DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof. Reference herein to any social initiative (including but not limited to Diversity, Equity, and Inclusion (DEI); Community Benefits Plans (CBP); Justice 40; etc.) is made by the Author independent of any current requirement by the United States Government and does not constitute or imply endorsement, recommendation, or support by the United States Government or any agency thereof.

A Real-Time Testbed for Smart Inverter Cyber Security Studies

Alfred Batu, Badr Semia, Lucas Ling

Advisor: Pablo Gomez

ECE 4820 ELECTRICAL & COMPUTER ENGINEERING DESIGN II

APRIL 25, 2024

Table of Contents

Abstract—Distributed energy resources (DER) have become a popular solution to modern-day issues surrounding the efficiency and reliability of power generation, as well as climate change concerns. Energy centers are shifting towards incorporating smart inverters with embedded functionalities such as high voltage ride through (HVRT), low voltage ride through (LVRT), active and reactive power compensation. However, the integration of smart inverters leave DER systems highly vulnerable to cybersecurity threats. The distributed network protocol 3 (DNP3) is a common method of communication between grid-tied hardware. Despite its popularity, the level of security leaves all hardware connected to the grid at risk of severe cyber-attacks. Thus, it is important to study any potential cybersecurity threats towards grid-tied smart inverters to mitigate cybersecurity vulnerabilities and refine existing cyber-security protections. This report describes the proposed testbed design to study cybersecurity threats to smart inverters. The testbed utilizes a real-time simulation case in RSCAD that includes a grid-tied wind turbine (WT) topology featuring two back-to-back two-level voltage source converters (BTB,2L-VSCs) and a permanent magnet synchronous machine (PMSM). The simulated case runs within the NovaCor real time digital simulator (RTDS). This report focuses on the design and implementation of a single module of the GTNETx2 card as a distributed network protocol and the configuration of an IEE 1518 DNP database file that includes input and output variables mapped to different connection points in the grid that transmit and receive discrete, analog, and binary signals on command. This allows realistic emulation of the communication between the smart inverter and the grid for cybersecurity studies.

Final Report Disclaimer

This report was generated by a group of engineering seniors at Western Michigan University. It is primarily a record of a project conducted by the students as part of the curriculum requirements for being awarded an engineering degree. Western Michigan University makes no representation that the material contained in this report is error-free or complete in all respects. Therefore, Western Michigan University, its faculty, its administration, or the students make no recommendation for the use of said material and take no responsibility for such usage. Thus, persons or organizations who choose to use said material for such usage do so at their own risk.

Senior Design Project Release Form

WESTERN MICHIGAN UNIVERSITY

COLLEGE OF ENGINEERING AND APPLIED SCIENCES

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

KALAMAZOO, MICHIGAN 49008

SENIOR DESIGN PROJECT REPORT RELEASE FORM

In accordance with the "Policy on Patents and Release of Reports Resulting from Senior Design Projects," as adopted by the Executive Committee of the College of Engineering and Applied Sciences on Feb. 9, 1989, permission is hereby granted by the individuals listed below to release copies of the final report written for the Senior Design Project entitled:

PROJECT TITLE: **A Real-Time Testbed for Smart Inverter Cyber Security Studies**
____-__________

PROJECT SPONSOR* Did this project have a sponsor? YES

Contact person and email address &/or telephone: pablo.gomez@wmich.edu

Company Name: WMU InterEnergy Center

Design team has requested the sponsor to verify in writing to the course coordinator that all promised deliverables have been received. YES____ NO____ (please check)

TEAM MEMBERS NAMES:

NAME PRINTED	NAME SIGNED	DATE
BADR SEMIA		4/25/2024
ALFRED BATU		4/25/2024
LUCAS LING		4/25/2024

* Those teams with a sponsor must have the sponsor provide the **course coordinator** with written evidence that they have provided the sponsor with a copy of the final project report as well as other items that the team has promised to the sponsor. The evidence could be a short note via email, fax, or US mail from the sponsor indicating receipt of a copy of the report and all promised deliverables.

1. Introduction

The electric grid is an intricate system that has a profound influence on people's daily lives. The positive climate impact alone is significant enough to promote granting additional resources to increase the electric grid's efficiency and availability [1]. To achieve the goal of high-power generation efficiency and availability of an electric grid, specifically those that include a grid-tied central smart inverter, a real-time simulation testbed is necessary to better understand any present and future cybersecurity threats [2]. The method of communication best suited for this application, according to the IEEE 1547-2018 for interconnection and Interoperability of distributed energy resources, is Distributed Network Protocol 3 (DNP3) [4]. The protocol will grant the user read or write control over different power variables to simulate a cyberattack and monitor the smart inverter's behaviour in response to the attack.

The RSCAD simulation includes an interactive SCADA system with manual input controls such as sliders for global parameter adjustments, system operating voltage, rated line-to-line voltages (VLLs), and others. It also features adaptive indicators and plots for voltage and current variables during a live simulation. Most of these settings remain constant during simulations to ensure consistent results. The signals of importance include smart inverters' control signals, which detect high, low voltage, and trigger a corrective function to the voltage change. The testbed is a safe environment where professionals and enthusiasts can experiment and study smart inverter cyber vulnerabilities without risk of injury or death, which could be an important concern if testing were done on a physical live system.

This project report compiles the design and implementation of a DNP3 communication module of the GTNETx2 card and the configuration of the DNP database I/O to simulate cyber-attack by integrating all related physical and simulated hardware in a power hardware-in-the-loop (PHIL) to ensure high-fidelity of results [3]. The IEC 61850-90-7 standard has effectively defined the capabilities of smart inverters [5]. However, there is a lack of a clear process detailing the testing procedures to validate smart inverter cybersecurity protections; this testbed will be a step towards expanding the understanding and testing of grid-tied smart inverter cybersecurity vulnerabilities.

1.1 Overview

1.2 Background

Modern RES include smart inverters with complex and sensitive controls that facilitate the integration of the RES into the grid. Studying their cyber vulnerabilities will help achieve the goal of uninterrupted operation and reduction of energy generation costs. The smart inverter cybersecurity test bed is a helpful tool in achieving these goals.

1.3 Need Statement

The rising number of smart inverter integrations within wind and solar electric grids creates a pressing need to protect electric grids against cybersecurity attacks. The world’s energy centers are moving towards incorporating DERs (distributed energy resources), which offer an environmentally friendly way of generating power to support the current electric grid. However, the safety and operation of the energy grid are imperative during this migration cycle from traditional energy generation methods to new renewable energy sources. Therefore, to better assist in maintaining safety and operation, the first step is to protect the facilitating component between the source and the grid, such as smart inverters, from cyberattacks. To do so, it is necessary to have a testing environment that utilizes a current industry standard smart inverter, where engineers can simulate cybersecurity attacks to validate the inverter’s functionalities, such as low voltage ride-through, high voltage ride-through, frequency ride-through, and active and reactive power compensation.

2. Specifications

This section provides an overview of the main specifications regarding physical characteristics and functionality.

2.1 Physical Characteristics

The project involves the utilization of a real-time digital simulator (RTDS) and grid modeling software (RSCAD) to conduct power hardware-in-the-loop (PHIL) testing. The project's main objective is to isolate the communication signals transmitted through an outstation. Multiple connection points to the grid will be established to test the built-in protection capabilities of smart inverters.

Most of the project activities are centered around real-time simulations. However, there are physical hardware components integrated into the simulations, and communication hardware allows for read/write capability to defined inputs and output tags. The RTDS NovaCor station includes a GTNET x2 DNP3 card module. The necessary model hardware is readily available in the RSCAD FX component library, and parameters can be manually configured to meet specific hardware specifications. The RTDS NovaCor station is linked to a computer by a hard wired ethernet connection, and through this link, the database server embedded in the DNP3 outstation module will handle all the output and input signals of the smart inverter. This is accomplished by a hardware-in-the-loop approach whereby the RSCAD DNP3 outstation module interfaces with the PAsuite simulated master as shown in Figure 1.

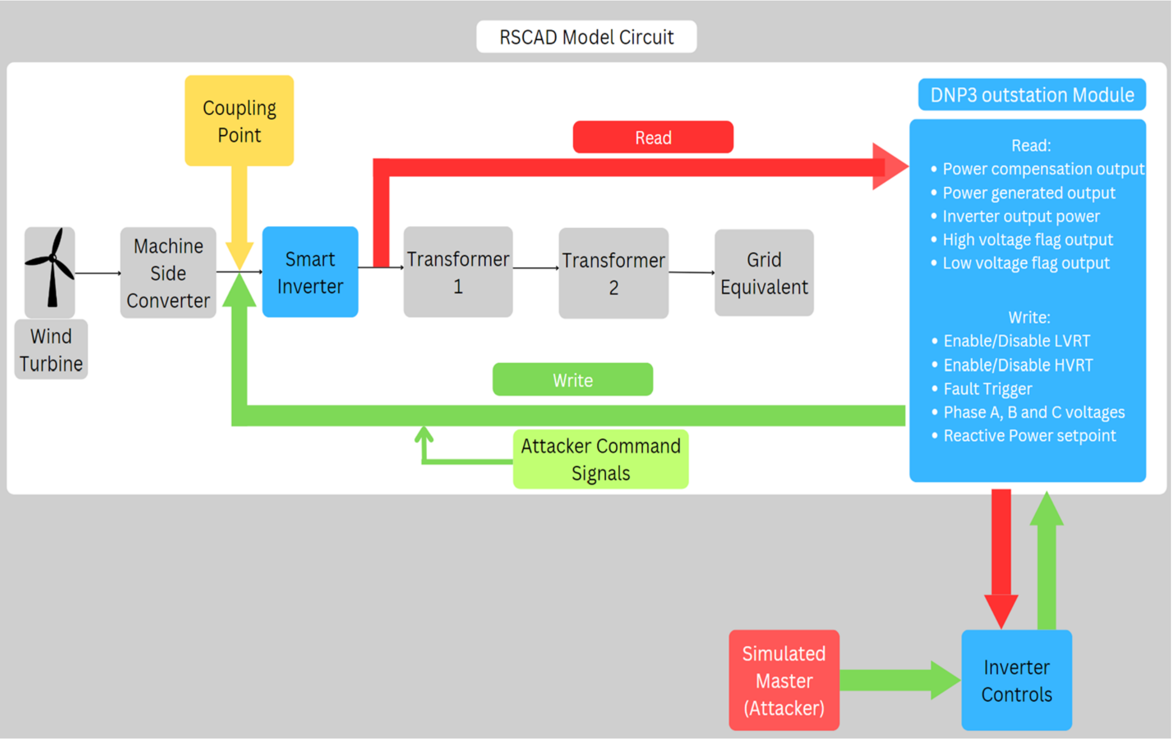


Figure 1: The system Diagram.

2.2 NovaCor and RSCAD Requirements

For the project's physical setup, there are specific requirements. The NovaCor station, in conjunction with the RSCAD FX software, is the initial requirement. The NovaCor station should be equipped to support the grid modelling software RSCAD and the various components necessary for the simulation project.

2.3 Communication Requirements

For testing purposes, a computer connected to the RTDS NovaCor station is required to configure the DNP3 communication protocol. The communication requirements are essential for the project's successful execution. When the components are correctly configured, they enable a responsive system that seamlessly exchanges data for any command signal transmitted from the master to the RSCAD outstation module.

2.3.1 Compatibility with Remote Terminal Units (RTUs)

The communication protocol DNP3 should be compatible with RTUs to ensure smooth data exchange. The RTU is the only tool capable of reading and writing data directly from the grid in real-time and making it available for an external controller to monitor and operate.

Access to Discrete Signals (ON and OFF): The system should be able to access discrete signals, such as ON and OFF signals, to grant the project's monitoring and controlling aspects.

2.3.2 Read/write Access to Analog and Binary Data

The defined tags in the RTU outstation IEE1815 database, needs to provide read and write access to analog values going into the smart inverter, these values should include input voltages and current, as well as binary signals that control ON/OFF switches.

3. Design and Implementation

3.1 Configuration of Hardware and Software

To transmit DNP 3 communication signals during HIL (Hardware in the loop) testing with RSCAD software, a Master station, and an Outstation, the GTNETx2 card hardware component should be set up as a Distributed Network Protocol DNP slave station. Additionally, the RTDS firmware must be upgraded to DNP 4.18 to allow the outstation to read and write to various grid points. This configuration allows the input and output signals to be communicated out of the RTDS simulation to the RTU slave outstation using DNP 3 communication.

The DNP 3 communication protocol has been successfully established using the GTNET hardware component in RSCAD. This component serves as a physical connection point that allows all signals to communicate within the grid through an outstation to the Master station. To ensure that signals are communicated appropriately between the outstation and the Master station, the protection and automation function tab must be configured in the RSCAD component master library. In addition, the RTDS firmware and I/O ports were configured to support the DNP 3 communication protocol and point mapping of the grid. Figure 2 shows the GTNET physical component. Also, a low-level SCADA system was used to create the Hardware in the Loop (HIL) testing, which includes an outstation responsible for generating the necessary point mapping file required for the communication of the simulation's inputs and outputs.

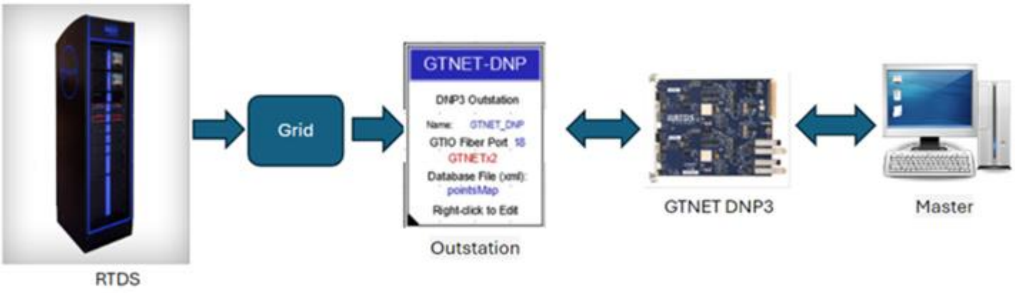


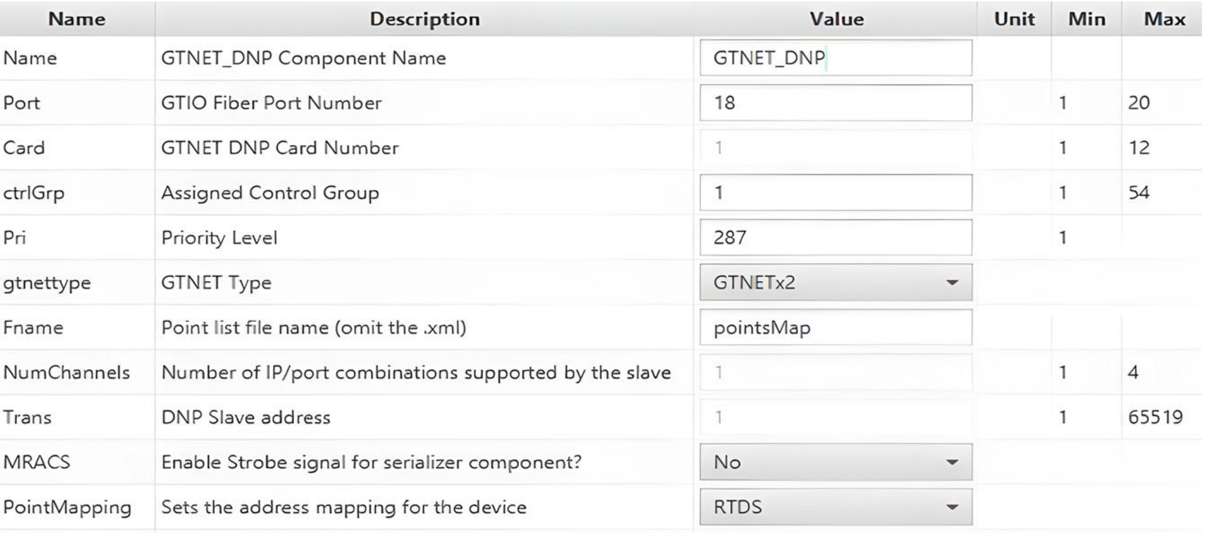
Figure 2: SCADA system components

The configuration of the NOVACOR core station's Rack, as illustrated in Table 1, is important for enabling the use of the DNP 3 communication protocol. To achieve this, it is necessary to configure the GTNET card to Port 18, which would allow for the communication of input and output signals from the RTDS simulation using DNP 3 communication. This setup ensures seamless data transactions within the system.

Table 1: I/O port configuration of the NOVACOR 1.0 Rack

CardType	IO Ports	Port connected to				
NOVACOR 1.0	Edit IO Ports	1	IO Card	+	GTFPIV2	
		2	IO Card	+	GTDIv2	
		3	IO Card	+	GTDOv2	
		4	IO Card	+	GTAIv2	
		17	IO Card	+	GTAOv2	
		18	IO Card	+	GTNETx2_DNP	GTNETx2_sv
		19	No Connection			
		20	IO Card	+	GTNET_DNP	
		21	No Connection			

Figure 3 shows the integrated GTNET-DNP RTU as an outstation set up with the wind turbine model file in RSCAD. The component name is set, and the Fiber port is set to Port 18. GTNET type is also set to GTNETx2. Note that the point map file named “pointsMap” is also created in the RSCAD files as a database for all signals within the DNP3 outstation RTU.



Name	Description	Value	Unit	Min	Max
Name	GTNET_DNP Component Name	GTNET_DNP			
Port	GTIO Fiber Port Number	18		1	20
Card	GTNET DNP Card Number	1		1	12
ctrlGrp	Assigned Control Group	1		1	54
Pri	Priority Level	287		1	
gtnettype	GTNET Type	GTNETx2			
Fname	Point list file name (omit the .xml)	pointsMap			
NumChannels	Number of IP/port combinations supported by the slave	1		1	4
Trans	DNP Slave address	1		1	65519
MRACS	Enable Strobe signal for serializer component?	No			
PointMapping	Sets the address mapping for the device	RTDS			

Figure 3 : GTNET-DNP RTU Configuration.

The pointmap configurations allow signals in the wind turbine model to be transmitted via the outstation RTU. Figure 4 illustrates the integration of a GTNET-DNP module as an outstation in the RSCAD model. The embedded IEEE 1815 database parameters provide read or write to defined grid points in the database. These grid points are presented as registers, categorized by their respective data types, such as analog, binary, counter, frozen counter, double binary, analog outputs, and binary output data registers.

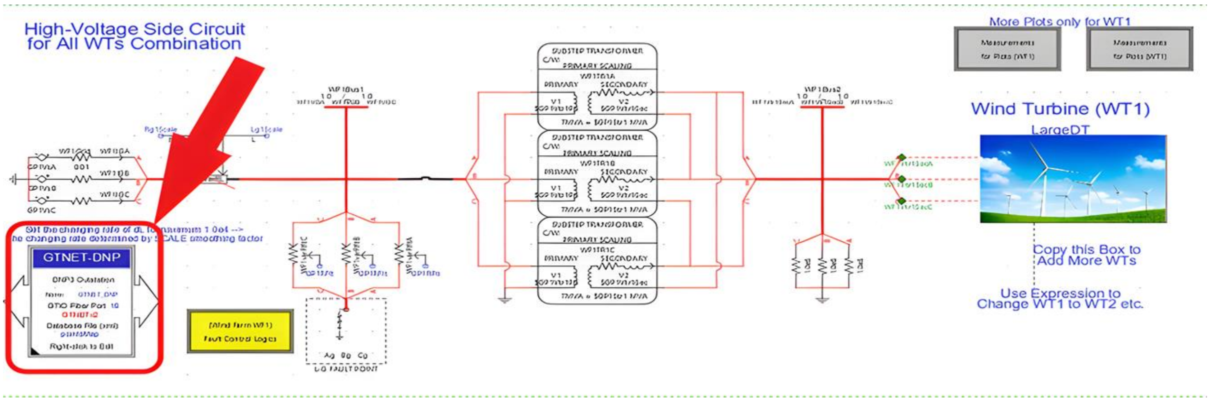


Figure 4: GTNET-DNP RTU as an outstation in the RSCAD model.

3.3 Voltage control circuits For Analog and Binary signal operation

The sequence for controlling the input AC source voltage begins with the activation of an ON/OFF button, depicted in Figure 5. This button initiates a Set-Reset (S-R) flip flop, which then triggers a pulse generator. The pulse generator is linked to a voltage multiplication process with a predefined constant value of 0.1. Additionally, there is a switch enabling the user to adjust the multiplication constant, thus modifying the phase AC input voltage.

The outstation within the model facilitates the exchange of analog signals between the coupling point of the AC bus and the Master Station. These signals encompass voltages and currents crucial for calculating positive and negative sequence voltages and currents. Disruption in these calculations can occur via the DNP 3 control signal. The Smart Inverter relies on the Per Unit (PU) magnitudes of the AC source voltages to compute DQ components. This computation aids in determining when the AC voltage control loops require reactive power. A low voltage flag is raised if the reactive power approaches its control limits, and the AC source voltage surpasses the 0.8 PU threshold. Subsequently, the AC grid voltage drops to approximately 0.885 PU to prevent overcurrent. Table 2 displays the Analog I/O signals enabling the Master station to interfere with the smart inverter's grid support functions. Among these signals are WT1Qconfilt, WT1PgenFlt, and WF1GFilt, representing the gride point reference set points for Wind turbine power generation. These signals are read-only signals; hence, the attacker, through the DNP3 master station using the protection and automation suite, can read the signals sent from the outstation RTU set up in the daft case. The data transmitted is displayed in real-time on analog meters that are connected to the signals.

Table 2: DNP3 Analog Signals (Inputs from RTDS)

Variable Name	DeadBand	DeadBand Type	Class	StaticVar	EventVar
WT1Qconfilt	1	Simple	Class1	Group30Var	Group32Var1
WT1PgenFlt	1	Simple	Class1	Group30Var	Group32Var1
WF1GFilt	1	Simple	Class1	Group30Var	Group32Var1

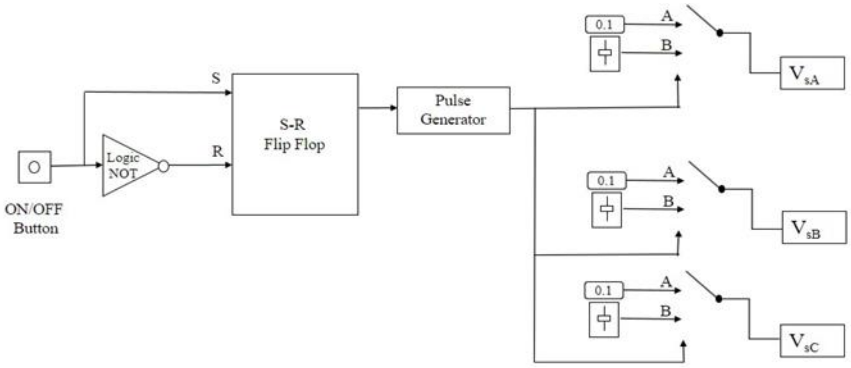


Figure 5: Input AC Source Voltage Change Control [6]

The analog signals transmitted via DNP 3 communications protocols, such as the analog output signals in Table 3, are configured in the IEEE 1815 DNP database point file via the outstation RTU set up in the daft case. The signals are signals inputs to the RTDS via the GTNETx2 card. These output signals configured provide the read and write functionality of signals transmitted via the DNP 3 communication protocol. Protection and Automation Master station is the created simulation master to simulate cyber-attacks. This will allow the user to change values of signals communicated via analog output signal register such as signals indicated below, including the frequency set points GP1freqset, Magnitude of Phase A, B and C grid point voltages GP1MagA, GP1MagB and GP1MagC respectively, to simulate changing the Per Unit magnitude of the voltage's signals as well as the wind turbine reactive power compensation reference points WT1Qacmax and VdcPURef the DC voltage Per Unit reference used in the voltage control loop of the smart inverter within the runtime simulation.

Table 3: DNP3 Analog Output Signals (Inputs to RTDS)

Variable Name	Default	Class	StaticVar	EventVar
GP1freqset	60	Class1	Group40Var1	Group42Var1
GP1MagA	1	Class1	Group40Var1	Group42Var1
GP1MagB	1	Class1	Group40Var1	Group42Var1
GP1MagC	1	Class1	Group40Var1	Group42Var1
WT1Qacmax	1	Class1	Group40Var1	Group42Var1
VdcPURef	1	Class1	Group40Var1	Group42Var1

3.4 LVRT & HVRT Control Signals

To transmit these signals using the DNP 3 communication protocol, a binary input and output signal is utilized via outstation to connect the Master station located in the Protection and Automation suite. Figure 4 presents the control grid sequence logic circuits, which also feature low HVRT (High Voltage Ride Through) and LVRT (Low Voltage Ride Through) functionalities in addition to fault recognition controls. The binary signal table and Binary output enable binary read/write control signals to be conveyed through the DNP3 communication protocols. These control signals facilitate the detection of low and high voltages by Smart inverters, with a flag sent via the master station to determine whether the low or high voltage is detected once grid voltages are increased and AC magnitudes are set. These signals can disrupt the smart inverter's functionality.

3.5 Grid Side Sequence Control Logic used in LVRT and HVRT

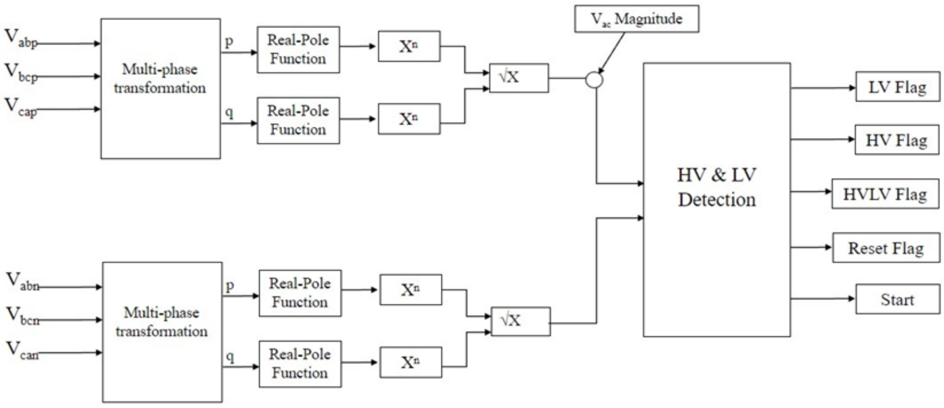


Figure 4: RSCAD Sample Control Model [6]

Tables 4 and 5 below display how Binary signals are communicated via the DNP3 outstation to enable the disruption of smart inverter control during operation. Table 4 Binary Inputs allows for signals to read via protection and automation DNP3 signals; however, these signals are inputs from the RTDS, which allow signals to be monitored, and staticVar and eventVar allow masters station to report real-time changes in the status of the binary signal in runtime simulation (on/ off). In Table 4, signals communicated are the WT1HVFlag and WTILVFlag, enabling the master station or attacker to see the status of voltage thresholds when an attack is simulated. These flags indicate the IEEE standard low and high voltage requirements parameters within the smart inverter control. **Table 4: DNP3 Binary (Inputs from RTDS)**

User Label	Variable Name	Bitmap	Class	StaticVar	EventVar
WT1HVFlag	WT1HVFlag	0	Class1	Group3Var1	Group4Var1
WTILVFlag	WTILVFlag	1	Class1	Group3Var1	Group4Var1

Binary inputs from the RTDS are recorded by the outstation and their status is mirrored to the remote master, simulating an attacker having access to the IEEE 1547- 2018 standard requirements of the smart inverter. This is achieved with the EnLVRT and EnHVRT, which are the binary signals used to enable the smart inverter controller's high voltage Ride-through and low voltage ride-through functionality. GP1VsinFlt is a binary signal used to inject a preset grid Per unit phase A, B, and C voltages. The protection and automation suite will allow these signals to be controlled via a control output relay block where signals can be turned on or off.

Table 5 below is the configuration of the binary output signals via the DNP point mapping database.

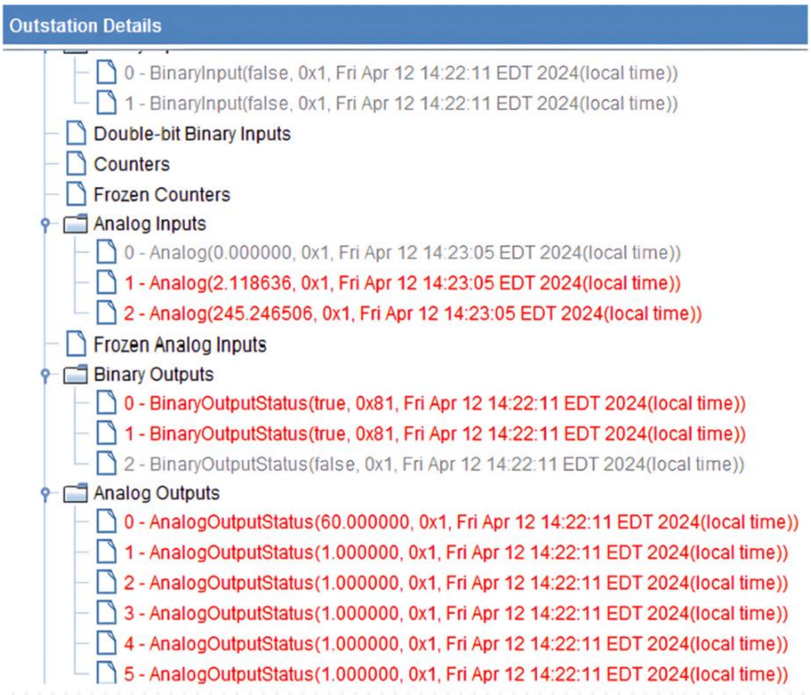
Table 5: DNP3 Binary Output (Input to RTDS)

User Label	Variable Name	Bitmap	Class	StaticVar	EventVar
EnLVRT	EnLVRT	0	Class1	Group10Var2	Group11Var2
EnHVRT	EnHVRT	0	Class1	Group10Var2	Group11Var2
GP1VsinFlt	GP1VsinFlt	0	Class1	Group10Var2	Group11Var2

3.6 Protection and Automation Suite (Simulated DNP3 Master Station)

The Protection and Automation suite is a simulated master station configured via internet IP as a remote station to allow for communication signals transmitted via DNP3 to a remote, once the wind turbine draft case is compiled and the simulation is started, the protection and automation in RSCAD utilities is used to set up a master station, the connection to the outstation is via the GTNETx2 DNP module set up within the wind turbine draft case via internet IP address and a remote port connection to the outstation.

The DNP3 master station in Figure 5 shows the outstation DNP3 master station details. The outstation details show the analog and binary inputs and output details with time stamping indicating the time the signal was sent and or received as well as the status of the I/O point. Analog values show the indicated set points and the current values in real-time. Connection status will be active when the connection is made. Each signal point is identified by the point number used in the configuration of the outstation. The Protection and Automation suite is the network interface of the attacker or user's computer and the GTNET-DNP outstation.



```
Outstation Details
        0 - BinaryInput(false, 0x1, Fri Apr 12 14:22:11 EDT 2024(local time))
        1 - BinaryInput(false, 0x1, Fri Apr 12 14:22:11 EDT 2024(local time))
    Double-bit Binary Inputs
    Counters
    Frozen Counters
    Analog Inputs
        0 - Analog(0.000000, 0x1, Fri Apr 12 14:23:05 EDT 2024(local time))
        1 - Analog(2.118636, 0x1, Fri Apr 12 14:23:05 EDT 2024(local time))
        2 - Analog(245.246506, 0x1, Fri Apr 12 14:23:05 EDT 2024(local time))
    Frozen Analog Inputs
    Binary Outputs
        0 - BinaryOutputStatus(true, 0x81, Fri Apr 12 14:22:11 EDT 2024(local time))
        1 - BinaryOutputStatus(true, 0x81, Fri Apr 12 14:22:11 EDT 2024(local time))
        2 - BinaryOutputStatus(false, 0x1, Fri Apr 12 14:22:11 EDT 2024(local time))
    Analog Outputs
        0 - AnalogOutputStatus(60.000000, 0x1, Fri Apr 12 14:22:11 EDT 2024(local time))
        1 - AnalogOutputStatus(1.000000, 0x1, Fri Apr 12 14:22:11 EDT 2024(local time))
        2 - AnalogOutputStatus(1.000000, 0x1, Fri Apr 12 14:22:11 EDT 2024(local time))
        3 - AnalogOutputStatus(1.000000, 0x1, Fri Apr 12 14:22:11 EDT 2024(local time))
        4 - AnalogOutputStatus(1.000000, 0x1, Fri Apr 12 14:22:11 EDT 2024(local time))
        5 - AnalogOutputStatus(1.000000, 0x1, Fri Apr 12 14:22:11 EDT 2024(local time))
```

Figure 5: Protection and Automation (DNP 3 Master Station) application - Outstation details

4. Design Considerations

4.1 Public Health (N/A)

4.2 Safety and Welfare

The testbed involves sensitive data used in power systems. It grants access to control strategies to disrupt the power supply of an industry-standard smart inverter. Due to the potential risks involved, robust measures should be taken to prevent unauthorized access to such equipment. It is important to ensure that all the simulation equipment's wires, cables, and components, including the RTDS and RTAC, are properly secured to prevent electrical hazards. Safety measures should be implemented to disconnect the leading power in case of an emergency or power instability during simulation.

4.3 Global Impact (N/A)

4.4 Cultural Impact (N/A)

4.5 Social Impact (N/A)

4.6 Environmental/ Sustainability

The Cybersecurity testbed features a wind turbine grid topology, The study of smart inverter cybersecurity will allow the improvement and development of cybersecurity protections of smart inverters. As cybersecurity protections of grid tied smart inverters improve, the capacity at which RES are deployed globally will drastically increase, consequently the environment will greatly benefit from the reduction of traditional power generation and increased use of RES that feature smart Inverters.

4.7 Economic

The utilization of the RTDS (Real-Time Digital Simulator) is essential when emulating industry-standard communication protocols sent between devices in a Wind Farm application. Testing the vulnerabilities of these communication signals of Smart Inverters in the industry has incurred significant costs. Therefore, having such a testbed will allow the industry to accurately forecast the vulnerability of the communications without disrupting the power of the inverter in the grid, which, in most cases, leads to losses and damage to expensive equipment.

5. DESIGN IMPACTS

5.1 Global

The real-time simulation provides valuable technical insights into the vulnerabilities of smart inverters that are commonly used in the power system industry. The simulation results can help the industry evaluate the vulnerabilities of smart inverters used in the grid network and the vulnerabilities of signals communicated using the DNP3 communication protocol. This, in turn, can facilitate the development of better safety protocols to safeguard smart inverters in operation and prevent power disruption or costly equipment repair due to cyberattacks.

5.2 Environmental (N/A)

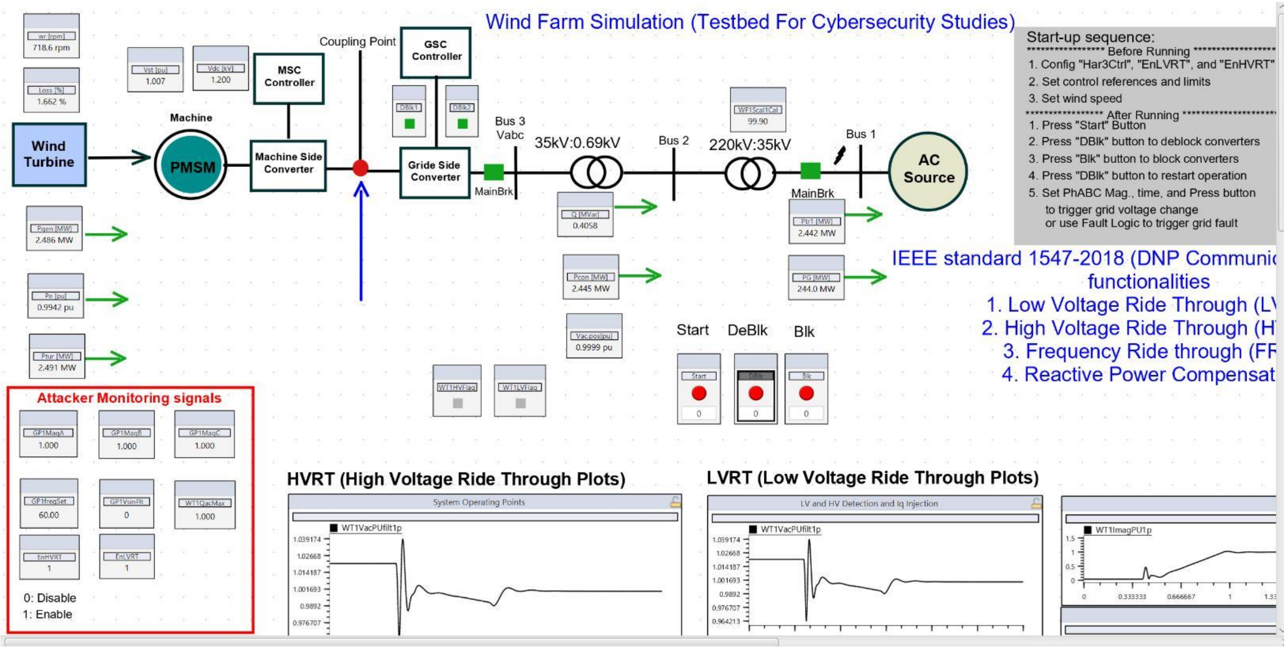
5.3 Societal

The real-time simulation results can provide an opportunity for the DER (Distributed Energy Resource) industry to gain valuable insights into the vulnerability of signals sent through the DNP3 communication protocol that can be used to mitigate potential cybersecurity risks and ensure the safe and reliable operation of the power system.

6. Designed Runtime of Testbed for Smart Inverter Cybersecurity Studies

The final runtime design incorporates the wind turbine generation modules. RTDS model is rated at 2.5 MW and includes two back-to-back 17 level VSCs (BTB, 2L-VSCs) and a permanent magnet synchronous machine (PMSM) [7]. The primary focus is on the coupling point between the DC/DC converter controller and the DC/AC smart inverter controller. The common coupling includes input parameters such as phase A, B, and C voltages that can be manipulated as a form of a cyber-attack. This cyber-attack will allow the validation of smart inverter functionalities such as low voltage ride-through (LVRT), high voltage ride-through (HVRT), and reactive power compensation.

Figure 6 below shows the wind turbine model with the power generation direction indicated by the green arrow. The power generated from the wind turbine is transmitted to the MSC converter then the grid side converter. Analog meters display the signals being monitored or controlled via DNP 3 master station. Amongst these signals are binary input signals from the RTDS that includes WT1HVFlag, WTILVFlag and binary output signals EnLVRT and EnHVRT.



Start-up sequence:

***************** Before Running ******************

1. Config "Har3Ctrl", "EnLVRT", and "EnHVRT"
2. Set control references and limits
3. Set wind speed

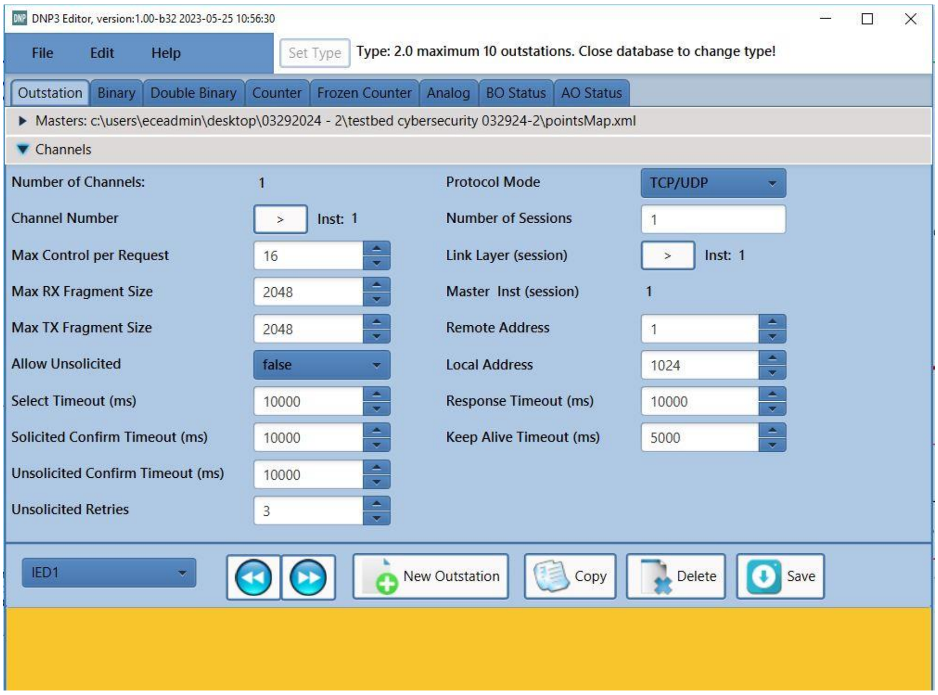
***************** After Running ********************

1. Press "Start" Button
2. Press "DBlk" button to deblock converters
3. Press "Blk" button to block converters
4. Press "DBlk" button to restart operation
5. Set PhABC Mag., time, and Press button
   to trigger grid voltage change
   or use Fault Logic to trigger grid fault

Figure 6: Wind Farm Simulation (Testbed For cybersecurity studies Runtime)

6.1 Configuration of Outstation Registers and Channel of Connection

The configuration of the outstation in Figure 7 shows the protocol mode, TCP/UDP mode of transmission, and the local address used for data transmission. However, TCP is the standard data transmission protocol used for DNP 3 data transmission. The local address can be configured to the user-desired address.



Type: 2.0 maximum 10 outstations. Close database to change type!

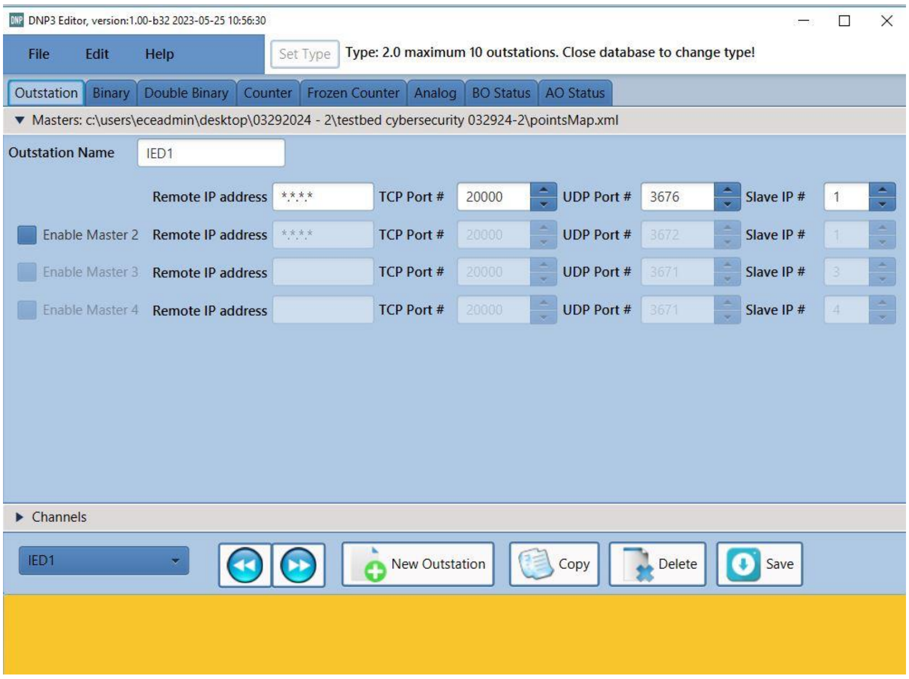
Masters: c:\users\eceadmin\desktop\03292024 - 2\testbed cybersecurity 032924-2\pointsMap.xml

Channels

Number of Channels:	1	Protocol Mode	TCP/UDP
Channel Number	> Inst: 1	Number of Sessions	1
Max Control per Request	16	Link Layer (session)	> Inst: 1
Max RX Fragment Size	2048	Master Inst (session)	1
Max TX Fragment Size	2048	Remote Address	1
Allow Unsolicited	false	Local Address	1024
Select Timeout (ms)	10000	Response Timeout (ms)	10000
Solicited Confirm Timeout (ms)	10000	Keep Alive Timeout (ms)	5000
Unsolicited Confirm Timeout (ms)	10000		
Unsolicited Retries	3		

Figure 7: Outstation (IED1) connection channel

Figure 8 shows that multiple masters can be created within the GTNET DNP3 by configuring a dedicated remote IP address, TCP port address, and UDP Port address.


DNP3 Editor, version:1.00-b32 2023-05-25 10:56:30

Type: 2.0 maximum 10 outstations. Close database to change type!

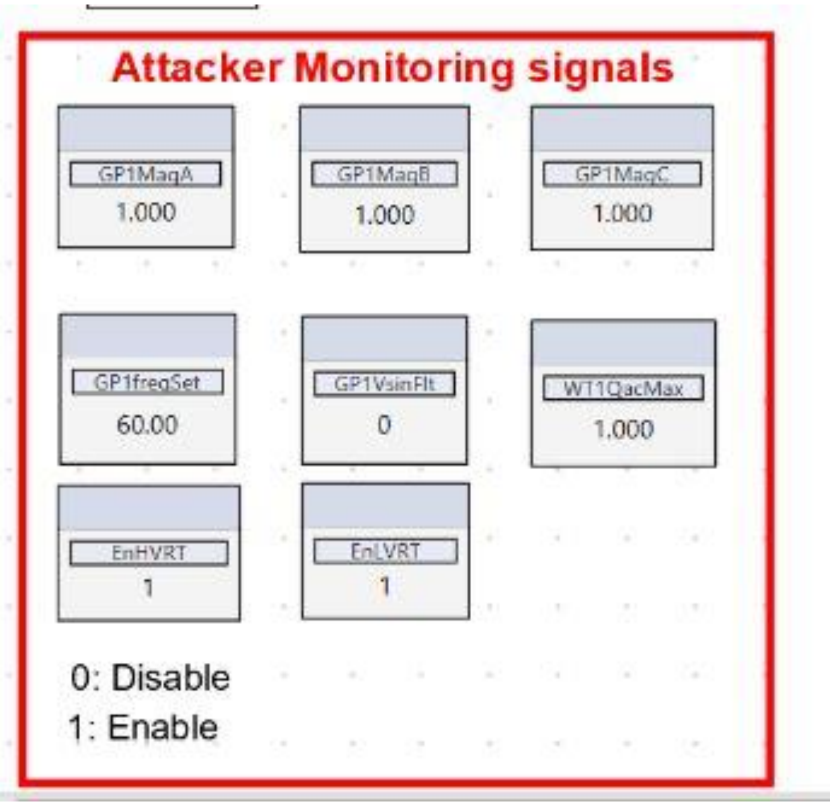
Masters: c:\users\eceadmin\desktop\03292024 - 2\testbed cybersecurity 032924-2\pointsMap.xml

Outstation Name: IED1

	Remote IP address *.*.*	TCP Port # 20000	UDP Port # 3676	Slave IP # 1
□ Enable Master 2	Remote IP address *.*.*	TCP Port # 20000	UDP Port # 3672	Slave IP # 1
□ Enable Master 3	Remote IP address	TCP Port # 20000	UDP Port # 3671	Slave IP # 3
□ Enable Master 4	Remote IP address	TCP Port # 20000	UDP Port # 3671	Slave IP # 4

Figure 8: Outstation

Figure 9 shows the attacker monitoring signals box created within the human-machine interface (HMI) to monitor important signals that attackers may manipulate to disrupt the functionality of the wind turbine model.



Attacker Monitoring signals

GP1MagA 1.000

GP1MagB 1.000

GP1MagC 1.000

GP1freqSet 60.00

GP1VsinFlt 0

WT1QacMax 1.000

EnHVRT 1

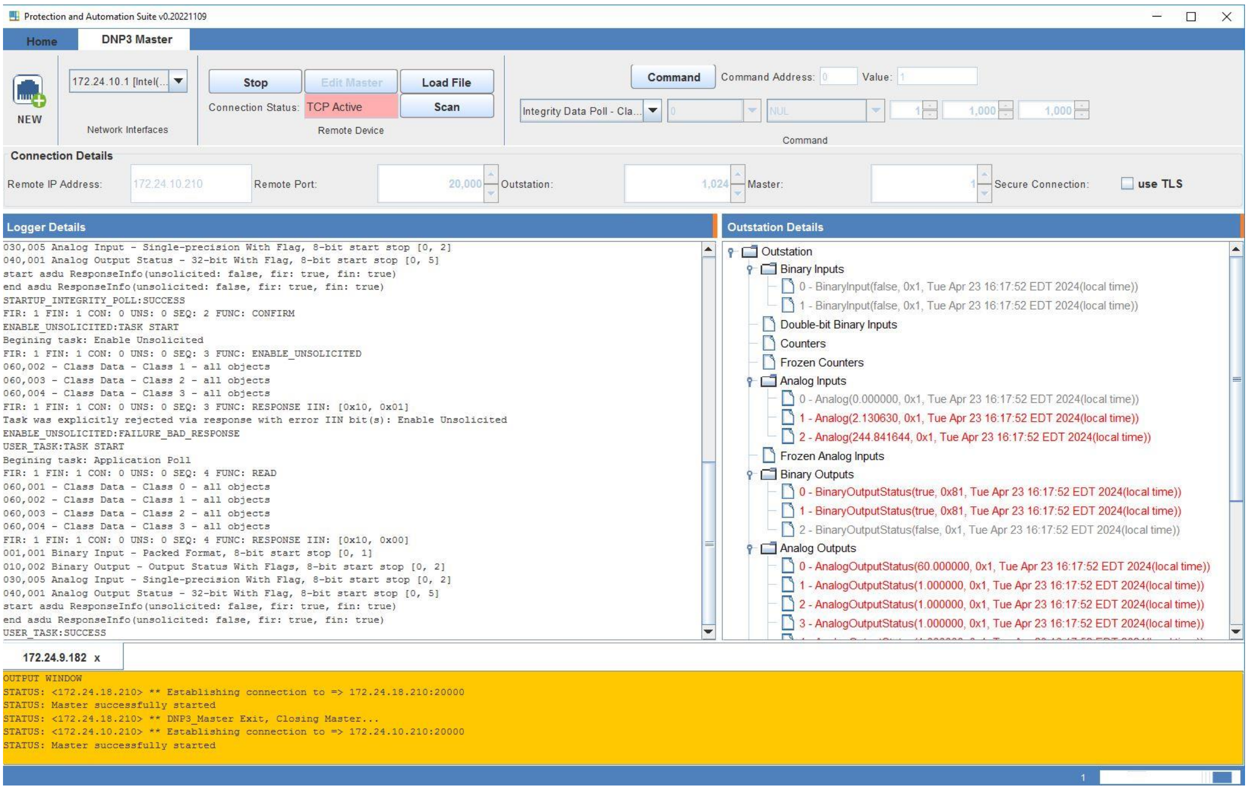
EnLVRT 1

0: Disable
1: Enable

Figure 9: Attacker Monitoring Signals

6.2 Simulated DNP3 Master Station

The Master DNP3 station allows binary and analog outputs defined within the outstation to be controlled in real-time during simulations. Below are the details of the protection and automation master station of the testbed. The interface allows the user or attacker to read log details showing the command instructions sent, time stamps, and signal values. Control input and output relay blocks functionality of the master stations allows for signal commands such as binary and analog values to be sent to the outstation's module in real-time simulation. Figure 11 shows the tab to access this functionality. An integrity class poll can be sent to read the status of all inputs in class 0 1 2 3 and report event changes if they occur.



172.24.10.1 [Intel(...

Connection Status: TCP Active

Integrity Data Poll - Cla... 0 NUL 1 1,000 1,000

Command Address: 0 Value: 1

Connection Details

Remote IP Address: 172.24.10.210 Remote Port: 20,000 Outstation: 1,024 Master: 1 Secure Connection: □ use TLS

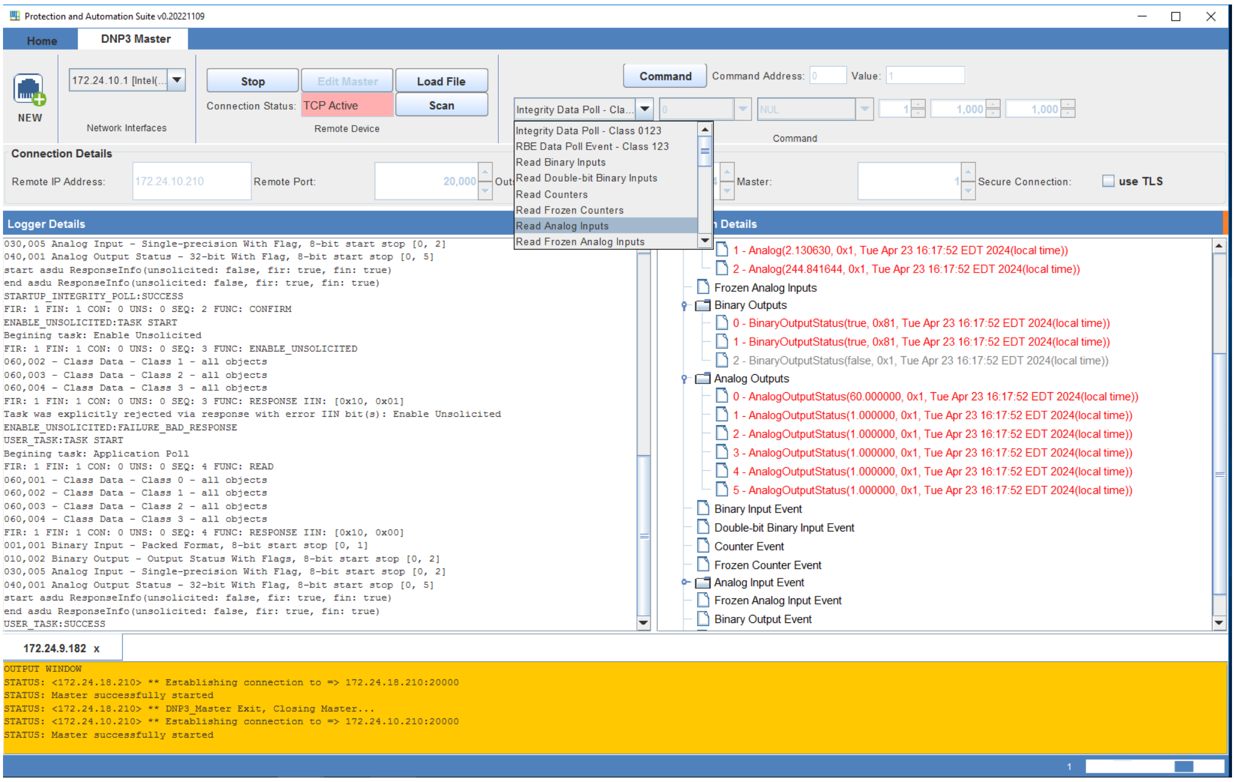
```
030,005 Analog Input - Single-precision With Flag, 8-bit start stop [0, 2]
040,001 Analog Output Status - 32-bit With Flag, 8-bit start stop [0, 5]
start asdu ResponseInfo(unsolicited: false, fir: true, fin: true)
end asdu ResponseInfo(unsolicited: false, fir: true, fin: true)
STARTUP_INTEGRITY_POLL:SUCCESS
FIR: 1 FIN: 1 CON: 0 UNS: 0 SEQ: 2 FUNC: CONFIRM
ENABLE_UNSOLICITED:TASK START
Begining task: Enable Unsolicited
FIR: 1 FIN: 1 CON: 0 UNS: 0 SEQ: 3 FUNC: ENABLE_UNSOLICITED
060,002 - Class Data - Class 1 - all objects
060,003 - Class Data - Class 2 - all objects
060,004 - Class Data - Class 3 - all objects
FIR: 1 FIN: 1 CON: 0 UNS: 0 SEQ: 3 FUNC: RESPONSE IIN: [0x10, 0x01]
Task was explicitly rejected via response with error IIN bit(s): Enable Unsolicited
ENABLE_UNSOLICITED:FAILURE_BAD_RESPONSE
USER_TASK:TASK START
Begining task: Application Poll
FIR: 1 FIN: 1 CON: 0 UNS: 0 SEQ: 4 FUNC: READ
060,001 - Class Data - Class 0 - all objects
060,002 - Class Data - Class 1 - all objects
060,003 - Class Data - Class 2 - all objects
060,004 - Class Data - Class 3 - all objects
FIR: 1 FIN: 1 CON: 0 UNS: 0 SEQ: 4 FUNC: RESPONSE IIN: [0x10, 0x00]
001,001 Binary Input - Packed Format, 8-bit start stop [0, 1]
010,002 Binary Output - Output Status With Flags, 8-bit start stop [0, 2]
030,005 Analog Input - Single-precision With Flag, 8-bit start stop [0, 2]
040,001 Analog Output Status - 32-bit With Flag, 8-bit start stop [0, 5]
start asdu ResponseInfo(unsolicited: false, fir: true, fin: true)
end asdu ResponseInfo(unsolicited: false, fir: true, fin: true)
USER_TASK:SUCCESS
```

```
Outstation
  Binary Inputs
    0 - BinaryInput(false, 0x1, Tue Apr 23 16:17:52 EDT 2024(local time))
    1 - BinaryInput(false, 0x1, Tue Apr 23 16:17:52 EDT 2024(local time))
  Double-bit Binary Inputs
  Counters
  Frozen Counters
  Analog Inputs
    0 - Analog(0.000000, 0x1, Tue Apr 23 16:17:52 EDT 2024(local time))
    1 - Analog(2.130630, 0x1, Tue Apr 23 16:17:52 EDT 2024(local time))
    2 - Analog(244.841644, 0x1, Tue Apr 23 16:17:52 EDT 2024(local time))
  Frozen Analog Inputs
  Binary Outputs
    0 - BinaryOutputStatus(true, 0x81, Tue Apr 23 16:17:52 EDT 2024(local time))
    1 - BinaryOutputStatus(true, 0x81, Tue Apr 23 16:17:52 EDT 2024(local time))
    2 - BinaryOutputStatus(false, 0x1, Tue Apr 23 16:17:52 EDT 2024(local time))
  Analog Outputs
    0 - AnalogOutputStatus(60.000000, 0x1, Tue Apr 23 16:17:52 EDT 2024(local time))
    1 - AnalogOutputStatus(1.000000, 0x1, Tue Apr 23 16:17:52 EDT 2024(local time))
    2 - AnalogOutputStatus(1.000000, 0x1, Tue Apr 23 16:17:52 EDT 2024(local time))
    3 - AnalogOutputStatus(1.000000, 0x1, Tue Apr 23 16:17:52 EDT 2024(local time))
```

172.24.9.182 x

```
OUTPUT WINDOW
STATUS: <172.24.18.210> ** Establishing connection to => 172.24.18.210:20000
STATUS: Master successfully started
STATUS: <172.24.18.210> ** DNP3_Master Exit, Closing Master...
STATUS: <172.24.10.210> ** Establishing connection to => 172.24.10.210:20000
STATUS: Master successfully started
```

Figure 10: Simulated DNP 3 Master station for Testbed



172.24.10.1 [Intel(...

Connection Status: TCP Active

Integrity Data Poll - Cla... 0 NUL 1 1,000 1,000

Command Address: 0 Value: 1

Connection Details

Remote IP Address: 172.24.10.210 Remote Port: 20,000 Master: 1 Secure Connection: □ use TLS

```
030,005 Analog Input - Single-precision With Flag, 8-bit start stop [0, 2]
040,001 Analog Output Status - 32-bit With Flag, 8-bit start stop [0, 5]
start asdu ResponseInfo(unsolicited: false, fir: true, fin: true)
end asdu ResponseInfo(unsolicited: false, fir: true, fin: true)
STARTUP_INTEGRITY_POLL:SUCCESS
FIR: 1 FIN: 1 CON: 0 UNS: 0 SEQ: 2 FUNC: CONFIRM
ENABLE_UNSOLICITED:TASK START
Begining task: Enable Unsolicited
FIR: 1 FIN: 1 CON: 0 UNS: 0 SEQ: 3 FUNC: ENABLE_UNSOLICITED
060,002 - Class Data - Class 1 - all objects
060,003 - Class Data - Class 2 - all objects
060,004 - Class Data - Class 3 - all objects
FIR: 1 FIN: 1 CON: 0 UNS: 0 SEQ: 3 FUNC: RESPONSE IIN: [0x10, 0x01]
Task was explicitly rejected via response with error IIN bit(s): Enable Unsolicited
ENABLE_UNSOLICITED:FAILURE_BAD_RESPONSE
USER_TASK:TASK START
Begining task: Application Poll
FIR: 1 FIN: 1 CON: 0 UNS: 0 SEQ: 4 FUNC: READ
060,001 - Class Data - Class 0 - all objects
060,002 - Class Data - Class 1 - all objects
060,003 - Class Data - Class 2 - all objects
060,004 - Class Data - Class 3 - all objects
FIR: 1 FIN: 1 CON: 0 UNS: 0 SEQ: 4 FUNC: RESPONSE IIN: [0x10, 0x00]
001,001 Binary Input - Packed Format, 8-bit start stop [0, 1]
010,002 Binary Output - Output Status With Flags, 8-bit start stop [0, 2]
030,005 Analog Input - Single-precision With Flag, 8-bit start stop [0, 2]
040,001 Analog Output Status - 32-bit With Flag, 8-bit start stop [0, 5]
start asdu ResponseInfo(unsolicited: false, fir: true, fin: true)
end asdu ResponseInfo(unsolicited: false, fir: true, fin: true)
USER_TASK:SUCCESS
```

```
    1 - Analog(2.130630, 0x1, Tue Apr 23 16:17:52 EDT 2024(local time))
    2 - Analog(244.841644, 0x1, Tue Apr 23 16:17:52 EDT 2024(local time))
  Frozen Analog Inputs
  Binary Outputs
    0 - BinaryOutputStatus(true, 0x81, Tue Apr 23 16:17:52 EDT 2024(local time))
    1 - BinaryOutputStatus(true, 0x81, Tue Apr 23 16:17:52 EDT 2024(local time))
    2 - BinaryOutputStatus(false, 0x1, Tue Apr 23 16:17:52 EDT 2024(local time))
  Analog Outputs
    0 - AnalogOutputStatus(60.000000, 0x1, Tue Apr 23 16:17:52 EDT 2024(local time))
    1 - AnalogOutputStatus(1.000000, 0x1, Tue Apr 23 16:17:52 EDT 2024(local time))
    2 - AnalogOutputStatus(1.000000, 0x1, Tue Apr 23 16:17:52 EDT 2024(local time))
    3 - AnalogOutputStatus(1.000000, 0x1, Tue Apr 23 16:17:52 EDT 2024(local time))
    4 - AnalogOutputStatus(1.000000, 0x1, Tue Apr 23 16:17:52 EDT 2024(local time))
    5 - AnalogOutputStatus(1.000000, 0x1, Tue Apr 23 16:17:52 EDT 2024(local time))
  Binary Input Event
  Double-bit Binary Input Event
  Counter Event
  Frozen Counter Event
  Analog Input Event
  Frozen Analog Input Event
  Binary Output Event
```

172.24.9.182 x

```
OUTPUT WINDOW
STATUS: <172.24.18.210> ** Establishing connection to => 172.24.18.210:20000
STATUS: Master successfully started
STATUS: <172.24.18.210> ** DNP3_Master Exit, Closing Master...
STATUS: <172.24.10.210> ** Establishing connection to => 172.24.10.210:20000
STATUS: Master successfully started
```

Figure 11: DNP 3 Master station control operations using binary and analog outputs

7. Conclusions

The objective of the project was to create a real-time testbed for studying cybersecurity attacks that affect smart inverters in distributed energy resource (DER) systems through the configuration of DNP database I/O and creating a Distributed Network Protocol 3 (DNP3) communication module. Cyberattacks occur more frequently in DER systems due to incorporating smart inverters with features like high- and low-voltage ride-through (HVRT and LVRT), frequency ride-through, and reactive power compensation. The input and output signals transmitted via the master station allow simulations of attacking and monitoring of signals. The testbed will allow for monitoring of the smart inverter in response when the signals are disrupted. With the help of real-time simulation technologies like RTDS and RSCAD, the project offers a secure setting to experiment and study without running the risk of physical system damage. The testbed's design and implementation allow the creation of stronger safety measures to protect power systems from cyberattacks by revealing essential information about the communication protocols and smart inverter vulnerabilities,

8. Recommendations for Future Work

We identified several recommendations for the next group undertaking a follow-on project. Firstly, the testbed's capabilities should be extended to include more signals to simulate additional cybersecurity threats and vulnerabilities of the smart inverter operation related to DNP3 communication. We can gain a deeper understanding of smart inverter cybersecurity by implementing different communication protocols like MODBUS and adding two or more 3 phase nodes to test interconnection attacks on multiple wind turbine systems. Secondly, we can add a physical master station outside of the RTDS, such as an Open Platform Communication (OPC) server, for process control. The testbed’s data manipulation will become more precise and flexible with the addition of an external master station. This will allow for an added layer of security for the signals transmitted via DNP3 communications from the outstation. Finally, we can use technologies like RTAC (Real Time Automation Controller) to monitor and analyze real-time cyberattacks on smart inverters. More efficient detection of anomalies and security breaches can be achieved by putting advanced data analytics techniques into practice.

9. References

[1] M. Liserre, T. Sauter and J. Y. Hung, "Future Energy Systems: Integrating Renewable Energy Sources into the Smart Power Grid Through Industrial Electronics", IEEE Industrial Electronics Magazine, vol. 4, no. 1, pp. 18-37, Mar. 2010

[2] T. Strasser, F. Andrén, J. Kathan et al., "A Review of Architectures and Concepts for Intelligence in Future Electric Energy Systems", IEEE Transactions on Industrial Electronics, vol. 62, no. 4, pp. 2424-2438, Apr. 2015.

[3] Kikusato, Hiroshi et al. “Developing Power Hardware-in-the-Loop Based Testing Environment for Volt-Var and Frequency-Watt Functions of 500 KW Photovoltaic Smart Inverter.” IEEE Access 8 (2020): 224135–224144.

[4] IEEE, 1547-2018, "IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces", 2018.

[5] IEC/IEEE International Standard - Communication networks and systems for power utility automation – Part 9-3: Precision time protocol profile for power utility automation, in IEC/IEEE 61850-9-3 Edition 1.0 2016-05, vol., no., pp.1-18, 31 May 2016

[6] RTDS Technologies, Standardization of Renewable Energy System Modelling.

[7] O. T. Soyoye and K. C. Stefferud, "Cybersecurity risk assessment for California's smart inverter functions", Proc. IEEE CyberPELS, pp. 1-5, 2019.