Digital Twin for Self-Security of Smart Inverters

Tareq Hossen, *Student Member, IEEE*, Mehmetcan Gursoy, *Student Member, IEEE*, and Behrooz Mirafzal, *Senior Member, IEEE*

***Abstract* — Smart inverters connected to a communication network are susceptible to man-in-the-middle attacks. In this paper, a self-security approach is implemented using the digital twin concept for smart inverters. The digital twin is formed using the inverter's normal operating region and the inverter's dynamic model. Then, the incoming setpoints are autonomously examined using the digital twin, and only the safe setpoints are engaged to the inverter's local controller. This paper demonstrates how the inverter's normal operating region and dynamic model are formed. In particular, the normal operation region is experimentally verified by changing the P and Q setpoints engaged to the local controller, using a laboratory setup including a three-phase 3-kVA SiC-MOSFET inverter and a 12-kW NHR 9410 regenerative power grid emulator. The results demonstrate that the self-security technique can potentially protect inverters from man-in-the-middle attacks by examining the incoming commands (new setpoints) using the inverter's digital twin before engaging the setpoints to the local controller.**

***Index Terms*— Smart inverters, cyber-physical devices, self-security, reference model, digital twin.**

I. INTRODUCTION

With the advancement of internet and communication technologies, the power network is emerging to the next generation. The next generation power network allows physical power network to interact and exchange information autonomously through a cyber network. Smart inverters can be performed as controllable interfaces between the physical devices and the cyber networks to make proactive and autonomous decisions based on the two-way communications. Communication enabled inverters can perform grid-supporting functionalities such as voltage regulation and harmonic compensation and also the grid-forming autonomous features like black-start and networked microgrid operation [1]-[3]. Recent investigation demonstrates that as a part of a cyber-physical system smart inverter can be programmed with cooperative strategies to overcome different instability issues. These advanced and autonomous features of smart inverters allow high penetration of renewable sources to power systems and ensure stable and safe operation of modern power grids [1], [4]-[7].

Although, the high penetration of renewable energy sources and new cyber-physical structures have numerous benefits but these introduce new reliability, stability, and security risks in the power grid [7]-[10]. Local measurements data, system information, and supervisory commands of power setpoints need to be exchanged between the physical device and common cyber network. The smart inverter connected to a cyber network can be in danger of erroneous data communication, operator error, or cyber-attack. With the increased number of smart inverters sharing the same communication link the risk of cyberattacks and erroneous operations increases, that may have severe impact on the power grids [7]. Specially, the low inertia units, such as the PV and the wind farm, which is more impactful on the stability of the grid, are more prone to the cyber-attacks. Any abnormal operation of a single inverter can cause sequential trips of multiple inverters, destruction of equipment, blackout of power system, and thus, high economic losses [11]-[12]. Therefore, cyberattack detection and prevention play an important role in avoiding potential hazardous events in the power network.

Several studies have been carried out to prevent the cyberattack and detect smart inverter anomalies. These researches can be classified into data-driven approaches and model-based approaches [12]-[13]. In data-driven approaches, a machine-learning-based heuristics algorithm is used to develop the model [13]-[16]. On the other hand, the model-based technique compares the measured values with a time-dependent threshold to detect the anomalies [13], [17]-[18]. The goal of this technique is to provide system-level security. Recently, model-based self-security is proposed and experimentally tested [19]. In [12], a model-based cyberattack detection filter is developed using a mathematical model where the inverter's normal operating region is defined by a trajectory within a bounded area with a constant radius, and abnormal operation is determined when the trajectory is outside of the bounded area. On the other hand, a model-based adaptive control is developed in [20] to ensure the synchronization of multiple grid-forming converters during cyberattacks.

This work presents a knowledge-based self-security algorithm to assess the incoming power setpoints, P and Q, and decide whether the setpoints are harmful before engaging to the inverter's local controller. The assessment is based on evaluating the inverter's linear operating region by a digital twin of the inverter. Any setpoints beyond the inverter linear operation region can cause non-linear behavior like over-modulation, which can also lead to substantial pulse dropping. As a consequence of pulse dropping, injected harmonics to the grid can exceed the IEEE 591 standard limits [24]. Notice, the injection of excessive harmonic components to the grid causes system instability.

In addition to this introduction, the paper contains four more sections. Section II presents the system description and self-security concept. Section III elaborates on the proposed self-security approach towards the digital twinning of the smart inverter. Section IV discusses on the device level self-security algorithm. Section V provides experimental results and Section VI summarizes the findings of this work.

This material is based upon work supported by the Department of Energy, Office of Energy Efficiency and Renewable Energy (EERE), Solar Energy Technologies Office, under Award Number DE-EE0008767.

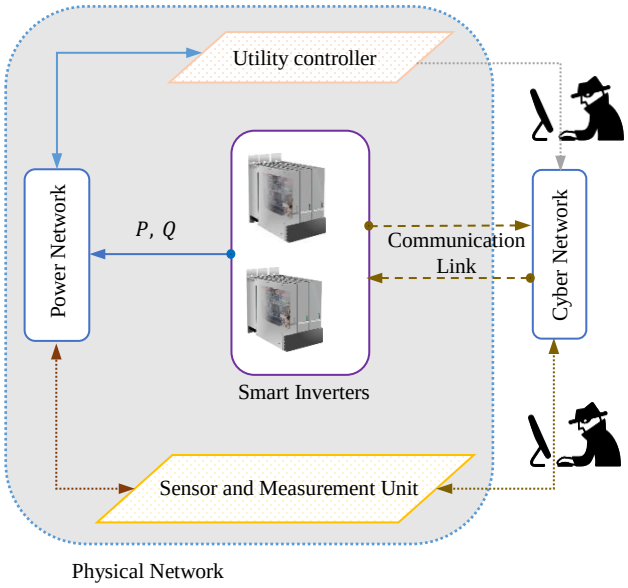

Fig. 1. Smart inverters connected to the power grid and possible cyberattack scenarios in a cyber-physical system.

II. System Description

In this section, the grid-interactive inverter based cyber-physical network, to be studied under different malicious cyberattacks device is introduced, see Fig. 1. Physical devices such as grid-connected inverters, smart meters, transmission cables, loads, battery chargers, transformers, capacitor banks, etc., form the physical network. On the contrary, devices such as utility controllers, third-party aggregator servers, data processors, etc., that can establish a remote connection to the inverters form a remote communication network, is known as a cyber network. The communication link is the channel that allows communication between the physical-devices into the cyber network. This communication link provides smartness to the inverters by allowing interactive and real-time control to provide services beyond only active and reactive power injection to the grid.

Additionally, the communication link allows data sharing between inverters that are connected to different local networks. This connectivity to the outside network and information exchange can cause anomaly in the smart inverters. These anomalies can be classified as artificial and natural. The artificial anomalies can be considered intentional and unintentional cyber-attacks. A hacker can monitor inverter operation, gradually change inverter settings, and perform a malicious activity by sending manipulated active and reactive power setpoints to the inverter's local controller through the cyber network. In this paper, manipulated external data, intentional or unintentional, sent from the authorized sources like utility operators requesting a change in the inverter's power setpoints is considered cyberattacks.

III. Self-Security Concept for Smart Inverters

Fig. 2 shows the inverter's power capability curve and the stability boundary along with the capability curve of a generator. The capability curve of a synchronous generator describes a limit within which the machine can operate safely, as shown in Fig. 2 (right). To ensure a safe generator operation, the field current should not exceed the safe region limited by the armature when the armature limit curve falls inside the field limit curve. 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 $V_t E_f/|X_s|$, centered at $(0, -{V_t}^2/X_s)$ where V_t is the terminal voltage of the generator, E_f is the field excitation voltage, and X_s is the synchronous reactance.

Similarly, the equation of power, transferring from the inverter to the grid, define the active and reactive power normal region as a disk in the PQ-plane with a radius R centered at C, where the dependency of the radius and the center to the grid parameters are provided in Fig. 2(left). The circle with a radius, S_{max}, centered at the origin, illustrates the rated capacity of the inverter. The region where two circles intersect with each other is the safe region for inverter operation and contains all valid PQ setpoints [21]. However, the boundary of the safe region can change instantaneously based on the grid and inverter parameters. One can say from Fig. 2 that the idea of normal operating regions defined for both the grid-interactive inverters and generators is analogous. Nevertheless, any points that fall outside of the inverter intersected operating region cause non-linearity or abnormal operation. Therefore, these points are not going to be engaged to the local controller.

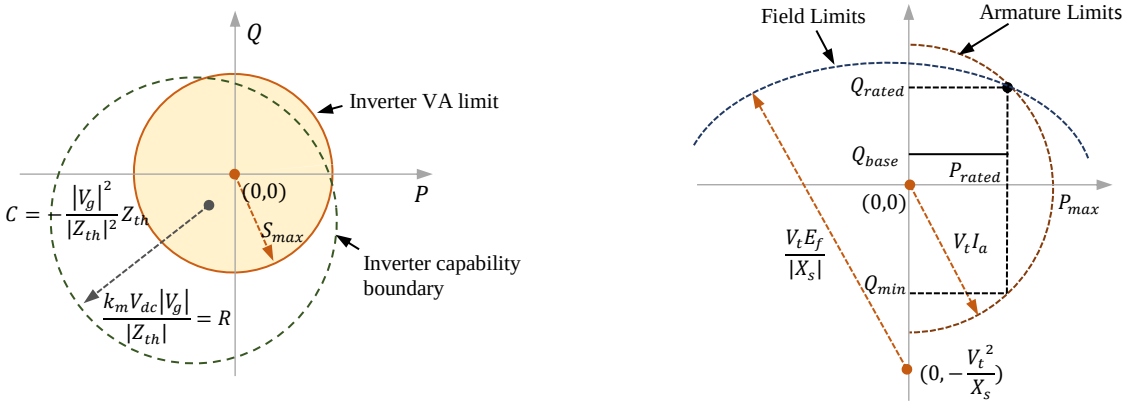

Fig. 2. Normal operating region of a grid-interactive inverter in a distribution grid compared with the capability curve of a synchronous generator.

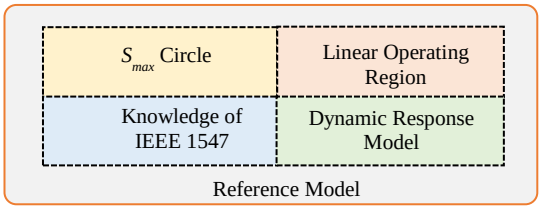

Fig. 3. knowledge-based for self-security techniques.

Self-security in smart inverters is an anomaly detection concept that ensures a safe operating region for smart inverters by providing an extra device-level protection layer on the existing communication- and system-level protections to examine the validity and applicability of incoming data. This concept is essential when the existing security measures fail or are bypassed due to incoming data appears to be coming from authorized sources. When a smart inverter knows its stability boundary, it can detect the bad setpoints that cause inverter abnormal or non-linear operation. The knowledge-based self-security techniques utilize reference models, as shown in Fig. 3, as a security wall before engaging the incoming data to the controller. A designer can choose a fixed reference model or adaptive reference model based on system requirements.

The inverter operates in a linear region when the incoming setpoints are inside the normal operating region, see Fig.3. The non-linear operation can be observed if the normal operation region is passed. In the non-linear region, for instance, $V_{LL} = m\sqrt{3}V_{DC}/(2\sqrt{2})$, can no longer be valid when sinusoidal PWM technique is used, and over-modulation can be observed. Consequently, current and voltage waveforms can be distorted, and this distortion can increase total harmonic distortion (THD). Significant pulse dropping can be seen if the total harmonic distortion (THD) of the system increases. According to IEEE Std. 591, see Table I., for low power applications, allowed THD for current and voltage are 5.0% and 8%, respectively [24]. Instability is the secondary impact of injecting harmonics into the system due to the non-linear behavior of the inverter. Maybe from a single inverter point of view, the system might still be operating normal or linear regions with low harmonics. However, in systems where coordinated inverter operations are utilized, the interaction between the inverters could lead to instability and reduce the power quality. On the other hand, PLL could lose its stability if the voltage is distorted. However, it must be noted that passing the normal operating region does not necessarily lead to instability.

Notice that, in the fixed reference model, model parameters cannot update in real-time operation. However, in the adaptive reference model, the parameters such as grid parameters need to be updated in real-time to represent the actual system characteristics. A well-tuned adaptive reference model that represents the actual system behavior can also be referred to as the digital twin of a smart inverter. Digital twins connect the physical and the digital platforms to validate real-time performance. When a smart inverter knows adequate information, it can learn its boundaries of operation and the dynamic characteristics at different operating conditions. This concept can be referred to as self-learning for self-security, which allows smart inverters to make accurate decisions during variable operating conditions.

TABLE I : IEEE 519

Voltage distortion limits		Current distortion limits	
$Voltage\ (V)$	$THD(\%)$	$Current\ ratio$	$THD(\%)$
$V < 1.0kV$	8.0	$I_{SC}/I_L < 20$	5.0
$1 < V < 69kV$	5.0	$20 < I_{SC}/I_L < 50$	8.0
$69 < V < 161kV$	2.5	$50 < I_{SC}/I_L < 100$	12.0

I_{SC}=Maximum short circuit current, I_L= Maximum demand load current

TABLE II : PARAMETERS FOR EXPERIMENTAL SET-UP

Parameters	Values
Fundamental frequency	60 Hz
PWM carrier frequency	20 kHz
$V_{LL,rms}$	208
V_{dc}	350 V
L_1 (Inverter-side of LCL)	1.0 mH
C_f (Δ)	30 µF
L_2 (Grid-side of LCL)	0.5 mH

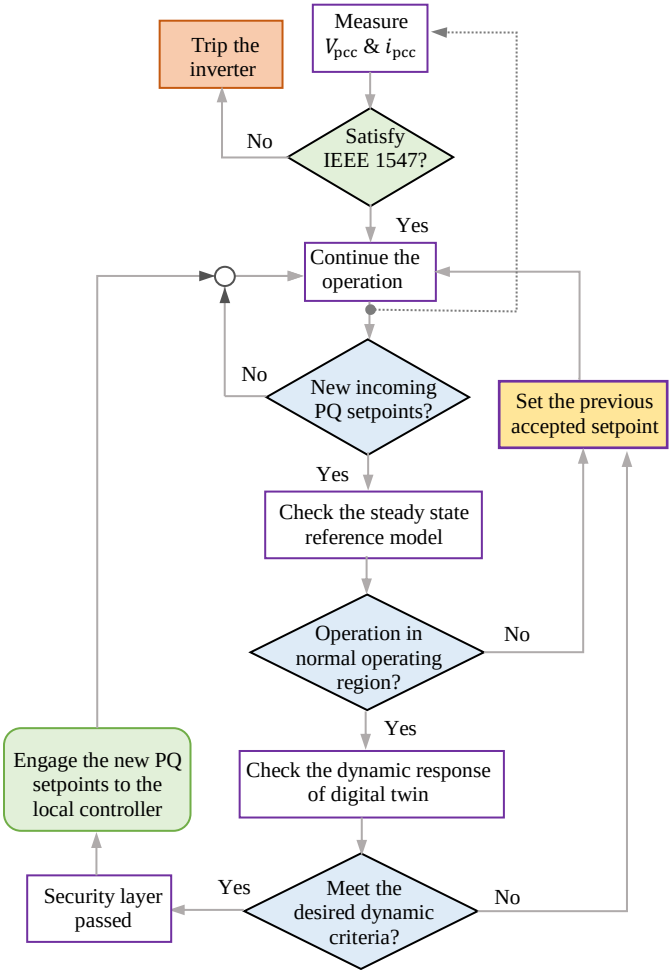

Fig. 4. Part of the self-security algorithm flowchart for smart inverters.

TABLE III: EXPERIMENTAL DATA FOR VOLTAGE VARIATION

Scenarios	$V_g(V)$	$I_a(A)$	pf (lag)	$V_{ab,pcc}(V)$	$V_{dc}(V)$	$Q^*(kVAr)$	$P^*(kW)$	$THD(\%)$	m
Impact of DC bus voltage, $V_{dc}(V)$	208	2.996	0.92	210.7	350	0.25	1.0	8.8	0.9902
	208	2.954	0.935	210.7	337.6	0.25	1.0	10.3	1.026
	208	3.016	0.93	211.1	324.5	0.25	1.0	20.6	1.070
Impact of grid voltage, $V_g(V)$	208	2.99	0.922	210.1	350	0.25	1.0	8.8	0.987
	217	2.796	0.927	219.2	350	0.25	1.0	10.1	1.029
	224	2.784	0.921	226.8	350	0.25	1.0	20.5	1.0649

TABLE IV: EXPERIMENTAL DATA FOR POWER INJECTION

Scenarios	$V_g(V)$	$I_a(A)$	pf (lag)	$V_{ab,pcc}(V)$	$V_{dc}(V)$	$Q^*(kVAr)$	$P^*(kW)$	$THD(\%)$
Change in P^* for $Q^*=0$	208	4.165	0.966	209.6	350	0	1.4	10.1
	208	4.136	0.968	209.8	350	0	1.394	10.2
	208	4.08	0.965	209.8	350	0	1.379	10.2
Change in P^* for $Q^*=0.35\ kVar$	208	3.035	0.902	212	350	0.35	0.998	10.2
	208	2.888	0.891	211.9	350	0.35	0.950	10.2
	208	2.939	0.901	211.8	350	0.35	0.969	10.5
Change in P^* for $Q^*=0.5kVar$	208	2.745	0.82	212	350	0.5	0.852	11.3
	208	2.499	0.79	211.9	350	0.5	0.748	10.8
	208	2.686	0.816	211.8	350	0.5	0.828	11

IV. DEVICE-LEVEL SELF-SECURITY ALGORITHM

The flowchart of the proposed self-security algorithm to detect the validity of the incoming PQ setpoints is presented in Fig. 4. This algorithm combines different reference models, including the knowledge of IEEE-1547, steady-state, and dynamic response reference models. The next step of this algorithm is to check the incoming PQ setpoints by the steady-state and dynamic reference model. After the PQ setpoints are satisfied by the steady-state and dynamic reference model requirements, the algorithm accepts the incoming PQ setpoints and engages them in the local PQ controller.

V. EXPERIMENTAL RESULTS

The effectiveness of the proposed self-security technique was verified experimentally using a three-phase hardware setup. In this hardware setup, a custom-built 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 three-phase LCL filter was connected at 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 I. All the experimental waveforms were measured using a Teledyne LeCroy HD4096 oscilloscope with CP030.

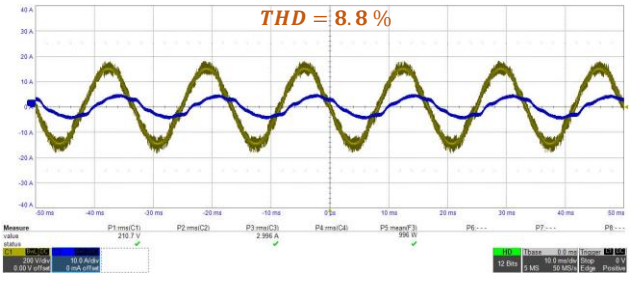

Fig. 5. Steady-state line-line voltage and line currents at $P = 1\ kW$, $Q = 0.25\ kVar$

First, the theory of the steady-state analysis was verified by an experimental test when the proposed self-security algorithm was disabled. The experimental results are outlined in Table III. The steady-state voltage and current waveforms at the inverter terminal are shown in Fig.5, where the inverter was at normal operation with $m < 1$, and current THD was within an acceptable limit, $< 10\%$. The dc-bus voltage and grid voltages were changed from their normal value to demonstrate the inverter's non-linear phenomenon. In all cases, active power and reactive power were set to $1kW$and $0.25kVAr$ respectively. In the first scenario, Fig. 6(a) and 6(b), the dc-bus voltage was reduced to $337.6V$ and $324.5V$, respectively. Reducing the dc-bus voltages caused over-modulation i.e., $m > 1$, which leads to higher THD. In the second scenario, Fig. 6(c) and 6(d), the grid voltage was increased to $217V$ and $224V$, respectively. Therefore, increasing the grid voltages also caused non-linear inverter operation.

To validate the inverter steady state linear operation region, different PQ setpoint was implemented in the hardware. For the given PQ setpoints total harmonic distortions (THD) was recorded using a power meter. Initially, reactive power setpoint was set to zero, and active power setpoint was increased until the THD reached to maximum acceptable limits, i.e. 10%.This process was repeated for three times and observed that active power setpoint for acceptable THD limit was around $P = 1.4\ kW$ which is represented as point A in Fig. 6. Then, reactive power setpoint was changed to $0.35\ kVar$ and observed active power setpoint was $P = 0.95\ kW$ for acceptable THD limits, represented as point B in Fig. 6. Finally, reactive power setpoint was set to $0.5\ kVar$ and observed active power setpoint for acceptable THD limit was $0.85\ kW$ which is represented as point C in Fig. 6. Notice, if the THD of the system increases significant pulse dropping can be seen and as a consequence a non-linear operation can be observed. Therefore, in inverter's normal or linear operation region PQ setpoints follows a trend

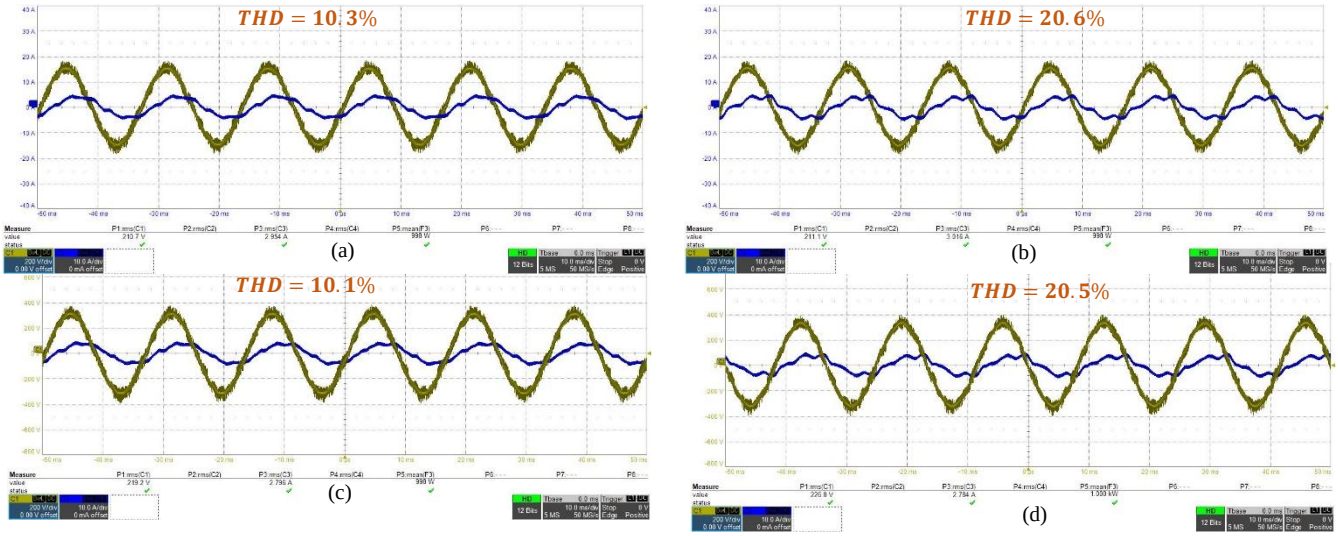

Fig. 6. Steady-state line-line voltage and line currents at $P = 1\ kW$, $Q = 0.25\ kVar$; (a) and (b), dc-bus voltages is reduced from normal value; (c) and (d), grid-voltage is increased from normal value.

of circle with radius R centered at O as shown in Fig. 6. Outside of this region, non-linear behavior like over-modulation can be observed, and voltage and current waveform become distorted.

The effectiveness of the self-security algorithm for the steady-state was checked in the hardware for different incoming PQ setpoints. By estimating the system's steady-state response, the incoming PQ setpoints were placed in the PQ-axis and detected whether they lied within the normal region or fall outside. When the incoming setpoints were inside the region, the proposed self-security algorithm accepted the setpoints.

Next, the incoming setpoints were checked by the dynamic response model. The dynamic reference model can be formed by a reduced fourth-order model [19],[23]. The transfer function of the fourth-order system with added zeros can be represented as follow.

$$\frac{\Delta V}{\Delta P} = \frac{K(s+z_1)(s+z_2)}{(s^2+2\zeta_L\omega_L+\omega_L^2)(s^2+2\zeta_H\omega_H+\omega_H^2)} \quad (1)$$

where, ζ_L, ζ_H represent low- and high-frequency damping ratios, ω_L, ω_H denote low- and high-frequency natural frequencies, and z_1, z_2 are the zeros, respectively. Notice, the low frequency poles are dominant in (1). This fourth-order model can be further simplified to a second-order model by including the low-frequency components only which can be represented as follows,

$$\frac{\Delta V}{\Delta P} = \frac{K_1(s+z)}{(s^2+2\zeta_L\omega_L+\omega_L^2)} \quad (2)$$

Where, K_1 is the gain and z is the zero of this second order system. The second-order model is computationally modest compared to fourth-order model and provide an accurate estimation of actual system response [25]. In this work, dynamic response model is formed by the second-order model. To validate the performance of second-order model, the peak amplitude of the voltage at PCC was recorded for both inverter circuit simulation and dynamic response model. For a given step change of active power, $\Delta P = 3\,\text{kW}$ at 0.13s, the recorded response is shown in Fig. 7., from which one can conclude that estimated results by the second-order system are in good agreement with full-order inverter circuit simulation. Thus, the proposed knowledge-based self-security algorithm can detect the incoming setpoints that cause abnormal operation in the inverter.

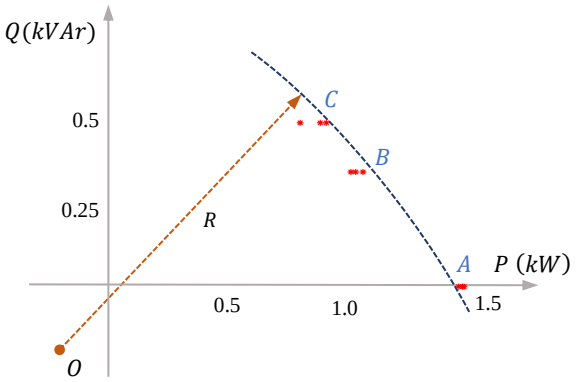

Fig. 6. Demonstration of inverter steady-state linear operation region for incoming PQ setpoints.

VI. Conclusion

In this paper, a knowledge-based self-security algorithm is developed for incoming power setpoints. The knowledge-based digital twin is formed by estimating the normal operating region of the inverter and its reduced order dynamic model. The non-

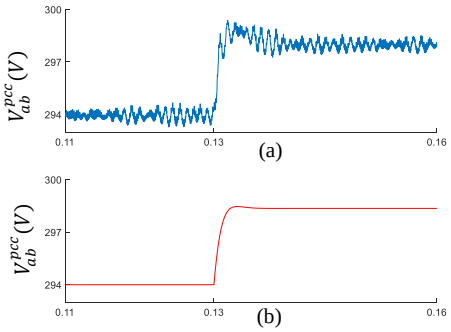

Fig. 7. For a given step change in the active power, ΔP, the dynamic responses obtained from a circuit simulation (Top), and second-order model of the inverter (bottom).

linear phenomenon of the inverter is experimentally demonstrated when the incoming setpoints are outside of the normal operating region. The incoming setpoints are checked through the steady-state reference and dynamic reference model to verify whether the inverter operation stays on linear or non-linear operation region to ensure safe operation of the inverter.

VII. References

[1] B. Mirafzal and A. Adib, "On grid-interactive smart inverters: features and advancements," *IEEE Access*, vol. 8, pp. 160526-160536, 2020.

[2] A. Adib, F. Fateh and B. Mirafzal, "Smart inverter stability enhancement in weak grids using adaptive virtual-inductance," *IEEE Trans. Ind. Appl.*, vol. 57, no. 1, pp. 814-823, Jan.-Feb. 2021.

[3] M. S. Pilehvar, M. B. Shadmand and B. Mirafzal, "Analysis of smart loads in nanogrids," *IEEE Access*, vol. 7, pp. 548-562, 2019.

[4] A. Adib and B. Mirafzal, "Virtual Inductance for stable operation of grid-interactive voltage source inverters," *IEEE Trans. Ind. Electron.*, vol. 66, no. 8, pp. 6002-6011, Aug. 2019.

[5] A. Adib, J. Lamb and B. Mirafzal, "Ancillary services via VSIs in microgrids with maximum DC-bus voltage utilization," *IEEE Trans. Ind. Appl.*, vol. 55, no. 1, pp. 648-658, Jan.-Feb. 2019.

[6] A. Singh and B. Mirafzal, "An efficient grid-connected three-phase single-stage boost current source inverter," *IEEE Power Energy Technol. Syst. J.*, vol. 6, no. 3, pp. 142-151, Sept. 2019.

[7] B. Arbab-Zavar, E. Palacios-Garcia, J. Vasquez, and J. Guerrero, "Smart inverters for microgrid applications: a review," *Energies*, vol. 12, no. 5, Mar. 2019.

[8] J. Qi, A. Hahn, X. Lu, J. Wang and C. Liu, "Cybersecurity for distributed energy resources and smart inverters," *IET Cyber-Physical Syst.: Theory Appl.*, vol. 1, no. 1, pp. 28-39, 12 2016.

[9] M. Gursoy and B. Mirafzal, "On Self-Security of Grid-Interactive Smart Inverters," 2021 IEEE Kansas Power and Energy Conference (KPEC), 2021, pp. 1-6.

[10] F. Sadeque, J. Benzaquen, A. Adib and B. Mirafzal, "Direct phase-angle detection for three-phase inverters in asymmetrical power grids," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 9, no. 1, pp. 520-528, Feb. 2021.

[11] North American Electric Reliability Corporation, "1200 MW fault induced solar photovoltaic resource interruption disturbance report," NERC, Jun. 2017.

[12] S. Sahoo, T. Dragičević and F. Blaabjerg, "Cyber Security in Control of Grid-Tied Power Electronic Converters–Challenges and Vulnerabilities," in *IEEE J. Emerg. Sel. Topics Power Electron.*

[13] S. Tan, J. M. Guerrero, P. Xie, R. Han and J. C. Vasquez, "Brief survey on attack detection methods for cyber-physical systems", *IEEE Syst. J.*, May 2020.

[14] 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 Trans. Smart Grid*, vol. 8, no. 5, pp. 2505–2516, Sep. 2017.

[15] 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 Trans. Neural Netw. Learn. Syst.*, vol. 27, no. 8, pp. 1773–1786, Aug. 2016.

[16] K. Abdollah, W. Su, and T. Jin, "A machine learning based cyber attack detection model for wireless sensor networks in microgrids," *IEEE Trans. Ind. Informat.*, Jan. 2020.

[17] Y. Shoukry and P. Tabuada, "Event-triggered state observers for sparse sensor noise/attacks," *IEEE Trans. Autom. Control*, vol. 61, no. 8, pp. 2079–2091, Aug. 2015.

[18] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control, vol.* 58, no. 11, pp. 2715–2729, Nov. 2013.

[19] T. Hossen, F. Sadeque, M. Gursoy and B. Mirafzal, "Self-secure inverters against malicious setpoints," *in Proc.* 2020 IEEE Electric Power and Energy Conference (EPEC), 2020, pp. 1-6.

[20] S. Sahoo, T. Dragičević, Y. Yang and F. Blaabjerg, "Adaptive Resilient Operation of Cooperative Grid-Forming Converters Under Cyber Attacks," *in Proc.* 2020 IEEE CyberPELS (CyberPELS), 2020, pp. 1-5.

[21] J. Lamb and B. Mirafzal, "Grid-interactive cascaded H-bridge multilevel converter PQ plane operating region analysis," *IEEE Trans. Ind. Appl.*, vol. 53, no. 6, pp. 5744-5752, Nov.-Dec. 2017.

[22] J. Lamb and B. Mirafzal, "Active and reactive power operational region for grid-interactive cascaded H-bridge multilevel converters," *2016 IEEE Energy Conversion Congress and Exposition (ECCE)*, Milwaukee, WI, 2016, pp. 1-6.

[23] A. Adib, F. Fateh, M. B. Shadmand, and B. Mirafzal, "A reduced-order technique for stability investigation of voltage source inverters," *2018 IEEE Energy Conversion Congress and Exposition (ECCE)*, Portland, OR, 2018, pp. 5351-5356.

[24] "IEEE Recommended Practice and Requirements for Harmonic Control in Electric Power Systems," *IEEE Std 519-2014 (Revision of IEEE Std 519-1992)* , vol., no., pp.1-29.

[25] A. Adib, F. Fateh, M. B. Shadmand and B. Mirafzal, "A Reduced-Order Technique for Stability Investigation of Voltage Source Inverters," *2018 IEEE Energy Conversion Congress and Exposition (ECCE)*, 2018, pp. 5351-5356