

A reference-model strategy for self-protective smart inverters

by

Tareq Hossen

B.Sc., Chittagong University of Engineering and Technology, 2013

M.Sc., University of North Dakota, 2018

AN ABSTRACT OF A DISSERTATION

submitted in partial fulfillment of the
requirements for the degree

DOCTOR OF PHILOSOPHY

Mike Weigers Department of Electrical and Computer Engineering
Carl R. Ice College of Engineering

KANSAS STATE UNIVERSITY
Manhattan, Kansas

2023

Abstract

This dissertation presents novel self-protective methods for grid-interactive inverters. The self-protective methods use reference models to inspect the incoming power setpoints, detect unsafe setpoints, and protect the inverter-based system accordingly. By employing these new self-protective methods based on reference models, grid-interactive inverters can effectively contribute to distributed energy generation within the energy infrastructure, where a supervisory control structure is required for energy management and economic dispatch. In a centralized supervisory control structure, the inverters need to be in contact with aggregators, other energy generation units, or the utility operating center. The communication capability makes a grid-interactive inverter a cyber-physical device. However, the connection of inverters to a communication network exposes the inverters to active attackers who can interfere with the control infrastructure and send malicious setpoints to the local controller. Such malicious setpoints can have harmful consequences, such as uncontrolled power oscillations, voltage sags and swells, equipment damage, and blackouts. This dissertation develops the self-protective methods using steady-state and dynamic reference models. The self-protection strategy inspects incoming power setpoints from the utility operator or third-party aggregators using the reference models before engaging the setpoints to the local controllers. At first, a self-learning feature for a self-protective inverter is developed. Self-protective inverters use the self-learning feature to learn their normal operating region by estimating unknown system parameters and employing known parameters from the measurements. The unknown system (grid) parameters are estimated by injecting a current at a different frequency than the fundamental power frequency. Consequently, two distinct real-time grid parameter estimation techniques, namely the model reference estimation and recursive least square method, have been developed and experimentally validated. Then,

analytical steady-state and dynamic reference models are developed to inspect the incoming power setpoints. The self-protection method uses these reference models to learn the safe operating region of the inverters. The steady-state reference model is developed based on steady-state linear and nonlinear operating regions, and the dynamic reference model is formed based on the full-order inverter model. Based on the risk of unsafe operation defined by the steady-state model, if the setpoints fall in a high-risk region, the setpoints are rejected by the self-protection method, and the previously accepted setpoints remain in operation. Following the steady-state model check, the accepted setpoints are further examined using the full-order dynamic model to predict the location of dominant eigenvalues of the system using root-locus studies, thus predicting the dynamic response and making the decision whether the commanded setpoints are safe or unsafe. The performance of the self-protection strategy using the analytical reference models is tested using hardware experiments. The steady-state analytical model demonstrates satisfactory performance, characterized by its mathematical simplicity and ease of implementation in real-time applications. However, despite the promising performance and enhanced capabilities of the full-order dynamic model, the complexity of the full-order model can cause a high computational burden on digital signal processors (DSP) for real-time applications. In order to address this challenge, a stability criterion is developed from a simplified inverter model to determine the stability margin, thus predicting the inverter behavior for commanded setpoints. This criterion serves as a predictive tool for ensuring the safe operation of the inverter. One notable advantage of the stability criterion is its ability to quickly estimate the gain margin of the controller without requiring knowledge of pole locations. Experimental tests are conducted on hardware to validate the effectiveness of the developed stability criterion. While the stability criterion successfully reduces the computational burden, it is important to note that the simplified criterion is inherently less accurate compared to the full-order inverter model. This is due to its incapability to capture the intricacies and dynamics of the system fully. To address this limitation, this dissertation proposes novel hybrid dynamic models by combining the data-driven model with the analytical model. This work presents two forms of hybrid dynamic models using a data-driven neural network platform. The first hybrid model uses analyti-

cally evaluated risk factors as one of the inputs of the neural network to predict stable and unstable operation as the output of the neural network. The other hybrid model uses the data-driven neural network and developed stability criterion in parallel to predict the stable and unstable operation. Furthermore, a standard neural network is implemented as a benchmark that considers all relevant information as input and predicts whether the operation of the inverter is safe or unsafe. This benchmark highlights the merits of the developed hybrid dynamic models. The effectiveness of the hybrid dynamic models is thoroughly evaluated through simulation and hardware tests to ensure their practical applicability.

A reference-model strategy for self-protective smart inverters

by

Tareq Hossen

B.Sc., Chittagong University of Engineering and Technology, 2013

M.Sc., University of North Dakota, 2018

A DISSERTATION

submitted in partial fulfillment of the
requirements for the degree

DOCTOR OF PHILOSOPHY

Mike Weigers Department of Electrical and Computer Engineering
Carl R. Ice College of Engineering

KANSAS STATE UNIVERSITY
Manhattan, Kansas

2023

Approved by:

Approved by:

Co-Major Professor

Co-Major Professor

Dr. Fariba Fateh

Professor Behrooz Mirafzal

Copyright

© Tareq Hossen 2023.

Abstract

This dissertation presents novel self-protective methods for grid-interactive inverters. The self-protective methods use reference models to inspect the incoming power setpoints, detect unsafe setpoints, and protect the inverter-based system accordingly. By employing these new self-protective methods based on reference models, grid-interactive inverters can effectively contribute to distributed energy generation within the energy infrastructure, where a supervisory control structure is required for energy management and economic dispatch. In a centralized supervisory control structure, the inverters need to be in contact with aggregators, other energy generation units, or the utility operating center. The communication capability makes a grid-interactive inverter a cyber-physical device. However, the connection of inverters to a communication network exposes the inverters to active attackers who can interfere with the control infrastructure and send malicious setpoints to the local controller. Such malicious setpoints can have harmful consequences, such as uncontrolled power oscillations, voltage sags and swells, equipment damage, and blackouts. This dissertation develops the self-protective methods using steady-state and dynamic reference models. The self-protection strategy inspects incoming power setpoints from the utility operator or third-party aggregators using the reference models before engaging the setpoints to the local controllers. At first, a self-learning feature for a self-protective inverter is developed. Self-protective inverters use the self-learning feature to learn their normal operating region by estimating unknown system parameters and employing known parameters from the measurements. The unknown system (grid) parameters are estimated by injecting a current at a different frequency than the fundamental power frequency. Consequently, two distinct real-time grid parameter estimation techniques, namely the model reference estimation and recursive least square method, have been developed and experimentally validated. Then,

analytical steady-state and dynamic reference models are developed to inspect the incoming power setpoints. The self-protection method uses these reference models to learn the safe operating region of the inverters. The steady-state reference model is developed based on steady-state linear and nonlinear operating regions, and the dynamic reference model is formed based on the full-order inverter model. Based on the risk of unsafe operation defined by the steady-state model, if the setpoints fall in a high-risk region, the setpoints are rejected by the self-protection method, and the previously accepted setpoints remain in operation. Following the steady-state model check, the accepted setpoints are further examined using the full-order dynamic model to predict the location of dominant eigenvalues of the system using root-locus studies, thus predicting the dynamic response and making the decision whether the commanded setpoints are safe or unsafe. The performance of the self-protection strategy using the analytical reference models is tested using hardware experiments. The steady-state analytical model demonstrates satisfactory performance, characterized by its mathematical simplicity and ease of implementation in real-time applications. However, despite the promising performance and enhanced capabilities of the full-order dynamic model, the complexity of the full-order model can cause a high computational burden on digital signal processors (DSP) for real-time applications. In order to address this challenge, a stability criterion is developed from a simplified inverter model to determine the stability margin, thus predicting the inverter behavior for commanded setpoints. This criterion serves as a predictive tool for ensuring the safe operation of the inverter. One notable advantage of the stability criterion is its ability to quickly estimate the gain margin of the controller without requiring knowledge of pole locations. Experimental tests are conducted on hardware to validate the effectiveness of the developed stability criterion. While the stability criterion successfully reduces the computational burden, it is important to note that the simplified criterion is inherently less accurate compared to the full-order inverter model. This is due to its incapability to capture the intricacies and dynamics of the system fully. To address this limitation, this dissertation proposes novel hybrid dynamic models by combining the data-driven model with the analytical model. This work presents two forms of hybrid dynamic models using a data-driven neural network platform. The first hybrid model uses analyti-

cally evaluated risk factors as one of the inputs of the neural network to predict stable and unstable operation as the output of the neural network. The other hybrid model uses the data-driven neural network and developed stability criterion in parallel to predict the stable and unstable operation. Furthermore, a standard neural network is implemented as a benchmark that considers all relevant information as input and predicts whether the operation of the inverter is safe or unsafe. This benchmark highlights the merits of the developed hybrid dynamic models. The effectiveness of the hybrid dynamic models is thoroughly evaluated through simulation and hardware tests to ensure their practical applicability.

Table of Contents

List of Figures	xiii
List of Tables	xix
Acknowledgements	xx
Dedication	xxii
1 Introduction	1
1.1 Motivation and Objectives	1
1.2 Literature Review	3
1.2.1 Smart Inverter as Cyber-Physical Device and Cyberattacks	3
1.2.2 Self-learning for Self-secure Inverters	10
1.2.3 Reference Model Framework for Self-Secure Inverters	11
1.3 Contribution of the Dissertation	18
1.4 Organization of the Dissertation	20
2 Self-learning Algorithms to Estimate the Grid Parameters	22
2.1 System Description and Modeling	23
2.2 Real-time Grid Parameters Estimation Algorithm	24
2.3 Recursive Least Square Estimation Method	25
2.4 Model-Reference Adaptive Estimation Method	27
2.5 Experimental Verification	28
2.6 Conclusion	32

3	Self-Protective Smart Inverters Using Analytical Reference Model	34
3.1	Self-Protection Concept for Inverters	34
3.2	Developed Self-Protection Method	36
3.3	Reference Models for Self-Protective Inverters	38
3.3.1	Load Flow Steady-State Model	38
3.3.2	Dynamic Model	41
3.4	Experimental Results	43
3.4.1	Steady-State Performance Analysis	44
3.4.2	Dynamic Performance Analysis	46
3.5	Conclusion	53
4	Development of Stability Criteria for Self-Protective Inverters	55
4.1	Instability Modes of Grid-Interactive Inverters	55
4.1.1	Instability and Circuit Impacts	56
4.1.2	Instability and Controller Impacts	58
4.2	Reduced-Order Model	60
4.2.1	Fifth-Order Model	61
4.2.2	Third-Order Model	64
4.3	Stability Criterion from Reduced-Order Model	66
4.4	State-Space Model for of Inverters	68
4.5	Eigenvalue Analysis	69
4.6	Experimental Results	74
4.6.1	Case I: Common Modes of Instability	75
4.6.2	Case II: Hidden Mode of Instability	78
4.7	The Stability Criterion Verification	81
4.8	Conclusion	85
5	An Analytical Criterion on Neural Network Platform for Self-Protective Inverters	87

5.1	Cyberattacks Scenarios and System Description	87
5.2	Hybrid Data-Driven and Analytical Model-Based Criterion for Safe Inverter Operation	89
5.2.1	Analytical Criterion from a Reduced-Order Model	90
5.2.2	Neural Network for Inverters' Stable and Unstable Operation Estima- tion	92
5.3	The Developed Self-Protection Approach	95
5.4	Experimental Results	97
5.5	Conclusion	104
6	Conclusions and Suggestions for Future Work	106
6.1	Summary and Conclusions	106
6.2	Suggestions for Future Work	109
	Bibliography	111
A	Full-Order Model Equations and Stability Criterion Formulation	136
A.1	Full-Order Model Equations	136
A.2	Stability Criteria Formulation	139
B	Analytical Method for Real-Time Grid Parameter Estimation	142
B.1	Analytical Method for Grid Parameters Estimation	142
B.2	Analytical Method Veification	145
C	Self-Protective Inverters Testbed Development	147
C.1	Hardware Development for Self-Protective Algorithm Verification	147
C.2	CHIL Testbed Development for Self-Protective Algorithm Verification	152

List of Figures

1.1	A taxonomy of smart inverter cybersecurity.	5
1.2	Device-level architecture and typical communication topology of smart inverters.	6
1.3	The concept of model/knowledge-based self-security approach to detect anomalies – the combination of the reference model and the security layer forms the device-level security.	12
1.4	Comparison of different types of data-driven models.	16
2.1	Smart inverters connected to the power grid and cyberattack scenarios in a cyber-physical system.	23
2.2	Simplified phase-a circuit of a three-phase grid-interactive VSI.	24
2.3	RLS formulation for grid impedance estimation.	26
2.4	General block-diagram of parallel-series model reference identification technique.	27
2.5	Hardware setup for 3 kVA three-phase grid-interactive inverter, implementing real-time grid parameter estimation.	29
2.6	Measured voltage (top) and current (bottom) waveform after low-frequency signal injection.	30
2.7	Estimation result from control desk (a) grid inductance (L_g), and (b) grid resistance (R_g) estimation using Model Reference Estimation method	31
2.8	Estimation result from control desk (a) grid inductance (L_g), and (b) grid resistance (R_g) estimation using Recursive Least Square Estimation method.	32
3.1	Unsafe PQ setpoints from authorized sources and man-in-the-middle attacks to smart inverters can pass the conventional security layers.	35
3.2	Flowchart of the self-protection concept for smart inverters.	36

3.3	The capability curve of a synchronous generator.	38
3.4	Operating regions of a grid-interactive inverter.	39
3.5	The PQ controller of the inverter used in the hardware setup for self-protective algorithm implementation.	42
3.6	Hardware setup for 3 kVA three-phase grid-interactive inverter, implementing device-level self-protection algorithm.	43
3.7	Inverter line-to-line voltage at PCC when (a) PQ setpoint is inside the safe region, and (b) PQ setpoint is at the stability boundary.	45
3.8	Statistics of the accuracy in risk prediction using the steady-state model. . .	46
3.9	Experimentally obtained inverter's dynamic responses when the output power is changing step-by-step from 150 W to 400 W.	48
3.10	(a) R_1 and R_2 versus current, and (b) the trajectory of the dominant positive eigenvalue of the full-order model of a 3kVA, 208V three-phase inverter for Case I.	49
3.11	Observing the inverter's dynamic behavior for Case II when the output power is changing step-by-step from 0.6 kW to 1.2 kW.	50
3.12	(a) R_1 and R_2 versus current, and (b) the trajectory of the dominant positive eigenvalue of the full-order model of a 3kVA, 208V three-phase inverter for Case II.	51
3.13	Statistics of dominant eigenvalues estimation for the dynamic reference model for changing active power from 100 W to 150 W (Point A)	52
3.14	Statistics of dominant eigenvalues estimation for the dynamic reference model for changing active power from 100 W to 250 W (Point C).	53
4.1	Circuit schematic of a grid-following inverter.	56
4.2	A example of unity feedback closed-loop system with proportional gain. . . .	58
4.3	Root locus studies of unity feedback closed-loop system with proportional gain	59

4.4	a) A simplified control schematic for fifth-order grid-following inverter model formulation, and (b) the system signal flow graph	61
4.5	a) A simplified control schematic for third-order grid-following inverter model formulation, and (b) the system signal flow graph	65
4.6	a) A simplified control schematic for stability criterion formulation, and (b) the system signal flow graph	67
4.7	Space vector of the inverter voltage, v_{inv} , with respect to the grid and PCC voltages.	69
4.8	A typical control block diagram for grid-following inverters.	70
4.9	The trajectory of low-frequency positive eigenvalue using the full-order dynamic model as P is increased from $0.003kW$ to $5kW$ for different L_g (right), a zoomed-in plot of dominant low-frequency positive eigenvalues for $L_g = 5mH$ (left).	71
4.10	The trajectory of low-frequency positive eigenvalue using the (a) third-order dynamic model (b) fifth-order dynamic model, as P is increased from $0.003kW$ to $5kW$	72
4.11	The trajectory eigenvalues using the full-order dynamic model as P is increased from $0.003kW$ to $5kW$ for $Q = 150Var$ (left), a zoomed-in plot of dominant positive eigenvalues for same inverter setup (right).	73
4.12	The trajectory of eigenvalues using the full-order dynamic model as L_g is increased from $5mH$ to $15mH$ (left), a zoomed-in plot of dominant low and mid-frequency eigenvalues.	74
4.13	The trajectory of a dominant positive eigenvalue using the full-order dynamic model of the inverter setups for different T_d (left), A zoomed-in plot of low-frequency eigenvalues (right).	75
4.14	Hardware setup for 3 kVA three-phase grid-interactive inverter	76

4.15	Experimentally obtained active power generation, PCC voltage, grid-side current, the zoomed-in voltage, and current waveforms, for $L_g = 10mH$ and the power setpoint of 1.2 kW, when the PWM frequency is 20 kHz.	77
4.16	Experimentally obtained active power generation, PCC voltage, grid-side current, the zoomed-in voltage, and current waveforms, for $L_g = 10mH$ and the power setpoint of 1.2 kW, when the PWM frequency is 8 kHz,	78
4.17	Experimentally obtained active power generation, for $L_g = 15mH$ and the power setpoint of 1.2 kW (a) the PWM frequency is 20 kHz, and (b) the PWM frequency is 8 kHz. (c) a family of curves for ΔP vs. PWM frequency at two different power levels.	79
4.18	Experimentally obtained inverter's dynamic responses when the output power is changing step-by-step from 150 W to 400 W for (a) $L_g = 2.5mH$ and (b) $L_g = 5mH$	80
4.19	Experimentally obtained (a) inverter's dynamic responses when the output power is changing step-by-step from 100 W to 1200 W and keeping $Q=100$ Var. (b)-(d) Voltage waveforms obtained from the oscilloscope for different dynamic responses.	82
4.20	Active power at PCC when $P = 150W$ at $t = t_1$ and a step-change to $P = 250W$ at $t = t_2$ with $L_1 = 1$, $L_2 = 0.5mH$, and $L_g = 5mH$ for $R_g = 0.35 \Omega$ followed by inserting additional L_1 or L_2 at $t = t_3$. (a) $L_1 = 1mH$, $L_2 = 1mH$ (b) $L_1 = 1.5mH$, $L_2 = 0.5mH$, (c) $L_1 = 1$, $L_2 = 1.5mH$ (d) $L_1 = 2mH$, $L_2 = 0.5mH$	83
4.21	Active power at PCC when $P = 1200W$ at $t = t_1$ and L_g change to $15mH$ from $L_g = 5mH$ at $t = t_2$ with $L_1 = 1$, and $L_2 = 0.5mH$ for $R_g = 0.35\Omega$ followed by inserting additional L_1 or L_2 at $t = t_3$. (a) $L_1 = 1mH$, $L_2 = 1.5mH$ (b) $L_1 = 3.5mH$, $L_2 = 0.5mH$, (c) $L_1 = 1$, $L_2 = 3mH$ (d) $L_1 = 2mH$, $L_2 = 0.5mH$	84

5.1	Smart inverters connected to the power grid and cyberattack scenarios in a cyber-physical system.	88
5.2	The PQ controller for grid-following inverters and unsafe operation from an authorized entity or modified by unauthorized source (man-in-the-middle attacks).	90
5.3	The flowchart of neural network offline training.	93
5.4	Implemented neural network topology for stable or unstable operation estimation.	94
5.5	Flow chart of the self-protective algorithm of a smart inverter integrating analytical model into neural network platform.	96
5.6	Experimental setup for a three-phase grid-following inverter.	97
5.7	Experimentally recorded inverter's dynamic responses from the control desk when the active power is changing step-by-step from 100 W to 1200 W for $Q = 0$ Var.	98
C.1	Schematic diagram of the control hardware-in-the-loop testbed for a self-protective inverter.	147
C.2	Inverters and grid-simulator used for the developed microgrid; (a) 5 kVA SiC inverter, (b) 30 kVA grid-simulator.	148
C.3	(a) The dSPACE MicroLabBox for controller implementation, (b) a high-level schematic of the controller in MATLAB-Simulink, and (c) control panel of the Control Desk software.	149
C.4	Interface between circuit and the controller; (a) Voltage and current measurement board, and (b) schematic of the measurement board.	150
C.5	Circuit components of the developed testbed for self-security algorithm implementation. (a) LCL filters board (b) Circuit breaker (c) Inserted inductance between PCC and grid simulator.	151
C.6	Schematic diagram of the developed testbed for self-protective inverter. . . .	153

C.7	(a) Typhoon HIL 402 (b)Interface between HIL and the DSP controller. (c)	
	TI F28379D LaunchPad	154
C.8	Validation of the self-security algorithm employing the real-time simulator -	
	Typhoon HIL.	156

List of Tables

2.1	System parameters to validate real-time grid parameter estimation methods	29
3.1	System parameters for experimental Setup to validate self-protective algorithm	44
3.2	System parameters to demonstrate the dynamic analysis of self-protective inverters	47
3.3	Eigenvalues using the full order model for Case I	50
3.4	Eigenvalues using the full order model for Case II	52
4.1	Simulation and Experimental Parameters for Case I (known mode of instability)	76
4.2	Simulation and Experimental Parameters for Case II (hidden mode of instability)	80
5.1	Circuit and Control Parameters of Experimental Setup used for Data Record- ing for active power setpoints, P^* , variation	100
5.2	Circuit and Control Parameters of Experimental Setup used for Data Record- ing for reactive power setpoints, Q^* , variation	102
5.3	Performance of Neural Network for Stable and Unstable Operation Estimation	103
B.1	Voltage and current signal multiplication for analytical method formulation .	144
B.2	Results obtained from CHIL using analytical grid parameter estimation method	146
C.1	DSP F28379D analog inputs employed for self-protective algorithm implemen- tation	155
C.2	DSP F28379D digital outputs employed for self-protective algorithm imple- mentation	155

Acknowledgments

This dissertation is a compilation of my four years of challenging endeavors. This tremendous task would not have been accomplished without the support of my near and dear ones. First, I want to express my gratitude towards the Almighty Creator, without whose divine guidance I would not have been able to succeed.

I sincerely thank my advisor and co-major professor, Prof. Behrooz Mirafzal, for his valuable guidance and technical advice throughout this dissertation's progress. I firmly believe his rich knowledge and proper guidance have shaped me into a better researcher and engineer. I am grateful to my co-major professor, Dr. Fariba Fateh, for her course on adaptive control, which significantly contributed to developing the real-time grid-parameter estimation technique in my dissertation.

I am grateful to my Ph.D. supervisory committee members Dr. Anil Pahwa, Dr. Hongyu Wu, and Dr. George Amariuca, for their insightful suggestions during my preliminary examination, which has helped me a lot in developing this dissertation.

I sincerely thank my knowledgeable ex-lab mates from the Smart Power Electronics and Control Systems (SPECS) Research Group, Dr. Joseph Benzaquen, Dr. Mohsen Pilehvar, and Dr. Fahmid Sadeque for their invaluable assistance and guidance in my research. My heartfelt thanks to my current lab mates, Mr. Mehmetcan Gursoy, Mr. Milad Sadoughi, and Ms. Arya Ponnarassery Sadasivan, whose support and positive attitude have made our research lab a truly enjoyable place.

All of my life's achievements are built upon my family's unparalleled support and love. I am deeply grateful to my mother, Yesmin Akther, and my father, Abdul Malek. Everything I have achieved in life, I owe it to my parents. I am always and will forever be grateful for the unconditional support of my brother, Shawkat Hossen. I am very grateful to my sister, Sharmin Akther, for always cheering for my success. I am extremely grateful to my wife, Nazmun Nahar Khan, for her unwavering love and support during my Ph.D. journey. Her

patience with my busy schedule and unwavering encouragement during challenging times have been pivotal in completing my Ph.D. I am also grateful to my daughter, Numairah Ayaat Hossen, for being a great source of joy and relief from my academic endeavors.

Dedication

To my family.

Chapter 1

Introduction

The primary objective of this dissertation is to develop device-level security for grid-interactive smart inverters based on reference models. The motivation and objectives of this dissertation are outlined in Section 1.1. Section 1.2 discusses the state-of-the-art smart inverters as cyber-physical devices, the self-learning feature of self-secure inverters, and the reference model framework for self-secure inverters. The contribution of this dissertation in developing various reference models to protect the inverters from unsafe operations is discussed in Section 1.3. Finally, the organization of this dissertation is outlined in Section 1.4.

1.1 Motivation and Objectives

A smart cyber-physical device, i.e., a smart inverter, provides controllable and interactive interfaces between the cyber network and physical devices using communication links [1, 2]. These interfaces allow autonomous and bi-directional information exchange between the parties while performing proactive actions [3]. For instance, a smart inverter can operate in different modes of operation, such as grid-supporting mode when voltage regulation and harmonic compensation are accomplished while overcoming various instability issues and grid-forming mode when networked microgrid operation with black-start capabilities can be achieved [4-6]. To perform these advanced features, execute control actions, and achieve

desired operating conditions, the inverters' control schemes require some system parameters to be identified[7–9]. These parameters can be estimated, measured, or received as external information, such as measurement data from nearby smart devices (smart inverters, smart meters, etc.), PQ setpoints from utility supervisory controllers, and forecasting data from the internet. However, communication with multiple parties through the cyber network can entail more surfaces for harmful events, particularly when the communication protocols are insecure, user credential information, and the operating system software, are outdated [2, 10–13].

Unsafe incidences can present in the form of intentional or unintentional harmful events or naturally occurred anomalies in the system, i.e., a malfunction in a physical system[14–17]. For instance, measurement data received from an external sensor can be intentionally modified by an unauthorized user, also known as a cyberattack. On the other hand, an authorized utility operator can unintentionally send harmful PQ setpoints that can force the inverter to operate beyond its capability limit or cause pulse dropping, high total harmonic distortions (THD), and undesired oscillations in the inverter's output power[18–20]. One should notice that the zero-inertia nature of the inverters is more prone to instant changes and can quickly lead to the asymmetrical operation or instability of the power grid, particularly when the grid is weak[21–24]. This can result in excessive power injection, voltage sags, and swells, damage of equipment, and blackouts. The risk of cyberattacks or erroneous operations can significantly increase when many smart inverters operate in a system and share the same communication link with the other smart devices. Therefore, security actions are essential to detect and prevent anomalies in the system to sustain safe system operation.

In the last decade, anomaly detection, mitigation, and defense have become a trending research area. Existing solutions focus on user interfaces and data network security, such as encryption, authentication, and cryptographic algorithms, to assure data availability, confidentiality, and integrity [25, 26]. To enhance the security in existing communication links, communication protocols are offered by IEC 61850 [27, 28]. A block-chain technique is proposed in [29, 30] to enhance authentication, message authentication code method is proposed in to check the validity of incoming data, and a multi-layer cyber defense method-

ology including Transport Access Control is developed in [31] by National Renewable Energy Laboratory (NREL). However, an expert hacker can breach the security layers of the basic protection, or an authorized operator can unintentionally bypass the communication and security protocols. On the other hand, some researchers are focused on system-level detection methods which employ system status and data received from nearby devices[32–35]. Data-driven techniques are heavily used in system-level approaches where measured data with time-dependent thresholds and known constants are compared [36, 37]. However, employing more data can increase the complexity of the calculations, computational period, processing power, and the risk of anomalies due to the increased need for external data [38], while the safety of the devices in the system cannot be ensured. For instance, oscillatory inverter operation can be observed due to input/output parameter uncertainties and malfunctions in the sensors, although anomalies may or may not be detected at the system-level [39]. This abnormal operation can immediately or gradually damage the devices connected to the system. Therefore, in addition to the basic security requirements and the system-level safety algorithms, device-level anomaly detection is vital to prevent instability and potential damage to the system.

1.2 Literature Review

This section discusses the state-of-the-art roles of smart inverters as cyber-physical devices, possible attack scenarios, the self-learning feature for self-secure inverters, and the concept of a reference model framework for self-protective inverters. At the beginning of this section, the roles of smart inverters as cyber-physical devices and potential cyber attack scenarios are discussed.

1.2.1 Smart Inverter as Cyber-Physical Device and Cyberattacks

When physical devices, such as smart inverters, communicate over a cyber network, they are referred to as cyber-physical devices. These smart cyber-physical devices facilitate real-time

data sharing and can receive commands to follow, thereby enhancing the system’s overall performance, efficiency, and reliability. For example, as illustrated in Fig. 1.1, a smart inverter can receive commands from a utility supervisory controller or a third-party aggregator via a communication link. These commands may include disconnecting from the grid or updating power setpoints to manage power demand efficiently. Similarly, in networked microgrids, which consist of interconnected microgrids, smart inverters can exchange measurements, operating points, and system status data using either a centralized controller or their own local controllers [40–43]. Enabling grid-interactive inverters to possess these intelligent capabilities expands their functionality beyond grid-feeding mode, allowing them to operate in grid-supporting roles (providing ancillary services) and even in grid-forming modes [24, 44]. Moreover, when inverters are geographically close, they can establish a clustered data communication network, reducing the vulnerability to cyber-attacks.

Maintaining security is the main challenge when operating a cyber-physical device because hackers can deliberately target to jeopardize the smart device’s operation. The increasing number of distributed energy resources (DER) and the widespread adoption of smart inverters on the consumer side make the smart inverter more vulnerable to cyber-attack [45–47]. For instance, installing numerous smart inverters on consumer sites extend the attack surface and makes smart inverters more accessible to hackers when they are linked with public networks or building automation. Notably, smart inverters are often remotely accessible by manufacturers and aggregators to monitor, configure, and even directly control the operation of smart inverters [48, 49]. They often provide online services (remote maintenance, fault diagnosis, cloud storage, etc.) that hackers can target. For instance, certain commercially available inverter models like the SOLECTRIA XGI 1500 series and the FIMER PVS980-58 series inverters can be accessed through Wi-Fi-accessible devices (Laptops, Tablet, mobile apps, etc.) from a single location. This accessibility allows for remote power curtailment and adjustment of reactive power [50]. Furthermore, the zero-inertia nature of the inverters is more prone to instant changes and can quickly lead to the asymmetrical operation or instability of the power grid, particularly when the grid is weak [51, 52]. The taxonomy of smart inverter cybersecurity is shown in Fig. 1.2. This taxonomy illustrates how smart

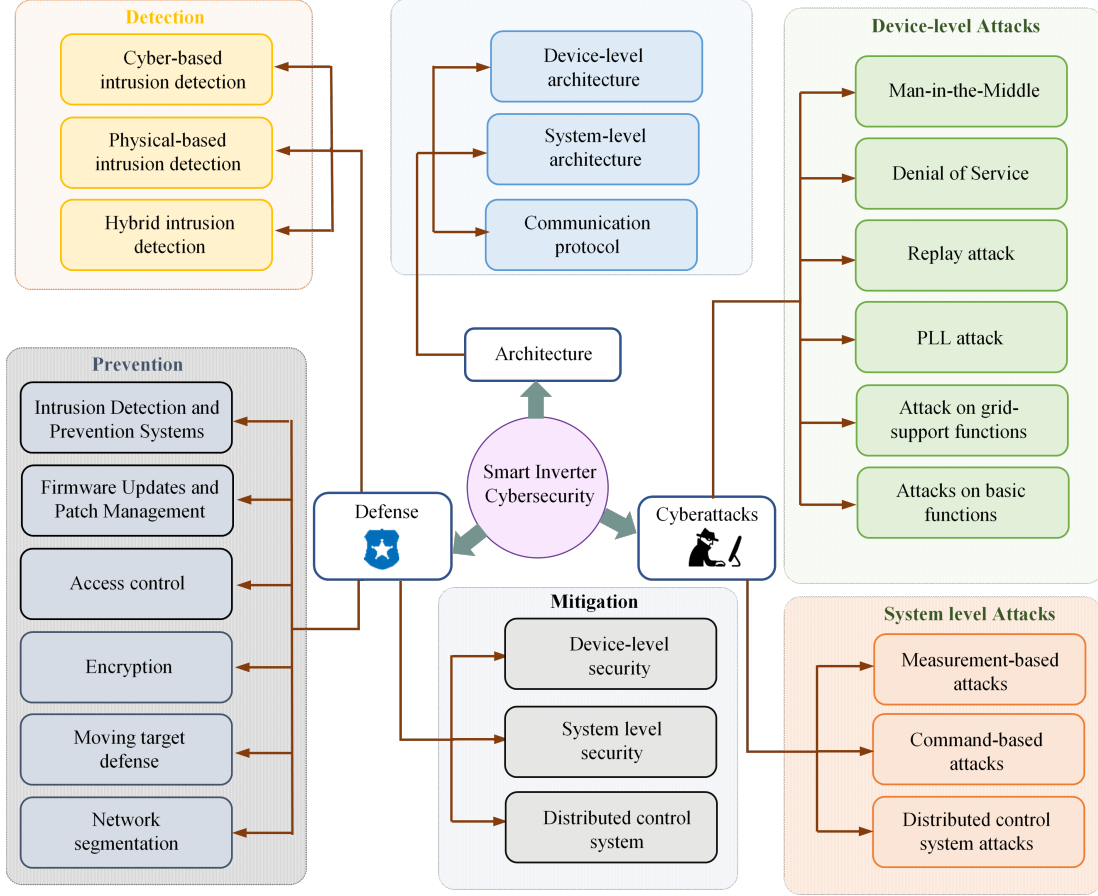


Figure 1.1: *A taxonomy of smart inverter cybersecurity.*

inverters are structured at the device and system level, the different types of cyberattacks they can face, and the methods used in the literature to defend against those attacks.

Smart Inverter Architectures and Communications Protocols

Fig. 1.2 illustrates the architecture of a smart inverter at the device level within a DER system. This architecture is typically utilized in DER systems that incorporate direct current (dc) sources such as photovoltaic (PV) panels and batteries. It consists of a high-voltage part that includes inverters, PWM drivers, voltage/current sensors, etc. and a low-voltage part that includes digital signal processors (DSP), Joint Test Action Group (JTAG) connectors, communication interface, and controllers. The DSPs are programmed with control functions that generate pulse-width modulation (PWM) signals, which are utilized to op-

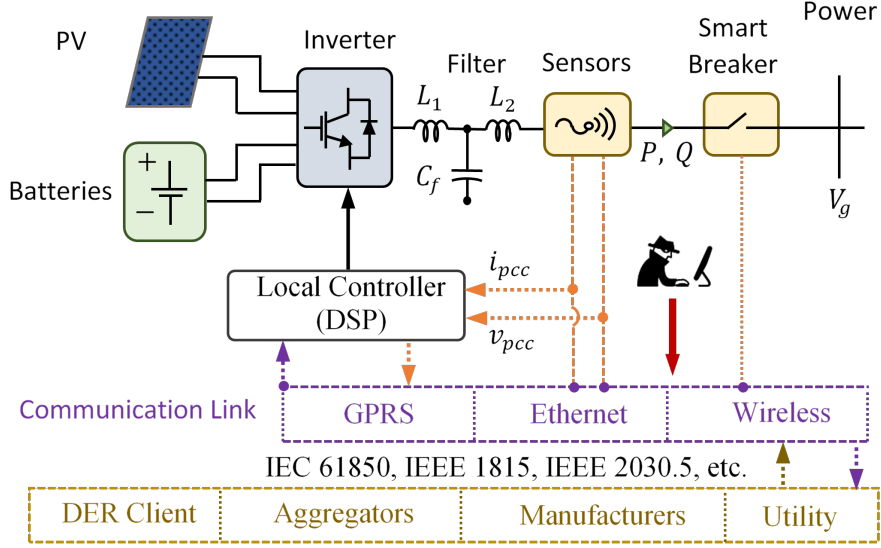


Figure 1.2: *Device-level architecture and typical communication topology of smart inverters.*

erate the inverters. The controller is programmed to control the injected active power, P , and reactive power, Q , based on the desired power setpoints, P^* , and Q^* . Smart inverter utilizes wireless networks, GPRS, or Ethernet ports to communicate with DER clients, inverter manufacturers, the utility, and other third-party aggregators. These communication channels facilitate a wide range of applications, energy management, real-time monitoring, remote firmware upgrades, etc. As per the IEEE 1547-2018 standard, smart inverters are needed to support at least one communication protocol selected from IEEE 2030.5, SunSpec Modbus, and IEEE 1815 (DNP3) [53–55]. IEEE 2030.5 facilitates monitoring and controlling smart inverters by utilities or aggregators, which is now a stringent requirement for DER within investor-owned utilities [56]. IEEE 1815 is utilized to interface smart devices and is widely used by the utility SCADA system [57]. The SunSpec Modbus enable interoperability among the DER system components [58]. Utilizing of these communication protocols offers significant benefits in making a device smart by enabling it to exchange information with other entities. However, this communication capability also introduces vulnerabilities, as it provides potential entry points for cyber threats.

Cyber-attacks on Smart Inverters

Fig. 1.1 provides a summary of potential cyberattack scenarios. Cyber-attacks targeting smart inverters can vary in scope, ranging from device-level attacks to system-level attacks, depending on the intended purpose of the attack. In device-level attacks, attackers aim to jeopardize a smart inverter operation, disrupt functionality, or intercept communication between the inverter and external devices. On the other hand, in grid-level attacks, the aim is to disrupt the interactions between the smart inverter and the control center, eventually preventing the grid operator from achieving desired goals [59]. The device-level attack includes reconnaissance, replay attacks, DoS attacks, MITM attacks, firmware replacements, hall spoofing, PLL attacks, attack on basic functions, etc. Reconnaissance uses network scanning tools such as OpenVAS, Nmap, etc., and operates on the attacker side devices to collect information on the inverters, which include IP addresses, identified vulnerabilities, open ports, and security patches[60]. A replay attack refers to a method where the transmitted data is captured, subsequently replicated, and potentially altered by hackers [61, 62]. Using the SPAN tool, Sandia National Laboratory executed this form of attack on two distinct inverters by manipulating the disconnection voltage setting transmitted from the customer side, employing UDP/IP and TCP/IP protocols for each respective case [60]. A denial-of-service (DoS) attack targeting a smart inverter where the attacker aims to render the inverter inaccessible to its authorized users for a temporary or prolonged period of time [63–65]. A Man-in-the-Middle (MITM) attack refers to a scenario in which an attacker secretly intercepts and manipulates the communication between two parties who falsely believe they are directly communicating with each other [13, 66]. In reality, the attacker secretly transmits and modifies the exchanged information, potentially leading to unauthorized access or malicious alterations [67, 68]. In addition to cyberattacks that specifically target communication links, there have been instances of hardware-based attacks on smart inverters [11, 69, 70]. These attacks exploit vulnerabilities within the hardware components of smart inverters, which typically include components such as microcontrollers (MCU), DSP, Hall sensors, external read-only memory (ROM), JTAG interfaces, communication interfaces, and

more [71, 72]. A noninvasive hardware-based attack was reported in [73, 74], where hackers executed spoof readings of Hall sensors used to measure the output quantities of an inverter. Another type of hardware-based attack focuses on directly manipulating the AC power input of inverters instead of attacking sensors [75–77]. This approach aims to intentionally provide wrong information to the inverter’s local controller and trigger an incorrect response. In [78], the impact of the phase-locked loop (PLL) attack is demonstrated by injecting an additional signal at the zero-crossing point of the ac voltage at the point of common coupling (PCC) point, which leads to jeopardizing the PLL operation.

The interaction between multiple inverters as well as between control centers to smart inverters can also be impacted by cyberattacks [79–82]. Smart inverter system-level attacks can be classified into measurement-based attacks, command-based attacks, distributed control system attacks, and attacks triggered by attacking other devices [2]. In [83], a dynamic stealthy attack model is demonstrated, where the primary frequency droop control curve of the inverter-based microgrid was constantly modified by changing active power measurements. A command-based attack aims to manipulate the control commands to jeopardize the system’s normal operation [84, 85]. In [86], authors investigated the harmful effect of manipulated setpoints on an inverter-based microgrid, where hackers tempered active power setpoints sent from the centralized secondary controller. Noteworthy, unsafe incidents can also occur unintentionally for devices and system levels. For example, a MITM can alter the command sent from the utility operator using the secure communication line. However, harmful setpoints can be sent by authorized operators intentionally or accidentally. Hence, it is crucial to implement protective measures at both the system and device levels to identify and prevent the occurrence of unsafe operations by commanded setpoints, ensuring the continuity of safe operations of smart inverters.

Detection and Defense Against Possible Attacks

This subsection reviewed various security measures proposed in the literature to detect and defend cyberattacks on smart inverters. One of the cyberattack detection strategies is to

deploy an intrusion detection system or IDS device that can monitor a network, system, or device to observe malicious activities. The development of IDS for smart grids is a trending field of research, particularly for SCADA systems and advanced metering infrastructure. As inverter-based distributed resources increase, more research is being conducted to develop IDS for smart inverters. The IDS device for smart inverters can be classified into three categories depending on the data types monitored: cyber-based IDS, physical-based IDS, and hybrid IDS. The cyber-based IDS collects data from the cyber network, which includes the IP address, source ports, packet length, firmware files, etc. In [87], the authors implemented Security Onion based on the Snort engine to implement signature-based IDS for Modbus-based smart inverters. The physical IDS collects data from physical devices, which includes output voltages and currents, phase angle, measured active and reactive power, frequency, etc. The authors in [88, 89] designed several indicators extracted from the inverters' output voltage and current signals to detect false data injection attacks (FDIAs) where cyberattacks alter the inverter's current. Notably, cyber-based IDS have the capability of detecting cyberattacks targeting communication networks and software.

Implementing cyberattack defense strategies allows the inverter or the entire DER system to respond effectively to cyber threats, mitigating adverse consequences and safeguarding the system against potential damage. The defense strategies can be categorized into system-level security and device-level security, as reported in [13]. System-level defense utilizes the system's status and data from nearby cyber-physical devices and controllers to detect anomalies. These defense strategies at the system level involve both data-driven and knowledge-based approaches. In [90, 91], AI-based defense techniques are introduced to detect False Data Injection (FDI) attacks. In [92], a nonlinear autoregressive exogenous model, a specific recurrent neural network (RNN) type, is applied in centralized DER controllers within DC microgrids. Developing data-driven methods requires a strong understanding of the system. Insufficient system knowledge can lead to inadequate training of the algorithm, potentially resulting in damages and significant economic impacts. Apart from data-driven approaches, model/knowledge-based investigations are documented in the literature. [93] introduces model-based centralized and distributed detection methods. Additionally, [94] proposes a

model-based partial primal-dual anomaly detection strategy to address attacks aimed at distributed secondary droop control in microgrids. It is important to note that the proposed technique solely focuses on link and node attacks. Additionally, dynamic authentication of IoT signals and game-theoretic frameworks for predicting sensitive IoT devices have been proposed [95]. While enhancing communication security can be effective, skilled hackers may still breach security measures. Moreover, most authentication and signature-based software protections prove inadequate when malicious data originate from authorized sources with authorized access, such as third-party aggregators interacting with grid-interactive inverters. In such scenarios, hackers exploit various access points in smart inverters, like reference setpoints, tunable parameters, and measured signals, to launch cyberattacks. Hence, an additional level of safety beyond system and communication levels becomes crucial to safeguard the inverters.

The self-protection concept for smart inverters is an additional anomaly detection feature to the existing communication- and system-level methodologies that can certify safe inverter operation and examine the applicability/validity of the incoming data. The device-level anomaly detection for smart inverters can implement model-based reference models, and the developed models can be used as the digital twin of the inverters. The concept of a smart knowledge-based approach to self-security at the device level was initially proposed by [96]. This approach relies on model-based anomaly detection, which serves as the foundation for device-level security. The authors highlight the potential for developing defense methods based on reference models to assess the authenticity of incoming data at the device level. It is possible to employ multiple reference models to improve anomaly detection performance [13]. Section 1.2.3 comprehensively explains reference model-based self-protection techniques.

1.2.2 Self-learning for Self-secure Inverters

Self-learning is a process in which smart devices can autonomously learn their capabilities or characteristics using their input and output data. Devices equipped with self-learning features can predict or examine their current or future operation points and behavior when

system parameters vary. Application of this feature to a grid-interactive smart inverter can become a powerful solution to predict whether the inverter's operation will remain in normal operation, operate in a highly nonlinear region, or cause instability when the incoming PQ setpoints are received or system parameters change. Hence, a smart inverter can be capable of protecting itself from intentional or unintentional data attacks if the inverter knows its input and output circuit parameters, such as DC-bus voltage and grid parameters, as long as the varying parameters are used in the twin models. Self-protection can be enhanced if the dynamic behavior of the inverter for a change applied at the input can be learned and combined with the security algorithm accordingly. The process of learning the safe and unsafe operation boundaries and dynamic behavior and using this information to build the self-security concept for smart inverters is called self-learning for self-secure inverters. In this paper, the self-learning process is used to determine: (i) the inverter stability boundary for steady-state analysis and (ii) characteristics of the grid-interactive smart inverter for dynamic analysis. Additional to the above mentioned self-learning features, the adaptive security algorithm can be programmed to adjust the inverters' output power in such a way that the adjusted setpoints can always operate in a linear operating region when unusual measurements received from the sensors are unusual due to fault or malfunction occurring in the system. To perform that, the system parameters should be estimated routinely compared to only estimating when the new PQ setpoints are received. This can provide extra protection during natural circumstances.

1.2.3 Reference Model Framework for Self-Secure Inverters

Investigations show that advanced encryption, authentication, and cryptography methodologies for user interface, data transfer, and network security are under development to ensure data availability, confidentiality, and integrity. Additional to these basic security requirements, enhanced communication and security protocols for smart devices are defined by organizations such as IEEE and IEC to provide a safer data exchange environment. While these technologies have the potential to improve communication security, it remains possible

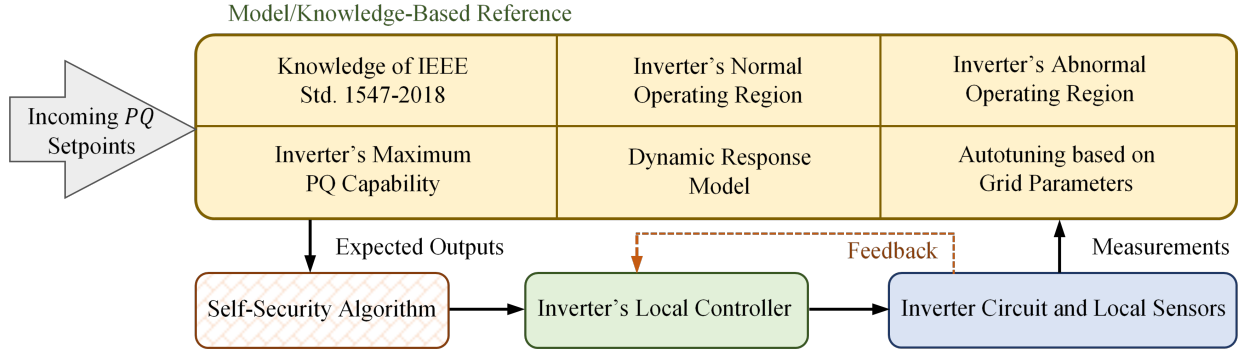


Figure 1.3: *The concept of model/knowledge-based self-security approach to detect anomalies – the combination of the reference model and the security layer forms the device-level security.*

for a skilled hacker to discover a way to breach protective measures.

On the other hand, anomaly detection methodologies used in system-level security monitor local or big-scale system statuses and utilize the information received from nearby devices to detect anomalies. System-level protection techniques lend a supporting hand to basic security practices and provide more comprehensive anomaly detection solutions. However, system-level solutions can require heavy computational processes and power consumption if data-driven approaches are applied. Moreover, basic security features and system-level methodologies can fail to examine the incoming PQ setpoints sent from an authorized user like a utility operator or measurement data from nearby trusted local devices using secure communication channels before engaging the harmful information to the inverter's local controller. Therefore, an additional protection layer to the existing methods is essential to maintain normal and safe system operation.

The self-security concept for smart inverters is an additional anomaly detection feature to the existing communication- and system-level methodologies that can certify safe inverter operation and examine the applicability/validity of the incoming data. The device-level anomaly detection for smart inverters can implement model-based reference models, and the developed models can be used as the digital twin of the inverters. When the malicious data bypasses the existing security features, the self-secure smart inverters can examine the integrity of the incoming data in real-time using the digital twin models (reference models) as

their security layer. If the reference models' output detects abnormal behavior, the harmful data is not engaged to the inverter's controller. Multiple reference models can be used to enhance to improve anomaly detection accuracy and enhance system protection. The structure of the multi-reference model framework for self-secure inverters is depicted in Fig. 1.3.

Similar to the capability boundary of synchronous generators, each inverter has a capability boundary that the device can inject power into the grid. When the inverter transfers maximum available power from the intermittent sources, i.e., $P = P_{max}$, and $Q = 0$, the inverter operates at unity power factor. Inverters may need to inject reactive power into the grid to provide voltage support. However, the current, thus the apparent power, must always stay below its nominal peak value, which can be written as $S^2 = P^2 + Q^2 \leq S_{max}^2$, where S_{max} is the maximum capacity of the generation unit in VA. The amount of active and reactive power injected by an inverter into the grid can be formulated as $S = P + jQ = |V_i||V_{th}|e^{-j(\delta-\theta_z)} - |V_{th}|^2e^{j\theta_z}/|Z|$. Where V_{inv} and V_{th} represents the inverter and grid Thevenin voltage, respectively, δ is the angle difference between V_{inv} and V_{th} . Z is the impedance seen from the inverter output terminals. Inverter safe operation region is represented as the overlap of the circle evaluated using this equation with S_{max} boundary [97]. An inverter's linear and nonlinear operating region is defined as a steady-state reference model in [96–98] based on these circles. Instability will be observed if the power setpoints are located at nonlinear operating regions [99, 100]. In [96], the setpoints are checked using the linear and non-linear boundary and protect the inverter from unsafe operation. Variations in the steady-state model can arise from uncertainties in the parameters, leading to the possibility of accepted setpoints being identified as harmful or vice versa. Therefore, accurate grid parameter estimation is essential for a steady-state reference model. The abnormal operation detection can also be improved by adding PV forecasting data and updating S_{max} data accordingly [13, 101].

Even when the inverter is operating inside its nominal operating range, where the steady-state model predicts that engaging a PQ setpoint is safe for the inverter, there can still be situations where the inverter can become unstable. The steady-state model may not account

for the inverter’s transient response, which refers to how it behaves when there is a sudden change in load, a grid disruption, or switching activities. Under some transient conditions, the inverter’s response may deviate from steady-state prediction, resulting in instability. Beside this, the inverter’s control system plays a crucial role in maintaining stability. If the control system design does not appropriately consider dynamic behavior or lacks proper feedback and compensation mechanisms, instability can arise, even in the nominal operating region. The behavior of the electrical grid can vary over time due to factors like renewable energy fluctuations, load variations, or grid faults. These variations might not be adequately captured by the steady-state model, leading to potential unstable operation during certain grid conditions. Therefore, it is essential to consider the dynamic reference model of the inverter that consider transient behaviour and controller impacts.

Developing the dynamic model for power converters can be divided into knowledge-based and data-driven approaches [102, 103]. A knowledge-based approach uses analytical mathematical models that estimate expected system characteristics and compare them with actual system characteristics when the system is in a specific state[104]. The analytical model relies on the explicit relationship between input variables to perform predictions or insights. Analytical models are typically derived through an empirical approach, where assumptions and simplifications are made to create a mathematical representation of the studied system or phenomenon [105]. Full-order and reduced-order models have frequently employed techniques for analytically modeling power electronics inverters[21, 106]. A full-order inverter model provides a detailed representation of the inverter’s behavior and dynamics. It includes a complete set of equations that describe the power conversion process, switching behavior, and associated control algorithms. Typically, the underlying circuit topology and mathematical equations of the inverter components are used to develop a full-order inverter model. The full-order inverter models are more complex and computationally intensive compared to the reduced-order inverter model. A full-order model has the advantage of accurately representing an inverter’s behavior, capturing the complex dynamics, including higher-order harmonics and transients, and is also suitable for detailed analysis and control design [107–110]. The full-order inverter model incorporates all significant dynamics and states of the

inverter, including the dynamics of all circuit components and their interconnections. An accurately designed full-order model can represent the complete behavior of the inverter system. The full-order model provides a higher level of accuracy because it includes all significant dynamics and states of the inverter system. The full-order inverter model also allows eigenvalue analysis of a closed-loop inverter system that allows to determine the stability of the system and identify any hidden mode of instability [111–113]. On the other hand, a reduced-order inverter model aims to simplify the complexity of the full-order model while maintaining acceptable accuracy for particular applications or analysis purposes. The reduced-order model can capture the essential dynamics of the inverter while neglecting certain higher-order harmonics or transient effects[97]. If the inverter system exhibits multiple time scales, such as fast and slow dynamics, the reduced model can exploit this separation. Fast dynamics can be simplified or approximated, leading to a reduced model that focuses on the slower dynamics [114–116]. The eigenvalue analysis of a reduced model can estimate the dynamic response of an inverter. For example, if the reduced-order model exhibits eigenvalues with negative real parts, indicating stability, the distance of these eigenvalues from the imaginary axis can provide an indication of the stability margin [117, 118]. A larger distance implies a greater stability margin, indicating that the system can tolerate more disturbances or parameter variations before becoming unstable [119, 120]. In addition, stability criterion derived from a reduced-order model can be used to predict the stability of a system[121–125]. The criterion utilizes the reduced-order model’s eigenvalues or other system properties to assess the system’s stability. It’s important to note that the stability criterion derived from a reduced-order model provides an indication of stability, but it is an approximation based on the simplified representation of the system. The accuracy of the criterion should be verified by comparing it with the stability properties of the original full-order model or experimental observations [126, 127].

Data-driven modeling, in contrast to analytical modeling, is based on the utilization of data to derive a model or determine parameters for a specific system. Analytical modeling relies on a complete understanding of the system, which can be challenging for complex systems. However, data-driven modeling requires little or partial information about the

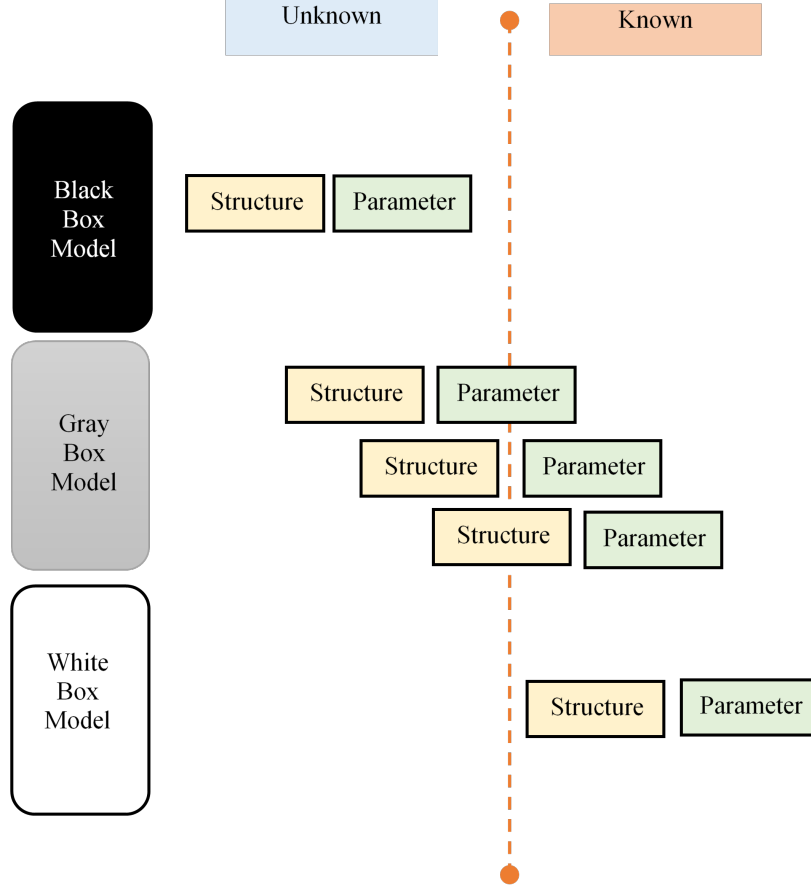


Figure 1.4: *Comparison of different types of data-driven models.*

system, as it infers the relationship between input and output from the available data. It relies on computational intelligence, classical statistics (such as ordinary least squares or maximum likelihood estimation), machine learning, and other techniques [128, 129]. Data-driven models assume that the data contains enough information to describe the actual system accurately. Examples of data-driven algorithms include artificial neural networks (ANN), support vector machines, random forests, and more. These models are capable of capturing system dynamics without relying on complete prior knowledge of the system's physical behavior [129–131].

Data-driven modeling can be utilized for the estimation of the structure, parameters, and behavior of grid-connected inverter systems. These models can be used as dynamic reference models to predict how the inverter will respond to different power setpoints. There are

three types of data-driven models: black-box, gray-box, and white-box models [102, 128], as shown in Fig. 1.4. A black-box model is one where no prior information about the system is known [132, 133]. In this case, a neural network can be used to analyze the collected data and capture the underlying linear relationships. In a gray-box model, some of the system's dynamic equations and/or parameters are known, while the rest are unknown. The unknown parts are determined by fitting the observed input-output data into the model, allowing for a characterization of the system's behavior [134, 135]. On the other hand, for a white box model, parameters and the system's structure are known to provide a comprehensive understanding of the system's characteristics [136, 137]. By utilizing data-driven modeling techniques, different types of models can be employed to estimate system behavior and predict dynamic responses, depending on the level of prior knowledge available. Data-driven models have the capability to capture unknown process behavior as long as it is reflected in the available data. However, it is important to note that data-driven models are highly dependent on the availability of rich and sufficient data to represent the process behavior accurately. Without proper caution, overfitting is a common problem that can result in poor extrapolation power when predicting future process conditions [138, 139].

Hybrid modeling combines analytical and data-driven modeling techniques and attempts to preserve the advantages while diminishing the disadvantages of the two approaches. The hybrid model typically consists of two main components: an analytical-based model and a data-driven model. The analytical-based model incorporates the fundamental principles and equations governing the behavior of the inverter system. It takes into account the physical characteristics, such as electrical components and control algorithms of the inverter [140]. This model is typically derived from the basic principles and offers an in-depth understanding of the system dynamics. However, analytical-based models often have limitations due to simplifications, assumptions, and uncertainties associated with parameter estimation [141]. These limitations can lead to inaccuracies in predicting the inverter's behavior under varying conditions. To address these limitations, a hybrid model introduced a data-driven model besides the analytical model. The data-driven model is developed using machine learning techniques, such as neural networks or regression algorithms, to capture the complex

relationships between input variables (such as incoming power setpoints for PQ-controlled inverter) and the corresponding output variables (such as stable or unstable system for given setpoints). This model learns from a large data set of measured or simulated input-output data, enabling it to approximate the inverter’s behavior without explicitly modeling the underlying physics. The idea of using a hybrid dynamic model to predict the inverter’s dynamic response is novel and has not been previously reported in the literature.

1.3 Contribution of the Dissertation

The dissertation presents novel self-protection methods based on reference models. It is essential to highlight that these methods are distinct from conventional cyber-security or anomaly detection techniques. The concept of self-protection for smart inverters serves as an additional layer of safety, complementing existing communication- and system-level methodologies. In this section, the contributions of this dissertation in developing self-protective methods using reference models are outlined.

This dissertation introduces the self-learning feature of self-protective inverters, which significantly enhances their ability to evaluate normal operating regions in real-time. This is achieved by estimating unknown system parameters and utilizing known parameters obtained from measurements. Inverters can avoid abrupt shutdowns and sustain normal operation by incorporating this feature. This feature can help a smart inverter to detect anomalies resulting from potentially harmful incoming setpoints, thereby preventing engagement with the local controller. Additionally, when inverters can estimate input and output circuit parameters, they can readjust the thresholds in the self-protection algorithm accordingly [97]. This dissertation introduces and validates two real-time techniques for estimating unknown system (grid) parameters [142]. The developed methods, namely model reference estimation and recursive least squares, have been experimentally verified and proven effective in real-time grid parameter estimation.

This work develops self-protection for grid-interactive smart inverters based on analytical reference models to inspect the validity of any incoming setpoints before engaging those to

the inverter’s local controller. There are many inverter dynamic models or stability criteria in the literature [96, 143] that can be implemented as the dynamic reference model for self-protective inverters. The proposed self-protection concept is formed using the inverter’s maximum power capability in the steady-state linear and nonlinear operating regions and the inverter’s dynamic response to any incoming setpoints [97]. In steady-state analysis, instability can be observed when the incoming setpoint is located outside the grid-interactive inverter’s stable operation boundary, resulting in oscillatory output power, high harmonic distortions, and low power quality. An incoming setpoint can pass the steady-state inspections, but it can cause unbounded power oscillation, which is also addressed in this work. It should be emphasized that the proposed self-protection (self-security) concept should not be confused with conventional cyber-security methods.

This dissertation introduces a stability criterion for grid-interactive inverters, improving the effectiveness of the self-protective algorithm in real-time applications. The stability criterion is derived from a reduced-order inverter model. Unlike the full-order model, the stability criterion derived from the reduced-order model requires less computational burden and enables faster analysis [111, 144]. This makes it particularly suitable for large-scale systems and real-time applications. The effectiveness of the stability criterion is validated through hardware experiments, confirming its accuracy in detecting both known and hidden instability modes.

This dissertation also introduces a novel hybrid dynamic model, combining data-driven and analytical approaches. Two forms of the model are presented using a data-driven neural network platform. One model uses analytically evaluated risk factors as inputs to predict stable and unstable operations [145]. The other model utilizes the data-driven neural network and a developed stability criterion to make predictions [124]. A standard neural network benchmark is implemented for comparison. The effectiveness of the hybrid dynamic models is thoroughly evaluated through simulations and hardware tests, demonstrating their practical applicability.

1.4 Organization of the Dissertation

The remainder of this dissertation is organized as follows.

Chapter 2 presents the self-learning feature for self-secure inverters. Self-learning is a process in which smart devices can autonomously learn their capabilities or characteristics using their input and output data. Self-learning inverter requires estimating the unknown grid parameters in real time. This chapter presents model reference methods and recursive least square methods to estimate the unknown grid parameters in real time.

Chapter 3 presents self-protection for grid-interactive smart inverters based on analytical reference models to inspect the validity of any incoming setpoints before engaging those to the inverter's local controller. The self-protection concept is formed using steady-state and dynamic reference models. The efficacy of the developed self-protection strategy has been tested using a laboratory setup, including a three-phase 3 kVA inverter and a 12 kW regenerative grid emulator.

Chapter 4 presents a stability criterion for inspecting the incoming power setpoints and predicting the safe operating region of an inverter. The stability criterion is developed from a reduced-order inverter model. The motivation behind employing the stability criterion instead of a full-order inverter model is discussed. The developed stability criterion is validated through a three-phase 3 kVA inverter for both known instability modes and hidden instability modes.

Chapter 5 presents a self-security algorithm using a hybrid neural network-based analytical criterion to detect malicious setpoints. This chapter presents a new method to secure grid-interactive inverters against manipulated setpoints. The results demonstrate that the proposed method can significantly enhance the security of inverters by examining power setpoints using the hybrid model before engaging the setpoint to the local controller. The findings of this work are experimentally verified using a small-scale two-level 208 V, 3 kVA inverter connected to a 12 kW NHR 9410 power grid emulator.

Finally, a summary of the presented research in this dissertation and the contribution

to the state-of-the-art regarding the self-protective methods are presented in Chapter 6. Furthermore, suggestions for future work in updating the developed self-protective methods for safety and security of smart inverters is also presented in Chapter 6.

Chapter 2

Self-learning Algorithms to Estimate the Grid Parameters

This chapter focuses on the self-learning feature of a self-protective inverter for unknown grid parameter estimation. The inverter must learn about the input and output circuits to determine its normal operating region by estimating unknown system parameters. To achieve this goal, two real-time grid parameter estimation techniques, namely the model reference adaptive estimation method and the recursive -least square method, are introduced in this chapter. The content of this chapter is organized into six sections.

Section 2.1 provides the system description and modeling details. The real-time grid parameter estimation algorithm is discussed in 2.2. The recursive-least square method is presented in 2.3. Section 2.4 discusses the model reference adaptive estimation method. The recursive-least square estimation method is utilized in this dissertation to develop the self-protective method for grid-interactive inverters, as discussed in chapter 3. Section 2.5 demonstrates the experimental validation of the developed grid parameter estimation methods. Concluding remarks are given in Section 2.6.

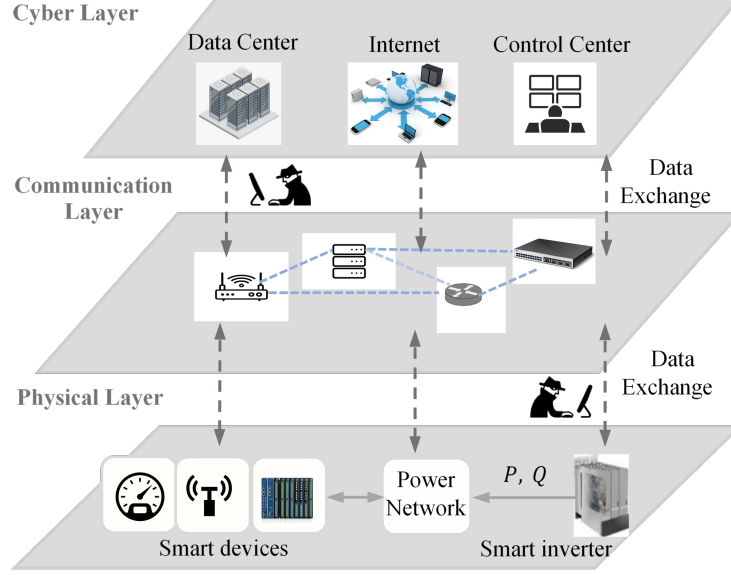


Figure 2.1: *Smart inverters connected to the power grid and cyberattack scenarios in a cyber-physical system.*

2.1 System Description and Modeling

The smart inverter-based cyber-physical network, studied under different malicious cyber-attacks, is presented in this section, see Fig. 2.1. Physical devices such as grid-connected inverters, transmission cables, loads, battery chargers, transformers, etc., can be considered physical device categories. On the contrary, devices such as utility controllers, central data processor units, etc., that can establish a remote connection to the inverters form a remote communication network, also known as a cyber network. The risk of cyber-attacks increases for smart inverters when a cyber network allows data sharing between inverters and utility operators. A three-phase two-level voltage source converter can be programmed as a smart inverter, as shown in Fig. 2.2. The inverter is connected to the point of common coupling (PCC) through an LCL filter, the controller of the smart inverter is programmed in a digital signal processor, DSP. The voltage and current sensors are located at the point of common coupling, PCC. Herein, L_1 , L_2 , C_f , and Z_g denote the inverter-side inductance, the grid-side inductance, and the capacitance of the filter connected in delta, the Thevenin equivalent impedance between the PCC and the grid, respectively. The input and output circuits of

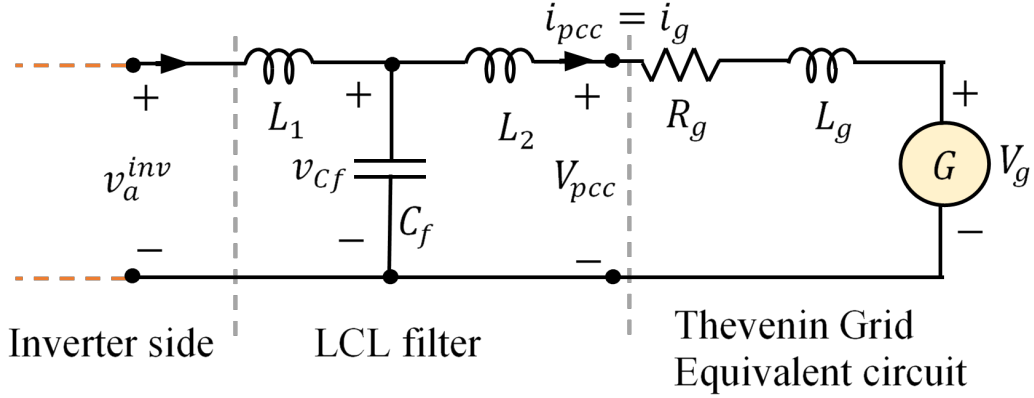


Figure 2.2: *Simplified phase-a circuit of a three-phase grid-interactive VSI.*

the inverter are required to determine its normal operating region. The normal operating region of the grid-interactive inverter is a function of the dc bus voltage, V_{dc} , the Thevenin voltage seen from the PCC, V_g , and the Thevenin impedance seen from the PCC, Z_g . This chapter formulates two different grid parameters estimation techniques to estimate Z_g in real time.

2.2 Real-time Grid Parameters Estimation Algorithm

This work implements two adaptive identification techniques: adaptive model reference and recursive least square methods to estimate unknown grid parameters. For the formulation of the real-time grid-parameter estimation techniques, one phase of a three-phase inverter is considered, as shown in Fig. 2.2. In the literature, there are many active and passive methods [146–148] for grid parameter estimation, such as adaptive identification techniques, voltage transients, signal injections, etc. However, these methods cannot be directly applied for Z_g and V_g estimation because the grid voltage, V_g , is unknown. Using KVL at the PCC in Fig. 2.2, one can obtain the following equation.

$$V_{pcc} = R_g i_g + L_g \frac{di_g}{dt} + V_g \quad (2.1)$$

This work uses the signal perturbation technique to find the grid parameters. There are two techniques for signal injection: (i) low-frequency signal injection and (ii) high-frequency signal injection [149–151]. Nevertheless, there are significant disadvantages to the high-frequency signal injection method. One of the problems is that the high-frequency injection should be performed precisely so the active LCL filter connected to the inverter output does not attenuate the high-frequency components of current or voltages [152–154]. On the other hand, the low-frequency signal is not attenuated by the LCL filter [155, 156]. In this work, a low-frequency signal injection method introduces an external perturbation momentarily when new setpoints are received. Applying KVL at the PCC, one can calculate

$$\hat{V}_{pcc} = R_g \hat{i}_g + L_g \frac{d\hat{i}_g}{dt} \quad (2.2)$$

where $\hat{i}_g$ represents the current injected into the grid at $f_{in} \neq 60Hz$ and $\hat{V}_{pcc}$ represents the measured voltage at the PCC at f_{in} . Notice, f_{in} is required to be chosen such that the grid voltage does not have any element at that frequency, i.e., $\hat{V}_g = 0$.

2.3 Recursive Least Square Estimation Method

This sub-section describes the RLS formulation for the Z_g estimation. The output measurement for the RLS, $y(t)$ at the time instant t_1 can be represented as follows, see Fig. 2.3

$$y(t_1) = \hat{i}_g(t_1), \quad (2.3)$$

and $u(t)$ is the input measurement for the RLS

$$u(t_1) = \hat{V}_{pcc}(t_1), \quad (2.4)$$

Consider T is the sampling time of the measurement and matrix $A = \begin{bmatrix} a_1 & a_2 \end{bmatrix}^T$, which includes unknown parameters and measurement matrix $W = \begin{bmatrix} -y(t_1) & u(t_1) \end{bmatrix}^T$. The parameters can be expressed as $a_1 = (L_g T / R_g - 1)$ and $a_2 = T / L_g$. Therefore, the grid

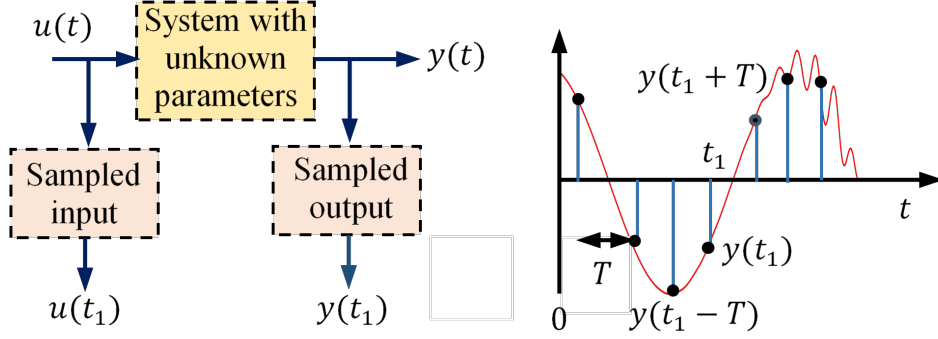


Figure 2.3: *RLS formulation for grid impedance estimation.*

inductance can be represented as $L_g = T/a_2$, and grid resistance can be represented as $R_g = L_g T/(1 + a_1)$. In the recursive form, the least square problem is formulated using (2.5) and (2.6). Here M is the number of measurements, R_M is the covariance matrix, where it is initialized as is 2 by 2 identity matrix, μ is the forgetting factor bounded as $\mu = [0 \ 1]$ where μ is selected between 0.85 and 0.95. In addition, the unknown parameter vector A can be estimated for M measurements as,

$$A_M = A_{M-1} - R_M^{-1} W(t_M) (W^T(t_M) A_{M-1} - y(t_M)), \quad (2.5)$$

where the covariance matrix R_M is defined as

$$R_M = \sum_{i=1}^{M-1} \mu^{M-i-1} W(t_i) W^T(t_i) + W(t_M) W^T(t_M), \quad (2.6)$$

Estimated R_g and L_g can be used to calculate the grid voltage using

$$V_g = V_{pcc} - R_g i_g - L_g \frac{di_g}{dt} \quad (2.7)$$

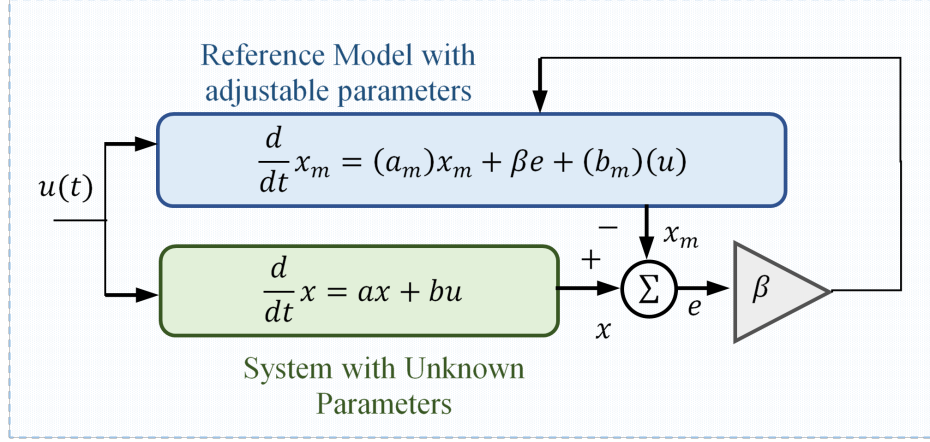


Figure 2.4: General block-diagram of parallel-series model reference identification technique.

2.4 Model-Reference Adaptive Estimation Method

In addition to the recursive least square method, the parallel-series model-reference parameter estimation method is implemented to estimate the unknown grid parameter. The system block diagram is presented in Fig. 2.4. Similar to the recursive least square estimation method model reference estimation method can be implemented using (2.2). From (2.3), the unknown system parameters are defined as $a = -R_g/L_g$ and $b = 1/L_g$. Likewise, the adaptable reference model parameters can represent as $a_m = (-R_{g,est})/L_{g,est}$ and $b_m = 1/L_{g,est}$. Thus, the discrepancy in parameter values can be calculated from $\Delta a = a - a_m = (-R_g)/L_g - (-R_{g,est})/L_{g,est}$ and $\Delta b = b - b_m = (1/L_g) - (1/L_{g,est})$. For accurate real-time estimation, δa and δb should be reduced. Furthermore, the error in the state variable is required to be reduced to ensure that the reference model and system are matched. The dynamics of the error can be presented as follows,

$$\frac{de}{dt} = (a_m - \beta)e + (a - a_m)\hat{i}_g + (b - b_m)(\hat{V}_{pcc}) \quad (2.8)$$

For the purpose of minimizing error, a proper positive definite Lyapunov function, V , presented in (2.9), can be defined for the system described in (2.8). The Lyapunov function must be selected such that $V \geq 0$ and $de/dt < 0$. The Lyapunov function defined in (2.9)

satisfied the requirements [157–159].

$$V = \frac{1}{2}(e^2 + \frac{1}{\gamma}\Delta a^2 + \frac{1}{\Delta b^2}) \quad (2.9)$$

where $\gamma > 0$. The change in V with time can represent by the following,

$$\frac{dV}{dt} = ee\frac{de}{dt} + \frac{1}{\gamma}\Delta a\frac{d\Delta a}{dt} + \frac{1}{\gamma}\Delta b\frac{d\Delta b}{dt} \quad (2.10)$$

Substituting (2.6) into (2.8) results in

$$\frac{dV}{dt} = (a_m - \beta)e^2 + \Delta a(\hat{i}_g e + \frac{1}{\gamma}\frac{d\Delta a}{dt}) + \Delta b(e(\hat{V}_{pcc}) + \frac{1}{\gamma}\frac{d\Delta b}{dt}) \quad (2.11)$$

Based on 2.11, if $a_m < 0$, $e\hat{i}_g + \frac{1}{\gamma}\Delta\dot{a}$, $e(\hat{V}_{pcc}) + \frac{1}{\gamma}\Delta\dot{b} = 0$, then $\dot{V} \leq 0$. Thus, $\Delta\dot{a} = -(\gamma)e\hat{i}_g$ and $\Delta\dot{b} = -(\gamma)e\hat{V}_{pcc}$. Consequently, we can write

$$\begin{cases} a_m = \gamma \int e(t)\hat{i}_g(t)dt \\ b_m = \gamma \int e(t)\hat{v}_{pcc}(t)dt \end{cases} \quad (2.12)$$

Once b_m is estimated, the grid inductance $L_{g,est} = 1/b_m$. The grid resistance can be estimated from $R_{g,est} = -a_m/b_m = -a_m L_{g,est}$. The accuracy of the real-time estimation can be enhanced by choosing γ properly [157, 158]. Then, the estimated grid parameters are sent to the self-protective reference model to adaptively check the validity of incoming power setpoints [97].

2.5 Experimental Verification

In this section, the performance of two grid-parameter estimation techniques is demonstrated experimentally using the hardware setup shown in Fig. 2.5. In this setup, a three-phase 5 kVA SiC MOSFET-based inverter is used, and the switching signals for the inverters are generated using the dSPACE MicroLabBox. In the experimental setup, the inverter feeds a 12

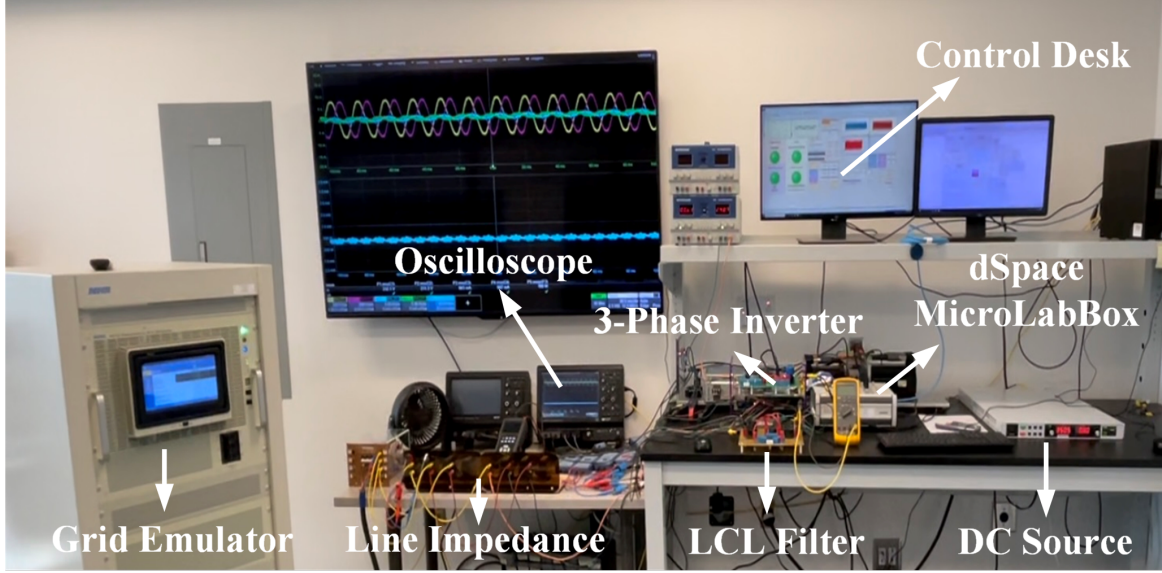


Figure 2.5: Hardware setup for 3 kVA three-phase grid-interactive inverter, implementing real-time grid parameter estimation.

Table 2.1: System parameters to validate real-time grid parameter estimation methods

Parameters	Value
Nominal line-line voltage, V_n	208 V
DC bus voltage, V_{dc}	350 V
Fundamental frequency, ω_n	$2\pi(60) \text{ rad/s}$
PWM switching frequency, f_{PWM}	20 kHz
Inverter side inductance, L_1	1 mH
PCC side inductance, L_2	0.5 mH
Filter capacitance, C_f (in Δ)	5 μF
Filter damping resistance, R_{cf} (in Δ)	3.3 Ω
Grid inductance, L_{grid}	5 mH
Grid resistance, R_{grid}	0.2 Ω

kW NHR 9410 power grid emulator through a three-phase LCL filter. Also, a programmable Magna-Power SL400-15/208 dc supply is used as an input dc source for the inverter. The presented result in this section are recorded using Control Desk, a real-time software interface with dSPACE MicroLabBox, and then plotted using MATLAB. Fig. 2.6 presents the measured voltage and current waveform after low-frequency signal perturbation. The Low-frequency signal must be perturbed for a very short period of time because prolonged perturbations can make the system unstable [160, 161].

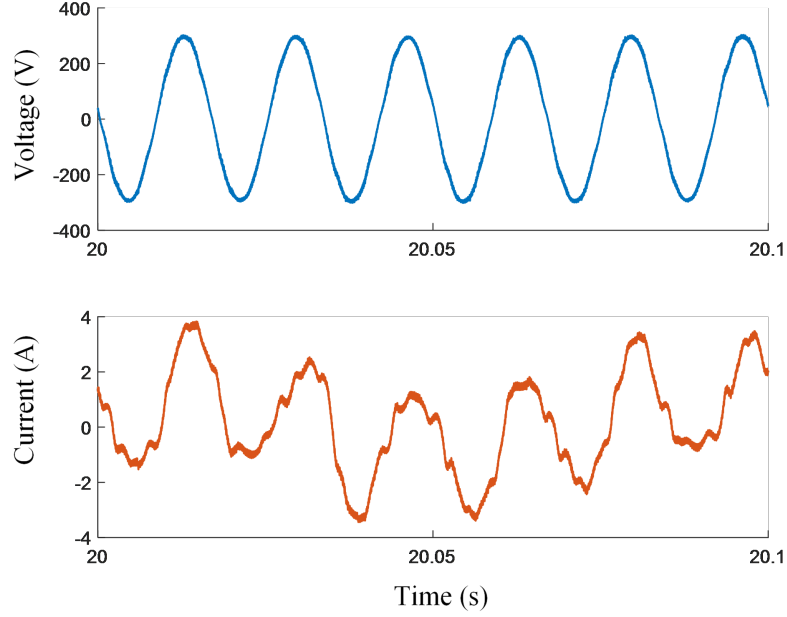


Figure 2.6: *Measured voltage (top) and current (bottom) waveform after low-frequency signal injection.*

The experimental results of estimating the grid inductance and resistance using the model reference adaptive estimation method are shown in Fig. 2.7. Initially, a per phase $2.5mH$ is inserted between the PCC and the grid emulator. The Thevenin equivalent inductance, observed from the PCC to the grid side, comprised the combined effect of the inserted inductance and the inherent inductance of the grid emulator. A low-frequency signal was injected for a short duration to perform real-time grid parameter estimation. The model reference estimation method yielded an estimated inductance of $5.5mH$, while the estimated R_g for $2.5mH$ inserted inductance was 0.42Ω . To validate the accuracy of the real-time grid parameter estimation method, additional inductance was introduced at time instances $t = t_1$ and $t = t_2$. Consequently, the estimated Thevenin inductances observed from the PCC were $8.3mH$ and $15.5mH$, respectively. The calculated error for these estimations is 8.04% and 15.38% , respectively.

The experimental results of estimating the grid inductance and resistance using the recursive-least square estimation method are shown in Fig. 2.8. Initially, a per phase $2.5mH$ is inserted between the PCC and the grid emulator. The Thevenin equivalent inductance,

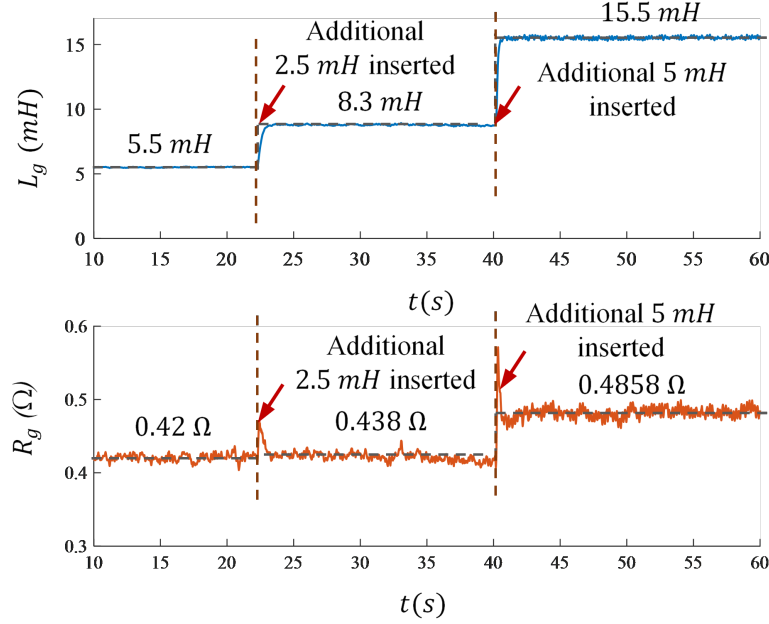


Figure 2.7: Estimation result from control desk (a) grid inductance (L_g), and (b) grid resistance (R_g) estimation using Model Reference Estimation method .

observed from the PCC to the grid side, comprised the combined effect of the inserted inductance and the inherent inductance of the grid emulator. A low-frequency signal was injected for a short duration to perform real-time grid parameter estimation. The recursive least square estimation method yielded an estimated inductance of 5.5 mH, while the estimated R_g for 2.5mH inserted inductance was 0.42. To validate the accuracy of the real-time grid parameter estimation method, additional inductance was introduced at time instances $t = t_1$ and $t = t_2$. Consequently, the estimated Thevenin inductances observed from the PCC were 8.3mH and 15.5mH, respectively. The calculated error for these estimations is 8.04% and 15.38%, respectively.

In addition to incorporating the recursive least square and model reference estimation methods, this dissertation goes a step further by introducing and developing an analytical method specifically designed for real-time grid parameter estimation. This novel approach is implemented and tested within control hardware in the loop (CHIL) using Typhoon-HIL real-time simulator. The details regarding the formulation of this analytical method and the results obtained through real-time simulations are extensively discussed in Appendix B. By

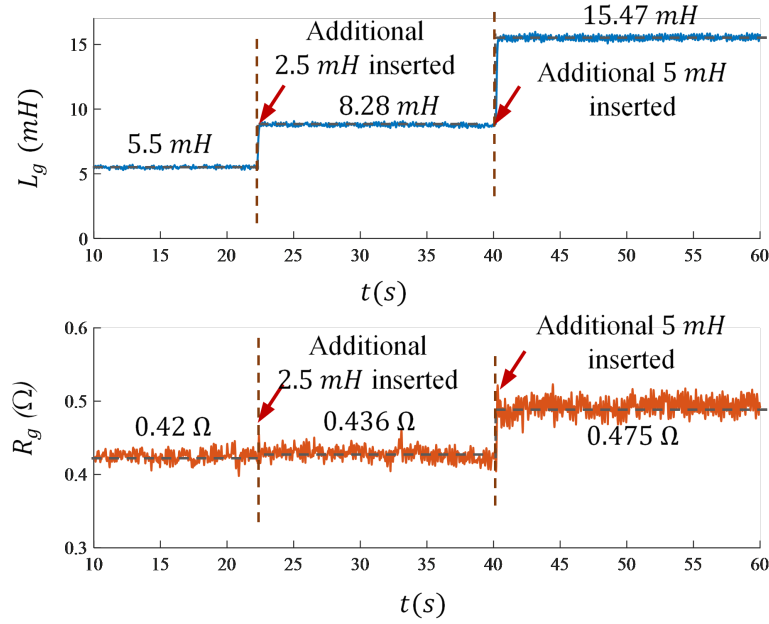


Figure 2.8: Estimation result from control desk (a) grid inductance (L_g), and (b) grid resistance (R_g) estimation using Recursive Least Square Estimation method.

presenting these findings, the dissertation aims to provide a comprehensive understanding of the analytical method's effectiveness and its potential impact on grid parameter estimation in real-time scenarios.

2.6 Conclusion

In this chapter, two methods for real-time grid parameter estimation have been developed and experimentally verified. The findings can be summarized as follows:

- A signal injection-based grid parameter estimation technique has been developed, enabling estimation when a new PQ setpoint is commanded to the controller of an inverter.
- The recursive-least square method has been formulated for real-time grid parameter estimation and implemented on the hardware.
- The model reference estimation method has been formulated for real-time grid parameter estimation and implemented on the hardware.
- Furthermore, the performance of both grid parameter estimation methods has been

compared. The results indicate that the recursive-least square estimation method outperforms the model reference adaptive estimation method. Based on these findings, the recursive-least square method has been chosen to develop the self-protective algorithm discussed in Chapter 3.

Chapter 3

Self-Protective Smart Inverters Using Analytical Reference Model

This chapter focuses on the concept of self-protective inverters using steady-state and dynamic reference models. The self-protection strategy inspects incoming setpoints from the utility operator or third-party aggregators using analytical reference models before engaging the setpoints to the inverter's local controller. When a malicious setpoint passes the existing security layers, a smart inverter can examine the integrity of an incoming setpoint in real time. The content of this chapter is organized into five sections.

The concept of self-protection is presented in Section 3.1. Section 3.2 provides the details of the developed Self-Protection method. 3.3 presents the description of reference models for the self-protective inverters, which includes the load flow steady-state model and full-order dynamic model. Section 3.4 demonstrates the experimental validation of the developed self-protective method of inverters. Concluding remarks are given in Section 3.5.

3.1 Self-Protection Concept for Inverters

The communication and security protocols and system-level security can fail to detect harmful incoming PQ setpoints that are sent from an authorized user like a utility operator. There-

fore, an additional protection layer is essential for inspecting incoming setpoints to maintain safe operation. This article considers setpoints sent from authorized or unauthorized sources, such as utility operators and man-in-the-middle; see Fig. 3.1. The self-protective inverters can predict any anomaly that may happen as a result of engaging an unsafe setpoint. The harmful setpoints can sneak around the communication protocols and system-level security systems, where this device-level strategy can apply reference models to protect the inverter. The models can be established based on physical and mathematical equations. Also, an inverter can be treated as a black box when the reference models can be formed based on input and output data using offline training and machine learning techniques. However, this article utilizes analytical multi-reference models to predict any anomaly that may happen due to a harmful setpoint. Implementing analytical reference models requires significantly less processing time than data-driven machine-learning techniques. When the malicious data bypasses the existing security features, self-protective (or self-secure) inverters can examine the integrity of the data in real-time using the reference models. If the analytical reference models can be updated in real-time, the accuracy of the self-protection strategy becomes promising. Updating data-driven models can be challenging compared to updating analytical reference models.

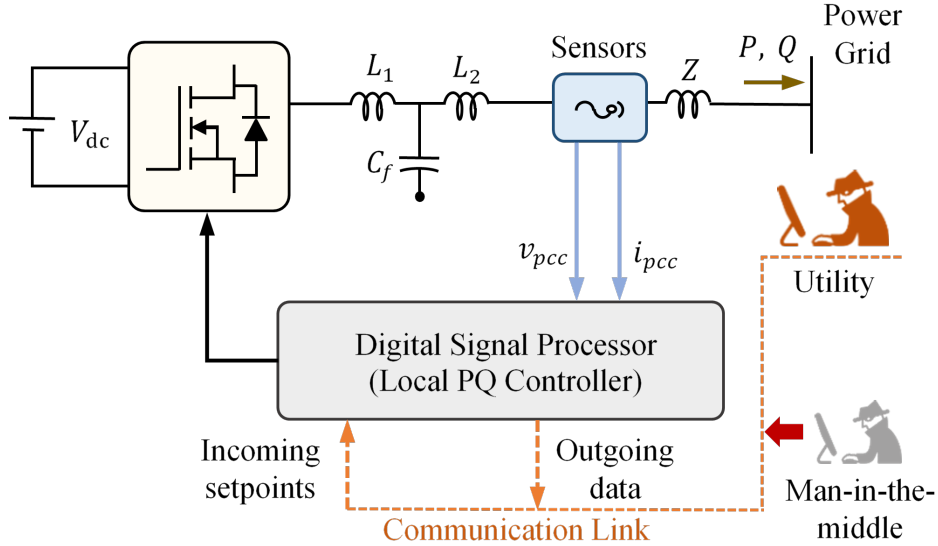


Figure 3.1: *Unsafe PQ setpoints from authorized sources and man-in-the-middle attacks to smart inverters can pass the conventional security layers.*

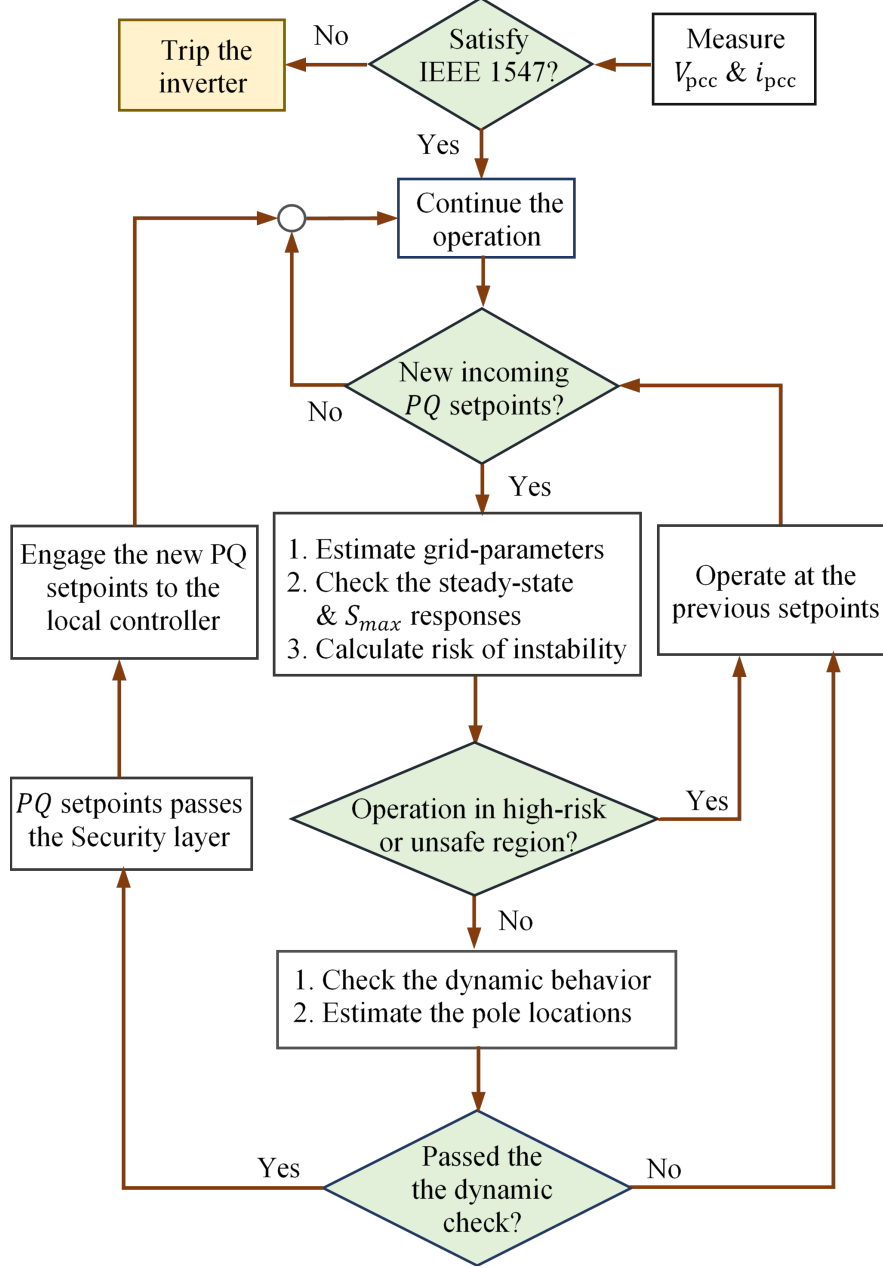


Figure 3.2: Flowchart of the self-protection concept for smart inverters.

3.2 Developed Self-Protection Method

Inverters equipped with self-learning features can examine or predict their current or future operation points [96]. Application of this feature to a grid-interactive smart inverter can become a powerful solution to predict whether the inverter's operation will remain in normal

operation, operate in a highly nonlinear region, or cause instability when the incoming setpoints are received or system parameters change. If an inverter can estimate the input and output circuit parameters, such as the dc-bus voltage and the grid impedance and voltage, the self-protection can be enhanced for any incoming setpoints. Learning the safe and unsafe operation boundaries and dynamic response before engaging an incoming setpoint is herein called self-learning for self-protective (or self-secure) inverters. In the proposed technique, the self-learning process is used to determine: (i) the inverter's normal operation and stability boundaries for steady-state analysis and (ii) the characteristics of the inverter for dynamic analysis.

The flowchart of the developed self-protection method is presented in Fig. 3.2. The incoming setpoints are first verified by the requirements of the IEEE Std. 1547 for PCC voltage measurements [53]. Once the IEEE standards are verified, the self-protection algorithm momentarily injects a low-frequency signal to estimate the grid parameters in real-time. Then, the incoming setpoints are first examined using the steady-state reference model that includes the capability, linear operation, and stable operation boundaries. Based on the risk of unsafe operation defined by the steady-state model for the incoming setpoints, if the incoming setpoints fall in high-risk or unsafe regions, the setpoints can be automatically rejected by the self-protection method, and the previously accepted setpoints remain in operation. The setpoints will not be examined using the dynamic reference model in such cases. However, if the incoming setpoints fall in no-risk (optimal) or low-risk regions, the setpoints will be further examined by the dynamic model to determine the location of the system eigenvalues from the A matrix of the full-order model, which is explained in 3.3.2. After the setpoints are verified by the steady-state and dynamic reference models, the incoming setpoints are accepted to be engaged as the new inputs to the local controller.

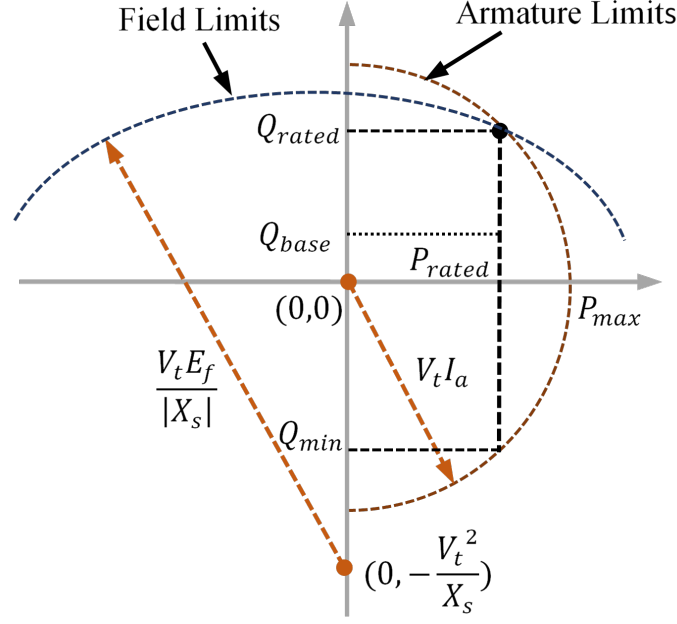


Figure 3.3: *The capability curve of a synchronous generator.*

3.3 Reference Models for Self-Protective Inverters

3.3.1 Load Flow Steady-State Model

The concept of the steady-state safe operation region of an inverter can be explained by comparing the normal/linear operating region of a grid-interactive inverter to the capability curve of a synchronous generator. The armature and field limits define the capability boundary of a synchronous generator in which the machine can operate safely, as shown in Fig. 3.3. The inverter's VA limit curve and the capability boundary is shown in Fig. 3.4. For the synchronous generator, the armature limit region is a circle with a radius $V_t I_a$, centered at $(0, 0)$. The field limit region is represented with an ellipse with a radius of $(V_t E_{af})/|X_s|$, centered at $(0, -V_t^2/X_s)$ where V_t is the terminal voltage of the generator, E_{af} is the field-induced voltage, and X_s is the synchronous reactance. The safe operation region can then be identified as the overlap area of the two limits. Similar to the safe operating region concept of synchronous generators, the power flow from the inverter to the grid can be written as [162].

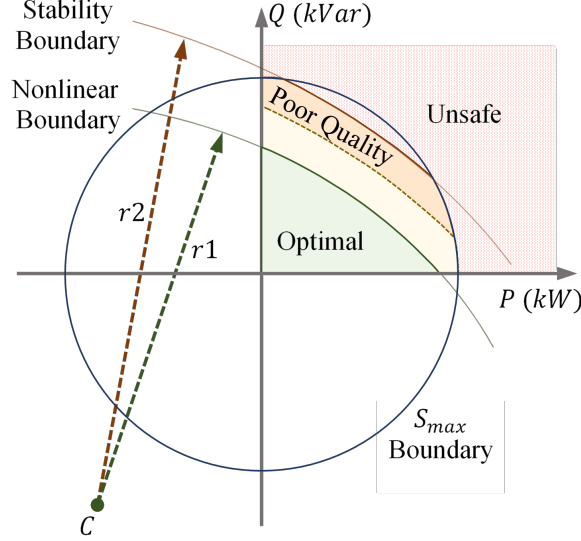


Figure 3.4: Operating regions of a grid-interactive inverter.

$$\left(P + \frac{|V_{Th}|^2 \cos(\theta_Z)}{|Z|}\right)^2 + \left(Q + \frac{|V_{Th}|^2 \sin(\theta_Z)}{|Z|}\right)^2 = \left(\frac{k_{m,i} V_{dc} |V_{Th}|}{|Z|}\right)^2 \quad (3.1)$$

The circle with the radius of S_{max} centered at the origin, as shown in Fig. 3.4, represents the rated capacity of an inverter, where $P^2 + Q^2 \leq S_{max}^2$ [99, 100, 163]. Similar to the normal operating region for synchronous generators, the power flow equation must also be satisfied. This equation can be written in terms of V_{th} , V_{dc} , and $Z_{th} = (Z_f + Z_g)$, where V_{th} and Z_{th} denote the estimated grid-side Thevenin voltage and impedance seen from the inverter terminals, respectively. The load flow equation will form the active and reactive power boundary region as a circle in the PQ-plane centered at C and radius of r and as follows [98]:

$$\begin{cases} C = -\frac{|V_{th}|^2 \cos \theta_z}{|Z_{th}|} - j \frac{|V_{th}|^2 \sin \theta_z}{|Z_{th}|} \\ r = \frac{k_m V_{dc} |V_{th}|}{|Z_{th}|}. \end{cases} \quad (3.2)$$

where θ_Z is the angle of the impedance, V_{dc} is the measured dc-bus voltage, and $k_m = V_{(LL,rms)}/V_{dc}$ is the dc-bus utilization factor. For SPWM in the linear region, this factor

equals $m\sqrt{3}/(2\sqrt{2})$ when $0 < m \leq 1$ [164–166]. As the modulation index increases to $m = 1$, the center point of the circle given in (3.2) does not change; however, the radius increases to the nonlinear boundary operation of a grid-interactive inverter, marked by r_1 in Fig. 3.4. Increasing k_m further to $2\sqrt{3}/(\pi\sqrt{2})$ pushes the inverter at its stability boundary, known as the six-step pattern when the inverter cannot utilize the dc-bus voltage more than that for a given line-to-line voltage; marked by r_2 in Fig. 3.4. Notice r_2 also denotes the radius of the load flow circle and the outer boundary of the nonlinear region. For $r_1 < r < r_2$, the inverter operates in the overmodulation PWM region, also known as the pulse-dropping region [167–169]. In the overmodulation region, low-order harmonics appear at the output terminals [170, 171].

The load flow circle overlapped with the capacity circle area, i.e., $S < S_{max}$, is the safe region for the inverter operation. On the other hand, the area between the inner circle with a radius of r_1 and the outer circle with a radius r_2 , overlapped by the capacity circle area is the operating area in which the inverter is overmodulated. This area has the risk of instability indirectly due to PLL malfunctions. The stability and nonlinear boundaries can change instantaneously based on the grid and inverter parameters, i.e., V_{th} , V_{dc} , and Z_{th} . The self-protective inverter should not engage any incoming PQ setpoints in unsafe or poor-quality regions shown in Fig. 3.4. Therefore, real-time estimation of these three variables is required and forms the steady-state reference model of self-protective inverters.

In this work, the recursive least square (RLS) technique is used to estimate the grid parameters, V_{th} and Z_{th} , as explained in detail in the literature, e.g., [172] and in chapter 2. A low-magnitude current with a prime frequency is injected into the grid. The prime frequency is selected to ensure that the grid voltage has zero magnitudes at that frequency. The frequency of the injected current should be selected such that the LCL filter does not attenuate the injected signal. Applying KVL at the PCC, see Fig. 3.4; one can calculate $\hat{v}_{pcc} = R_g \hat{i}_g + L_g (d\hat{i}_g/dt)$, where $\hat{i}_g$ is the current injected into the grid, and $\hat{v}_{pcc}$ is the PCC voltage measured at the selected prime frequency when $\hat{V}_g = 0$; herein, $(\hat{\cdot})$ denotes the voltage and current components at the frequency of the injected current.

3.3.2 Dynamic Model

Even in the nominal operating region, where the steady-state model indicates a PQ setpoint is safe to get engaged to the controller, the inverter can be unstable under certain conditions. A dynamic model is also needed to detect such conditions, besides the steady-state load flow restriction shown in Fig. 3.4. The behavior of the PQ-controlled grid-interactive inverter shown in Fig. 3.4 cannot be assumed linear for two simple reasons. The first reason is that the active and reactive control loops measure P and Q, which are nonlinear expressions [144]. The second reason is that the resistance and inductance of the LCL filter are functions of the current (power) flow, temperature, and proximity effects in the filter inductors.

The full-order state-space representation, presented in [21, 173], has been duplicated in this work as the dynamical reference model. The control scheme of a PQ-controlled inverter is shown in Fig. 3.5. The full-order model of the PQ-controlled inverter can be expressed as given in (3.3).

$$\begin{aligned}
 \frac{d}{dt} \begin{bmatrix} i_{inv} \\ v_c \\ i_{gL} \\ y_1 \\ y_2 \\ v_{inv} \end{bmatrix} &= \begin{bmatrix} A_{11} & A_{12} & A_{13}^L & 0 & 0 & A_{16}^C \\ A_{21} & A_{22} & A_{23}^L & 0 & 0 & 0 \\ A_{31}^C & A_{32}^C & A_{33}^C & 0 & 0 & 0 \\ A_{41}^C & A_{42}^C & A_{43}^C & 0 & 0 & 0 \\ A_{51}^C & A_{52}^C & A_{53}^C & A_{54} & 0 & 0 \\ A_{61}^C & A_{62}^C & A_{63}^C & A_{64} & A_{65} & A_{66} \end{bmatrix} \begin{bmatrix} i_{inv} \\ v_c \\ i_{gL} \\ y_1 \\ y_2 \\ v_{inv} \end{bmatrix} \\
 &+ \begin{bmatrix} 0 & b_1 & 0 \\ 0 & b_2 & 0 \\ B_{31}^C & b_3^C & 0 \\ B_{41}^C & b_4^C & B_{43} \\ B_{51}^C & b_5^C & B_{53} \\ B_{61}^C & b_6^C & B_{63} \end{bmatrix} \begin{bmatrix} v_g \\ \omega \\ R^* \end{bmatrix}.
 \end{aligned} \tag{3.3}$$

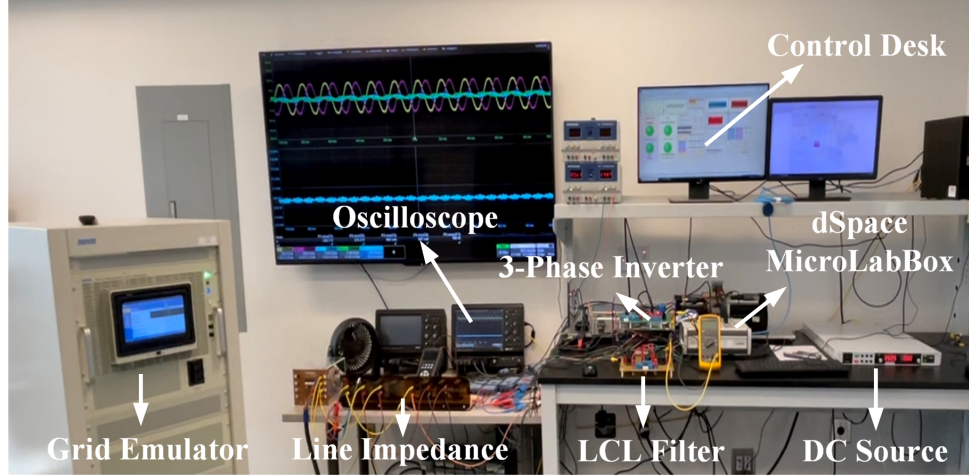


Figure 3.6: *Hardware setup for 3 kVA three-phase grid-interactive inverter, implementing device-level self-protection algorithm.*

the nonlinearity effects at low power levels is experimentally demonstrated in Section 3.4.2.

3.4 Experimental Results

The effectiveness of using reference models for self-protective inverters is verified experimentally using a three-phase grid-interactive hardware setup, as shown in Fig. 3.6. In this setup, a custom-built three-phase 3 kVA SiC MOSFET-based inverter is used. The switching signals of the inverters were generated using the dSPACE MicroLabBox DS-1202 controller board. A custom-made three-phase LCL filter was connected to the inverter's output terminal to filter out the high-frequency components. The three-phase inverter was programmed to inject the desired power into a 12 kW NHR 9410 power-grid emulator. A Magna-Power SL400-15/208 programmable DC supply was employed as the DC source for the inverter. The system parameters are outlined in Table III. All the experimental waveforms were measured using a Teledyne LeCroy HD4096 oscilloscope with CP030 current probes and ADP300 high-voltage differential probes.

Table 3.1: *System parameters for experimental Setup to validate self-protective algorithm*

Parameters	Value
Nominal line-line voltage, V_n	208 V
DC bus voltage, V_{dc}	350 V
Fundamental frequency, ω_n	$2\pi(60)$ rad/s
PWM switching frequency, f_{PWM}	20 kHz
Inverter side inductance, L_1	1 mH
PCC side inductance, L_2	0.5 mH
Filter capacitance, C_f (in Δ)	5 μ F
Filter damping resistance, R_{cf} (in Δ)	3.3 Ω
Grid inductance, L_{grid}	5 mH
Grid resistance, R_{grid}	0.2 Ω

3.4.1 Steady-State Performance Analysis

In this subsection, the steady-state stability boundary is experimentally demonstrated when incoming PQ setpoints fall inside the maximum inverter capacity, i.e., $S < S_{max}$, but outside the steady-state stability region. In order to prove the concept, system parameters were intentionally selected so that unsafe and poor-quality regions of the inverter partly fall inside the inverter's capacity, as depicted in Fig. 3.4. Also, the initial setting is selected to represent practical scenarios following the IEEE Std. 1547 [53]. For instance, the line-to-line voltage of the grid emulator is 219 V in a test scenario, ensuring that the voltage at PCC remains below 1.1 p.u (228.8 V) to satisfy the IEEE Std. 1547.

Assume a safe operating point as $V_{dc} = 350V$ and $V_{LL,rms} = 208V$, when P is 2 kW, and Q is 0.5 kVar. For this 3 kVA inverter, at this operating point, P is curtailed, and Q is injected to raise the voltage at PCC. This PQ setpoint is slightly outside of the optimal operating region. In this test, the boundary of stability is slowly brought to the point where the applied PQ setpoint becomes unsafe by applying the following steps; (i) the grid emulator voltage is first gradually increased from 208 V to 219 V, and then (ii) the dc-bus voltage is slowly reduced until the setpoint is detected as unsafe (outside the stability boundary). As a result, the oscillatory output power is observed when $V_{dc} = 300V$ after $t = 12.5s$, see Fig. 3.7 (a). Notice that the inverter operation gradually becomes unstable, leading to power

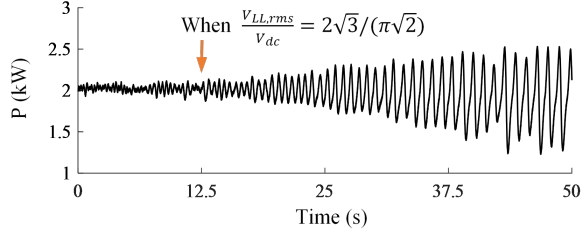


Fig. 6. Experimentally obtained inverter's output power when PQ setpoints gradually fall outside the steady-state stability boundary.

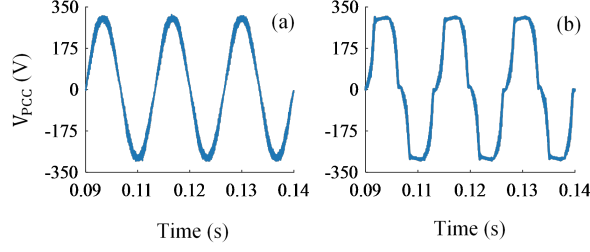


Figure 3.7: Inverter line-to-line voltage at PCC when (a) PQ setpoint is inside the safe region, and (b) PQ setpoint is at the stability boundary.

fluctuations, and gradually increases over time. Also, the voltage waveforms of the baseline condition and near the instability boundaries are compared in Fig. 3.7 (b). Notice that a nearly sinusoidal waveform is observed for the baseline scenario while a square-like, known as a six-step waveform is observed around the stability boundary. This transformation from sinusoidal to distorted waveform verifies the discussion in Section 3.3 regarding the steady-state stability boundary. It is critical at the system level to identify an orchestrated attack on setpoints of inverters, jeopardizing the overall power system stability if the inverters operate in their poor-quality regions.

Fig. 3.7 shows three cases near the instability boundary to statistically evaluate the accuracy of predicting the risk of engaging an incoming setpoint. In these cases, the initial operating points are $PQ_{o1} = (0.5kW, 0.5kVar)$, $PQ_{o2} = (0.5kW, 0.25kVar)$, and $PQ_{o3} = (0.75kW, 0.25kVar)$ at $V_g = 219V$ and $V_{dc} = 300V$, and the incoming setpoints for these three cases are $PQ_1 = (2kW, 0.5kVar)$ for PQ_{o1} , and $PQ_2 = (2kW, 0.25kVar)$ for both PQ_{o2} and PQ_{o3} . The risk is predicted when the self-security algorithm is enabled and the incoming setpoints are received. Then, the self-protection algorithm is disabled, and the

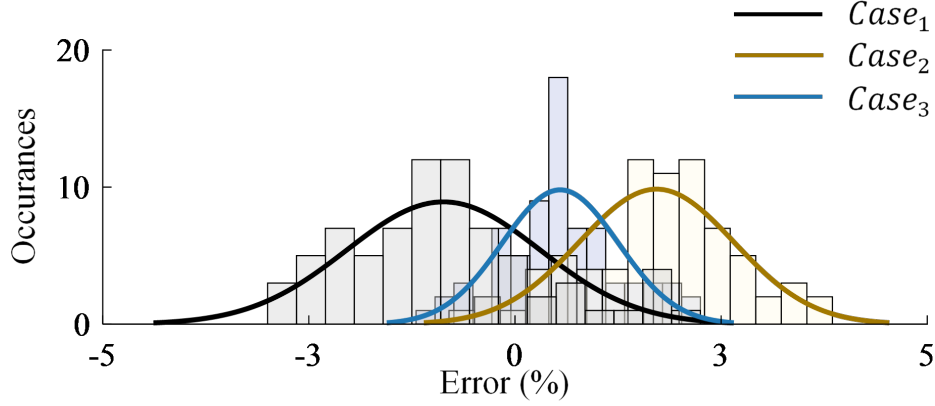


Figure 3.8: *Statistics of the accuracy in risk prediction using the steady-state model.*

actual risks are calculated. The risk factor is evaluated by comparing the distance between the incoming setpoint and the nonlinear boundary (estimated in real-time) to the distance between the instability and nonlinear boundaries, all with respect to the center, C , as shown in Fig. 3.4. This process has been repeated 75 times for each case, and the statistical results are provided in Fig. 3.7. Notice, PQ_1 for the given operating condition leads to instability, see 3.7. In this case, the actual risk is mainly greater than the estimated risk when the mean error μ is -0.87% , and the standard deviation σ is 1.7174 , see $Case_1$ in Fig. 3.7. The results of the other two cases are also shown in Fig. 3.8, wherein $Case_2$ has a mean error of $\mu = 1.72\%$ with a standard deviation of $\sigma = 0.94$, and $Case_3$ has $\mu = 0.55$ with $\sigma = 0.7\%$, respectively. Since $P_{o3} > P_{o2}$, the operating power approaches the incoming P setpoint, and the estimated grid impedance will be closer to the actual effective impedance when $P = 2kW$. Thus, less error can be observed in the risk prediction. The results show that the maximum estimation error is 4.7 . Hence, the steady-state model can nicely predict the harmful incoming setpoints before engaging the setpoint to the controller.

3.4.2 Dynamic Performance Analysis

Prediction of the dynamic response to an incoming PQ setpoint might be the most challenging mission of a self-protective inverter [39]. To demonstrate the need for a dynamic

Table 3.2: *System parameters to demonstrate the dynamic analysis of self-protective inverters*

Case I: $L_2 = 0.5mH$	Case I: $L_2 = 1mH$
$k_{p1} = k_{p3} = 0.001$	$k_{p1} = k_{p3} = 0.0009$
$k_{p2} = k_{p4} = 0.01$	$k_{p2} = k_{p4} = 0.008$
$k_{i1} = k_{i3} = 0.08$	$k_{i1} = k_{i3} = 0.06$
$k_{i2} = k_{i4} = 2.2$	$k_{i2} = k_{i4} = 2$
$V_{dc} = 335V$	$V_{dc} = 332V$
$V_{LL,rms} = 208V$	$V_{LL,rms} = 208V$
$L_1 = 1mH$	$L_1 = 1mH$
$C_f(\Delta) = 27\mu F$	$C_f(\Delta) = 27\mu F$
$L_g = 5mH$	$L_g = 5mH$

reference model, two different case scenarios are considered. The parameters selected for this test scenario are shown in Table 3.2. In Case I, the LCL filter has the grid-side inductance, $L_2 = 0.5mH$, while for Case II, $L_2 = 1mH$. The controller used in these tests is shown in 3.5, and the control parameters selected for these two scenarios are shown in Table 3.2. Notice that an unauthorized and malicious activist can manipulate these gains during a firmware/software update [13]. For this study, the gains and the dc-bus voltage are intentionally selected to place the dominant eigenvalues closer to the stability boundary. Fig. 3.9 shows a hidden unstable setpoint at a low power level, where the setpoint passes the steady-state evaluation. The system is stable initially when $P^* = 100W$ and $Q^* = 0$. An underdamped-stable response is observed when $P^* = 150W$. Once $P^* = 190W$, a marginally stable response is observed (Fig.3.9, Point-B). When $P^* = 250W$, the inverter becomes unstable (Fig. 3.9, Point-C), with the oscillation frequency of $(2\pi/3.02) = 2.08rad/s$. Increasing the input (command) power to $P^* = 400, W$ makes the inverter return to a stable underdamped operation. Notice that the system behavior is nonlinear.

This nonlinear behavior can be explained by considering the active and reactive power in the synchronously rotating dq reference frame locked at PCC, i.e., $v_d^{pcc} = 0$, as $P = (3/2)(v_q^{pcc}i_q)$ and $Q = (3/2)v_q^{pcc}i_d$ [174], where v_q^{pcc} is the magnitude of the phase voltage at PCC, and i_q and i_d represent the line currents in dq-frame if the power equations are linearized around a steady-state operating point as; $P = (3/2)(V_{qo}^{pcc}i_q + i_{qo}v_q^{pcc})$ and $Q =$

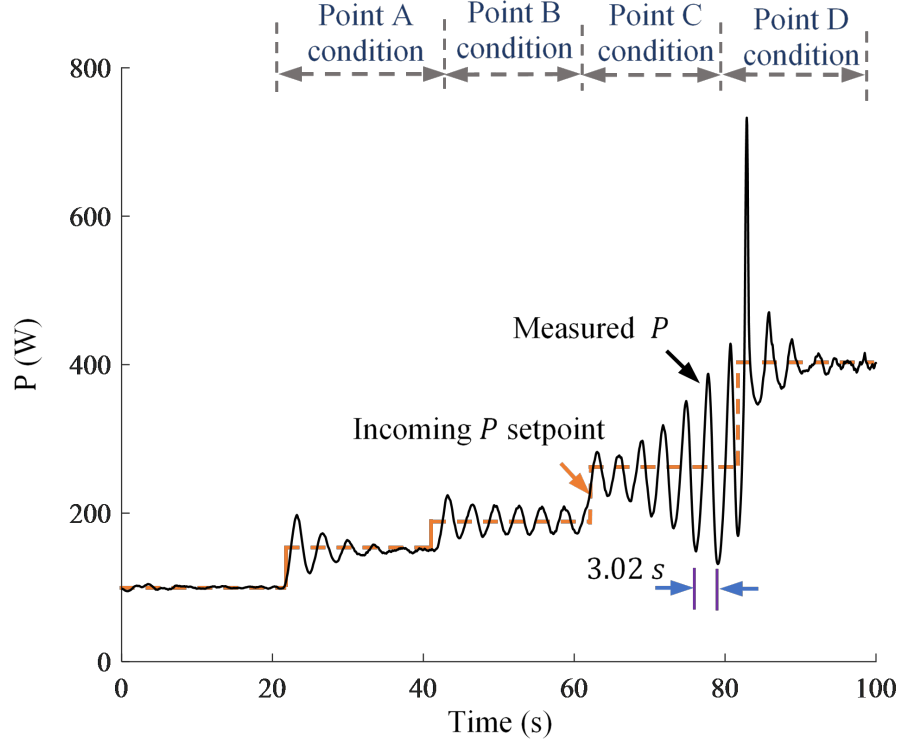


Figure 3.9: Experimentally obtained inverter's dynamic responses when the output power is changing step-by-step from 150 W to 400 W.

$(3/2)(V_{qo}^{pcc}i_d + I_{do}v_q^{pcc})$, where V_{qo}^{pcc} is the q-axis operating voltage, and I_{qo} and I_{do} are the q-axis and d-axis currents, respectively, the operating current, i.e., I_{qo} and I_{do} , will appear in the closed-loop transfer function coefficients. Therefore, the system stability is undeniably a function of setpoints in this nonlinear system.

In Fig. 3.10, the trajectories of a dominant eigenvalue of the system are shown using the full-order model in (3.3). In this root locus study, the filter resistance variation by the current flow has been modeled in Fig. 3.10(a). The low-frequency pole of the full-order dynamic model is initially located at the left-half plane and crosses the stability region at low power levels, see Fig 3.10(b). Furthermore, an incoming PQ setpoint can cause variations in the inverter circuit parameters, particularly in the filter resistance. While for a given set of control parameters, the system can be unstable as the injected power increases, the inherent resistance of the filter and switches can then help the system stability. Therefore, if the control parameters are manipulated or poorly selected, the inverter can become

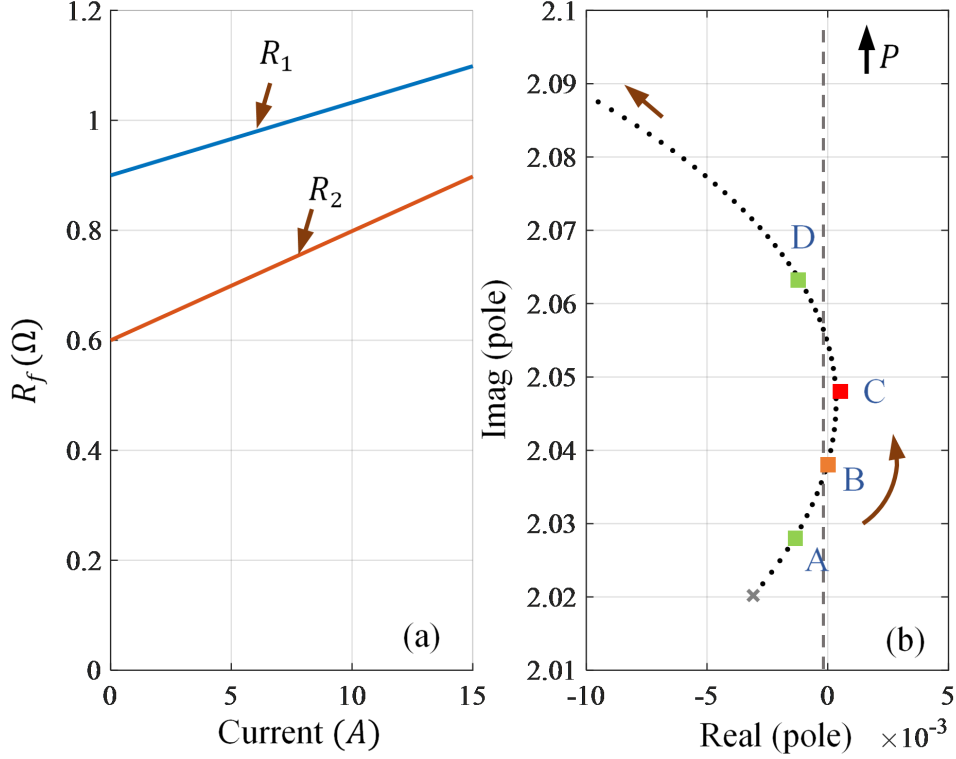


Figure 3.10: (a) R_1 and R_2 versus current, and (b) the trajectory of the dominant positive eigenvalue of the full-order model of a 3kVA, 208V three-phase inverter for Case I.

unstable at low power levels, but as the injected power is increased, the system damping will increase, and the system will return to a stable point, as shown in Figs. 3.9 and 3.10. This irregularity can happen for specific control parameters and at low power setpoints. The full-order system eigenvalues for Case I are presented in Table 3.3 Comparing the frequency of power oscillations in Fig. 3.9 and the eigenvalue at point-C in Fig. 3.10(b) demonstrates how closely the dynamic reference model in (3.3) can predict the system response before engaging the setpoint to the controller. The process of examining a new setpoint on the full-order reference model takes nearly 1 s. Again, this PQ setpoint falls in the steady-state safe operating region. Hence, the dynamic reference is necessary for inspecting incoming PQ setpoints.

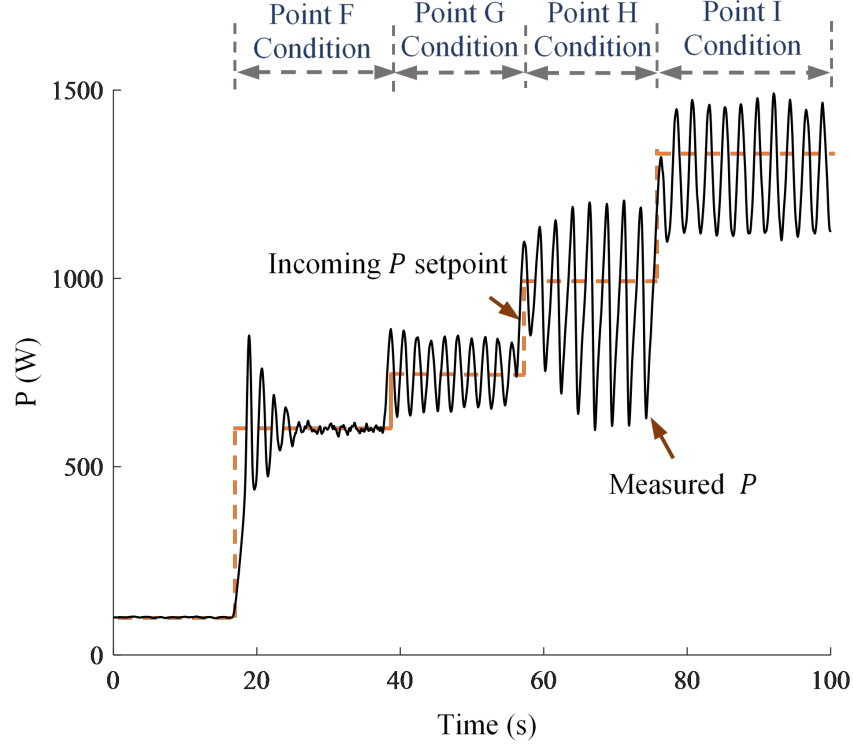


Figure 3.11: Observing the inverter's dynamic behavior for Case II when the output power is changing step-by-step from 0.6 kW to 1.2 kW.

Table 3.3: Eigenvalues using the full order model for Case I

Point A	Point C
$-0.9 \pm 2.2j$	$-0.87 \pm 2.047j$
$-0.7 \pm 1.8j$	$-0.7 \pm 1.8j$
$-212.3 \pm 611.5j$	$-215.3 \pm 617.6j$
$-120.83 \pm 1311j$	$-121.4 \pm 1314j$
$-2600.83 \pm 2030j$	$-2600.3 \pm 2039j$
$-2000.58 \pm 3860j$	$-2013.8 \pm 3859j$

Fig. 3.11 shows a hidden unstable setpoint for Case II, where the setpoint passes the steady-state evaluation similar to the previous scenario. For the newly selected condition, the test scenario was started with $P = 150W$. One can notice from the measured P provided in Fig. 3.11 that a stable operation is observed when $t < 19$ s, as the dominant eigenvalues are on the left-half plane initially, see Fig. 3.12(b). When $t = 19$ s, $P = 600W$ were applied to the controller, and an underdamped-stable response was observed, see Point E Condition

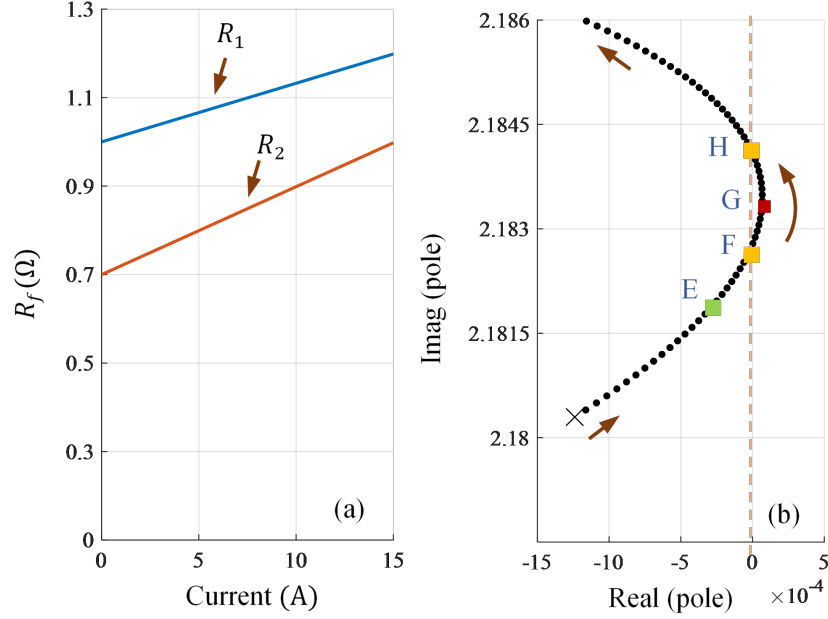


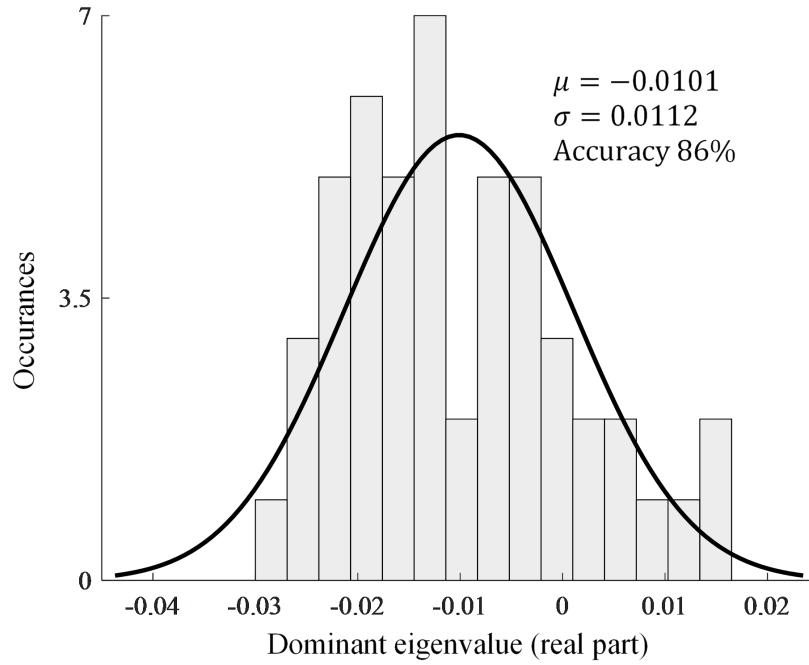
Figure 3.12: (a) R_1 and R_2 versus current, and (b) the trajectory of the dominant positive eigenvalue of the full-order model of a 3kVA, 208V three-phase inverter for Case II.

in Fig. 3.11, as eigenvalues moving closer to the stability boundary in Fig. 3.12(b). When $t = 39s$, $P = 750W$ were applied to the controller, and a marginally-stable response was observed, see Point F Condition in Fig. 13, as eigenvalues are located on the stability boundary in Fig. 3.12(b). When $t = 59s$, $P = 1000W$ were applied to the controller, and an unstable response was observed, see Point G Condition in Fig. 3.11, as eigenvalues are located in the right-half plane in Fig. 3.12(b). When $t = 79s$, $P = 1200W$ were applied to the controller, and a marginally stable response was observed, see Point H Condition in Fig. 3.11, as eigenvalues are located on the stability boundary in Fig. 3.12(b). To observe a stable operation where the eigenvalues move from the right- to the left-half plane, more power needs to be applied. The full-order system eigenvalues for Case II are presented in Table 3.4. To protect the system from being damaged the maximum applied power was limited to 2 kW due to the oscillatory power behavior, the ratings of the inverter, filter, and wires. The full-order model of the inverter can predict the dynamic response, and then the self-protection algorithm can prevent the harmful setpoint from being engaged.

However, a simple stability criterion or a reduced-order model that can approximately

Table 3.4: *Eigenvalues using the full order model for Case II*

Point E	Point F
$-0.000124 \pm 2.18j$	$-0.000124 \pm 2.18j$
$-0.8354 \pm 1.787j$	$-0.8354 \pm 1.787j$
$-616.9 \pm 71.9j$	$-616.9 \pm 71.9j$
$-648.7 \pm 2748j$	$-648.7 \pm 2748j$
$-930 \pm 4290j$	$-930 \pm 4290j$
$-1100.83 \pm 5030j$	$-1100.83 \pm 5030j$

**Figure 3.13:** *Statistics of dominant eigenvalues estimation for the dynamic reference model for changing active power from 100 W to 150 W (Point A)*

represent the system's behavior can be applied for the setpoint inspection [124]. If a stability criterion is used, the inspection process will be less. This can shorten the duration of examining new setpoints compared to a full-order model. Fig. 3.13 and Fig. 3.14 show the calculated real part of the dominant eigenvalue, i.e., R_λ , for the system parameters associated with Points A and C in Fig. 3.11, respectively. The grid parameters are estimated using the recursive least square (RLS) technique [96]. The grid parameters estimation and the eigenvalue calculation can be repeated many times for each point, herein 50 times.

The statistics for estimating the location of the dominant eigenvalue for case I are shown

in Fig. 3.13 and 3.14. The mean value (μ) and the standard deviation (σ) for Point A are -0.0101 and 0.0112, respectively. For Point C, $\mu = 0.0081$ and $\sigma = 0.0112$. Notice that Point A is a stable point, i.e., $R_\lambda < 0$., and Point C is unstable, i.e., $R_\lambda > 0$.. Therefore, from the statistic shown in Fig. 3.14, Point A can be determined as a stable point with 86% accuracy and Point C as an unstable point with 78% accuracy.

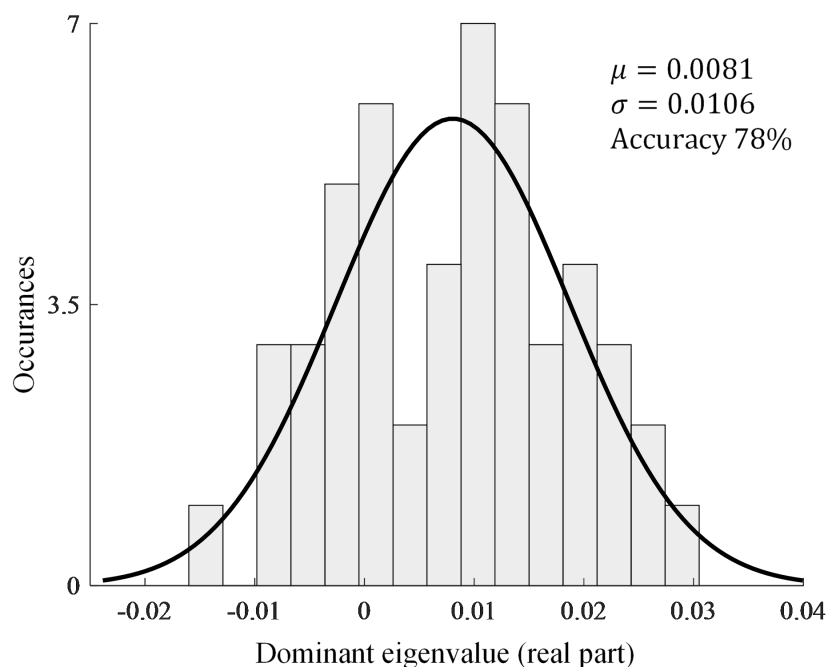


Figure 3.14: *Statistics of dominant eigenvalues estimation for the dynamic reference model for changing active power from 100 W to 250 W (Point C).*

3.5 Conclusion

This chapter has experimentally and statistically verified the self-protection method for grid-interactive inverters. In the self-protection method, the analytical steady-state and dynamic reference models used to inspect incoming PQ setpoints have been explained and validated. The following conclusions can be highlighted-

- The reference models have been developed based on the steady-state linear and non-linear operating regions and a full-order dynamic model of grid-interactive inverters.

- The nonlinear behavior of the inverter has been experimentally demonstrated for both dynamic and steady-state analyses.
- In the steady-state experiment, it has been verified that a decrease in the dc-bus voltage or an increase in the grid voltage can significantly reduce the normal operating region for a given setpoint.
- Furthermore, it has been verified that a change in the setpoint can change the system parameters due to PQ control loops and move the eigenvalues to the instability region for a given set of control gains.
- The developed models for the self-protection method can significantly provide self-security for grid-interactive inverters against intentional (malicious) and unintentional (accidental) unsafe setpoints when the communication protocols, system-level security, and cybersecurity solutions fail to detect those unsafe setpoints.

Chapter 4

Development of Stability Criteria for Self-Protective Inverters

This chapter focuses on analyzing and validating the stability criterion for Self-protective inverters. The contents of this chapter are organized into five sections. Section 4.1 provides the details of the instability modes of grid-interactive inverters, which includes the impacts of the circuit and controller on the instability of inverters. Additionally, this section also describes known and hidden modes of instability. Section 4.2 develops the third-and fifth-order inverter model. Section 4.3 derives the stability criterion to predict hidden and known instability modes. Section 4.4 briefly describes the state-space full-order model of inverters. Eigenvalue analysis for known and hidden instability modes is presented in Section 4.5. Section 4.6 demonstrates the experimental validation of the different instability modes and the developed stability criterion. Concluding remarks are given in Section 4.7.

4.1 Instability Modes of Grid-Interactive Inverters

A grid-following inverter is depicted in Fig. 4.1, injecting power into the grid through an LCL filter. The grid is represented by an equivalent grid inductance, L_g , and resistance, R_g , with grid voltage, v_g . The voltage and current sensors are located after the *LCL* filter

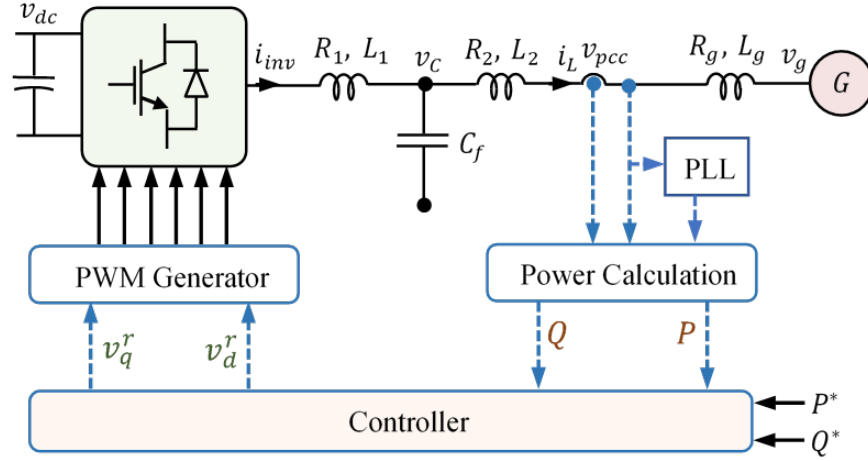


Figure 4.1: Circuit schematic of a grid-following inverter.

at PCC, where the measured voltages and currents are converted to the q-axis and d-axis counterparts. Each P and Q controller has two cascaded loops consisting of an outer power loop and an inner current control loop in q – axis and d-axis, respectively. To generate the reference signal for the PWM generator, the output of the PQ controller provides v_q^r and v_d^r , see Fig. 4.1.

4.1.1 Instability and Circuit Impacts

In this subsection, two high-frequency modes of instability are discussed. The inverter becomes unstable when the output voltage and current waveforms are significantly distorted. A distortion in the output current can also excite the resonance frequency of the LCL filter, which is

$$f_r = \frac{1}{2\pi} \sqrt{\frac{L_1 + (L_2 + L_g)}{L_1(L_2 + L_g)C_f}} \quad (4.1)$$

From (4.1), it can be seen that the filter resonance frequency, f_r , may vary by the grid inductance, L_g , and core nonlinearity of the filter's inductors, L_1 and L_2 . Therefore f_r can slightly vary by the operating point and grid condition. The inherent changes in these

inductances can lead to undesirable harmonic amplification. The PQ control parameters are designed for finite bandwidth and are based on the fixed resonance frequency of the output LCL filter. However, the PWM frequency is typically chosen close to $2f_r$. Thus, a control design with a proper stability margin can prevent this type of instability [175–178]. To avoid filter resonance, one solution is to introduce a resistor in series with the *LCL* filter’s capacitor, C_f , which is called passive damping. However, the current and voltage waveforms can be distorted at a frequency above the fundamental frequency. If a specific harmonic component, typically 5^{th} or 7^{th} , is amplified, PLL may lose its accuracy in tracking the phase-angle of the PCC voltage. Notice that overmodulation (or pulse-dropping phenomenon) can also lead to voltage distortion at PCC, appearing mainly in the 5^{th} or 7^{th} harmonic components.

A grid-interactive inverter can inject power into the grid as $P^2 + Q^2 \leq S_{max}^2$, where S_{max} is the maximum capacity of the inverter and/or the input source. The amount of active and reactive power delivered from the inverter’s terminal to the grid can be formulated as [98]

$$S = \frac{|V_i||V_{th}|e^{-j(\delta-\theta_z)} - |V_{th}|^2e^{j\theta_z}}{|Z|} \quad (4.2)$$

where $V_i = |V_i|\angle\delta$ represents inverter output and $V_{th} = |V_{th}|\angle 0$ denotes grid Thevenin voltages, δ is the angle difference between the inverter and grid voltages. $Z = (Z_f + Z_{th})\angle\theta_Z$ is the impedance seen from the inverter’s output terminals. Herein, the inverter’s fundamental output voltage can be represented as $v_i = V_i \sin(\omega t + \delta)$, where $V_i = k_m V_{dc}$ is RMS of the line-to-line voltage, and k_m is called the dc-bus utilization factor. For inverters using sinusoidal PWM (SPWM) $k_m = 0.612m$, and for the space-vector PWM technique (SVPWM), $k_m = 0.707m$, where $0 < m \leq 1$ denotes the modulation index. The capability boundary of an inverter in pumping more power into the grid is limited at $k_m = V_i/V_{dc} = 2\sqrt{3}/(\pi\sqrt{2})$ when the inverter output voltage loses all pulses, and each harmonic component of the line-line voltage is expressed as $v_{i,h} = (\frac{2\sqrt{(3)}}{\pi h})V_{dc} \sin(h\omega t + \delta_h)$. However, the pulse dropping appears at a lower dc-bus utilization factor, i.e., voltage distortion appears if $k_m \geq 0.612$ for SPWM and $k_m \geq 0.707$ for SVPWM. When the inverter operates in this region, the voltage distortion due to over-modulation can indirectly cause the inverter to become unstable.

4.1.2 Instability and Controller Impacts

The controller gain holds significant importance in maintaining stability within grid-connected inverter systems. Specifically, the controller gains in the control system of grid-tied Voltage Source Inverters (VSIs) must be carefully selected and adjusted to ensure stability, particularly in weak grid conditions. In a study referenced as [179], a feasible region is presented for the proportional gains of the controller, taking into account the grid impedance. This region offers guidance on selecting appropriate controller gain values that facilitate stable operation in weak grids. Another study referenced as [180] provides conservative design recommendations for the filter and controller parameters to achieve stability in weak grids. These recommendations help in determining suitable values for the filter and controller parameters that support stable operation. Additionally, the ratio between the resonance frequency of the LCL (Inductor-Capacitor-Inductor) filter and the sampling frequency of the controller is considered. This ratio establishes an upper limit for the controller gains. The system can maintain stable operation by adhering to this limit [181, 182]. Therefore, achieving the desired dynamic characteristics and maintaining stable operation requires appropriate controller gain tuning.

A base case is provided below to demonstrate how an unstable system can become stable by adjusting the controller gain and returning to an unstable state. The open loop system model for an electric machine is given by $G_p(s) = 1/[(s - 1)(s + 3)(s + 8)]$. The poles of the open loop system are $s = 1$, $s = -3$, and $s = -8$. A controller gain K , and negative unity feedback is applied to make the system faster, as shown in Fig. 4.2.

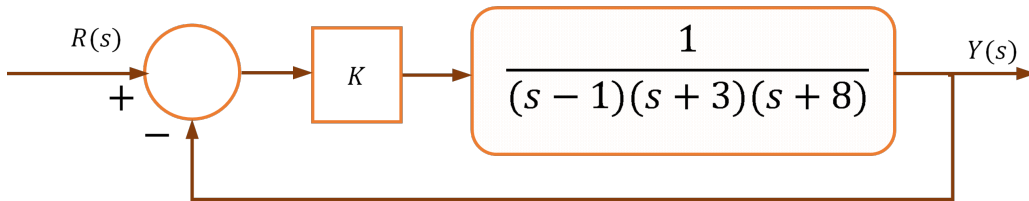


Figure 4.2: *A example of unity feedback closed-loop system with proportional gain.*

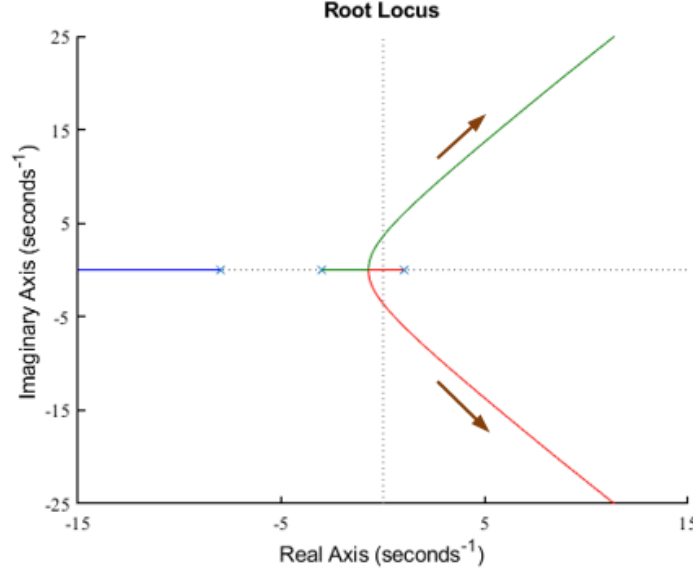


Figure 4.3: Root locus studies of unity feedback closed-loop system with proportional gain

The transfer function of the closed-loop system is $H(s) = kG_p/(1 + kG_p)$, i.e., $H(s) = k/[(s - 1)(s + 3)(s + 8) + k]$. The characteristics equation of $H(s)$ can be written as, $\Delta(s) = [(s - 1)(s + 3)(s + 8) + k] = [s^3 + 10s^2 + 13s + (k - 24)]$. The root locus studies of the system are shown in Fig. 4.3. By applying the Routh-Hurwitz tabulation method, one can write $(154 - K)/10 > 0$ and $(K - 24) > 0$. Hence, the range of K for the system to be stable is $24 < K < 154$. Therefore, the controller gain must be adjusted properly to ensure the inverter's operation in stable regions.

Besides the controller gain, the non-linearity of the PQ-controlled inverter can lead to a hidden mode of instability at low power levels. The dynamics of a PQ-controlled inverter cannot be considered linear for two reasons. First, the feedback P and Q quantities are non-linear expressions. The active and reactive power in the synchronously rotating dq reference frame locked at PCC, i.e., $v_d^{pcc} = 0$, can represent as $P = (3/2)(v_q^{pcc}i_q)$ and $Q = (3/2)(v_q^{pcc}i_d)$, where v_q^{pcc} is the magnitude of the line-to-line voltage at PCC, and i_q and i_d represent the line currents in dq -frame. As a side note, the $dq0$ transformation has different formats. Herein, the q-axis is assumed ahead of the d-axis as described in [174]; however, the following derivations are valid by swapping the axes for the convention that the d-axis is assumed ahead of the q-axis.

If these power expressions are linearized around a steady-state operating point, one can write

$$\begin{cases} \delta P = \frac{3}{2}(V_{qo}^{pcc}\delta i_q + I_{qo}\delta v_q^{pcc}) \\ \delta Q = \frac{3}{2}(V_{qo}^{pcc}\delta i_d + I_{do}\delta v_q^{pcc}) \end{cases} \quad (4.3)$$

where V_{qo}^{pcc} is the q-axis operating voltage, and I_{qo} and I_{do} are the q-axis and d-axis currents, respectively. The operating current, i.e., I_{qo} and I_{do} , will appear in the inverter closed-loop small-signal model. Therefore, the eigenvalues become functions of I_{qo} and I_{do} . Thus, the system stability is affected by incoming setpoints. Furthermore, the controller gain plays a critical role in determining the stability of a closed-loop system. Depending on the controller gain, a closed-loop system can become unstable. By adjusting the controller gain, the unstable system can become stable again. When the controller gain is changed further, the system becomes unstable again. Hence, there is a particular range of controller gain for which the system is stable.

The eigenvalues of the state-space model of grid-following inverters can explain the hidden mode of instability. A full-order model of an inverter can provide the details of the system eigenvalues with parameter variations [183, 184]. For explaining the hidden mode of instability, the sensitivity of eigenvalues with the variation of operating conditions (power flow) requires to be considered. Noteworthy, hidden modes of instability can also be identified by a stability criterion. A stability criterion is convenient for real-time implementation. The details of the stability criterion are provided in the following subsection.

4.2 Reduced-Order Model

The dynamic response of an inverter can be predicted by employing either a reduced-order model or a stability criterion as a dynamic reference model. In this section, two specific reduced-order models, namely a fifth-order model and a third-order model, derived from a simplified inverter model, are presented.

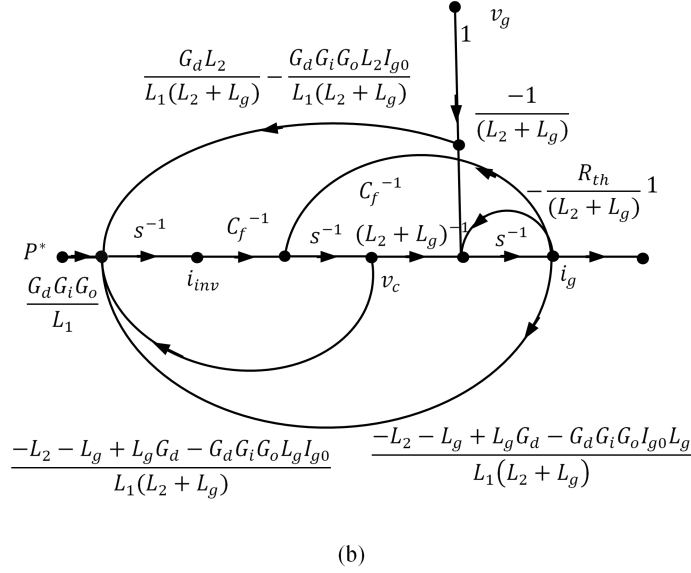
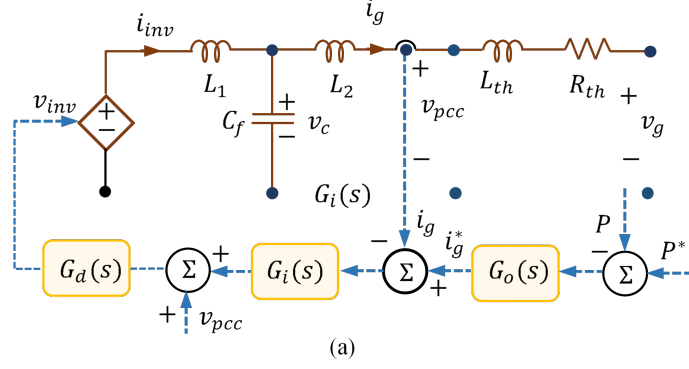


Figure 4.4: a) A simplified control schematic for fifth-order grid-following inverter model formulation, and (b) the system signal flow graph

4.2.1 Fifth-Order Model

In this sub-section, a fifth-order model is developed for grid-interactive inverter. For the purposes of this section, a more simplified schematic of the VSI is chosen, as shown in Fig. 4.4, upon which the analysis is performed. The reduced-order dynamic reference model of a grid-interactive inverter is derived from this simplified circuit. As one can see from the Fig. 4.4 that the inverter can represent as a controlled voltage source, where the inverter input voltage, v_i , can be regulated with two cascaded controller loops, namely outer power loop and inner current control loop having transfer function of $G_o(s)$ and $G_i(s)$ respectively. A feed-forward path is also included in the output of the inner current controller. The delay

associated with the control loop is represented by $G_d(s)$ also included in the simplified model. As shown in Fig. 4.4, L_1, L_2 , and C_f denote the inverter-side inductance, the grid-side inductance, and the capacitance of the filter connected in delta, respectively. Z_{th} represents the Thevenin equivalent impedance between the PCC and the grid, consisting of resistance, R_{th} , and inductance, L_{th} . The PCC voltage v_{pcc} , capacitor voltage v_c , inverter current i_{inv} , grid current i_g , the desired grid current i_g^* , measured active power at PCC P , and the desired active power at PCC P^* . The KVL equation on the left side of C_f can be expressed as

$$-v_{inv} + L_1 \frac{di_{inv}}{dt} + v_c = 0, \quad (4.4)$$

Similarly, the KVL equation on the right side of C_f can be expressed as

$$-v_c + L_2 \frac{di_g}{dt} + v_{pcc} = 0, \quad (4.5)$$

In the same way, the KVL equation at PCC can be expressed as,

$$v_{pcc} = v_g + L_g \frac{di_g}{dt} + R_{th} i_g, \quad (4.6)$$

Similarly, applying KCL at the capacitor node, the capacitor voltage can be expressed as,

$$\frac{dv_c}{dt} = \frac{1}{C_f} i_{inv} - \frac{1}{C_f} i_g, \quad (4.7)$$

Transferring (4.4)-(4.7) into the Laplace domain and replacing v_{pcc} from (4.5) in (4.6) yield

$$sI_g = \frac{V_c}{L_2 + L_g} - \frac{V_g}{L_2 + L_g} - \frac{R_g I_g}{L_2 + L_g}, \quad (4.8)$$

For a grid-interactive closed-loop VSI design, the power equations at PCC can be linearized around a steady-state operating point considering reactive power, $Q = 0$, as follows:

$$P = V_{pcc0} i_g + v_{pcc} I_{g0}, \quad (4.9)$$

Herein, V_{pcc0} and I_{g0} are the steady-state operating voltage and current at PCC, respectively. The desired grid current i_g^* can also be represented using the outer control loop variables shown in Fig. 4.4 as follows,

$$I_g^* = G_o(s)(P^* - P), \quad (4.10)$$

The inverter voltage can also be represented using the control variables shown in Fig. 4.4 as follows:

$$V_i = G_d(s)(V_{pcc} + G_i(s)(I_g^* - I_g)), \quad (4.11)$$

Replacing V_{pcc} from (4.6) in (4.9) yields,

$$V_{inv} = \frac{L_g V_c + L_2 V_g}{L_2 + L_g} + I_g \left(\frac{R_g L_2}{L_2 + L_g} - G_i(s) \right) + G_i(s) I_g^*, \quad (4.12)$$

Replacing V_i from (4.10) in (4.4) in s-domain gives

$$sI_{inv} = -\frac{L_2 V_c}{L_1(L_2 + L_g)} + I_g \left(\frac{R_g L_2}{L_1(L_2 + L_g)} - \frac{G_i}{L_1} \right) + \frac{L_2 V_g}{L_1(L_2 + L_t h)} + \frac{G_o I_g^*}{L_1}. \quad (4.13)$$

A signal flow graph of the grid-tied system in this work can be sketched as represented in Fig. 4.4 using equation(4.7), (4.8), and (4.13) in Laplace domain. Notice the signal flow graph is considered lossless for simplification. The output of the current-controlled VSI unit is I_g , while the inputs to the system are P^* and V_g . And also considering, $G_i(s) = K_{p1} + K_{i1}/s$, and $G_o(s) = K_{p2} + K_{i2}/s$, where K_p and K_i are the proportional and integral gain of the controller, respectively. Now, using Mason's rule on the signal flow graph presented in Fig. 4.4, the transfer function of the simplified system can be determined as $H(s) = I_g/P^* = N(s)/D(s)$. Here $N(s)$ and $D(s)$ are the numerators and denominators of the transfer function, respectively, as presented in equations (4.14) and (4.15).

$$\begin{aligned}
D(s) = & s^5 C_f L_1 (L_2 + L_g)^2 + s^4 C_f (L_2 + L_g) + s^3 [L_2 + L_g + L_1 (L_2 + L_g) + L_2 (L_2 + L_g) \\
& + L_g (L_2 + L_g) - G_d L_g (1 + L_2 + L_g) + G_d L_g I_{g0} k_{p1} k_{p2} (1 + L_2 + L_g)] + s^2 [G_d L_g I_{g0} \\
& k_{i2} k_{p1} (1 + L_2 + L_g) + G_d L_g I_{g0} k_{i1} k_{p2} (1 + L_2 + L_g) - R_g (L_2 + L_g) + G_d L_g R_g \\
& - R_g (L_2 + L_g) + G_d L_g R_g - G_d L_g I_{g0} R_g k_{p1} k_{p2}] + s [G_d L_g I_{g0} k_{i1} k_{i2} (1 + L_2 + L_g) \\
& - G_d L_g I_{g0} k_{i2} k_{p1} R_g - G_d L_g I_{g0} k_{i1} k_{p2} R_g] - G_d L_g I_{g0} R_g k_{i1} k_{i2},
\end{aligned} \tag{4.14}$$

$$N(s) = s^2 (L_2 + L_g) C_f G_d k_{p1} k_{p2} + s C_f G_d (L_2 + L_g) (k_{i2} k_{p1} + k_{i1} k_{p2}) + C_f G_d (L_2 + L_g) k_{i1} k_{i2}. \tag{4.15}$$

4.2.2 Third-Order Model

In this subsection, a third-order model is developed for grid-interactive inverter. For the third-order model formulation, the impact of the LCL filter capacitor, C_f , is ignored. And also, LCL filter inductance, L_1 and L_2 is simplified as $L_f = L_1 + L_2$, see Fig. 4.5. The KVL equation on the left side of C_f can be expressed as

$$v_i = (L_f + L_g) \frac{di_g}{dt} + i_g R_g + v_g = 0, \tag{4.16}$$

Similarly, the KVL equation on the right side of C_f can be expressed as

$$v_{pcc} = L_g \frac{di_g}{dt} + i_g R_g + v_g, \tag{4.17}$$

The linearized power, P , desired grid current, i_g^* , and inverter voltage, v_{inv} using the control variable can be represented as (4.9), (4.10), (4.11), respectively. A signal flow graph (SFG) of the grid-interactive system can be sketched as represented in Fig. 4.5 using equations (4.16) and (4.17) in the Laplace domain. Here, the SFG is assumed lossless for simpli-

[illegible]

The output of the current-controlled VSI unit is I_g , while the inputs to the system are P^* and v_g . Now, using Mason's rule on the signal flow graph presented in Fig. 4.5, the transfer function of the simplified system can be determined as $H(s) = I_g/P^* = (N(s))/D(s)$. Here $N(s)$ and $D(s)$ are the numerators and denominators of the transfer function, respectively, where $N(s) = G_p(s)G_i(s)$, and $D(s) = s(L_f + G_p(s)G_i(s)L_g i_{g0}) + G_i(s) + G_p(s)G_i(s)v_{pcc0} - R_g + G_p(s)G_i(s)R_g i_{g0}$. Considering $G_i(s) = K_{p1} + K_{i1}/s$, and $G_p(s) = K_{p2} + K_{i2}/s$, where K_p and K_i are the proportional and integral gain of the controllers, and replacing $G_i(s)$ and $G_p(s)$ in $N(s)$ and $D(s)$ yields equation (4.18) and (4.19).

$$\begin{aligned}
D(s) = & s^3(L_f + k_{p1}k_{p2}L_gI_{g0}) + s^2(k_{p1}k_{i2}L_gI_{g0} + k_{p2}k_{i1}L_gI_{g0} + k_{p2} + k_{p1}k_{p2}V_{pcc0} + k_{p1}k_{p2} \\
& I_{g0}R_g) + s(k_{i1}k_{i2}L_gI_{g0} + k_{i2} + k_{p1}k_{i2}V_{pcc0} + k_{p2}k_{i1}V_{pcc0} + k_{p1}k_{i2}I_{g0}R_g + k_{p2}k_{i1} \\
& I_{g0}R_g) + k_{i1}k_{i2}I_{g0}R_g + k_{i1}k_{i2}V_{pcc0},
\end{aligned} \tag{4.18}$$

$$N(s) = s^2k_{p1}k_{p2} + s(k_{i2}k_{p1} + k_{i1}k_{p2}) + k_{i1}k_{i2}. \tag{4.19}$$

From the transfer function of the third and fifth-order models, one can notice that the operating condition, i.e., I_{g0} and V_{pcc0} , can impact the system stability.

4.3 Stability Criterion from Reduced-Order Model

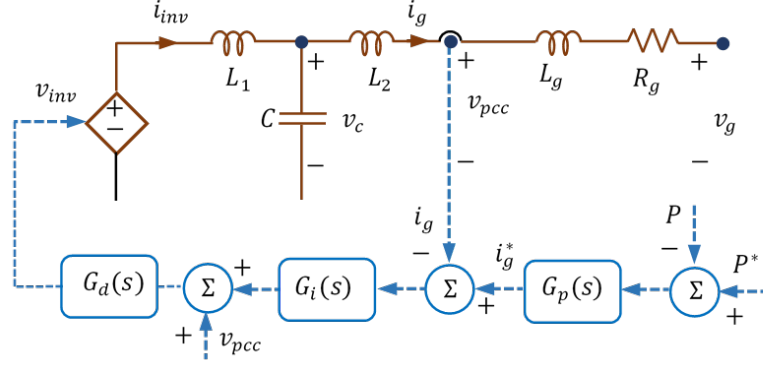
If the signal flow graph of a simplified control schematic for a grid-following inverter is considered, see Fig. 4.6, the transfer function of the inverter can be written, and then, using the Routh–Hurwitz rule, the following stability criterion can be derived as

$$|G_c| < R_g \left(\frac{L_1 + L_2}{L_2 + L_g} \right) \text{ with feedforwarding } v_{pcc} \tag{4.20}$$

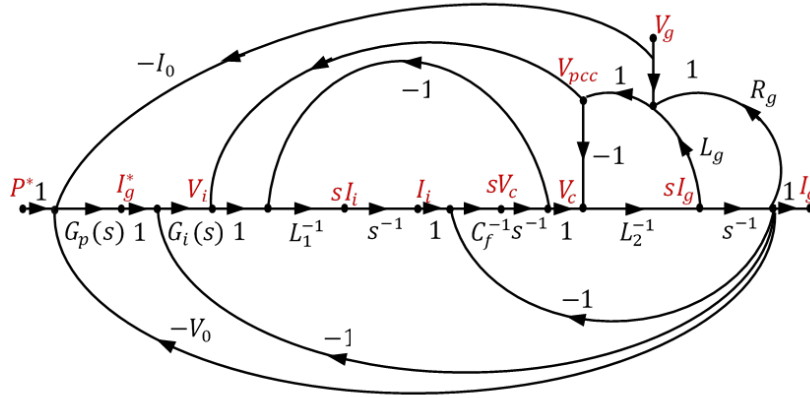
$$|G_c| < R_g \left(\frac{L_1}{L_2 + L_g} \right) \text{ without feedforwarding } v_{pcc} \tag{4.21}$$

where $G_c(j\omega)$ represents the controller transfer function, which depends on the outer power controller, $G_p(j\omega)$, inner current controller, $G_i(j\omega)$, operating conditions (V_0, I_0) and the output circuit parameters. If $G_p(s) = k_{p1} + k_{i1}/s$ and $G_i(s) = k_{p2} + k_{i2}/s$, are substituted in the system's transfer function, and then the Routh–Hurwitz rule is applied, see Appendix A, the stability boundary can be expressed, $|G_c| = M_c$, as follows:

$$M_c \approx k_{p2} + (k_{p1}k_{i2} + k_{p2}k_{i1})(L_gI_0) + k_{p1}k_{p2}(V_0). \tag{4.22}$$



(a)



(b)

Figure 4.6: a) A simplified control schematic for stability criterion formulation, and (b) the system signal flow graph

For the transfer function and Routh–Hurwitz derivations, check Appendix A. If only the inner current control loop is considered, then $M_c = k_{p2}$. From both stability criteria in (4.20) and (4.21), one can say that a higher L_g value leads to a smaller stability margin. One can also notice from (4.20) and (4.21) that an increase in L_1 can result in a larger stability margin, but L_1 is limited by other circuit restrictions. For high L_g values, i.e., weak grid conditions, with respect to L_2 , the gain margin is approximately given by $(L_1 + L_2)(R_g)/(L_g)$. Thus, an increase in L_2 can also result in a larger stability margin in weak grid conditions. In Fig. 4.6, if the feedforward voltages, v_q^{pcc} , and v_d^{pcc} are not implemented, the stability criterion does not have L_2 in the numerator, as also given in (4.21). For such a controller, an increase in L_1 results in a high stability margin, whereas an increase in L_2 causes a low stability

margin. Nevertheless, the convenient criterion in (4.20) and (4.21) provides a quick check for estimating the gain margin of the controller without providing information about pole locations. The feedforward voltages are typically included to enhance the inverter's dynamic response. The experimental verification of the stability criterion in (4.20) for the hidden mode of instability is presented in Section 4.5 when feedforward paths are implemented.

4.4 State-Space Model for of Inverters

The steady-state model of the system can provide more details on how much the system poles are sensitive to the system parameters. Let us consider the system shown in Fig. 4.1. The small-signal (linearized) model of the open-loop system can be written as:

$$\frac{d}{dt} \begin{bmatrix} \tilde{i}_{qd}^{inv} \\ \tilde{v}_{qd}^c \\ \tilde{i}_{qd}^g \end{bmatrix} = \begin{bmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{bmatrix} \begin{bmatrix} \tilde{i}_{qd}^{inv} \\ \tilde{v}_{qd}^c \\ \tilde{i}_{qd}^g \end{bmatrix} + \begin{bmatrix} 0 & B_{12} & b_1 \\ 0 & 0 & b_2 \\ B_{31} & 0 & b_3 \end{bmatrix} \begin{bmatrix} \tilde{v}_{qd}^{pcc} \\ \tilde{z} \\ \tilde{\omega} \end{bmatrix}, \quad (4.23)$$

where $\tilde{i}_{inv} = \begin{bmatrix} \tilde{i}_q & \tilde{i}_d \end{bmatrix}^T$ is the inverter output current, $\tilde{v}_c = \begin{bmatrix} \tilde{v}_q & \tilde{v}_d \end{bmatrix}^T$ is the capacitor voltage, $\tilde{i}_g = \begin{bmatrix} \tilde{i}_q^g & \tilde{i}_d^g \end{bmatrix}^T$ is the grid current, and $\tilde{v}_{pcc} = \begin{bmatrix} \tilde{v}_q^{pcc} & \tilde{v}_d^{pcc} \end{bmatrix}^T$ is the PCC voltage. In (4.23), $\tilde{\omega}$ represents the grid frequency perturbation, and $\tilde{u} = \begin{bmatrix} \tilde{m} & \tilde{\psi} \end{bmatrix}^T$, where $\tilde{m}$ and $\tilde{\psi}$ are the modulation index and angle between Phase-A of the inverter's output voltage and the q-axis, see Fig. 4.7. Furthermore, the inverter voltage can be expressed in terms of m and ψ as

$$\begin{cases} v_q^{inv} = mv_{dc} \cos \psi \\ v_d^{inv} = -mv_{dc} \sin \psi \end{cases} \quad (4.24)$$

After linearizing these equations, $\tilde{u} = \begin{bmatrix} \tilde{m} & \tilde{\psi} \end{bmatrix}^T$, can be expressed as $\tilde{u} = M^{-1} \tilde{i}_{inv}$. Notice $\tilde{v}_{inv}$ is the output of the controller; see Fig. 4.2. If the inner current and the outer power control loops in Fig. 4.8 are linearizing, the state space model of the control loops

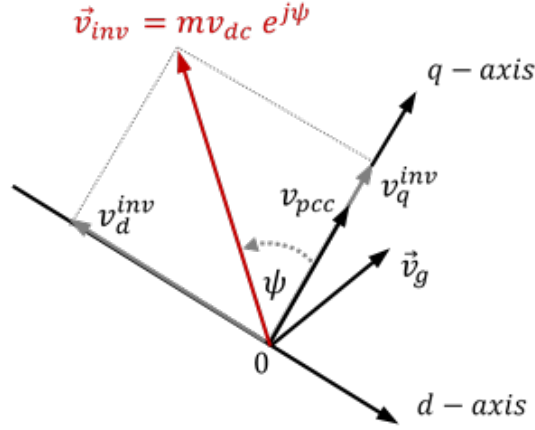


Figure 4.7: Space vector of the inverter voltage, v_{inv} , with respect to the grid and PCC voltages.

can be expressed as follows:

$$\frac{d}{dt} \begin{bmatrix} \tilde{y}_1 \\ \tilde{y}_2 \end{bmatrix} = \begin{bmatrix} A_{43} & 0 & 0 \\ A_{53} & A_{54} & 0 \end{bmatrix} \begin{bmatrix} \tilde{i}_{gL} \\ \tilde{y}_1 \\ \tilde{y}_2 \end{bmatrix} + \begin{bmatrix} B_{41} & B_{43} \\ B_{51} & B_{53} \end{bmatrix} \begin{bmatrix} \tilde{v}_{pcc} \\ R^* \end{bmatrix}, \quad (4.25)$$

where $\tilde{y}_1 = \begin{bmatrix} \tilde{y}_p & \tilde{y}_q \end{bmatrix}^T$, $\tilde{y}_2 = \begin{bmatrix} \tilde{y}_{iq} & \tilde{y}_{id} \end{bmatrix}^T$ and $\tilde{R}^* = \begin{bmatrix} \tilde{P}^* & \tilde{Q}^* \end{bmatrix}^T$. The two input variables are the desired active and reactive power. Combining (4.7) and (4.9), the full-order model of the system can be written as (A.1), given in Appendix A.

4.5 Eigenvalue Analysis

Three instability scenarios are studied in this section using root loci of the full-order model. Then these three scenarios are experimentally verified using the hardware setup in the next section. Fig. 4.5 shows the root locus of a dominant low-frequency eigenvalue when the active power in the model increases from $P = 0.003kW$ to $P = 5kW$ at zero reactive power, i.e., $Q = 0Var$. In this study, the filter resistances, R_1 and R_2 , have been increased continuously with power because the resistances of the *LCL* filter are a function of the current (power)

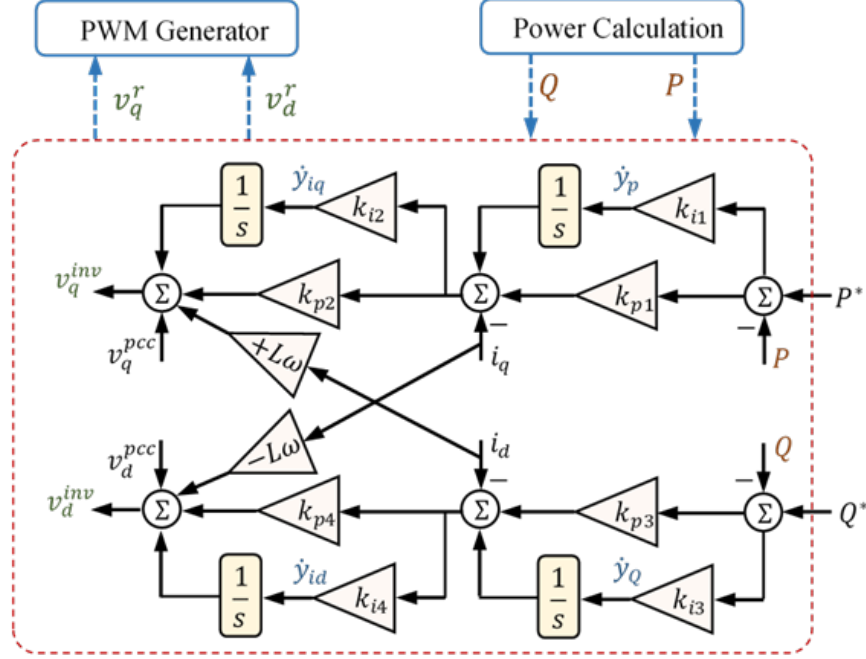


Figure 4.8: A typical control block diagram for grid-following inverters.

flow, temperature, and proximity effects in the filter inductors. The dominant pole is on the left-half plane initially, and the system is stable until $P = 200W$ (Point B). When $P > 200W$, the low-frequency dominant pole crosses the stability boundary and becomes unstable. When $P > 400W$ (Point D), the low-frequency pole returns to the left-half plane again.

In Fig. 4.9 (right), the dominant low-frequency eigenvalue is plotted as P is increased up to $5kW$ for different X_g/R_g values ranging from 4 to 8 by changing L_g from $2.5mH$ to $5mH$ with the same inverter setup. The value of R_g is chosen as 0.27Ω . The system has a low-power hidden instability region for $L_g = 5mH$, $X_g/R_g = 8.2 > 5$). For both $L_g = 2.5mH$, $X_g/R_g = 4.01$ and $L_g = 3mH$, $X_g/R_g = 4.81$, the root locus of the low-frequency dominant pole is entirely on the left-half plane. As one can observe in Fig. 4.9, the system can get unstable for a certain low power range or stay entirely in the stable left-half plane, depending on the grid condition. Fig. 4.10 represents the eigenvalue analysis with a similar simulation setup using the reduced-third and fifth-order models, respectively.

Fig. 4.11 shows the second scenario, in which multiple instability modes occur at different

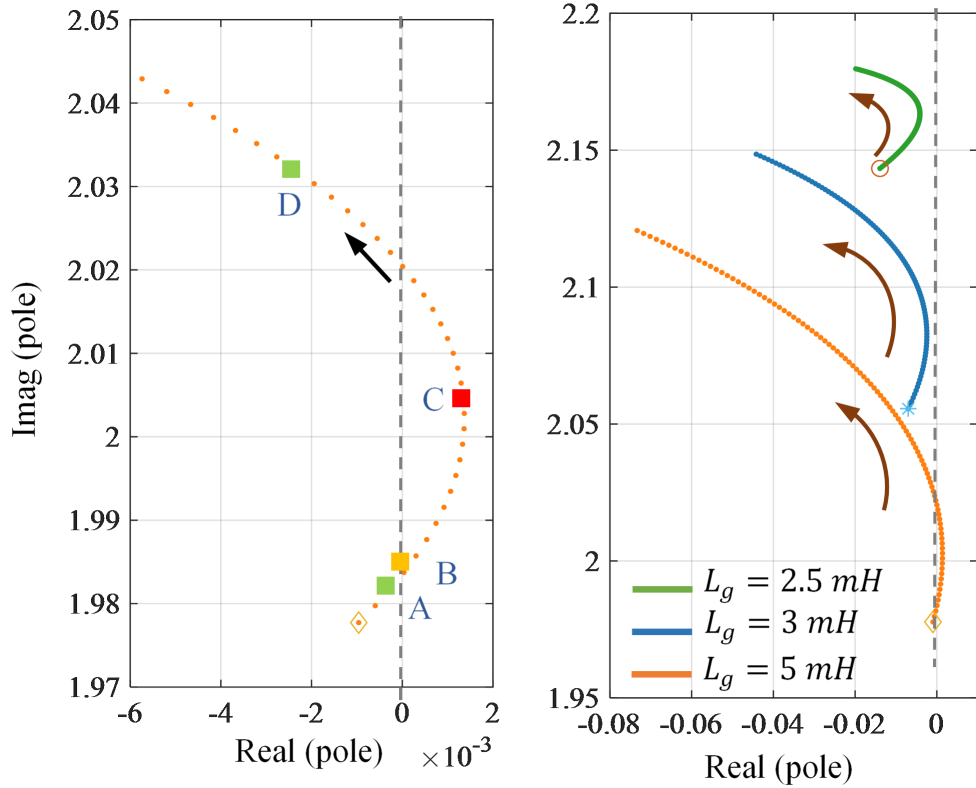


Figure 4.9: The trajectory of low-frequency positive eigenvalue using the full-order dynamic model as P is increased from $0.003kW$ to $5kW$ for different L_g (right), a zoomed-in plot of dominant low-frequency positive eigenvalues for $L_g = 5mH$ (left).

power levels. For the root-locus studies, the filter resistance, R_1 and R_2 , has been raised up slightly as power (current) increases from $P = 0.003kW$ to $P = 5kW$ for constant reactive power, i.e., $Q = 100Var$. Fig. 4.11 shows two different eigenvalues (poles) of the full-order model. These two poles are on the left-half plane initially, and the system is stable until $P = 200W$ (Point E). When $P > 250W$ (Point F), the low-frequency dominant pole crosses the stability boundary and becomes unstable. When $P > 350W$ (Point G), the low-frequency pole returns to the left-half plane again, and the system is stable until $P = 1kW$. However, when $P > 1kW$ (Point H), the other pole, at a higher frequency, crosses the stability boundary and makes the system unstable, see Fig. 4.11 (right). Hence, the nonlinear operation of the inverter can lead to multiple instability events at different power-level depending on the movement of eigenvalues in the closed-loop system.

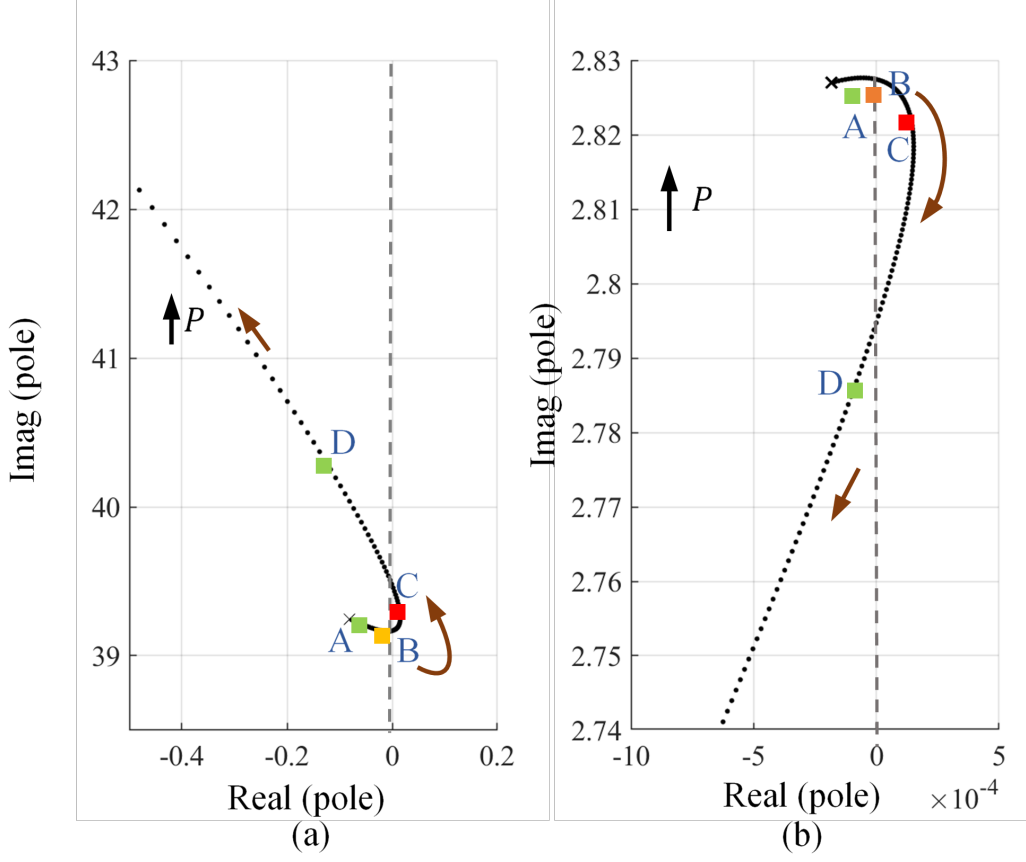


Figure 4.10: The trajectory of low-frequency positive eigenvalue using the (a) third-order dynamic model (b) fifth-order dynamic model, as P is increased from 0.003kW to 5kW

The root-locus studies of the system eigenvalues are shown in Fig. 4.12, as L_g is increased from 2.5mH to 15mH when $R_g = 0.27\Omega$ and the filter resistance, R_1 , is first assumed 0.4Ω , representing low damping. As shown in Fig. 4.12 (right), increasing L_g drives a pair of poles toward instability while other poles stay stable. Higher damping can be observed at a higher switching frequency due to the skin effect in the filter inductance, L_1 . In the second scenario, filter resistance, $R_1 = 1.2\Omega$, is assumed to verify this. Like the previous Case, L_g is changed from 2.5mH to 15mH . It can be seen from the root-locus studies that for $R_1 = 1.2\Omega$, the pair of poles move toward the instability boundary but stays on the left-half plane for the same change in L_g ; see Fig. 4.12 (right). Therefore, high PWM frequency introduces more damping to the filter inductance, L_1 , which can positively impact the stability of the inverter.

To demonstrate the effect of T_d on inverter stability, the root-locus of eigenvalues is plotted as P is gradually changing from 0.003 kW to 5 kW for three different time delays see

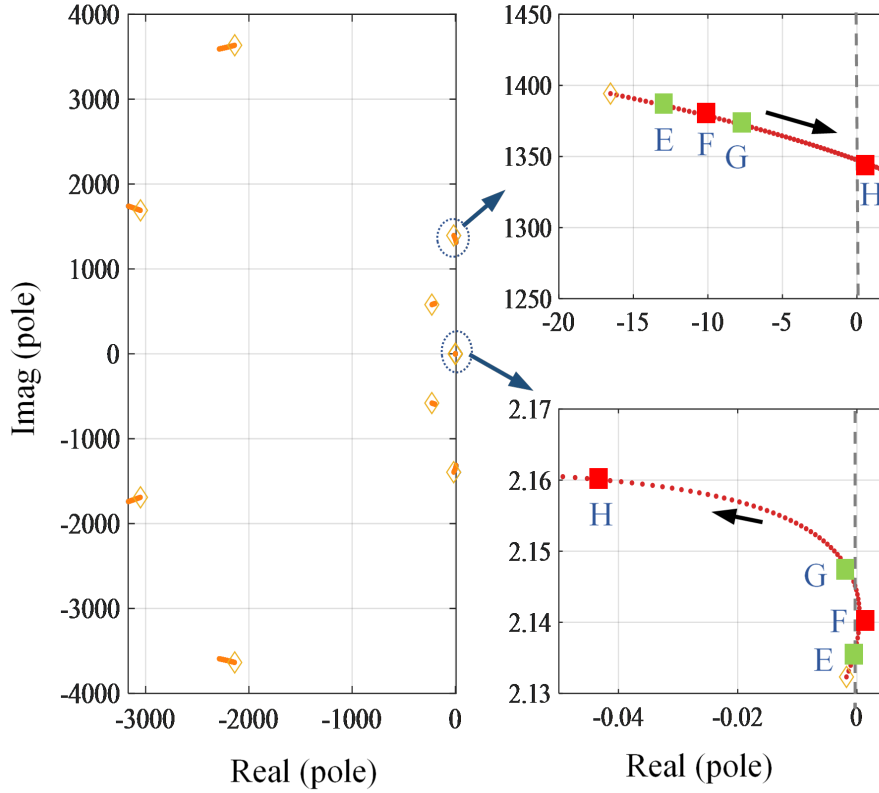


Figure 4.11: The trajectory eigenvalues using the full-order dynamic model as P is increased from $0.003kW$ to $5kW$ for $Q = 150Var$ (left), a zoomed-in plot of dominant positive eigenvalues for same inverter setup (right).

Fig. 4.13. It can be seen that increasing T_d from $300\mu s$ to $400\mu s$ shifts the high-frequency poles λ_5 and λ_6 of the system further to the left-half plane, i.e., positively impact the system stability, see Fig. 4.13 (left). However, increasing T_d can shift the low-frequency eigenvalues λ_1 and λ_2 to unstable regions at certain power levels and when $T_d = 350\mu s$ or $400\mu s$, see Fig. 4.13 (right). In this setup, the low-frequency eigenvalues are the dominant poles. Notice that the root locus is plotted in this study when the (setpoint) power increases; however, in [185], the root locus was plotted for a specific operating point as the delay increased. Nevertheless, a range of delay always exists for both low- and high-frequency poles to remain stable in weak grids. The study of the delay effects on stability is important as the trend is toward employing collaborative inverters in modern architectures.

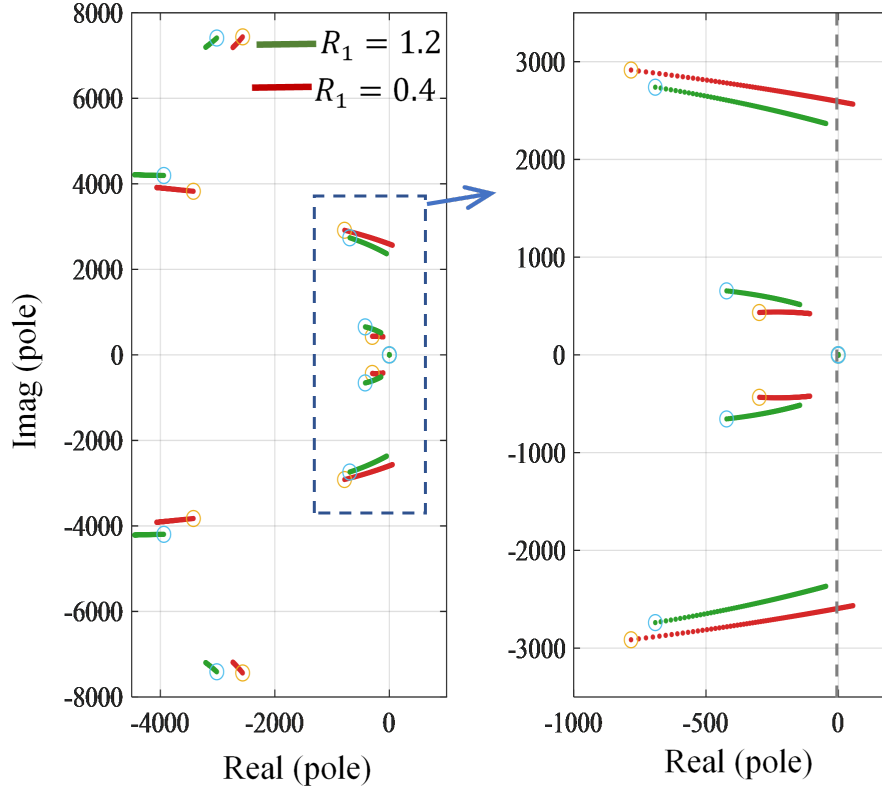


Figure 4.12: The trajectory of eigenvalues using the full-order dynamic model as L_g is increased from 5mH to 15mH (left), a zoomed-in plot of dominant low and mid-frequency eigenvalues.

4.6 Experimental Results

A nonhidden mode of instability, Case I, and a hidden mode of instability, Case II, are verified experimentally using a hardware setup, see Fig. 4.14. In this setup, a three-phase 3kVA SiC MOSFET-based inverter was applied when the switching signals for the inverters were generated using the dSPACE MicroLabBox DS-1202 controller board. In the setup, the inverter followed and fed a 12 kW NHR 9410 power grid emulator through a three-phase LCL filter. Also, a Magna-Power SL400-15/208 programmable dc supply is employed as the dc source for the inverter. In this study, the circuit and control parameters are intentionally selected to place the dominant eigenvalues closer to the stability border to validate the instability modes, see Table 4.1, and 4.2.

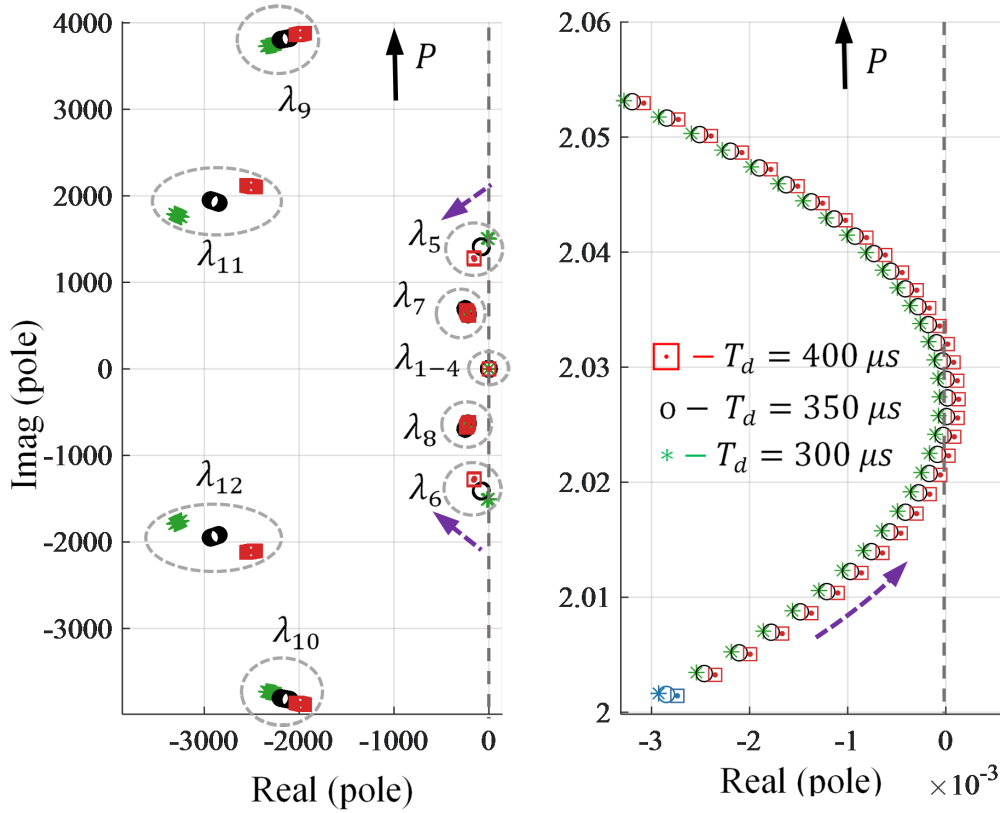


Figure 4.13: The trajectory of a dominant positive eigenvalue using the full-order dynamic model of the inverter setups for different T_d (left), A zoomed-in plot of low-frequency eigenvalues (right).

4.6.1 Case I: Common Modes of Instability

Two known modes of instability scenarios are demonstrated at rated power level when the effect of damping is considered, as discussed and shown earlier in Fig. 4.12. Higher PWM frequency results in more effective resistance in the side inductor, i.e., L_1 , of the LCL filter. In the first test scenario, the PWM switching frequency is $20kHz$. The system initially operates near the rated power under a stiff grid condition, injecting 1.2 kW into the grid, see Fig. 4.15. At $t = t_1$, $L_g = 10mH$ per phase is inserted between the grid and the PCC point in the circuit using a three-phase circuit breaker. As expected, the system becomes unstable after inserting the $10mH$ inductor per phase. At $t = t_2$, the three-phase circuit breaker bypasses the inductors, and the system becomes stable again. Between t_1 and t_2 , the

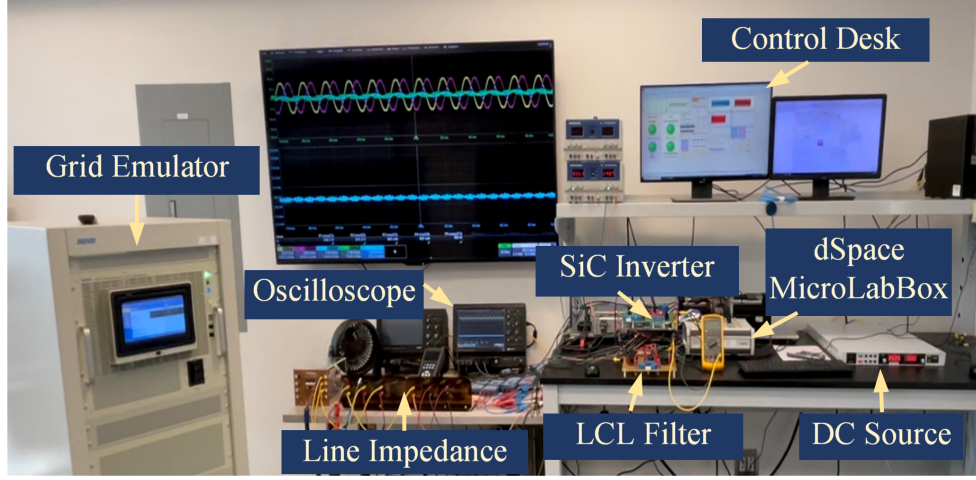


Figure 4.14: *Hardware setup for 3 kVA three-phase grid-interactive inverter*

Table 4.1: *Simulation and Experimental Parameters for Case I (known mode of instability)*

Parameters	Value
Nominal line-line voltage, V_n	185 V
DC bus voltage, V_{dc}	350 V
Fundamental frequency, ω_n	$2\pi(60)$ rad/s
PWM switching frequency, f_{PWM}	20 kHz
Inverter side inductance, L_1	1 mH
PCC side inductance, L_2	0.5 mH
Filter capacitance, C_f (in Δ)	5 μ F
Filter damping resistance, R_{cf} (in Δ)	3.3 Ω
Grid inductance, L_{grid}	15 mH
Grid resistance, R_{grid}	0.27 Ω
Outer control loop proportional gain, k_{p1}, k_{p3}	0.021
Inner control loop proportional gain, k_{p2}, k_{p4}	0.8
Outer control loop integral gain, k_{i1}, k_{i3}	0.06
Inner control loop integral gain, k_{i2}, k_{i4}	1.2

voltage and current waveforms are distorted, and the level of distortion can be quantified by the 5th and 7th harmonics in the current and voltage waveforms, see Fig.4.15.

In the second test scenario, the PWM switching frequency is reduced to 8 kHz, and the same test scenario has been performed. In this test scenario, artificially inserting L_g makes the voltage and current waveforms distorted so that the fundamental component cannot be distinguished, a clear demonstration of harmonic instability, see Fig. 4.16. One can

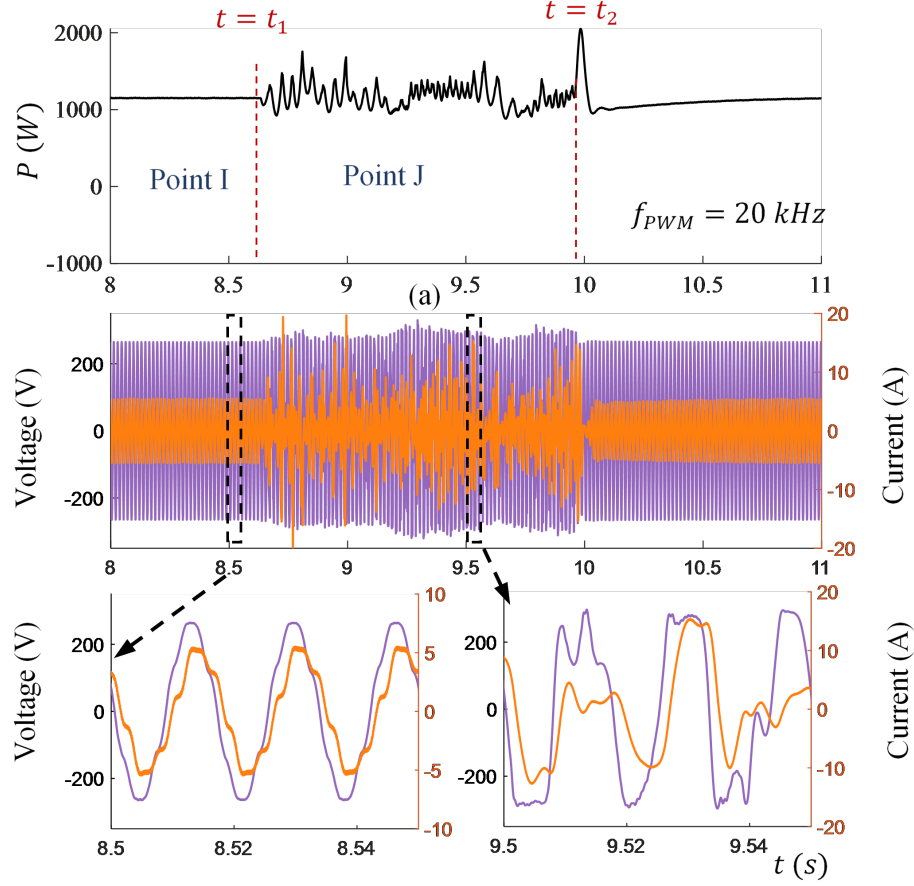


Figure 4.15: Experimentally obtained active power generation, PCC voltage, grid-side current, the zoomed-in voltage, and current waveforms, for $L_g = 10$ mH and the power setpoint of 1.2 kW, when the PWM frequency is 20 kHz.

notice that the distortion level increases when the PWM switching frequency is reduced. The system operating with a high PWM frequency introduces more effective resistance with filter inductance, L_1 , increasing the level of damping effect.

The impact of PWM frequency on the effective resistance of the filter and inverter circuit damping is presented in Fig. 4.17 (c). Here ΔP represents the maximum change in active power from the desired level for changes in L_g from 5 mH to 15 mH. The value of ΔP is recorded and plotted for eight different switching frequencies at two different power levels, $P_1 = 1000$ W and $P_2 = 1200$ W. One can notice from Fig. 4.17 (c) that an increase in PWM switching frequency reduces ΔP , i.e., adds more damping effect in the inverter circuit.

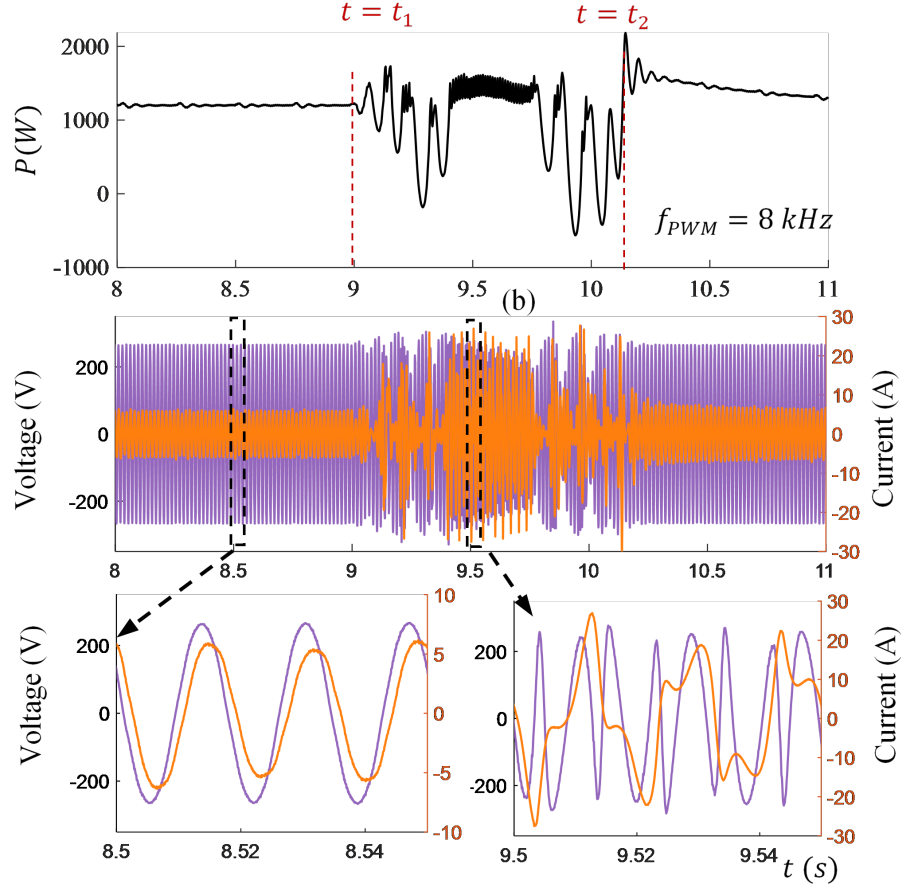


Figure 4.16: Experimentally obtained active power generation, PCC voltage, grid-side current, the zoomed-in voltage, and current waveforms, for $L_g = 10\text{mH}$ and the power setpoint of 1.2 kW , when the PWM frequency is 8 kHz .

4.6.2 Case II: Hidden Mode of Instability

The inverter operation at a low power level is examined to demonstrate the hidden mode of instability. In the first test scenario, the system initially runs when $L_g (= 2.5\text{mH})$ and the setpoint is $P^* = 100\text{W}$ and $Q^* = 0\text{Var}$. Different active power setpoints, P , ranging from 150 W to 400 W when keeping $Q^* = 0\text{VAR}$ are applied, and the dynamic responses are recorded from the dSPACE control desk. For the applied setpoints ($P^* = 150\text{W}, 190\text{W}, 250\text{W}, \text{and } 400\text{W}$), the dynamic responses are stable; see Fig. 4.18(a).

In the second low-frequency instability test scenario, the inverter runs in a weak grid when $L_g (= 5\text{mH})$, but for the same setpoints as the previous test scenario, see Fig. 4.18(b).

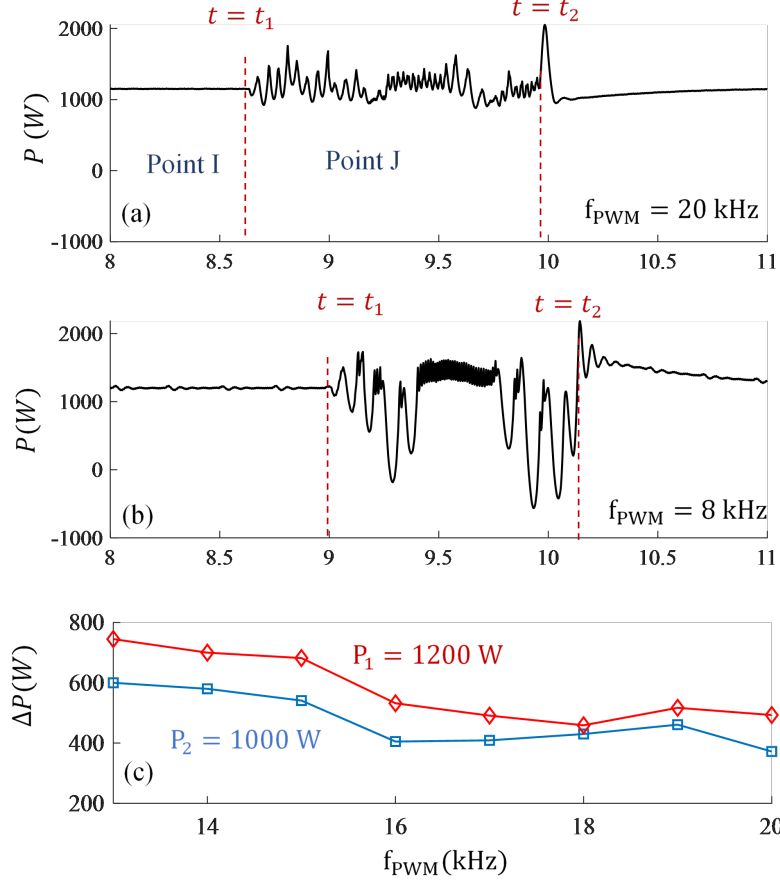
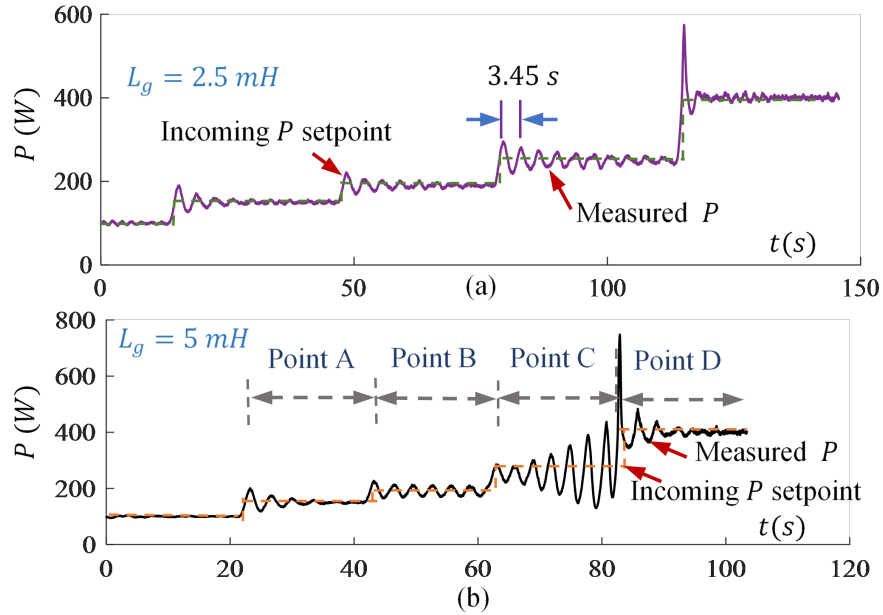


Figure 4.17: Experimentally obtained active power generation, for $L_g = 15\text{mH}$ and the power setpoint of 1.2 kW (a) the PWM frequency is 20 kHz , and (b) the PWM frequency is 8 kHz . (c) a family of curves for ΔP vs. PWM frequency at two different power levels.

The root locus study for this test scenario can be found in Fig. 4.9. At $t = 21\text{s}$, when $P^* = 150\text{W}$, an underdamped-stable response can be seen, as marked by Point A. At $t = 42\text{s}$, when $P^* = 190\text{W}$, the dynamic response of the inverter is marginally stable, and undamped oscillation can be observed (Point B). At $t = 61\text{s}$, the setpoint is $P^* = 250\text{W}$, when the power fluctuates, and the system gradually becomes unstable (Point C). At $t = 83\text{s}$, when $P^* = 400\text{W}$, and the system is again stable (Point D). Thus, an inverter can move from stable to unstable and unstable to stable depending on the setpoints. These two experimental test outcomes are also in agreement with the stability analysis demonstrated in Fig. 4.9. Therefore, for weak grid conditions, i.e., high L_g , power setpoints can cause low-frequency instability if the damping is insufficient in the system.

Table 4.2: *Simulation and Experimental Parameters for Case II (hidden mode of instability)*

Parameters	Value
Nominal line-line voltage, V_n	208 V
DC bus voltage, V_{dc}	335 V (341 V) V
Fundamental frequency, ω_n	$2\pi(60)$ rad/s
PWM switching frequency, f_{PWM}	20 kHz
Inverter side inductance, L_1	1 mH
PCC side inductance, L_2	0.5 mH
Filter capacitance, C_f (in Δ)	27 μ F (5 μ F)
Filter damping resistance, R_{cf} (in Δ)	3.3 Ω (1.65 Ω)
Grid inductance, L_{grid}	5 mH
Grid resistance, R_{grid}	0.09 Ω
Outer control loop proportional gain, k_{p1}, k_{p3}	0.001
Inner control loop proportional gain, k_{p2}, k_{p4}	0.1
Outer control loop integral gain, k_{i1}, k_{i3}	0.06
Inner control loop integral gain, k_{i2}, k_{i4}	1.2

**Figure 4.18:** *Experimentally obtained inverter's dynamic responses when the output power is changing step-by-step from 150 W to 400 W for (a) $L_g = 2.5$ mH and (b) $L_g = 5$ mH.*

In the third test scenario, the inverter runs when $L_g = 5$ mH, and the setpoint of $P^* = 50$ W, and $Q^* = 150$ Var. Different active power setpoints, P^* , ranging from 50 W to 1200 W by 50 W steps are applied to the controller when $Q^* = 100$ Var. The dynamic responses are

shown in Fig. 4.16(a). The voltage waveforms obtained from the oscilloscope for different dynamic responses are shown in Fig. 4.16 (b)-(d). When $50 < P^* < 200W$ (Point E), the system is stable, i.e., measured active power following the commanded setpoints. It can be observed that both line-to-line and phase voltage waveforms are pure sinusoidal, and the THD is insignificant. When $200 < P^* < 350W$, the system is unstable, and an oscillatory behavior can be observed with a frequency of 1.54 rad/s when $350 < P^* < 950W$ (Point F), the system is again stable, i.e., P following the P^* . When $950 < P^* < 1200W$ (Point H), measured power increasingly elevated to higher values, with a frequency of 6.28 rad/s. The voltage waveforms are also distorted, clearly demonstrating an instability mode. The phenomena in this test scenario have been conceptually shown earlier in Fig. 4.8, where it has been shown that two pairs of eigenvalues in the state-space model can lead to instability at different power levels and different frequencies. The frequency of two pairs of eigenvalues of the state-space models that cause instability is 2.14 rad/s and 1350 rad/s, respectively, see Fig. 4.8. The frequency of eigenvalues should not be confused with the frequency of power oscillation in Fig. 4.16. Herein, the frequency of eigenvalues represents the frequency of state variables, i.e., measured voltages or currents, whether measured power is a secondary variable that results from measured voltage and currents. Regardless of the source of instability, which could be low- or high-frequency eigenvalues, the frequency of power oscillations is below a few hertz.

4.7 The Stability Criterion Verification

According to the stability criterion in (4.20), the magnitude of the PQ-controller, i.e., $|G_c| = M_c$ as defined in Appendix A, must not exceed the upper stability margin, i.e., $(R_g(L_1 + L_2))/((L_2 + L_g))$. The stability criterion can be verified in two ways. The first approach is to alter M_c by changing the controller parameters when circuit parameters are constant. The second approach is to vary the margin by intentionally changing the filter circuit parameters, L_1 and L_2 , and comparing the margin with M_c . To verify the criterion in (4.20) and demonstrate the impact of the circuit, the second approach is performed for

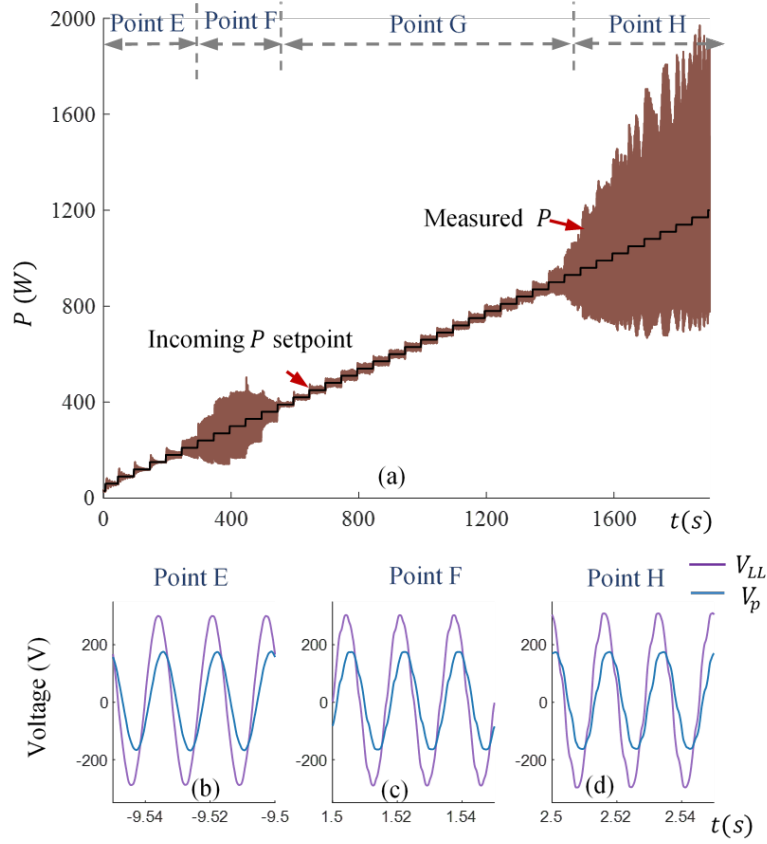


Figure 4.19: Experimentally obtained (a) inverter's dynamic responses when the output power is changing step-by-step from 100 W to 1200 W and keeping $Q=100$ Var. (b)-(d) Voltage waveforms obtained from the oscilloscope for different dynamic responses.

the hidden mode of instability, as shown in Fig. 4.20.

The low-frequency hidden mode of instability is shown in Fig. 4.20. In this case, the active power setpoint is increased in two steps. In the second step, the power oscillates, and the system becomes unstable; see Fig. 4.20. At $t = t_3$, the stability margin is increased by inserting an inductor into the LCL filter. This is achieved by opening a bypass three-phase circuit breaker in the laboratory. In this case, four different combinations of L_1 and L_2 are considered; see Figs. 4.20 (a)-(d). Notice that when the margin is lower than M_c , the system is unstable; see Fig. 4.20 (a). However, the system becomes stable for higher margins, as shown in Fig. 4.20 (b)-(d). It can be seen from the experiments that a higher value of margin adds more damping to the system and makes the system stable, which verifies the stability

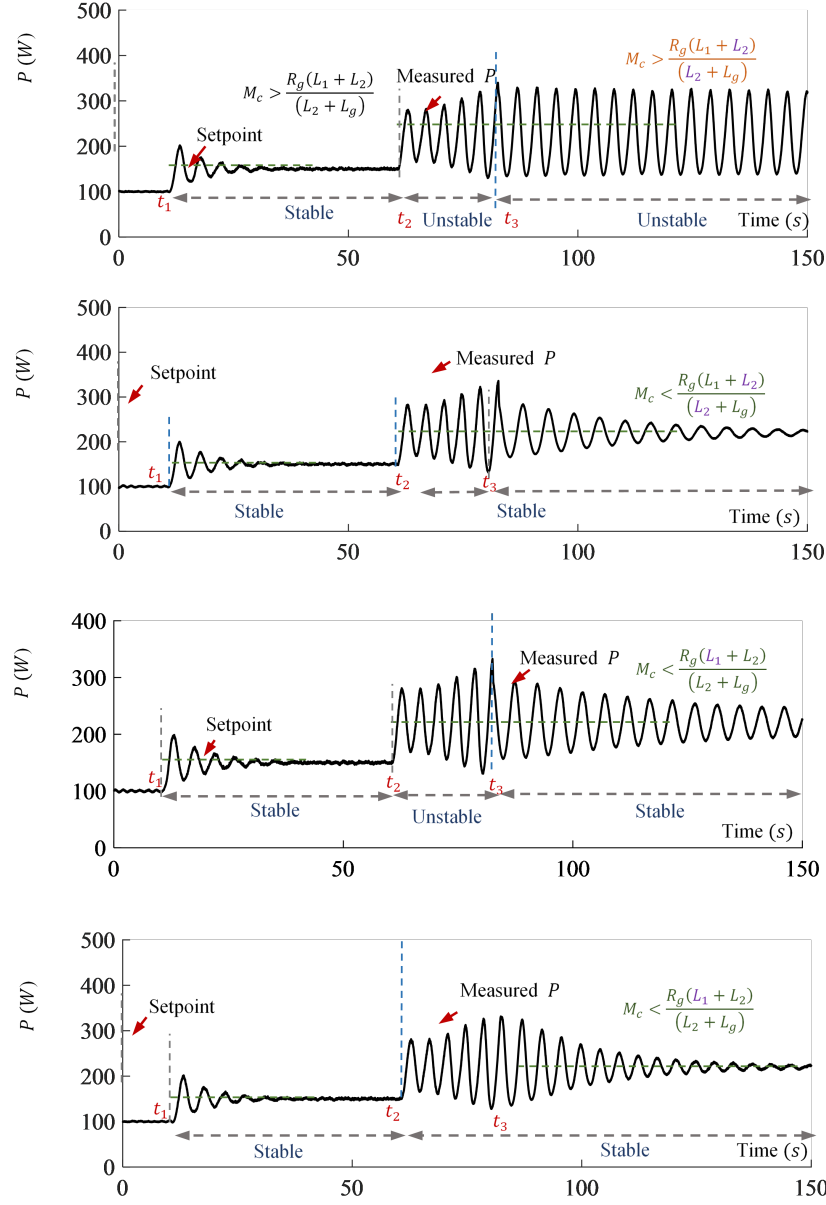


Figure 4.20: Active power at PCC when $P = 150\text{W}$ at $t = t_1$ and a step-change to $P = 250\text{W}$ at $t = t_2$ with $L_1 = 1$, $L_2 = 0.5\text{mH}$, and $L_g = 5\text{mH}$ for $R_g = 0.35 \text{ } \Omega$ followed by inserting additional L_1 or L_2 at $t = t_3$. (a) $L_1 = 1\text{mH}$, $L_2 = 1\text{mH}$ (b) $L_1 = 1.5\text{mH}$, $L_2 = 0.5\text{mH}$, (c) $L_1 = 1$, $L_2 = 1.5\text{mH}$ (d) $L_1 = 2\text{mH}$, $L_2 = 0.5\text{mH}$.

criterion in (4.20). Therefore, the criterion in (4.20) can be applied to select the controller's gain, preventing instability at the values below the rated power.

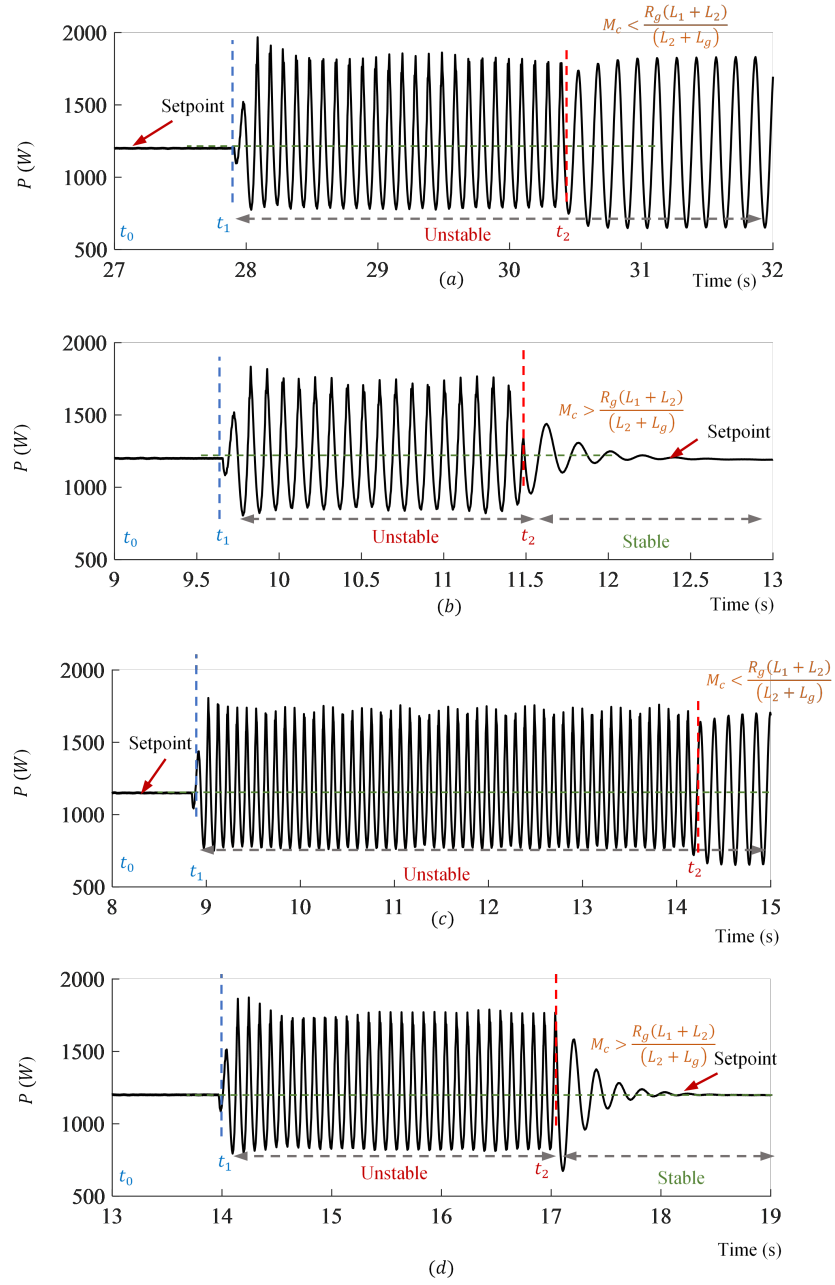


Figure 4.21: Active power at PCC when $P = 1200$ W at $t = t_1$ and L_g change to 15 mH from $L_g = 5$ mH at $t = t_2$ with $L_1 = 1$, and $L_2 = 0.5$ mH for $R_g = 0.35 \Omega$ followed by inserting additional L_1 or L_2 at $t = t_3$. (a) $L_1 = 1$ mH, $L_2 = 1.5$ mH (b) $L_1 = 3.5$ mH, $L_2 = 0.5$ mH, (c) $L_1 = 1$, $L_2 = 3$ mH (d) $L_1 = 2$ mH, $L_2 = 0.5$ mH.

The known mode of instability is shown in Fig. 4.21. In this case, the circuit parameters are changed in two steps. In the first step, the grid inductances change intentionally at $t = t_1$

by opening a bypass three-phase circuit breaker in the laboratory. For these changes, the system becomes unstable because of the harmonic instability, as shown in Fig. 4.21. For the second step, at $t = t_2$, the stability margin is increased by inserting an inductor into the LCL filter. This is achieved by opening a bypass three-phase circuit breaker in the laboratory.

Notice that when the margin is lower than M_c , the system is unstable; see Fig. 4.21 (a) and (c). However, the system becomes stable for higher margins, as shown in Fig. 4.21 (b) and (d). It can be seen from the experiments that a higher value of margin adds more damping to the system and makes the system stable, which verifies the stability criterion in (4.20). Therefore, the criterion in (4.20) can be applied to select the controller's gain, preventing instability because of the change in the inverter circuit.

4.8 Conclusion

This chapter has developed and experimentally verified a stability criterion for the self-protection method of grid-interactive inverters. The following conclusions can be highlighted-

- A hidden instability mode has been introduced and analyzed for PQ-controlled inverters. This unforeseen instability issue has been identified at a power range below the rated level, mainly when the inverter operates in weak grids.
- Several scenarios have been investigated to understand the impact of controller nonlinearity and filter parameters variation on the stability of the inverter
- It has been shown that low-frequency eigenvalues of the closed-loop model can dominate the overall system dynamics. It has also been demonstrated that the inverter system moves to a stable or unstable region for different power setpoints.
- Additionally, it has been verified that multiple pairs of eigenvalues in the state-space model can lead to instability at different power levels and different frequencies.
- Furthermore, it has been verified that a change in the setpoint can change the system parameters due to PQ control loops and move the eigenvalues to the instability region for a given set of control gains.
- A stability criterion has been developed for inspecting the power setpoints and pre-

dicting the instability and verified through hardware experiments carried out on three-phase grid-interactive inverters.

Chapter 5

An Analytical Criterion on Neural Network Platform for Self-Protective Inverters

This chapter focuses on analyzing and validating an analytical Criterion on a neural network platform for self-protective inverters. The contents of this chapter are organized into five sections. Section 5.1 provides the details of the cyberattack scenarios and system description. Section 5.2 develops a hybrid data-driven and analytical model-based criterion for Safe Inverter Operation. Section 5.3 provides the details of the self-protection approach. Section 5.4 demonstrates the experimental validation of the developed self-protection approach. Concluding remarks are given in Section 5.5.

5.1 Cyberattacks Scenarios and System Description

This section discusses malicious data-attack scenarios for the grid-interactive smart inverters in a cyber-physical network and the system description of this work. Physical devices such as grid-connected inverters, smart sensors, electrical buses, circuit breakers, phasor measurement units, etc., form the physical device category, so-called the physical network. Devices

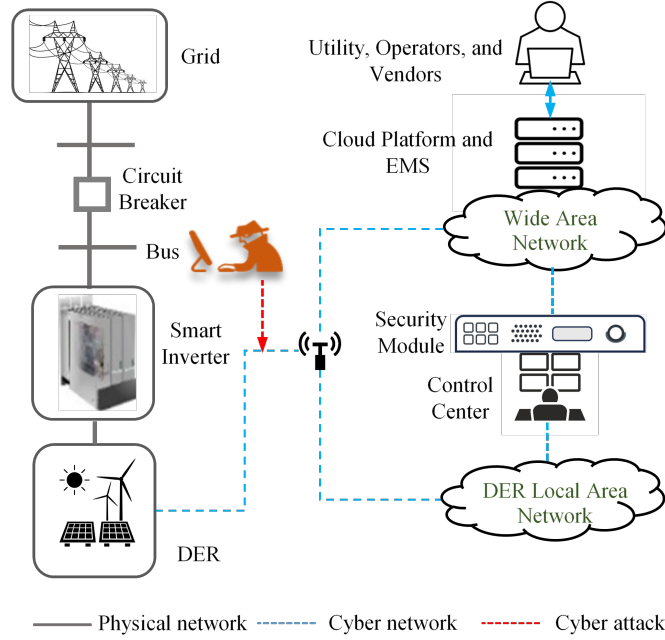


Figure 5.1: *Smart inverters connected to the power grid and cyberattack scenarios in a cyber-physical system.*

such as utility supervisory controllers, third-party aggregator servers, data centers, energy management systems (EMS), etc., can remotely connect to the other smart devices to form a communication network, so-called a cyber network. This communication network provides smartness to the inverters by allowing interactive and real-time control to deliver services beyond active and reactive power injection to the grid, i.e., ancillary services. This interaction also allows data sharing between inverters that are connected to different local networks through the control and data centers, as shown in Fig. 5.1. Also, inverters connected to the same local network can directly share information through wired or wireless channels. Notice smart inverters are accessible from many channels through the communication link. Received data using communication links can be processed in the inverter's local controllers. As authorized sources use secure communication channels, existing basic security features can fail to examine the incoming data sent from an authorized user, like a utility operator or data from nearby trusted local devices. Therefore, an additional device-level security layer

to the existing security methods is essential to maintain normal and safe system operation.

In this chapter, manipulated external data sent from authorized sources like utility operators requesting a change in the inverter's power setpoints are considered cyberattacks, see Fig. 5.2. The schematic of the PQ-controlled grid-following inverter is demonstrated in Fig. 5.2, where the LCL filter is used at the output terminals of the inverter. The grid is represented by an equivalent grid inductance, L_g and grid resistance, R_g , with grid voltage, v_g . In the PQ control structure, both P and Q controllers consist of two cascaded control loops. One can notice that the outer power loops compare the desired power setpoints, $R^* = [P^* \ Q^*]$ to the measured power $R = [P \ Q]$, where $P = (3/2)(V_{qo}^{pcc}i_q + I_{qo}v_q^{pcc})$ and $Q = (3/2)(V_{qo}^{pcc}i_d + I_{do}v_q^{pcc})$ [111]. Therefore, the line current in the control loop can shift system eigenvalues to the right-half plane and lead to unsafe hidden mode instability in the inverter below the rated power level [111]. The safe operation of the grid-interactive inverter can be compromised intentionally or accidentally [97]. A man-in-the-middle can manipulate the commanded power setpoints delivered from authorized sources such as utility operators, as shown in Fig. 5.2. Furthermore, a trusted source can unknowingly command unsafe power setpoints that can jeopardize the safe operation of inverters. Here, both power equations are linearized at a steady-state operating point. V_{qo}^{pcc} represents the q-axis operating voltage, and I_{qo} and I_{do} represent the q -axis and d-axis currents, respectively. Notice, $v_d^{pcc} = 0$ for the synchronously rotating dq frame of reference locked at PCC.

5.2 Hybrid Data-Driven and Analytical Model-Based Criterion for Safe Inverter Operation

The inverter operation can be unsafe, e.g., unstable, within its nominal operating region, even when the inverter control parameters are appropriately selected, and a commanded PQ setpoint appears safe to be engaged to the controller. For example, hidden-mode instability can occur at a low power level, as reported in [111]. A full-order dynamic model or any reduced-order model can be used to inspect the incoming power setpoints. However, inspect-

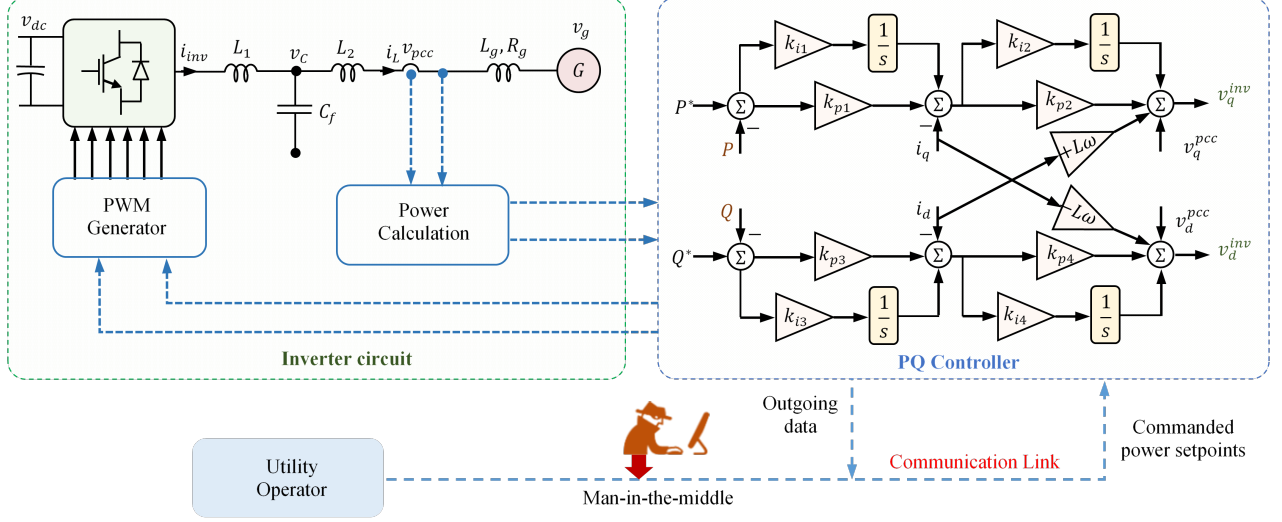


Figure 5.2: The PQ controller for grid-following inverters and unsafe operation from an authorized entity or modified by unauthorized source (man-in-the-middle attacks).

ing incoming power setpoints using a full-order model can be computationally burdensome. A suitable criterion is computationally efficient to inspect the power setpoints and can be a promising solution. This work formulates a hybrid model that combines a neural network and an analytical criterion to detect unsafe operations of inverters for commanded power setpoints.

5.2.1 Analytical Criterion from a Reduced-Order Model

An analytical criterion can be derived from the simplified circuit of a grid-following inverter shown in Fig. 5.2. Then, the transfer function of the inverter can be formulated, and using the Routh–Hurwitz rule, the following stability criterion can be derived as,

$$|G_c| < R_g \frac{L_1 + L_2}{L_2 + L_g} \quad (5.1)$$

Where $|G_c|$ represents the controller transfer function, and the lower stability boundary in (5.1) can be expressed, $|G_c| = M_c$, as follows

$$M_c \approx k_{p2} + (k_{p1}k_{i2} + k_{p2}k_{i1})(L_g I_0) + k_{p1}k_{p2}(V_0). \quad (5.2)$$

Where k_{p1}, k_{i1} , k_{p2} , and k_{i2} represent the PI controller gains of the cascaded active power control loops, as shown in Fig. 5.2. Notice similar expression can also be written for the reactive power control loop. Herein, the last two terms of the lower stability boundary (5.2) depend on the operating condition, i.e., V_o and I_o . However, the impact of dc-bus voltage and grid voltage is not considered in (5.2). Hence, steady-state risk, R_{isk} , is used in (5.2) as a multiplication factor for the last two terms that include operating points. Notice the steady-state risk factor is a function of dc-bus voltage, V_{dc} , the dc-bus utilization factor, k_m , grid-side Thevenin voltage, V_{th} , and impedance seen from the inverter side, Z_{th} . The detailed risk factor calculation is provided in [98]. The expression in (5.2) can be adjusted as follows,

$$M_c \approx k_{p2} + R_{isk}[(k_{p1}k_{i2} + k_{p2}k_{i1})(L_g I_0) + k_{p1}k_{p2}(V_0)]. \quad (5.3)$$

The upper stability boundary, i.e., the ratio $R_g(L_1 + L_2)/(L_2 + L_g)$, determines the stability margin of the grid-following inverter for given control parameters. Also, for high L_g , i.e., weak grid conditions and relatively low L_2 , the gain margin is approximately given by $(L_1 + L_2)(L_g)/(R_g)$. The inverter's safe operation region can be verified by using this useful criterion,

$$M_c < M_{LR}. \quad (5.4)$$

Here $M_{LR} = R_g(L_1 + L_2)/(L_2 + L_g)$ is the upper safety margin. The value of M_c depends on P, Q, V_{dc} , V_{th} , Z_{th} , L_g , $L_2, R_g, k_{p1}, k_{p2}, k_{i1}, k_{i2}$ and the operating condition of the inverters. The analytical criterion in (5.4) cannot distinguish between unsafe operations resulting from manipulations of PQ setpoints (cyberattacks) and weak grid conditions. This work develops a hybrid model that includes analytical criterion (5.4) and a data-driven neural network that can predict the stable or unstable operation of inverters. The details of the neural network are provided in the following subsection.

5.2.2 Neural Network for Inverters' Stable and Unstable Operation Estimation

This work uses a multilayer perception neural network model to predict whether the inverter operation is stable or unstable. An artificial neural network (ANN) is a powerful tool for predicting unknown parameters [186–189]. The control parameters and the steady-state risk factor that determines the safe boundary of inverter operations in (5.3) are used to train the neural network. The outcome of the neural network can be expressed as a function, F , that accepts nine inputs which can represent as follows,

$$y = F(x) = F([R_{isk}, k_{p1}, k_{p2}, k_{p3}, k_{p4}, k_{i1}, k_{i2}, k_{i3}, k_{i4}]) \quad (5.5)$$

where R_{isk} is the steady-state risk factor, depending on V_{dc} , V_{th} , Z_{th} , and k_m . Herein, k_{p1} , k_{p2} , k_{p3} , k_{p4} , k_{i1} , k_{i2} , k_{i3} , and k_{i4} are the PI controller gains. The problem is a binary classification problem where the size of $|y| = \gamma = 2$, where the set of target classes is stable, unstable. As F is unknown, the function's responses, y_i , to the input vector, x_i , can be observed. Therefore, a set S of observed input-output points (x, y) are known. The task of ANN is to learn the relation expressed by the set S and come up with an approximated expression, G of F , that can capture such behavior. Generally, $S = S_t \cup S_v$, where S_t represents the training set and S_v represents the validation set to check whether G can accurately estimate the unknown function F . The training process is completed when the following errors become lower than a specified threshold ϵ_0 .

$$\epsilon = \sum_i \|\mathbf{G}(\mathbf{x}_i) - \mathbf{F}(\mathbf{x}_i)\|^2 = \sum_i \|\mathbf{G}(\mathbf{x}_i) - \mathbf{y}_i\|^2 < \epsilon_0 \quad (5.6)$$

For ANN implementation, the training objective is required to define first and then develop an approach to train the neural network to achieve the objective. In this work, the training objective is to minimize the cost function in (5.6).

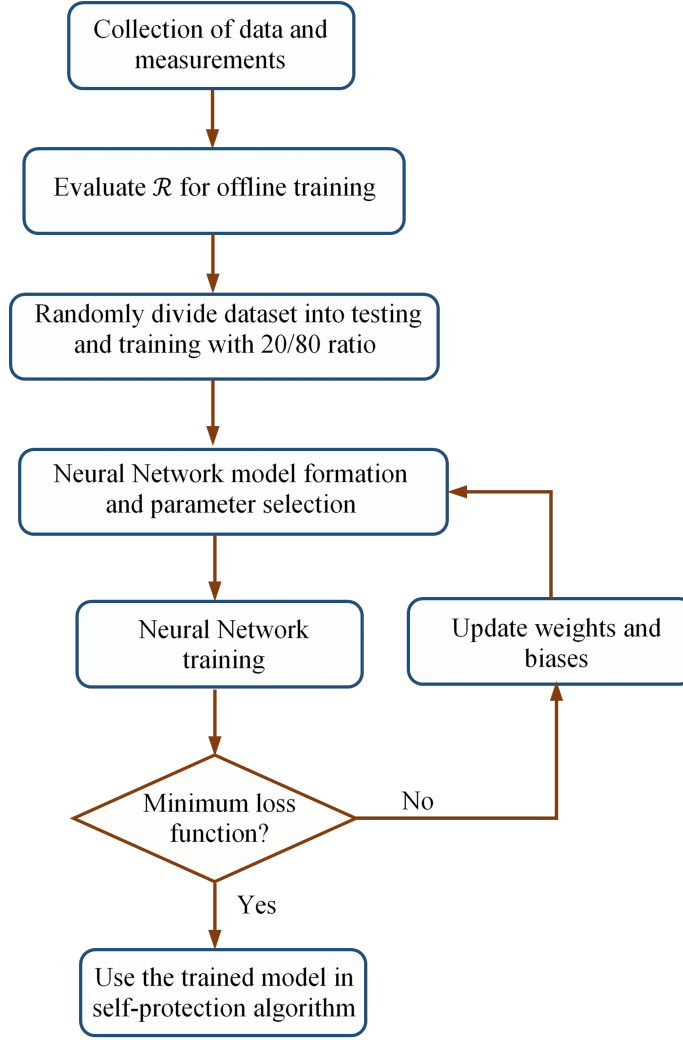


Figure 5.3: *The flowchart of neural network offline training.*

$$J(t, \hat{t}_i) = -\frac{1}{N} \sum_{i=1}^N [t_i \log(\hat{t}_i) + (1 - t_i) \log(1 - \hat{t}_i)] \quad (5.7)$$

where t_i is the true label and $\hat{t}_i$ is predicted output. Notice the cost function in (5.7) is standard cross-entropy. The model parameters that minimized the loss function $J(t_i, \hat{t}_i)$ can be obtained by calculating the gradient of the loss function and implementing (5.7).

$$w_{k+1} = w_k - \alpha \frac{\partial J(t_i, \hat{t}_i)}{\partial w_k} \quad (5.8)$$

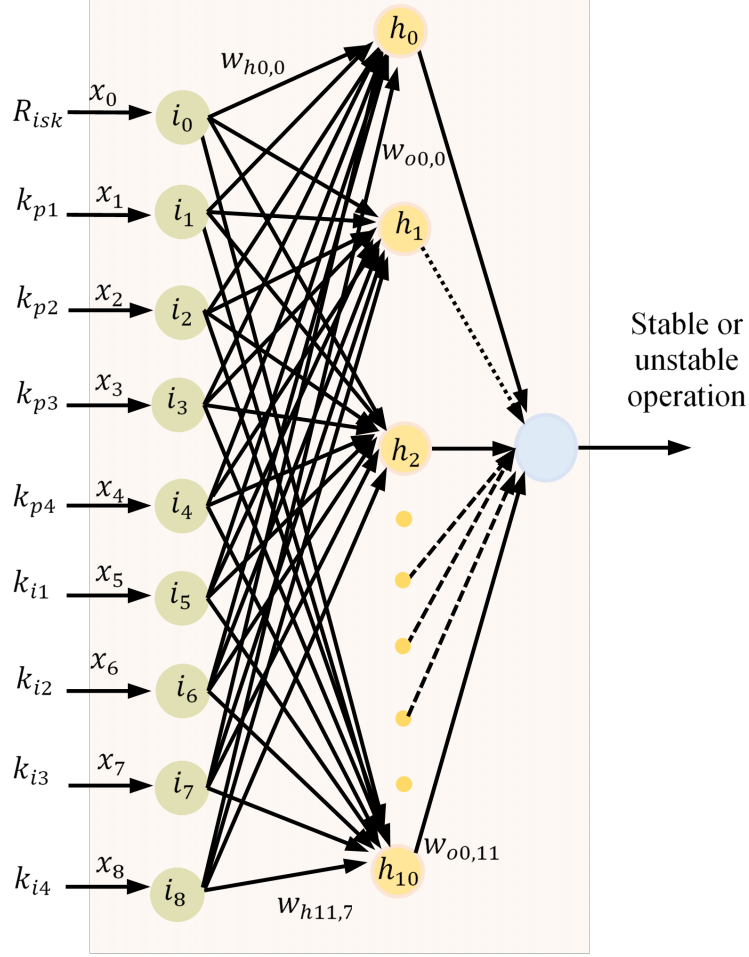


Figure 5.4: *Implemented neural network topology for stable or unstable operation estimation.*

Here α is the step size. The gradient descent method is used to update the weight parameters of the model to minimize the loss function. The algorithm flowchart is presented in Fig. 5.3. The implemented neural network topology is shown in Fig. 5.4. In this work, the developed neural network has nine input nodes, two hidden layers with ten and five nodes, respectively, and an output layer with a single node that indicates the true level of t . Here, the hidden layer is used to learn the unknown function to predict the value of t . The inspection of the neural network in Fig. 5.4 returns the following analytical formulation,

$$y = f_{AN} \sum_{p=0}^{H-1} w_{(o0,hp)} h_p = f_{AN} \sum_{m=0}^{H-1} w_{(o0,hp)} \sum_{q=0}^{l-1} w_{(hp)} i_q x_q \quad (5.9)$$

Here f_{AN} is the activation function by which each neuron implements the learning function. There are several activation functions, such as hyperbolic tangent, sigmoid, rectified linear unit, etc. In this work, the sigmoid function is chosen as the activation function. Noteworthy, this work utilizes a basic neural network structure and standard training approach to develop the self-protective algorithm that effectively ensures the safety of the inverter. For neural network training, a set of training data is collected from an experimental hardware setup. The experimental data is collected for different circuit conditions by changing power setpoints from low to high values. For each setpoint, the inverter dynamic responses, i.e., whether the inverter operation is stable or unstable for commanded power setpoints, are recorded. The trained neural network is used in the self-protective algorithm. However, the inverter operation is highly nonlinear for the hidden mode of instability and also under very weak grid conditions. The performance of a trained neural network could be less accurate depending on the operating conditions. Therefore, the probability of correct prediction using the trained neural network under different operating conditions is determined. The hybrid model sets a predefined threshold for the probability of correct prediction by the trained neural network, determining whether the hybrid model labels the commanded setpoints as safe setpoints.

5.3 The Developed Self-Protection Approach

The flowchart of the proposed self-protective approach is presented in Fig. 5.5. The incoming setpoints are first verified by the requirements of the IEEE Std. 1547 for PCC voltage measurements. The self-protection algorithm momentarily injects a low-frequency signal to estimate the grid parameters in real-time when the IEEE 1547 requirements are verified. Then, the incoming setpoints are examined using the steady-state model. The details of the online grid parameters estimation technique and steady-state model can be found in [97]. If the incoming setpoints are detected unsafe by the steady-state model, the setpoints are rejected by the self-protection algorithm, and the inverter operates on previously accepted setpoints. If the steady-state model passes the setpoints, the dynamic behavior of the inverter for commanded setpoints is inspected by the hybrid dynamic model.

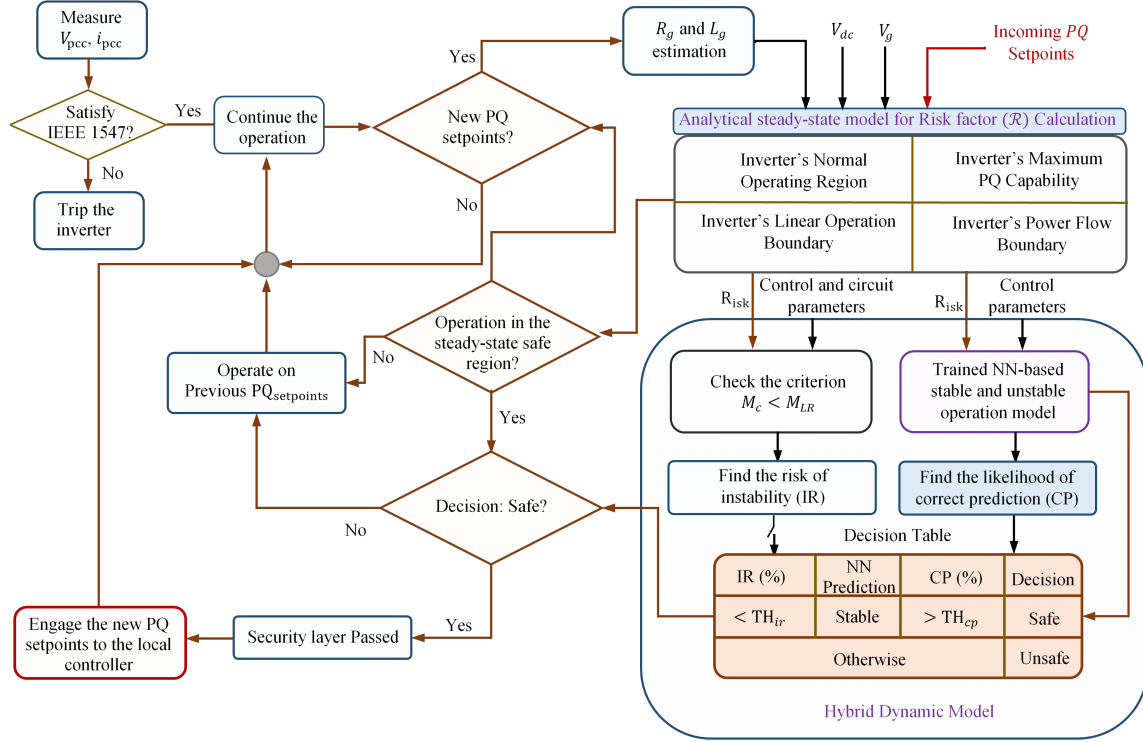


Figure 5.5: Flow chart of the self-protective algorithm of a smart inverter integrating analytical model into neural network platform.

This hybrid model incorporates the analytical criteria defined in equation (5.4) and a trained neural network model. In the hybrid model, the commanded setpoints are assessed using the analytical criterion specified in equation (5.4) to determine the risk of instability. Concurrently, a trained neural network model is employed to predict inverter dynamic behavior. Herein, the neural network takes analytically calculated risk factor, R_{risk} , and control parameters as inputs to predict whether the inverter operation is stable or unstable for commanded power setpoints. The probability of correct prediction of the trained neural network is subsequently calculated to enhance the performance of the hybrid model. The algorithm allows the setpoint to be passed and engaged in the local controller if two conditions are met: first, the instability risk evaluated from the analytical criterion falls below TH_{ir} ; second, the neural network predicts stable operation with a probability of correct prediction exceeding TH_{cp} for the commanded power setpoint. Herein, TH_{ir} , and TH_{cp} denote the threshold for assessing instability risk using the analytical criterion and the probability of accurate

prediction by the neural network, respectively. In contrast, when the hybrid dynamic model determines that the commanded power setpoints are unsafe, the algorithm will reject these setpoints and instead operate based on the previously accepted safe PQ setpoints. It is important to note that the decision regarding safe setpoints derived from the hybrid model depends on the user-defined threshold value. Based on the performance of both the model and operating condition, the decision rule can be updated and implemented in the algorithm accordingly. Notably, the neural network in the developed hybrid dynamic model can be replaced by any alternative classification scheme.

5.4 Experimental Results

The effectiveness of the hybrid data-driven and analytical criterion-based self-protection algorithm is verified in this section. The experimental setup is shown in Fig. 5.6. In this setup, a three-phase 5 kVA SiC MOSFET-based inverter is used, and the switching signals for the inverters are generated using the dSPACE MicroLabBox DS-1202 controller board. In the experimental setup, the inverter feeds a 12 kW NHR 9410 power grid emulator through a three-phase LCL filter. Also, a Magna-Power SL400-15/208 programmable dc supply is employed as the dc source for the inverter. The presented dynamic responses for different

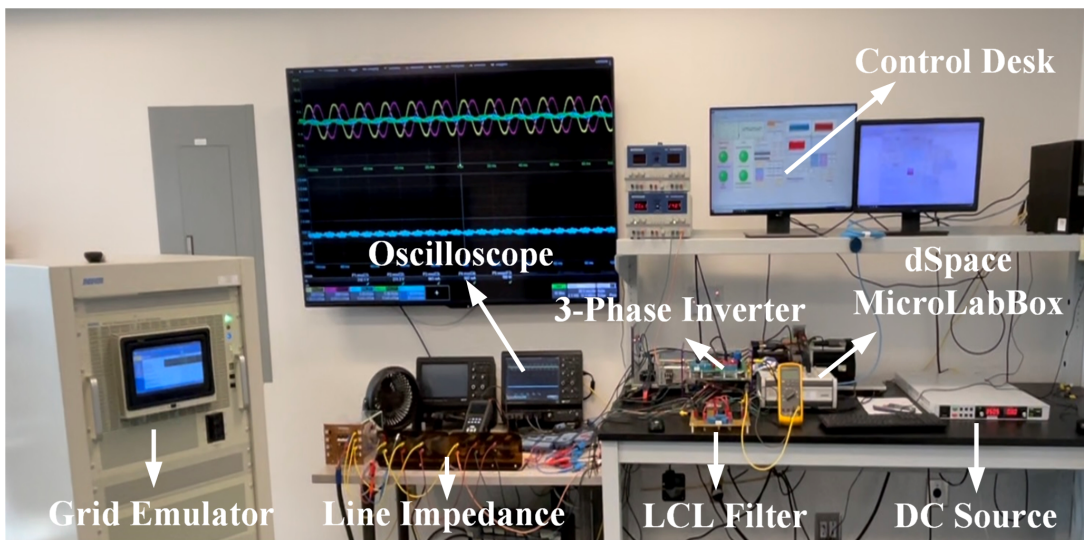


Figure 5.6: *Experimental setup for a three-phase grid-following inverter.*

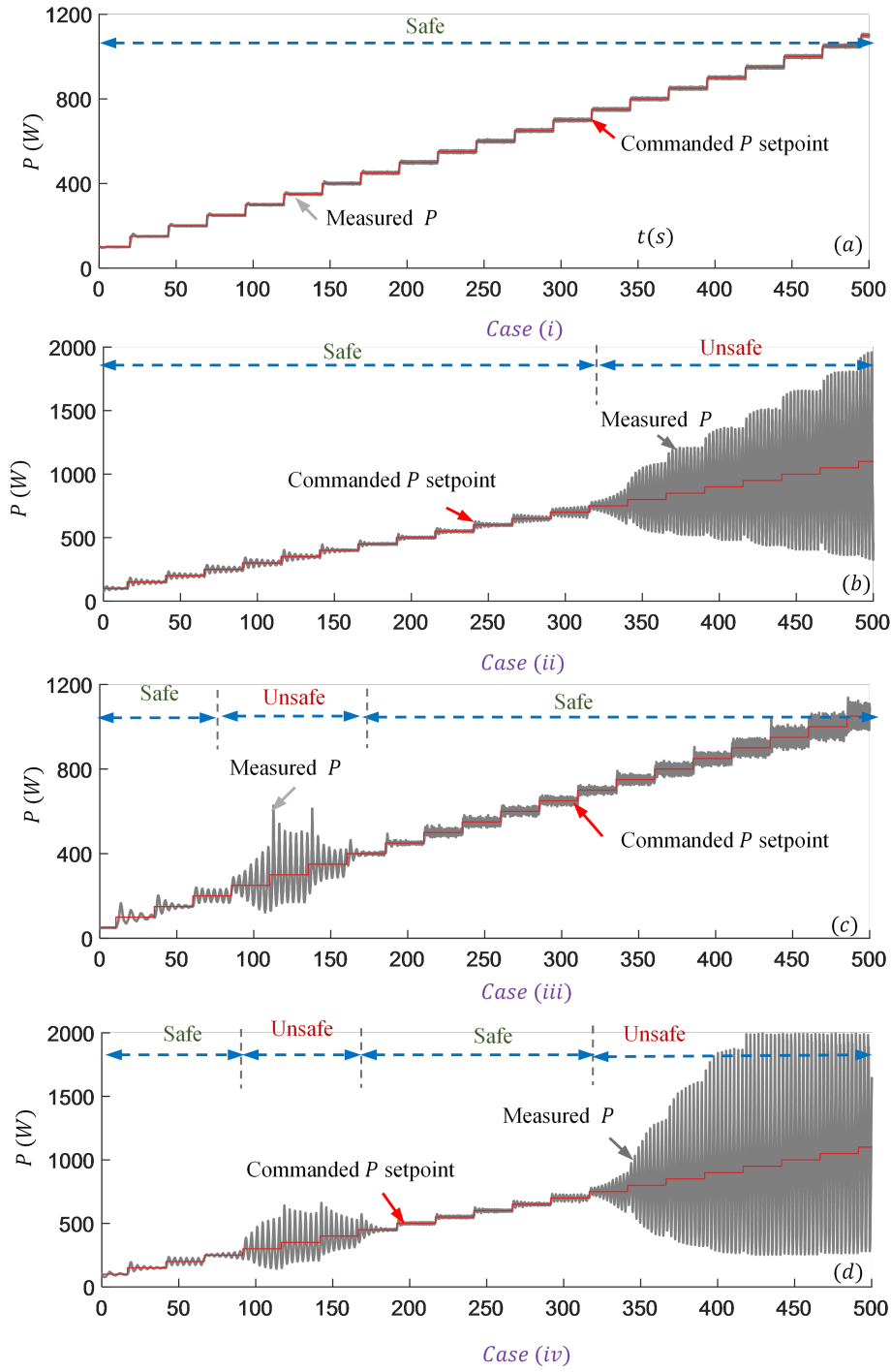


Figure 5.7: Experimentally recorded inverter's dynamic responses from the control desk when the active power is changing step-by-step from 100 W to 1200 W for $Q = 0$ Var.

scenarios in this section are recorded using Control Desk, a real-time software interface with dSPACE, and then plotted in MATLAB. The test scenarios in Fig. 5.7 demonstrate the nonlinear and uncertain behavior of the inverter. In the first test scenario, the controller gain parameters are chosen as $k_{p1} = k_{p3} = 0.021$, $k_{p2} = k_{p4} = 0.8$, $k_{i1} = k_{i3} = 0.06$, $k_{i2} = k_{i4} = 1.2$. Different active power setpoints P^* ranging from 50 W to 1100 W by a step of 50 W are applied to the controller when $Q^* = 0$. The dynamic responses of measured active power are shown in Fig. 5.7 (a). For this control setup, the measured active power follows the desired active power, and the inverter operation is always stable, i.e., safe. For the remaining test scenarios, the controller gains parameters are chosen as $k_{p1} = k_{p3} = 0.009$, $k_{p2} = k_{p4} = 0.1$, $k_{i1} = k_{i3} = 0.06$, $k_{i2} = k_{i4} = 1.2$ to demonstrate the nonlinear behavior of the grid-following inverter.

In the second test scenario, different active power setpoints are applied to the controller as a step similar to Fig. 5.7(a). One can observe that when $0 < P^* < 700W$, the system is in safe operation, and measured active power is following the commanded active power setpoints. However, the dynamic response of the inverter becomes oscillatory beyond 700 W, and the system becomes oscillatory, a clear indication of unsafe operations. In the third test scenario, the dc-bus voltage is reduced to 335 V, and then an oscillatory response is observed when $250 < P^* < 350W$, which occurs below the rated power level; see Fig. 5.7 (c). In the fourth test scenario, the inverter runs when $L_g = 5mH$. For this test scenario, an oscillatory behavior at low power $250 < P^* < 350W$ and at high power $700 < P^* < 1100W$ are present; see Fig. 5.7 (d). Thus, an inverter can move from safe to unsafe or unsafe to safe regions depending on the system parameters, controller setup, and power setpoints. Therefore, one can conclude that a suitable criterion is required to predict the unexpected nonlinear behavior of grid-following inverters, as experimentally demonstrated in Fig. 5.7 (b)-(d).

For the self-protection algorithm implementation, a trained neural network-based stable and unstable operation model is required, as shown in Fig. 5.4. For developing an offline-trained model, a set of experimental datasets is collected for active and reactive power variations. Table I presents the various experimental test scenarios and controller gains that

Table 5.1: *Circuit and Control Parameters of Experimental Setup used for Data Recording for active power setpoints, P^* , variation*

Parameters		Case P1	Case P2	Case P3	Case P4	Case P5	Case P6	Case P7	Case P8	Case P9	Case P10
Controller gain	k_{p1}	0.02	0.001	0.001	0.001	0.001	0.02	0.001	0.001	0.001	0.001
	k_{p2}	0.8	0.1	0.8	0.4	0.2	0.8	0.1	0.8	0.4	0.2
	k_{i1}	0.06	0.06	0.06	0.06	0.06	0.06	0.06	0.06	0.06	0.06
	k_{i2}	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2
Grid inductance (mH)		2.5	2.5	2.5	2.5	2.5	5	5	5	5	5
DC bus voltage		$341V \leq V_{dc} \leq 350V$ (with an increase of 1 V)									
PQ setpoints		$0 \leq P^* \leq 2kW$ (with a step change of 30 W) for $Q^* = 0$ Var									
Tested setpoints		670	670	670	670	670	670	670	670	670	670
Unstable setpoints		0	570	0	168	168	0	497	0	196	458

have been utilized to investigate the dynamic response of inverters for the variation of both active and reactive power setpoints.

A total of 10,700 data samples were acquired from this specific experimental setup and are utilized for the neural network offline training. Two distinct neural network models were developed to evaluate neural network performance. The initial model, NN-A, considers all pertinent experimental testing information as input and predicts the output as safe or unsafe inverters operation for commanded power setpoints. For the second neural network model, namely the NN-B model, the inputs are the steady-state risk factor, R_{isk} , and controller parameters. The trained NN-B model predicts whether the inverter operation is safe or unsafe. The data obtained from different test scenarios are used to evaluate the steady-state risk factor, R_{isk} , analytically. Notice the steady-state risk factor is a function of dc-bus voltage, V_{dc} , the dc-bus utilization factor, k_m , grid-side Thevenin voltage, V_{th} and Thevenin impedance that seen from the inverter side, Z_{th} . The detailed risk factor calculation is provided in [97].

All the tested experimental scenarios in this work are in the safe operating region by the steady-state inverter model defined in [97]. From the collected experimental dataset, 80% of the data are used for training, 10% for the validation procedure, and the remaining 10% for the validation procedure. The Levenberg–Marquardt algorithm was chosen as the neural network training algorithm, a powerful tool for offline batch training [190, 191]. Then the offline trained neural network is implemented in the microprocessor to predict stable and unstable operation. The comparison between the performance matrices of NN-A and NN-B is shown in Table II. The definition of various performance matrices is given in (10).

$$\left\{ \begin{array}{l} \textit{Accuracy} = (T_p + T_n)/(F_p + F_n + T_p + T_n) \\ \textit{Precision} = T_p/(T_p + F_p) \\ \textit{True Positive Rate or Recall} = T_p/(F_n + T_p) \\ \textit{True Negative Rate} = T_n/(F_p + T_n) \\ \textit{False Positive Rate} = F_p/(F_p + T_n) \\ \textit{False Negative Rate} = F_n/(F_n + T_p) \end{array} \right. \quad (5.10)$$

Herein, T_p, T_n, F_p , and F_n represent true positive, true negative, false positive, and false negative, respectively. Different performance metrics are employed to gain a better understanding of the neural network's performance when utilizing the analytically evaluated risk factor, R , as an input instead of using all available experimental information. With a single output for both NN-A and NN-B, NN-A was structured with 14 input nodes and 15 sigmoid nodes, while NN-B had 9 input nodes and 15 sigmoid nodes. These models were trained using MATLAB software version 2020a, utilizing the NN toolbox, on a computer equipped with an Intel Core i9 processor and 32 GB of RAM. The convergence times for NN-A and NN-B were determined to be 0.761 s and 0.699 s, respectively. Table II clearly demonstrates that the performance of NN-B surpasses that of NN-A. The trained NN-B model is employed for the subsequent implementation of a hybrid dynamic model. The performance of the offline trained neural network may deviate due to the highly nonlinear behavior of the inverter,

Table 5.2: *Circuit and Control Parameters of Experimental Setup used for Data Recording for reactive power setpoints, Q^* , variation*

Parameters		Case Q1	Case Q2	Case Q3	Case Q4	Case Q5	Case Q6	Case Q7	Case Q8	Case Q9	Case Q10
Controller gain	k_{p1}	0.02	0.001	0.001	0.001	0.001	0.02	0.001	0.001	0.001	0.001
	k_{p2}	0.8	0.1	0.8	0.4	0.2	0.8	0.1	0.8	0.4	0.2
	k_{i1}	0.06	0.06	0.06	0.06	0.06	0.06	0.06	0.06	0.06	0.06
	k_{i2}	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2
Grid inductance (mH)		2.5	2.5	2.5	2.5	2.5	5	5	5	5	5
DC bus voltage		$341V \leq V_{dc} \leq 350V$ (with an increase of 1 V)									
PQ setpoints		$0 \leq Q^* \leq 1.2kW$ (with a step change of 30 Var) for $P^* = 500W$									
Tested setpoints		400	400	400	400	400	400	400	400	400	400
Unstable setpoints		0	97	0	0	0	0	258	0	39	90

including factors such as hidden modes of instability or weak grid conditions. Therefore, the probability of correct prediction of the trained neural network is evaluated offline to improve the performance. In order to assess the probability of correct prediction, the entire dataset is divided into multiple regions based on the experimental circuit and control parameters. The setpoints are classified as safe when the probability of correct prediction exceeds TH_{cp} . In this work, the neural network's architecture is chosen using the trial and error method. The initial numbers of hidden neurons can be selected using the following rules of thumb [192]: a) The number of hidden neurons should be less than twice the size of the input layer (b) The number of hidden neurons should be two-thirds the size of the input layer, plus the size of the output layer, etc. Noteworthy, the neural network classification accuracy tends to increase with the number of hidden layers and neurons on each layer. However, more hidden layers and neurons may cause the problem of overfitting depending on the training dataset. Therefore, the number of hidden layers and neurons should be appropriately chosen.

Table 5.3: *Performance of Neural Network for Stable and Unstable Operation Estimation*

Performance matrix	NN-A		NN-B	
	Training dataset	Testing dataset	Training dataset	Testing dataset
Accuracy (%)	89	87.3	94.73	93.9
TPR (%)	95.2	93.64	97.7	97
TNR (%)	82.8	78.2	92.33	90.7
$FPR(\%)$	29.9	31.7	14.40	14.9
$FNR(\%)$	9.3	10.16	4.6	5.1
Precision(%)	90.7	89.83	97.69	94.94
F1 score (%)	92.89	91.69	95	94.91

The power setpoints are evaluated simultaneously using the analytical stability criterion described in equation (5.4) and the neural network. For a particular range of R_g , the value of instability risk is evaluated using (5.4). Depending on the value of M_c and $(L_1+L_2)/(L_2+L_g)$, the value of R_g i.e., the instability risk is estimated. When the estimated R_g is at the maximum value, the risk of instability is high, i.e., 100%, and for minimum R_g , the risk is low, i.e., 0%. A threshold, TH_{ir} , can be defined for the evaluated instability risk to mark commanded power setpoint as safe or unsafe. When the instability risk falls below a defined threshold, TH_{ir} , the power setpoints are classified as safe. Conversely, power setpoints are considered unsafe when the instability risk exceeds the threshold.

The performance of the hybrid model is evaluated by using a test dataset. The test dataset consists of two case scenarios of 1070 data points for both active and reactive power variations. The true number of stable and unstable points in this test datasets are 835 and 235, respectively. For these tested points, the range of R_g in (5.4) varies from 0.2 to 1.15. Based on the analytical criterion, there are 781 power setpoints with instability risk below 50% and 289 power setpoints with instability risk above 50%. For this testing dataset, the trained NN-B model predicts 802 and 268 power setpoints as stable and unstable operations, respectively. The probability of correct prediction for these two case scenarios is 93.7% and 91.7%, respectively. To improve the performance of the neural network model, an additional threshold, TH_{cp} , can be established. Above this threshold, the commanded setpoints are classified as safe by the neural network. By setting a higher threshold, the neural network

can enhance its ability to distinguish and classify setpoints that are deemed safe with a higher degree of confidence. Thus, the utilization of the hybrid model can enhance the safety of an inverter by protecting against unsafe operations caused by malicious power setpoints. The presented hybrid model lacks the capability to distinguish between unsafe operations resulting from manipulations of PQ setpoints (cyberattacks) and weak grid conditions. Also, under weak grid conditions, where the grid exhibits higher uncertainty and variability, the estimation of unknown grid parameters can be impacted, which can jeopardize the performance of the self-protection algorithm. Noteworthy, even a marginal improvement in detecting malicious power setpoints using this hybrid model can yield substantial advantages by preventing undesirable power interruptions or blackouts caused by the unstable operation of an inverter.

5.5 Conclusion

This chapter developed an artificial intelligence-based analytical criterion to predict the safe inverter operation. The following conclusions can be highlighted-

- It has been shown that manipulated power setpoints can cause unexpected unsafe operations below the rated power level.
- Two forms of hybrid dynamic model have been developed that incorporate an analytical criterion and offline-trained neural network model to examine the power setpoints.
- The first hybrid model employs analytically evaluated risk factors as inputs for the neural network. These risk factors are determined through analytical methods and are fed into the neural network model. The neural network then processes these inputs and generates predictions regarding the stability or instability of the inverter's operation. This model effectively uses the evaluated risk factors to predict whether the operation of the inverter is stable or unstable.
- The other hybrid model combines a neural network with a stability criterion introduced in Chapter 4. It uses the neural network and the stability criterion in parallel to predict stable and unstable operations.
- Furthermore, a standard neural network is implemented as a benchmark that considers

all relevant information as input and predicts whether the operation of the inverter is safe or unsafe.

- It has been found that the proposed hybrid dynamic model can prevent engaging unsafe setpoints to the local controller and ensure safe inverter operation.

Chapter 6

Conclusions and Suggestions for Future Work

In this chapter, the contents of this dissertation are summarized with the contributions of the work highlighted. This chapter is organized into two sections. In Section 6.1, the summary of the dissertation is presented. In Section 6.2, suggestions for possible future work based are discussed.

6.1 Summary and Conclusions

In this dissertation, a novel self-protective algorithm has been developed to enhance the safety of smart inverters. Inverters play an important role in distributed energy generation in the energy infrastructure, where a supervisory control structure is required for energy management and economic dispatch. In a centralized supervisory control structure, the inverters need to be in contact with aggregators, other energy generation units, or the utility operating center. The communication capability makes a grid-interactive inverter a cyber-physical device. However, the connection of inverters to a communication network exposes the inverters to active attackers who can interfere with the control infrastructure and send malicious setpoints to the local controller. Chapter 1 discussed the role of smart inverters

as cyber-physical devices and possible cyberattack scenarios, the concept of self-learning for self-secure inverters, and the reference model framework for self-secure Inverters.

In 2, two real-time grid parameter estimation techniques have been formulated and experimentally validated. The first approach, called recursive-least square, and model reference estimation, relies on a low-frequency signal injection-based method. These techniques facilitate grid parameter estimation whenever a new PQ setpoint is commanded to the inverter's controller. A comparison of the performance between both grid parameter estimation methods was conducted, revealing that the recursive-least square estimation method outperforms the model reference adaptive estimation method. Based on these results, the recursive-least square method was selected for the development of the self-protective algorithm discussed in Chapter 3.

A self-protection method has been developed for grid-interactive inverters in Chapter 3. In the self-protection method, the analytical steady-state and dynamic reference models used to inspect incoming PQ setpoints have been explained and validated. The reference models have been developed based on the steady-state linear and nonlinear operating regions and a full-order dynamic model of grid-interactive inverters. The nonlinear behavior of the inverter has been experimentally demonstrated for both dynamic and steady-state analyses. In the steady-state experiment, it has been verified that a decrease in the dc-bus voltage or an increase in the grid voltage can significantly reduce the normal operating region for a given setpoint. Furthermore, it has been verified that a change in the setpoint can change the system due to PQ control loops and move the eigenvalues to the instability region for a given set of control gains. The developed models for the self-protection method can significantly provide self-security for grid-interactive inverters against intentional (intrusion) and unintentional (accidental) unsafe setpoints when the communication protocols, system-level security, and cybersecurity solutions fail to detect those unsafe setpoints.

A stability criterion has been developed for inspecting the power setpoints and predicting the safe operation of the inverter in Chapter 4. The stability criterion is developed from a reduced-order model of a simplified inverter circuit. A hidden instability mode has been introduced and analyzed for PQ-controlled inverters. This unforeseen instability issue has

been identified at a power range below the rated level, mainly when the inverter operates in weak grids. Several scenarios have been investigated to understand the impact of controller nonlinearity and filter parameters variation on the stability of the inverter. It has been shown that low-frequency eigenvalues of the closed-loop model can dominate the overall system dynamics. It has also been demonstrated that the inverter system moves to a stable or unstable region for different power setpoints. It has also been verified that multiple pairs of eigenvalues in the state-space model can lead to instability at different power levels and frequencies. Furthermore, it has been verified that a change in the setpoint can change the system parameters due to PQ control loops and move the eigenvalues to the instability region for a given set of control gains. The hidden instability mode and the stability criterion are verified by a set of experiments using a 3kVA inverter feeding a programmable 208V, 12kW power grid emulator.

Furthermore, a novel hybrid dynamic model has been developed to inspect the incoming PQ setpoint of a grid-interactive inverter in Chapter 5. The hybrid dynamic model was developed by combining a data-driven neural network with an analytical model. The neural network is used to learn the relationship between the PQ setpoint and the inverter's stability, while the analytical model provides a theoretical foundation for the neural network. Two forms of the hybrid dynamic model have been developed in this dissertation. The first form uses the analytical model to evaluate the steady-state risk factors of the inverter's operation. These risk factor has been used as inputs to the neural network, which predicts the stability of the inverter. The second form of the model uses the neural network and the analytical model in parallel. The neural network predicts the stability of the inverter, while the analytical model provides a measure of the uncertainty in the neural network's prediction. The effectiveness of the hybrid dynamic model has been evaluated through simulation and hardware tests.

In conclusion, this dissertation contributes novel self-protective methods for grid-interactive inverters. It develops self-learning features and reference models to inspect and detect unsafe power setpoints, protecting the inverter-based system from malicious attacks and potential damage. The dissertation also presents analytical steady-state and dynamic reference models

for assessing the safety of setpoints, as well as a stability criterion to predict inverter behavior. To address computational challenges, hybrid dynamic models combining data-driven and analytical approaches are proposed. The effectiveness of these methods is validated through hardware experiments and simulations, demonstrating their practical applicability in ensuring the safe operation of grid-interactive inverters.

6.2 Suggestions for Future Work

The effectiveness of the techniques proposed in this dissertation has been extensively validated through rigorous testing and experimentation. The results demonstrate their capability to detect and protect against unsafe power setpoints, ensuring the secure operation of grid-interactive inverters. However, it is important to acknowledge that there are further opportunities for advancement and expansion based on the findings and methodologies presented in this study.

- The recursive least square and model reference adaptive estimation technique has been presented in this dissertation to estimate the grid parameters in real-time. There are several potential research directions based on the grid parameter estimation techniques presented in Chapter 2. While these techniques are developed for self-protective algorithms, they can also be applied to other areas of interest. These include islanding detection [193–195], power flow control [196], passive filter design [197], active filter control [198], etc.

- As a future area of research, it could be explored to implement a strategy where the inverter operating power setpoints are dynamically adjusted based on the risk factor, specifically when the risk factor is high. In this context, the "high-risk factor" refers to situations where power setpoints are in close proximity to the steady-state stability boundary.

- The analytical reference model developed in Chapter 3 can provide extra security for inverters to ensure safe operation. The self-protective method is independent and does not require information on the entire system. The developed self-protective method can be used by energy management system vendors, inverter development companies, and Research institutions.

- The stability criterion presented in Chapter 4 can estimate the gain margin of the controller. It offers a simplified yet effective means to predict the stability of the system, enabling the selection of suitable controller gains that ensure stability and reliable operation.

- The hybrid model developed in Chapter 5 effectively combined an analytical criterion with an offline-trained neural network model to analyze and predict inverter performance. As a future research direction, exploring online trained models can be pursued further to enhance the capabilities and adaptability of the hybrid model. An online trained model continuously updates and refines the neural network's parameters using real-time data. By incorporating online training, the hybrid model can adapt to changing operating conditions, environmental factors, and system dynamics, leading to more accurate and up-to-date predictions of inverter dynamic responses.

Bibliography

- [1] B. Mirafzal and A. Adib, “On grid-interactive smart inverters: Features and advancements,” *IEEE Access*, vol. 8, pp. 160526–160536, 2020.
- [2] Y. Li and J. Yan, “Cybersecurity of smart inverters in the smart grid: A survey,” *IEEE Transactions on Power Electronics*, vol. 38, no. 2, pp. 2364–2383, 2023.
- [3] S. Madichetty and S. Mishra, “Cyber attack detection and correction mechanisms in a distributed dc microgrid,” *IEEE Transactions on Power Electronics*, vol. 37, no. 2, pp. 1476–1485, 2022.
- [4] F. Sadeque, J. Benzaquen, A. Adib, and B. Mirafzal, “Direct phase-angle detection for three-phase inverters in asymmetrical power grids,” *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 1, pp. 520–528, 2021.
- [5] S. Zhao, Y. Peng, Y. Zhang, and H. Wang, “Parameter estimation of power electronic converters with physics-informed machine learning,” *IEEE Transactions on Power Electronics*, vol. 37, no. 10, pp. 11567–11578, 2022.
- [6] A. Singh and B. Mirafzal, “An efficient grid-connected three-phase single-stage boost current source inverter,” *IEEE Power and Energy Technology Systems Journal*, vol. 6, no. 3, pp. 142–151, 2019.
- [7] A. Kawamura, T. Haneyoshi, and R. Hoft, “Deadbeat controlled pwm inverter with parameter estimation using only voltage sensor,” *IEEE Transactions on Power Electronics*, vol. 3, no. 2, pp. 118–125, 1988.
- [8] Z. Li, G. Feng, D. O’Donnell, W. Li, and N. C. Kar, “Novel machine parameter estimation scheme toward accurate maximum torque production for dual three-phase

- pmsms,” *IEEE Transactions on Transportation Electrification*, vol. 7, no. 4, pp. 2715–2727, 2021.
- [9] B. Mirafzal, G. L. Skibinski, and R. M. Tallam, “A failure mode for pwm inverter-fed ac motors due to the antiresonance phenomenon,” *IEEE Transactions on Industry Applications*, vol. 45, no. 5, pp. 1697–1705, 2009.
 - [10] T. S. Ustun, “Cybersecurity vulnerabilities of smart inverters and their impacts on power system operation,” in *2019 International Conference on Power Electronics, Control and Automation (ICPECA)*, pp. 1–4, 2019.
 - [11] N. D. Tuyen, N. S. Quan, V. B. Linh, V. Van Tuyen, and G. Fujita, “A comprehensive review of cybersecurity in inverter-based smart power system amid the boom of renewable energy,” *IEEE Access*, vol. 10, pp. 35846–35875, 2022.
 - [12] S. S. Hussain and T. S. Ustun, “Smart inverter communication model and impact of cybersecurity attack,” in *2020 IEEE International Conference on Power Electronics, Drives and Energy Systems (PEDES)*, pp. 1–5, 2020.
 - [13] M. Gursoy and B. Mirafzal, “On self-security of grid-interactive smart inverters,” in *2021 IEEE Kansas Power and Energy Conference (KPEC)*, pp. 1–6, 2021.
 - [14] S. Kim, Y. Eun, and K.-J. Park, “Stealthy sensor attack detection and real-time performance recovery for resilient cps,” *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7412–7422, 2021.
 - [15] Y. Wang, Q. Liu, E. Mihankhah, C. Lv, and D. Wang, “Detection and isolation of sensor attacks for autonomous vehicles: Framework, algorithms, and validation,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, pp. 8247–8259, 2022.
 - [16] H. Jeon and Y. Eun, “A stealthy sensor attack for uncertain cyber-physical systems,” *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6345–6352, 2019.

- [17] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, 2017.
- [18] K. Sun, W. Qiu, Y. Dong, C. Zhang, H. Yin, W. Yao, and Y. Liu, "Wams-based hvdc damping control for cyber attack defense," *IEEE Transactions on Power Systems*, vol. 38, no. 1, pp. 702–713, 2023.
- [19] Y. Zhao, W. Yao, C.-K. Zhang, X. Ai, and J. Wen, "Resilient wide-area damping control to mitigate strong cyber attack: A multiple-controller switching approach," *IEEE Transactions on Smart Grid*, vol. 14, no. 3, pp. 2326–2337, 2023.
- [20] C. Burgos-Mellado, F. Donoso, T. Dragičević, R. Cárdenas-Dobson, P. Wheeler, J. Clare, and A. Watson, "Cyber-attacks in modular multilevel converters," *IEEE Transactions on Power Electronics*, vol. 37, no. 7, pp. 8488–8501, 2022.
- [21] A. Adib, B. Mirafzal, X. Wang, and F. Blaabjerg, "On stability of voltage source inverters in weak grids," *IEEE Access*, vol. 6, pp. 4427–4439, Jan. 2018.
- [22] A. Adib, F. Fateh, and B. Mirafzal, "Smart inverter stability enhancement in weak grids using adaptive virtual-inductance," *IEEE Transactions on Industry Applications*, vol. 57, no. 1, pp. 814–823, 2021.
- [23] D. Du, M. Zhu, X. Li, M. Fei, S. Bu, L. Wu, and K. Li, "A review on cybersecurity analysis, attack detection, and attack defense methods in cyber-physical power systems," *Journal of Modern Power Systems and Clean Energy*, vol. 11, no. 3, pp. 727–743, 2023.
- [24] A. Adib, J. Lamb, and B. Mirafzal, "Ancillary services via vsis in microgrids with maximum dc-bus voltage utilization," *IEEE Transactions on Industry Applications*, vol. 55, no. 1, pp. 648–658, 2019.
- [25] T. S. Ustun, J. Hashimoto, and K. Otani, "Impact of smart inverters on feeder hosting capacity of distribution networks," *IEEE Access*, vol. 7, pp. 163526–163536, 2019.

- [26] D. J. Sebastian and A. Hahn, “Exploring emerging cybersecurity risks from network-connected der devices,” in *2017 North American Power Symposium (NAPS)*, pp. 1–6, 2017.
- [27] I. Serban, S. Céspedes, C. Marinescu, C. A. Azurdia-Meza, J. S. Gómez, and D. S. Hueichapan, “Communication requirements in microgrids: A practical survey,” *IEEE Access*, vol. 8, pp. 47694–47712, 2020.
- [28] R. A. G. Burbano, M. L. O. Gutierrez, J. A. Restrepo, and F. G. Guerrero, “Ied design for a small-scale microgrid using iec 61850,” *IEEE Transactions on Industry Applications*, vol. 55, no. 6, pp. 7113–7121, 2019.
- [29] U. Sinha, A. A. Hadi, T. Faika, and T. Kim, “Blockchain-based communication and data security framework for iot-enabled micro solar inverters,” in *2019 IEEE CyberPELS (CyberPELS)*, pp. 1–5, IEEE, 2019.
- [30] A. H. Lone and R. Naaz, “Applicability of blockchain smart contracts in securing internet and iot: A systematic literature review,” *Computer Science Review*, vol. 39, p. 100360, 2021.
- [31] D. Saleem, A. Sundararajan, A. Sanghvi, J. Rivera, A. I. Sarwat, and B. Kroposki, “A multidimensional holistic framework for the security of distributed energy and control systems,” *IEEE Systems Journal*, vol. 14, no. 1, pp. 17–27, 2019.
- [32] Y. He, G. J. Mendis, and J. Wei, “Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism,” *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2505–2516, 2017.
- [33] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, “Machine learning methods for attack detection in the smart grid,” *IEEE transactions on neural networks and learning systems*, vol. 27, no. 8, pp. 1773–1786, 2015.
- [34] A. Kavousi-Fard, W. Su, and T. Jin, “A machine-learning-based cyber attack detection

- model for wireless sensor networks in microgrids,” *IEEE Transactions on Industrial Informatics*, vol. 17, no. 1, pp. 650–658, 2020.
- [35] A. Adib, K. K. Afridi, M. Amirabadi, F. Fateh, M. Ferdowsi, B. Lehman, L. H. Lewis, B. Mirafzal, M. Saeedifard, M. B. Shadmand, and P. Shamsi, “E-mobility — advancements and challenges,” *IEEE Access*, vol. 7, pp. 165226–165240, 2019.
- [36] S. K. Mazumder, A. Kulkarni, S. Sahoo, F. Blaabjerg, H. A. Mantooth, J. C. Balda, Y. Zhao, J. A. Ramos-Ruiz, P. N. Enjeti, P. Kumar, *et al.*, “A review of current research trends in power-electronic innovations in cyber–physical systems,” *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 5, pp. 5146–5163, 2021.
- [37] S. Tan, J. M. Guerrero, P. Xie, R. Han, and J. C. Vasquez, “Brief survey on attack detection methods for cyber-physical systems,” *IEEE Systems Journal*, vol. 14, no. 4, pp. 5329–5339, 2020.
- [38] J. Ye, A. Giani, A. Elasser, S. K. Mazumder, C. Farnell, H. A. Mantooth, T. Kim, J. Liu, B. Chen, G.-S. Seo, *et al.*, “A review of cyber–physical security for photovoltaic systems,” *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 10, no. 4, pp. 4879–4901, 2021.
- [39] T. Hossen, D. Sharma, and B. Mirafzal, “Smart inverter twin model for anomaly detection,” in *2021 IEEE 22nd Workshop on Control and Modelling of Power Electronics (COMPEL)*, pp. 1–6, 2021.
- [40] M. S. Pilehvar, D. Sharma, and B. Mirafzal, “Forming interphase microgrids in distribution systems using cooperative inverters,” *CPSS Transactions on Power Electronics and Applications*, vol. 7, no. 2, pp. 186–195, 2022.
- [41] M. S. Pilehvar, M. B. Shadmand, and B. Mirafzal, “Analysis of smart loads in nanogrids,” *IEEE Access*, vol. 7, pp. 548–562, 2019.
- [42] O. Dag and B. Mirafzal, “On stability of islanded low-inertia microgrids,” in *2016 Clemson University Power Systems Conference (PSC)*, pp. 1–7, 2016.

- [43] M. S. Pilehvar and B. Mirafzal, “Frequency and voltage supports by battery-fed smart inverters in mixed-inertia microgrids,” *Electronics*, vol. 9, no. 11, p. 1755, 2020.
- [44] S. Sahoo, Y. Yang, and F. Blaabjerg, “Resilient synchronization strategy for ac microgrids under cyber attacks,” *IEEE Transactions on Power Electronics*, vol. 36, no. 1, pp. 73–77, 2021.
- [45] S. Goel and R. Sharma, “Performance evaluation of stand alone, grid connected and hybrid renewable energy systems for rural application: A comparative review,” *Renew. Sustain. Energy Rev.*, vol. 78, pp. 1378–1389, 2017.
- [46] H. He and J. Yan, “Cyber-physical attacks and defences in the smart grid: a survey,” *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 13–27, 2016.
- [47] H. Wang, M. Liserre, and F. Blaabjerg, “Toward reliable power electronics: Challenges, design tools, and opportunities,” *IEEE Industrial Electronics Magazine*, vol. 7, no. 2, pp. 17–26, 2013.
- [48] D. M. Scholten, N. Ertugrul, and W. Soong, “Micro-inverters in small scale pv systems: A review and future directions,” in *2013 Australasian universities power engineering conference (AUPEC)*, pp. 1–6, IEEE, 2013.
- [49] U. Cert, “Russian government cyber activity targeting energy and other critical infrastructure sectors,” *Us Cert*, pp. 1–19, 2018.
- [50] “Installation and operation guide SOLECTRIA ® XGI 1500-250 series inverters.” https://www.solectria.com//site/assets/files/2981/xgi-1500_175-250_manual_rev_7_-_30_may_2023-1.pdf. Accessed: 2023-8-6.
- [51] Y. Wang, X. Wang, F. Blaabjerg, and Z. Chen, “Harmonic instability assessment using state-space modeling and participation analysis in inverter-fed power systems,” *IEEE Transactions on Industrial Electronics*, vol. 64, no. 1, pp. 806–816, 2017.

- [52] M. A. Awal, L. D. Flora, and I. Husain, “Observer based generalized active damping for voltage source converters with lcl filters,” *IEEE Transactions on Power Electronics*, vol. 37, no. 1, pp. 125–136, 2022.
- [53] T. S. Basso and R. DeBlasio, “Ieee 1547 series of standards: interconnection issues,” *IEEE Transactions on Power Electronics*, vol. 19, no. 5, pp. 1159–1162, 2004.
- [54] I. Murzakhanov, S. Gupta, S. Chatzivasileiadis, and V. Kekatos, “Optimal design of volt/var control rules for inverter-interfaced distributed energy resources,” *IEEE Transactions on Smart Grid*, 2023.
- [55] N. Sadan and B. Renz, “New der communications platform enables derms and conforms with ieee 1547–2018 requirements,” in *2020 IEEE/PES Transmission and Distribution Conference and Exposition*, pp. 1–5, 2020.
- [56] M. Ghalib, A. Ahmed, I. Al-Shiab, Z. Boudia, and M. Ibnkahla, “Implementation of a smart grid communication system compliant with ieee 2030.5,” in *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1–6, IEEE, 2018.
- [57] J. Johnson, B. Fox, K. Kaur, and J. Anandan, “Evaluation of interoperable distributed energy resources to ieee 1547.1 using sunspec modbus, ieee 1815, and ieee 2030.5,” *IEEE Access*, vol. 9, pp. 142129–142146, 2021.
- [58] E. D. G. Mlot, J. Saldana, and R. J. Rodríguez, “Towards a testbed for critical industrial systems: Sunspec protocol on der systems as a case study,” in *2022 IEEE 27th International Conference on Emerging Technologies and Factory Automation (ETFA)*, pp. 1–4, IEEE, 2022.
- [59] M. A. H. Sadi, D. Zhao, T. Hong, and M. H. Ali, “Time sequence machine learning-based data intrusion detection for smart voltage source converter-enabled power grid,” *IEEE Systems Journal*, vol. 17, no. 2, pp. 2477–2488, 2023.

- [60] C. Carter, I. Onunkwo, P. Cordeiro, and J. Johnson, “Cyber security assessment of distributed energy resources,” in *2017 IEEE 44th Photovoltaic Specialist Conference (PVSC)*, pp. 2135–2140, 2017.
- [61] A. K. Jain, N. Sahani, and C.-C. Liu, “Detection of falsified commands on a der management system,” *IEEE Transactions on Smart Grid*, vol. 13, no. 2, pp. 1322–1334, 2021.
- [62] S. Hossain-McKenzie, A. Chavez, N. Jacobs, C. B. Jones, A. Summers, and B. Wright, “Proactive intrusion detection and mitigation system: Case study on packet replay attacks in distributed energy resource systems,” in *2021 IEEE Power and Energy Conference at Illinois (PECI)*, pp. 1–6, IEEE, 2021.
- [63] S. Liu, Z. Hu, X. Wang, and L. Wu, “Stochastic stability analysis and control of secondary frequency regulation for islanded microgrids under random denial of service attacks,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 7, pp. 4066–4075, 2019.
- [64] J. Lai and X. Lu, “Resilient distributed voltage synchronization of ci networks under denial of service attacks,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 68, no. 6, pp. 2052–2056, 2021.
- [65] S. Liu, P. Siano, and X. Wang, “Intrusion-detector-dependent frequency regulation for microgrids under denial-of-service attacks,” *IEEE Systems Journal*, vol. 14, no. 2, pp. 2593–2596, 2020.
- [66] 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,” *IET Cyber-Physical Systems: Theory & Applications*, vol. 5, no. 3, pp. 274–282, 2020.
- [67] P. Wlazlo, A. Sahu, Z. Mao, H. Huang, A. Goulart, K. Davis, and S. Zonouz, “Man-

- in-the-middle attacks and defence in a power system cyber-physical testbed,” *IET Cyber-Physical Systems: Theory & Applications*, vol. 6, no. 3, pp. 164–177, 2021.
- [68] A. Sahu, P. Wlazlo, Z. Mao, H. Huang, A. Goulart, K. Davis, and S. Zonouz, “Design and evaluation of a cyber-physical testbed for improving attack resilience of power systems,” *IET Cyber-Physical Systems: Theory & Applications*, vol. 6, no. 4, pp. 208–227, 2021.
- [69] A. P. Kuruvila, I. Zografopoulos, K. Basu, and C. Konstantinou, “Hardware-assisted detection of firmware attacks in inverter-based cyberphysical microgrids,” *International Journal of Electrical Power & Energy Systems*, vol. 132, p. 107150, 2021.
- [70] D. J. Sebastian, U. Agrawal, A. Tamimi, and A. Hahn, “Der-tee: Secure distributed energy resource operations through trusted execution environments,” *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6476–6486, 2019.
- [71] A. Barua and M. A. Al Faruque, “Premsat: Preventing magnetic saturation attack on hall sensors,” *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 438–462, 2022.
- [72] Z. Zhang, M. Easley, M. Hosseinzadehtaher, G. Amariuca, M. B. Shadmand, and H. Abu-Rub, “An observer based intrusion detection framework for smart inverters at the grid-edge,” in *2020 IEEE Energy Conversion Congress and Exposition (ECCE)*, pp. 1957–1962, IEEE, 2020.
- [73] A. Barua and M. A. Al Faruque, “Hall spoofing: a noninvasive dos attack on grid-tied solar inverter,” in *Proceedings of the 29th USENIX Conference on Security Symposium*, pp. 1273–1290, 2020.
- [74] K. Gupta, S. Sahoo, R. Mohanty, B. K. Panigrahi, and F. Blaabjerg, “Distinguishing between cyber attacks and faults in power electronic systems—a non-invasive approach,” *IEEE Journal of Emerging and Selected Topics in Power Electronics*, 2022.

- [75] S. Abhinav, H. Modares, F. L. Lewis, F. Ferrese, and A. Davoudi, “Synchrony in networked microgrids under attacks,” *IEEE Transactions on Smart Grid*, vol. 9, no. 6, pp. 6731–6741, 2017.
- [76] I. Zografopoulos and C. Konstantinou, “Detection of malicious attacks in autonomous cyber-physical inverter-based microgrids,” *IEEE Transactions on Industrial Informatics*, vol. 18, no. 9, pp. 5815–5826, 2022.
- [77] M. Jamali, M. S. Sadabadi, M. Davari, S. Sahoo, and F. Blaabjerg, “Resilient cooperative secondary control of islanded ac microgrids utilizing inverter-based resources against state-dependent false data injection attacks,” *IEEE Transactions on Industrial Electronics*, 2023.
- [78] H. M. Albusnashee, C. Farnell, A. Suchanek, K. Haulmark, R. A. McCann, J. Di, and A. Mantooth, “A test bed for detecting false data injection attacks in systems with distributed energy resources,” *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 10, no. 1, pp. 1303–1315, 2022.
- [79] F. Sadeque and B. Mirafzal, “Frequency restoration of grid-forming inverters in pulse load and plug-in events,” *IEEE Journal of Emerging and Selected Topics in Industrial Electronics*, vol. 4, no. 2, pp. 580–588, 2023.
- [80] D. Sharma, F. Sadeque, and B. Mirafzal, “Synchronization of inverters in grid forming mode,” *IEEE Access*, vol. 10, pp. 41341–41351, 2022.
- [81] F. Sadeque, D. Sharma, and B. Mirafzal, “Multiple grid-forming inverters in black-start: The challenges,” in *2021 IEEE 22nd Workshop on Control and Modelling of Power Electronics (COMPEL)*, pp. 1–6, 2021.
- [82] F. Sadeque and B. Mirafzal, “A universal controller for grid-forming inverters in micro-grid during islanding for low transient current,” in *2022 1st IEEE International Conference on Industrial Electronics: Developments and Applications (ICIDeA)*, pp. 62–67, 2022.

- [83] J. Ramos-Ruiz, J. Kim, W.-H. Ko, T. Huang, P. Enjeti, P. R. Kumar, and L. Xie, “An active detection scheme for cyber attacks on grid-tied pv systems,” in *2020 IEEE CyberPELS (CyberPELS)*, pp. 1–6, 2020.
- [84] S. Liu, P. X. Liu, and X. Wang, “Effects of cyber attacks on islanded microgrid frequency control,” in *2016 IEEE 20th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, pp. 461–464, 2016.
- [85] M. Chlela, G. Joos, and M. Kassouf, “Impact of cyber-attacks on islanded microgrid operation,” in *Proceedings of the Workshop on Communications, Computation and Control for Resilient Smart Energy Systems*, pp. 1–5, 2016.
- [86] H. Zhang, W. Meng, J. Qi, X. Wang, and W. X. Zheng, “Distributed load sharing under false data injection attack in an inverter-based microgrid,” *IEEE Transactions on Industrial Electronics*, vol. 66, no. 2, pp. 1543–1551, 2019.
- [87] M. Uddin and A. A. Rahman, “Dynamic multi layer signature based intrusion detection system using mobile agents,” *arXiv preprint arXiv:1010.5036*, 2010.
- [88] M. R. Habibi, H. R. Baghaee, T. Dragičević, and F. Blaabjerg, “False data injection cyber-attacks mitigation in parallel dc/dc converters based on artificial neural networks,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 68, no. 2, pp. 717–721, 2021.
- [89] C. Burgos-Mellado, C. Zuñiga-Bauerle, D. Muñoz-Carpintero, Y. Arias-Esquivel, R. Cárdenas-Dobson, T. Dragičević, F. Donoso, and A. Watson, “Reinforcement learning-based method to exploit vulnerabilities of false data injection attack detectors in modular multilevel converters,” *IEEE Transactions on Power Electronics*, vol. 38, no. 7, pp. 8907–8921, 2023.
- [90] M. R. Habibi, H. R. Baghaee, T. Dragičević, and F. Blaabjerg, “Detection of false data injection cyber-attacks in dc microgrids based on recurrent neural networks,”

- IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 5, pp. 5294–5310, 2021.
- [91] M. R. Habibi, S. Sahoo, S. Rivera, T. Dragičević, and F. Blaabjerg, “Decentralized coordinated cyberattack detection and mitigation strategy in dc microgrids based on artificial neural networks,” *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 4, pp. 4629–4638, 2021.
 - [92] Y. He, G. J. Mendis, and J. Wei, “Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism,” *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2505–2516, 2017.
 - [93] F. Pasqualetti, F. Dörfler, and F. Bullo, “Attack detection and identification in cyber-physical systems,” *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, 2013.
 - [94] L.-Y. Lu, H. J. Liu, H. Zhu, and C.-C. Chu, “Intrusion detection in distributed frequency control of isolated microgrids,” *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6502–6515, 2019.
 - [95] A. Ferdowsi and W. Saad, “Deep learning for signal authentication and security in massive internet-of-things systems,” *IEEE Transactions on Communications*, vol. 67, no. 2, pp. 1371–1387, 2019.
 - [96] T. Hossen, F. Sadeque, M. Gursoy, and B. Mirafzal, “Self-secure inverters against malicious setpoints,” in *2020 IEEE Electric Power and Energy Conference (EPEC)*, pp. 1–6, 2020.
 - [97] T. Hossen, M. Gursoy, and B. Mirafzal, “Self-protective inverters against malicious setpoints using analytical reference models,” *IEEE Journal of Emerging and Selected Topics in Industrial Electronics*, vol. 3, no. 4, pp. 871–877, 2022.
 - [98] M. Gursoy and B. Mirafzal, “Self-security for grid-interactive smart inverters using

- steady-state reference model,” in *2021 IEEE 22nd Workshop on Control and Modelling of Power Electronics (COMPEL)*, pp. 1–5, 2021.
- [99] J. Lamb, B. Mirafzal, and F. Blaabjerg, “Pwm common mode reference generation for maximizing the linear modulation region of chb converters in islanded microgrids,” *IEEE Transactions on Industrial Electronics*, vol. 65, no. 7, pp. 5250–5259, 2018.
- [100] A. Khan, M. Hosseinzadehtaher, M. B. Shadmand, D. Saleem, and H. Abu-Rub, “Intrusion detection for cybersecurity of power electronics dominated grids: Inverters pq set-points manipulation,” in *2020 IEEE CyberPELS (CyberPELS)*, pp. 1–8, 2020.
- [101] A. R. Malekpour and A. Pahwa, “A dynamic operational scheme for residential pv smart inverters,” *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2258–2267, 2016.
- [102] C. Shah, J. D. Vasquez-Plaza, D. D. Campo-Ossa, J. F. Patarroyo-Montenegro, N. Guruwacharya, N. Bhujel, R. D. Trevizan, F. A. Rengifo, M. Shirazi, R. Tonkoski, *et al.*, “Review of dynamic and transient modeling of power electronic converters for converter dominated power systems,” *IEEE Access*, vol. 9, pp. 82094–82117, 2021.
- [103] L. Fan, Z. Miao, S. Shah, P. Koralewicz, V. Gevorgian, and J. Fu, “Data-driven dynamic modeling in power systems: A fresh look on inverter-based resource modeling,” *IEEE Power and Energy Magazine*, vol. 20, no. 3, pp. 64–76, 2022.
- [104] E. Muljadi, M. Singh, and V. Gevorgian, “User guide for pv dynamic model simulation written on pscad platform,” tech. rep., National Renewable Energy Lab.(NREL), Golden, CO (United States), 2014.
- [105] D. Yan, C. Yang, L. Hang, Y. He, P. Luo, L. Shen, and P. Zeng, “Review of general modeling approaches of power converters,” *Chinese Journal of Electrical Engineering*, vol. 7, no. 1, pp. 27–36, 2021.

- [106] P. Benner, T. Mitchell, and M. L. Overton, “Low-order control design using a reduced-order model with a stability constraint on the full-order model,” in *2018 IEEE Conference on Decision and Control (CDC)*, pp. 3000–3005, 2018.
- [107] O. Ajala, N. Baeckeland, B. Johnson, S. Dhople, and A. Domínguez-García, “Model reduction and dynamic aggregation of grid-forming inverter networks,” *IEEE Transactions on Power Systems*, pp. 1–16, 2022.
- [108] W. Du, F. K. Tuffner, K. P. Schneider, R. H. Lasseter, J. Xie, Z. Chen, and B. Bhattarai, “Modeling of grid-forming and grid-following inverters for dynamic simulation of large-scale distribution systems,” *IEEE Transactions on Power Delivery*, vol. 36, no. 4, pp. 2035–2045, 2020.
- [109] S. Nag, Z. Qu, and Y. Xu, “A unified grid-forming and grid-following primary control design with optimized enforcement of grid operational constraints,” *IEEE Access*, 2023.
- [110] A. Singhal, T. L. Vu, and W. Du, “Consensus control for coordinating grid-forming and grid-following inverters in microgrids,” *IEEE Transactions on Smart Grid*, vol. 13, no. 5, pp. 4123–4133, 2022.
- [111] T. Hossen and B. Mirafzal, “Hidden modes of instability for inverters in weak grids,” *IEEE Transactions on Industry Applications*, pp. 1–10, 2023.
- [112] X. Peng and H. Yang, “Impedance-based stability criterion for the stability evaluation of grid-connected inverter systems with distributed parameter lines,” *CSEE Journal of Power and Energy Systems*, 2020.
- [113] X. Liu, Z. Zou, J. Yang, J. Tang, Z. Liu, G. Buticchi, Z. Wang, and M. Cheng, “Stability assessment of a radial grid with power converters,” *IEEE Open Journal of Power Electronics*, vol. 3, pp. 61–74, 2021.
- [114] P. Yu, Z. Tian, X. Zha, J. Sun, P. Zhong, and M. Huang, “Impact analysis of fast dynamics on stability of grid-tied inverter based on oscillator model and damping

- torque analysis,” *IEEE Transactions on Power Systems*, vol. 37, no. 3, pp. 1881–1892, 2021.
- [115] R. Chan, J. Baek, and S. Kwak, “Simple algorithm with fast dynamics for cascaded h-bridge multilevel inverter based on model predictive control method,” in *2017 IEEE Applied Power Electronics Conference and Exposition (APEC)*, pp. 696–702, 2017.
- [116] L. Zheng, R. P. Kandula, K. Kandasamy, and D. Divan, “Fast dynamic control of stacked low inertia converters,” in *2018 IEEE Energy Conversion Congress and Exposition (ECCE)*, pp. 3126–3133, 2018.
- [117] C. Yu, H. Xu, C. Liu, C. Chen, Q. Wang, and X. Zhang, “Stability margin analysis of multi-inverter grid-connected system considering asynchronous control period under high penetration,” in *2021 IEEE 12th Energy Conversion Congress and Exposition - Asia (ECCE-Asia)*, pp. 2080–2085, 2021.
- [118] C. Tu, J. Gao, F. Xiao, Q. Guo, and F. Jiang, “Stability analysis of the grid-connected inverter considering the asymmetric positive-feedback loops introduced by the pll in weak grids,” *IEEE Transactions on Industrial Electronics*, vol. 69, no. 6, pp. 5793–5802, 2022.
- [119] Y. Si, N. Korada, Q. Lei, and R. Ayyanar, “A robust controller design methodology addressing challenges under system uncertainty,” *IEEE Open Journal of Power Electronics*, vol. 3, pp. 402–418, 2022.
- [120] P. Kundur, J. Paserba, V. Ajjarapu, G. Andersson, A. Bose, C. Canizares, N. Hatziargyriou, D. Hill, A. Stankovic, C. Taylor, *et al.*, “Definition and classification of power system stability ieee/cigre joint task force on stability terms and definitions,” *IEEE transactions on Power Systems*, vol. 19, no. 3, pp. 1387–1401, 2004.
- [121] V. Krishnamurthy and V. Seshadri, “Model reduction using the routh stability criterion,” *IEEE Transactions on Automatic Control*, vol. 23, no. 4, pp. 729–731, 1978.

- [122] S. Anand and B. G. Fernandes, “Reduced-order model and stability analysis of low-voltage dc microgrid,” *IEEE Transactions on Industrial Electronics*, vol. 60, no. 11, pp. 5040–5049, 2013.
- [123] D. Pal and B. K. Panigrahi, “Reduced-order modeling and transient synchronization stability analysis of multiple heterogeneous grid-tied inverters,” *IEEE Transactions on Power Delivery*, vol. 38, no. 2, pp. 1074–1085, 2023.
- [124] T. Hossen, F. Sadeque, F. Fateh, and B. Mirafzal, “Projection of safe operation for inverters using artificial intelligence-based stability criterion,” in *2023 IEEE Applied Power Electronics Conference and Exposition (APEC)*, pp. 3083–3088, 2023.
- [125] M. Imran, A. Ghafoor, and M. Imran, “Stability preserving model reduction technique for 1-d and 2-d systems with error bounds,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 69, no. 3, pp. 1084–1088, 2022.
- [126] V. Purba, B. B. Johnson, M. Rodriguez, S. Jafarpour, F. Bullo, and S. V. Dhople, “Reduced-order aggregate model for parallel-connected single-phase inverters,” *IEEE Transactions on Energy Conversion*, vol. 34, no. 2, pp. 824–837, 2019.
- [127] Y. Gu, N. Bottrell, and T. C. Green, “Reduced-order models for representing converters in power system studies,” *IEEE Transactions on Power Electronics*, vol. 33, no. 4, pp. 3644–3654, 2017.
- [128] A. Alqahtani, M. Alsaffar, M. El-Sayed, B. Alajmi, *et al.*, “Data-driven photovoltaic system modeling based on nonlinear system identification,” *International Journal of Photoenergy*, vol. 2016, 2016.
- [129] D. P. Solomatine and A. Ostfeld, “Data-driven modelling: some past experiences and new approaches,” *Journal of hydroinformatics*, vol. 10, no. 1, pp. 3–22, 2008.
- [130] K. Moradi, H. Sheikahmadi, P. Zamani, Q. Shafiee, and H. Bevrani, “A data-driven pi control of grid-connected voltage source inverters interfaced with lcl filter,” in *2022 13th*

- Power Electronics, Drive Systems, and Technologies Conference (PEDSTC)*, pp. 645–650, 2022.
- [131] S. Subedi, R. Fournay, H. M. Rekabdarkolaee, R. Tonkoski, T. M. Hansen, J. D. Vasquez-Plaza, and F. Andrade, “Impact of pll design on data-driven models for grid-connected single-phase inverters,” in *2022 International Symposium on Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM)*, pp. 930–935, 2022.
 - [132] S. Sahoo, H. Wang, and F. Blaabjerg, “On the explainability of black box data-driven controllers for power electronic converters,” in *2021 IEEE Energy Conversion Congress and Exposition (ECCE)*, pp. 1366–1372, 2021.
 - [133] G. Rojas-Dueñas, J.-R. Riba, K. Kahalerras, M. Moreno-Eguilaz, A. Kadechkar, and A. Gomez-Pau, “Black-box modelling of a dc-dc buck converter based on a recurrent neural network,” in *2020 IEEE International Conference on Industrial Technology (ICIT)*, pp. 456–461, 2020.
 - [134] D. F. Z. Romero, A. S. Vélez, and J. B. Gómez-Mendoza, “Non-linear grey-box models applied to dc motor identification,” in *2019 IEEE 4th Colombian Conference on Automatic Control (CCAC)*, pp. 1–5, 2019.
 - [135] W. Zhou, R. E. Torres-Olguin, Y. Wang, and Z. Chen, “A gray-box hierarchical oscillatory instability source identification method of multiple-inverter-fed power systems,” *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 3, pp. 3095–3113, 2021.
 - [136] P. Khaledian, *Data-Driven Analysis and Dynamic Modeling of Inverter-Based Resources Under Grid Disturbances Enabled by Automated Event Region Identification*. University of California, Riverside, 2022.
 - [137] A. S. Zamzam, X. Fu, and N. D. Sidiropoulos, “Data-driven learning-based optimization for distribution system state estimation,” *IEEE Transactions on Power Systems*, vol. 34, no. 6, pp. 4796–4805, 2019.

- [138] Q. Deng, Z. Li, J. Liu, S. Li, P. Luo, and K. Cui, “Data-driven modeling and control considering time delays for wpt system,” *IEEE Transactions on Power Electronics*, vol. 37, no. 8, pp. 9923–9932, 2022.
- [139] W. Tang and P. Daoutidis, “Data-driven control: Overview and perspectives,” in *2022 American Control Conference (ACC)*, pp. 1048–1064, 2022.
- [140] H. Long, S. Xu, X. Lu, Z. Yang, C. Li, J. Jing, and Z. Wu, “Data-driven hybrid equivalent dynamic modeling of multiple photovoltaic power stations based on ensemble gated recurrent unit,” *Frontiers in Energy Research*, vol. 8, p. 185, 2020.
- [141] C.-H. Choi, K.-R. Cho, and J.-K. Seok, “Inverter nonlinearity compensation in the presence of current measurement errors and switching device parameter uncertainties,” *IEEE Transactions on Power Electronics*, vol. 22, no. 2, pp. 576–583, 2007.
- [142] T. Hossen and B. Mirafzal, “On projection of safe operation for grid-following inverters - grid parameter estimation,” in *2022 1st IEEE International Conference on Industrial Electronics: Developments and Applications (ICIDeA)*, pp. 68–72, 2022.
- [143] T. Hossen, M. Gursoy, and B. Mirafzal, “Digital twin for self-security of smart inverters,” in *2021 IEEE Energy Conversion Congress and Exposition (ECCE)*, pp. 713–718, 2021.
- [144] T. Hossen and B. Mirafzal, “On stability of pq-controlled grid-following and droop-control grid-forming inverters,” in *2022 IEEE Energy Conversion Congress and Exposition (ECCE)*, pp. 1–7, 2022.
- [145] T. Hossen, G. Amariuca, and B. Mirafzal, “Integrating an analytical risk factor into a neural network framework for self-protective inverters,” *IEEE Journal of Emerging and Selected Topics in Power Electronics*, pp. 1–1, 2023.
- [146] G. Wang, F. Gao, J. Liu, Q. Li, and Y. Zhao, “Design consideration and performance analysis of a hybrid islanding detection method combining voltage unbalance/total

- harmonic distortion and bilateral reactive power variation,” *CPSS Transactions on power electronics and applications*, vol. 5, no. 1, pp. 86–100, 2020.
- [147] M. F. Umar, M. Easley, B. Nun, A. Khan, M. B. Shadmand, S. Bayhan, and H. Abu-Rub, “Single-phase grid-interactive inverter with resonance suppression based on adaptive predictive control in weak grid condition,” *IEEE Journal of Emerging and Selected Topics in Industrial Electronics*, vol. 3, no. 3, pp. 809–820, 2021.
- [148] P. Garcia, M. Sumner, Á. Navarro-Rodríguez, J. M. Guerrero, and J. Garcia, “Observer-based pulsed signal injection for grid impedance estimation in three-phase systems,” *IEEE Transactions on Industrial Electronics*, vol. 65, no. 10, pp. 7888–7899, 2018.
- [149] J. H. Suárez, H. M. Gomes, A. J. Sguarezi Filho, D. A. Fernandes, and F. F. Costa, “Grid impedance estimation for grid-tie inverters based on positive sequence estimator and morphological filter,” *Electrical Engineering*, vol. 102, no. 3, pp. 1195–1205, 2020.
- [150] J. M. Cano, Á. Navarro-Rodríguez, A. Suárez, and P. García, “Variable switching frequency control of distributed resources for improved system efficiency,” *IEEE Transactions on Industry Applications*, vol. 54, no. 5, pp. 4612–4620, 2018.
- [151] J. Fang, H. Deng, and S. M. Goetz, “Grid impedance estimation through grid-forming power converters,” *IEEE Transactions on Power Electronics*, vol. 36, no. 2, pp. 2094–2104, 2020.
- [152] D. Reigosa, F. Briz, C. B. Charro, P. García, and J. M. Guerrero, “Active islanding detection using high-frequency signal injection,” *IEEE Transactions on Industry Applications*, vol. 48, no. 5, pp. 1588–1597, 2012.
- [153] M. Sumner, B. Palethorpe, and D. W. Thomas, “Impedance measurement for improved power quality-part 1: the measurement technique,” *IEEE Transactions on Power Delivery*, vol. 19, no. 3, pp. 1442–1448, 2004.

- [154] N. Hoffmann and F. W. Fuchs, “Minimal invasive equivalent grid impedance estimation in inductive–resistive power networks using extended kalman filter,” *IEEE Transactions on Power Electronics*, vol. 29, no. 2, pp. 631–641, 2013.
- [155] L. Asiminoaei, R. Teodorescu, F. Blaabjerg, and U. Borup, “Implementation and test of an online embedded grid impedance estimation technique for pv inverters,” *IEEE Transactions on Industrial Electronics*, vol. 52, no. 4, pp. 1136–1144, 2005.
- [156] A. V. Timbus, P. Rodriguez, R. Teodorescu, and M. Ciobotaru, “Line impedance estimation using active and reactive power variations,” in *2007 IEEE Power Electronics Specialists Conference*, pp. 1273–1279, IEEE, 2007.
- [157] J. Benzaquen, F. Fateh, and B. Mirafzal, “On the dynamic performance of variable-frequency ac–dc converters,” *IEEE Transactions on Transportation Electrification*, vol. 6, no. 2, pp. 530–539, 2020.
- [158] J. Benzaquen, F. Fateh, M. B. Shadmand, and B. Mirafzal, “One-step-ahead adaptive control scheme for active rectifiers in wild frequency applications,” in *2019 IEEE Applied Power Electronics Conference and Exposition (APEC)*, pp. 588–593, 2019.
- [159] J. Benzaquen and B. Mirafzal, “Seamless dynamics for wild-frequency active rectifiers in more electric aircraft,” *IEEE Transactions on Industrial Electronics*, vol. 67, no. 9, pp. 7135–7145, 2020.
- [160] E. A. Soto, L. B. Bosman, E. Wollega, and W. D. Leon-Salas, “Analysis of grid disturbances caused by massive integration of utility level solar power systems,” *Eng*, vol. 3, no. 2, pp. 236–253, 2022.
- [161] N. Guo, Z. Qu, X. Shang, H. Ding, K. Liu, W. Song, H. Wang, J. Wang, D. Zhao, and Q. Xue, “Analysis and improvement of performance instability in extended interaction klystrons with random geometrical perturbations,” *IEEE Transactions on Electron Devices*, vol. 69, no. 10, pp. 5886–5894, 2022.

- [162] N. Nilsson and J. Mercurio, “Synchronous generator capability curve testing and evaluation,” *IEEE Transactions on Power Delivery*, vol. 9, no. 1, pp. 414–424, 1994.
- [163] J. Lamb and B. Mirafzal, “Grid-interactive cascaded h-bridge multilevel converter pq plane operating region analysis,” *IEEE Transactions on Industry Applications*, vol. 53, no. 6, pp. 5744–5752, 2017.
- [164] A. Bahrami and M. Narimani, “A sinusoidal pulsewidth modulation (spwm) technique for capacitor voltage balancing of a nested t-type four-level inverter,” *IEEE Transactions on Power Electronics*, vol. 34, no. 2, pp. 1008–1012, 2019.
- [165] B. Mirafzal, *Power Electronics in Energy Conversion Systems*. McGraw-Hill Education, 2022.
- [166] J. Lamb and B. Mirafzal, “Active and reactive power operational region for grid-interactive cascaded h-bridge multilevel converters,” in *2016 IEEE Energy Conversion Congress and Exposition (ECCE)*, pp. 1–6, 2016.
- [167] J. A. Houldsworth and D. A. Grant, “The use of harmonic distortion to increase the output voltage of a three-phase pwm inverter,” *IEEE Transactions on industry applications*, no. 5, pp. 1224–1228, 1984.
- [168] R. M. Tallam and D. Leggate, “Control of a pwm voltage-source inverter in the pulse-dropping region to reduce reflected-wave motor overvoltage,” *IEEE Transactions on Industry Applications*, vol. 49, no. 2, pp. 873–879, 2013.
- [169] S. Hasan, K. M. Muttaqi, D. Sutanto, and M. A. Rahman, “A novel dual slope delta modulation technique for a current source inverter based dynamic voltage restorer for mitigation of voltage sags,” *IEEE Transactions on Industry Applications*, vol. 57, no. 5, pp. 5437–5447, 2021.
- [170] B. Mirafzal, M. Saghaeini, and A. K. Kaviani, “An svpwm-based switching pattern for stand-alone and grid-connected three-phase single-stage boost inverters,” *IEEE Transactions on Power Electronics*, vol. 26, no. 4, pp. 1102–1111, 2011.

- [171] J. Lamb and B. Mirafzal, “An adaptive spwm technique for cascaded multilevel converters with time-variant dc sources,” *IEEE Transactions on Industry Applications*, vol. 52, no. 5, pp. 4146–4155, 2016.
- [172] N. Mohammed, T. Kerekes, and M. Ciobotaru, “An online event-based grid impedance estimation technique using grid-connected inverters,” *IEEE Transactions on Power Electronics*, vol. 36, no. 5, pp. 6106–6117, 2021.
- [173] F. A. Alskran, *Dynamic modeling and analysis of the three-phase voltage source inverter under stand-alone and grid-tied modes*. PhD thesis, Kansas State University, 2014.
- [174] D. G. Holmes and T. A. Lipo, *Pulse width modulation for power converters: principles and practice*, vol. 18. John Wiley & Sons, 2003.
- [175] L. Harnefors, A. G. Yepes, A. Vidal, and J. Doval-Gandoy, “Passivity-based controller design of grid-connected vscs for prevention of electrical resonance instability,” *IEEE Transactions on Industrial Electronics*, vol. 62, no. 2, pp. 702–710, 2015.
- [176] X.-M. Zhang, Q.-L. Han, X. Ge, and L. Ding, “Resilient control design based on a sampled-data model for a class of networked control systems under denial-of-service attacks,” *IEEE Transactions on Cybernetics*, vol. 50, no. 8, pp. 3616–3626, 2020.
- [177] H. Zhang, Z. Zhang, Z. Wang, and Q. Shan, “New results on stability and stabilization of networked control systems with short time-varying delay,” *IEEE Transactions on Cybernetics*, vol. 46, no. 12, pp. 2772–2781, 2016.
- [178] M. Gursoy and B. Mirafzal, “Direct vs. indirect control schemes for grid-forming inverters – unveiling a performance comparison in a microgrid,” *IEEE Access*, pp. 1–1, 2023.
- [179] S. Zhou, X. Zou, D. Zhu, L. Tong, Y. Zhao, Y. Kang, and X. Yuan, “An improved design of current controller for lcl-type grid-connected converter to reduce negative

- effect of pll in weak grid,” *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 6, no. 2, pp. 648–663, 2018.
- [180] Y. He, H. S.-H. Chung, C.-T. Lai, X. Zhang, and W. Wu, “Active cancelation of equivalent grid impedance for improving stability and injected power quality of grid-connected inverter under variable grid condition,” *IEEE Transactions on Power Electronics*, vol. 33, no. 11, pp. 9387–9398, 2018.
- [181] X. Chen, Y. Wang, Y. Zhang, J. Chen, and C. Gong, “Hybrid damping adaptive control scheme for grid-connected inverters in a weak grid,” *IET power electronics*, vol. 9, no. 15, pp. 2760–2768, 2016.
- [182] X. Li, J. Fang, Y. Tang, X. Wu, and Y. Geng, “Capacitor-voltage feedforward with full delay compensation to improve weak grids adaptability of lcl-filtered grid-connected converters for distributed generation systems,” *IEEE Transactions on Power Electronics*, vol. 33, no. 1, pp. 749–764, 2017.
- [183] A. Singh, A. K. Kaviani, and B. Mirafzal, “On dynamic models and stability analysis of three-phase phasor pwm-based csi for stand-alone applications,” *IEEE Transactions on Industrial Electronics*, vol. 62, no. 5, pp. 2698–2707, 2015.
- [184] A. K. Kaviani and B. Mirafzal, “Dynamic model of the three-phase single-stage boost inverter for grid-connected applications,” in *2012 IEEE Energy Conversion Congress and Exposition (ECCE)*, pp. 4627–4634, 2012.
- [185] J. Lu, B. Jiang, and W. X. Zheng, “Potential impacts of delay on stability of impulsive control systems,” *IEEE Transactions on Automatic Control*, vol. 67, no. 10, pp. 5179–5190, 2022.
- [186] B. K. Bose, “Neural network applications in power electronics and motor drives—an introduction and perspective,” *IEEE Transactions on Industrial Electronics*, vol. 54, no. 1, pp. 14–33, 2007.

- [187] Y. Liao, Y. Li, M. Chen, L. Nordström, X. Wang, P. Mittal, and H. V. Poor, “Neural network design for impedance modeling of power electronic systems based on latent features,” *IEEE Transactions on Neural Networks and Learning Systems*, pp. 1–13, 2023.
- [188] M.-H. Kim, M. Simoes, and B. Bose, “Neural network-based estimation of power electronic waveforms,” *IEEE Transactions on Power Electronics*, vol. 11, no. 2, pp. 383–389, 1996.
- [189] S. Mohagheghi, R. G. Harley, T. G. Habetler, and D. Divan, “Condition monitoring of power electronic circuits using artificial neural networks,” *IEEE Transactions on Power Electronics*, vol. 24, no. 10, pp. 2363–2367, 2009.
- [190] S. Zhang, H. Huang, and Z. Han, “A levenberg-marquardt algorithm based incremental scheme for complex-valued neural networks,” in *2019 IEEE Symposium Series on Computational Intelligence (SSCI)*, pp. 1479–1485, 2019.
- [191] J. d. J. Rubio, “Stability analysis of the modified levenberg-marquardt algorithm for the artificial neural network training,” *IEEE Transactions on Neural Networks and Learning Systems*, vol. 32, no. 8, pp. 3510–3524, 2021.
- [192] G.-B. Huang, “Learning capability and storage capacity of two-hidden-layer feedforward networks,” *IEEE Transactions on Neural Networks*, vol. 14, no. 2, pp. 274–281, 2003.
- [193] J. Sun, “Impedance-based stability criterion for grid-connected inverters,” *IEEE Transactions on Power Electronics*, vol. 26, no. 11, pp. 3075–3078, 2011.
- [194] R. E. Serrano-Finetti, “Output impedance measurement in low-power sources and conditioners,” *IEEE Transactions on Instrumentation and Measurement*, vol. 58, no. 1, pp. 180–186, 2009.

- [195] L. Asiminoaei, R. Teodorescu, F. Blaabjerg, and U. Borup, “A digital controlled pv-inverter with grid impedance estimation for ens detection,” *IEEE Transactions on Power Electronics*, vol. 20, no. 6, pp. 1480–1490, 2005.
- [196] M. Ciobotaru, V. G. Agelidis, R. Teodorescu, and F. Blaabjerg, “Accurate and less-disturbing active antiislanding method based on pll for grid-connected converters,” *IEEE Transactions on Power Electronics*, vol. 25, no. 6, pp. 1576–1584, 2010.
- [197] J. C. Vasquez, J. M. Guerrero, A. Luna, P. Rodríguez, and R. Teodorescu, “Adaptive droop control applied to voltage-source inverters operating in grid-connected and islanded modes,” *IEEE transactions on industrial electronics*, vol. 56, no. 10, pp. 4088–4096, 2009.
- [198] J. Das, “Passive filters-potentialities and limitations,” in *Conference Record of the 2003 Annual Pulp and Paper Industry Technical Conference, 2003.*, pp. 187–197, 2003.

Appendix A

Full-Order Model Equations and Stability Criterion Formulation

A.1 Full-Order Model Equations

The closed-loop state-space model of the PQ-controlled grid-interactive inverter used in Chapter 3 is represented here to duplicate the eigenvalue analysis demonstrated in Section V

$$\begin{aligned}
 A_{11} &= \begin{bmatrix} \frac{-3R_1-R_f}{3L_1} & -\omega \\ \omega & \frac{-3R_1-R_f}{3L_1} \end{bmatrix}, A_{12} = \begin{bmatrix} \frac{-1}{2L_1} & \frac{\sqrt{3}}{6L_1} \\ \frac{-\sqrt{3}}{6L_1} & \frac{-1}{2L_1} \end{bmatrix}, A_{13} = \begin{bmatrix} \frac{R_f}{3L_1} & 0 \\ 0 & \frac{R_f}{3L_1} \end{bmatrix}, \\
 A_{21} &= \begin{bmatrix} \frac{1}{2C_f} & \frac{\sqrt{3}}{6C_f} \\ \frac{-\sqrt{3}}{6C_f} & \frac{1}{2C_f} \end{bmatrix}, A_{22} = \begin{bmatrix} 0 & -\omega \\ \omega & 0 \end{bmatrix}, A_{23} = \begin{bmatrix} \frac{-1}{2C_f} & \frac{-\sqrt{3}}{6C_f} \\ \frac{\sqrt{3}}{6C_f} & \frac{-1}{2C_f} \end{bmatrix}, \\
 A_{31} &= \begin{bmatrix} \frac{R_f}{3L_2} & 0 \\ 0 & \frac{R_f}{3L_2} \end{bmatrix}, A_{32} = \begin{bmatrix} \frac{1}{2L_2} & \frac{-\sqrt{3}}{6L_2} \\ \frac{\sqrt{3}}{6L_2} & \frac{1}{2L_2} \end{bmatrix}, A_{33} = \begin{bmatrix} \frac{-3R_2-R_f}{3L_2} & -\omega \\ \omega & \frac{-3R_2-R_f}{3L_2} \end{bmatrix}.
 \end{aligned} \tag{A.1}$$

The full-form of the block matrices introduced in matrix B of (3.3) are provided below:

$$\begin{aligned}
B_{12} &= \begin{bmatrix} \frac{V_{dc}\cos(\psi)}{\sqrt{3}L_1} & \frac{-MV_{dc}\sin(\psi)}{\sqrt{3}L_1} \\ \frac{-V_{dc}\sin(\psi)}{\sqrt{3}L_1} & \frac{-MV_{dc}\cos(\psi)}{\sqrt{3}L_1} \end{bmatrix}, B_{32} = \begin{bmatrix} \frac{-1}{2L_2} & \frac{\sqrt{3}}{6L_2} \\ \frac{-\sqrt{3}}{6L_2} & \frac{-1}{2L_2} \end{bmatrix}, \\
b_1 &= \begin{bmatrix} -I_d^{inv} \\ I_q^{inv} \end{bmatrix}, b_2 = \begin{bmatrix} -V_d^c \\ V_q^c \end{bmatrix}, b_3 = \begin{bmatrix} -I_d^g \\ I_q^g \end{bmatrix},
\end{aligned} \tag{A.2}$$

$$A_{43} = \begin{bmatrix} \frac{-k_{i1}V_q^{pcc}}{2} & 0 \\ 0 & \frac{-k_{i3}V_q^{pcc}}{2} \end{bmatrix}, A_{53} = \begin{bmatrix} -k_{i2} - \frac{k_{p1}k_{i2}V_q^{pcc}}{2} & 0 \\ 0 & -k_{i4} - \frac{k_{p3}k_{i4}V_q^{pcc}}{2} \end{bmatrix}, A_{54} = \begin{bmatrix} k_{i2} & 0 \\ 0 & k_{i4} \end{bmatrix}. \tag{A.3}$$

$$\begin{aligned}
B_{41} &= \begin{bmatrix} \frac{-k_{i1}I_{qL}}{2} & \frac{-k_{i1}I_{dL}}{2} \\ \frac{-k_{i3}I_{dL}}{2} & \frac{k_{i3}I_{qL}}{2} \end{bmatrix}, B_{43} = \begin{bmatrix} k_{i1} & 0 \\ 0 & k_{i3} \end{bmatrix}, \\
B_{51} &= \begin{bmatrix} \frac{-k_{p1}k_{i1}I_{qL}}{2} & \frac{-k_{p1}k_{i1}I_{dL}}{2} \\ \frac{-k_{p3}k_{i3}I_{dL}}{2} & \frac{k_{p3}k_{i3}I_{qL}}{2} \end{bmatrix}, B_{53} = \begin{bmatrix} k_{p1}k_{i2} & 0 \\ 0 & k_{p3}k_{i4} \end{bmatrix}.
\end{aligned} \tag{A.4}$$

$$\begin{aligned}
A_{63} &= \frac{1}{T_d} \begin{bmatrix} -k_{p2} - \frac{k_{p1}k_{p2}V_q^{pcc}}{2} & \omega L \\ -\omega L & -k_{p4} - \frac{k_{p3}k_{p4}V_q^{pcc}}{2} \end{bmatrix}, A_{64} = \frac{1}{T_d} \begin{bmatrix} k_{p2} & 0 \\ 0 & k_{p4} \end{bmatrix}, A_{65} = \frac{1}{T_d} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \\
B_{61} &= \frac{1}{T_d} \begin{bmatrix} 1 - \frac{k_{p1}k_{p2}I_{qL}}{2} & -\frac{k_{p1}k_{p2}I_{dL}}{2} \\ -\frac{k_{p3}k_{p4}I_{dL}}{2} & 1 + \frac{k_{p3}k_{p4}I_{qL}}{2} \end{bmatrix}, A_{66} = -\frac{1}{T_d} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, B_{63} = \frac{1}{T_d} \begin{bmatrix} k_{p1}k_{p2} & 0 \\ 0 & k_{p3}k_{p4} \end{bmatrix}.
\end{aligned} \tag{A.5}$$

$$\begin{aligned}
A_{13}^L &= A_{13}T, A_{23}^L = A_{23}T, A_{31}^L = T^{-1}A_{31}, A_{32}^L = T^{-1}A_{32}, \\
A_{33}^L &= T^{-1}A_{33}T, B_{31}^L = T^{-1}B_{31}, b_3^L = T^{-1}b_3,
\end{aligned} \tag{A.6}$$

$$\text{where } T = \begin{bmatrix} \frac{1}{2} & -\frac{1}{2\sqrt{3}} \\ \frac{1}{2\sqrt{3}} & \frac{1}{2} \end{bmatrix}.$$

$$M = \begin{bmatrix} V_{dc}\cos(\psi) & -MV_{dc}\sin(\psi) \\ -V_{dc}\sin(\psi) & -MV_{dc}\cos(\psi) \end{bmatrix}. \quad (\text{A.7})$$

$$G_1 = \begin{bmatrix} R_g & \omega L_g \\ -\omega L_g & R_g \end{bmatrix}, G_2 = L_g. \quad (\text{A.8})$$

$$\left\{ \begin{array}{l} A_{3n}^c = A_{3n}^L + B_{3n}^L(I - G_2 B_{31}^L)^{-1} G_2 A_{3n}^L, n \in 1, 2, \\ A_{33}^c = A_{33}^L + B_{31}^L(I - G_2 B_{31}^L)^{-1} (G_1 + G_2 A_{33}^L), \\ A_{n1}^c = B_{n1}(I - G_2 B_{31}^L)^{-1} G_2 A_{31}^L, n \in 4, 5, 6, \\ A_{n2}^c = B_{n1}(I - G_2 B_{31}^L)^{-1} G_2 A_{32}^L, n \in 4, 5, 6, \\ A_{n3}^c = A_{n3} + B_{n1}(I - G_2 B_{31}^L)^{-1} (G_1 + G_2 A_{33}^L), n \in 4, 5, 6. \end{array} \right. \quad (\text{A.9})$$

$$\left\{ \begin{array}{l} B_{31}^c = B_{31}^L(I - G_2 B_{31}^L)^{-1}, \\ B_{n1}^c = B_{n1}(I - G_2 B_{31}^L)^{-1} G_2 A_{31}^L, n \in 4, 5, 6 \\ b_3^c = b_3^L + B_{31}^L(I - G_2 B_{31}^L)^{-1} G_2 b_3^L, \\ b_n^c = B_{n1}(I - G_2 B_{31}^L)^{-1}, n \in 4, 5, 6. \end{array} \right. \quad (\text{A.10})$$

Enter the content for Appendix A in the appendixA.tex file. If you do not have an Appendix A, see comments in the etdrtemplate.tex file for instructions on how to remove this page.

A.2 Stability Criteria Formulation

For the signal flow graph of the inverter in Fig. 2(b), the loop gains and non-touching loop gains are given as,

$$\begin{aligned}
 \text{loop 1, } L1 &: \frac{-G_p G_i V_o}{s^3 L_1 L_2 C} \\
 \text{Loop 2, } L2 &: \frac{-G_i}{s^3 L_1 L_2 C} \\
 \text{Loop 3, } L3 &: \frac{-1}{s^2 L_2 C} \\
 \text{Loop 4, } L4 &: \frac{-G_p G_i R_g I_o}{s^3 L_1 L_2 C} \\
 \text{Loop 5, } L5 &: \frac{-G_p G_i L_g I_o}{s^2 L_1 L_2 C} \\
 \text{Loop 6, } L6 &: \frac{-1}{s^2 L_1 C} \\
 \text{Loop 7, } L7 &: \frac{-L_g}{L_2} \\
 \text{Loop 8, } L8 &: \frac{-R_g}{s L_2} \\
 \text{Loop 9, } L9 &: \frac{L_g}{s^2 L_1 L_2 C} \\
 \text{Loop 10, } L10 &: \frac{R_g}{s^3 L_1 L_2 C}
 \end{aligned} \tag{A.11}$$

Two non-touching loops:

$$\begin{aligned}
 \text{Loop 6, 7, } DL1 &= L6 \times L7 = \frac{L_g}{s^2 L_1 L_2 C} \\
 \text{Loop 6, 8, } DL2 &= L6 \times L8 = \frac{R_g}{s^3 L_1 L_2 C}
 \end{aligned} \tag{A.12}$$

Therefore, the transfer function is given in (B3).

$$H_1 = \frac{G_p G_i}{s^3(L_2 + L_g)L_1C + s^2L_1CR_g + s(L_1 + L_2 + G_pG_iL_gI_o) + G_i + G_p(V_o + R_gI_o)} \quad (\text{A.13})$$

For $G_p = (sk_{p1} + k_{i1})/s$ and $G_i = (sk_{p2} + k_{i2})/s$, the transfer function in (A.1) can be represented as (A.2).

$$H_2 = \frac{(sk_{p1} + k_{i1})(sk_{p2} + k_{i2})}{a_5s^5 + a_4s^4 + a_3s^3 + a_2s^2 + a_1s^1 + a_0s^0} \quad (\text{A.14})$$

where $a_5 = \text{Coefficient of } s^5 = (L_2 + L_g)L_1C$

$a_4 = \text{Coefficient of } s^4 = R_gL_1C$

$a_3 = \text{Coefficient of } s^3 = L_1 + L_2 + k_{p1}k_{p2}L_gI_o$

$a_2 = \text{Coefficient of } s^2 = k_{p2} + (k_{p1}k_{i2} + k_{p2}k_{i1})L_gI_o + k_{p1}k_{p2}(V_o + R_gI_o)$

$a_1 = \text{Coefficient of } s^1 = k_{i2} + (k_{i1}k_{i2}L_gI_o + (k_{p1}k_{i2} + k_{p2}k_{i1})(V_o + R_gI_o))$

$a_0 = \text{Coefficient of } s^0 = +k_{i1}k_{i2}(V_o + R_gI_o)$

The characteristic equation of (A.2) is written as,

$$a_5s^5 + a_4s^4 + a_3s^3 + a_2s^2 + a_1s^1 + a_0s^0 = 0 \quad (\text{A.15})$$

Using the Routh–Hurwitz rule, $-a_5a_2 + a_4a_3 > 0$ The inequality can be written as

$$(L_2 + L_g)(k_{p2} + (k_{p1}k_{i2} + k_{p2}k_{i1})L_gI_o + k_{p1}k_{p2}(V_o + R_gI_o)) > R_g(L_1 + L_2 + k_{p1}k_{p2}L_gI_o) \quad (\text{A.16})$$

which can be rewritten as

$$\frac{(L_1 + L_2)R_g}{(L_2 + L_g)} > (k_{p2} + (k_{p1}k_{i2} + k_{p2}k_{i1})L_gI_o + k_{p1}k_{p2}(V_o + R_gI_o)) - \frac{k_{p1}k_{p2}L_gI_o}{(L_2 + L_g)} \quad (\text{A.17})$$

If we assume

$$G_c = M_c = k_{p2} + (k_{p1}k_{i2} + k_{p2}k_{i1})L_gI_o + k_{p1}k_{p2}(V_o + R_gI_o) - \frac{k_{p1}k_{p2}L_gI_o}{L_2 + L_g} \quad (\text{A.18})$$

Therefore, the stability criterion can be formulated as follows:

$$M_c < R_g \frac{(L_1 + L_2)}{(L_2 + L_g)} \quad (\text{A.19})$$

Notice M_c can be rewritten as

$$M_c = k_{p2} + (k_{p1}k_{i2} + k_{p2}k_{i1})L_gI_o + k_{p1}k_{p2}(V_o + R_gI_o) - \frac{L_gI_o}{L_2 + L_g} \quad (\text{A.20})$$

Since $0 < R_g < 1$ and $0 < L_g/((L_2 + L_g) < 1)$, therefore results of the last two terms, i.e., I_oR_g and $I_oL_g/((L_2 + L_g)$, which have different signs, is much less than, V_o . Therefore, M_c can be approximately written as

$$M_c = k_{p2} + (k_{p1}k_{i2} + k_{p2}k_{i1})L_gI_o + k_{p1}k_{p2}(V_o) \quad (\text{A.21})$$

Appendix B

Analytical Method for Real-Time Grid Parameter Estimation

B.1 Analytical Method for Grid Parameters Estimation

In this appendix, the formulation of an analytical model for real-time grid parameter estimation is presented. The measured voltage at PCC is given by

$$v = V_m \sin(2\pi\omega t + \psi) + \hat{V}_m \sin(2\pi\hat{\omega}t + \hat{\psi}_v) \quad (\text{B.1})$$

The fundamental frequency of the grid voltage is $60Hz$, i.e., $\omega = 60Hz$. The frequency of the injected signal has to be chosen such that grid voltage does not have any component at that frequency.

Multiply (B.1) by $\sin 2\pi\hat{\omega}t$ results

$$x_v = v \sin 2\pi\hat{\omega}t = (V_m \sin(2\pi\omega t + \psi) + \hat{V}_m \sin(2\pi\hat{\omega}t + \hat{\psi}_v)) \sin 2\pi\hat{\omega}t \quad (\text{B.2})$$

Equation (B.2) can be written as,

$$x_v = V_m \sin(2\pi\omega t + \psi) \sin 2\pi\hat{\omega}t + \hat{V}_m \sin(2\pi\hat{\omega}t + \hat{\psi}_v) \sin 2\pi\hat{\omega}t \quad (\text{B.3})$$

Applying the trigonometric identities of (B.4) and after simplifications B.3 can be written as B.5

$$\sin a \sin b = \frac{1}{2} [\cos(a - b) - \cos(a + b)] \quad (\text{B.4})$$

$$x_v = \frac{Vm}{2} [\cos(\omega - \hat{\omega})t + \psi + \cos(\omega + \hat{\omega})t + \hat{\psi}] + \frac{\hat{V}_m}{2} [\cos \hat{\psi} - \cos(2\hat{\omega}t + \hat{\psi}_v)] \quad (\text{B.5})$$

Notice, the signal x_v in (B.5) consists of both dc and ac parts. The dc parts, i.e., zero frequency components, can be achieved using a low-pass filter. After passing the signal x through a low-pass filter, $LPF = 1/(\tau s + 1)$, the dc part can be obtained as presented in (B.6)

$$m_v = \frac{\hat{V}_m}{2} [\cos \hat{\psi}_v] \quad (\text{B.6})$$

For the measured current at PCC,

$$i = I_m \sin(2\pi\omega t + \psi) + \hat{I}_m \sin(2\pi\hat{\omega}t + \hat{\psi}_i) \quad (\text{B.7})$$

The fundamental frequency of the grid current is $60Hz$, i.e., $\omega = 60Hz$.

$$x_i = i \sin 2\pi\hat{\omega}t = (I_m \sin(2\pi\omega t + \psi) + \hat{I}_m \sin(2\pi\hat{\omega}t + \hat{\psi}_i)) \sin 2\pi\hat{\omega}t \quad (\text{B.8})$$

Equation (B.8) can be written as,

$$x_i = I_m \sin(2\pi\omega t + \psi) \sin 2\pi\hat{\omega}t + \hat{I}_m \sin(2\pi\hat{\omega}t + \hat{\psi}_i) \sin 2\pi\hat{\omega}t \quad (\text{B.9})$$

Applying the trigonometric identities of (B.4) and after simplifications (B.9) can be written

as (B.10)

$$x_i = \frac{Vm}{2}[\cos(\omega - \hat{\omega})t + \psi + \cos(\omega + \hat{\omega})t + \hat{\psi}] + \frac{\hat{V}_m}{2}[\cos \hat{\psi} - \cos(2\hat{\omega}t + \hat{\psi}_i)] \quad (\text{B.10})$$

Notice, the signal x_i in (B.10) consists of both dc and ac parts. The dc parts can be separated using a low-pass filter. After passing the signal x through a low-pass filter, $LPF = 1/(\tau s + 1)$, the dc part can be obtained as presented in (B.11)

$$m_i = \frac{\hat{V}_m}{2}[\cos \hat{\psi}_i] \quad (\text{B.11})$$

Then, by injecting two signals of low-frequency, $\hat{\omega}$, separated by an angle difference of 90° . The voltage and current signal for this low-frequency signal injection can be represented in Table B.1.

Table B.1: *Voltage and current signal multiplication for analytical method formulation*

	Voltage signal	Current signal
Case 1	$m'_v = \frac{\hat{V}_m'}{2}[\cos \hat{\psi}'_v]$	$m'_i = \frac{\hat{I}_m'}{2}[\cos \hat{\psi}'_i]$
Case 2	$m''_v = \frac{\hat{V}_m''}{2}[\cos \hat{\psi}''_v]$	$m''_i = \frac{\hat{I}_m''}{2}[\cos \hat{\psi}''_i]$

Here, $\hat{\psi}''_v$ and $\hat{\psi}'_v$ are separated by 90° , i.e., $\hat{\psi}''_v = \hat{\psi}'_v - \pi/2$ and also, $\hat{\psi}''_i = \hat{\psi}'_i - \pi/2$. Hence, the voltage signal of case 2 becomes,

$$m''_v = \frac{\hat{V}_m''}{2} \sin(\hat{\psi}'_v - \pi/2) = \frac{\hat{V}_m''}{2} \sin \hat{\psi}'_v \quad (\text{B.12})$$

Similarly, the current signal can be written as,

$$m''_i = \frac{\hat{I}_m''}{2} \sin(\hat{\psi}'_i - \pi/2) = \frac{\hat{I}_m''}{2} \sin \hat{\psi}'_i \quad (\text{B.13})$$

Squaring and adding the voltage signal for case 1 and case 2 can be represented as,

$$v_m'' = \sqrt{4[(m_v')^2 + (m_v'')^2]} \quad (\text{B.14})$$

Squaring and adding the current signal for case 1 and case 2 can be represented as,

$$i_m'' = \sqrt{4[(m_i')^2 + (m_i'')^2]} \quad (\text{B.15})$$

The magnitude of the Thevenin impedance,

$$|Z| = \frac{m_v''}{m_i''} \quad (\text{B.16})$$

The angle of the Thevenin impedance can be calculated using (B.16),

$$\theta_z = \theta_v' - \theta_i' - \theta_v'' - \theta_i'' \quad (\text{B.17})$$

θ_v' can be obtained using (B.18)

$$\theta_v' = \cos^{-1}\left(\frac{2m_v'}{v_m''}\right) \quad (\text{B.18})$$

θ_i'' can be obtained using (B.19)

$$\theta_i' = \cos^{-1}\left(\frac{2m_i'}{i_m''}\right) \quad (\text{B.19})$$

B.2 Analytical Method Veification

This section focuses on the verification of the formulated analytical method using a Control Hardware in the Loop (CHIL) simulation setup. The integration of the Typhoon HIL system with real control hardware, such as microcontrollers, digital signal processors (DSP), or PLCs, is essential for implementing CHIL. In this study, the analytical grid parameter estimation algorithm is programmed using the TI LAUNCH XL-F28379 DSP module. Fig. C.1 represents the grid-connected inverter system designed using a typhoon HIL 602 sim-

Table B.2: *Results obtained from CHIL using analytical grid parameter estimation method*

Actual	Calculated
$ Z = 0.019$	$ Z = 0.017$
$\angle Z = 58.5^\circ$	$\angle Z = 57^\circ$
$R_g = 0.01mH$	$R_g = 0.009mH$
$L_g = 16mH$	$L_g = 14mH$

ulation environment. The developed analytical method for grid parameter estimation is implemented on the TI DSP board, as shown in Fig. C.8 To successfully execute the algorithm, the DSP board requires measurements from various sources, including the DC-bus voltage, line-to-line voltages, and line currents at the point of common coupling (PCC), as depicted in Fig. C.1. The DSP board generates six PWM reference signals (r_a, r_b, r_c) to operate the inverter model in Typhoon HIL. It is important to note that the input pins on the selected DSP board can only measure signals ranging from 0 to 3 V. Hence, a calibration process is necessary to convert the peak values of the input signals to match the required voltage range of the DSP board. By utilizing the CHIL simulation setup, the formulated analytical method can be thoroughly tested and verified in a realistic environment. The integration of real control hardware enables real-time feedback and control signal generation, ensuring an accurate assessment of the algorithm's performance and functionality. The performance of the analytical method for the grid parameter estimation is shown in Table B.2. The discrepancy in the estimated impedance magnitude and angles using the developed method is 10.52% and 2.5% respectively.

Appendix C

Self-Protective Inverters Testbed Development

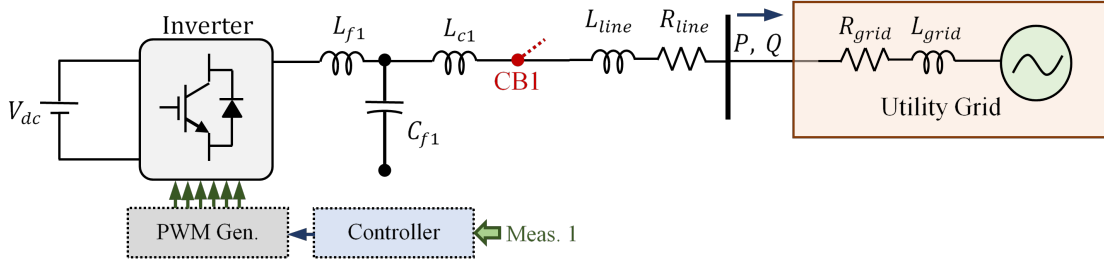


Figure C.1: Schematic diagram of the control hardware-in-the-loop testbed for a self-protective inverter.

C.1 Hardware Development for Self-Protective Algorithm Verification

In this section, a brief description of the hardware development used to test the performance of the self-protective algorithm developed in this dissertation is provided. Fig. C.1 illustrates the schematic diagram of the test-bed that was constructed for this purpose. The test bed consists of various components, which are crucial for evaluating the effectiveness of the self-protective algorithm. Firstly, a three-phase voltage source inverter is employed and

connected to the power grid. This inverter is equipped with a DC power supply, an LCL filter setup, a measurement board, a circuit breaker, and a controller. These elements work in conjunction to facilitate the operation and assessment of the algorithm's performance. The DC supply ensures a stable and reliable power source for the inverter, while the LCL filter setup is responsible for reducing any unwanted harmonics or disturbances in the system. The measurement board plays a critical role in acquiring essential data and monitoring various parameters during the testing phase. Moreover, the circuit breaker acts as a means to establish or break the connection between the inverter and the power grid. Importantly, the testbed allows for the separation of the power grid from the inverter through the circuit breaker. This feature enables controlled experimentation and analysis by selectively isolating the inverter from the grid when necessary. By employing this well-designed hardware setup, the performance of the self-protective algorithm can be thoroughly investigated and evaluated.

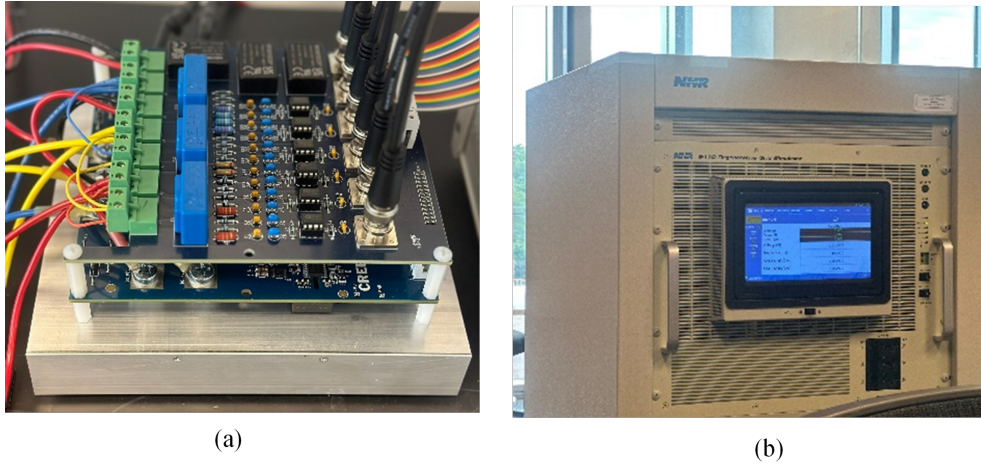


Figure C.2: *Inverters and grid-simulator used for the developed microgrid; (a) 5 kVA SiC inverter, (b) 30 kVA grid-simulator.*

Fig.C.2 (a) displays the 5 KVA SiC inverter that was utilized to verify the effectiveness of the self-protective algorithm. This inverter comprises a commercial Wolfspeed CREE CGD15FB45P1; 1200V six-channel SiC gate driver board, and a Wolfspeed *CCS020M12CM2*; 1200V, 20A SiC six-pack module. To ensure optimal cooling and serve as the foundation of the inverter, a high-efficiency heat sink is securely attached to the SiC module. Addition-

ally, a laboratory-developed measurement board is integrated with the gate driver board, switches, and heat sink, featuring a built-in interface specifically designed for the controllers. It is important to note that a separate measurement board, as shown in Fig. C.4 (a), is essential for this particular setup. In order to replicate the behavior of the power grid, a 30 NHR 9410 grid simulator, depicted in Fig. C.2 (b), was employed.

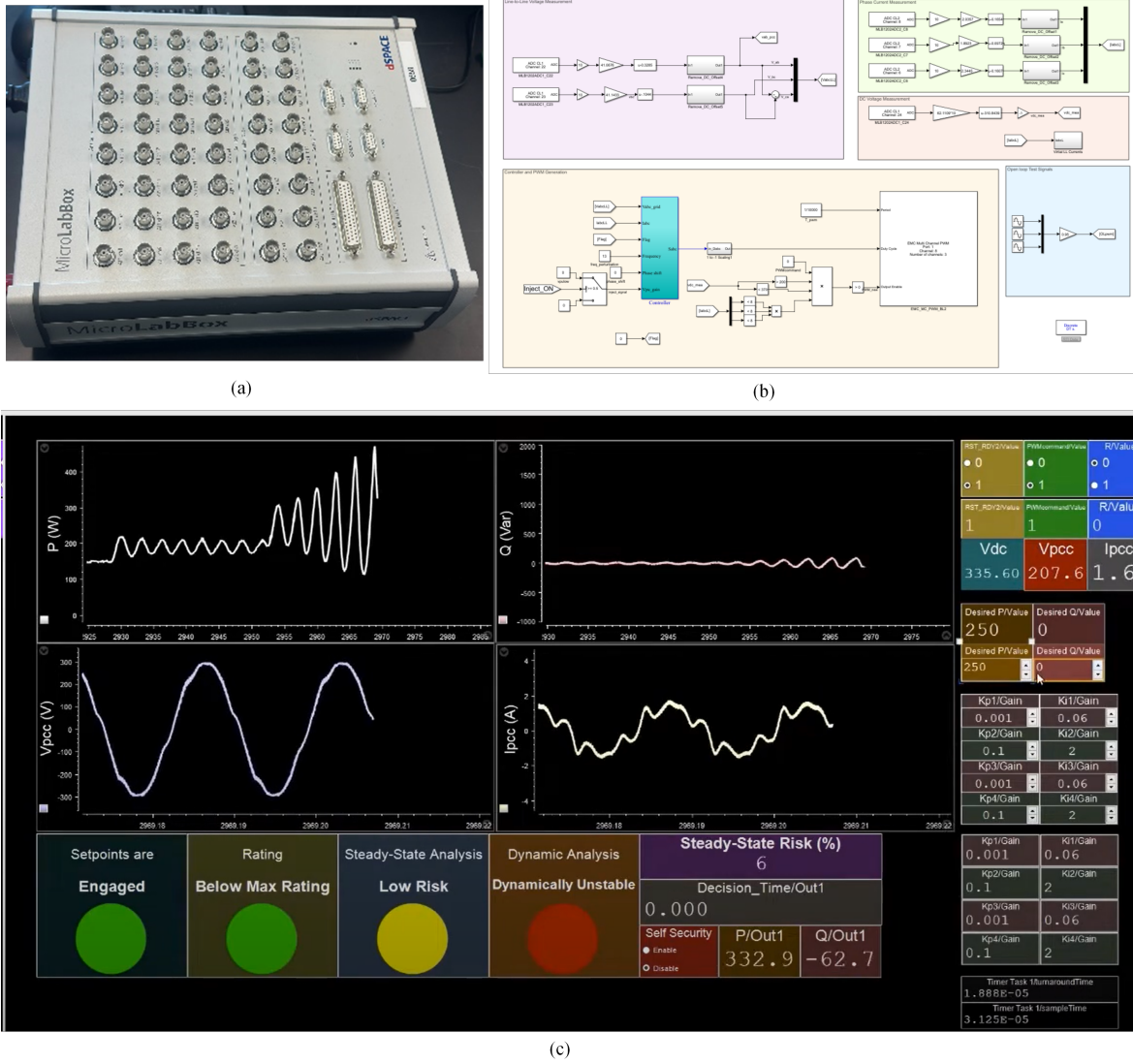


Figure C.3: (a) The dSPACE MicroLabBox for controller implementation, (b) a high-level schematic of the controller in MATLAB-Simulink, and (c) control panel of the Control Desk software.

This grid simulator offers the capability to configure three-phase line-line voltage signals, supply and absorb active and reactive power, and can be conveniently operated either

through the control panel or via a computer. The simulator serves as a reliable representation of the power grid, enabling accurate testing and evaluation of the self-protective algorithm.

To control the inverters, separate dSPACE MicrolabBox 1202 modules, as depicted in Fig. C.3(a), are utilized. The control algorithms are developed within the MATLAB-Simulink environment and then programmed into the dSPACE controllers. Fig. C.3(b) presents a high-level schematic representation of the inverter controller that is created using MATLAB-Simulink. For convenient access to control operations and processed data, the ControlDesk software is employed, which establishes communication with the dSPACE modules through an Ethernet connection. This software allows for effective monitoring of the control system. Additionally, Fig. C.3(c) showcases the control panel specifically designed for the self-protective algorithm of the inverters. Equipped with digital and analog input/output channels, the dSPACE controllers efficiently handle the measurement signals. These signals are initially converted into digital format through the A/D (analog-to-digital) input, after which they undergo digital filtering within the controller. The resulting Pulse Width Modulation (PWM) signals are then transmitted to the hardware via the digital output port of the controllers. It is important to note that the measurement board, gate-driver board, and controller must have a common ground to ensure accurate measurement and control. To minimize electromagnetic interference, electromagnetic shields are employed to protect the ribbons carrying the PWM signals.

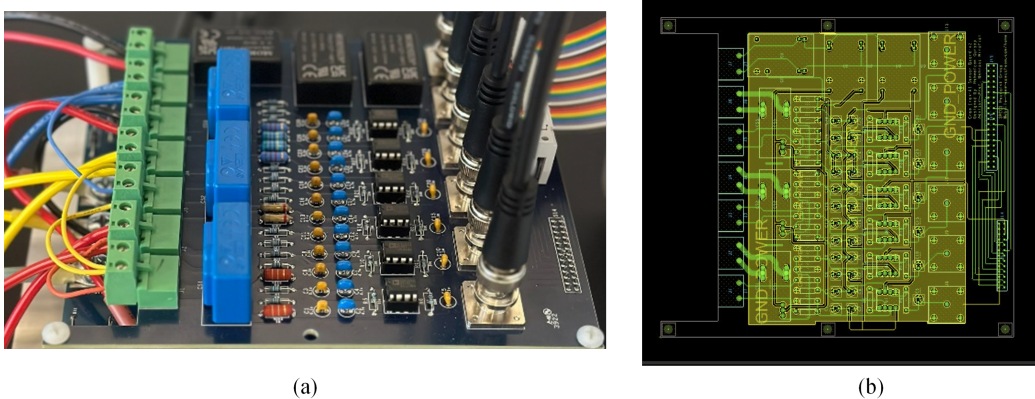


Figure C.4: *Interface between circuit and the controller; (a) Voltage and current measurement board, and (b) schematic of the measurement board.*

As shown in Fig. C.4, the measurement board forms the interface between the circuit and the controller. The board in Fig. C.4 has three AC voltage sensors, one DC voltage sensor, and three AC current sensors with a maximum measurement capacity of up to 340 V, 400 V, and 30 A. Here, the voltages are reduced by resistor based voltage divider followed by the operational amplifiers (OpAmps). The currents are directly passed through the sensors, converted to small current signals, and then passed through the OpAmps. The purposes of the OpAmps are to control the output of the measurement board within the permissible limit of the dSPACE controller and to provide stable output. Since the output voltages are digitally filtered inside the controller, no external filter is needed in this board. As shown in Fig. C.4, the width of current paths through the current sensors must be sufficient to allow 30 A of current. The board also consists of an interface to the controller where PWM and other control signals are sent. Therefore, a rectangular surface is used for ground to reduce the effect of external noises due to the high switching of PWM signals. In addition, to nullify the EMI effect between two crossing traces through the upper and lower layer of the board, all crossing traces are drawn perpendicular to each other.

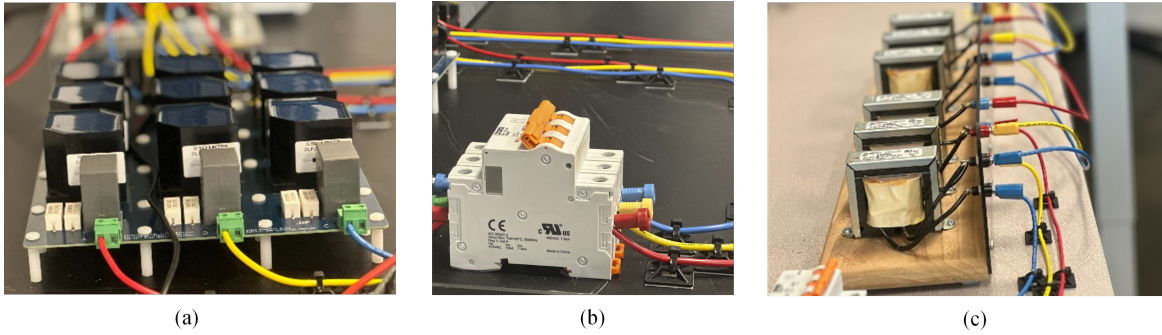


Figure C.5: *Circuit components of the developed testbed for self-security algorithm implementation. (a) LCL filters board (b) Circuit breaker (c) Inserted inductance between PCC and grid simulator.*

Fig. C.5 (a)-(c) represents various components essential to the setup, including the LCL filter board, the circuit breaker, and an inserted inductance between the Point of Common Coupling (PCC) and the grid. The LCL filter plays a crucial role in filtering out the fundamental components from the output voltages of the inverters. It ensures that only the desired frequencies pass through while attenuating unwanted harmonics. The filter board

is specifically tested and designed to sustain current up to 20 A within the 5-20 kHz frequency range. Metal Oxide Varistors (MOVs) are connected to each line-line voltage output to protect the inverters from overvoltage occurrences. These MOVs act as surge protectors, safeguarding the inverters from potential voltage spikes. To effectively isolate all the inverters and the grid, 20 A circuit breakers are incorporated into the setup, as depicted in Fig. C.5 (b). These circuit breakers serve as switching devices, allowing for controlled separation and reconnection of the inverters from the grid. Furthermore, constant DC power is provided to the inverters using DC power supplies. A Magna-Power DC power supply with ratings of 0-600 V, 0-6 A, and 0-6 kW is employed in the developed testbed. It is essential to set up appropriate voltage and current limits on the DC power supply before conducting any experiments to ensure safe operation. To monitor the waveforms and acquire accurate measurements, a WaveRunner 64Xi-A 600 MHz oscilloscope is utilized. Voltage measurements are obtained using the Teledyne Lecroy ADP300 high-voltage differential probe, while the CP030 current probe facilitates current measurements. This oscilloscope also allows capturing data at a speed of 10 GB/s across four channels. Since the inverter generates three-phase voltage signals, it is crucial to ensure that the phase sequence of the output voltages matches that of the grid before closing the circuit breakers. During the development of the testbed, this verification is performed by observing two line-line voltages for each of the two inverters using the oscilloscope. If any discrepancies are detected, the phase sequence can be easily adjusted from the controller without requiring any changes in the hardware setup.

C.2 CHIL Testbed Development for Self-Protective Algorithm Verification

This section provides a brief description of the development of the Control Hardware in the Loop (CHIL) testbed, specifically designed for evaluating the performance of the self-protective algorithm developed in this dissertation. Fig. C.6 presents the schematic diagram of the CHIL testbed, which incorporates a real-time simulator (Typhoon HIL), an

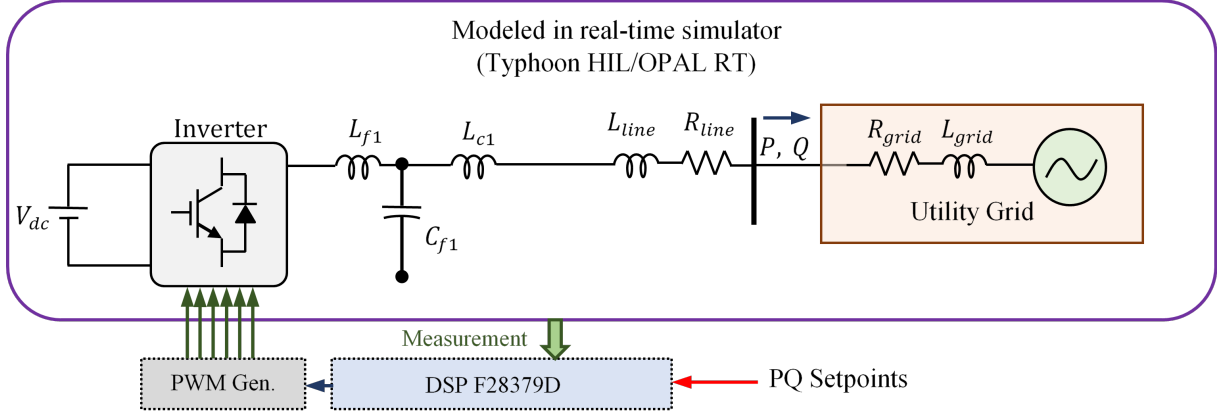


Figure C.6: Schematic diagram of the developed testbed for self-protective inverter.

HIL TI Launchpad Interface, and a TI F28379D LaunchPad to facilitate the testing the self-protective algorithm. Fig. C.7 (a)-(c) represents various components of CHIL setup, including Typhoon HIL 402, an HIL TI Launchpad Interface, and TI F28379D LaunchPad. The schematic diagram shown in Fig. C.6 modeled in Typhoon HIL 402. The self-security algorithm is programmed in a DSP (Digital Signal Processor) board (C2000- TI LAUNCH XL-F28379). The DSP requires measurement from the DC-bus voltage (V_{dc}), line-to-line voltages (V_{ab}^{pcc} , V_{bc}^{pcc} , V_{ca}^{pcc}) and line currents (I_a^{pcc} , I_b^{pcc} , I_c^{pcc}) at the point of common coupling (PCC) see Fig. C.6. The DAC generates two PWM reference signals r_a , and r_b for PWM modulator of the real-time simulator. Third PWM reference signal, r_c , is to be calculated based on $r_c = -(r_a + r_b)$ in the Typhoon HIL real-time simulator. Herein, r_a , r_b and r_c represents the reference signals for phase a, phase b, and phase c respectively.

The six PWM signals can be generated using internal modulator of the real-time simulator using r_a , r_b , and r_c . The DSP is also programmed to receive the P and Q setpoints externally from the real-time simulator. In summary, two DAC pins and, nine ADC pins are used to implement the self-security algorithm. The utilized pins are shown in Fig. C.7 (c)-J3, and J7. Notice, the input pins on the selected DSP board can only measures signal between 0 to 3 V. Therefore, calibration is needed to convert the peak values of the input signals to the required voltage range of the DSP board.

A set of equations have been derived for calibration. These equations will ensure that

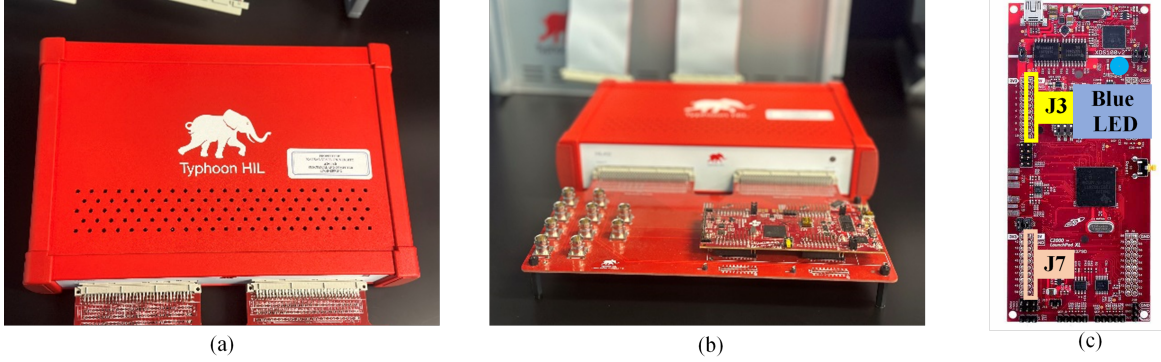


Figure C.7: (a) *Typhoon HIL 402* (b) *Interface between HIL and the DSP controller.* (c) *TI F28379D LaunchPad*

the DSP voltage will stay in the range change between $[0.2 \text{ V}, 3 \text{ V}]$ or $[0 \text{ V}, 3 \text{ V}]$. For AC measured signal calibrated range is considered $[0.2 \text{ V}, 3 \text{ V}]$ instead of $[0 \text{ V}, 3 \text{ V}]$. For additional security, user may add limiters to the output channels of the real-time simulator to ensure analog signals do not exceed 3 V. The measured values must stay within the specified ranges in Table C.2. The DSP board can be powered from a USB or 5 V external supply. Table C.2 represents the analog input to the DSP with corresponding pin numbers and maximum ranges. The measured values must stay within the specified ranges in Table C.2. The DSP board can be powered from a USB or 5 V external supply. Table C.2 represents the analog input to the DSP with corresponding pin numbers and maximum ranges.

The ground (GND) pin numbers for J3 and J7 are 22 and 62, respectively. Table C.2 represents the analog output from the DSP with corresponding pin numbers and maximum ranges. The reference signals (r_a, r_b) generated at DACA and DACB have a DC offset and are also scaled down to appropriate values. After taking these inputs in Typhoon HIL, first, the DC offset needs to be removed using any technique for removing DC offset, and then the signals need to be multiplied by 2.5 to obtain the actual reference signals (r_a, r_b) that are used for calculation of $r_c = -(r_a + r_b)$. The ground (GND) pins for DACA and DACB are 22 and 62, respectively. Fig. C.7 represents the testbed developed for validating the self-security algorithm using the TI DSP board.

The self-security algorithm takes approximately 35-40 seconds to examine the incoming setpoints and assess their validity carefully. To provide a clear indication of the status of the

Table C.1: *DSP F28379D analog inputs employed for self-protective algorithm implementation*

Measured Signals	Voltage calibration for DSP ports		DSP F28379D Analog Input	Pin Number (J3)	Pin Number (J7)	Maximum Voltage (V)
	Allowable Measurement Range (Peak)	Calibrated Range (V)				
V_{dc}	[0V, 1200V]	[0, 3]	ADCIN14	23	-	3
V_{ab}^{pcc}	$[-500\sqrt{2}V, 500\sqrt{2}V]$	[0, 3]	ADCINA2	29	-	3
V_{bc}^{pcc}	$[-500\sqrt{2}V, 500\sqrt{2}V]$	[0, 3]	ADCINB2	28	-	3
V_{ca}^{pcc}	$[-500\sqrt{2}V, 500\sqrt{2}V]$	[0, 3]	ADCINC2	27	-	3
I_a^{pcc}	$[-300\sqrt{2}A, 300\sqrt{2}A]$	[0, 3]	ADCINA3	26	-	3
I_b^{pcc}	$[-300\sqrt{2}A, 300\sqrt{2}A]$	[0, 3]	ADCINB3	25	-	3
I_c^{pcc}	$[-300\sqrt{2}A, 300\sqrt{2}A]$	[0, 3]	ADCINC3	24	-	3
P^*	[0kW, 30kW]	[0, 3]	ADCIN15	-	63	3
Q^*	[0 kW, 30 kVar]	[0, 3]	ADCINC5	-	64	3

PQ setpoints, a blue LED indicator, as shown in Fig. C.7, is employed. When the new PQ setpoints are commanded, the self-security algorithm actively checks the setpoints. When the setpoints are predicted safe by the algorithm, the blue LED illuminates, indicating safe operation. Conversely, if the PQ setpoints are predicted to be potentially malicious or unsafe, the blue LED is turned off, indicating that the operation may lead to unsafe conditions. In such cases, the algorithm continues its operation based on the previously accepted safe setpoints, ensuring the system's security. This visual representation of the PQ

Table C.2: *DSP F28379D digital outputs employed for self-protective algorithm implementation*

PWM Reference Signal	DSP Analog Output	Pin Number (J3)	Pin Number (J7)	Scaling factor in real-time simulator	Maximum Voltage (V)
r_a	DACA	30	-	2.5	3
r_b	DACB	-	70	2.5	3

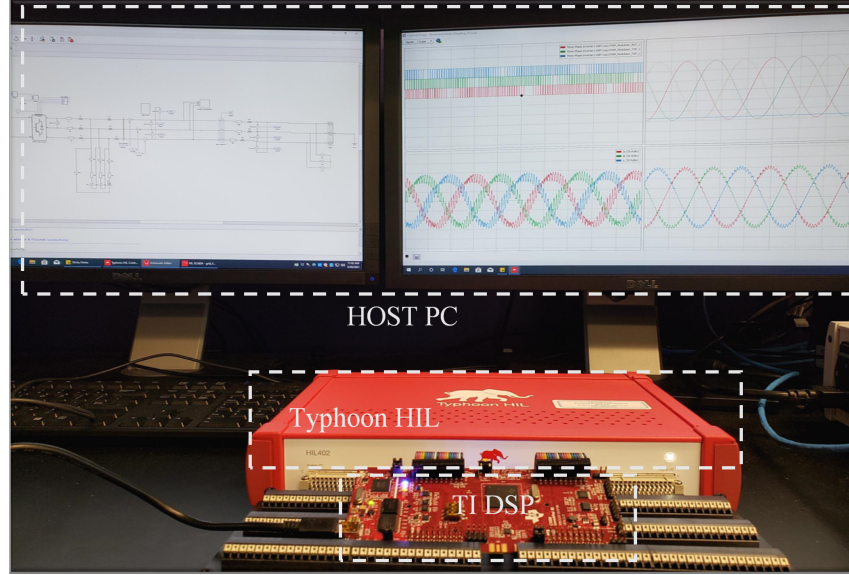


Figure C.8: *Validation of the self-security algorithm employing the real-time simulator - Typhoon HIL.*

setpoint validity through the blue LED indicator enables easy monitoring and verification of the algorithm's functionality. It allows operators and users to quickly assess whether the newly commanded setpoints have been deemed safe or if they pose potential risks.