STABILITY IMPACT OF INCREASED DER PENETRATION IN REGARD TO THE IEEE 1547 STANDARD IN THE PRESENCE OF CYBERADVERSARIES

BY

PRERAK CHAPAGAIN

THESIS

Submitted in partial fulfillment of the requirements
for the degree of Master of Science in Electrical and Computer Engineering
in the Graduate College of the
University of Illinois Urbana-Champaign, 2021

Urbana, Illinois

Adviser:

Professor Peter Sauer

ABSTRACT

The Institute of Electrical and Electronics Engineers (IEEE) 1547 standard addresses the integration of distributed energy resources (DER) into area electric power system (AEPS). First released in 2003, with multiple revisions ongoing, the most recent version from 2018 is used in this thesis to develop several use cases to assess the stability risks in the presence of cyberadversaries. The updated standard specifies the need for more flexible settings, requiring DER to remain connected during certain disturbances and provide voltage support via active and reactive power modes.

The advent of these functionalities also introduces possible risks where certain settings combinations, which, while allowable under the standard, may actually create instability. The notion that DER should be equipped with a communication interface to be able to communicate with the AEPS operator exposes DER to numerous attack vectors from cyberadversaries.

This concern is amplified as DER penetration increases, where under a reasonable threat model, multiple DER could be attacked simultaneously. Through several illustrative use cases, this thesis addresses in detail how potentially adverse combinations of mode change, mode setting parameters, and ride-through and tripping settings could lead to instability. The use cases are then validated through simulations of a hypothetical AEPS with varying degrees of DER penetration. It was concluded that certain adverse mode changes or settings, whether through error or cyberattack, can lead to unstable conditions with DER penetration as low as 24 % of the AEPS system capacity. This is a motivation to look into possible mitigation strategies on both the cybersecurity and cyberphysical sides of the problem.

To my family, for their love and support.

ACKNOWLEDGMENTS

I wish to express my sincere gratitude and deep appreciation to my adviser Professor Peter Sauer for taking me as his student and for his constant encouragement, valuable inputs and support to sustain my efforts. He is an excellent mentor with not only technical skills but also empathetic attributes which were helpful for me to transition from undergraduate to graduate school research and classes. His guidance in my research, thesis, career prospects, and graduate life overall is invaluable. I would also like to thank him for referring me to the Information Trust Institute team for the IEEE 1547 project which gave me an opportunity to work with power experts within and outside the university.

I would like to express my deep gratitude to my research co-advisor Alfonso Valdes for being available and guiding me in my research work. His ability to give ideas to overcome the researcher's block and his help in connecting me with various industry experts have made me a better researcher. His commitment to making progress in research while ensuring everyone on the team is happy is what makes him a great mentor and research lead.

My acknowledgment would be incomplete without my sincere thanks to our industry partners Hitachi ABB power grids, Duke Energy, and ORNL, especially industrial experts Dr. Dmitry Ishchenko and Dr. Mehmet Cintuglu, for answering many of my questions and giving practical advice in helping realize a more realistic approach to the research.

I would not have been able to make this much progress without support of my teammates Megan, Richard, Professor Bose, and Ken. I would also like to thank Professor Gross for his guidance during my first few months at UIUC. Special thanks to all my teachers, colleagues and friends for their wishes and moral support. I am deeply indebted to my father, mother, and sister for constantly encouraging me to give my best in both research and graduate classes. After all, you are what you are because of the people around you.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AC	Alternating Current
AEPS	Area Electric Power Systems
CB	Circuit Breakers
CBEMA	Computer and Business Equipment Manufacturers Association
DC	Direct Current
DER	Distributed Energy Resources
DERs	Distributed Energy Resources (bulk of two or more than two)
DNP3	Distributed Network Protocol 3
EPS	Electric Power Systems
ESS	Energy Storage Systems
FDI	False Data Injection
FPGA	Field Programmable Gate Array
GOOSE	Generic Object Oriented System-wide Events
IEEE	Institute of Electrical and Electronics Engineers
IEC	International Electrotechnical Commission
ITIC	Information Technology Industry Council
MPPT	Maximum Power Point Tracking
PCC	Point of Common Coupling

PoC	Point of Connection
PI	Proportional Integral
PV	Photovoltaic
RMS	Root Mean Square
RPA	Reference Point of Applicability
RPS	Renewable Portfolio Standard
RTU	Remote Terminal Unit
SEP2	Smart Energy Profile 2.0

Chapter 1

INTRODUCTION

Policymakers across the United States are reacting to calls for grid modernization and demands for cleaner energy by setting aggressive goals to reduce carbon output. From 50% clean renewable energy in California by 2030, to 100% clean energy in Hawaii by 2045, to 70% renewable energy in New York by 2030 [2–4], these policies show the emphasis the United States is placing on the green movement by being careful about where their electricity is

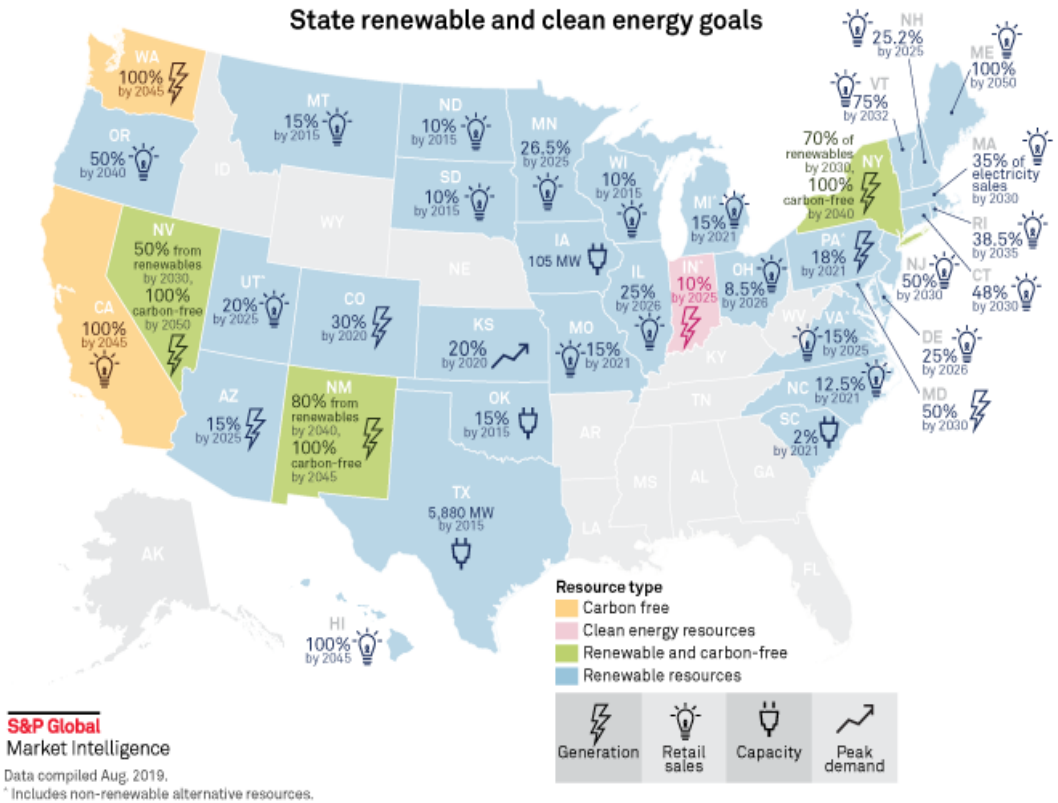


Figure 1.1: United States map for RPS goals [1]

coming from. The United States map shown in Figure 1.1 shows a few other states' goals in a more descriptive and granular manner.

Though clean and renewable energy can come from a variety of sources, including nuclear, geothermal, and hydroelectric, almost all initiatives include plans for expanding distributed energy resources (DER), such as solar, wind, and storage. For example, there are more than 2.3 million solar generators on the U.S. distribution system today, with steady growth expected in the future [6]. Ability to adjust the system size of DER geographically as per the demand, and having the generation and load close to each other, are two main reasons for the appeal of DER. This adaptive nature and flexibility in deploying DER has motivated in their rise across the United States.

Another instance where localized DER systems can help the system be more resilient is when disruption occurs because of natural disasters and hazards. During these times, the power system can be reconfigured into

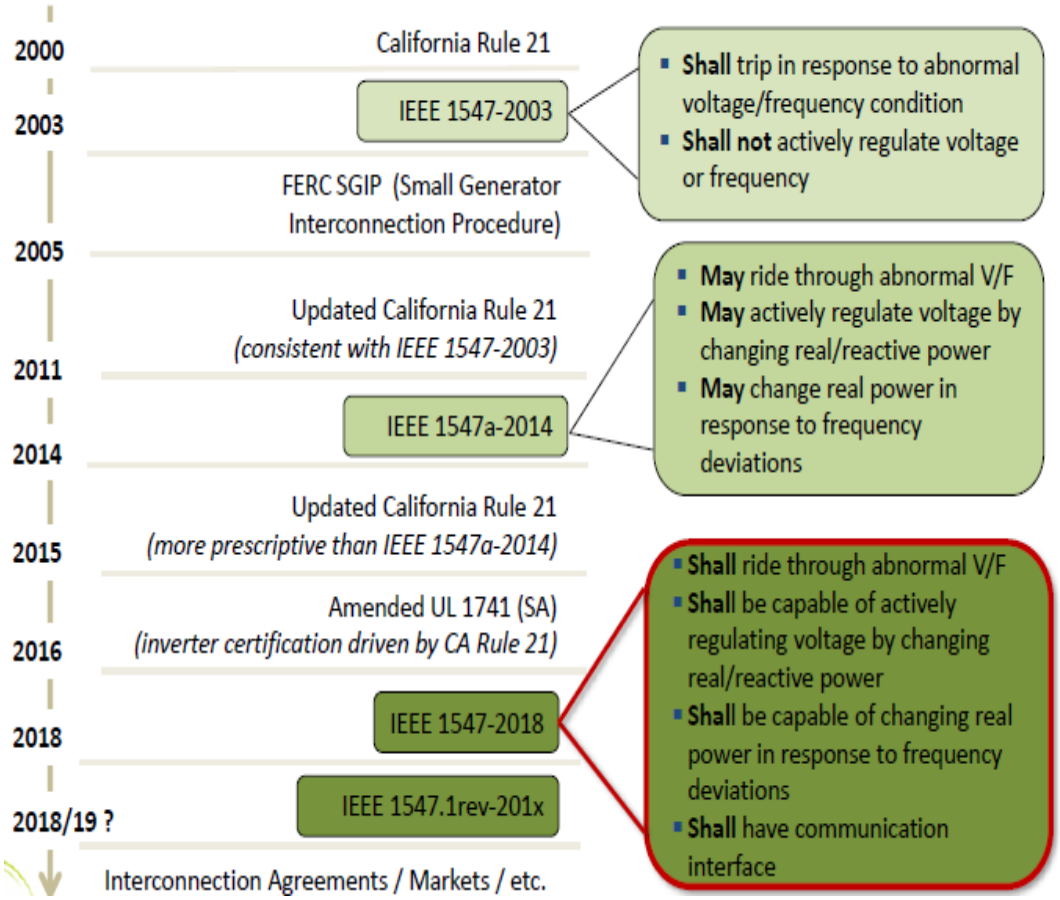


Figure 1.2: Evolution of IEEE standard and California Rule 21 [5]

independent secure segments that each contain load and generation which can enhance grid resilience to keep critical services online and restore service faster with help from the fast-responding power electronics in solar generation and energy storage systems [6].

This expected growth in DER motivated the update to the IEEE 1547 standard on DER interconnections with the grid. Figure 1.2 shows the timeline of the evolution of the IEEE 1547 standard alongside California Rule 21 which also covers the requirement standards for the connection of DER. The working group in 2003 did not foresee that DER would achieve such high penetration and did not consider continuous DER operation as important to the grid [7]. The original standard required DER to immediately trip off for any disturbances and did not require DER to actively regulate voltage or frequency. Immediate tripping in response to a disturbance might have been a viable response when DER were a small proportion of the grid. At that time, losing their little generation would not have severely affected the demand, nor would the participation of DER in active regulation of frequency and voltage been of great significance. Thus, in order to safeguard DER without having to worry too much about its impact on the grid, DER were required to be tripped off in response to frequency and voltage deviations.

However, this approach is no longer feasible when DER form a major proportion of the grid. Not only would the grid lose huge amounts of DER supplying the distribution load, but this loss might affect the stability of the area electric power system (AEPS). In response to this realization, and seeing the continued rise of DER, the revised standard requires DER to provide reactive power support, ride through certain disturbances, and only trip when a threshold determined by the AEPS is reached. It can be seen from the timeline how it went from "shall not" to "may" to "shall" in the 2003, 2014, and 2018 versions of the standard with regard to DER's requirement on the engagement of ride-through and active response to voltage and frequency deviations. This update requires the addition of more complex features to the control systems and power electronics of DER inverters and opens up possibilities for both grid support modes and islanding modes.

Another feature that sets apart the IEEE 2018 standard from previous revisions is the communication interface. With increasing number of DER meeting the load through coordinated generation, it is necessary to have communication among DER, and with the main grid. Figure 1.3 shows com-

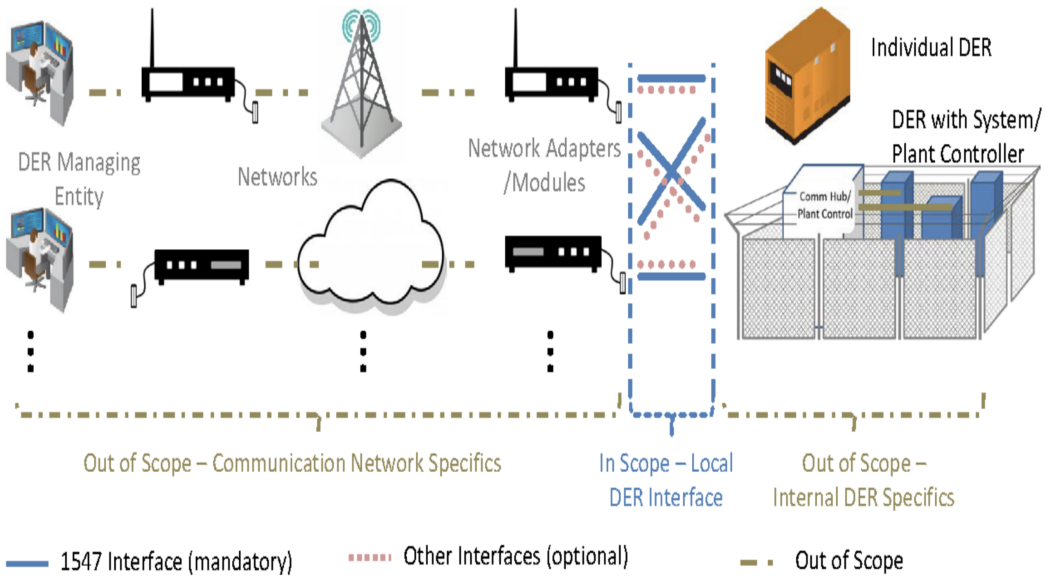


Figure 1.3: Control protocol in/out of scope mapping [8]

munication protocol requirements where the local DER interface that talks between the managing entity and DER is within the scope of the standard. This smart feature, however, exposes the system to several cybersecurity risks where an adversary may spoof the communication messages to compromise the system. Ongoing research has revealed the importance of cybersecurity for DER and IEEE 1547−2018 leaves the issue up to mutual agreement from the DER and AEPS and local regulations [8].

It is inevitable that the increased communications and capabilities naturally result in potential attack surfaces. These attack surfaces could arise as a result of exploitation by an adversary, or they could be exposed by error, creating adverse conditions. Ongoing research points to the importance of cybersecurity of DER [9–12]. In response to that, the IEEE 1547.3 working group is currently drafting a companion cybersecurity guide. Though the details will be more clear after drafting the IEEE 1547.3, it is obvious that there is flexibility in the extended capabilities of DER described in the standard that could create adverse conditions through malicious or mistaken combinations of modes.

There has been a lot of research exploring the possibilities of cyberattack and ways to mitigate them with reference to the new IEEE 1547 standard. Based on the literature review, the most commonly known attack types are

man-in-the-middle, replay, eavesdropping, spoofing through security certificates, denial of service, least privilege violation, and brute force credential harvesting [13], [14].

The standard specifies that the communication interface may use SunSpec Modbus or Distributed Network Protocol 3 (DNP3) for communication, with more recent consideration of International Electrotechnical Commission (IEC) 61850 Generic Object Oriented System-wide Events (GOOSE). These are protocols that are already widely used in power systems. Among the protocols, SunSpec Modbus is the simplest and has no security measures whereas DNP3 has a few security measures, such as authentication and message integrity check [13]. A new coordination strategy is used with the IEC 61850 GOOSE protocol to exchange the DER status with voltage regulated devices in DER and the existing field devices for advanced power distribution systems, and is validated using field programmable gate arrays (FPGAs) based real-time simulation [14]. The IEEE Std.2030.5, also referred to as Smart Energy Profile 2.0 (SEP2), is the only communication protocol that requires and implements cryptography [13].

However, no matter what kind of protocol is used, there is always a possibility of an attack and thus it is important to look at this from the cyberphysical point of view as well. Even if cryptography is used, an attacker who has compromised an operator workstation in a control room can have the commands issued from that workstation satisfy cryptographic requirements. Thus, there is need for detection and defense based on the analysis of the potential physical impact of the operator commands such that it defends against adversarial attack as well as operator error. The high impact attacks on the power grid and similar systems have come from attackers first compromising the organization. After that, they eventually hack into engineering workstations from where they can send commands that do not just impersonate the control center but legitimately come from the control center which makes protocol security features less useful [15].

To accommodate reactive power participation from multiple DER, various static and dynamic voltage regulation control strategies are used in reducing the switching operations of voltage regulating devices and grid oscillatory actions to improve voltage quality in the power distribution [16]. When it comes to fault detection, due to the new standard mandating low voltage ride-through functionalities in inverters, a different approach is needed

in the detection of faults for low voltage ride-through. Measurements of positive sequence voltage magnitude and root mean square (RMS) voltage measurements were a few of the techniques explored. Due to the lag in detecting RMS voltage measurements, it was concluded that using a Kalman filter provides faster results in the detection of the operating regions of low voltage ride-through [17]. Machine learning can also be used in the detection and mitigation strategies for a system with attacked DER. For example, deep reinforcement learning could be used as a tool to learn the optimal parameters for the control logic of a set of non-compromised DER units to actively mitigate the effects of a cyberattack on a subset of network DER [18].

In this thesis, a simple model of two aggregate DERs connected to the AEPS, which may compose a significant fraction of total system generation capacity, is considered. A simulation analysis of potentially adversarial combinations of modes that lead to voltage depression on a hypothetical AEPS with varying degrees of DER penetration was conducted. It was concluded that certain adverse mode changes, whether through error or cyberattack, can lead to unstable conditions with DER penetration as low as 24% of the AEPS system capacity. This is significantly lower than many currently proposed Renewable Portfolio Standard (RPS) goals [19].

This observation helps in performing reachability analysis where the current system states and candidate commands from the AEPS are considered. Based on off-line power system analysis and simulation, reachability analysis estimates the probability that an undesirable state is "reachable" from the current state and the candidate command. If this is unacceptably high, it is important to consider the command suspicious and block it from reaching the DER controller. This technique can be used to implement a possible state estimation strategy in situations where cybersecurity engineers with limited resources need to deploy a firewall mechanism in a large bus system on selected buses. It would be ideal to have all the nodes equipped with sophisticated security mechanisms. However, due to economic and time constraints, these security mechanisms may not be deployable to all nodes. Thus, through the knowledge of state estimation, it would be easier to rank nodes based on their DER penetration and the dire need to have the level of security mechanism deployed.

The remainder of this thesis is organized as follows. The background on the revised standard is summarized in Chapter 2. The system model is described

in Chapter 3. Use cases and attack descriptions are explored in Chapter 4. Results are shown in Chapter 5. Chapter 6 outlines ongoing and future work. Chapter 7 concludes the thesis with a summary.

Chapter 2

BACKGROUND ON IEEE 1547 STANDARD

The motivation behind developing an updated standard for IEEE 1547 is due to the growing penetration of DER. The original 2003 standard was written at a time when the impact of DER on distribution systems was unknown, so utilities took a conservative approach [7]. However, with high penetration of DER becoming common and only expected to grow in recent years, the revised version calls for mandatory, but adjustable, reactive power support from the DER, as well as more permissive ride-through settings that ensure DER will stay connected for small disturbances. Mandatory tripping requirements are adjustable based on the AEPS calculation to maintain grid resiliency. This is necessary due to the fact that the grid is relying on support from several forms of DER. Therefore, IEEE 1547-2018 attempts to delineate the required features and functionalities for any DER that is planning on interconnecting with the grid and be a part of the larger AEPS.

2.1 Reference point of applicability

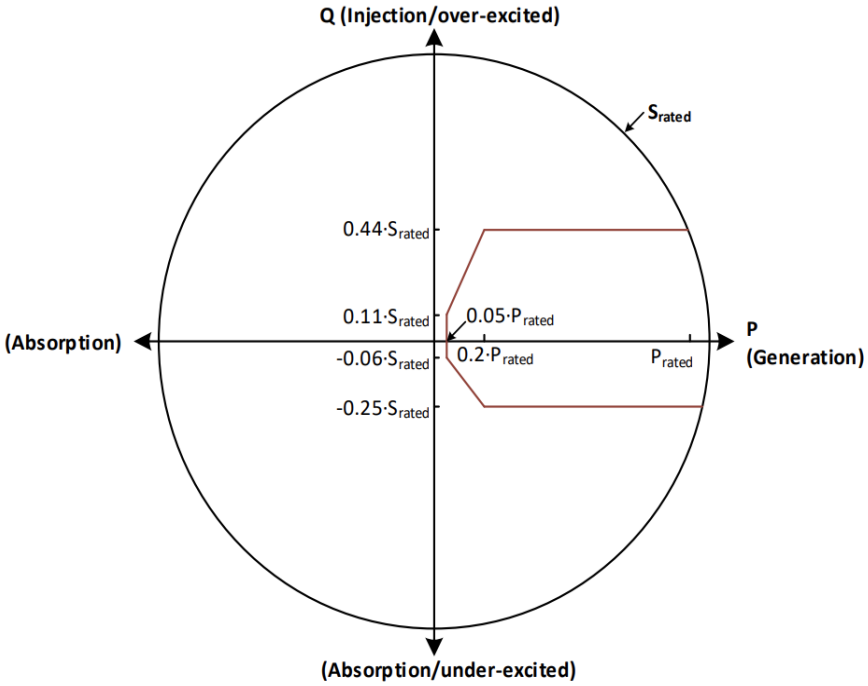
Reference point of applicability (RPA), as the name suggests, is the location where the interconnection and interoperability performance requirements specified in this standard apply. The performance requirements include voltage and frequency monitoring and implement ride-through and trip functionalities. Point of common coupling (PCC) is defined as the point of connection between the AEPS and local electric power system (EPS) where local EPS in this case is the DER. Point of connection (PoC), on the other hand, is defined as the point where a DER unit is electrically connected in a local EPS. The characteristics of the local EPS and DER shall determine if the RPA will be PCC or PoC. However, if the impedance between the PoC and PCC is less than 0.5% of the DER rated apparent power and voltage

base, individual DER units that are considered fully compliant at the PoC may be considered fully compliant at the PCC as well [8]. Throughout the remainder of the thesis, PCC is chosen as the RPA.

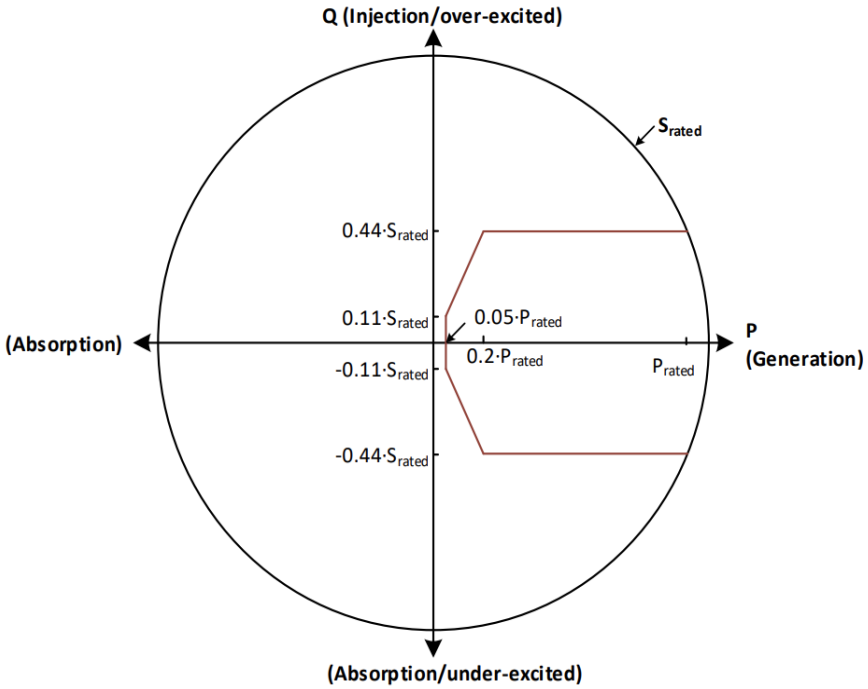
2.2 Minimum reactive power capability

All DER are required to have reactive power injection and absorption capability as per the new IEEE 1547−2018 standard depending on over-excited and under-excited states respectively. However, not all DER have the same capability to absorb reactive power. For example, synchronous generators have limitations to their reactive power absorption capability but are preferred technology for recovering energy from bio-gas, backup generation, and other functions [7]. Thus to avoid excluding those types of DERs, the standard has defined two different categories of DER based on reactive power capability. Category A has requirements that are feasible for all known DER technologies to meet. Category B has enhanced requirements that are beneficial to the power system, but may not be achievable by all technologies. DER belonging to Category B, which is intended for systems with higher DER penetration, must be able to inject and absorb at least 44% of the nameplate apparent power rating of reactive power. All DER belonging to Category A must be able to inject 44% and absorb 25% of the nameplate apparent power rating of reactive power. This is to accommodate DER with lower absorption capability and is deemed adequate for applications where the DER penetration in the distribution system is lower [8].

Figure 2.1 shows minimum reactive power capability for Category A and Category B DER as a function of active power output. If the active power output is less than 5% of the rated active power, DER is not obligated to provide any reactive power support. For active power output between 5% and 20%, the DER shall be capable of exchanging reactive power up to the 44% (except for Category A absorption which would be 25%) multiplied by the active power output divided by 20% of rated active power. For example, for Category B, at 5%, reactive power capability is calculated by $0.44 * 0.05 * P_{rated}/(0.2 * P_{rated})$ which comes out to be $0.11S_{rated}$ and similarly, at 20%, it comes out to be $0.44S_{rated}$, as is seen on the y-axis. When the DER is providing active power at or above 20% of its rated capacity, the maximum



Category A



Category B

Figure 2.1: Minimum reactive power capability of Category A and B DER [8]

required reactive power absorption remains at 44% of the apparent power. Since it is common for DER to be generating at least 20% of rated power output, DER are assumed to be operating in that region of the chart for the remainder of the thesis.

Note that operation at any active power output above 20% of rated active power shall not constrain the delivery of reactive power injection or absorption, i.e., curtailment of active power to meet apparent power constraints is permissible. The DER may produce active power up to the kVA rating provided that the DER remains capable at all times to absorb or inject reactive power, to the full extent of the reactive power capability ranges as defined in the standard. The DER P_{rated} may be less than or equal to S_{rated} and the DER may need to reduce active power in order to meet the demanded reactive power in order to respect its apparent power limits [8].

Table 2.1: Voltage and reactive/active power control function requirements for DER normal operating performance categories

DER category	Category A	Category B
Voltage regulation by reactive power control		
Constant power factor (*p.f.*) mode	Mandatory	Mandatory
Voltage—reactive power (*Volt-VAR*) mode	Mandatory	Mandatory
Active power—reactive power (*Watt-VAR*) mode	Not required	Mandatory
Constant reactive power (*VAR*) mode	Mandatory	Mandatory
Voltage regulation by active power control		
Voltage—active power (*Volt-Watt*) mode	Not required	Mandatory

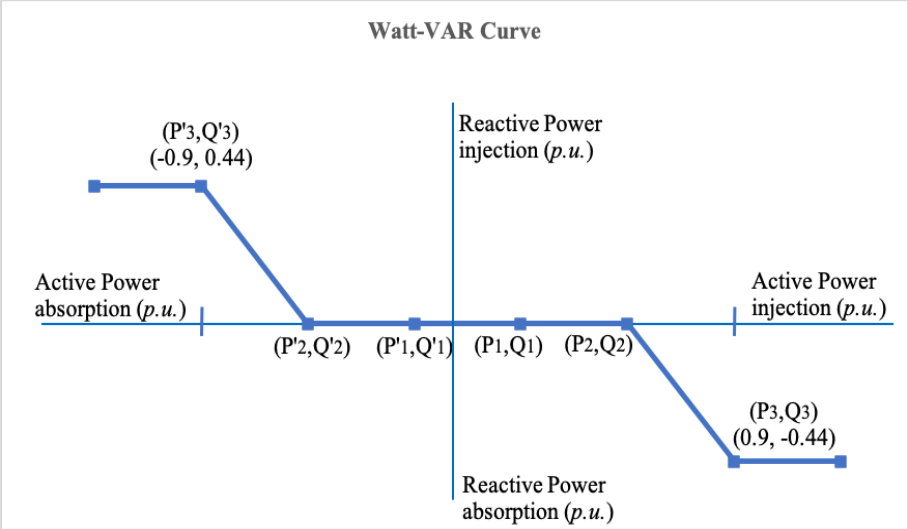


Figure 2.2: Associated curve for default Watt-VAR mode

2.3 Operating modes

To be able to connect to the grid, the DER is supposed to have functionalities of being able to operate in certain modes. The standard specifies four reactive power operating modes and one active power operating mode that allows DER to support voltage and frequency at the PCC. Table 2.1 lists different types of reactive and active power modes for DER of Categories A and B. Category A does not require Watt-VAR and Volt-Watt mode functionalities while Category B is mandated to have functionalities for all the modes listed. Throughout the thesis, DER is assumed to be of Category B with the minimum reactive power capability of 0.44 per unit (p.u.) of the apparent power. This assumption is made because it gives flexibility to operate at any mode. Note that the setpoints for the curves for each mode can be changed by the AEPS operator. In the presence of no attack, the default values as defined in the standard are assumed for the setpoints for all the modes.

Out of the four reactive power modes mentioned in Table 2.1, Constant Power Factor mode, is the default set mode. With Constant Power Factor mode, AEPS operator is able to set desired power factor as it fits the needs of the grid. By default, it would be operating at a unity power factor. Voltage-Reactive Power mode, commonly referred to as Volt-VAR mode, provides the reactive power output based on voltage readings. Active Power-Reactive Power mode, also known as Watt-VAR mode, provides reactive power output

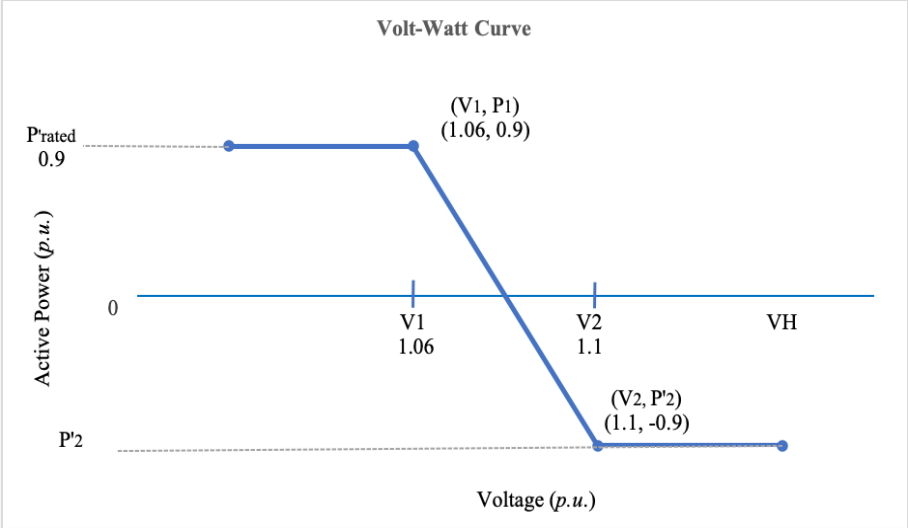


Figure 2.3: Associated curve for default Volt-Watt mode

based on active power output from the DER. That active power can either come from maximum power point tracking (MPPT) controllers or from Volt-Watt mode depending on the type of DER. An example curve is shown in Figure 2.2, with reactive power injected when active power is absorbed and reactive power absorbed when active power is injected. The last mode of the reactive power modes is the Constant Reactive Power mode which sets a single, fixed reactive power output when the mode is active. It is important to note that these four reactive power modes are mutually exclusive; one and only one may be selected at a time [8].

For the active power mode, there is only one option, which is the Volt-Watt mode. As the name suggests, the active power is dependent on the voltage readings based on the current PCC voltage. Only mandatory in Category B DER, this mode can be enabled or disabled while one of the above reactive power modes is enabled. An example of the curve with default setpoints for this mode is shown in Figure 2.3, with maximum active power injected at the nominal voltage and below, and absorbed only when the PCC voltage is higher than the nominal voltage (nominal voltage is set as 1 p.u.). Note that this curve is for DER that are able to both inject and absorb reactive power. For the DER only able to inject power, the curve would have no absorption levels below the x-axis, and instead have lower injection levels for higher voltages.

Since the active power mode may be on or off as determined by the AEPS

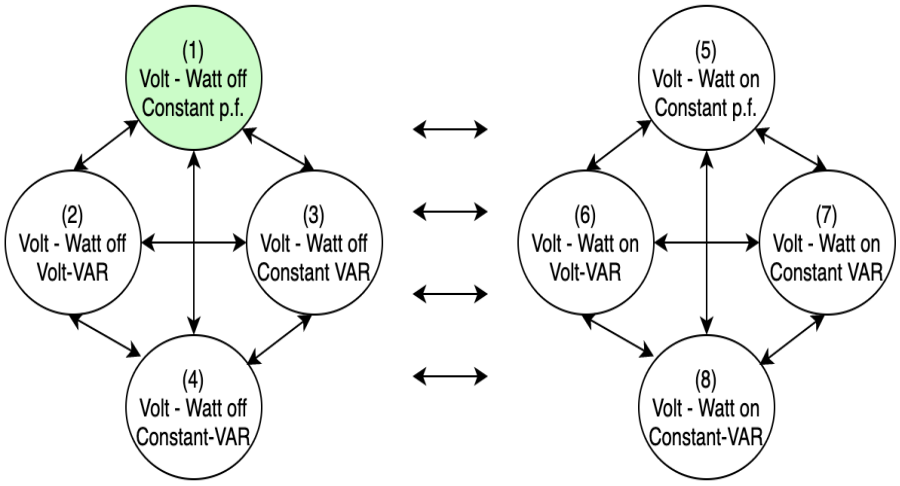


Figure 2.4: State representation of all the possible mode combinations

operator, there are 8 possible combinations for modes. Figure 2.4 depicts the modes as different states numbered from 1 to 8 where states 1 to 4 on the left side are where the active power mode is off, and states 5 to 8 are where active power mode is on. State 1 highlighted in green is the default state as defined in the standard with Constant Power Factor mode on and active power mode off. Note that states 1 to 4 can go to any states from 5 to 8 and vice-versa. This is shown by the help of bidirectional arrows. As will be shown later in this thesis, certain combinations of modes may result in a situation where a voltage instability is introduced or exacerbated. In other words, jumping from a certain state x to state y might be deemed harmful and the adversary can exploit this to cause instability in the system. Also, since the set-points for all the modes discussed above are adjustable within certain limits, this adjustability exposes the system to potential adversary attacks which shall be discussed more in Chapter 4.

2.4 Ride-through and trip settings

The rise of renewables also gives rise to fluctuations in the generation due to the intermittent nature of sources of energy for renewables such as wind and solar. The same can be said for consumption due to variation in the load. The famous duck curve portrays very well how load profiles can be variable,

and lots of forecasting tools have been pursued to predict how generation can be coupled with consumption [20].

In addition to this capricious nature of loads and generation, different disturbances can cause the overall grid to be unstable, and voltage and frequency might not operate in nominal ranges. Breakers are usually designed to detect such fluctuations and take necessary actions accordingly. As previously discussed, when IEEE 1547 was written in 2003, tripping off DER when they faced any fluctuations would have sufficed to avoid further damage. The abnormality in voltages and the degree of change over time that can be sustained by devices led to the development of Computer and Business Equipment Manufacturers Association (CBEMA) and Information Technology Industry Council (ITIC) curves [21]. Hence, ride-through and trip settings are important in monitoring the power quality to increase the longevity of electronic devices. However, with the rise of DER, the standard should be able to define allowable ranges and times for DER to sustain ride-through

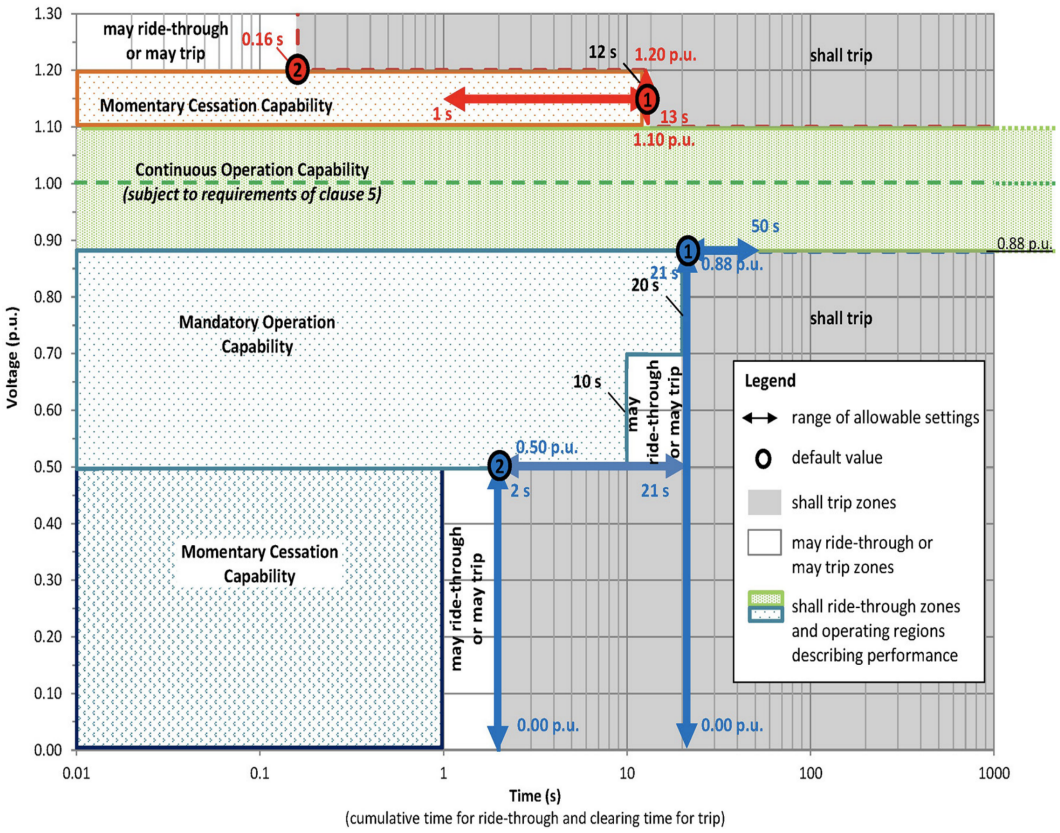


Figure 2.5: DER response to abnormal voltages and voltage ride-through requirements for DER of abnormal operating performance Category III [8]

during abnormal conditions to avoid loss of multiple DER.

Ride-through settings are therefore mandatory and they specify the amount of time that a DER must remain connected to the AEPS during voltage or frequency disturbances of certain magnitudes. The trip settings are adjustable by the AEPS operator and it specifies the maximum allowable times to compulsorily disconnect at times when nominal voltage or frequency thresholds are way beyond the nominal values. In the range of voltage and frequency between the ride-through requirements and the trip settings is a grey area where the DER may trip or may ride through, depending on how conservative the trip settings are [22]. The standard lists three different categories for varying ranges of tripping and ride-through settings. To take an example, consider the voltage ride-through and trip settings for a Category III DER as shown in Figure 2.5. While Category A and B classify DER based on the reactive power and mode functional capabilities, Category I, II, and III classify DER based on different ride-through and trip settings. The reason Category III is chosen for the devised use cases is because this has the least complicated ride-through and trip settings, and is the most permissive setting among the three categories. The significance of permissive settings becomes more evident when designing use cases and mitigation strategies.

The horizontal dashed line with y-axis as 1 p.u. denotes the nominal state with no voltage deviations, and all these voltage regions apply at the RPA. If the voltage stays between 0.88 p.u. and 1.1 p.u., DER do not have to trip and can ride through for an infinite amount of time. If the voltage is between 1.1 p.u. and 1.2 p.u., then the DER has to ride through for 12 s. However, if the voltage is more than 1.2 p.u., it has to trip within 0.16 s. Similar logic applies to undervoltage conditions where the DER has to ride through for 21 s for voltages between 0.88 p.u. and 0.70 p.u., and for 10 s for voltages between 0.5 p.u. and 0.7 p.u.. A similar idea is applied to Category I and Category II with different settings.

Note that the default trip and ride-through settings as defined in the standard are used. Changing trip settings may cause adverse effects. The effects of these changes are not discussed in detail in this thesis, although they are the subject of ongoing work.

2.5 Attacks on the DER interface

A part of the smart grid movement is the requirement to have proper communication interface with and among the DER. This project's scope is limited to attacks being made through changing commands via communication interface to the DER. Communication with the DER can happen via various industrial protocols. IEEE 1547 particularly identifies IEEE2030.5, DNP3, 61850 GOOSE, and Sunspec Modbus [8]. Adverse attackers would be using these protocols to exploit the communication interface.

It is possible that bad combination of modes or incorrect setpoints and commands leading to an unstable system could be the result of an accident or initiated by an attacker with access to communication interface. Most of the work of this thesis is concerned with the aftermath of receiving a malicious command and is less concerned about the technical communication and network details. However, other members of the team are looking into relevant communication protocols, possible attacks through man-in-the-middle or spoofing mechanisms, and possible mitigation strategies revolving around strong firewalls and data inspection tools.

Chapter 3

SYSTEM DESCRIPTION

The criteria and requirements of the IEEE 1547 standard are applicable to all distributed energy resource technologies interconnected to EPS at typical primary or secondary distribution voltage levels. As specified in Chapter 2, the scope of the standard lies in the communication between the AEPS and local EPS which could be DER, load, or the combination of both. Figure 3.1 shows various types of EPS involving DER and loads. The example of Local EPS 1 includes only load. Any requirements for this Local EPS are outside the scope of this standard.

The example of Local EPS 2 includes only DER. The DER unit in this ex-

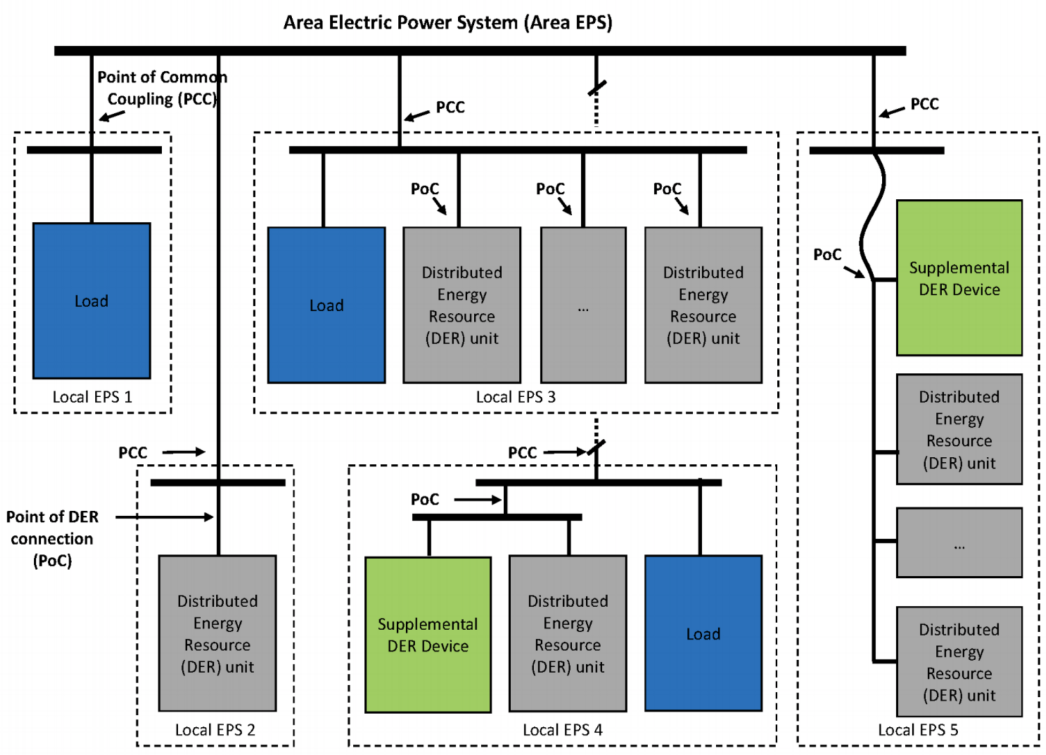


Figure 3.1: Simplified model consisting of two DERs connected to the AEPS [8]

ample is able to meet requirements at its terminals without any supplemental DER device. The example of Local EPS 3 includes both DER units and load. The DER could be multiple and they are able to meet requirements at their terminals without any supplemental DER device. Supplemental devices are additional devices used to satisfy DER functionalities as mandated by the standard in the case where DER is not self-sufficient [8]. The example of Local EPS 4 includes a DER unit, a supplemental DER device, and load. The example of Local EPS 5 includes two (or more) DER units and a supplemental DER device but no load. The curved line indicates that the PCC and PoC may be located well apart from each other. Note that for all types of Local EPS, depending on the aggregate DER units' rating and the percent of average load demand, requirements of the standard (voltage, frequency, trip and ride-through) apply either at the PCC or the PoC [8]. The main difference that sets apart DER from microgrids is that a DER may not necessarily be self-sustaining whereas microgrids are assumed to be self-sustaining.

Figure 3.2 shows a simplified system diagram with two DER circuits connected to a larger AEPS. Each equivalent DER circuit may be thought of as a DER plant (i.e. aggregate offshore wind or aggregate residential solar), a microgrid with DER sources, or an individual DER. For the purposes of this thesis, the focus is on DER that individually or combined make up a large portion of the AEPS capacity. It is also of interest to see how DER may have an impact on the bulk power system, but for preliminary studies, the focus is on medium voltage systems.

For each DER circuit, a controller such as the eMesh SCADA from Hitachi ABB Power Grids could act as both the substation remote terminal unit (RTU) for all the communications within the DER circuit, and also as a gateway that provides the local DER communication interface to the AEPS operator [23]. The DER mode changes, curve parameters, tripping and ride-through settings shall be all set by the AEPS operator using the local DER communication interface for each of the DER circuits per the configuration and management information as defined in the standard. Along with sending configuration and management data, the AEPS operator shall also be able to receive nameplate and monitoring information from each of the DER circuits through their respective local DER interface. Finally, the major assumption in all the following use cases is that the attacker only has access to the information exchange between the AEPS and the local DER communication

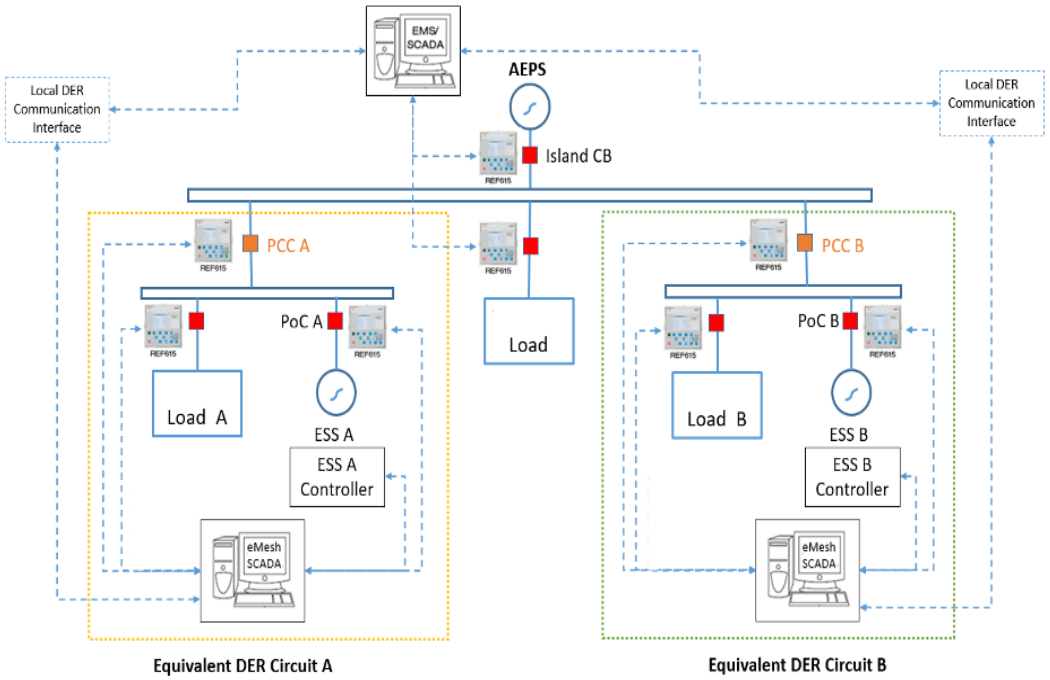


Figure 3.2: Simplified model consisting of two DERs connected to the AEPS [22]

interface.

Each DER circuit consists of an inverter-controlled energy storage system (ESS) that is capable of generating and absorbing both active and reactive power. In Simulink, the AEPS is modeled as a three-phase synchronous generator source separated by a 10 km line from the two ESSs as direct current (DC) voltage sources to simplify use case application and to utilize absorbing and injecting functionalities of storage systems. The reason for having two DERs instead of just one is to enable sophisticated mode changes that could possibly take advantage of power-sharing between the two DERs [22]. Also, the idea of having multiple DERs becomes useful when it is necessary to plan possible mitigation strategies where one DER might be compromised and the other one can help to maintain the stability. Though not discussed in this thesis, power-sharing becomes more relevant when considering islanding conditions where AEPS requires support from DER to serve its load.

For this model description, each DER is provided a rating of 400 kVA and the size of the AEPS is set as a variable ratio to the aggregate power rating of the two DERs. This is done to test various levels of DER penetration.

AEPS apparent power rating is defined by the variable AEPS rating where

$$AEPS\ rating = \frac{2(400 \times 10^3)}{DER\ percent} \tag{3.1}$$

In the cases where there is low DER penetration, for instance, less than 1%, AEPS rating stays high which corresponds to a stiff grid. For such cases, a stiff AEPS might act like an infinite bus with a fixated voltage of 1 p.u. However, considering the rise of penetration of renewables in the form of DER, the ratio of DERs/AEPS is going to be higher as time progresses. This is going to make the AEPS rely on DER for its overall stability and health. Moreover, any change in DER is going to change the trajectories of voltage and frequency at the PCC. The increase in DER penetration also means that the AEPS is now more vulnerable to attacks or disturbances on DER. DER could come in the form of photovoltaic (PV) inverters, wind plants, or just ESS. These renewable resources are able to inject and absorb reactive power through the use of smart inverters [24]. Ideally, for a system like a PV plant, they would use MPPT to maximize the active power output. However, as discussed in Chapter 2, when demanded from the AEPS operator, DER operators might have to curtail their active power output to be able to regulate reactive power. To simplify the system, two DERs as ESS are assumed to have the minimum reactive power capability of Category B DER as defined in the standard. This allows the implementation of the use cases without having to worry about power curtailment requirements [22].

The controllers in both DERs consist of a grid-feeding converter and a control layer governing mode change functionality, namely mode changes or adjustments to the curve parameters [22]. In addition to be able to change DC to alternating current (AC), inverters are now also required to have this new mode change functionality as per the new IEEE 1547 standard. In the case of grid-feeding converters, the reference values for currents are usually provided by a power controller that regulates the active and reactive power delivered to the grid [25]. For this system model, the power controller is tied to a MATLAB script which is scripted to have mode change functionality. Whenever, any mode is chosen, the Simulink and MATLAB script communicate with each other to provide the power output reference values depending on the mode chosen. The standard gives default setpoints for all the modes. These default set-points were used to define functions in the MATLAB script

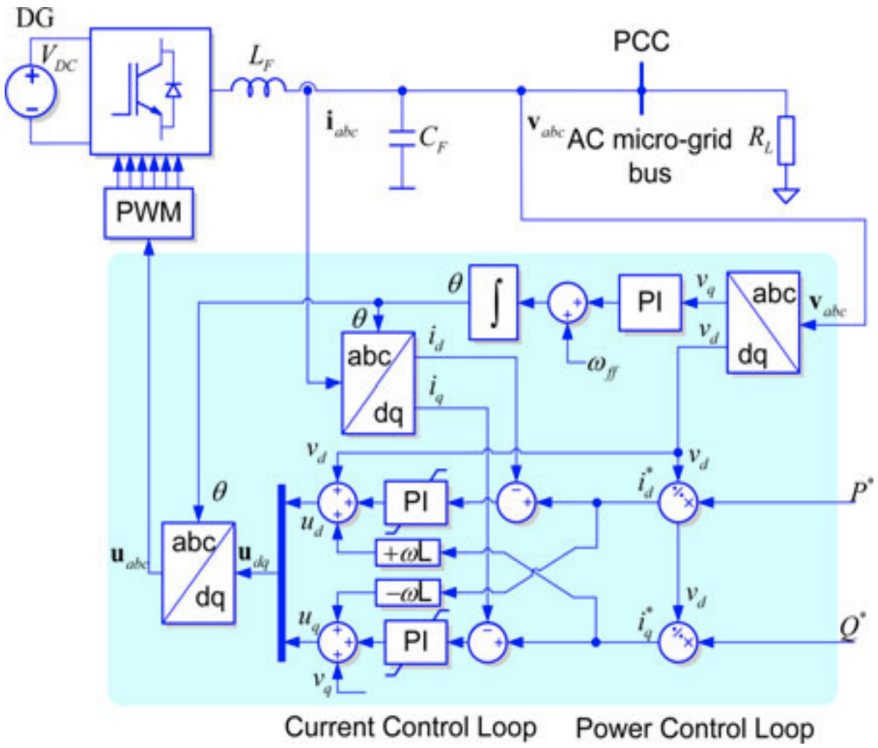


Figure 3.3: Basic control structure in a three-phase grid-feeding power converter [25]

to determine active and reactive power setpoints. Once the active and reactive power values are determined based on the mode combinations, these values serve as reference values for calculating the required current values to be set by the inverter. The instantaneous active and reactive power components are defined by

$$p = v_d * i_d + v_q * i_q; \qquad q = v_d * i_q - v_q * i_d \tag{3.2}$$

This implementation of current controllers based on the dq synchronous reference frame is commonly used in the control of AC currents in three-phase systems [25]. The abc phase voltage coordinate system is converted to $dq0$ reference frame where v_0 is zero, v_q component is driven to zero, and v_d is simply the transformed voltage coordinate at the PCC. The equation thus simplifies to

$$i_d = \frac{p}{v_d}; \qquad i_q = \frac{q}{v_d} \tag{3.3}$$

These i_d and i_q reference values are then fed to the converter as shown in

Figure 3.3 where i_d and i_q go through proportional integral (PI) controllers to match the reference values with the measured value. After that, the reference values goes to pulse width modulation (PWM) and the filter to finally connect to the AC grid, which in our case, is the AEPS.

In order to enable tripping and ride-through requirements, the AEPS and two DERs have circuit breakers (CB) tied to distribution lines. A pi-circuit transmission line model is used in Simulink to model the transmission line parameters. Length of the transmission line between the AEPS and the point of connection of DERs, is assigned to be 10 km. From the common point of connection to two individual DERs, both transmission lines (from PCC A to PoC A and PCC B to PoC B as shown in Figure 3.2) are assumed to be 0.5 km. This corresponds to a very small impedance that amounts to less than 0.5% of the DER's rated apparent power and voltage. Therefore, as discussed in the previous section, the reference point of applicability for this system model can be either the PoC or the PCC. This is evident when the same voltage and frequency readings are measured at PoC and PCC because of a short transmission line of 0.5 km with a low impedance. However, if the transmission line was long and it exceeded the 0.5% threshold, different readings would be seen at the PoC and the PCC [8].

All the loads in both the DERs side and the AEPS side are modeled as constant loads consuming active and reactive power. In realistic scenarios, the load profiles keep changing. The reason loads are modeled as constant is to avoid mixing variables that change the trajectory of voltage and frequency. Since the target is to see how certain use cases affect the system, using constant loads guarantees that any changes seen in the system's states are due to the effect of implementation of those attack vectors from those use cases. Having said that, depending on the use case, the constant load is changed in such a way that the solution converges for all DER penetration levels for any particular setup.

For the solver, Simulink's powergui tool is used to discretize the system for a solution at fixed time steps, and the Tustin/Backward Euler method is used to carry out the simulations [26].

Chapter 4

USE CASES AND ATTACK DESCRIPTION

Most of the time on this project was spent on devising the use cases to be able to capture different attack vectors resulting from the communication interfaces. Some of the use cases revolve around the idea that the AEPS operator can access most of the real-time monitoring information from the DER circuit. Thus, there could be scenarios where the attacker maliciously falsifies some or all of the monitoring information from the DER circuit causing possible system instability and tripping. One of the items of monitoring information that is provided to the AEPS operator via the local DER communication interface is the operational state of charge of the DER circuit which can be falsely communicated by an adversary to potentially cause local load shedding in the DER circuit along with possible frequency instability at the PCC. Similarly, there could be multiple other use cases of false data injection (FDI) which is part of an extensive work by other colleagues working in the IEEE 1547 project.

Few other use cases revolve around the idea of changing combination of modes or changing the set-points of Volt-Watt, Watt-VAR, Volt-VAR, and Volt-Watt curves. Though the standard has default curves, the setpoints can be changed by the AEPS operator within a predefined range and the adversary can utilize this range of setpoints to cause adverse impacts. For example, when operating on Volt-Watt mode, with both DER and AEPS on low load conditions where DER are absorbing power from the AEPS, the curves can be changed in the such a way that DER go from absorbing some active power to absorbing zero active power. This change in operating mode of the DER circuit from absorption (acting as a load) to no power output further exacerbates the high voltage conditions at the PCC, causing high voltage trip conditions and disconnecting the DER circuit from the AEPS. In a situation where the AEPS was reliant on the DER circuit to perform voltage regulation, the sudden tripping of the DER circuit can cause localized

voltage instability issues on the AEPS. In the situation that this command can be sent to many DER simultaneously, the high voltage scenarios that cause tripping may trip off enough DER to have a significant impact on the AEPS. Following the same notion, it is imperative to realize that system topology is going to change the intensity of the aftermath of an attack be it through changing the combination of modes or changing the curve parameters. Possible attack vectors on the popular Volt-VAR curve and attack due to malicious change in combination of modes are discussed in detail in this chapter.

For all the use cases described, the magnitude of the voltage depression varies with the dependency of AEPS on both DERs for active and reactive power support. The use cases that will be discussed in detail are change in modes or curves in reactive power modes. However, enabling the Volt-Watt mode is not necessary to carry out these reactive power mode attacks. In the case where Volt-Watt mode is off, the active power reference would come from a tertiary controller, such as the MPPT, and is usually close to the rated power.

The attack is split into two different steps. The first DER receives the mode change or curve change malicious command at 2 s, and the second DER receives the same malicious command at 5 s, depending on the use case. These two time stamps are arbitrarily chosen and similar results are obtained for any other arbitrarily chosen time stamps as well. This attack strategy models a situation where the adversary changes the mode of all the connected DERs, not precisely simultaneously, but within a short interval and hence imitating a potential common mode change attack. Per unit convention is used throughout the text and figures except for simulation results in Chapter 5 for frequency and reactive power output from both DERs. The base value for apparent power is 400 kVA, and for voltage is 12 kV.

4.1 Change of set-points in Volt-VAR mode

The DER is assumed to be operating at the very commonly used Volt-VAR mode which is one of the reactive power modes. Knowing the system dynamics is advantageous from the attacker's standpoint but is not a necessary condition to carry out the attack. The attacker can simply randomly change

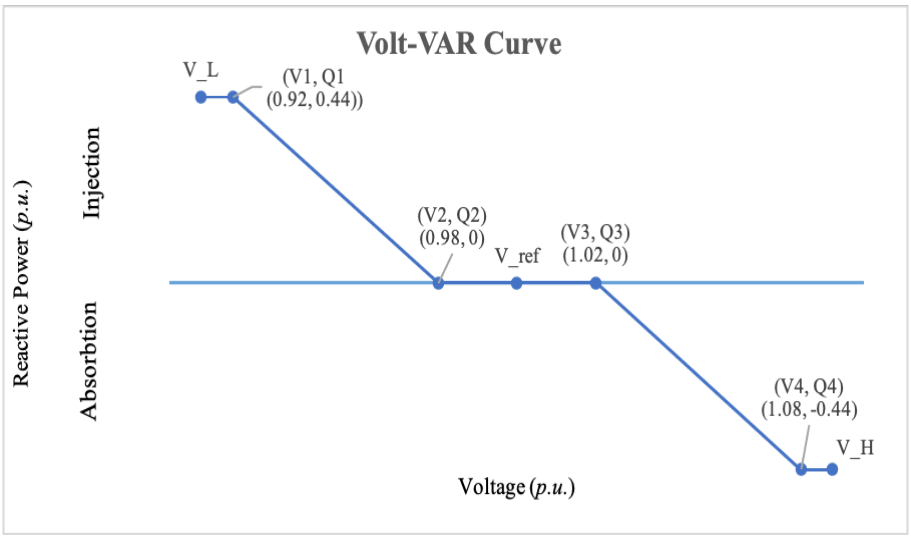


Figure 4.1: Associated curve for the default Volt-VAR mode

the set-points of the Volt-VAR curve so that these settings are used to control the reactive power output. If the DER is not operating at Volt-VAR mode, the attacker can always change the mode to Volt-VAR before maliciously changing the curve settings. A default curve shape is shown in Figure 4.1 with Category B's default settings. In this situation, reactive power is injected in low voltage situations, which drives the voltage up towards nominal, and reactive power is absorbed in high voltage situations, which drives the voltage down towards nominal. However, there is a lot of leeway in the Q and V setpoints, recognizing that based on the placement of the DER in the AEPS, there may be a need to inject or absorb reactive power at nominal voltage to correct for losses, or other unusual situations. A few malicious curves that could be set by an attacker are theorized.

4.1.1 Manipulated Volt-VAR sawtooth curve

One of the most generically damaging settings would likely be a malicious curve, as shown in Figure 4.2 where a very small deviation from nominal voltage (between the range of V_1 and V_4) will cause swift changes in reactive power output. Not only that, but a drop in voltage will cause reactive power to be absorbed, which will further drive the voltage downward. Similarly, with this malicious curve, an increase in voltage will cause reactive power to be injected, which will further drive the voltage upward. As discussed

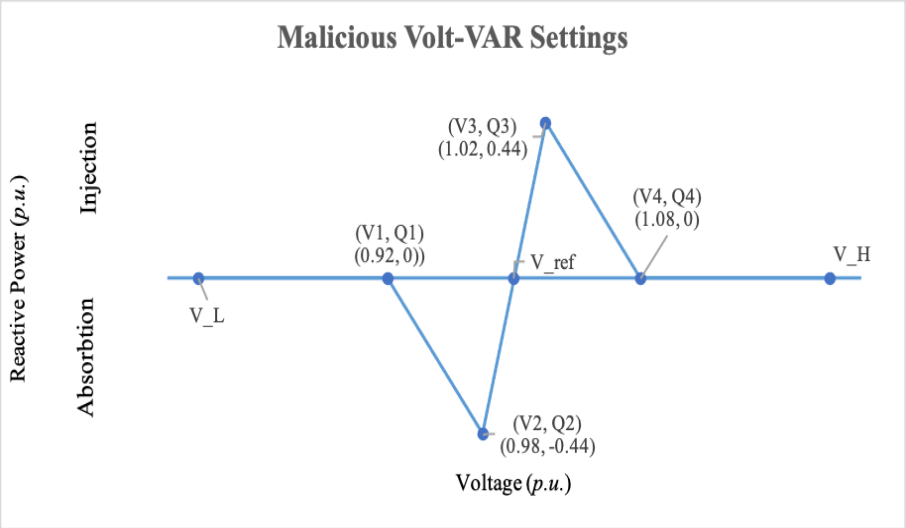


Figure 4.2: Curve for Volt-VAR mode after the malicious setting

earlier, the AEPS operator can change the ride-through and trip parameters; therefore, the attacker can set the undervoltage and overvoltage tripping requirements narrowly which would result in DER tripping off sooner that they are supposed to. This results in untimely tripping of DER even under narrow voltage fluctuations. Note that there could be multiple combinations of curves for this malicious setting with different slopes by changing the range for the voltage as well.

4.1.2 Manipulated Volt-VAR curve to drive up the voltage

There are other possible settings that could also cause a similar, but more targeted effect. For example, the settings in Figure 4.3 have all voltages set at their maximum setting ($V_{ref} = 1.05$ of V_N and V_1, V_2, V_3, and V_4 set at the high extrema of the given allowable range as defined in the standard), and all reactive power at their maximum levels (100% injection for all points except Q_4, which has a maximum setting of 0). This means that for all voltages below 1.08 p.u., the DER will inject maximum reactive power, driving the voltage upwards. Above 1.08 p.u. reactive power will still be injected, at lower rates, up to 1.23 p.u. voltage. Again, tripping requirements can be set conservatively so that the system will be forced to trip [8]. These settings could potentially be even more effective as an attack than the first. Despite any external voltage deviations, the system will still inject maximum reactive

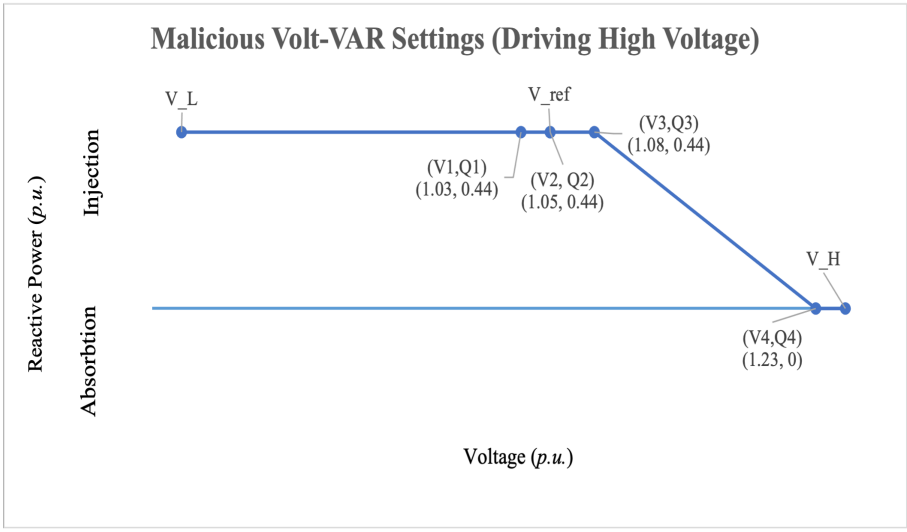


Figure 4.3: Manipulated Volt-VAR curve to drive up the voltage

power at nominal voltage, which will start to drive the voltage up.

4.1.3 Manipulated Volt-VAR curve to drive down the voltage

Similar to the curve described above, the attacker can change the curve in a way to drive the voltage down. For example, the settings in Figure 4.4 have all voltages set at their minimum setting ($V_{ref} = 0.95$ of V_N and V_1, V_2, V_3, and V_4 set at the low extrema of the given allowable range as defined in the

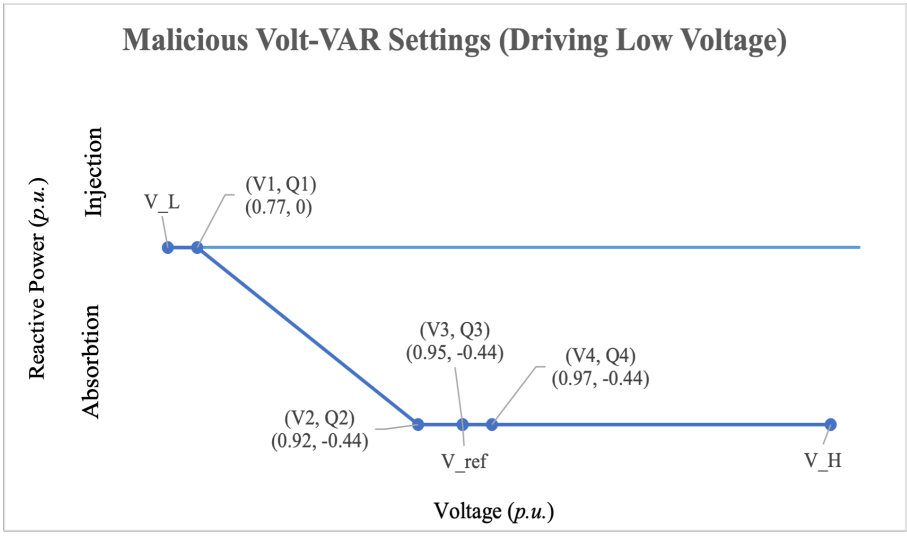


Figure 4.4: Manipulated Volt-VAR curve to drive down the voltage

standard), and all reactive power at their minimum levels (100% absorption for all points except Q_1, which has a minimum setting of 0). This means that for all voltages above 0.92 p.u., the DER will absorb maximum reactive power, driving the voltage downwards. Below 0.92 p.u., reactive power will still be absorbed, at lower rates, up to 0.77 p.u. voltage. This might be more dangerous than driving the voltage high because the default tripping setting for a Category III DER is 0.88 p.u. for undervoltage condition to ride through for no more than 21 s. This is a difference of just 0.12 p.u. from the nominal versus a difference of 0.20 p.u. (for overvoltage threshold of 1.2 p.u.) for the default trip settings for a Category III DER. Thus, even without changing the default tripping settings, the adversary can cause low voltage situations that could lead to tripping of DER.

4.2 Malicious change of contradictory modes

Following the standard, the DER circuit can have simultaneous enabling of the Volt-Watt mode along with any of the reactive power regulation modes. As discussed in Chapter 2, Category B is used in areas with higher DER penetration. Since varying levels of higher penetration of DER were considered in these simulation studies, both of the DERs are assumed to be of Category B. Also, Category B mandates all the modes. Two different scenarios are considered to demonstrate the use case and attack description. Both scenarios have the same attack path but different initial conditions. This use case is relevant because the system begins with default conditions for the DER in a typical operating normal grid system [22]. The attacks described in the following sections could relate to either an adversary or just a human error.

4.2.1 Scenario 1: Both DERs operating with Volt-Watt mode on and Constant Power Factor of 1

The default operating mode, as defined in the standard, is the unity power factor mode and it resembles a scenario where voltage and frequency are at nominal values and the system does not need support from DER. The active power output is being regulated by Volt-Watt mode, and Constant Power Factor mode is regulating the reactive power output at the PCC. In the case

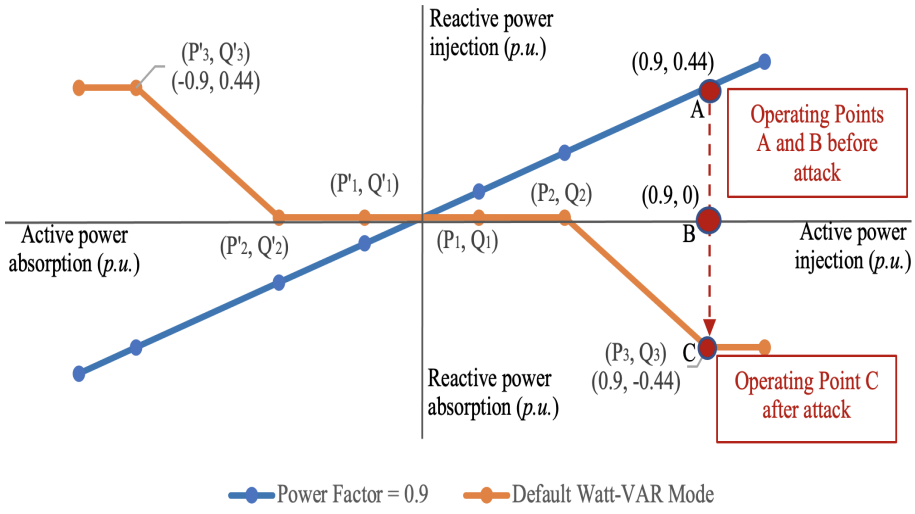


Figure 4.5: Attack showing change from Constant Power Factor mode to Watt-VAR mode [22]

where Volt-Watt is disabled (as it would be as the default setting for active power mode) and active power output is close to the rated power, this use case would still remain valid. Note that a unity power factor means that the DER circuit is not providing any reactive power support into AEPS. This operating point is visible as point B in Figure 4.5.

The adversary sends a command to change the reactive power regulation mode from Constant Power Factor to Watt-VAR without changing the Volt-Watt setting. Figure 2.3 shows the regulation curve for the Volt-Watt mode, where DER circuit would be generating the maximum rated active power P_1 at a voltage near or below the nominal 1 p.u. voltage. Note that the curves are flexible, but default settings for Volt-Watt and Watt-VAR modes are considered. When the mode changes from Constant Power Factor to Watt-VAR, the active power output, determined by the Volt-Watt curve, governs the reactive power output. Since Volt-Watt mode specifies maximum power injection for any voltage near or below nominal, maximum real power injection is expected. As shown in Figure 4.5, the system goes from point B to point C after the attack, where point B is the operating point before attack of a Constant Power Factor mode of 1 injecting rated active power of P_3 and zero reactive power. According to Watt-VAR mode, the reactive power output of Category B DER would be set to maximum reactive power absorption, or -0.44 p.u. at point C (P_3, Q_3) on the Watt-VAR curve assuming the

apparent power rating of 1 p.u.. The change from the DER acting as a neutral reactive power asset to absorbing maximum reactive power causes a voltage depression at the PCC, and as DER penetration rises, the system may enter an unstable operating region [22].

4.2.2 Scenario 2: Both DERs operating with Volt-Watt mode on and Constant Power Factor of 0.9

A more severe scenario is imagined where the starting mode has both DERs operating at a power factor of 0.9. A high DER penetration increases the probability of all emergency scenarios concerning over- or under-voltage voltage situations because certain DER (solar, wind, etc.) are unpredictable and intermittent [27], [28], [29], [30]. Undervoltage scenario could occur if these resources produce less generation than projected. DER capable of injecting power should be able to inject during situations as such [31]. Undervoltage scenarios are typically solved with complex load shedding since large generators cannot ramp up quickly enough to fix the power mismatch [32], [33], [34], [35]. However, if DER were being used to inject both active and reactive power instead of performing load shedding, the reliability of the system would be better. Therefore, this scenario is considered where two DERs are operating as generating sources providing both active and reactive power support in response to a system with higher load demand, specifically higher reactive load demand. This scenario is shown as operating point A in Figure 4.5.

Similar to what was explained in Scenario 1, the adversary sends a command to change the reactive power regulation mode from Constant Power Factor to Watt-VAR while the Volt-Watt mode is still active. According to Watt-VAR mode, shown in Figure 2.2, after the attack of mode change has been made, the final reactive power output would be set to point C which is maximum reactive power absorption, or -0.44 p.u. at (P_3, Q_3) on the Watt-VAR curve after starting at point A, which is the Constant Power Factor of 0.9. It can be postulated that the aftermath of this scenario will be worse than the previous scenario, because the starting point with injection of reactive power from both the DERs allows the system to start with higher load.

When the attack occurs and there is a sudden loss in reactive generation, the AEPS becomes responsible for supporting even more reactive power since the system started with a higher base load [22]. This will result in a voltage depression at the PCC. In the condition where the net reactive power load, the sum of base load and DER absorbing power, becomes large enough, the system will cease to collapse. This is because AEPS will not be able to support as many DER absorbing reactive power as in Scenario 1; system collapse is expected to occur even under lower DER penetration.

4.3 Unfavorable regions

Another consideration is the unfavorable regions in the curves of Volt-VAR or Watt-VAR mode. Taking Volt-VAR curve as shown in Figure 4.1 as an example, with y-axis drawn vertically at the V_{ref} point, anything in the first and third quadrant is unfavorable. This is because as the voltage increases, it is not wise to further increase the voltage by injecting the reactive power. Similarly, as voltage drops below the reference voltage, it is not wise to absorb the reactive power and further decrease the voltage. Knowing unfavorable regions like these helps in the mitigation strategies where a simple rule based algorithm could avoid attacks that fall into these unfavorable regions [36].

For the other use case mentioned above, the nature of point C in Figure 4.5 is unfavorable. It is evident that DER operating at point C act as reactive power load consumption. The system remains stable with a low penetration of DER operating at point C. However, as the ratio of DERs/AEPS increases, the AEPS will not be large enough to provide enough reactive power to maintain a nominal voltage trajectory even after performing load-shedding to the existing load in the system. To demonstrate this, 10 differently deterministic simulations from point B to point C with varying power factors are considered to gauge the power factor and DERs/AEPS ratio at which the system will end up operating in an unstable state. This is done for both load and no load situations. To begin, it is assumed that the system is operating as described in Scenario 1 with unity power factor with load on. This system with load on is referred to as Situation 1. Then, the power factor is decreased in the direction that follows from B to C with varying level of DER penetration. The same procedure is repeated on a system that undergoes load-shedding

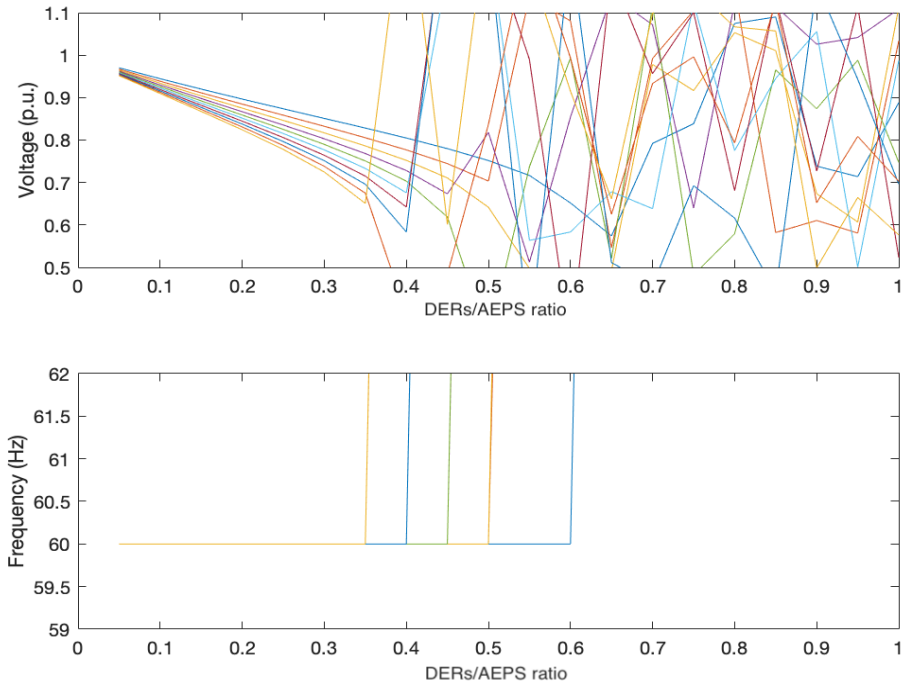


Figure 4.6: Voltage trajectory for different DERs/AEPS ratio and different power factors for Situation 1

and that system is referred to as Situation 2.

Figure 4.6 shows Situation 1 and Figure 4.7 shows Situation 2. Both figures have ten differently colored lines for different power factors from 0.99 to 0.9 in the negative direction from B to C in the decrements of 0.1. The top blue line in Figures 4.6 and 4.7 represents 0.99 p.f. and the bottom one represents 0.9 p.f.. The horizontal axis consists of varying level of DER penetration with DERs/AEPS ratio ranging from 0 to 1. The voltage and frequency for each DER penetration level (ranging from 0% to 100% in the increments of 5%) for different power factors are sampled and then plotted in MATLAB. Looking at the charts, it is obvious that the situation worsens as the power factor is decreased and as the DERs/AEPS ratio is increased. Referring back to Figure 4.5, the decrease in power factor from B to C translates to both DERs generating active power and absorbing reactive power. As it approaches closer to C, DER demand higher reactive power absorption which corresponds to depression in voltage. This is what is reflected in Figures 4.6 and 4.7.

Another dimension to note is that the magnitude of depression depends on the ratio of DERs/AEPS. For instance, a low ratio of one or less than one percent is too minuscule to cause any voltage depression due to the reduction in the operating power factor of the DER. In fact, DER are commonly operated under Constant Power Factor mode or the power factor is adjusted according to the active power feeding of the generating unit [37]. Thus, for a low DER penetration, lowering power factor might not cause any significant stability issues. However, as the DERs/AEPS ratio increases, the magnitude of depression increases because then the system would be relying on DER for reactive power. All DERs operating at this region of absorption would surely depress the voltage. Hence, the depression is higher for high DER penetration for all the power factors and gets worse for lower power factors. The oscillations seen towards the end for higher DER penetration are the results of voltage collapse due to high depression.

Note that the difference between Figure 4.6 and Figure 4.7 is that they are representing Situation 1 and Situation 2 respectively, where Situation 1 has

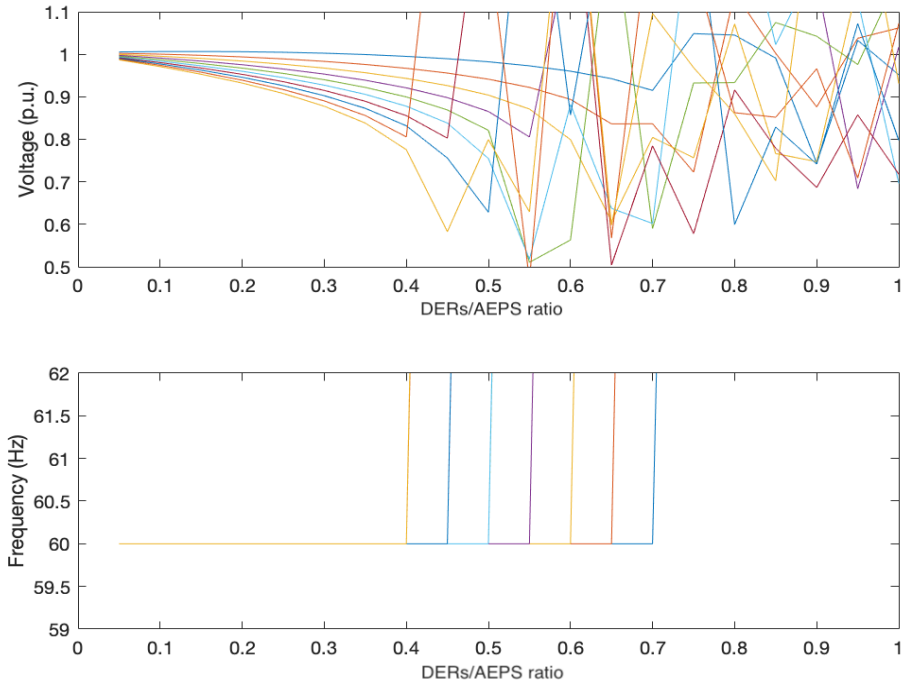


Figure 4.7: Voltage trajectory for different DERs/AEPS ratio and different power factors for Situation 2

load and Situation 2 has no load as a result of load-shedding . Load-shedding is a common solution when voltage depression occurs and is analogous to the use of under-frequency load-shedding in other circumstances. As with under-frequency load-shedding, undervoltage load-shedding provides protection for unusual disturbances outside planning and operating criteria [38]. Though load-shedding is not the most viable solution for voltage depression, this scenario is used as Situation 2 to demonstrate the outcome even after performing load shedding. It is clear that the magnitude of voltage depression is significantly decreased for Situation 2 due to the load-shedding. However, as shown in Figure 4.7, as the power factor decreases and DER penetration increases, load-shedding will no longer be a viable solution. Thus, mitigation strategies involving the knowledge of the state of the system and DERs/AEPS ratio are needed in blocking attacks that are deemed to cause instability.

Chapter 5

SIMULATION RESULTS AND FINDINGS

Two hundred different Monte Carlo simulations were conducted with varying DER penetration for all the use cases proposed in the earlier chapter [1]. Monte Carlo is often used in reachability analysis to explore the effect on the trajectory of the states due to a change in certain parameters [39]. The parameters subject to change are the randomly generated ratios of DERs/AEPS. The trajectories that are of interest are of voltage and frequency at the PCC due to the attack over the course of time. After running the simulations, voltage and frequency are observed at the PCC because those two states serve as the indicators of stability.

The top graph in Figures 5.1 to 5.5 shows reactive power output from both DERs, measured in kVAR, over the course of 10 s with changes at 2 s and 5 s due to two-step attacks as discussed in Chapter 4. The graph in the middle shows voltage trajectory at the PCC, measured in p.u., over the course of 10 s with changes at 2 s and 5 s. And lastly, the bottom graph shows the frequency trajectory at the PCC, measured in Hz, over the course of ten seconds with changes at 2 s and 5 s.

Note that simply using deterministic methods to generate ratios of DERs/AEPS from 0 to 100 percent would have sufficed to observe the voltage and frequency trajectories for different levels of DER penetration. However, the rea-

[1]This material is based upon work supported by the Department of Energy under Award Number DE-OE0000896.

son for using stochastic method lies in finding the critical ratios of DERs/AEPS ratio to find the cut-off ratios for feasible operation under different operating conditions. This is discussed more in detail later in Sections 5.1.2 and 5.2.2.

5.1 Change of set-points in Volt-VAR mode

As was discussed previously, there could be multiple variations of attack by changing the curve of Volt-VAR mode. Three possible curve settings were considered which were implemented in Simulink to see the effect on trajectory of voltage and frequency at the PCC.

Figure 5.1 shows simulation results of the manipulated Volt-VAR saw-tooth curve, Figure 5.2 shows results of the manipulated voltage curve that drives the voltage up and Figure 5.3 shows results of the manipulated voltage curve that drives the voltage down. Each line represents a different ratio of DERs/AEPS and the effect of the curve changes on voltage and frequency at the PCC over 10 s. The top graphs in all figures show the reactive power measurements (in kVAR) from both DERs where a positive value indicates generation, a negative value indicates absorption, and 0 kVAR simply indicates neither absorption nor generation. Since both DERs were operating at Volt-VAR mode under nominal conditions (voltage of 1 p.u. and frequency of 60 Hz), no VAR support was required from either DER before the attacks.

At the 2 s mark, when the first attack takes place through malicious curve, the first DER's reactive power output rapidly changes, and at the 5 s mark, the second DER does the same. This change in the reactive power support is reflected in the voltage and frequency readings at the PCC. Note that the fast response time of power controllers is common in modern inverters due to improved power electronics [40].

5.1.1 Findings from Monte Carlo simulation

There are three potential outcomes of the simulation: continuous operation, oscillation of voltage, and trip after a sustained ride-through.

The first outcome results in the system still operating in the continuous operating mode, though at a slightly different state than the initial state.

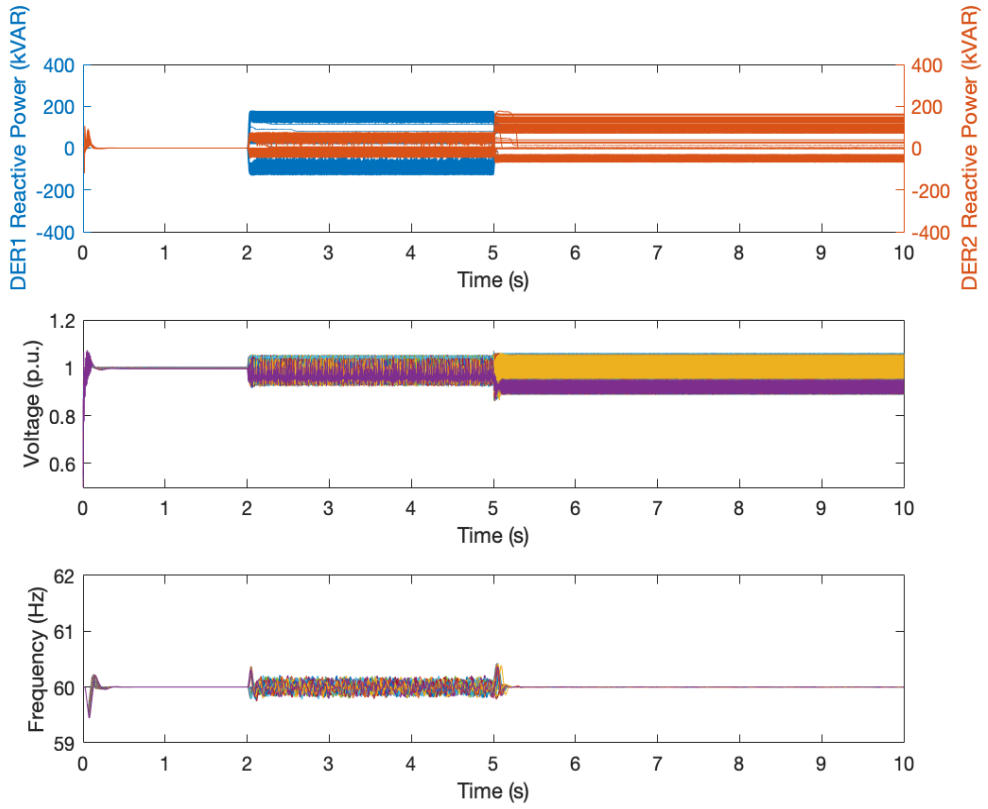


Figure 5.1: DERs operating at Volt-VAR mode being attacked with the malicious sawtooth curve

The second outcome results in the system operating within the voltage range of ride-through and trip settings but oscillating up and down within few cycles. This kind of outcome would cause a lot of stress to the grid and compromise stability.

The third outcome would be either voltage depression or high voltage depending on the type of malicious curve designed to either drive down or drive up the voltage. The time to activate trip commands varies according to the category of the DER used [8]. For this model, both DERs are assumed to be of Category III, the most robust category as defined in the standard, to show that even the DER with the most permissive default trip settings are affected by this adverse attack. For example, as shown in Figure 2.5, if the PCC voltage is between 0.70 p.u. and 0.88 p.u., a Category III DER is required to sustain undervoltage ride-through for a minimum of 21 s. Similarly, for the high voltage scenario, a Category III DER is required to sustain overvoltage ride-through for a minimum of 13 s for voltages above 1.10 p.u.. Though the

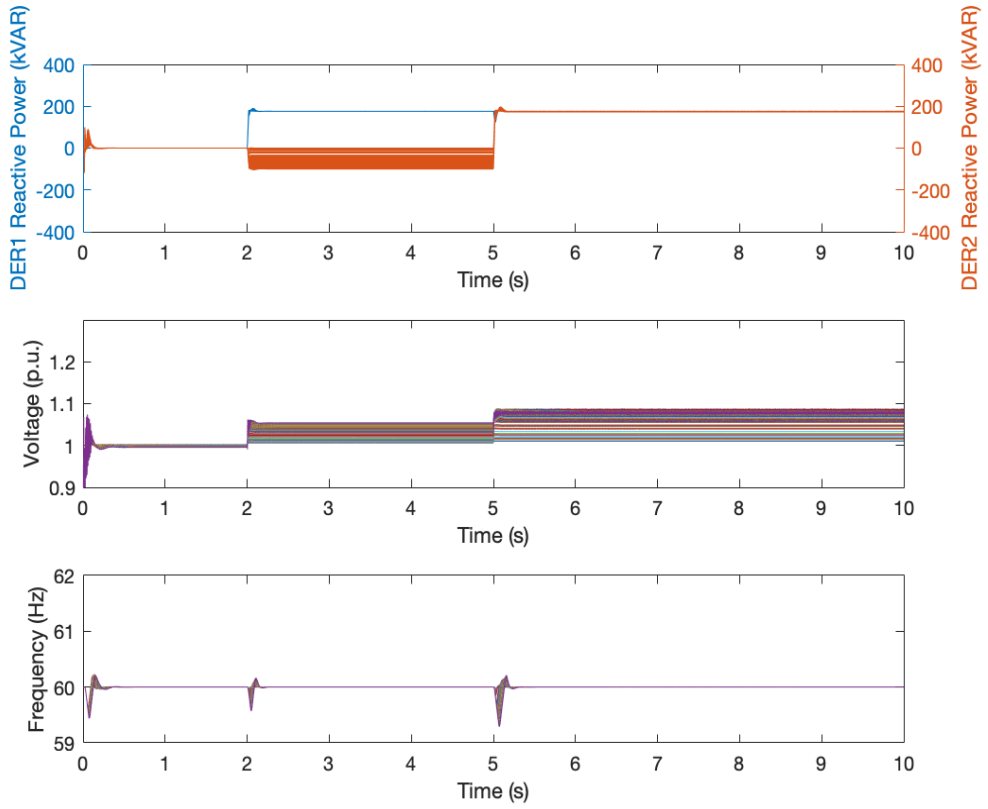


Figure 5.2: DERs operating at Volt-VAR mode being attacked to drive up the voltage

voltage results shown in simulations are only for 10 s, simulations of longer duration indicated that once the voltage drops or drives up, it does not recover. With no voltage support from other devices, the voltage depression or high voltage cannot be mitigated and hence it will trip after the ride-through.

A lot of oscillations can be seen in voltage and frequency trajectories for the malicious sawtooth curve as shown in Figure 5.1 for higher DER penetration. This makes sense looking at the shape of the malicious curve shown in Figure 4.2. Because of the slope around the nominal voltage, there are many oscillations in the states due to change of reactive power from absorption to generation and vice-versa. The magnitude of oscillations increase as the DER penetration ratio increases. The attack made at 2 s changes DER 1's reactive power mode curve to the malicious setting which, depending on the voltage trajectory, is going to either absorb reactive power (when voltage is low) or inject reactive power (when voltage is high). In response to that, DER 2 (which is not attacked yet) follows the default Volt-VAR to inject re-

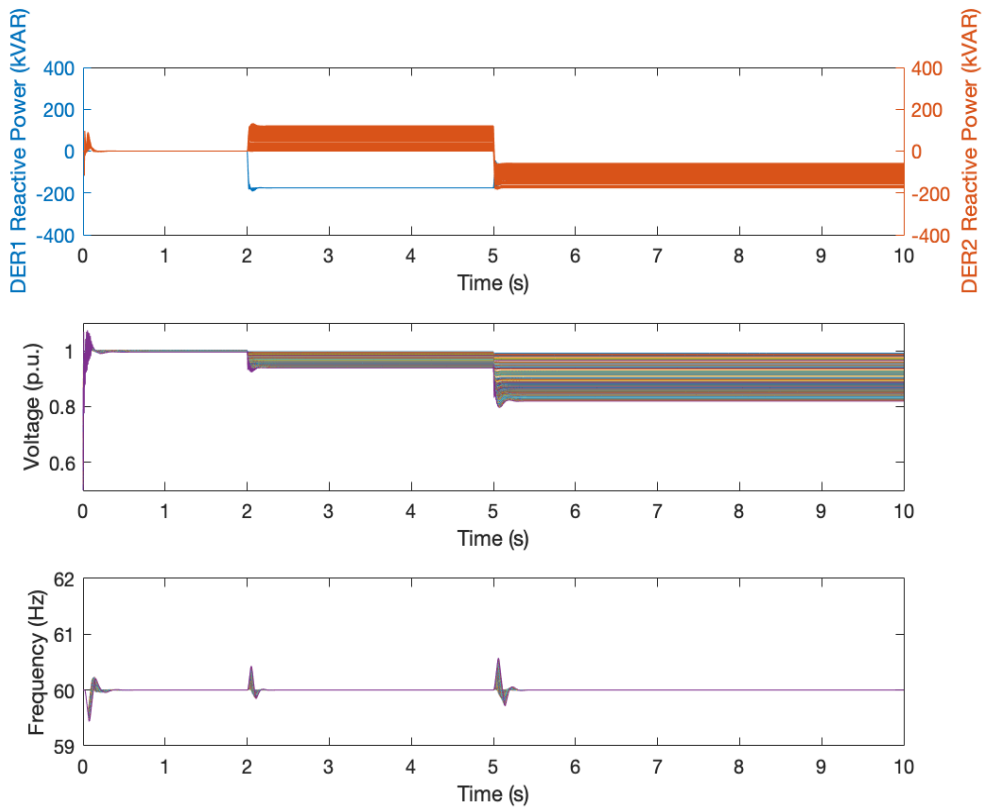


Figure 5.3: DERs operating at Volt-VAR mode being attacked to drive down the voltage

active power (when voltage is low) and absorb reactive power (when voltage is high).

This constant change causes oscillations in voltage. Though not shown in the graph, this also leads to slight change in active power output fluctuations due to Volt-Watt being enabled. The reactive power from two DERs fighting with each other coupled with slight fluctuations in active power output is the reason why more fluctuations are seen in the frequency trajectories between 2 s and 5 s. After 5 s, DER 2 also gets compromised and hence resonates with the reactive power output of DER 1. The voltage oscillations and frequency oscillations are reduced significantly but there are still fluctuations present in smaller range. The aftermath of the second attack on DER 2 results in voltages being driven either down or up.

Figure 5.2, the result of the malicious curve intended to drive the voltage up, shows voltage being driven up for all the simulations and rising with higher intensity as the DER penetration increases. This becomes more ev-

ident looking at the reactive power graph of two DERs. DER 1's reactive power shown by the blue line goes from zero injection of reactive power to full injection of 0.44 p.u. (176 kVAR) after the attack made at 2 s with the malicious curve intended to drive up the voltage. At this point, DER 2 is not compromised and it can be seen that the DER 2 tries to absorb reactive power following the default Volt-VAR curve to bring down the voltage. The amount of absorption from DER 2 varies with the DER penetration and it can be seen in the gradient in the figure for varying levels of DER penetration. At 5 s attack, DER 2 also gets compromised with the malicious curve driving the voltage up which compels the DER controller to inject maximum reactive power of 0.44 p.u. (176 kVAR) worsening the voltage trajectory by driving the voltage even higher.

Similarly, Figure 5.3, the result of the malicious curve intended to drive the voltage down, shows voltage being driven down for all the simulations and dropping with higher intensity as the DER penetration increases. This again becomes more evident looking at the reactive power graph of two DERs. DER 1 shown by the blue line goes from zero injection of reactive power to full absorption of 0.44 p.u. (176 kVAR) after the attack made at 2 s with the malicious curve intended to drive down the voltage. At this point, DER 2 is not compromised and it can be seen that the DER 2 tries to inject reactive power following the default Volt-VAR curve to bring up the voltage. The amount of injection from DER 2 varies with the DER penetration and it is apparent from the gradient in the figure for varying levels of DER penetration. At 5 s attack, DER 2 also gets compromised with the malicious curve driving the voltage down which compels the DER controller to inject reactive power. Due to the way the malicious curve was set, DER 2 will be absorbing a certain amount of reactive power as set by the slope of the malicious curve which results in worsening the voltage trajectory by driving the voltage even lower. For different DER penetration, the gradient is seen for DER 2 reactive power absorption, with absorption being higher for higher DER penetration.

5.1.2 Findings on critical DER penetration ratios

Tables 5.1, 5.2, and 5.3 show critical ratios of DERs/AEPS where a two-step attack alters the nominal operating condition for various levels of DER penetration. Table 5.1 indicates that in a system where the DERs/AEPS ratio is less than 22%, the system may operate continuously in a state different than in the nominal state. However, a system with a DERs/AEPS ratio of more than 22% is going to cause oscillations in the grid as was discussed earlier.

Table 5.2 shows there are no critical ratios for the malicious curve driving

Table 5.1: Critical DERs/AEPS percentages for the malicious sawtooth curve

Different Attack Steps	**System Operating Condition**		
	Continuous operating	***Oscillatory behavior***	***Ride through then trip***
No attack	0% – 100%	N/A	N/A
First attack	0% – 22%	22% – 100%	N/A
Second attack	0% – 22%	22% – 100%	N/A

Table 5.2: Critical DERs/AEPS percentages for the curve that drives up the voltage

Different Attack Steps	**System Operating Condition**		
	Continuous operating	***Oscillatory behavior***	***Ride through then trip***
No attack	0% – 100%	N/A	N/A
First attack	0% – 100%	N/A	N/A
Second attack	0% – 100%	N/A	N/A

Table 5.3: Critical DERs/AEPS percentages for the curve that drives down the voltage

Different Attack Steps	**System Operating Condition**		
	Continuous operating	***Oscillatory behavior***	***Ride through then trip***
No attack	0% – 100%	N/A	N/A
First attack	0% – 100%	N/A	N/A
Second attack	0% – 34%	N/A	34% – 100%

up the voltage. This means that even for max penetration of 100%, the voltage does not exceed 1.10 p.u. for it to initiate any trip commands. This does not mean that this curve is innocuous. The voltage rises as high as 1.08 p.u. for high DER penetration. It is not good for the grid to be operating at high voltages for a long time and this might cause equipment damage following the idea of CBEMA curve [21].

In Table 5.3, for the malicious curve driving down the voltage, the last row indicates that in a system where the DERs/AEPS ratio is less than 34%, the system may survive a two-step attack. However, a system with a DERs/AEPS ratio of more than 34% is going to sustain a low voltage ride-through for some time. During this time, other devices on the AEPS with the voltage support capability may respond and help restore the voltage, a step that is left for future work. However, without any voltage support, DER are going to trip after 21 s for a Category III DER. This tripping of DER will cause not only load-shedding but also grid instability upon losing more than 34% of the DER that were initially supporting the grid.

5.2 Malicious change of contradictory modes

Figures 5.4 and 5.5 show Monte Carlo simulation results carried out in MATLAB, where each line represents a different ratio of DERs/AEPS and the effect of the mode changes on voltage and frequency at the PCC over 10 s for both scenarios of 1 p.f. and 0.9 p.f. [22]. The top graphs in both figures show the reactive power measurements (in kVAR) from both DERs where a positive value of 176 kVAR (+0.44 p.u.) indicates generation, a negative value of 176 kVAR (−0.44 p.u.) indicates absorption, and 0 kVAR simply indicates neither absorption nor generation. Simulations with unequally sized DER were also carried out and the results were qualitatively similar [22].

At 2 s, when the first mode change takes place, the first DER's reactive power output rapidly changes from no-generation to absorption for Scenario 1 as shown in Figure 5.4 and from generation to absorption for Scenario 2 as shown in Figure 5.5. At 5 s, the second DER does the same. This change in the reactive power support is reflected in the voltage and frequency readings at the PCC.

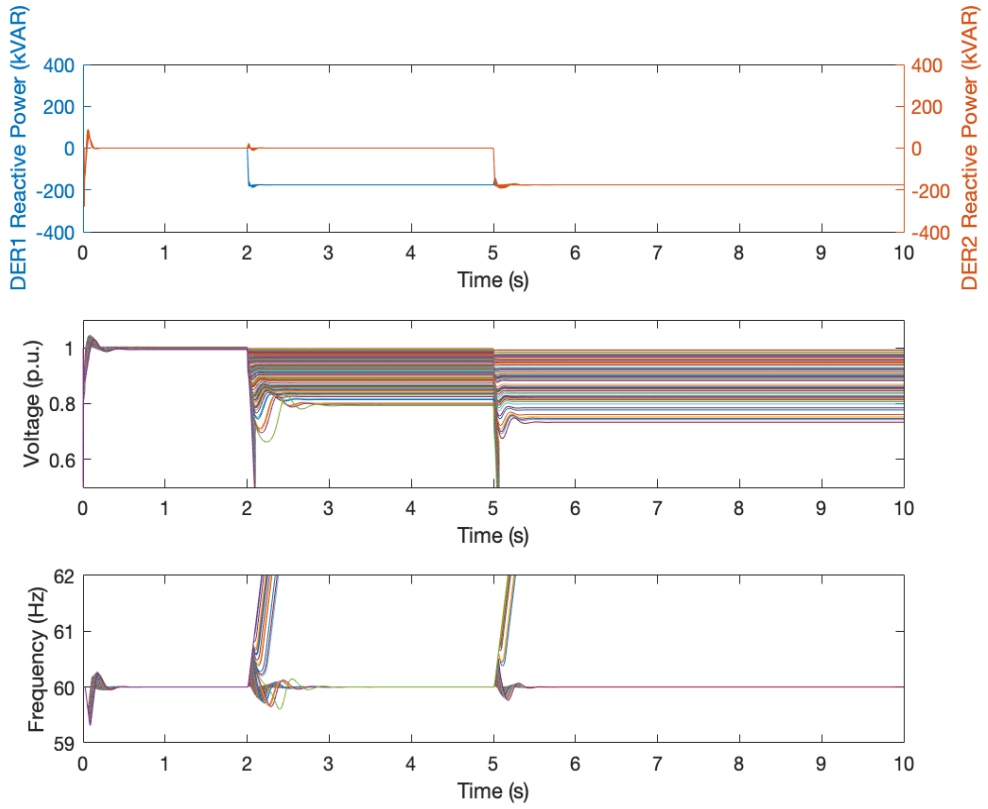


Figure 5.4: DERs with Volt-Watt mode on and Constant Power Factor of 1 [22]

5.2.1 Findings from Monte Carlo simulation

For the results of this particular use case of combination of modes, there are three potential outcomes of the simulation: continuous operation, trip after a sustained ride-through, and voltage and frequency collapse.

The first outcome consists of small transients that result in the system still operating in the continuous operating mode. This means that system states might have changed but not enough to cause any immediate damage to the system. In this outcome, there are, however, a few cases where the voltage is close to 0.88 p.u.. This undervoltage condition is still concerning and could affect electronic devices. The cases of this first outcome corresponding to lower levels of DER penetration can be seen on the top portion of the 200 simulations shown in Figures 5.4 and 5.5.

The second outcome is voltage depression at the PCC that the system tries to ride through but eventually must trip due to the absence of volt-

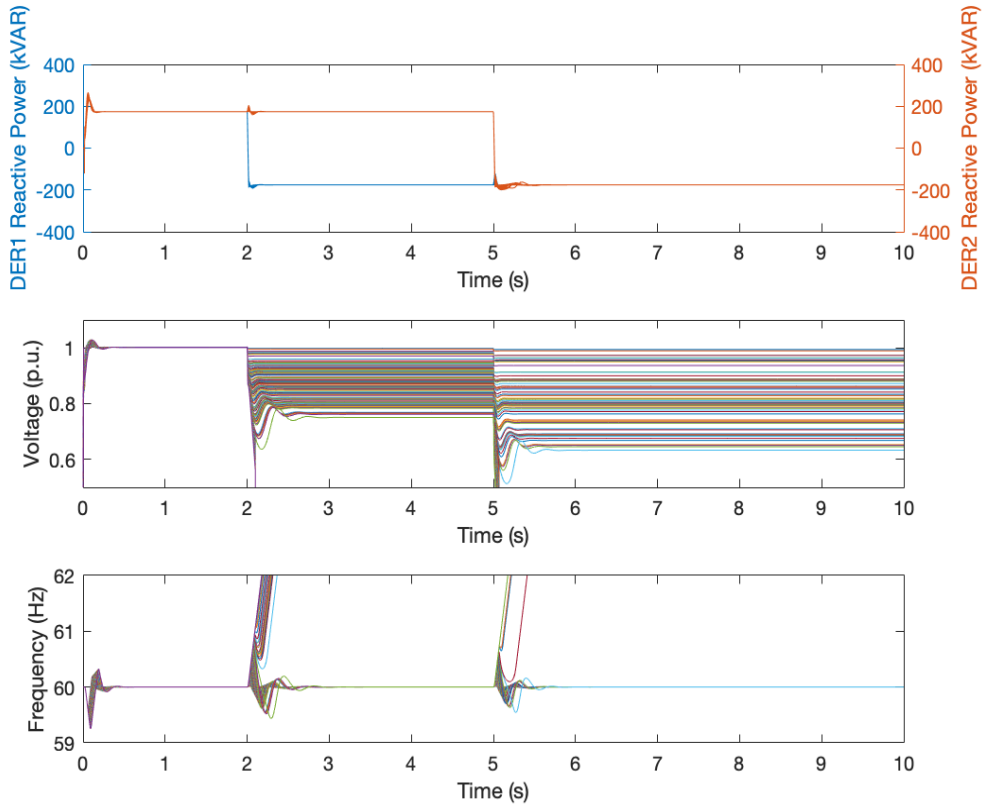


Figure 5.5: DERs with Volt-Watt mode on and Constant Power Factor of 0.9 [22]

age recovery. This outcome is similar to the outcome explained earlier for the use case of malicious Volt-VAR curve driving the voltage down causing the voltage to ride through low voltage and trip after certain time. Note that this outcome resulting in tripping after a certain time varies with the category of DER used, and the assumption that it will trip after a certain time comes from the lack of intelligent automated reactive power support from non-compromised DER. Using non-compromised DER intelligently as a mitigation strategy to prevent this outcome is part of the future work and is discussed in detail in Chapter 6. The cases resulting in this outcome can be seen in the Figures 5.4 and 5.5 right in middle of those 200 simulations.

The third outcome is the result of power mismatch causing the operating point to be unstable, leading to voltage and frequency collapse. These transients will not last long due to strict tripping requirements for high fluctuations in voltage and frequency readings at the PCC. A Category III DER, by default, should trip after 2 s when voltage drops below 0.50 p.u. or after

0.16 s when frequency rises above 62 Hz [8]. The resulting cases for the third outcome can be seen in the trajectory of frequencies shooting beyond 62 Hz and with voltage collapsing. Instead of showing non-converging solution of oscillating voltage trajectories, the voltage trajectories for the third outcome are shown as approaching zero, and frequency shooting upwards, for better legibility of the figure. This corresponds to immediate tripping after the breakers detect low voltage and high frequency readings. It is evident that these cases happen in simulations where DER penetration is higher. The ratios for which this outcome is caused, along with ratios for first and second outcomes, are discussed in Section 5.2.2.

The time difference for the DER to trip sets apart the second and third outcome. Since the third outcome occurs almost immediately, it would be harder to implement mitigation strategies for the third outcome than it would be for the second outcome. Also, the third outcome is the result of voltage and frequency collapse which can be best avoided by DPI and stronger firewall measures rather than system-level physical mitigation strategies.

The differences in voltage and frequency trajectories can be seen between Scenario 1 and Scenario 2. The range of frequency fluctuations is higher for Scenario 2 than it is for Scenario 1. The difference in the results between two scenarios is more noticeable in the voltage trajectories where larger voltage depression is noticed in Scenario 2 compared to that in Scenario 1. This confirms the speculation that the AEPS reliance on both DERs to inject reactive power in high load scenarios is prone to more adversarial impacts due to the state of both DERs going from injection to absorption versus no reactive power support to reactive power absorption.

5.2.2 Findings on critical DER penetration ratios

As discussed earlier in the chapter, one of the main objectives to carry out these stochastic simulations, with randomly generated DER penetration levels, is to find out the critical ratios where different resulting outcomes would be seen. This is more relevant for this particular use case involving combination of modes because of higher sensitivity on the trajectories of voltage and frequency for varying levels of DER penetration. Tables 5.4 and 5.5 show critical ratios of DERs/AEPS where a two-step attack alters the nominal

Table 5.4: Critical DERs/AEPS percentages for Scenario 1 (both DERs operating at a p.f. of 1) [22]

Different Attack Steps	**System Operating Condition**		
	Continuous operating	***Ride through then trip***	***Immediate trip***
No attack	0% – 100%	N/A	N/A
First attack	0% – 48%	48% – 63%	63% – 100%
Second attack	0% – 24%	24% – 48%	48% – 100%

operating condition.

In Table 5.4, for example, the last row indicates that in a system where the DERs/AEPS ratio is less than 24%, the system may survive a two-step attack. This means the system will remain in continuous operating region with different voltage and frequency trajectories but within the range without causing direct instability in the system. However, a system with a DERs/AEPS ratio of anywhere between 24% and 48% is going to sustain ride-through for some time. During this time, other devices on the AEPS with the voltage support capability may respond and help restore the voltage, a step that is left for future work. However, without any support, it is deemed to trip after a few seconds. The worst-case scenario would be when the DERs/AEPS ratio crosses 48% and the attack causes the system to trip immediately. This is the third outcome discussed in the prior section where the system operator would have no chance to mitigate and the AEPS would lose a large portion of its capacity, resulting in system instability and load-shedding.

Following up on to the speculation from the previous section, Table 5.5 shows unfavorable conditions for DER penetration as low as 14%, 10% lower than the unfavorable conditions for Scenario 2. This is because Scenario 1 had a higher load demand to begin with and was relying on reactive power injection from both DERs. Thus, the attack becomes more successful even with lower penetration.

The only anomaly in this table lies in a comparatively lower tripping threshold of 63% for Scenario 1 compared to 73% for Scenario 2 after first attack. This is primarily because the rate of voltage depression is higher right after the first attack for Scenario 1 and is significant enough to cause volt-

Table 5.5: Critical DERs/AEPS percentages for Scenario 2 (both DERs operating at a p.f. of 0.9) [22]

Different Attack Steps	**System Operating Condition**		
	Continuous operating	***Ride through then trip***	***Immediate trip***
No attack	0% – 100%	N/A	N/A
First attack	0% – 34%	34% – 73%	73% – 100%
Second attack	0% – 14%	14% – 36%	36% – 100%

age collapse sooner than the system's inertial response and Simulink solver's time response [22]. This does not happen for the second attack because by the time second attack hits, the voltage is already depressed enough. Therefore, the solver and inertial response work as expected. To help explain these anomalies more mathematically, part of the future work also involves detailing the model in a more granular way.

Chapter 6

ONGOING AND FUTURE WORK

The current trends of DER penetration serve as motivation to focus on two aspects in parallel: identifying potential cybersecurity threat vectors that might destabilize the system, and finding mitigating solutions for disturbances arising from either cyberattacks, human errors, or naturally occurring faults and disturbances [22]. The simulation results from one of the use cases (change of combination mode case: Scenario 1) show that even an attack on default nominal operating conditions can cause significant issues with penetration as low as 24% of the AEPS system capacity. With current RPS goals calling for high penetration of renewables, this number is concerning.

As a part of ongoing work, the team is trying to implement the use cases discussed in this thesis in a hardware-in-the-loop setting using tools such as OPAL−RT. This is to see the real-time effects of this attack. Though OPAL−RT supports hardware in the loop, there are no 1547-compliant DER controllers yet that could be put in the loop to test these use cases. However, using OPAL−RT at least allows the implementation of mitigation strategies in real time as well to compare the timing and efficacy of different strategies for different attack vectors.

The ongoing work also involves developing rule based data inspection tools using a Python script that receives and sends network traffic. The receiving network traffic could be commands that are either benign or malicious. The script then performs heuristic analysis which could be a simple rule-based method but could also potentially utilize sophisticated machine learning methods. After the analysis is done, the script then rejects or forwards the packets to be sent to the simulated AEPS. The simulated AEPS can be either in Simulink or OPAL−RT. Since these use cases are not time sensitive, MATLAB should be sufficient for now. However, if it was needed to implement voltage support and incorporate timers to check for ride-through and tripping requirements, OPAL−RT might be essential. The dynamics of the

combined system can then be tested with reachability analysis to validate benign configurations or detect susceptibility to malicious commands that could lead to abnormal and unstable states.

To mitigate the outcome of a sustained ride-through until mandatory trip is required, one way to implement a mitigation strategy would be by deploying non-compromised DER to compensate for the attack on compromised DER. This could be done through a control logic that determines the mitigating mode combination and optimal set-points associated with it. Mitigating strategies with Volt-VAR support can be used for the first use cases discussed regarding malicious Volt-VAR curves [41]. Using centralized Volt-VAR optimization strategy against malicious attack on control of DER can lead to an optimal operation of the system [42].

For the Scenario 2 in the change of combination of modes use case (both DERs starting with a p.f. of 0.9), a mitigation strategy can be considered where there is a system with n DERs where x is the number of DERs that have been compromised. This means the overall system is left with $n - x$ DERs to mitigate issues. Without loss of generality, it can be assumed that all the DERs meet the minimum absorption requirement of 0.44 p.u. of the apparent power for all the n DERs. Also, it can be assumed that the x DERs that were compromised were operating with active power mode on and reactive power mode on with the Constant Power Factor of 0.9. This resembles a situation where the AEPS operator is relying on those x DERs to inject reactive power to maintain the nominal voltage while the $n - x$ DERs are just operating at the default mode as defined in the standard, which is the Constant Power Factor mode for the reactive power mode. The active power mode is usually off and is turned on when there is a possibility of high voltage situations. For this case, it is assumed that the active power mode is on because that means the active power output for nominal and less than nominal voltage levels are set to be 0.9 p.u. which gives the space for 0.44 p.u. of reactive power capability. The active power mode might as well have been turned off and the active power production could have been limited as reactive power production is increased, but the former approach is simpler to work with.

For this example of mode change resulting in generation to absorption, the mitigation lies in raising the voltage to the nominal value. This means that raising the voltage is achieved by injection of reactive power from $n-x$ DERs.

In this example case, the mitigation is guaranteed if $n - x >= 2 * x$ because of the nature of the use case which turns x DERs reactive power state from generation to absorption which means it needs $2 * x$ DERs to compensate for that sudden change of reactive power. For cases where $n - x <= 2 * x$ but close to $2 * x$, DERs may reach close to the nominal voltage within the threshold. One could either deploy all non-compromised $n-x$ DERs in raising the voltage or use selective compensation. With the selective compensation mitigation strategy, instead of choosing all $n - x$ DERs to participate in reactive power injection, only a few of the $n - x$ DERs would be chosen to help with mitigation. This is very useful when some DER have a high active power output, such as solar plants on a sunny day, and other DER produce little active power, such as solar plants with cloud spots or wind plants with very weak wind profile in that particular time. It would not be efficient to decrease the active power production in order to provide reactive power for DER with potentially high power output. Instead, DER producing low active power output can be leveraged to participate in the reactive power injection which would not require capping the active power.

While a simplistic model is used to demonstrate the use cases, it is evident that these use cases remain valid for larger systems with multiple DER as well. The two DERs used in the system can be thought of as groups of DER such as PV, wind, and storage devices. These use cases and implementation can be translated to a bigger system with different kinds of DER and longer transmission lines among the DER in order to imitate a more realistic system.

The system model can be explained mathematically to be able to substitute Monte Carlo simulations with a sensitivity analysis that determines confidence intervals for states' trajectories (voltage and frequency for instance) with respect to several participation factors [43]. With the help of confidence intervals for each use case and its attack vectors, it saves a lot of computational time. The AEPS operator would also be able to carry out several what-if scenarios for different use cases. Without the need to computationally run simulations, it also helps in examining ride-through and trip functionalities for longer simulation duration and coupling the simulations to test any possible mitigation strategies.

Digging deeper into the new functionalities of the IEEE 1547 is going to help come up with more use cases. Developing use cases revolving around FDI, changing the ride-through and trip parameters, access to monitoring in-

formation, combination of modes and change in settings of modes will enable the AEPS operator to recognize vulnerability. Devising use cases and implementing the use cases with real-time simulations will help in understanding the severity of several attack vectors. This study will be useful to developing mitigation strategies for both the cyberphysical and cybersecurity sides of the problem.

Chapter 7

CONCLUSION

The IEEE 1547 standard plays a vital role in addressing the interconnection requirements of DER into the main grid. It is necessary to think of this standard as a living document subject to change in the years to come. The research work presented in this thesis is intended to give a glimpse at possible threats and their consequences that could arise with the advent of new functionalities. Due to changing nature of grid modernization, standards are prone to change. This means that a special emphasis should be placed on the continuous research and development of several use cases and attack vectors, and their ramifications as regulatory bodies keep updating policies, standards and regulations.

While the requirements of interfaces in smart inverters are intended to make the grid smarter, smart inverters also expose the grid to several cybersecurity threats, some of which were discussed in detail in this thesis. As RPS goals increase the share of renewables in the grid, and as the inverters connecting the renewables to the grid get smarter, it is vital to make the grid more secure and resilient against any possible cyberadversaries or human error.

The results from the research show that attacks or human errors made in systems with DER penetration as low as 24% for default operating conditions, or as low as 14% for some special scenarios, lead to unfavorable conditions. Therefore, the use cases mentioned in the thesis and the results following from those might help smart grid researchers to prevent instability outcomes by planning for mitigation strategies in both the cybersecurity and cyberphysical layers.

BIBLIOGRAPHY

[1] M. Christian, "US states face uneven paths in movement for 100% "clean energy"," *SP Global Market Intelligence*, Aug 2019, https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/us-states-face-uneven-paths-in-movement-for-100-clean-energy-53419260.

[2] Hawaii House Bill 623, 2015, Hawaii State Legislature.

[3] SB-350 Clean Energy and Pollution Reduction Act of 2015, 2015, California Energy Commission.

[4] Associated Press, "New York climate plan sets 30-year goal for 100% renewable energy," *Los Angeles Times*, Jul. 2019.

[5] C. Sasidharan, "Insights on smart inverters and IEEE 1547: 2018," Nov 2018. [Online]. Available: https://www.linkedin.com/pulse/insights-smart-inverters-ieee-1547-2018-chandana-sasidharan/

[6] B. Mather and G. Yuan, "Onward and upward: Distributed energy resource integration [guest editorial]," *IEEE Power and Energy Magazine*, vol. 18, no. 6, pp. 16–19, 2020.

[7] R. Walling, "Revision of IEEE standard 1547: The background for change," *TechSurveillance*, Nov. 2016.

[8] *IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces*, IEEE 1548-2018, 2018.

[9] D. J. Sebastian and A. Hahn, "Exploring emerging cybersecurity risks from network-connected DER devices," in *2017 North American Power Symposium (NAPS)*. IEEE, 2017, pp. 1–6.

[10] J. Qi, A. Hahn, X. Lu, J. Wang, and C.-C. Liu, "Cybersecurity for distributed energy resources and smart inverters," in *IET Cyber-Physical Systems: Theory Applications*, vol. 1, no. 1, Dec. 2016, pp. 28–39.

[11] J. Johnson, I. Onunkwo, P. Cordeiro, B. J. Wright, N. Jacobs, and C. Lai, "Assessing DER network cybersecurity defences in a power-communication co-simulation environment," in *IET Cyber-Physical Systems: Theory Applications*, Mar. 2020.

[12] I. Onunkwo, P. Cordeiro, B. Wright, N. Jacob, C. Lai, J. Johnson, T. Hutchins, W. Stout, A. Chavez, B. T. Richardson, and K. Schwalm, "Cybersecurity assessments on emulated DER communication networks," Sandia National Laboratories Tech. Rep. SAND2019-2406, , Mar. 2019.

[13] R. S. de Carvalho and D. Saleem, "Recommended functionalities for improving cybersecurity of distributed energy resources," in *2019 Resilience Week (RWS)*, vol. 1, 2019, pp. 226–231.

[14] H. Albunashee and R. A. Mc Cann, "DER coordination strategy for Volt/VAR control using IEC61850 GOOSE protocol," in *2019 North American Power Symposium (NAPS)*, 2019, pp. 1–5.

[15] "CRASHOVERRIDE: Analyzing the threat to electric grid operations," *Dragos Inc.*, https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf.

[16] A. Joseph, K. Smedley, and S. Mehraeen, "Secure high DER penetration power distribution via autonomously coordinated Volt/VAR control," *IEEE Transactions on Power Delivery*, vol. 35, no. 5, pp. 2272–2284, 2020.

[17] K. Pittol, R. A. S. Kraemer, C. M. de Oliveira Stein, E. G. Carati, J. P. da Costa, and R. Cardoso, "Low voltage ride-through strategy for distributed energy resources according to IEEE 1547-2018 standard," in *2019 21st European Conference on Power Electronics and Applications (EPE '19 ECCE Europe)*, 2019, pp. P.1–P.10.

[18] C. Roberts, S. T. Ngo, A. Milesi, S. Peisert, D. Arnold, S. Saha, A. Scaglione, N. Johnson, A. Kocheturov, and D. Fradkin, "Deep reinforcement learning for DER cyber-attack mitigation," in *2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2020, pp. 1–7.

[19] R. Bowers, "Updated renewable portfolio standards will lead to more renewable electricity generation," Feb 2019. [Online]. Available: https://www.eia.gov/todayinenergy/detail.php?id=38492

[20] D. Tait, "The Duck Curve: What is it and what does it mean?" May 2017. [Online]. Available: https://alcse.org/the-duck-curve-what-is-it-and-what-does-it-mean/

[21] "CBEMA Curve - The power acceptability curve for computer business equipment," Apr 2011. [Online]. Available: http://www.powerqualityworld.com/2011/04/cbema-curve-power-quality-standard.html

[22] P. Chapagain, M. Culler, D. Ishchenko, and A. Valdes, "Stability impact of IEEE 1547 operational mode changes under high DER penetration in the presence of cyber adversary," in *IEEE Green Technologies Conference*, 2021.

[23] "e-mesh™ SCADA." [Online]. Available: https://www.hitachiabb-powergrids.com/offering/product-and-system/grid-edge-solutions/our-offering/e-mesh/e-mesh-scada

[24] M. J. Reno, R. J. Broderick, and S. Grijalva, "Smart inverter capabilities for mitigating over-voltage on distribution systems with high penetrations of PV," in *2013 IEEE 39th Photovoltaic Specialists Conference (PVSC)*, 2013, pp. 3153–3158.

[25] J. Rocabert, A. Luna, F. Blaabjerg, and P. Rodríguez, "Control of power converters in AC microgrids," *IEEE Transactions on Power Electronics*, vol. 27, no. 11, pp. 4734–4749, 2012.

[26] "Simulating discretized electrical systems." [Online]. Available: https://www.mathworks.com/help/physmod/sps/powersys/ug/simulating-discretized-electrical-systems.html

[27] X. Xu, Y. Cao, H. Zhang, S. Ma, Y. Song, and D. Chen, "A multi-objective optimization approach for corrective switching of transmission systems in emergency scenarios," *Energies*, vol. 10, no. 8, p. 1204, Aug 2017. [Online]. Available: http://dx.doi.org/10.3390/en10081204

[28] J. H. Kim and S. A. Alameri, "Harmonizing nuclear and renewable energy: Case studies," *International Journal of Energy Research*, vol. 44, no. 10, pp. 8053–8061, 2020. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/er.4987

[29] L. Olatomiwa, S. Mekhilef, M. Ismail, and M. Moghavvemi, "Energy management strategies in hybrid renewable energy systems: A review," *Renewable and Sustainable Energy Reviews*, vol. 62, pp. 821 – 835, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1364032116301502

[30] J. Nair, S. Adlakha, and A. Wierman, "Energy procurement strategies in the presence of intermittent sources," in *2014 ACM International Conference on Measurement and Modeling of Computer Systems*. New York, NY, USA: Association for Computing Machinery, June 2014. [Online]. Available: https://doi.org/10.1145/2637364.2591982

[31] M. Brenna, F. Foiadelli, M. Longo, and D. Zaninelli, "Ancillary services provided by BESS in a scenario characterized by an increasing penetration of unpredictable renewables," in *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, 2017, pp. 1–6.

[32] B. Otomega and T. Van Cutsem, "Undervoltage load shedding using distributed controllers," *IEEE Transactions on Power Systems*, vol. 22, no. 4, pp. 1898–1907, 2007.

[33] C. Mozina, "Undervoltage load shedding," in *2007 Power Systems Conference: Advanced Metering, Protection, Control, Communication, and Distributed Resources*, 2007, pp. 39–54.

[34] R. M. Larik, M. W. Mustafa, and M. N. Aman, "A critical review of the state-of-art schemes for under voltage load shedding," *International Transactions on Electrical Energy Systems*, vol. 29, no. 5, p. e2828, e2828 ITEES-18-0343.R1. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/2050-7038.2828

[35] H. Nemouchi, A. Tiguercha, and A. A. Ladjici, "An adaptive decentralized under voltage load shedding in distribution networks," *International Transactions on Electrical Energy Systems*, vol. 30, no. 11, p. e12592.

[36] J. Johnson, J. Quiroz, R. Concepcion, F. Wilches-Bernal, and M. J. Reno, "Power system effects and mitigation recommendations for DER cyberattacks," *IET Cyber-Physical Systems: Theory & Applications*, vol. 4, no. 3, pp. 240–249, 2019. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/iet-cps.2018.5014

[37] S. Liemann, L. Robitzky, and C. Rehtanz, "Impact of varying shares of distributed energy resources on voltage stability in electric power systems," in *2019 IEEE Milan PowerTech*, 2019, pp. 1–6.

[38] C. W. Taylor, "Concepts of undervoltage load shedding for voltage stability," *IEEE Transactions on Power Delivery*, vol. 7, no. 2, pp. 480–488, 1992.

[39] I. A. Hiskens and M. A. Pai, "Power system applications of trajectory sensitivities," in *2002 IEEE Power Engineering Society Winter Meeting. Conference Proceedings (Cat. No.02CH37309)*, vol. 2, 2002, pp. 1200–1205 vol.2.

[40] R. K. Varma and E. M. Siavashi, "PV-STATCOM: A new smart inverter for voltage control in distribution systems," *IEEE Transactions on Sustainable Energy*, vol. 9, no. 4, pp. 1681–1691, 2018.

[41] M. J. E. Alam, K. M. Muttaqi, and D. Sutanto, "A multi-mode control strategy for VAR support by solar PV inverters in distribution networks," *IEEE Transactions on Power Systems*, vol. 30, no. 3, pp. 1316–1326, 2015.

[42] A. Majumdar, Y. Agalgoankar, B. Pal, and R. Gottschalg, "Centralized Volt-VAR optimization strategy considering malicious attack on distributed energy resources control," in *2018 IEEE Power Energy Society General Meeting (PESGM)*, 2018, pp. 1–1.

[43] I. A. Hiskens and J. Alseddiqui, "Sensitivity, approximation, and uncertainty in power system dynamic simulation," *IEEE Transactions on Power Systems*, vol. 21, no. 4, pp. 1808–1820, 2006.