Digital Twin of an ANPC inverter with integrated Design-For-Trust

Paulo Custodio
Department of Electrical Engineering
University of Arkansas
Fayetteville, Arkansas
pdcustod@uark.edu

Brady McBride
Department of Electrical Engineering
University of Arkansas
Fayetteville, Arkansas
bjmcbrid@uark.edu

Thao Le
Department of Electrical Engineering
University of Arkansas
Fayetteville, Arkansas
tpl001@uark.edu

Justin Jackson
Department of Electrical Engineering
University of Arkansas
Fayetteville, Arkansas
jej029@uark.edu

Kelby Haulmark
Department of Computer Science
University of Arkansas
Fayetteville, Arkansas
klhaulma@uark.edu

Jia Di
Department of Computer Science
University of Arkansas
Fayetteville, Arkansas
jdi@uark.edu

Chris Farnell
Department of Electrical Engineering
University of Arkansas
Fayetteville, Arkansas
cfarnell@uark.edu

H. Alan Mantooth
Department of Electrical Engineering
University of Arkansas
Fayetteville, Arkansas
mantooth@uark.edu

***Abstract*—Reducing costs and increasing manufacturing output while creating reliable products are three essential components needed to keep a business competitive. In the past, having an asset that could address these three challenges at the same time would be challeging. However, recent advances in computer processing capabilities coupled with increases to network speeds allowed such a system to become possible; and this is known as a Digital Twin (DT), which represents a virtual copy of a production system or a product. This work exhibits a DT application of an Active Neutral Point Clamped (ANPC) inverter using a controller. The controller emulates the ANPC responses of a new Digital Signal Processing (DSP) firmware and validates this new firmware by using Design-For-Trust (DFTr) characteristics. If the new firmware is malicious, then it should be rejected, thus adding preemptive protection measures for inverter based distributed energy resources.**

Keywords— cybersecurity, Design-For-Trust. Digital twin, distributed energy resources, embedded systems, grid connected. ,

I. Introduction

Advancements in technology such as increases to computing power while reducing overall device footprint and the significant increases in the availability and speed of communication lead to the number of internet connected devices to increase significantly. However, while emergence of smart devices being connected to the internet brings many benefits, including increased situational awareness, it also creates additional attack vectors and channels for cyber-attacks to be carried out. A cyber-attack usually starts in the communication layer, which commonly involves Phishing, Man-in-the-Middle (MitM) and Denial of Service (DoS) attacks. If attackers gain access to the communication layer, they can traverse the network to gain access to the other cyber-physical layers. For instance, an adversary gaining access to the supervisory layer, or even to control and hardware layers, has the potential to result in a complete shutdown of the system [1]. In 2015, Ukraine had to disconnect twenty-three 35kV and seven 110kV substations for three hours due to a cyber-attac. This attack began with a phishing technique that resulted in the power loss of 225,000 customers. Another cyber-attack that occurred in 2016 in Kiev, Ukraine, caused part of the capital to be deprived of electricity for more than one hour [2]. Later in 2017 in response to this new threat potential, United States' President Donald Trump signed an order to intensify the cyber security of federal networks and critical infrastructures which specifically contains a section pointing to the risks of "electricity disruption" [2]. Therefore, this work proposes an improvement to the hardware layer of cyber-physical devices, creating a Digital Twin of an ANPC inverter within a custom controller. In the controller, a Field Programmable Gate-Array (FPGA) emulates an ANPC inverter and is used toauthenticate a Digital Signal Processor (DSP) firmware. This authentication prevents the update, or patching, of a malicious firmware that could carry out a cyber-physical attack on solar distributed energy resources (DERs) via grid-connected inverters.

II. Digital Twin

The concept of the Digital Twin (DT) was first introduced in 2003 by Professor Grieves from the University of Michigan during a product life cycle management course. Grieves explained that a DT is considered a virtual information structure that could represent a manufactured product [3]. Grieves also believed that a DT model should have three-dimensions: physical entity, virtual entity, and an interconnection between them [4]. However, the interpretation of what constitutes a DT can change depending on each application. For instance, [1] affirmed that DTs of cyber-secure grid-connected devices are Real-Time simulations and can be used to monitor system

978-1-6654-7999-8/22/$31.00 ©2022 IEEE

health, event response, and overall efficiency during cyber-attack scenarios. As these efforts were based on the work presented by [1], this paper discusses the Digital Twin concept and its application in terms of hardening an ANPC inverter against potential cyber-attacks.

III. ANPC Inverter and Modulation

The 3-level ANPC inverter has six clamped switches, as opposed to four used on NPC inverters, to better balance the loss distribution throughout the switches. The benefit of a better-balanced inverter is an improvement in the power output efficiency, even though this topology has an increase in its cost, weight and complexity. Fig. 1, first introduced in [5], illustrates one phase of a 3-level ANPC inverter using six switches.

To control the inverter, this paper uses the modulation type II described in [6] as the switching state configuration requires fewer high frequency switches. Table 1 in [6] illustrates the modulation type II switching states.

Table 1- Switch states modulation type II [6]

State	Output	Q1	Q2	Q3	Q4	Q5	Q6
P	0.5Vdc	1	1	0	0	0	1
O^+	0	1	0	1	0	0	1
O^-	0	0	1	0	1	1	0
N	-0.5Vdc	0	0	1	1	1	0

As the ANPC inverter has six switches that work independently, there is the potential for some hazardous switching states that could put the device and the load into jeopardy. For example, Fig. 2 illustrates a short-circuit scenario where Q1 and Q5 are active at the simultaneously. Hazardous switching configurations as such need to be avoided, which is where the firmware authentication system's DFTr capabilities are utilized.

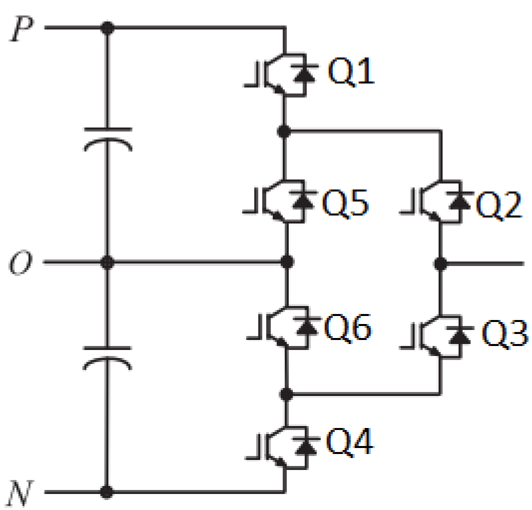

Fig. 1 - Phase leg of a three-level ANPC inverter topology

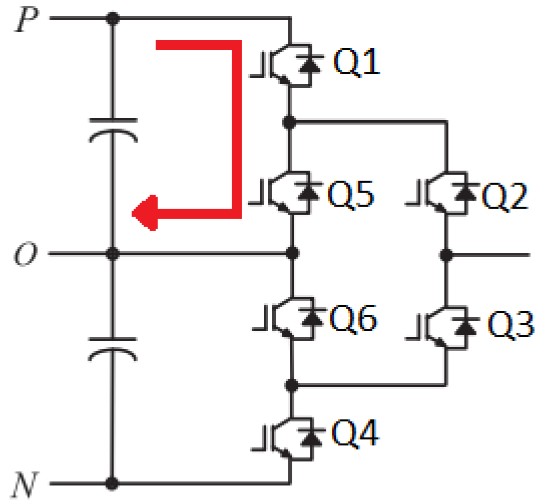

Fig. 2 - Short-Circuit Scenario

IV. Controller and Design-For-Trust

This work is based on [1], where the DT's system architecture in Fig. 3 includes one FPGA and two DSPs. The hardware description language VHDL (VHSIC Hardware Description Language) was used to instantiate the emulated physical system while C programming language was used in the firmware design to control the DSPs. In [1], the system utilizes one DSP as actively controlling the inverter while the emulation of a 2-level inverter occurs on the standby DSP for testing and validation purposes. However, in this work, the FPGA emulates an ANPC inverter as opposed to a 2-level inverter. The emulation of an ANPC inverter allows this work to have real-world application while further investigating the cyber-hardening of cyber-physical devices.

The device controller is responsible for operating a commercial off-the-shelf grid connected ANPC inverter and is also tasked with validating that a newly received firmware update is not malicious. The controller authenticates a new DSP firmware using the outputs from the standby/inactive DSP to emulate a three-phase ANPC inverter, creating a DT of the ANPC. This emulation must generate a phase output voltage virtually identical to the real inverter that was presented in [6], as seen in Fig. 4. When receiving the outputs from the inactive DSP, the FPGA tests all the requirements that were designed by the DFTr strategy. If the new firmware successfully recreates the expected outputs and has all the operational requirements to take over control of the inverter, the standby DSP seamlessly assumes control while utilizing the newly validated firmware without any system downtime.

To facilitate the human interactive portion of the system status and controls the graphical programming environment LabVIEW was utilized. In Fig. 5a, the LabVIEW GUI (Graphical User Interface) illustrates which DSP is currently active (1 or 2), if the firmware is undergoing the loading process, and displays the results of the DFTr validation tests. After the DFTr tests are performed, the GUI indicates whether the system is ready to hot-patch on the user's command, or if the DFTr system returned authentication issues and hot-patching has been disabled for the current new firmware. Fig. 5b displays the visualization of the possible errors that the DFTr system can report as detected and how this graphical environment was designed using LabVIEW.

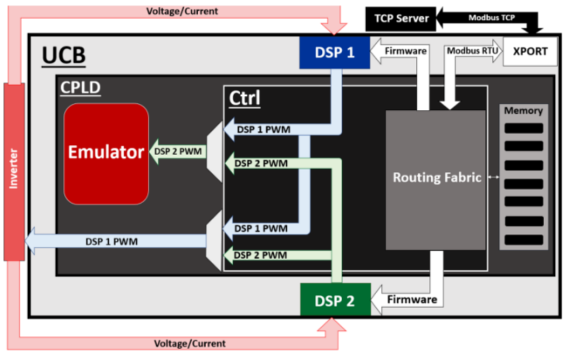

Fig. 3 - Hardware Architecture [1]

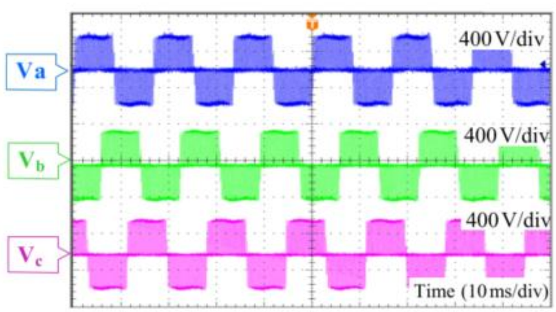

Fig. 4 - Inverter phase output voltage waveforms [6]

A. Design-For-Trust

The DFTr strategy design was developed based on system state scenarios that could jeopardize the ANPC inverter or the power grid. All the firmware tests are performed simultaneously, increasing the efficiency of the authentication process. The following checks are performed after a new firmware is uploaded, but before the firmware becomes active. If any of these DFTr testing scenarios fail to pass their respective checks, the firmware will be considered malicious by nature and the system will not allow this firmware to become active.

1) Test 1: Short-Circuit

The short-circuit tests evaluates the operational switching states of the new firmware to ensure that a short-circuit condition among the switches is never met, such as the scenario presented in Fig. 2.

2) Test 2: Dead Time

The dead time test ensures that there is enough time delay between the switching states to prevent shoot-through current among switches that should not be in a conducting state simultaneously. This invalid switching configuration could lead to a system short-circuit.

3) Fundamental Frequency

The current frequency in the US electrical systems operates at 60Hz and should be as stable as possible to maintain a reliable electric system [7][8]. Frequency variations can be caused due to various reasons, such as generation loss and demand overload [8][9], which have negative impacts on the grid. Loss of generation can trigger protection relays involuntarily or cause the grid to reach the lowest acceptable frequency resulting in severely impacting the systems stability [9].

As this work is directly related with grid-connected energy resources, providing stable operational frequency is vital to avoid the introduction of unwanted harmonic distortions to the grid. The DFTr controller verifies that the DSP firmware is able to operate the inverter to generate the 60Hz frequency on the grid.

4) Timer

The last check of the DFTr strategy is to check that the DSP firmware will not put the controller in a stall position. A stall position is considered when the FPGA is waiting for the DSP PWM signals, but the malicious firmware does not contain any rising or falling edge in the control signals. During the firmware tests, if the timer reaches the maximum waiting time, the new DSP firmware is rejected.

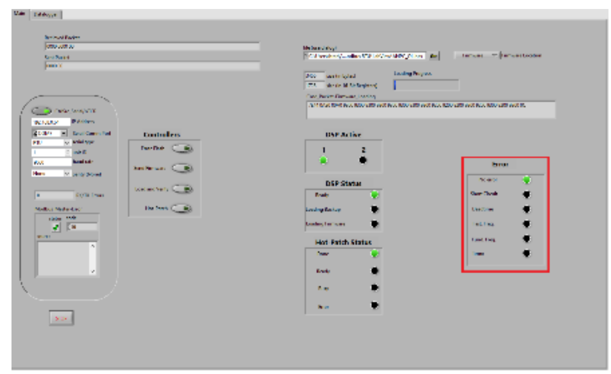

Fig. 5a - LabVIEW Interface

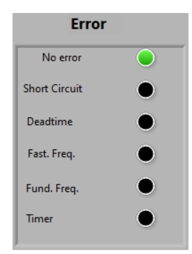

Fig. 5b - LabVIEW Interface – Error types

V. Results

This section will discuss the process and actions performed by the DT system in its emulation and validation process of newly received firmware. The process of verifying known good firmware is discussed initially, followed by the attempt to load firmware that is known to be malicious in nature.

First, a standard DSP firmware was sent to the FPGA. This DSP firmware possesses all the operational requirements that were previously specified. To confirm that the firmware meets operational requirements, and to determine if it is malicious or not, a Tektronix MSO 4034 oscilloscope was used to monitor the DSP's output signals. Fig. 6 presents the signals obtained using the oscilloscope when a non-malicious firmware is under operation.

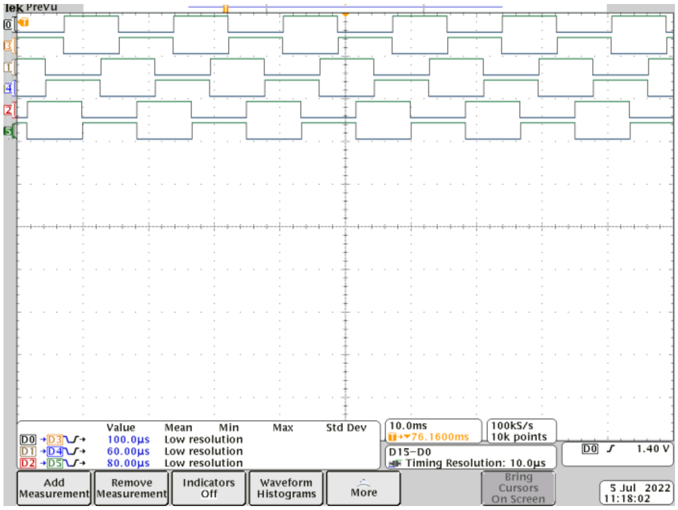

Fig. 6 - Standard Firmware

From Fig.6, channels 0 and 3 represent Phase A, where channel 0 is the signal that controls Q1 and Q6, and channel 3 controls Q4 and Q5. Channels 1 and 4 represent Phase B, and channels 2 and 5 are Phase C (Table 1). As the fast frequency transistors behavior does not present a risk to the ANPC inverter, they were not monitored.

At the bottom of Fig.6, there are values in blue text that indicate the dead time between D0 and D3. Thus, the firmware from Fig. 6 has 100µs of dead time between channel 0 and channel 3, while the dead time between channel 1 and 4 is 60 µs.

Table 2 – Transistors/Channels relation

Phase A	
Q1 & Q6	Channel 0
Q4 & Q5	Channel 3
Phase B	
Q1 & Q6	Channel 1
Q4 & Q5	Channel 4
Phase C	
Q1 & Q6	Channel 2
Q4 & Q5	Channel 5

After performing the DFTr checks, the FPGA has authenticated the DSP firmware and is able to emulate the ANPC inverter output. Fig. 7 exhibits the emulation generated by the FPGA which is displayed using LabVIEW. Despite the resolution of the waveforms displayed in Fig. 7, it is noticeable that the signals obtained through the emulation are similar to that of a real ANPC inverter (Fig. 3).

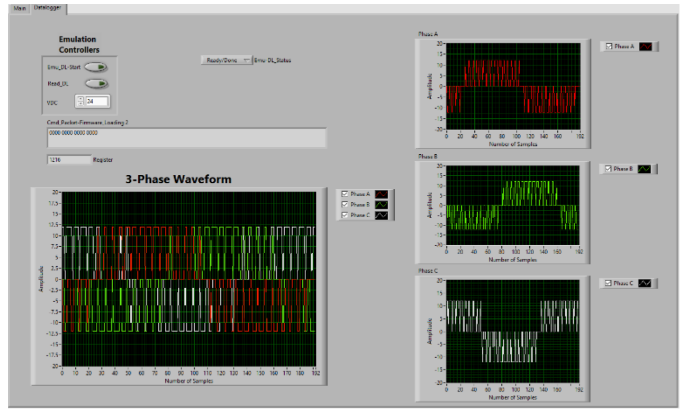

Fig. 7 - ANPC Emulation

When a malicious firmware is sent to take control of the inverter, the FPGA must reject it and fall back to a reliable firmware, or in this case, a backup firmware. Additionally, the FPGA must not allow the enabling of the hot-patching feature while keeping the currently active DSP operating the known good firmware.

To test the DT, multiple versions of firmware with known bad operational states were loaded into the FPGA.

First, a firmware where Phase A has Q1, Q4, Q5 and Q6 on simultaneously (Fig. 8) is sent to the FPGA. Fig. 9 exhibits that the FPGA rejected the firmware while returning an error state. The indicated error was a short-circuit scenario and the system responds by loading the backup firmware, as indicated in the graphical display.

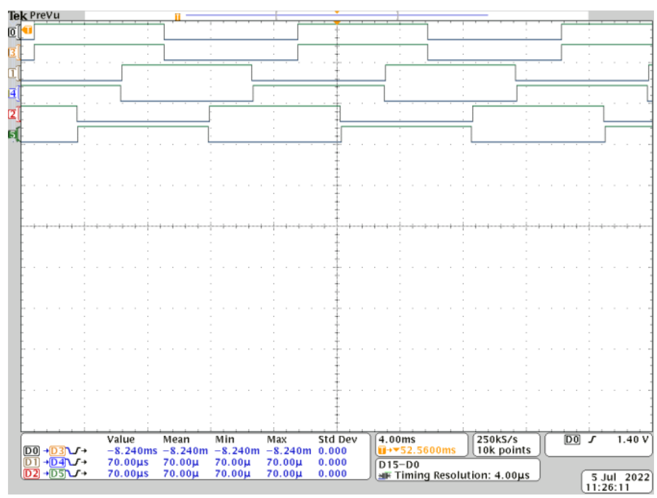

Fig. 8 - Channel 0 and 3 on at simultaneously

Fig. 9 - Short-Circuit Error

Next, a malicious firmware that does not have any dead time applied was sent to the FPGA. Fig. 10 illustrates the firmware without dead time, as the measurement indicators at the bottom left indicate that the dead time between channel 0 (D0) and channel 3 (D3) is 0s.

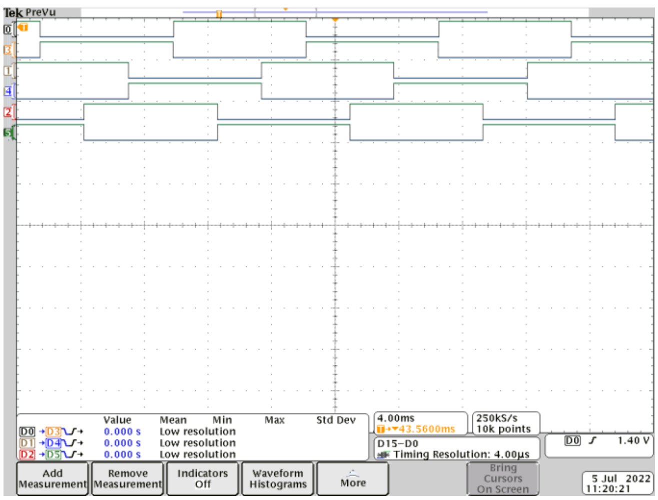

Fig. 10 - No Dead Time between D0&D3, D1&D4 and D2&D5

When the FPGA detected the dead time error, it rejected the firmware and fell back to the backup firmware, as seen in Fig. 11.

Fig. 11 - Dead Time Error

In the case that the malicious firmware has proper dead time and does not contain a short-circuit scenario, the fundamental frequency still needs to be verified. Operation at an unacceptable fundamental frequency, such as 30 Hz, could lead to an obvious negative impact on the grid. In this instance, the DT should also reject this firmware to protect the inverter hardware and the power grid itself. Fig. 12 illustrates a firmware with an out of operational bounds fundamental frequency of 30 Hz.

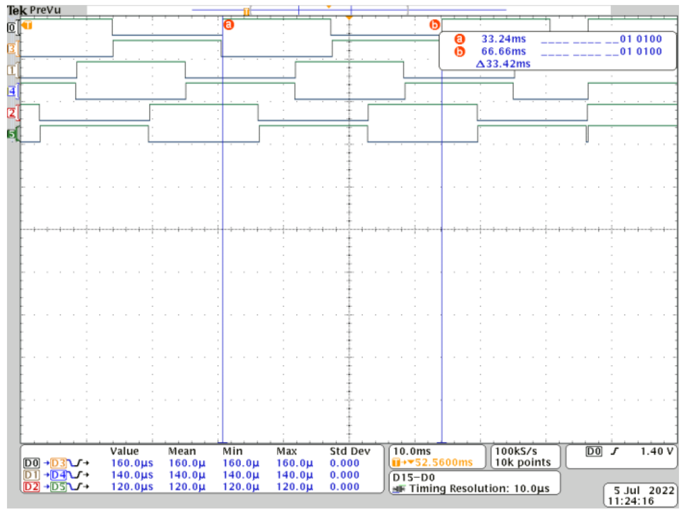

Fig. 12 - 30Hz Firmware

From Fig. 12, a value of 33.42ms is indicated at the top right corner. This value represents the period of the signal on channel 0 and 3. A period of 33.42ms represents a 30Hz signal as opposed to the ideal target frequency of 60Hz (16.66ms). This firmware should also be rejected, and Fig. 13 exhibits the FPGA's response to this malicious firmware.

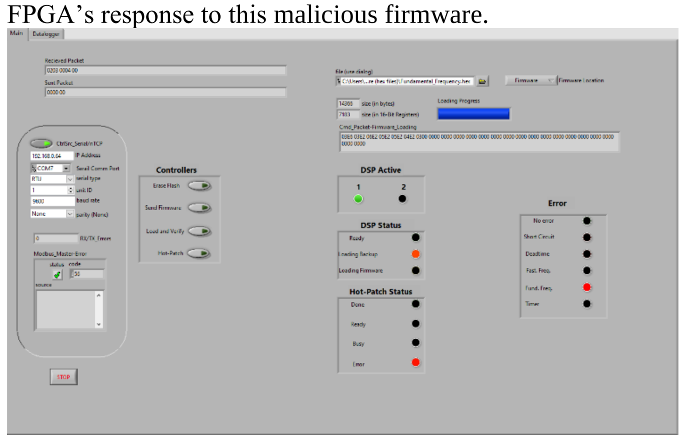

Fig. 13 - Fundamental Frequency Error

Lastly is the case of a firmware that has constant values as signals instead of pulse width modulated signals. In the event this type of firmware was sent to the FPGA, a timer error will indicate that the checking process is taking longer than expected and the DFTr system will stop the validation process. If this process is stopped prematurely, the firmware will be flagged as bad firmware. Fig. 14 illustrates a firmware where all signal outputs are constant values, while Fig. 15 presents the DT's response.

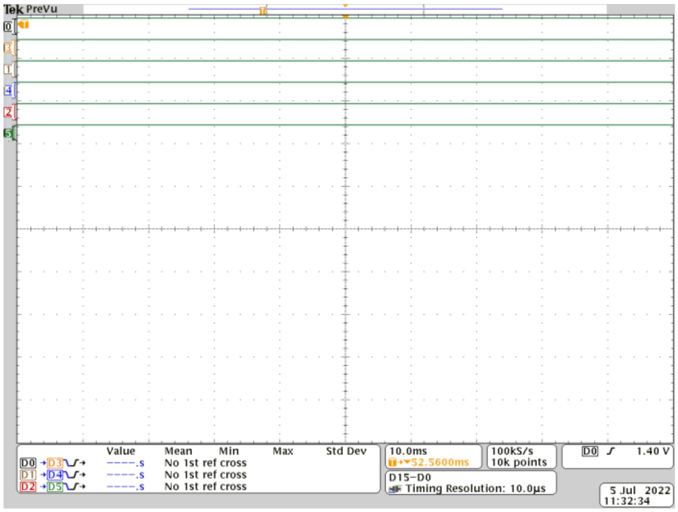

Fig. 14 - Constants Firmware

Fig. 15 - Timer Error

VI. Conclusions and Future Work

Advances in technology, the widespread availability of high-speed internet, and power-grids becoming increasingly connected to various network allow for a multitude of benefits in the realm of DER applications. Some advantages include increased situational awareness, supporting cross-disciplinary event response strategies, and advanced secondary and tertiary controls to increase efficiency and grid resilience. While these benefits are necessary to meet the growing demand on the bulk electric grid, connecting these devices to the internet opens additional attack vectors that can introduce vulnerabilities to the power grid. Thus, the need for an improvement in cyber-security focused devices to protect the power grid from cyber-attacks is an ever present demand. This newly developed system can protect the hardware layer of distributed energy resource controls and block many cyber-attacks that try to manipulate the inverter's behavior, even if a cyber-attack is successful in obtaining control of the network layer.

The proposed work continued what was presented in [1] and successfully demonstrated an application of the controller that is utilized to design a DT that was able to replicate and emulate an ANPC inverter output in addition to checking if the new DSP firmware has all the requirements stipulated by the DFTr.

The current DT can be improved in future works through additions to the types of emulations supported, such as a phase-to-phase emulation instead of phase-to-neutral. Also, comparing system performance and efficiencies between the new firmware and active firmware could help identify situations where the new firmware satisfies all operating requirements but may result in potentially worse system performance. These efforts also provide the groundwork and system structure to potentially modify the emulation architecture to accommodate different types of inverter topologies.

Acknowledgement

This material is based upon work supported by the U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy (EERE) under Solar Energy Technologies Office (SETO) Agreement Number DE-EE0009026.

Testing for this project was conducted at the National Center for Reliable Electric Power Transmission (NCREPT), the University of Arkansas' High-Power Test Facility.

References

[1] C. Farnell, E. Soria, J. Jackson and H. A. Mantooth, "Cyber Protection of Grid-Connected Devices Through Embedded Online Security," 2021 IEEE Design Methodologies Conference (DMC), 2021, pp. 1-6, doi: 10.1109/DMC51747.2021.9529935.

[2] B. Huang, M. Majidi and R. Baldick, "Case Study of Power System Cyber Attack Using Cascading Outage Analysis Model," 2018 IEEE Power & Energy Society General Meeting (PESGM), 2018, pp. 1-5, doi: 10.1109/PESGM.2018.8585921.

[3] J. Wu, Y. Yang, X. Cheng, H. Zuo and Z. Cheng, "The Development of Digital Twin Technology Review," 2020 Chinese Automation Congress (CAC), 2020, pp. 4901-4906, doi: 10.1109/CAC51589.2020.9327756.

[4] M. Van Den Brand, L. Cleophas, R. Gunasekaran, B. Haverkort, D. A. M. Negrin and H. M. Muctadir, "Models Meet Data: Challenges to Create Virtual Entities for Digital Twins," 2021 ACM/IEEE International Conference on Model Driven Engineering Languages and Systems Companion (MODELS-C), 2021, pp. 225-228, doi: 10.1109/MODELS-C53483.2021.00039

[5] J. Li, A. Q. Huang, S. Bhattacharya and G. Tan, "Three-Level Active Neutral-Point-Clamped (ANPC) Converter with Fault Tolerant Ability," 2009 Twenty-Fourth Annual IEEE Applied Power Electronics Conference and Exposition, 2009, pp. 840-845, doi: 10.1109/APEC.2009.4802759.

[6] D. Woldegiorgis, Y. Wu, Y. Wei and H. A. Mantooth, "A High Efficiency and Low Cost ANPC Inverter Using Hybrid Si/SiC Switches," in IEEE Open Journal of Industry Applications, vol. 2, pp. 154-167, 2021, doi: 10.1109/OJIA.2021.3091549

[7] E. Ela, V. Gevorgian, A. Tuohy, B. Kirby, M. Milligan and M. O'Malley, "Market Designs for the Primary Frequency Response Ancillary Service—Part I: Motivation and Design," in IEEE Transactions on Power Systems, vol. 29, no. 1, pp. 421-431, Jan. 2014, doi: 10.1109/TPWRS.2013.2264942.

[8] M. Folgueras, E. Wenger, A. Florita, K. Clark and V. Gevorgian, "Grid "Frequency Extreme Event Analysis and Modeling", 2017 International Workshop on Large-Scale Integration of Wind Power into Power Systems as well as on Transmission Networks for Offshore Wind Power Plants, October 25-27, 2017, Berlin Germany.

[9] J. H. Eto, J. Undrill, P. Mackin, R. Daschmans, B. Williams, B. Haney, R. Hunt, J. Ellis, H. Illian, C. Martinez, M. O'Malley, K. Coughlin, and K. Hamachi LaCommare, "Use of frequency response metrics to assess the planning and operating requirements for reliable integration of variable renewable generation," eScholarship, 2011