5-2022

Signal Analysis of Photovoltaic Systems for Multilevel Cybersecurity

Wesley G. Schwartz
University of Arkansas, Fayetteville

Signal Analysis of Photovoltaic Systems for Multilevel Cybersecurity

A thesis submitted in partial fulfillment
of the honors requirements for the degree of
Bachelor of Science in Electrical Engineering

by

Wesley Garrett Schwartz
University of Arkansas

May 2022
University of Arkansas

ABSTRACT

The cybersecurity of grid-connected power electronics is a rapidly developing field as more and more of these devices become a part of the Internet of Things. The objective of this thesis to analyze the current control signals of a photovoltaic (PV) inverter and develop an interface board for the implementation of a new cyber-secure controller.

In this thesis, the testing and in-depth analysis of the current PV inverter control system will be conducted. Using the data collected, an interface board will be developed to allow the use of the Unified Control Board (UCB), developed by Chris Farnell, in the PV inverter. This UCB will act as the new cyber-secure controller and help satisfy the project requirements of system and inverter level cybersecurity. Finally, after full integration, the PV inverter will undergo a 6-month field demonstration.

ACKNOWLEDGEMENTS

I would like to thank my advisor Dr. H. Alan Mantooth for this opportunity to complete a bachelor's degree in Electrical Engineering with honors and his support and guidance throughout my time as an undergraduate student. I would especially like to thank Dr. Chris Farnell, Dr. Shannon Davis, and Justin Jackson for their advisement and mentorship throughout my undergraduate career.

I would also like to thank my friends and fellow students Sloan Becker, Rosten Sweeting, Vinson Jones, Eric Allee, Andrea Wallace, and Logan Walz. This thesis is dedicated to my parents, Donald and Karen, and my brother, Daniel, for their unwavering support.

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Motivations for Research: The Growing Importance of Photovoltaic Systems

The world has seen substantial growth in the utilization of renewable energy sources like photovoltaic (PV) systems. In an effort to respond to climate change, governments around the world have implemented policies to incentivize PV systems. PV systems provide several benefits. This includes increased energy security, as solar power is an import-independent energy source. Additionally, solar energy systems result in minimal environmental impacts. The energy conversion process releases no carbon dioxide and the main component in the manufacturing process of PV arrays is silicon, which is abundant and environmentally safe [1,2].

The sun is the most significant energy source on Earth. The amount of irradiated energy from the sun seen on Earth in one day is enough to satisfy the electrical energy demand for more than twenty years. The safe and efficient harvesting of this energy could be revolutionary for the sustainability of the civilizations on Earth [3].

1.2 The Role of Cybersecurity

With the advent of the Internet of Things (IoT) and the smart grid, cybersecurity has taken a priority in power electronics. The Department of Energy (DOE) has identified attack resistance as one of seven properties required for smart grids to meet future demand. Smart grids require significant dependence on intelligent and secure communication. The current technologies can be vulnerable to cyber-attacks and could create potentially disastrous situations for both power companies and consumers [4,5]. In 2015, coordinated cyber-attacks compromised three power distribution companies in Ukraine. This created large scale power outages affecting

nearly a quarter of a million people for several hours. Multiple styles of attacks were used to successfully bring down the power grid, but the main attack was a hijack of the Supervisory Control and Data Acquisition (SCADA) system which included the takedown of field devices with malicious firmware [6]. With the growth of smart grids and smart grid-connected power electronics, the threat of large-scale attacks like those that occurred in Ukraine is more prominent. Thus, the development of cyber-secure power electronics, such as PV systems, is crucial for the health and reliability of electric power distribution.

1.3 References

[1] C. Nemes, F. Munteanu, M. Rotariu and D. Astanei, "Availability assessment for grid-connected photovoltaic systems with energy storage," *2016 International Conference and Exposition on Electrical and Power Engineering (EPE)*, 2016, pp. 908-911, doi: 10.1109/ICEPE.2016.7781467.

[2] Ahmadi, MH, Ghazvini, M, Sadeghzadeh, M, et al. Solar power technology for electricity generation: A critical review. *Energy Sci Eng*. 2018; 6: 340– 361. https://doi.org/10.1002/ese3.239

[3] Review and comparison of different solar energy technologies, Global Energy Network Institute (GENI); 2011.

[4] S. Sridhar, A. Hahn and M. Govindarasu, "Cyber–Physical System Security for the Electric Power Grid," in *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210-224, Jan. 2012, doi: 10.1109/JPROC.2011.2165269.

[5] Y. Yan, Y. Qian, H. Sharif and D. Tipper, "A Survey on Cyber Security for Smart Grid Communications," in *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 998-1010, Fourth Quarter 2012, doi: 10.1109/SURV.2012.010912.00035.

[6] G. Liang, S. R. Weller, J. Zhao, F. Luo and Z. Y. Dong, "The 2015 Ukraine Blackout: Implications for False Data Injection Attacks," in *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317-3318, July 2017, doi: 10.1109/TPWRS.2016.2631891.

CHAPTER 2

TEST PLAN FOR SIGNAL ANALYSIS

2.1 Pass-Through Testing Boards

To create an interface board for a new cyber-secure controller, an in-depth analysis of the current control system installed on the PV inverter must be conducted. In order to analyze this system, four pass-through style boards were developed to enable easy access to the controller pins. These boards established test points for two 40-pin IDC connectors and two 60-pin IDC connectors. These test boards are shown in Figure 2.1 and Figure 2.2.

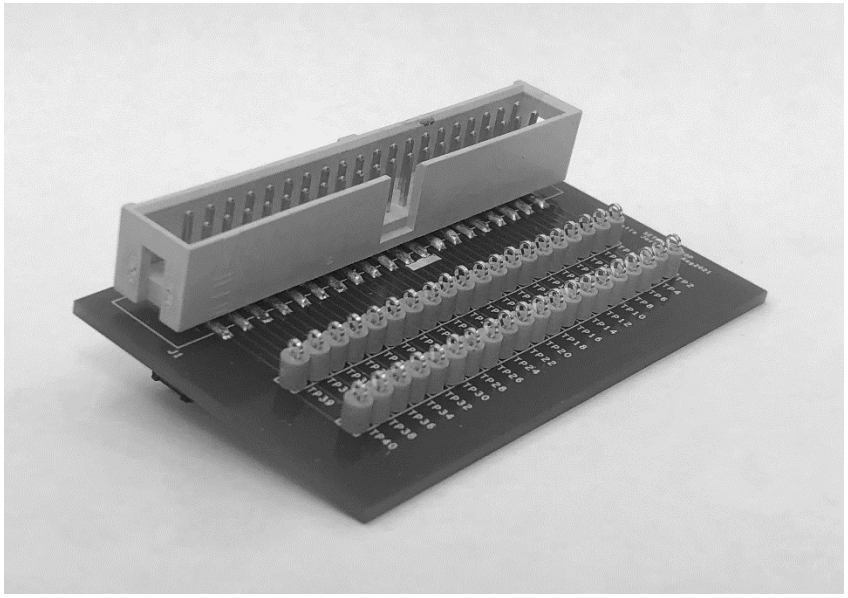

Figure 2.1: 40-pin IDC Pass-Through Board

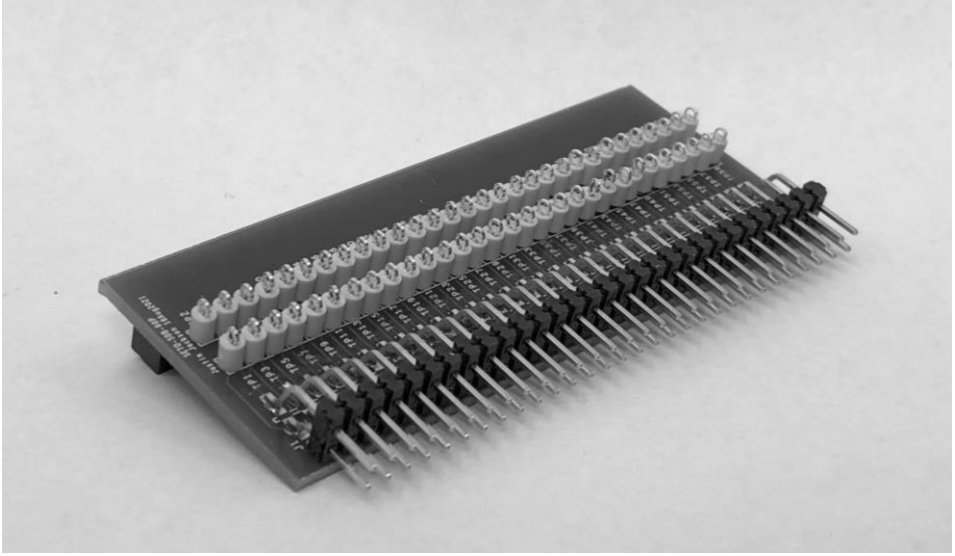

Figure 2.2: 60-pin IDC Pass-Through Board

Once the boards were received from the manufacturer, they were fabricated, and 200 test points were soldered to the boards. Then, all of the connections were tested for electrical shorts and open circuits.

2.2 Testing Procedure

After the pass-through boards were fabricated and tested, the test setup could be completed. The PV inverter was carefully disassembled to allow for the addition of the pass-through boards. Some connecting cables were lengthened to account for the added height. The addition of the boards is shown in Figure 2.3.

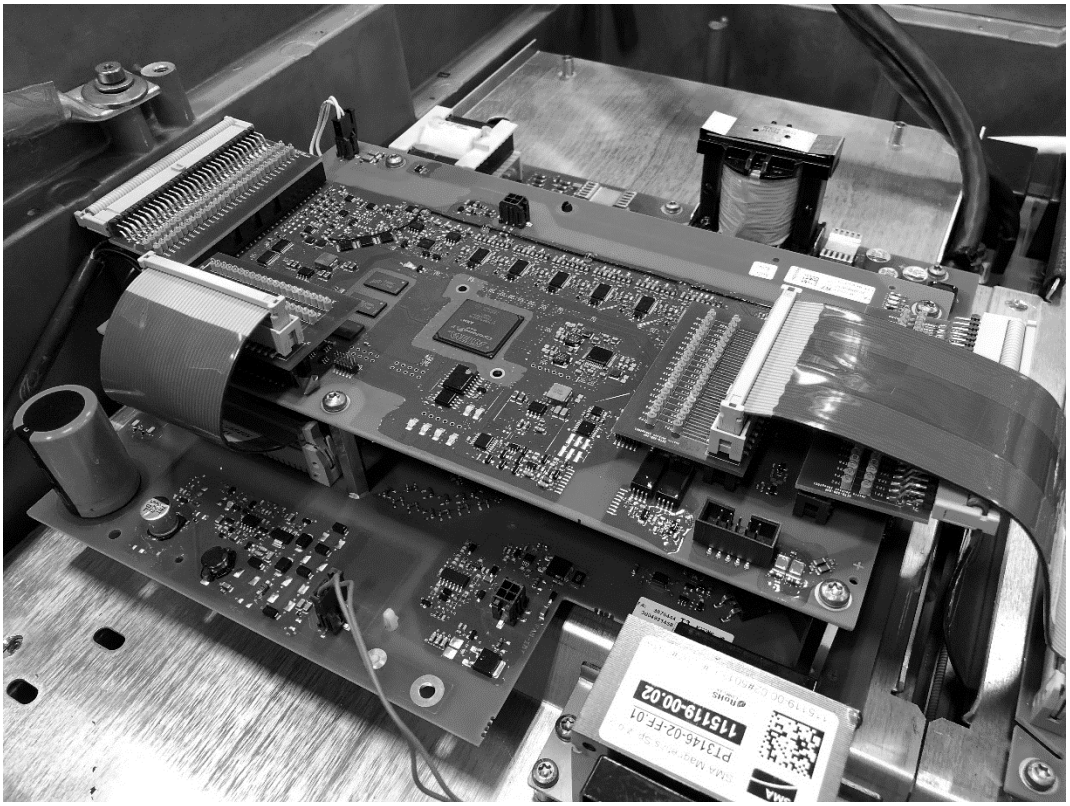

Figure 2.3: Pass-Through Board Installation

Once the pass-through boards were properly installed and all of the factory control boards re-installed, the testing equipment could be set-up. The SMA PV inverter requires a three-phase, 480V connection and a DC power supply. The DC power supply simulates the connected solar panel. This was provided by a Sorensen DC power supply. The inverter was also connected to the local network via an ethernet connection for remote control of the system. To analyze the signals, the pins connected to digital ground were identified and an 8-channel oscilloscope was connected to the remaining pins of the pass-through boards. The completed test stand set-up is shown in Figure 2.4. For each test, the start-up procedure for the inverter was completed and the inverter limited to 10 kW.

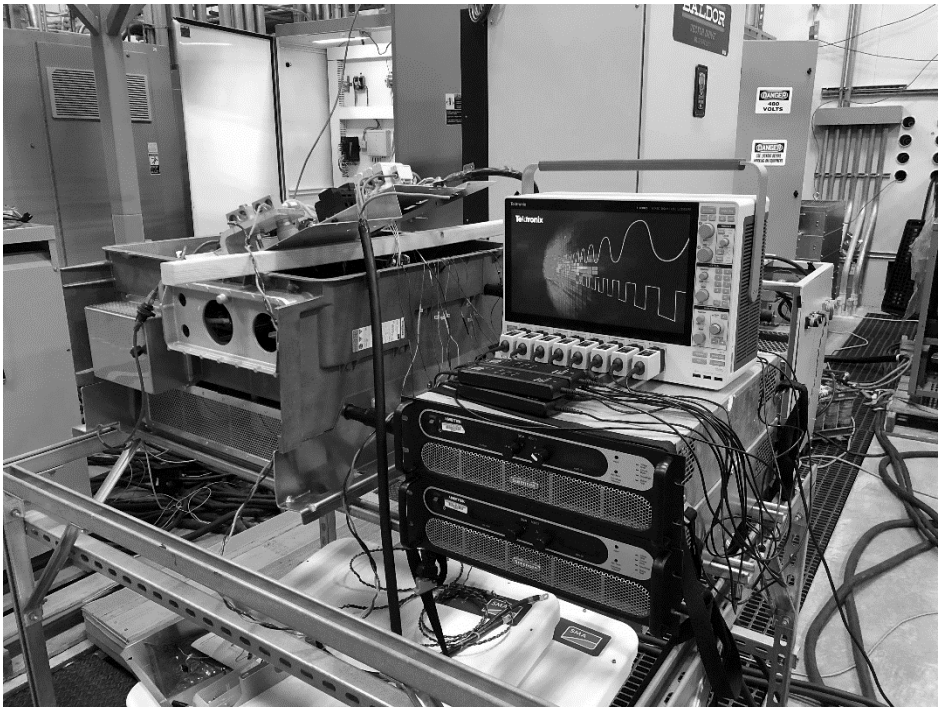

Figure 2.4: Test Stand Set-up

2.3 Signal Analysis Results

To correctly identify each of this signals, multiple tests were run throughout a multi-week testing procedure. Signals were tested 6 to 8 at a time with all the available voltage probes. With each test, the start-up procedure was monitored closely, and each signal's behavior was reviewed and documented. Some critical signals for UCB integration, such as the current sensors, were traced from the physical PCB part to the controller board. The result of the signal analysis for each pass-through board are shown in their respective tables below.

Table 2.1: 40-Pin 1 Results

40 Pin IDC Pass-Through 1			
Pin	Type	Range	Comments:
1	PWR	15V	15V Power
2	GND	0V	Ground
3	PWR	15V	15V Power
4	GND	0V	Ground
5	PWR	15V	15V Power
6	GND	0V	Ground
7	PWR	15V	15V Power
8	GND	0V	Ground
9	PWR	15V	15V Power
10	GND	0V	Ground
11	PWR	15V	15V Power
12	GND	0V	Ground
13	PWR	15V	15V Power
14	GND	0V	Ground
15	PWR	15V	15V Power
16	GND	0V	Ground
17	PWR	15V	15V Power
18	GND	0V	Ground
19	PWR	15V	15V Power
20	GND	0V	Ground
21	n/a	0V	Noise
22	n/a	0V	Noise
23	n/a	0V	Noise
24	SIG	1.4V	1.4V @810 Vdc; changed with DC voltage
25	SIG	1.6V	Spiked to 6V
26	GND	0V	Ground
27	SIG	1.34V	1.34V @810 Vdc; changed with DC voltage
28	SIG	0.5V	Possible DC voltage measurement
29	REF	2V	Constant voltage no change
30	REF	1.5V	Constant voltage no change
31	GND	0V	Ground
32	REF	1.5V	Constant voltage no change
33	REF	1.5V	Possible DC current signal
34	REF	1.5V	Constant voltage no change
35	REF	2.1V	Constant voltage no change
36	SIG	0V	n/a
37	REF	3.0V	Constant voltage no change
38	REF	1.5V	Constant voltage no change
39	GND	0V	Ground
40	SIG	5V	High with power supplies

Table 2.2: 40-Pin 2 Results

40 Pin IDC Pass-Through 2			
Pin	Type	Range	Comments:
1	N/A	5V	Noise
2	GND	0V	Ground
3	PWR	15V	15V Power
4	PWR	15V	15V Power
5	GND	0V	Ground
6	GND	0V	Ground
7	PWR	15V	15V Power
8	PWR	15V	15V Power
9	GND	0V	Ground
10	GND	0V	Ground
11	PWM	2V	Active low at 60% duty cycle
12	PWM	2.1V	Active low at 60% duty cycle
13	GND	0V	Ground
14	PWM		High then low before relays
15	GND	0V	Ground
16	RLY		Relay Signal/Output of comparator/Possible RST signal
17	GND		Ground
18	N/A	0.6V	Noise
19	GND		Ground
20	N/A	0V	Noise
21	GND		Ground
22	REF	2.162V	Constant 2.162V on w/Power supplies
23	GND		Ground
24	SIG	2.505V	Current sensor output (3P combined)
25	REF	2.5V	Reference voltage for current sensor
26	GND	0V	Ground
27	SINE	2V mean	0.5148V ACrms high to 2V w/Power Supplies, Voltage Sensing w/relay
28	SINE	2V mean	0.5136V ACrms high to 2V w/Power Supplies, Voltage Sensing w/relay
29	SINE	2V mean	0.5099V ACrms high to 2V w/Power Supplies, Voltage Sensing w/relay
30	GND	0V	Ground
31	SINE	1.5V	0.5099V ACrms, on with power supplies.
32	SINE	1.5V	0.5047V ACrms, on with power supplies.
33	SINE	1.5V	0.5056V ACrms, on with power supplies.
34	GND	0V	Ground
35	SIG	1.5V	Possible DC Voltage
36	SINE	1.5V	1.5V sine wave. Constant did not change. Maybe Voltage
37	GND		Ground
38	PWR	5V	15V Power
39	N/A		Noise
40	N/A	5V	Noise

Table 2.3: 60-Pin 1 Results

60 Pin IDC Pass-Through 1			
Pin	Type	Range	Comments:
1	N/A	0V	noise
2	SIG	4.9V	possible PWM enable signals
3	SIG	5V	possible PWM enable signals
4	SIG	5V	possible PWM enable signals
5	PWM	2.5V	PWM signal, 60Hz
6	PWM	2.5V	42khz PWM
7	PWM	2.5V	42khz PWM
8	GND	0V	DIGITAL GROUND
9	PWM	2.5V	PWM signal, 60Hz
10	PWM	2.5V	PWM signal, 60Hz
11	PWM	2.41V	PWM signal, 60Hz
12	GND	0V	DIGITAL GROUND
13	PWM	2.5V	PWM signal, 60Hz
14	PWM	2.5V	42khz PWM
15	PWM	2.5V	42khz PWM
16	GND	0V	DIGITAL GROUND
17	PWM	2.5V	PWM signal, 60Hz
18	PWM	2.5V	PWM signal, 60Hz
19	PWM	2.5V	PWM signal, 60Hz
20	GND	0V	DIGITAL GROUND
21	PWM	2.6V	PWM signal, 60Hz
22	PWM	2.6V	42khz PWM
23	PWM	2.64V	42khz PWM
24	GND	0V	DIGITAL GROUND
25	PWM	2.67V	PWM signal, 60Hz
26	PWM	WF	PWM signal, 60Hz
27	PWM	2.58V	PWM signal, 60Hz
28	SIG	WF	Went high when relay activated
29	SIG	4.89V	Went high (4.8V) before current fluctuations
30	SIG	5V	Went high (4.8V) before current fluctuations
31	PWR	15V	15V Power
32	GND	0V	DIGITAL GROUND
33	PWR	15V	15V Power
34	GND	0V	DIGITAL GROUND
35	REF	2.048V	could be a reference signal
36	GND	0V	DIGITAL GROUND
37	REF	2.05V	no change constant voltage
38	GND	0V	DIGITAL GROUND
39	REF	2.05V	no change constant voltage
40	GND	0V	DIGITAL GROUND

41	REF	1.8V	no change constant voltage
42	GND	0V	DIGITAL GROUND
43	REF	1.8V	no change constant voltage
44	GND	0V	DIGITAL GROUND
45	REF	5.2V	no change constant voltage
46	REF	5.2V	no change constant voltage
47	SINE	1.4V	AC current sensor - 269 ACrms @ 10kW
48	GND	0V	DIGITAL GROUND
49	SINE	1.51V	AC current sensor - 283 ACrms @ 10kW
50	GND	0V	DIGITAL GROUND
51	SINE	1.51V	AC current sensor - 256 ACrms @ 10kW
52	SIG	WF	Possible voltage sensor on AC side 515mV at 1kW
53	SIG	1.49V	Possible voltage sensor on AC side 515mV at 1kW
54	GND	0V	DIGITAL GROUND
55	SIG	WF	sine wave - Possible voltage sensor on AC side 515mV at 1kW
56	GND	0V	DIGITAL GROUND
57	REF	1.88V	no change constant voltage
58	GND	0V	DIGITAL GROUND
59	REF	1.5V	no change constant voltage
60	REF	2.2V	no change constant voltage

Table 2.4: 60-Pin 2 Results

60 Pin IDC Pass-Through 2			
Pin	Type	Range	Comments:
1	N/A	0V	noise
2	SIG	4.9V	possible PWM enable signals
3	SIG	5V	possible PWM enable signals
4	SIG	5V	possible PWM enable signals
5	PWM	2.5V	PWM signal, 60Hz
6	PWM	2.5V	42khz PWM
7	PWM	2.5V	42khz PWM
8	GND	0V	DIGITAL GROUND
9	PWM	2.5V	PWM signal, 60Hz
10	PWM	2.5V	PWM signal, 60Hz
11	PWM	2.41V	PWM signal, 60Hz
12	GND	0V	DIGITAL GROUND
13	PWM	2.5V	PWM signal, 60Hz
14	PWM	2.5V	42khz PWM
15	PWM	2.5V	42khz PWM
16	GND	0V	DIGITAL GROUND
17	PWM	2.5V	PWM signal, 60Hz
18	PWM	2.5V	PWM signal, 60Hz

19	PWM	2.5V	PWM signal, 60Hz
20	GND	0V	DIGITAL GROUND
21	PWM	2.6V	PWM signal, 60Hz
22	PWM	2.6V	42khz PWM
23	PWM	2.64V	42khz PWM
24	GND	0V	DIGITAL GROUND
25	PWM	2.67V	PWM signal, 60Hz
26	PWM	WF	PWM signal, 60Hz
27	PWM	2.58V	PWM signal, 60Hz
28	SIG	WF	Went high when relay activated
29	SIG	4.89V	Went high (4.8V) before current fluctuations
30	SIG	5V	Went high (4.8V) before current fluctuations
31	PWR	15V	15V Power
32	GND	0V	DIGITAL GROUND
33	PWR	15V	15V Power
34	GND	0V	DIGITAL GROUND
35	REF	2.048V	could be a reference signal
36	GND	0V	DIGITAL GROUND
37	REF	2.05V	no change constant voltage
38	GND	0V	DIGITAL GROUND
39	REF	2.05V	no change constant voltage
40	GND	0V	DIGITAL GROUND
41	REF	1.8V	no change constant voltage
42	GND	0V	DIGITAL GROUND
43	REF	1.8V	no change constant voltage
44	GND	0V	DIGITAL GROUND
45	REF	5.2V	no change constant voltage
46	REF	5.2V	no change constant voltage
47	SINE	1.4V	AC current sensor - 269 ACrms @ 10kW
48	GND	0V	DIGITAL GROUND
49	SINE	1.51V	AC current sensor - 283 ACrms @ 10kW
50	GND	0V	DIGITAL GROUND
51	SINE	1.51V	AC current sensor - 256 ACrms @ 10kW
52	SIG	WF	Possible voltage sensor on AC side 515mV at 1kW
53	SIG	1.49V	Possible voltage sensor on AC side 515mV at 1kW
54	GND	0V	DIGITAL GROUND
55	SIG	WF	sine wave - Possible voltage sensor on AC side 515mV at 1kW
56	GND	0V	DIGITAL GROUND
57	REF	1.88V	no change constant voltage
58	GND	0V	DIGITAL GROUND
59	REF	1.5V	no change constant voltage
60	REF	2.2V	no change constant voltage

CHAPTER 3

BOARD DESIGN

3.1 Design Parameters

After identifying the signals needed to integrate the UCB, it was noted that certain design parameters would be necessary accomplish the integration tasks. To make UCB integration as seamless as possible, the interface boards were to be designed to fit into the existing layout. Careful measurements were taken to ensure that the boards would sit neatly in the inverter housing and not interfere with any of remaining electronics. Additionally, after more closely reviewing the signal results, it was determined that the best course of action would be to design the boards in a way that allows for the original PV inverter control signals to pass-through the board if it was not a signal to be controlled by the UCB. This would make it possible to select whether each signal would be controlled by the UCB or by the original controller. Due to the complexity of the original PV inverter design, not every signal was positively identified. Therefore, the boards were designed such that the extra unidentified inverter pins and all additional ADC and GPIO pins from the UCB were routed to auxiliary banks. This would allow for easy routing if a signal was determined necessary to integration once the boards were fabricated. It was also discovered that the PV inverter control board was using 5V signals to run the inverter. This presented a problem, as the UCB is a 3.3V system. To mitigate this problem, bi-directional level shifting circuitry needed to be included in the interface board design. Additionally, the software integration team wanted the ability to inject bad signals into the feedback lines from the voltage and current sensors to test their controller's resilience to false data injection attacks. All these considerations were taken into the final design of the interface boards.

3.2 Schematic Layout

To begin the schematics, the known signals were routed through 3 pin terminals to allow the placement of a jumper to determine the source of the controls: Original controller or UCB. The pins going to the original controller were routed to their corresponding pass-through pin and the pins going to the UCB were routed to the UCB connector and, if necessary, the level-shifting circuitry. For the first 40-pin board, no level shifting circuitry was required, as the board consisted mostly of dedicated power. The second 40-pin interface board did require level shifting, so both an octal bus transceiver and a bi-directional logic translator were added to the design. Additionally, to power these circuits, a 5V to 3.3V LDO was also included in the design.

The 60-pin boards contained the features found on the 40-pin boards but added a false data injection circuit. To accomplish this functionality, a non-inverting op-amp summing circuit, pictured in Figure 3.1, was used.

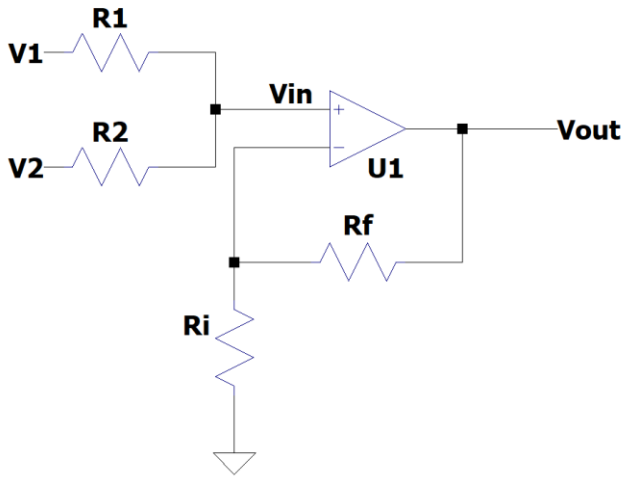

Figure 3.1: Non-Inverting Summing Op-Amp

The weighting of the signals can be adjusted by the selection of R1 and R2. In the case of interface boards, all of the resistors were selected to have the same weight so the equation for V_{OUT} can be simplified to the following:

$$V_{OUT} = (1 + \frac{R_f}{R_i})(\frac{V_1 + V_2}{2})$$

For the case of the UCB interface boards, R_f was selected to be 0 Ω and R_i was selected to be 1 kΩ. Only two input voltages were summed, so the output equation was simplified to the following:

$$V_{OUT} = (\frac{V_1 + V_2}{2})$$

Additional Op-amps were included in the event that more signals needed to have false data injection capability. These op-amp inputs and outputs were routed to an auxiliary bank on the interface boards.

3.3 PCB Design

The design of the PCB was largely influenced by the current layout of the SMA inverter and the projected location of the new UCB controller. To make the installation tidy, all of the connections for the UCB were placed on the board edge closest to the bottom of the inverter. The simplicity of the two 40-pin interface boards allowed for a two-layer design. The level shifting circuitry on 40-pin board 2 was kept together and labeled. Additionally, the auxiliary banks were labeled to aid in integration.

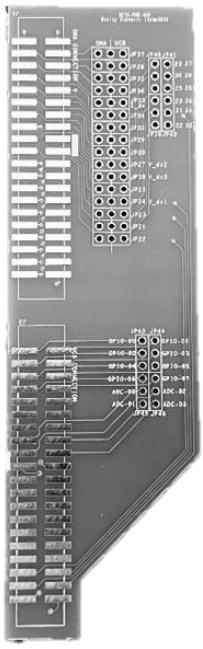

Figure 3.2: 40-pin Board 1

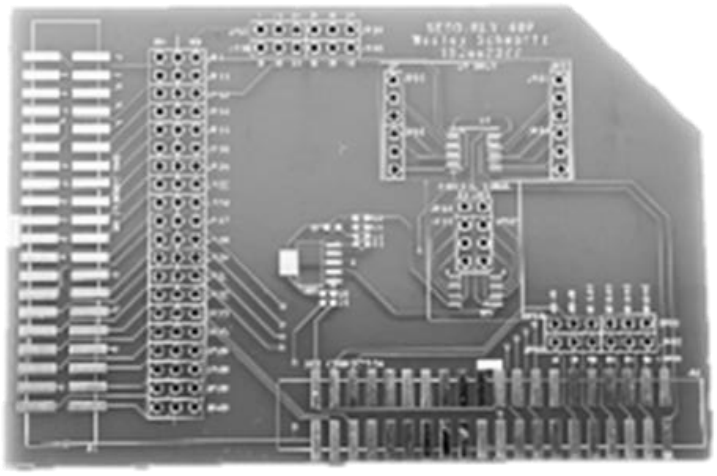

Figure 3.3: 40-pin Board 2

Due to the complexity and sheer number of signals, both 60-pin interface boards were designed as 4-layer boards. Like the earlier boards, the level-shifting and false signal injection circuity was placed together and clearly labeled. Although the two 60-pin schematics were symmetrical, the physical boards were not due to space constraints.

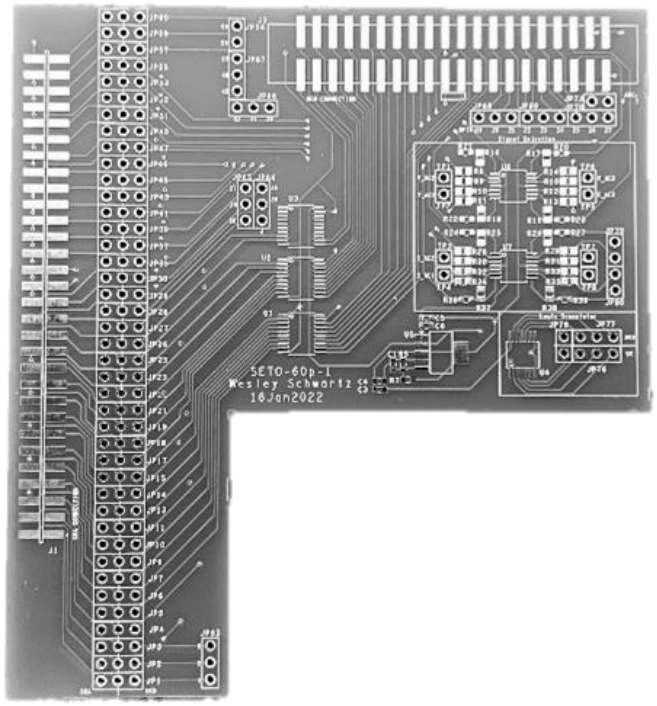

Figure 3.4: 60-pin Board 1

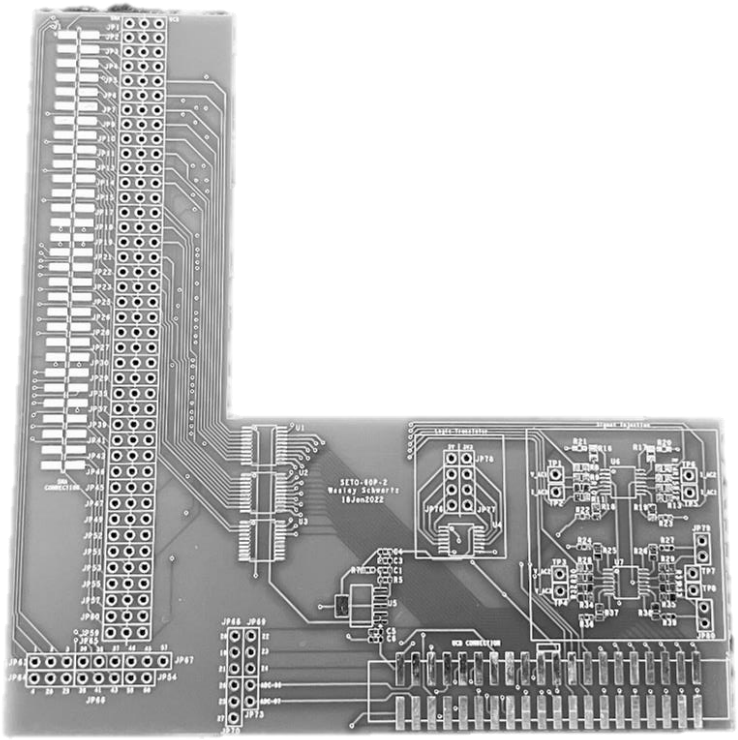

Figure 3.5: 60-pin Board 2

Once all four boards were received from the manufacturer, they were fabricated and tested for signal continuity. Once this was verified, they were ready to be installed in the inverter.

3.4 UCB Integration

Once the boards were installed in the SMA inverter, a test of the original inverter controller was conducted to ensure correct functionality of the interface boards. In the pass-through configuration, all of the boards functioned as expected. However, during software integration, it was determined that using the original inverter peripheral boards with the UCB was not an advantageous path forward. Therefore, the hardware integration design changed. The relay and power boards were removed from the inverter and the two 40-pin boards were no longer necessary for the UCB controller. Additionally, 24V, 15V, and 5V power supplies were added. To obtain same functionality of the original SMA inverter, voltage sensors were added for the DC input and each phase of the AC output. The UCB was mounted in the inverter and a contactor and relay board were added to enable connection to the grid. Once all of the new components were added, the inverter was tested at low power to tune the control algorithms.

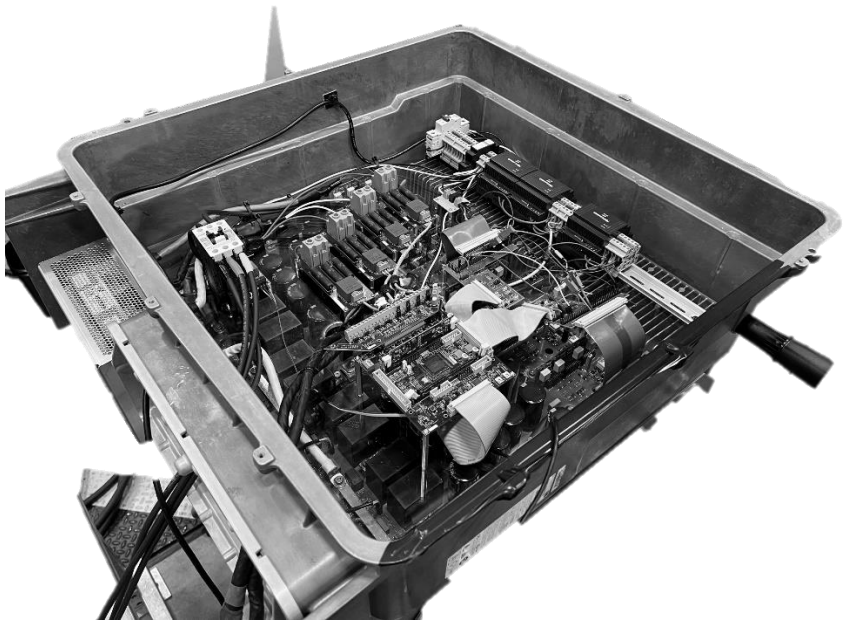

Figure 3.6: UCB Integration Overview

Figure 3.7: UCB Integration Layout

CHAPTER 4

CONCLUSIONS AND RECOMMENDATIONS FOR FUTURE WORK

4.1 Conclusions

Chapter 1 introduced concept of cybersecurity in grid-connected power electronics like the PV inverter and provided examples of large-scale attacks seen in recent history. This stresses the critical need for cyber-secure controllers for today's power electronics.

In Chapter 2, the 40-pin and 60-pin pass-through boards were fabricated and installed in the PV inverter. Using these boards, the acquisition of signals from the unmodified PV inverter was completed by observing the start-up sequence and limiting the inverter at 10kW. Each signal was closely monitored and documented for the development of the interface boards.

Chapter 3 details the design procedure for the UCB interface boards. Using the results from Chapter 2, a list of design parameters was created. Then, these design considerations were translated to the schematics and overall PCB design. The PCBs were fabricated, tested, and installed in the PV inverter. This chapter also discusses some other design modifications to the overall inverter design.

With the modifications, the integration of the Unified Control Board was successful. The software integration team was able to run the PV inverter at low power and receive feedback signals from the various sensors on the PV inverter using the code they developed. With this task competed, further integration of cyber-secure controls can be completed.

4.2 Recommendations for Future Work

The work presented in this honors thesis could be continued with the following recommendations:

- Interface board redesigns to allow for easier mounting in the newly modified system.
- Pins for the 15V and 5V power connections that were originally pass-through only could be changed to terminals allowing for easier interface with the power supplies included in the new modified design.

The integration of the above recommendations would provide a better mounting solution and cleaner install into the modified inverter.