





A Photovoltaic MPPT Charge Controller Real-Time Testbed for Cybersecurity Applications

Isaac Bagley , Noah Braasch , Pablo Gomez , Shameek Bhattacharjee 

Western Michigan University*

Email: pablo.gomez@wmich.edu*

Abstract—The increasing deployment of distributed energy resources (DER) over the last decade is a great ally to combat climate change and strengthen the grid during increasingly common extreme weather events. However, DER systems, combined with the ongoing transition to a digital power grid, also pose substantial cybersecurity threats. One of the most common communication protocols used in DER integration is the Distributed Network Protocol 3 (DNP3), which is known to have many security vulnerabilities. Thus, it is essential to investigate cyberattack behaviors and mitigation on power systems using DNP3. In this paper, we designed and implemented a cybersecurity testbed for a simulated photovoltaic (PV) maximum power point tracking (MPPT) charge controller. Our testbed uses an MPPT charge controller simulated on a Typhoon HIL602+ real-time simulator with a real DNP3 communication connection over TCP/IP, allowing for safe and efficient monitoring and manipulation of data traffic between the simulated hardware and supervisory control and data acquisition (SCADA) systems.

Keywords—Cybersecurity, Testbed, Real Time, Simulator, DNP3 Protocol, SCADA, Photovoltaic System, Maximum Power Point Tracking

I. Introduction

Electric power grids are the largest controlled industrial systems in existence. Large-scale grid operation requires complex controls and considerations to maintain system reliability. One such consideration is the use of communication systems to control physically separated devices from a centralized location. In power systems, one of the major communication protocols used for such controls is DNP3 [1].

DNP3 allows for telemetry data from multiple points (outstations) within the grid to report to a centralized decision-making hub (master). While this is useful for controlling a distributed network, it also introduces vulnerabilities, which a malicious individual could exploit to hinder the safe and effective operation of the system [2]. In addition, DNP3 is one of the only 3 communication protocols accepted for DER interoperability

according to the main standard for interconnecting distributed resources to power grids, IEEE Std. 1547-2018 [3]. Therefore, as its use in real-world systems increases, it is of paramount importance that we study the cybersecurity of DNP3.

On the other hand, power systems if mismanaged pose a variety of threats to users; not least among these is physical harm to end users and incapacitation of electrical systems. Hence, it is important to consider the safety of researchers when conducting tests on power systems. The large-scale nature of power systems also prevents easy experimentation and research involving them. Real-time simulation is a solution to maintain the precision and accuracy of testing at near real-world levels while also preserving the safety of researchers and remaining logistically feasible. For this reason, real-time simulation testbeds of power systems which include real communications hardware are necessary to examine the limitations and benefits of particular power systems and communications protocols.

This paper proposes the design and implementation of a testbed to study the effects of cyber-attacks on power systems with the Typhoon HIL602+ (HIL device) real-time hardware-in-the-loop (HIL) simulator, by harnessing the real-time circuit simulation capabilities of the HIL device along with real DNP3 communication. Specifically, we develop a circuit that represents a single node in an off-grid power system; implemented with control signals and telemetry being sent to a physically and electronically separate human-machine interface (HMI) control system, using the DNP3 protocol supported over a Transmission Control Protocol and Internet Protocol (TCP/IP) connection. The power electronic system represented in the testbed is a photovoltaic (PV) Maximum Power Point Tracking battery charge controller.

In addition to the DNP3 HMI, the simulator can also be interfaced through the HIL device's host computer's SCADA panel. In the system, the SCADA works as a

part of the HIL simulation to achieve the following: (i) display the values measured from the simulation in real time; (ii) provide inputs to the simulation, such as a change in irradiation of the PV cell or a change in load resistance. In a real system, these inputs' values are dependent on outside factors, such as the daylight cycle or the actions of end users, so they are not the target of cyberattacks. Since these quantities are not the target of cyberattacks and are independent of the controller state, their control is not sent through the communication layer to the offsite controller. Instead, the user manually controls all changes in load resistance, solar panel irradiance, and temperature through either the graphical interface on the HIL SCADA panel or via Python scripts. For the test cases in our paper, these quantities remain constant. For the test cases presented in this paper, the following are the subjects of simulated cyberattacks: (i) the signals connecting the MPPT charge controller to the battery, enabling the charge controller, and (ii) the signal connecting the battery to the discharge resistance.

II. Testbed Network

A. Testbed Network Topology

Fig. 1 shows the communications, control, and electrical networks used in the proposed testbed, as well as an avenue for a man-in-the-middle (MITM) attack. In an MITM attack, a malicious entity intercepts data between a source and destination that can be read or modified before sending it to the destination [4]. The gray background in Fig. 1 denotes parts of the testbed that are emulated by the HIL device. This includes the electrical circuit and the DNP3 outstation (i.e., DNP3 clients/slave devices) of the communication network.

Arrows outside of the gray box represent all digital signals outside of the HIL device that are transmitted with DNP3 over TCP/IP on the local area network (LAN). The DNP3 master station is emulated with open-source software, CDOAN-DNP3 (CDOAN) [5]. CDOAN allows a Windows-based PC to communicate using DNP3 with a DNP3 outstation over TCP/IP. In the testbed, the DNP3 master station receives data such as PV power output and load current from the simulated circuit in real time and responds by making control decisions. In this case, the DNP3 master station is configured to toggle the state of a) a contactor connected to a load resistance, b) a contactor connected to a discharge resistance, and c) an enable signal to the boost converter in the simulated PV circuit.

B. MPPT Circuit Topology

The circuit used in the testbed is a boost converter with an MPPT algorithm example from Typhoon HIL

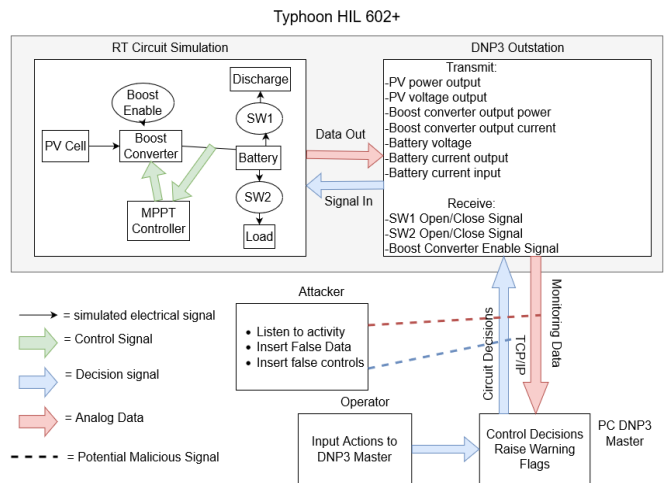


Fig. 1. Network Diagram of the Testbed

[6] with augmentations made for use with DNP3 communication and control. The testbed circuit, as shown in Fig. 2, is comprised of a PV generator, a boost converter, a battery, a load resistor, and a discharge resistor. The PV cell is a model of a Jinko JKM200M-72 200-watt panel and generates power based on irradiance and temperature. Both of these variables can be controlled through the Typhoon HIL SCADA interface throughout the simulation in real time. The details of the PV generator used in the simulation are listed in Table I. The boost converter is controlled by an MPPT controller using a perturb and observe (P&O) control algorithm, which works by continuously observing and comparing power and voltage measurements at present with samples taken previously, and inducing a small change to move the power point. If the change leads to measurements closer to that of the maximum power point (MPP) output of the PV, then the controller continues in the same direction. If the change leads to measurements further away than that of the MPP, the controller perturbs negatively [7]. The battery is used for energy storage; its physical parameters are listed in Table II. Its discharge vs. voltage curve is shown in Fig 2. The resistive load and the discharge resistor can be disconnected or connected from the system via independent contactors.

Table I: Photovoltaic Parameters

Open Circuit Voltage	45.6V
Short Circuit Current	5.8 A
Number of Cells	72
Temperature Coefficient of Short Circuit Current	0.232%

The battery charge percentage is approximated by reading the voltage across the battery, and the current flow from the PV cell to the battery is turned off once it reaches 100%. We accomplish this using a DNP3 signal

Table II: Lead-Acid Battery Parameters

Nominal Voltage	48V
Capacity	10 Ah
Full Charge Voltage	51.84V
Internal Resistance	0.12 Ω
Capacity at Nominal Voltage	50%

to turn off the battery charge enable signal once the battery reaches 52V. For controlling the MPPT charge control circuit examined in the paper, the enable signal is set to OFF once the battery voltage reaches 52V to avoid overcharging and ON again if the battery output voltage drops to 48V, which is equivalent to a 50% reduction in charge, as shown in Fig. 2.

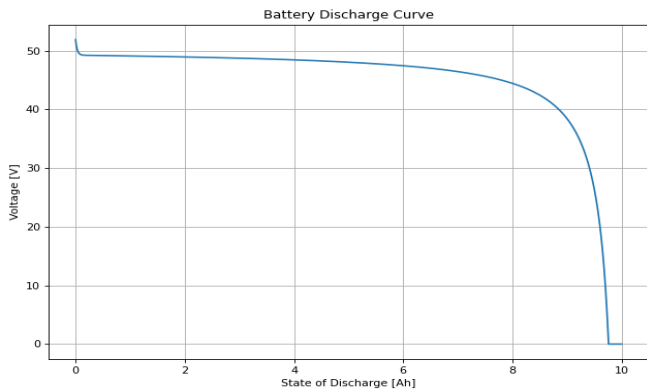


Fig. 2. Battery Discharge Curve for the Battery in Simulation [6]

The purpose of the boost converter enable signal is to keep the battery above 50% charge to preserve the battery's longevity [8]. The load and discharge resistances are each connected to their contactor, which is remotely controlled by a signal from the DNP3 master that the DNP3 outstation acts upon. The decision for opening/closing the contactors is currently made by the user at the human-machine interface (HMI), but this function could be automated for future testing. The DNP3 outstation tracks key circuit performance quantities, such as power output of the PV cell (PV Power), output power of the battery (Power Out), battery voltage level (Batt. Voltage), current output from the battery (Batt. Current), current output through the load (Output Current), current through the discharge resistor (Discharge Current), voltage supplied by the PV (PV Voltage), and battery percentage charge (Batt. %). Table III illustrates how these quantities are configured to output through the simulated DNP3 outstation.

Not all signals are controlled by the master. Since there is latency introduced in the communication due to the need for a macro and the inherent latency of TCP/IP [9], the circuit also needs local control to ensure smooth operation over small time changes. This is

accomplished through the use of the MPPT controller using the P&O algorithm. This controller operates independently of DNP3 to control the output of the boost converter at the center of the MPPT charge controller. The effect of the MPPT controller can be cut out of the system through the use of the Boost Converter Output Enable signal, which is controlled by DNP3. Fig. 3 shows a circuit diagram detailing which signals are measured and controlled by each system.

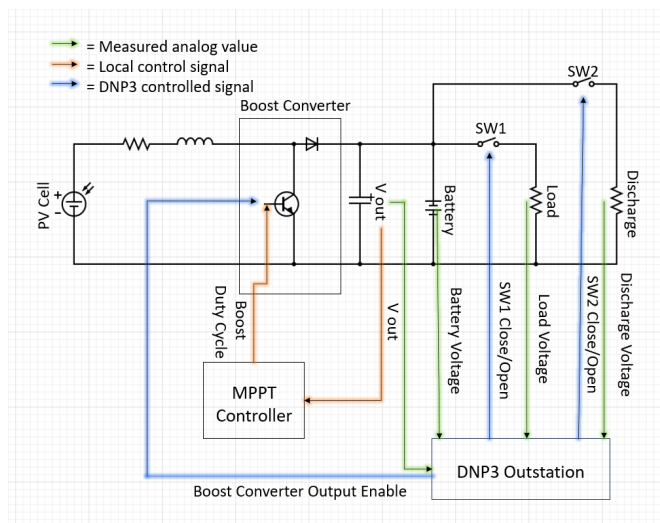


Fig. 3. Simplified Control and Circuit Diagram of the Testbed.

C. Typhoon-HIL Outstation Setup

In the Typhoon-HIL schematic, each point of measurement is connected to an input of a nine-input bus-join component. This allows multiple data points to be sent through a single analog input on the DNP3 outstation. The output of the bus-join is connected to the analog input of a DNP3-Outstation component. Because contactors are controlled by Boolean values and DNP3 sends binary values, which are not implicitly converted in Python, a translation is necessary to allow remote control through binary values from DNP3. For the testbed, this was achieved through a macro on the Typhoon HIL SCADA panel that reads the binary input from the DNP3 outstation every 500 ms and closes the corresponding contactor if the input is a 1, or opens it if the input is a 0.

The polling rate for reading the DNP3 input is set to 500 ms since this is the shortest time slot available in the predefined SCADA macro from Typhoon HIL that did not return simulation errors from overrunning the time slot on long simulation test cases. A time slot overrun freezes the SCADA panel and automatic data collection for the HIL device, but it does not crash the simulation. After an overrun, the DNP3 master still

receives up-to-date information from the outstation and the simulator, but this data is not reflected on the SCADA outputs for the HIL device. As a precaution, the 250 ms time slot, the shortest time slot and fastest polling available in the HIL device was abandoned to preserve the integrity of the data collected through automatic data collection. The solution of moving to the 500 ms time slot allows the data to be recorded accurately throughout an hours-long simulation at the cost of an extra 250 ms of latency between DNP3 commands being issued from the master and changes being reflected in the real-time simulation. However, in some tests, the simulation utilized over 75% of the 500ms time slot, so it is likely that this would have to be increased again for the investigation of more complex electronic circuits or control systems.

The outstation component is configured to have a local DNP3 address of 1024. The outstation is set to output 9 analog values and accept 3 binary input values. The configuration of the analog inputs on the outstation is shown in Table III, Similarly, the binary input configurations are shown in Table IV.

Table III: Analog Input Configuration

Name	Index	Static Variation	Event Variation	Class
Reference Voltage	0	Float W/ Flag	32-bit w/ time	1
PV Power	1	Float W/ Flag	32-bit w/ time	1
Power Out	2	Float W/ Flag	32-bit w/ time	1
Batt. Voltage	3	Float W/ Flag	32-bit w/ time	1
Batt. Current	4	Float W/ Flag	32-bit w/ time	1
Output Current	5	Float W/ Flag	32-bit w/ time	1
Discharge Current	6	Float W/ Flag	32-bit w/ time	1
PV Voltage	7	Float W/ Flag	32-bit w/ time	1
Batt. %	8	Float W/ Flag	32-bit w/ time	1

Table IV: Binary Output Configuration

Name	Index	Static Variation	Event Variation	Class
Contactor Enable	0	Group 10 Var 2	Group 11 Var 2	1
Discharge Enable	1	Group 10 Var 2	Group 11 Var 2	1

D. DNP3 Master Station Setup

CDOAN-DNP3 (CDOAN) is a free, Windows-based DNP3 simulator and test tool capable of simulating a DNP3 master and outstations. For the testbed, we configure CDOAN to act as a DNP3 master, issuing control commands and reading telemetry data from the HIL device, which acts as an outstation. CDOAN is capable of communication through several communication layer protocols, such as TCP and UDP. In the case of the proposed testbed, TCP/IP is used since it most closely resembles what is recommended for use in industry [10].

The HIL device is automatically assigned a unique IP address and, by default, communicates over port 20000. These values are entered into the Outstation

Address box and Network Port box, respectively, in the CDOAN configuration window. In CDOAN, the source destination is set to 1, and the outstation address is set to 1024 to match the HIL device configuration. Upon enabling communication between the two devices, the point data window within CDOAN is populated with the analog output data automatically upon receiving the first successful DNP3 communication from the outstation. The control commands are configured by navigating to the CDOAN Master Station Configuration window and adding three binary direct control requests with on-demand frequency and index values of 0, 1, and 2, respectively, as seen in Table V. The command to close or open the contactor is sent by selecting the corresponding latch-on or latch-off value under the control relay output block (CROB) dropdown box and clicking send in the CDOAN GUI.

III. Sample Simulated Attacks

Under ordinary conditions, the MPPT controller makes many control decisions for the circuit automatically based on its perturb and observe algorithm. Telemetry data is sent to the DNP3 master to monitor the operation of the circuit. The battery powers a static 1000 Ω load through a connection in parallel, which can be disconnected by the same DNP3 master. In future cases, this load could be varied during simulation using the Typhoon HIL SCADA interface. In the case of the battery being completely charged, or with a voltage of 52V, as shown in Fig. 2, the master takes the action of turning off the enable signal to the boost converter to ensure that the battery is not overcharged. Once the battery drops below 50% charge, or 48V, as shown in Fig. 2, the enable signal is reasserted by the master, and battery charging resumes.

In addition to the enable signal, the master also controls the connection to the load. This connection is made when the battery has over 50% charge, or when it exceeds its nominal voltage of 48V (Table II). Under normal operation, the battery is not allowed to go under its nominal voltage with the load connected to preserve battery life [8]. This can be manually overridden by the master at any time, however. A potential real-world situation that would cause an override is if the battery were used to power a critical device at a time when the PV is not able to generate electricity, such as during nighttime.

The circuit contains an extra safety mechanism in the form of a battery discharge resistor. This resistor is 5 Ω and can be connected by the master to discharge the battery in the case that the enable signal does not work to stop the flow of current from the PV to the battery once the battery is fully charged. The value of 5 Ω is

Table V: CDOAN Master Configuration

Name	Type	Request	Variation	Frequency	Qualifier	Index	CROB
Initial Response	CLASS	1/2/3/0	All Class	Once	All	-	-
Class 0-3 Polling	CLASS	1/2/3/0	All Class	Periodic	All	-	-
Class 1-3 Polling	CLASS	1/2/3	Class 123	Periodic	All	-	-
Load Contactor	CONTROL	Binary Direct	1-Command	On-Demand	Point Index	0	Latch Off
Discharge Contactor	CONTROL	Binary Direct	1-Command	On-Demand	Point Index	0	Latch Off
Boost Converter Enable	CONTROL	Binary Direct	1-Command	On-Demand	Point Index	0	Latch Off

selected to enable a timely discharge of the battery during testing. In normal operation, this resistor would be connected only when the battery is above 52V or 100% charge, and disconnected again once the battery is below 49.3V, or 90% charge, as shown in Fig. 2. The connection of this resistor in parallel with the load resistor makes the total resistance for the system an equivalent of 4.975Ω . Reduced resistance to the battery causes a large amount of current to flow through the elements connected to the battery, rapidly discharging the battery. In order to not exceed a potential current limit for the load, the load should be disconnected before the discharge resistor is connected.

For this paper, a worst-case scenario is assumed where the 50% battery charge limit on load connection is overridden and the battery has run down to 15% of its total capacity by the start of each simulation. All test cases use a value of 1000 W/m for solar irradiance and a panel temperature of 25°C, both of which remain constant throughout the simulation.

A. Normal Circuit Behavior

In this section, we observe the ability of the system to charge the battery from a 15% charge starting point while still powering the load. As seen in Fig. 4, the circuit charges the battery fully to 52V and then regulates the voltage between 52V and 48V using the enable signal to the PV connection to the battery. Battery charging happens slowly and in accordance with the battery discharge graph (See Fig. 2). The PV voltage is seen as an indicator of when the PV is disconnected from the battery. The PV disconnection corresponds to the point at which the battery voltage begins to decrease. During the period that the PV is connected, the MPPT controller regulates its output within a 0.3V range from 35.4V and 35.7V. Disconnecting the PV makes the PV voltage jump to its open circuit voltage, as shown when the PV is disconnected at 7920 seconds. When operating correctly, even with the worst-case scenario of the battery protections being overridden (allowing the battery charge to get as low as 15%), the MPPT boost charger control system is capable of providing a consistent voltage to the load within 10% of the battery's nominal voltage.

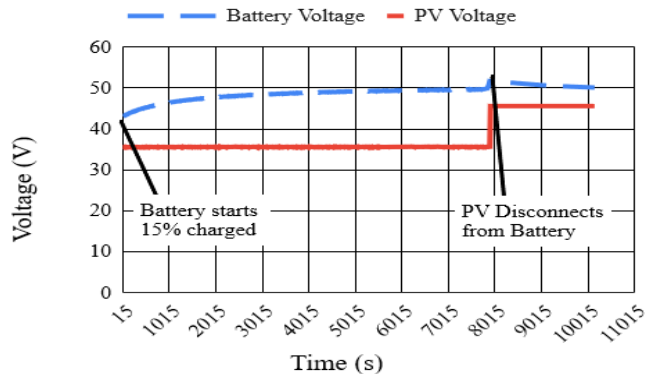


Fig. 4. Battery Voltage Over Time During Normal Operation of the Circuit.

B. Additional Discharge Attack

In this attack, a false discharge contactor close signal is asserted constantly until the battery discharges completely. This causes the battery to be unable to power the load, even though the PV is still connected to the load through the boost converter. As shown in Fig. 5, the battery voltage immediately drops from its starting voltage and continues to drop until the battery loses charge and the load is only powered by the PV output. The output voltage from the PV is not enough to keep the battery at the same charge while the discharge resistor is attached. This is the way the circuit is intended to operate in a potential overcharge scenario, but the attacker has hijacked this safety feature to discharge the battery.

Since the total resistance in the circuit is low, the current limitation of the PV precludes it from supplying the load with a consistent voltage near the full charge voltage of 52V, or the nominal battery voltage of 48V. In fact, the current limitation of the PV begins impacting the circuit after only 565 seconds, as shown in Fig. 5. The PV, powering the circuit on its own once the battery is discharged, settles in to supply the load at around 26.6V by 3510 seconds, with slight fluctuations due to changes in input from the MPPT controller. This reduction in voltage also represents a reduction in supply current to the load of 44% below the supplied current by the battery and PV when the battery is at its nominal voltage. The inability to supply a consistent

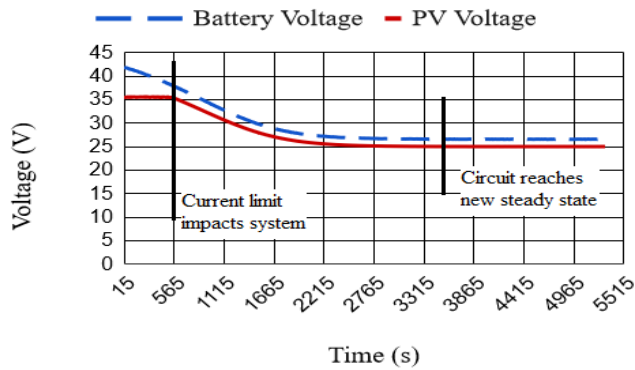


Fig. 5. Battery and PV Voltage Over Time in the Additional Discharge Attack

voltage and current means that the MPPT controller has failed due to an action from the simulated attack.

C. Battery Overcharge Attack

In the battery overcharge scenario, the simulated attack interrupts the enable signal communicated from the master so the battery does not stop charging at an appropriate time. Fig. 6 shows the effect of this attack on the battery voltage. The voltage waveform follows the same trend shown in Fig. 4 until the battery reaches its full charge state of 52V at 7920 seconds. At that point, the voltage increases exponentially, doubling in just 90 seconds and reaching a maximum voltage of 367V by 10185 seconds. This is over 6 times the nominal voltage of the battery and would cause many issues in a real-world system. Since the battery is in parallel with the load, an increase in battery voltage is directly related to an increase in load current.

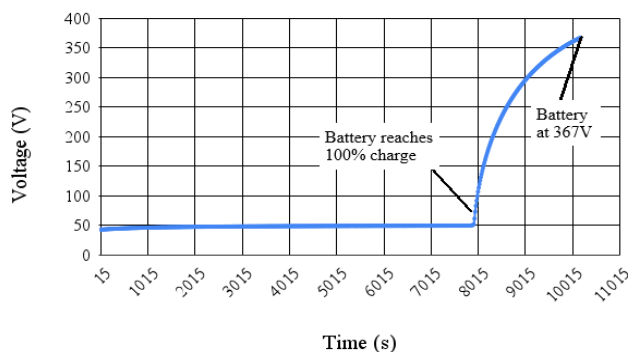


Fig. 6. Battery Voltage Over Time in the Battery Overcharge Attack.

IV. Conclusions and Future Work

In this paper, we have developed a testbed for a PV MPPT boost charge controller system through the use of real-time simulation and DNP3 communication. This

system is capable of emulating cyberattacks using the real DNP3 communications of the system, directly affecting the simulated electrical system's performance.

The approach of using real-time simulation for the circuit elements of the testbed allows for more rapid testing of different power systems using the same communication interface through DNP3 once a more robust method for emulating cyber attacks is implemented. This approach will also help in the development of attack mitigation strategies due to the ability of the testbed to rapidly change circuit and control parameters for testing novel mitigation strategies.

Acknowledgment

The authors thank the Summer of Power Engineering Research Initiation and Training (SPERIT) program at WMU Power Lab, funded through NSF grant #2138408, for providing support for this research work. This work is also supported by the US Department of Energy through grant DE-CR0000029.

References

- [1] H. Huang, C. M. Davis, and K. R. Davis, "Real-time power system simulation with hardware devices through dnp3 in cyber-physical testbed," in *2021 IEEE Texas Power and Energy Conference (TPEC)*, 2021, pp. 1–6.
- [2] S. East, J. Butts, M. Papa, and S. Sheno, "A taxonomy of attacks on the DNP3 protocol," in *Critical Infrastructure Protection III*, C. Palmer and S. Sheno, Eds. Springer Berlin Heidelberg, 2009, pp. 67–81.
- [3] "IEEE standard for interconnection and interoperability of distributed energy resources with associated electric power systems interfaces," *IEEE Std 1547-2018 (Revision of IEEE Std 1547-2003)*, pp. 1–138, 2018.
- [4] F. Callegati, W. Cerroni, and M. Ramilli, "Man-in-the-middle attack to the HTTPS protocol," *IEEE Security & Privacy*, vol. 7, no. 1, pp. 78–81, 2009.
- [5] Jack Verson, "CDOAN-DNP3." [Online]. Available: <https://www.cdoan.com/dnp3>
- [6] Typhoon HIL, "Typhoon HIL control center." [Online]. Available: <https://www.typhoon-hil.com/>
- [7] M. Kamran, M. Mudassar, M. R. Fazal, M. U. Asghar, M. Bilal, and R. Asghar, "Implementation of improved perturb & observe mppt technique with confined search space for standalone photovoltaic system," *Journal of King Saud University-Engineering Sciences*, vol. 32, no. 7, pp. 432–441, 2020.
- [8] M. R. Palacín and A. de Guibert, "Why do batteries fail?" *Science*, vol. 351, no. 6273, p. 1253292, 2016.
- [9] N. Kasoro, S. Kasereka, G. Alpha, and K. Kyamakya, "ABCSS: A novel approach for increasing the TCP congestion window in a network," *Procedia Computer Science*, vol. 191, pp. 437–444, 2021.
- [10] VTScada, "DNP3: TCP versus UDP," Trihedral Engineering Limited, Tech. Rep., 2023.