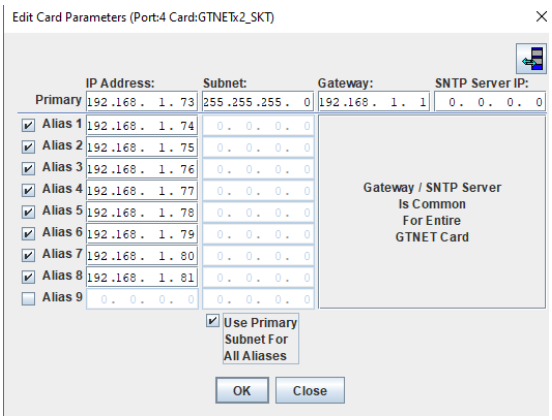


Figure 12: Screenshot of IP address assignment in GTNET

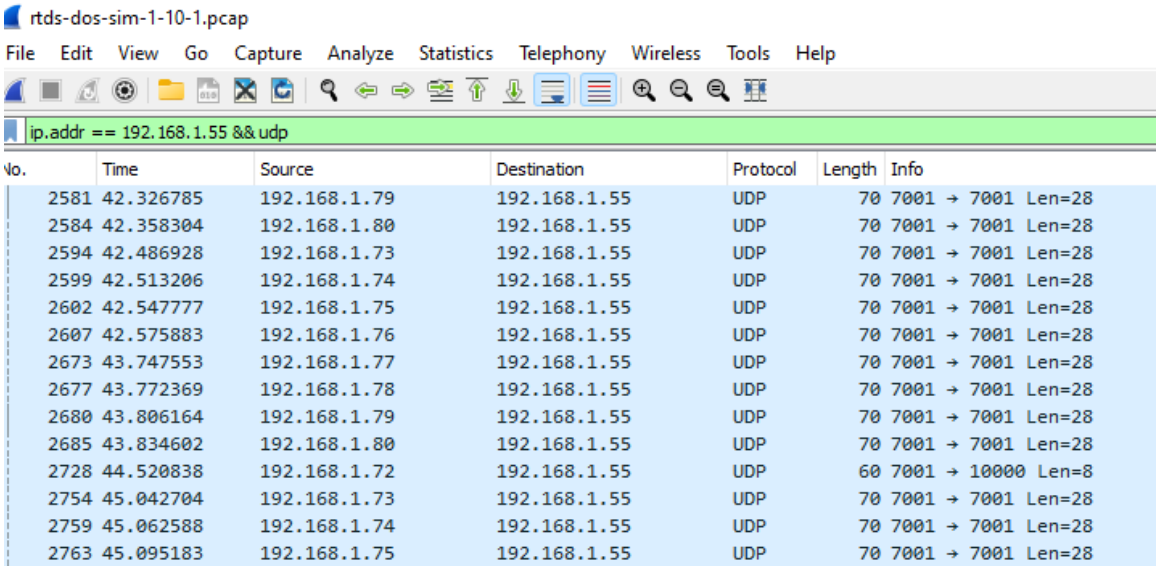
3.3.4 Communication (cyber) layer

The cyber layer is modeled and simulated in NS-3. NS-3 is an open-source, discrete event network simulator. The NS-3 source code is built on a Linux virtual machine (using Oracle VM VirtualBox) with two network interface cards (2 ethernet ports in this case). The ingress port transfers the measurement packets from the RTDS to the simulated network. The egress port transfers the packets that exit the network back into the RTDS. The ability of NS-3 to accurately simulate or emulate communication networks allows for detailed study and replication of cybersecurity events. When interfaced with a power system simulator, the impact of those cyber events on the physical system can be monitored and appropriate defense mechanisms can be developed. The protocols simulated in NS-3 are close to their real-world implementation. Furthermore, the data packets generated within the simulation are real data packets, which facilitates the integration with external hardware. Typical communication networks can be represented by a point-to-point star topology or a mesh topology. The star topology enables a single-hop communication between a source and a destination device. The mesh topology requires the data generated at a source to traverse multiple nodes (multi-hop) before reaching their destination. The point-to-point topology can have a prohibitive cost for large networks due to the number of devices required. However, for small distribution networks or microgrid devices connected as a Local Area Network (LAN), the star topology is a good option (using a network switch). Each LAN can then be connected in a meshed topology to other LANs through their gateways (usually a router). In this work, the network components with communication features are modeled as nodes in NS-3. Each node is assigned an individual IP (Internet Protocol) address and MAC (Media

Access Control) address. For the devices within a LAN, the connection with the network switch is represented by a CSMA link, which is a close approximation to a real-world ethernet cable link.

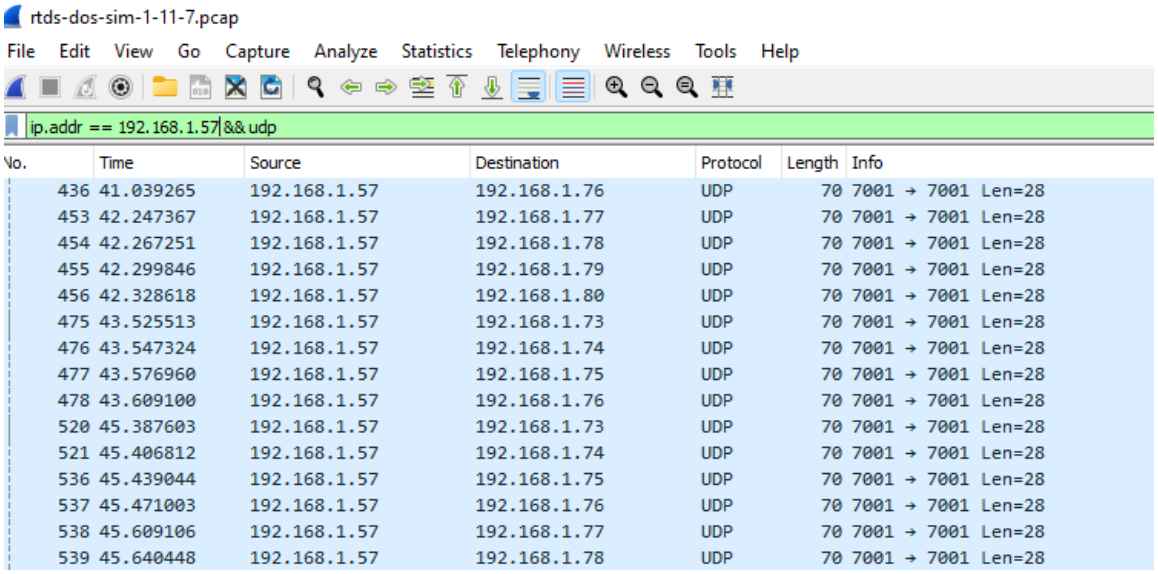
UDP socket communication (part of TCP/IP protocol suite) is used as the transport layer protocol for all connections. The initial plan for this work was to implement TCP socket communication. However, a TCP connection requires a “client” computer to initiate a conversation with the “server” computer. A server cannot typically initiate a connection with the client. This feature limits the ability for bidirectional communication. UDP communication allows direct bidirectional communication between the devices, which simplifies the implementation.

In the simulation, all devices are modeled as nodes. The nodes contain interfaces for communication (called NetDevice abstractions). The packets received by each node are processed following a queuing policy. The First-In-First-Out (FIFO) policy is implemented in this project using the ns-3 FifoQueueDisc class. The queuing discipline requires a buffer size which represents the maximum number of packets that can be held in the queue. When the buffer is full, incoming packets are dropped. The software Wireshark is used to verify the health of the communication between the NS-3 simulation and the GTNET interface by capturing packets sent back and forth (Figure 13 and Figure 14).



No.	Time	Source	Destination	Protocol	Length	Info
2581	42.326785	192.168.1.79	192.168.1.55	UDP	70	7001 → 7001 Len=28
2584	42.358304	192.168.1.80	192.168.1.55	UDP	70	7001 → 7001 Len=28
2594	42.486928	192.168.1.73	192.168.1.55	UDP	70	7001 → 7001 Len=28
2599	42.513206	192.168.1.74	192.168.1.55	UDP	70	7001 → 7001 Len=28
2602	42.547777	192.168.1.75	192.168.1.55	UDP	70	7001 → 7001 Len=28
2607	42.575883	192.168.1.76	192.168.1.55	UDP	70	7001 → 7001 Len=28
2673	43.747553	192.168.1.77	192.168.1.55	UDP	70	7001 → 7001 Len=28
2677	43.772369	192.168.1.78	192.168.1.55	UDP	70	7001 → 7001 Len=28
2680	43.806164	192.168.1.79	192.168.1.55	UDP	70	7001 → 7001 Len=28
2685	43.834602	192.168.1.80	192.168.1.55	UDP	70	7001 → 7001 Len=28
2728	44.520838	192.168.1.72	192.168.1.55	UDP	60	7001 → 10000 Len=8
2754	45.042704	192.168.1.73	192.168.1.55	UDP	70	7001 → 7001 Len=28
2759	45.062588	192.168.1.74	192.168.1.55	UDP	70	7001 → 7001 Len=28
2763	45.095183	192.168.1.75	192.168.1.55	UDP	70	7001 → 7001 Len=28

Figure 13: Wireshark capture of packets from RTDS simulation to NS-3 simulation ingress port



No.	Time	Source	Destination	Protocol	Length	Info
436	41.039265	192.168.1.57	192.168.1.76	UDP	70	7001 → 7001 Len=28
453	42.247367	192.168.1.57	192.168.1.77	UDP	70	7001 → 7001 Len=28
454	42.267251	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28
455	42.299846	192.168.1.57	192.168.1.79	UDP	70	7001 → 7001 Len=28
456	42.328618	192.168.1.57	192.168.1.80	UDP	70	7001 → 7001 Len=28
475	43.525513	192.168.1.57	192.168.1.73	UDP	70	7001 → 7001 Len=28
476	43.547324	192.168.1.57	192.168.1.74	UDP	70	7001 → 7001 Len=28
477	43.576960	192.168.1.57	192.168.1.75	UDP	70	7001 → 7001 Len=28
478	43.609100	192.168.1.57	192.168.1.76	UDP	70	7001 → 7001 Len=28
520	45.387603	192.168.1.57	192.168.1.73	UDP	70	7001 → 7001 Len=28
521	45.406812	192.168.1.57	192.168.1.74	UDP	70	7001 → 7001 Len=28
536	45.439044	192.168.1.57	192.168.1.75	UDP	70	7001 → 7001 Len=28
537	45.471003	192.168.1.57	192.168.1.76	UDP	70	7001 → 7001 Len=28
538	45.609106	192.168.1.57	192.168.1.77	UDP	70	7001 → 7001 Len=28
539	45.640448	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28

Figure 14: Wireshark capture of packets from NS-3 simulation egress port to RTDS simulation

3.4 Denial-of-Service cyberattack modeling

Denial-of-service attacks can be implemented in different ways depending on the transport layer protocol used. For a TCP connection between two devices, the TCP protocol requires a "three-way handshake" process [36]. A legitimate client initially sends a connection request using a "synchronize" (SYN) packet to a specific port on the server (Figure 7). The server responds to the request by sending an acknowledgment (ACK) packet and keeping the session open on the port. The handshake is completed when the client sends another ACK packet to the server port within a specified time window. If the third packet is not received, the server port remains open until the end of the time window. A TCP SYN flood attack (Figure 15) happens when an illegitimate client sends multiple initial SYN packets using fake IP addresses or slave computers (in the case of a distributed denial-of-service attack) to multiple ports of the attacked server. Because the IP addresses used are fake, the ACK packet responses from the server are sent but not acknowledged by the clients. The three-way handshake cannot be completed, and the session remains open on attacked ports for the remaining time window. The server becomes unavailable to legitimate traffic during that period. By sending many of these SYN packets for an extended duration, the server is effectively incapacitated, and legitimate packets are dropped or significantly delayed.

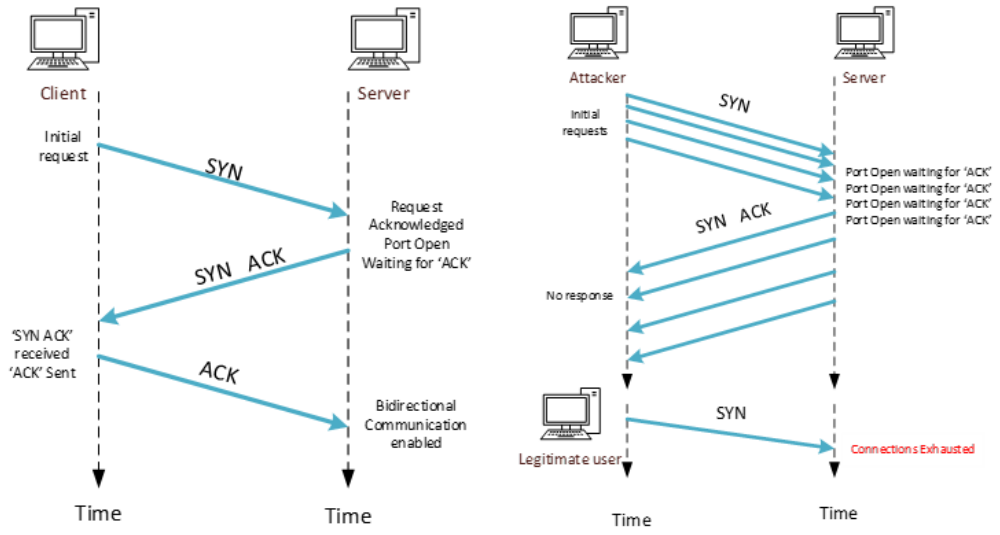


Figure 15: TCP three-way handshake and TCP SYN flood attack process

The process is much simpler when using the UDP communication. UDP is a "connectionless" protocol through which datagrams (packets) can be sent to a server without the need for an acknowledgement. This feature makes UDP a fast, efficient but unreliable communication method. Packet losses are more frequent. Attackers can cause a UDP flood by sending fake data packets to a server port at a very high data rate. The server's processing buffer is filled, and all legitimate packets are dropped (Figure 16). UDP flooding is implemented in this work.

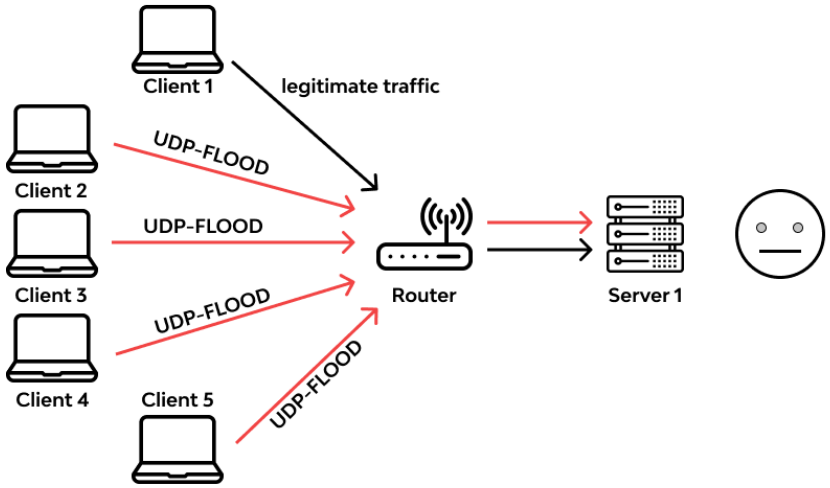


Figure 16: UDP flooding attack process

3.5 System planning, decision support and cyber-security with DT

The DT can be utilized for studies of system planning (integration of inverter-based resources, resilience planning), decision support, and cyber-security monitoring and mitigation. One of the most promising applications of the digital twin is cyber vulnerability assessment. This is carried out by emulating different types of attacks (e.g., denial of service, man-in-the-middle, false data injection) within the virtual environment. The results of testing are then used to determine improvement recommendations for the real system. As it is not realistic to test cyber defense algorithms directly on the physical system, the DT is used for the development, initial implementation, and testing of security strategies before their integration into the real-world environment. Furthermore, the DT is a physics-based simulation of the full topology of the system and, therefore, it is used to detect abnormalities in the data received from the physical system. It can thus constitute an added layer of protection against false data injection and topology attacks.

Finally, the deployment of smart grid technologies may necessitate new communication channels. Telecommunication infrastructure can introduce delays or be prone to outages that affect system operations. Those telecommunication methodologies can be tested first on the DT of the cyber-power system.

3.6 Cyber resilience planning with DT

Due to resource constraints, small utilities and campus systems may not have comprehensive intrusion detection and attack mitigation measures. Sophisticated attackers can exploit those vulnerabilities to conduct direct switching attacks that interrupt power supply by compromising switching devices. These attacks may be coordinated and aim at maximizing damage through deliberate selection of switches and nodes. In a worst-case scenario, coordinated cyberattacks on small distribution systems can lead to cascading events and severe outages. It is therefore important to create resilience plans that leverage grid assets to sustain electricity supply to critical loads and accelerate the recovery process after a major cyberattack.

A resilience plan relying on the grid-forming capabilities of power electronics converters is proposed for VTES. The resilience enhancement is quantified as the amount of electric energy that can be supplied to critical loads during a restoration horizon following an extreme event. The VT's DT is used to validate the resilience plan. The 10 MW battery energy storage system (BESS) is expected to be lithium-ion battery cells interfaced through a voltage-sourced inverter that can operate in both the grid-following and grid-forming control modes. The 2 MW solar plant uses Maximum Power Point Tracking

(MPPT) to ensure optimal output depending on weather conditions. The PV panels are interfaced through inverters using grid-following control because the intermittent solar resource and the lack of reserves makes it harder for efficient implementation of grid-forming control.

The resiliency metric introduced in chapter 2 is used to quantify the resiliency improvement due to the DERs in the VT Smart Grid.

$$R = \sum_{c \in C} W_c \cdot P_c^N \cdot T_c^R$$

In this case, it is assumed that all critical loads have the same weight $W_c = 1$. The sum of the of the critical loads in the VTES system is $\sum P_c^N \approx 3\ MW$. According to the 2022 Corporate Sustainability Report published by AEP [37], the average SAIDI of their distribution system between 2020-2022 is about 233 minutes. Considering a 30-minute delay for situation assessment, it is estimated that the DER-based critical load restoration duration for each event is $T_c^R \approx 203\ mn \approx 3.38\ hrs$. Based on this assumption, the resilience improvement due to microgrid formation is:

$$R = 1 \times 3 \times 3.38 = 10.15\ MWh$$

Chapter 4: Simulation cases and results

4.1 Base case of RTDS simulation of VTES

This section provides a description of the base case simulation of the VTES smart grid in the RSCAD Runtime environment (Figure 17). Closed switches are represented by red squares in the simulation case and open switches are green squares. It is important to note that the switches represented in this case are required to be remote-controlled for a time-efficient implementation of the resiliency plan. In normal operating conditions, the VTES system is divided into three zones separated by normally open switches. Zone B is formed by substation B, the 10 MW BESS and all the green branches and loads connected to the bus bar at substation B. Zone C is formed by substation C, the 2 MW PV plant and all the orange branches and loads connected to the bus bar at substation C. Zone D is formed by the substation D, the 5 MW synchronous generator and all the blue branches and loads connected to substation D. The critical loads, B7 and D1, are highlighted within blue rectangles in the simulation case. In this simulation, both critical loads have a 1.5 MW/0.75 MVAr size.

In the base case, all three substations are active and all steady state voltage magnitudes and phase angles match values previously obtained in an offline power flow analysis performed using DIgSILENT PowerFactory. The BESS inverter operates in a grid-following mode, allowing users to adjust the real and reactive power injected using a slider component. The PV inverter also operates in a grid-following mode. The amount of power injected by the PV system can be set by changing the insolation level and ambient

temperature at the location. This is currently done using slider components, but time-series data containing varying insolation levels and temperatures can be fed directly to the simulation using RSCAD scripts or GTNET communication. The distributed synchronous generator is on stand-by and expected to have a black-start capability.

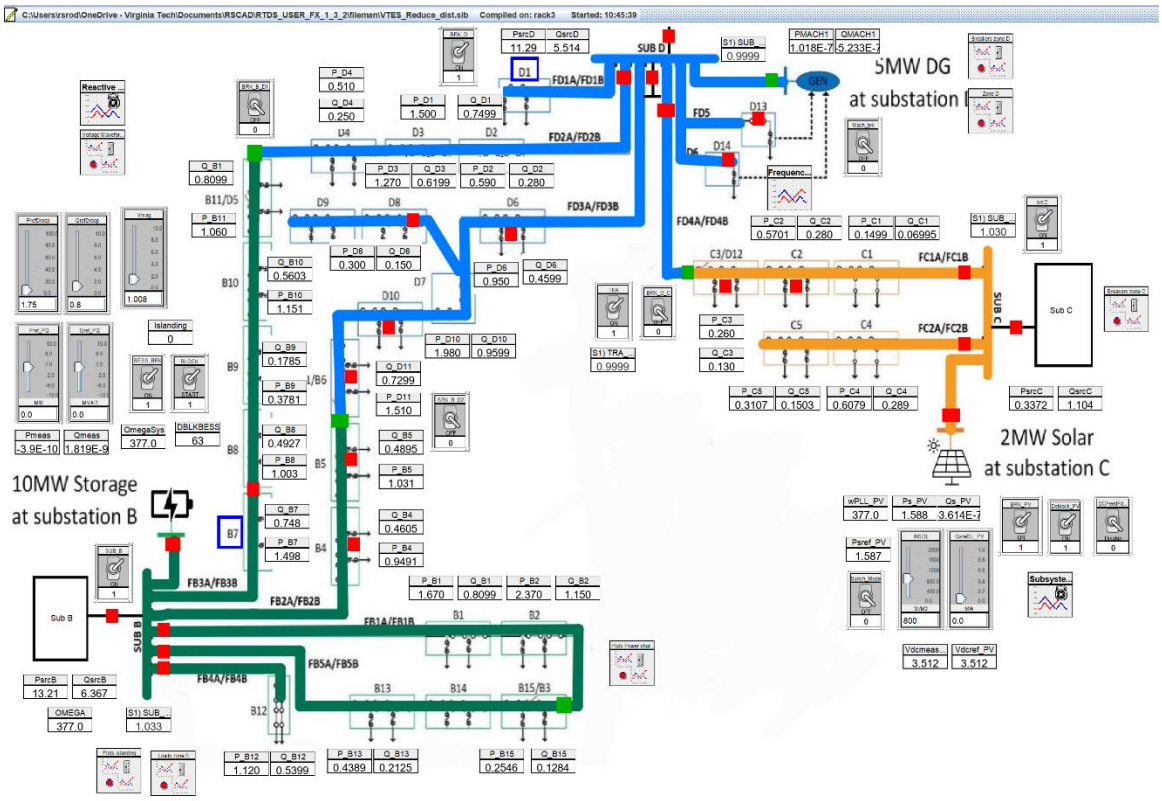
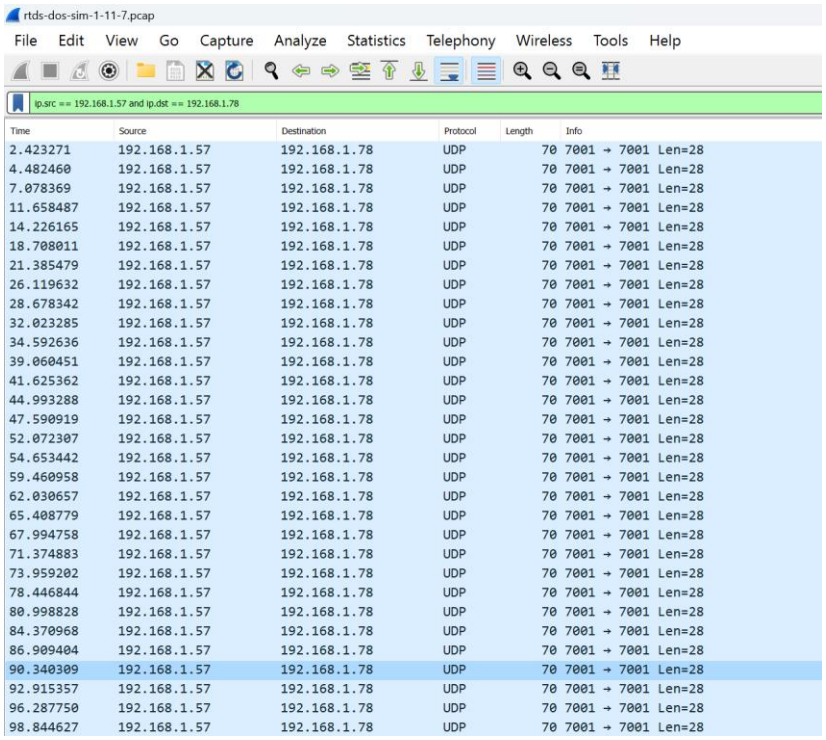


Figure 17: Screenshot VTES base case simulation in RSCAD Runtime

4.2 Resilience plan

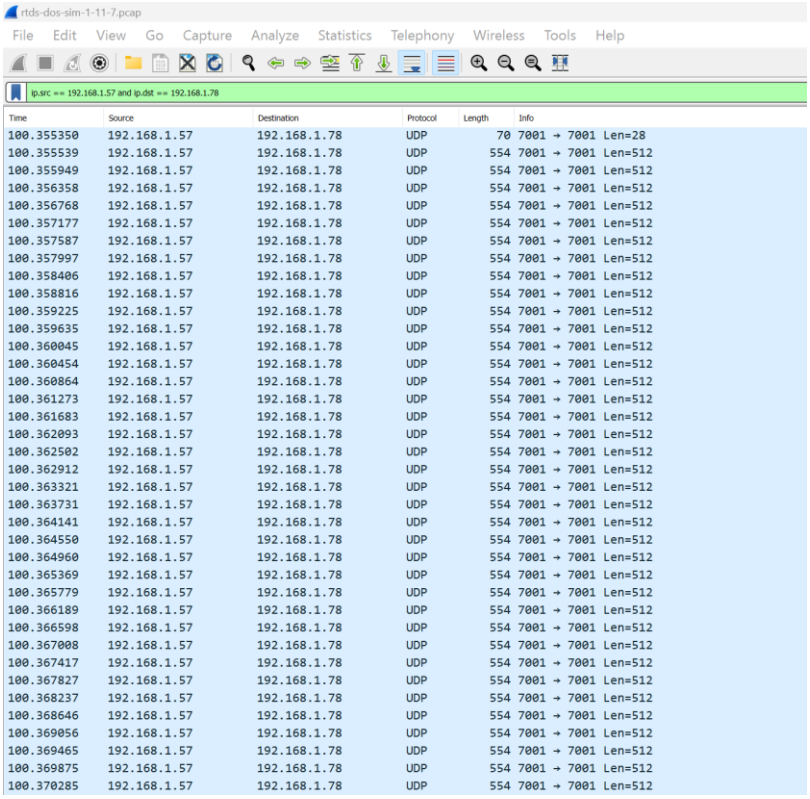
4.2.1 Coordinated cyberattack scenario

A coordinated direct switching attack is simulated with the VTES digital twin. The attack program is written in C++ and launched within the NS-3 network simulation. A sophisticated attacker with knowledge of the system simultaneously opens the breakers (SUB_B, SUB_D and SUB_C) connecting the three substations to the distribution feeders. In the absence of a resiliency plan, this attack causes a complete blackout in the VTES microgrid. However, since the breakers are remote-controlled, operators can quickly send a signal to reclose the breakers. In order to maximize the duration of the attack, the adversary also launches a denial-of-service (DoS) attack that disables communications to/from the compromised assets. This attack starts at $t = 100\ s$ and is executed by sending large UDP packets from the simulated attacker node in NS-3 to the GTNET IP addresses of the switches at a rate of 1000 Mbps. Figure 18 and Figure 19 show the result of a wireshark packet capture before and during the DoS attack, respectively. Before the DoS attack (Error! Re), the packet inter-arrival time is between 2 and 5 seconds with a 28-byte payload. During the attack (Figure 19), the packet inter-arrival time is in the order of milliseconds with a 512-byte payload. The high rate of incoming data fills the GTNET buffer and thus stops legitimate commands from reaching their destination. This kind of sophisticated attack would cause an extended outage.



Time	Source	Destination	Protocol	Length	Info
2.423271	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28
4.482460	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28
7.078369	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28
11.658487	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28
14.226165	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28
18.708011	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28
21.385479	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28
26.119632	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28
28.678342	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28
32.023285	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28
34.592636	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28
39.060451	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28
41.625362	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28
44.993288	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28
47.590919	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28
52.072307	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28
54.653442	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28
59.460958	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28
62.030657	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28
65.408779	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28
67.994758	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28
71.374883	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28
73.959202	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28
78.446844	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28
80.998828	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28
84.370968	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28
86.909404	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28
90.340309	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28
92.915357	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28
96.287750	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28
98.844627	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28

Figure 18: Wireshark capture from the NS-3 simulation to GTNET before the DoS attack.



Time	Source	Destination	Protocol	Length	Info
100.355350	192.168.1.57	192.168.1.78	UDP	70	7001 → 7001 Len=28
100.355539	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.355949	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.356358	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.356768	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.357177	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.357587	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.357997	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.358406	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.358816	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.359225	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.359635	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.360045	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.360454	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.360864	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.361273	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.361683	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.362093	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.362502	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.362912	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.363321	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.363731	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.364141	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.364550	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.364960	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.365369	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.365779	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.366189	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.366598	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.367008	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.367417	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.367827	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.368237	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.368646	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.369056	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.369465	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.369875	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512
100.370285	192.168.1.57	192.168.1.78	UDP	554	7001 → 7001 Len=512

Figure 19:Wireshark capture from the NS-3 simulation to GTNET during the DoS attack (t > 100s).

4.2.2 Sequence of actions in zone B

After the direct switch attack disconnects substation B, a sequence of actions is triggered:

- All non-critical loads in zone B are disconnected.
- The BESS inverter seamlessly switches to grid-forming mode (islanded operation).
- Critical load B7 is picked up by the BESS.

Figure 20 shows that critical load B7 is re-energized by the BESS within 1 second. The voltage and frequency transients observed during these operations are shown in Figure 21. It can be seen that the BESS inverter in a grid-forming mode can restore and maintain both nominal frequency and voltage at the point of common connection (PCC).

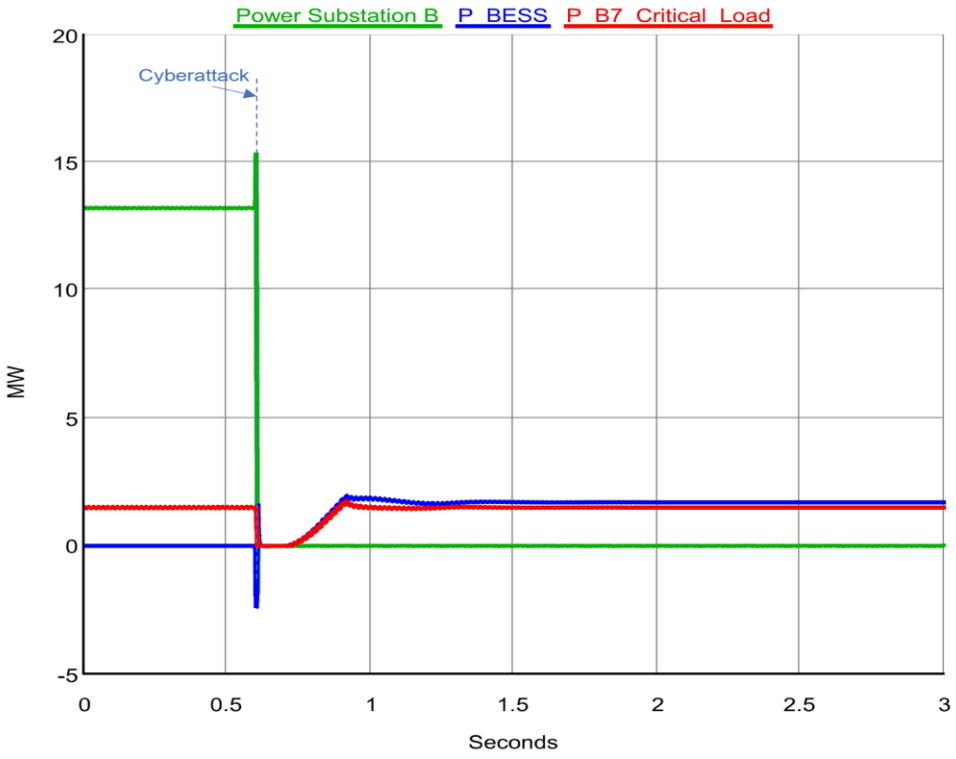


Figure 20: After cyberattack disconnects substation B, BESS quicky restores critical load B7

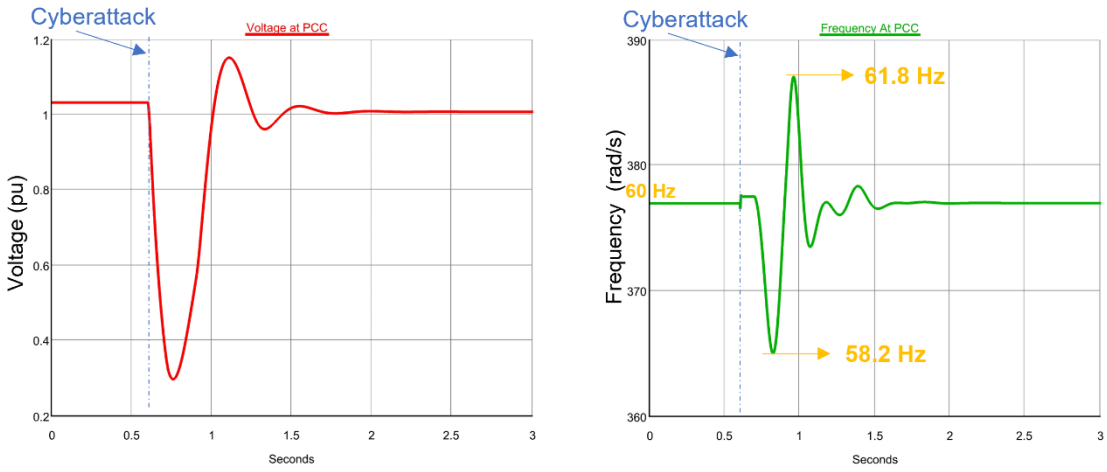


Figure 21: Voltage and Frequency transients observed at PCC during cyberattack and critical load pick-up.

4.2.3 Sequence of actions in zone D

After substation D is disconnected by the direct switching, the synchronous machine cannot seamlessly pick up the critical. The sequence of actions in this zone is as follows:

- All non-critical loads in zone D are disconnected.
- The synchronous machine is started with no load and connected to the transfer bus at substation D.
- Critical load D1 is picked up by the synchronous machine.

As shown in Figure 22, the synchronous machine is initially operating at no-load before picking the critical load at D1. Figure 23 and Figure 24 show the voltage and frequency transients before and after picking the critical load. Because only a primary droop controller is implemented, the no-load frequency is higher than the nominal frequency (~381 rad/s). Nominal frequency is restored after picking up the critical load.

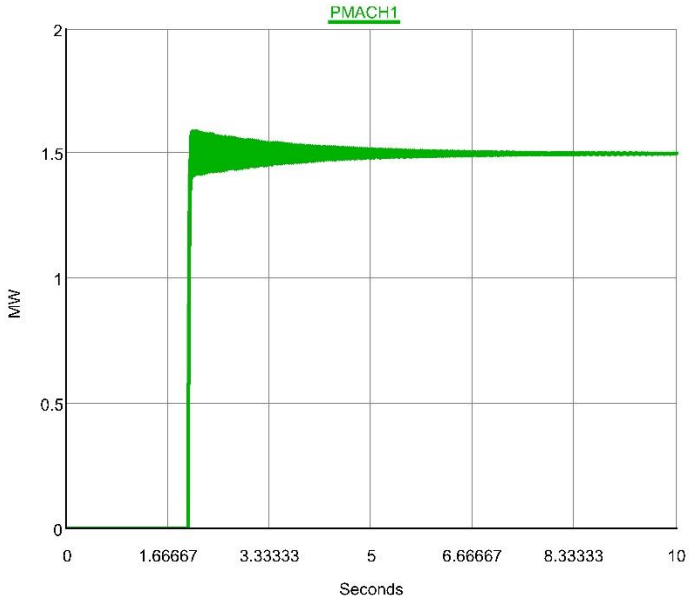


Figure 22: Synch. Machine Power at critical load D1 pickup

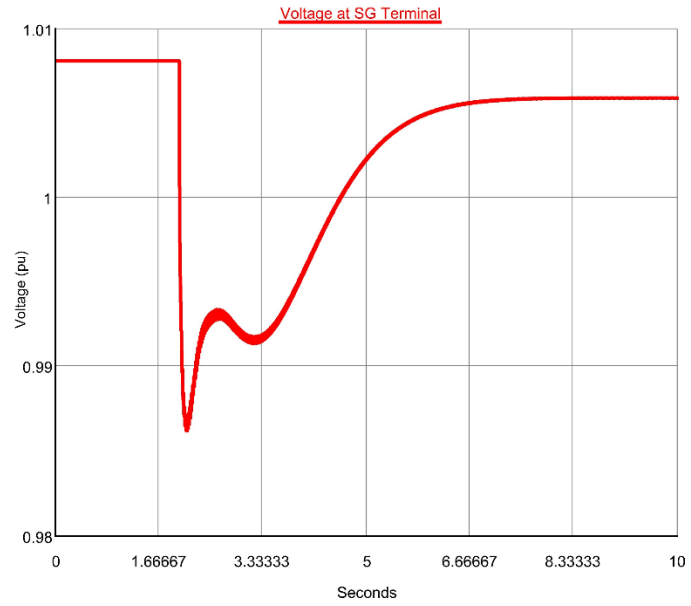


Figure 23:Voltage at terminal of SG at no-load and after critical load pickup

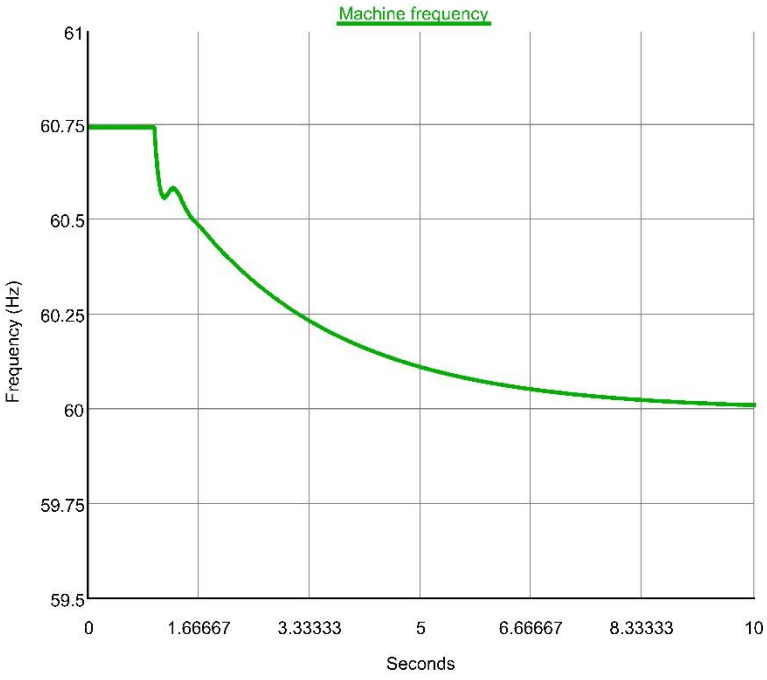


Figure 24: SG frequency at no load and after critical load pickup

4.2.4 Interconnection of the electrical islands

By the proposed resiliency plan, there are two electrical islands: the BESS is supplying power to critical load B7 in zone B and the SG is supplying critical load D1 in zone D. In order to increase the robustness of the microgrid, the two islands are synchronized and interconnected by closing the normally open breaker BRK_B_D. The synchro-check tool available in RSCAD is used to check the voltage magnitude, the frequency, phase sequence and phase angle on both sides of the breaker before closing. By following this procedure, large transients are avoided, and the primary droop controllers can ensure adequate power sharing (Figure 25).

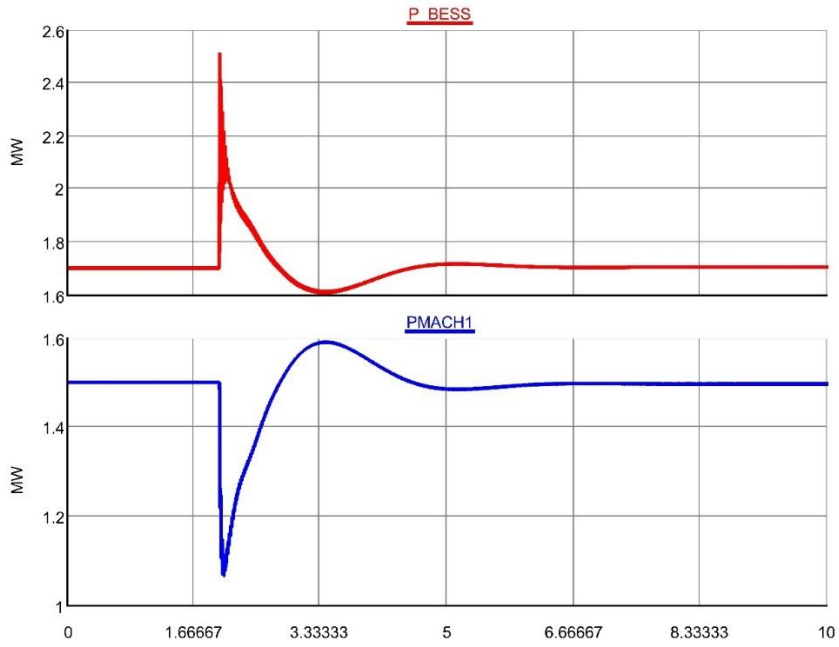


Figure 25: Power sharing between BESS and SG after interconnection

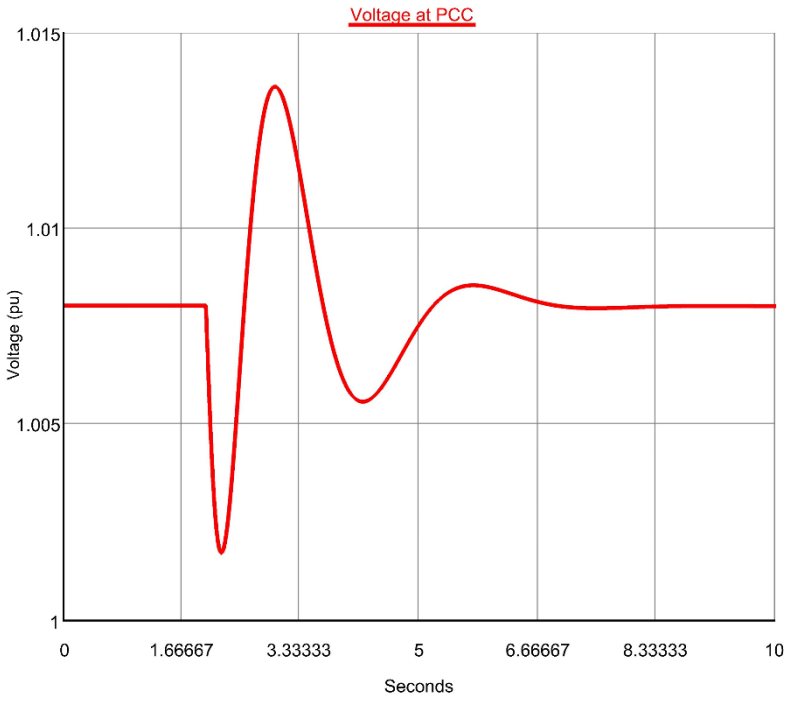


Figure 26: Voltage swings at PCC after interconnection.

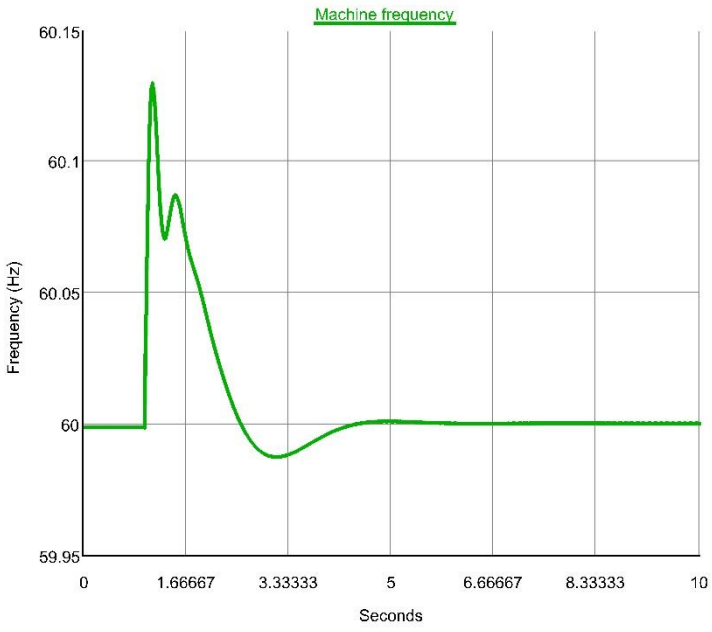


Figure 27: SG frequency swings after interconnection

4.2.5 Interconnection with PV plant

The PV inverter only operates in a grid-following mode. Therefore, when substation C is deenergized, the PV plant stops generating power. In order to use the solar plant during the resiliency scenario, it is necessary to provide new external voltage and frequency references to the PLL. This is the sequence of actions in Zone C after the loss of substation C:

- The PV inverter is disconnected from the grid.
- All non-critical loads are disconnected.
- The normally open circuit breaker BRK_D_C is closed to energize the branch FC1A/FC1B and the bus bar at substation C: this provides new references to the PLL.
- The PLL is used to synchronize the voltage and frequency of the PV (no generation) with the rest of the microgrid. Figure 28 shows that the PV inverter voltage is in phase with the voltage at the bus bar.
- Close the breaker BRK_PV to connect the PV plant to the microgrid.
- Start generating power from the PV.

By following this procedure, closing the breaker causes no voltage or frequency transients. Figure 29 shows the power sharing between the three DERs when after connection the PV at $t = 2\ s$ with no PV generation.

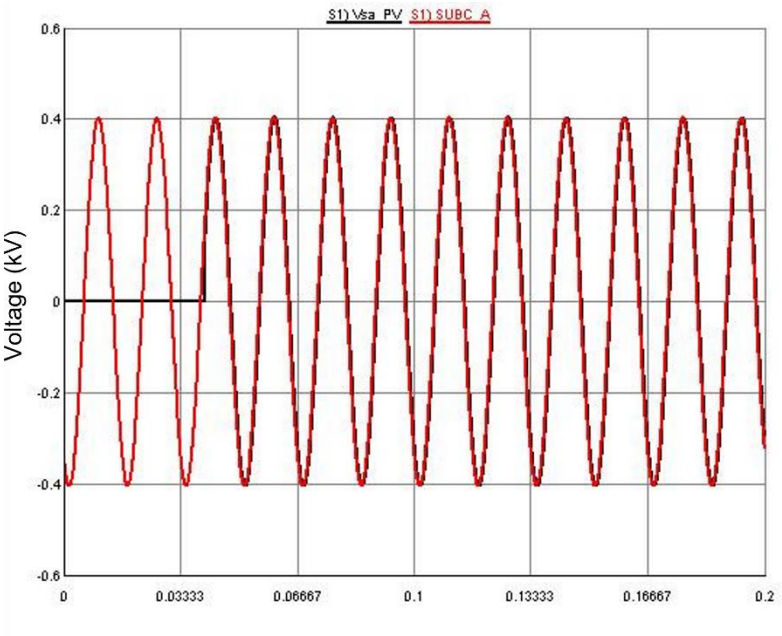


Figure 28: Waveforms of phase A of the PV terminal voltage and the bus bar voltage.

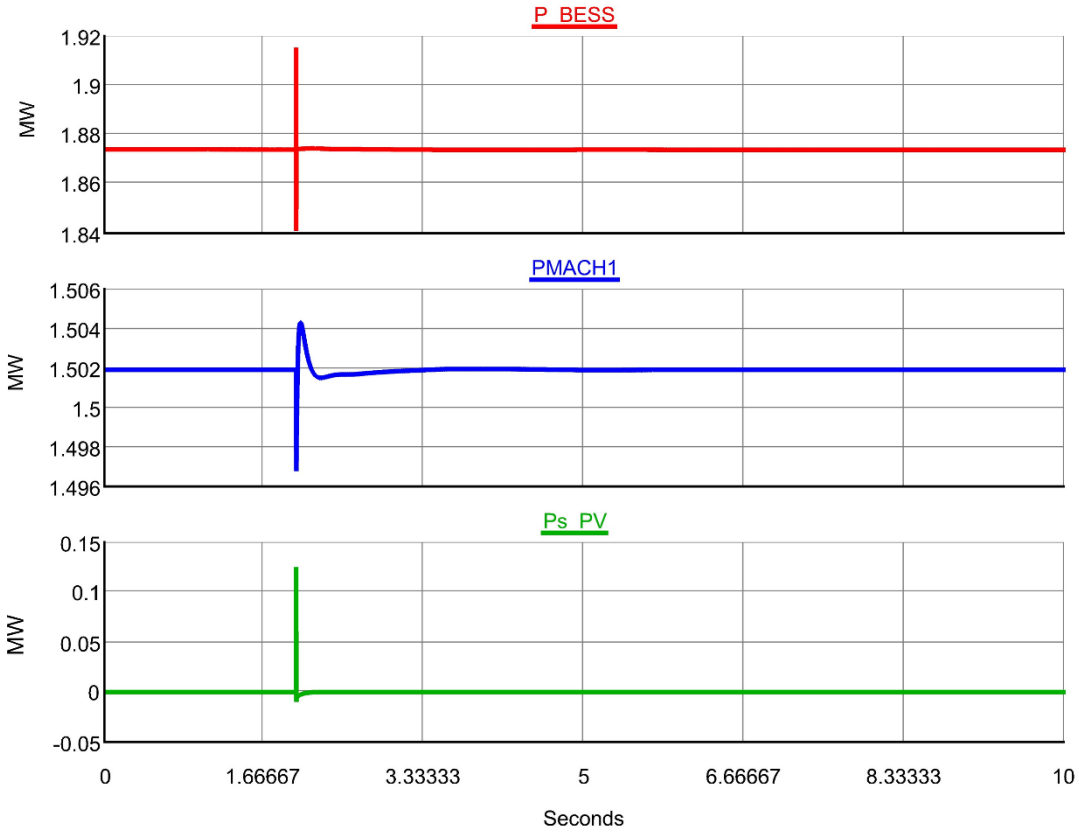


Figure 29: Power sharing at PV connection (no PV generation)

After reconnection, the PV generation is gradually increased to 1 MW by changing the insolation level (Figure 30). The remaining load is shared between the BESS and the synchronous machine. However, the load is not shared equally. This is due to the absence of a secondary, centralized controller that adjusts the droop set points of both the BESS inverter and the SG depending on the load. It is needed to manually change the setpoints to achieve a more desirable dispatch. A secondary controller will be added in a future extension of this work.

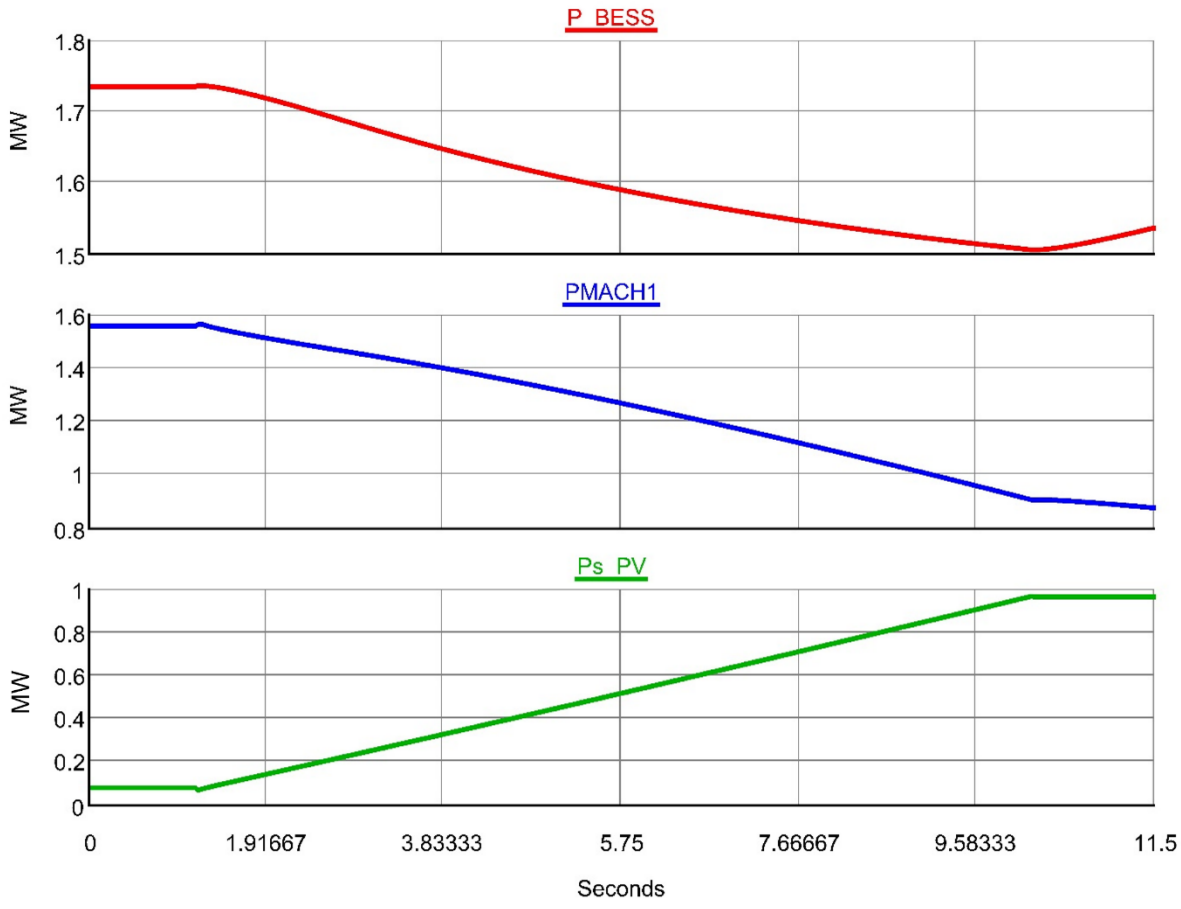


Figure 30: Power sharing among DERs when PV generation is gradually increased.

Chapter 5: Conclusion and future work

5.1 Conclusion

In this thesis, the vulnerability of the modern power grid with respect to extreme weather events and coordinated attacks, both physical and cyber, is studied. It is shown that the expansive nature of distribution systems and the fast-increasing rate of deployment of ICT devices make them vulnerable. A background on possible techniques to enhance the resilience of power distribution systems is presented. These techniques include event impact prediction tools, construction and maintenance programs, distribution automation and the usage of microgrids. A metric used to quantify the resilience improvement due to DER-based critical load restoration is introduced. The operational issues created by the integration of DER, especially inverter-based resources, are detailed in the thesis. The study of these operational issues requires the usage of accurate power systems and cyber network simulation tools. Therefore, the architecture of a comprehensive real-time cyber-power co-simulation environment using RTDS and NS-3 is presented. This co-simulation testbed is implemented as a digital twin using real-world information of the Virginia Tech Electric Service as a test case. A coordinated directed switching attack combined with a Denial-of-Service attack scenario is simulated within the digital twin. This attack scenario shows that attacks conducted in the communication networks can cause extended outages in the distribution system. A DER-based resilience plan, relying on the grid-forming capabilities of IBRs, is created using the digital twin. The sequence of actions required to achieve a robust microgrid in resiliency operation is explained. This

resilience plan is capable of restoring critical loads while meeting IEEE disturbance ride-through requirements and maintaining switching transients within acceptable limits.

5.2 Future work

The methods presented in this thesis can be improved in several ways. On the communication side, the network simulation implements the UDP communication protocol. This is a major limitation as most application-level protocols used in power systems (DNP3, Modbus…) rely on the TCP protocol. The GTNET interface card already supports these protocols. The communication simulation will thus be updated with the implementation of TCP, allowing the routing of power systems protocols. Additionally, only direct switching attacks and DoS attacks are simulated in this work. Future extensions of the project will focus on the implementation of false data injection and Man-In-The-Middle cyberattacks. The development of defense mechanisms is beyond the scope of this work; however, future extensions will propose and test intrusion detection as well as attack mitigation strategies. A novel algorithm that can predict the motives of an attacker in real-time is being developed in the digital twin environment. The algorithm, implemented by distributed agents, can detect an attack, and extract relevant parameters used to learn from the attacker's behavior. Following this, appropriate mitigation strategies at the communication network level will be implemented. More improvements can also be made to the power system simulation. Currently, only conventional droop controls are implemented as primary controllers for the BESS inverter islanded operation. In the future, the proposed method will be extended to incorporate Virtual Synchronous Generator (VSG) and Virtual Oscillator

Control (VOC) methods for power sharing between parallel grid-forming generators in an islanded system. It is also desirable to implement secondary coordinated control and automate the sequence of switching actions using Controller-Hardware-In-The-Loop (CHIL) simulation in addition to the digital twin.

Bibliography

[1] C.-C. Liu, “Distribution systems: Reliable but not resilient? [in my view],” *IEEE Power and Energy Magazine*, vol. 13, no. 3, pp. 93–96, 2015.

[2] A. Menati and L. Xie, “A preliminary study on the role of energy storage and load rationing in mitigating the impact of the 2021 texas power outage,” in *2021 North American Power Symposium (NAPS)*, pp. 1–5, 2021.

[3] Z. E. Mrabet, N. Kaabouch, H. E. Ghazi, and H. E. Ghazi, “Cyber-security in smart grid: Survey and challenges,” Computers & Electrical Engineering, vol. 67, pp. 469–482, Apr. 2018, doi: 10.1016/j.compeleceng.2018.01.015.

[4] D. E. Whitehead, K. Owens, D. Gemmel, and J. Smith, “Ukraine cyber-induced power outage: Analysis and practical mitigation strategies,” in 2017 70th Annual Conference for Protective Relay Engineers (CPRE), Apr. 2017, pp. 1–8. doi: 10.1109/CPRE.2017.8090056.

[5] Y. Xu, C.-C. Liu, K. P. Schneider, and D. T. Ton, “Toward a resilient distribution system,” in *2015 IEEE Power Energy Society General Meeting*, pp. 1–5, 2015.

[6] D. T. Ton and W.-T. P. Wang, “A more resilient grid: The U.S. Department of Energy joins with stakeholders in an R&D plan,” *IEEE Power and Energy Magazine*, vol. 13, no. 3, pp. 26–34, 2015.

[7] Y. Wang, C. Chen, J. Wang, and R. Baldick, “Research on resilience of power systems under natural disasters—a review,” *IEEE Transactions on Power Systems*, vol. 31, no. 2, pp. 1604–1613, 2016.

[8] K. P. Schneider, F. K. Tuffner, M. A. Elizondo, C.-C. Liu, Y. Xu, and D. Ton, “Evaluating the feasibility to use microgrids as a resiliency resource,” *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 687–696, 2017.

[9] J. Li, X.-Y. Ma, C.-C. Liu, and K. P. Schneider, “Distribution system restoration with microgrids using spanning tree search,” *IEEE Transactions on Power Systems*, vol. 29, no. 6, pp. 3021–3029, 2014.

[10] S. Poudel and A. Dubey, “Critical load restoration using distributed energy resources for resilient power distribution system,” *IEEE Transactions on Power Systems*, vol. 34, no. 1, pp. 52–63, 2019.

[11] S. Poudel, A. Dubey, and K. P. Schneider, “A generalized framework for service restoration in a resilient power distribution system,” *IEEE Systems Journal*, vol. 16, no. 1, pp. 252–263, 2022.

[12] Y. Wang, Y. Xu, J. He, C.-C. Liu, K. P. Schneider, M. Hong, and D. T. Ton, “Co ordinating multiple sources for service restoration to enhance resilience of distribution systems,” *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 5781–5793, 2019.

[13] H. Gao, Y. Chen, Y. Xu, and C.-C. Liu, “Resilience-oriented critical load restoration using microgrids in distribution systems,” *IEEE Transactions on Smart Grid*,

vol. 7, no. 6, pp. 2837–2848, 2016.

[14] Y. Xu, C.-C. Liu, K. P. Schneider, F. K. Tuffner, and D. T. Ton, "Microgrids for service restoration to critical load in a resilient distribution system," *IEEE Transactions on Smart Grid*, vol. 9, no. 1, pp. 426–437, 2018.

[15] Y. Xu, C.-C. Liu, Z. Wang, K. Mo, K. P. Schneider, F. K. Tuffner, and D. T. Ton, "DGs for service restoration to critical loads in a secondary network," *IEEE Transactions on Smart Grid*, vol. 10, no. 1, pp. 435–447, 2019.

[16] Y. Du, H. Tu, X. Lu, J. Wang, and S. Lukic, "Black-start and service restoration in resilient distribution systems with dynamic microgrids," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, pp. 1–1, 2021.

[17] D. E. Olivares, A. Mehrizi-Sani, A. H. Etemadi, C. A. Cañizares, R. Iravani, M. Kazerani, A. H. Hajimiragha, O. Gomis-Bellmunt, M. Saeedifard, R. Palma-Behnke, G. A. Jiménez-Estévez, and N. D. Hatziargyriou, "Trends in microgrid control," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1905–1919, 2014.

[18] M. Yazdanian and A. Mehrizi-Sani, "Distributed control techniques in microgrids," *IEEE Transactions on Smart Grid*, vol. 5, no. 6, pp. 2901–2909, 2014.

[19] Lin, Yashen, Joseph H. Eto, Brian B. Johnson, Jack D. Flicker, Robert H. Lasseter, Hugo N. Villegas Pico, Gab-Su Seo, Brian J. Pierre, and Abraham Ellis. 2020. *Research roadmap on grid-forming inverters*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5D00-73476. https://www.nrel.gov/docs/fy21osti/73476.pdf.

[20] W. Du, F. K. Tuffner, K. P. Schneider, R. H. Lasseter, J. Xie, Z. Chen, and B. Bhat tarai, "Modeling of grid-forming and grid-following inverters for dynamic simulation of large-scale distribution systems," *IEEE Transactions on Power Delivery*, vol. 36, no. 4, pp. 2035–2045, 2021.

[21] L.-A. Lee, C.-C. Liu, Y. Xu, K. P. Schneider, F. K. Tuffner, K. Mo, and D. Ton, "Dynamics and control of microgrids as a resiliency source," *International Transactions on Electrical Energy Systems*, vol. 30, 11 2020.

[22] A. Tayyebi, D. Groß, A. Anta, F. Kupzog, and F. Dörfler, "Frequency stability of synchronous machines and grid-forming power converters," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 8, no. 2, pp. 1004–1018, 2020.

[23] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and A. K. Srivastava, "Analyzing the cyber-physical impact of cyber events on the power grid," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2444–2453, Sep. 2015, doi: 10.1109/TSG.2015.2432013.

[24] B. Chen, K. L. Butler-Purry, A. Goulart, and D. Kundur, "Implementing a real-time cyber-physical system test bed in RTDS and OPNET," in 2014 North American Power Symposium (NAPS), Sep. 2014, pp. 1–6. doi: 10.1109/NAPS.2014.6965381.

[25] M. Panteli and P. Mancarella, "The Grid: Stronger, bigger, smarter?: Presenting a conceptual framework of power system resilience," *IEEE Power Energy Mag.*, vol. 13, no. 3, pp. 58–66, May 2015, doi: 10.1109/MPE.2015.2397334.

[26] G. Davis, A. F. Snyder, and J. Mader, “The future of distribution system resiliency,” in *2014 Clemson University Power Systems Conference*, Mar. 2014, pp. 1–8. doi: 10.1109/PSC.2014.6808134.

[27] Y. Xu, C.-C. Liu, K. P. Schneider, and D. T. Ton, “Placement of remote-controlled switches to enhance distribution system restoration capability,” *IEEE Trans. Power Syst.*, vol. 31, no. 2, pp. 1139–1150, Mar. 2016, doi: 10.1109/TPWRS.2015.2419616.

[28] Y. Xu and W. Liu, “Novel multiagent based load restoration algorithm for microgrids,” *IEEE Trans. Smart Grid*, vol. 2, no. 1, pp. 152–161, Mar. 2011, doi: 10.1109/TSG.2010.2099675.

[29] C.-C. Liu *et al.*, “Cyber–physical system security of distribution systems,” *Found. Trends® Electr. Energy Syst.*, vol. 4, no. 4, pp. 346–410, 2021, doi: 10.1561/3100000026.

[30] A. Kwasinski, V. Krishnamurthy, J. Song, and R. Sharma, “Availability evaluation of micro-grids for resistant power supply during natural disasters,” *IEEE Trans. Smart Grid*, vol. 3, no. 4, pp. 2007–2018, Dec. 2012, doi: 10.1109/TSG.2012.2197832.

[31] A. Hussain, V.-H. Bui, and H.-M. Kim, “Microgrids as a resilience resource and strategies used by microgrids for enhancing resilience,” *Appl. Energy*, vol. 240, pp. 56–72, 2019, doi: https://doi.org/10.1016/j.apenergy.2019.02.055.

[32] F. Alsaeidi, C.-C. Liu, and L.-A. Lee, “Graph-theoretic partitioning for differential zone protection in an islanded microgrid,” in *2023 IEEE Power & Energy*

Society Innovative Smart Grid Technologies Conference (ISGT), Jan. 2023, pp. 1–5. doi: 10.1109/ISGT51731.2023.10066434.

[33] Kenward, A. and Raja, U. "Blackout: Extreme weather, climate change and power outages," Climate Central Report, 2014. [Online]. Available: http://assets.climatecentral.org/pdfs/PowerOutages.pdf

[34] Office of Cybersecurity, Energy Security, & Emergency Response, "OE-417 Electric emergency and disturbance report - Calendar year 2022," U.S. Department of Energy, 2022. [Online]. Available: https://www.oe.netl.doe.gov/download.aspx?type=OE417PDF&ID=82

[35] A. Yazdani and R. Iravani, *Voltage-sourced converters in power systems: Modeling, control, and applications*. Hoboken, NJ: IEEE Press/John Wiley, 2010.

[36] J. F. Kurose and K. W. Ross, *Computer networking: a top-down approach*, 6th ed. Boston: Pearson, 2013.

[37] "2022 TCFD report - AEP Sustainability." [Online]. Available: https://www.aepsustainability.com/performance/docs/FINAL%202022%20TCFD%20Report.pdf [Accessed: 07-Apr-2023].