Real-time Power System Simulation with Hardware Devices through DNP3 in Cyber-Physical Testbed

Hao Huang
Texas A&M University
hao_huang@tamu.edu

C. Matthew Davis
PowerWorld Corporation
matt@powerworld.com

Katherine R. Davis
Texas A&M University
katedavis@tamu.edu

2021 IEEE Texas Power and Energy Conference (TPEC) | 978-1-7281-8612-2/21/$31.00 ©2021 IEEE | DOI: 10.1109/TPEC51183.2021.9384947

***Abstract*—Modern power grids are dependent on communication systems for data collection, visualization, and control. Distributed Network Protocol 3 (DNP3) is commonly used in supervisory control and data acquisition (SCADA) systems in power systems to allow control system software and hardware to communicate. To study the dependencies between communication network security, power system data collection, and industrial hardware, it is important to enable communication capabilities with real-time power system simulation. In this paper, we present the integration of new functionality of a power systems dynamic simulation package into our cyber-physical power system testbed that supports real-time power system data transfer using DNP3, demonstrated with an industrial real-time automation controller (RTAC). The usage and configuration of DNP3 with real-world equipment in to achieve power system monitoring and control of a large-scale synthetic electric grid via this DNP3 communication is presented. Then, an exemplar of DNP3 data collection and control is achieved in software and hardware using the 2000-bus Texas synthetic grid.**

***Index Terms*—DNP3 Protocol, SCADA, Hardware-in-the-Loop, Interactive Control, Cyber Security**

I. Introduction

Electric power systems are some of the largest industrial control systems (ICS). In these systems, operations taken by physical actuators depend on data, where this data may be delivered through a communications infrastructure. A power system is also a critical infrastructure; hence, its reliability and resilience are its key requirements. For example, it is important to ensure the integrity of generator dispatch to achieve effective utilization of energy resources and reasonable electricity prices. To achieve such goals, a reliable and secure communication network is essential. However, increasing cyberattacks are occuring worldwide [1], [2], and more studies are showing vulnerabilities in current communication protocols [3]. Thus, how to analyze, detect, and respond to cyber attacks is a vital research topic in power systems.

Distributed Network Protocol 3 (DNP3) [4] is commonly used in ICS for data acquisition and control [5]. However, several studies show the vulnerability of DNP3 and implement different types of attacks, such as event buffer flooding [6], man-in-the-middle [7], packet sniffing and modification [8], etc. Such explorations historically stay within the scope of only the communication network and its emulation, while neglecting real hardware devices and analysis of power system impact. To study the cyber-physical security of power systems, it is important to consider both cyber and physical elements. Recently, several hardware-in-the-loop testbeds are built with Real-Time Digital Simulator (RTDS) or OPAL-RT for power system cyber-physical security studies and algorithm validation [9]–[11]. Even though the incorporation of these commercial products for hardware-in-the-loop testbeds can replicate certain impacts of cyber adversaries in power systems, they cannot capture the detailed cyber attack process in the cyber network. Therefore, it is necessary to have a stand-alone power system real-time simulation that also has the functionality to communicate over a cyber network.

This paper introduces usage of a new DNP3 functionality of PowerWorld Dynamic Studio (PWDS) that allows the communication of PWDS with DNP3 clients, which enables the detailed analysis of DNP3 communication among real-time power system simulation, cyber adversaries, and industrial intelligent electronic devices (IEDs). PWDS provides an interactive simulation environment for real-time power system analysis. It can run either stand-alone or as a server; as a server, one of its capabilities is to generate IEEE C37.118 phasor measurement unit (PMU) data [12]–[14] which has been utilized in [15]–[17] for real-time power system data visualization, interactive control through a web interface, and digital PMU data to analog signal conversion. The addition of DNP3 functionality allows PWDS to run as a DNP3 server, generate DNP3 packets, and deliver the packets over the communication network to DNP3 clients/masters.

The U.S. Department of Energy (DOE) has funded several projects for power system cyber-physical security. In [18], the Cyber Physical Resilient Energy Systems (CYPRES) project is developing a secure cyber-physical modeling foundation that is truly cyber-physical: a secure end-to-end system for managing the energy system, communications, security, and modeling and analytics. PWDS with DNP3 communication capability is used in creating the hardware-in-the-loop testbed with power system modeling and analysis. This testbed is performing hardware integration over physical and emulated utility communication networks, enabling realistic security studies bridging both cyber and physical domains for CYPRES.

The main contributions of this paper are as follows:

1) This paper presents a cyber-physical testbed implementation of new functionality of PWDS that enables the communication between real-time power system simulation with industry hardware devices through DNP3.
2) We utilize an industrial control and automation device, SEL Real-Time Automation Controller (RTAC), to communicate with PWDS through DNP3.
3) With the synthetic Texas power grid [19], we present an exemplar of how to use RTAC and PWDS to mimic real-world applications of reading measurements and

978-1-7281-8612-2/21/$31.00 ©2021 IEEE

Authorized licensed use limited to: Texas A M University. Downloaded on May 10,2022 at 21:51:22 UTC from IEEE Xplore. Restrictions apply.

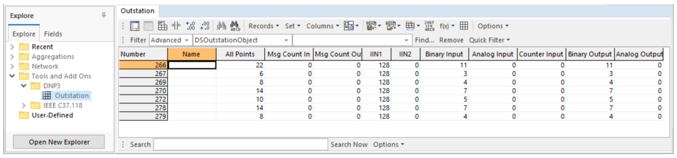

Figure 1. Outstation Records

controlling devices using DNP3.

II. PowerWorld Dynamic Studio DNP3 Functionality

PowerWorld Dynamic Studio (PWDS) is a transient stability based simulation running as a server. It is capable of sending and receiving data from connected clients, thus allowing multiple users to interact with the transient stability simulation. The PWDS "speaks" several protocols. It is capable of communicating via a proprietary protocol called the DS protocol (PWDSP), the IEEE C37.118 protocol [12] as output, and DNP3 [4]. The use of standard protocols allows the DS to function as a stand-in for a real power system in a wide range of applications including those that are modeling cyber infrastructure.

Just like the cases used for running the simulations, where the transient stability data must be setup ahead of time for the PWDS, a case's DNP3 data is also set up in PowerWorld Simulator before being used in PWDS. The DNP3 configurations are presented to the user in terms of two objects in Simulator: *DNP3Objects* and *Outstations*. The *Outstation* is a container object that groups together several *DNP3Objects*. A simple example of the use of an *Outstation* is to group together all the points from a particular substation. However, there is no restriction in the software about which points can be assigned to an outstation, so within each DNP3 outstation, we can insert the *DNP3Object* for different devices. In the PWDS, Figure 1 shows the list of outstations in a sample case, while Figure 2 shows the dialog for an outstation. Dialogs in Simulator allow the user to create *Outstation* objects and insert *DNP3Objects*.

The *DNP3Object* is configured using the "DNP3 Point Information" dialog as shown in Figure 3. This dialog allows the user to map an object and field in the power system model to a DNP3 point. As shown in Figure 3, there are 5 DNP3 *Point Type* to choose, which are *Binary Input*, *Analog Input*, *Counter Input*, *Binary Output*, and *Analog Output*. The *Point Field* determines the specific data. For example, generator's *STATUS* is set in *Binary Input*. When the generator is on, the binary input data is represented as 1, otherwise, it is 0. In *Binary Output*, the generator's status can be controlled by connected DNP3 client/master. For a generator's power data, such as its real power and reactive power output, these are set in *Analog Input* as *MW* and *MVar*. For *Analog Output*, PWDS DNP3 only supports *MWSETPOINT* and *VPUSETPOINT* for generators to set generator's real power and voltage values. Other devices, including loads, shunts, branchs, and buses, can be configured in the same way. The *Event Class* determines when the data should be reported to DNP3 client, and these are customized by the user or application. Events are each placed in one of three buffers, associated with "Classes" 1, 2

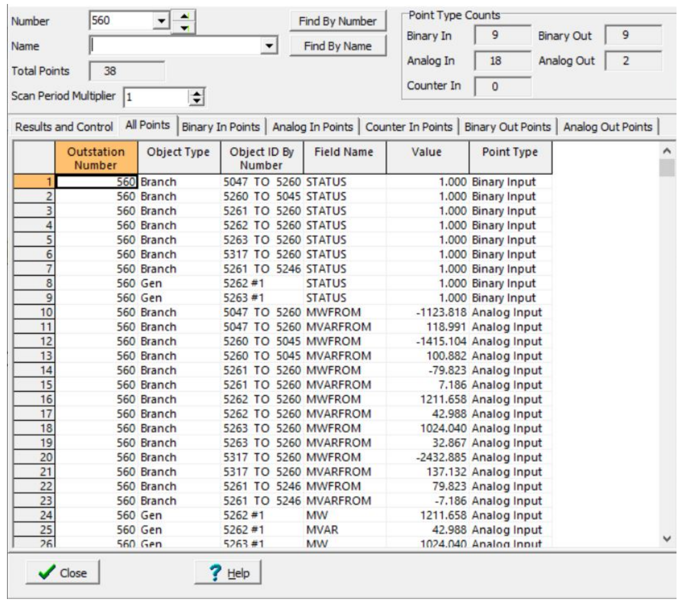

Figure 2. Outstation Information Dialog

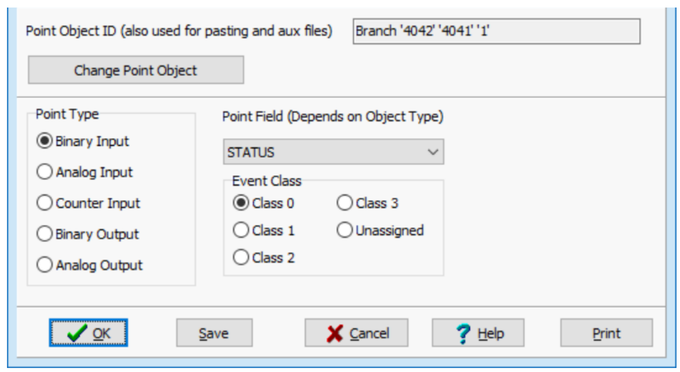

Figure 3. DNP3 Point Information Dialog

and 3. In addition to these, Class 0 is defined as "static" or and gives the current status of the monitored data [4].

III. SEL Real-Time Automation Controller (RTAC)

The SEL RTAC is an industrial automation and control device that supports various communication protocols, such as DNP3, Modbus, IEC 61850, etc. [20]. RTACs have been utilized in SCADA systems as remote terminal units (RTUs) for data collection and protocol conversion. The built-in IEC 61131 engine enables flexible customer-designed logic with incoming power system data and the RTAC's system tags for substation control. The RTAC is configured through the SEL AcSELerator RTAC software (SEL-5033) that provides a programmable interface for users to configure the communication protocol types and parameters, the connection type, and user defined logic [21]. The embedded flex parse messaging within the SEL protocol allows users to create customized regular expressions to collect specific information, such as connected device configurations, energy measurements, etc. [22]. Additionally, the RTAC can be accessed through its web interface, where we can configure its ethernet ports' IP

Authorized licensed use limited to: Texas A M University. Downloaded on May 10,2022 at 21:51:22 UTC from IEEE Xplore. Restrictions apply.

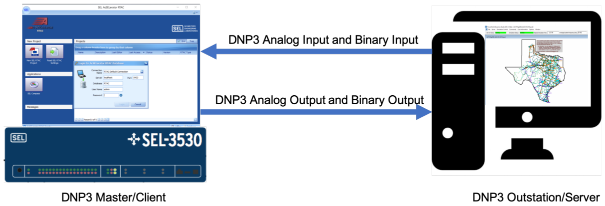

Figure 4. PWDS Communicates with SEL RTAC Over DNP3

address, check connected IEDs, access the system alarms and event logs, and get a diagnostic report.

RTAC has been utilized in various power testbeds for cyber-physical security studies [23], [24], algorithm validation [25]–[27], and data collection, conversion and control [16], [28]. Within those applications, the RTAC is ether connected to relays working as a RTU or communicating with phasor data concentrators (PDC) to collect PMU data for real-time automated control. Any application or devices that support DNP3 communication can communicate with RTAC through serial or TCP/IP communication, which can be utilized in power system cyber-physical security studies.

Hence, PWDS can generate DNP3 packets based on the pre-defined outstation and DNP3 tags and send them through TCP/IP network to its destination. In this way, PWDS can communicate with the RTAC and supply each outstation's DNP3 data, including the measurements, such as current, voltage, power flow, etc., and the on/off status of generators, branches, loads and shunts. This functionality provides for new approaches to study cyber-physical security among power system real-time simulation, hardware devices, and communication network.

IV. DNP3 Communication between PowerWorld DS and RTAC

DNP3 is frequently used in power system supervisory control and data acquisition (SCADA) systems to collect data and send control commands. As PWDS runs the simulation in real-time, each device modeled in the case has its own data including status (open/close) and measurements (e.g., real power, reactive power, voltage). With the DNP3 functionality in PWDS, the real-time simulation data is wrapped in DNP3 packets and delivered to DNP3 clients/masters. This allows the integration of real-time power system simulation with other software and hardware to replicate realistic SCADA systems with both cyber and physical elements.

The integration of PWDS and RTAC presents one characteristic of a cyber-physical hardware-in-the-loop testbed. The data generated by the simulation represents the field device measurements. The RTAC collects the data through DNP3, emulating real data transmission in the communication network. The DNP3 packets can then be captured by network analysis tools such as WireShark for further analysis. Then, within RTAC, as the DNP3 client, we can observe the collected data and control devices to mimic real-world operation.

This section presents how to set the PowerWorld case to generate DNP3 packets and configure the RTAC to collect the corresponding DNP3 data. In this paper, we utilize the synthetic 2000-bus Texas case [19] to configure the PowerWorld case and RTAC to establish the DNP3 communication and collect data and control devices. With 1250 substations in the case, we use the Substation 560 (GLEN ROSE1) as the example to show the procedure, whose one-line diagram is shown in Figure 5 with two generators, three transformers, four transmission lines and four buses. The procedure can be replicated for all other substations and devices.

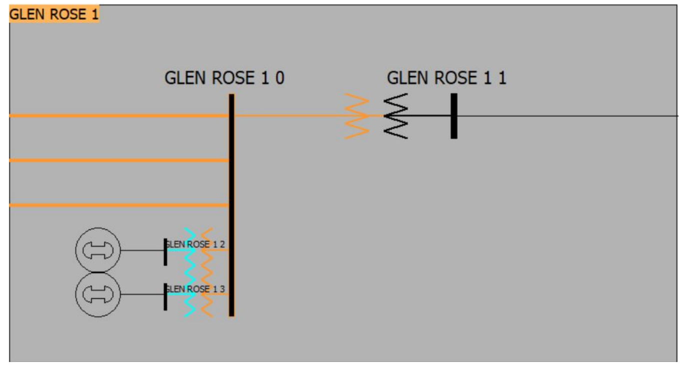

Figure 5. One-Line Diagram of Substation GLEN ROSE1

A. *Configuration of PWDS and RTAC*

To enable the PWDS DNP3 functionality, the first step is to configure the corresponding power system case in Simulator under the **DNP3** folder. Within the *Outstation*, we can insert as many DNP3 outstations as needed. Then, in the *DNP3Object*, we can insert different DNP3 *Point Type*, including *Analog Input*, *Analog Output*, *Binary Input* and *Binary Output*, for various devices under corresponding *Outstation*. With 1250 substations, for convenience, we configure the *outstation number* based on the substation ID. Then, the devices within each substation, including generators, branches, loads, shunts and buses, and their corresponding data are configured to different *Point Field* as discussed in Section II. Once the DNP3 configuration for the power system case is done, we can load the case to PWDS, run the real-time simulation and turn on the server. The host machine of PWDS can generate DNP3 packets at all its Ethernet ports, whose IP addresses are the DNP3 Server IP Address for DNP3 client/master to collect data for different local area networks (LANs). Regarding to DNP3 Protocol Port, it can be configured in PWDS, which is set to 20000 in this case.

For RTAC, it is the DNP3 client for outstations in PWDS. To establish the DNP3 communication between PWDS and RTAC, RTAC's Ethernet port that connects to the host machine of PWDS and one of the host machine's Ethernet ports should be under the same LAN. In this paper, the connected RTAC Ethernet port's IP is 172.168.2.2 and one of the host machine's Ethernet port's IP is 172.168.2.10. Then, for each outstation, we can program a corresponding DNP3 client through SEL 5033 by inserting *DNP Protocol* with *Client-Ethernet* connection type. For clarity, we name the DNP3 client based on the substation ID. Within the client, the *Server IP Address* is 172.168.2.10 and the *Server IP Port* is 20000. The *Server DNP Address* is the corresponding outstation number, which is the substation ID in this paper. As to *Client IP Port* and

Authorized licensed use limited to: Texas A M University. Downloaded on May 10,2022 at 21:51:22 UTC from IEEE Xplore. Restrictions apply.

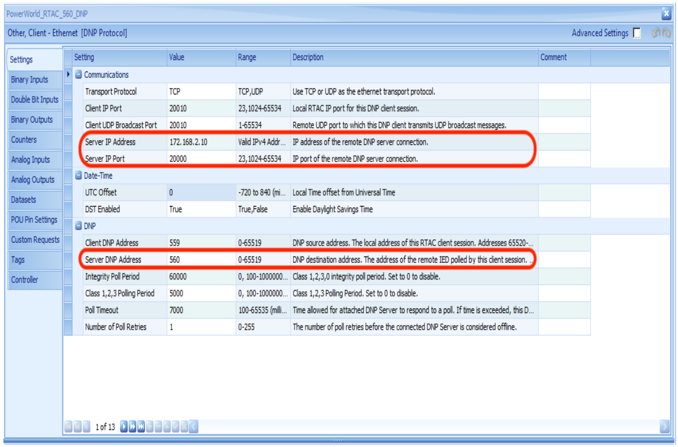

Figure 6. RTAC Configuration for Client PowerWorld_RTAC_560 for Substation 560.

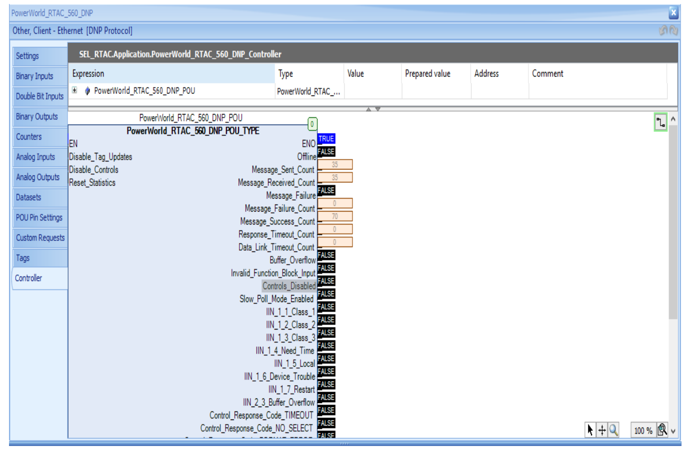

Figure 7. Client PowerWorld_RTAC_560 Controller

Client DNP Address, they can be configured based on user's preference as long as that port and address are not taken by other DNP3 applications/clients. The example of communication configuration for Substation 560 (GLEN ROSE) is shown in Figure 6. For DNP3 communication settings, other parameters, such as *Integrity Poll Period*, *Class 1,2,3 Polling Period* and *Poll Timeout*, are the default settings in SEL 5033.

After configuring the communication settings, we create *Analog Input*, *Analog Output*, *Binary Input* and *Binary Output* in RTAC to receive the data from PWDS. Once the configuration of RTAC is done, we can load the settings to RTAC through SEL 5033 by *Go Online* option. Then, the RTAC configuration will be loaded to the hardware device for DNP3 communication. To check the communication between RTAC and PWDS, we can check the *Controller* after the SEL 5033 is online. As shown in Figure 7, a successful DNP3 connection's *Offline* tag is **FALSE** and the *Message_Sent_Count*, *Message_Received_Count* and *Message_Success_Count* are keeping increasing simultaneously. If there is any message fail to transmit, the *Message_Failure* will become **TRUE** and *Message_Failure_Count* will show the number. From PWDS, we can check the *Logs*, where shows the *Connected Clients* and *DNP3Log* as shown in Figure 8. There is an online period for SEL 5033. After the online period is passed, RTAC's settings are already configured and it can work as normal until the program has been updated and reloaded.

B. Exemplar of DNP3 Reading and Control

After the DNP3 communication between RTAC and PWDS is established, we can check the data in RTAC and send the control from RTAC to PWDS.

For simplicity and clarity, when we configure the PowerWorld case with *DNP3Object*, we also create corresponding DNP3 tags for RTAC with the following pattern, *DataType_SubstationID_DeviceType_Keyfield_DataName*. In this way, we can easily check the data from RTAC with detailed information of corresponding PowerWorld case information. For DNP3 data transition between client and server, it is based on the Zero-based Index (PWDS) and Point Number (RTAC) as shown in Figure 9 for *Analog Input* data. RTAC

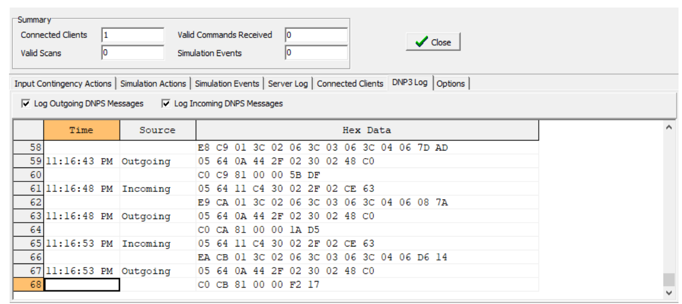

Figure 8. DNP3 Connection Logs

collects the data from PWDS to corresponding tag based on the index and point number. This is the same for *Analog Output*, *Binary Input*, and *Binary Output* data.

Once the DNP3 communication is successfully established, we can observe the data in RTAC *Tag* list. As shown in Figure 10 and 11, they show the *Analog Input* and *Binary Input* data for Branch 5047_5260_1's reactive power flow and status respectively and they are the same value as in PWDS. Besides the RTAC Controller tags, we can also check *q* and its *validity* value to see whether the DNP3 communication is successful or not. As shown in Figure 10 and 11, both tags show **good**, so the current communication is established. When there is misconfiguration or cyber intrusion in the communication network, this tag will become **invalid**.

RTAC client can also control the status of the device and change the generator *MWSETPOINT* through *Analog Output* and *Binary Output* data. As shown in Figure 12, we send a control command to Generator 5262_1 in Substation 560 to change its real power output as 1000 MW through *Analog Output* using the force value function in SEL 5033. After the generator receives the command, it gradually reduces its output from 1211 MW to 1004 MW. Because of the generator's exciter and governor model in PWDS, the generator's output will not reduce to 1004 MW immediately. In Figure 12, there are two reading for Generator 5262_1 real power output, one is *instMag* whose value is 1004 MW and the other is *mag* whose value is 1015 MW. The *instMag* is the instantaneous value of corresponding tag's data, while the *mag* is the value

Authorized licensed use limited to: Texas A M University. Downloaded on May 10,2022 at 21:51:22 UTC from IEEE Xplore. Restrictions apply.

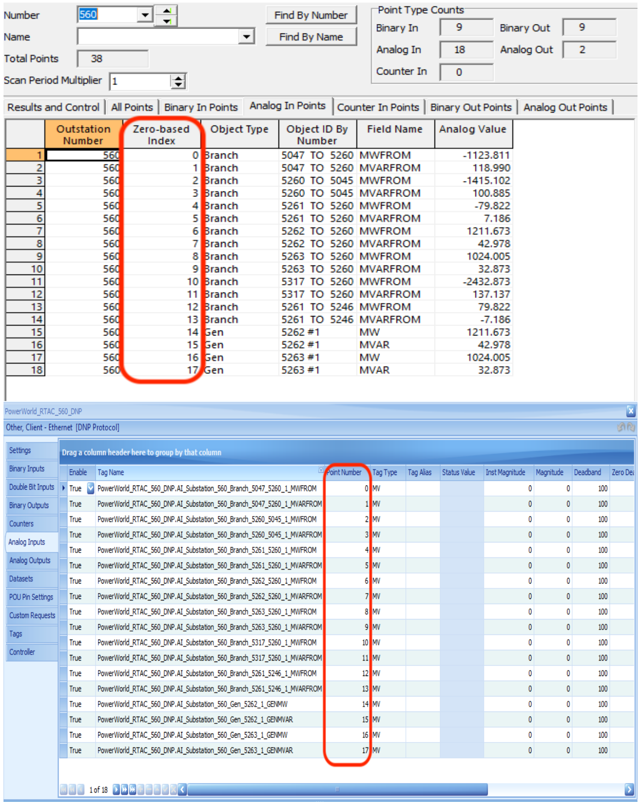

Figure 9. DNP3 Analog Input Configuration in PWDS (Up) and RTAC (Bottom) for Data Mapping

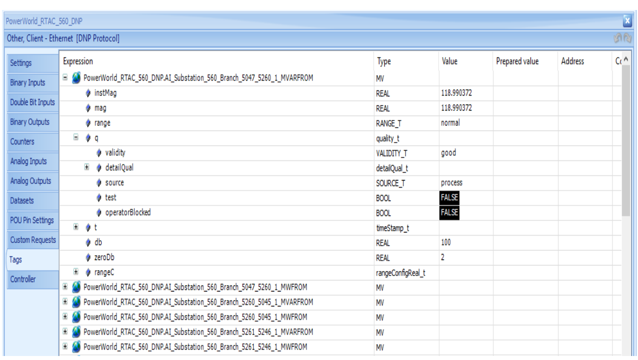

Figure 10. RTAC Analog Input Data for Branch 5047_5260_1 Reactive Power Flow.

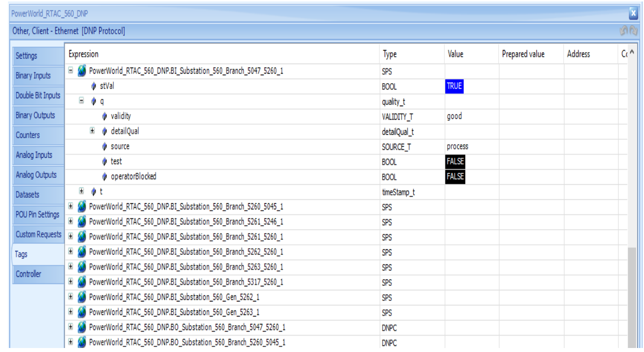

Figure 11. RTAC Analog Input Data for Branch 5047_5260_1 Status.

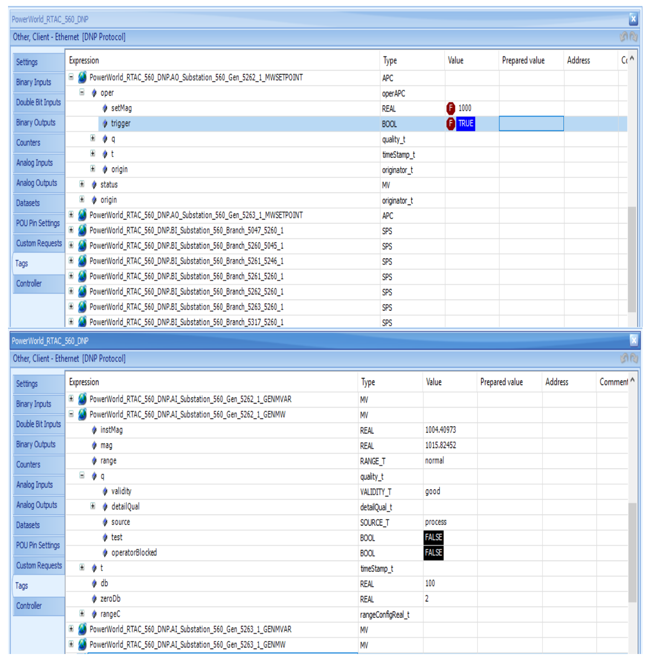

Figure 12. RTAC DNP3 Client Control Generator 5262_1 real power output (Top) and the updated Analog Input reading (Bottom)

snapshot after *instMag* exceeds the dead-band value, which is the time-stamped dead-banded event value [20].

Figure 13 shows the RTAC client open Branch 5047_5260_1 through Binary Output. After the command is executed, the branch will be open and updated *Binary Input* for corresponding data will be **FALSE**.

All the commands sent from RTAC is logged in PWDS as shown in Figure 14 with specific execution time and the counts of events.

V. Conclusion

In this paper, we present the cyber-physical testbed implementation of new functionality of PWDS that supports DNP3 communication capability, enabling real-time power system simulation in PWDS to generate DNP3 packets and deliver to DNP3 clients/masters. With an industrial automation and control device, this paper shows how to configure the synthetic power system case and RTAC to establish a successful DNP3 communication. It also shows the data that collected in RTAC *Analog Input* and *Binary Input* for corresponding measurement and status, and how the control command can be sent with *Analog Output* and *Binary Output* and committed in PWDS for real-time power system simulation.

The new functionality of DNP3 communication in PWDS provides a new mechanism to establish a hardware-in-the-loop testbed for power system cyber-physical security studies. PWDS can generate DNP3 packets based on configured DNP3 outstations and objects and deliver these packets to the DNP3 clients in industrial hardware, like RTAC, or EMS software, through a communication network. For future work, we can incorporate real or emulated communication network between

Authorized licensed use limited to: Texas A M University. Downloaded on May 10,2022 at 21:51:22 UTC from IEEE Xplore. Restrictions apply.

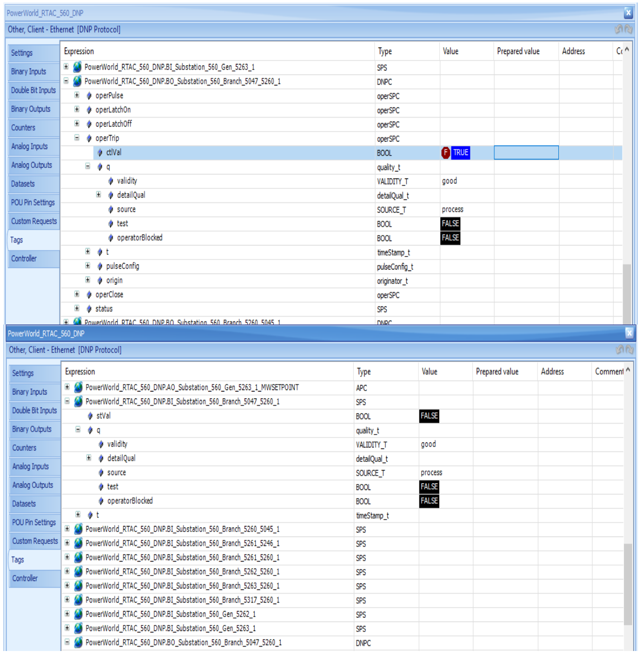

Figure 13. RTAC DNP3 Client Control Branch 5047_5260_1 to Open (Top) and the updated Binary Input reading (Bottom)

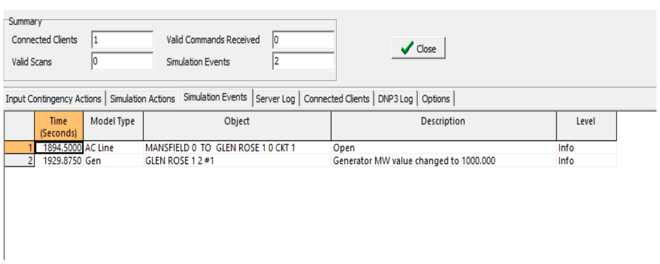

Figure 14. DS Logs for Operations from RTAC Client.

PWDS and industrial hardware and software. Cyber intrusions can then be performed in the communication network, and the power system impacts can be observed in PWDS with real-time simulation; hardware devices can also detect such events with pre-defined alerts and control logic.

VI. Acknowledgement

The work described in this paper was supported by funds from the US Department of Energy under award DE-OE0000895 and the National Science Foundation under Grant 1916142.

References

[1] Defense Use Case, “Analysis of the cyber attack on the ukrainian power grid,” *Electricity Information Sharing and Analysis Center (E-ISAC)*, vol. 388, 2016.
[2] R. K. Knake, *A cyberattack on the US power grid*, 2017.
[3] Y. Xu, Y. Yang, T. Li, J. Ju, and Q. Wang, “Review on cyber vulnerabilities of communication protocols in industrial control systems,” in *2017 IEEE Conference on Energy Internet and Energy System Integration (EI2)*. IEEE, 2017, pp. 1–6.
[4] “IEEE Standard for Electric Power Systems Communications - Distributed Network Protocol (DNP3),” *IEEE Std. 1815-2012*, pp. i –799, 2012.
[5] G. Clarke, D. Reynders, and E. Wright, *Practical modern SCADA protocols: DNP3, 60870.5 and related systems*. Newnes, 2004.
[6] D. Jin, D. M. Nicol, and G. Yan, “An event buffer flooding attack in dnp3 controlled scada systems,” in *Proceedings of the 2011 Winter Simulation Conference (WSC)*. IEEE, 2011, pp. 2614–2626.
[7] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, E. G. Im, Z. Yao, B. Pranggono, and H. Wang, “Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in smart grid scada systems,” 2012.
[8] D. Lee, H. Kim, K. Kim, and P. D. Yoo, “Simulated attack on dnp3 protocol in scada system,” in *Proceedings of the 31th Symposium on Cryptography and Information Security, Kagoshima, Japan*, 2014, pp. 21–24.
[9] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, “Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid,” *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 847–855, 2013.
[10] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and A. K. Srivastava, “Analyzing the cyber-physical impact of cyber events on the power grid,” *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2444–2453, 2015.
[11] S. Poudel, Z. Ni, and N. Malla, “Real-time cyber physical system testbed for power system security and control,” *International Journal of Electrical Power & Energy Systems*, vol. 90, pp. 124–133, 2017.
[12] *IEEE Std C37.118.1-2011 (Revision of IEEE Std C37.118-2005)*.
[13] T. J. Overbye, Z. Mao, K. S. Shetye, and J. D. Weber, “An interactive, extensible environment for power system simulation on the pmu time frame with a cyber security application,” in *2017 IEEE Texas Power and Energy Conference (TPEC)*. IEEE, 2017, pp. 1–6.
[14] T. J. Overbye, Z. Mao, A. Birchfield, J. D. Weber, and M. Davis, “An interactive, stand-alone and multi-user power system simulator for the pmu time frame,” in *2019 IEEE Texas Power and Energy Conference (TPEC)*. IEEE, 2019, pp. 1–6.
[15] Z. Mao, H. Huang, and K. Davis, “W4ips: A web-based interactive power system simulation environment for power system security analysis,” in *Proceedings of the 53rd Hawaii International Conference on System Sciences*, 2020.
[16] T. Becejac, C. Eppinger, A. Ashok, U. Agrawal, and J. O’Brien, “Prime: a real-time cyber-physical systems testbed: from wide-area monitoring, protection, and control prototyping to operator training and beyond,” *IET Cyber-Physical Systems: Theory & Applications*, 2020.
[17] I. Idehen, T. Overbye, and L. Klemesrud, “An electric power system energy management platform (emp) research testbed,” in *2020 IEEE Texas Power and Energy Conference (TPEC)*. IEEE, 2020, pp. 1–6.
[18] “Cyber Physical Resilient Energy Systems (CYPRES).” [Online]. Available: https://cypres.engr.tamu.edu/
[19] A. B. Birchfield, T. Xu, K. M. Gegner, K. S. Shetye, and T. J. Overbye, “Grid structural characteristics as validation criteria for synthetic networks,” *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3258–3265, July 2017.
[20] D. Sheet-SEL, “3555 real time automation controller (rtac),” *Accessed: Aug*, vol. 3, pp. 20 181 231–170 401, 2019.
[21] R. AcSelerator, “Sel-5033 software, instruction manual,” 2017.
[22] H. Huang and K. Davis, “Extracting substation cyber-physical architecture through intelligent electronic devices’ data,” in *2018 IEEE Texas Power and Energy Conference (TPEC)*. IEEE, 2018, pp. 1–6.
[23] I. A. Oyewumi, A. A. Jillepalli, P. Richardson, M. Ashrafuzzaman, B. K. Johnson, Y. Chakhchoukh, M. A. Haney, F. T. Sheldon, and D. C. de Leon, “Isaac: The idaho cps smart grid cybersecurity testbed,” in *2019 IEEE Texas Power and Energy Conference (TPEC)*. IEEE, 2019, pp. 1–6.
[24] H. Albunashee, C. Farnell, A. Suchanek, K. Haulmark, R. McCann, J. Di, and A. Mantooth, “A testbed for detecting false data injection attacks in systems with distributed energy resources,” *IEEE Journal of Emerging and Selected Topics in Power Electronics*, 2019.
[25] F. Shariatzadeh, C. B. Vellaithurai, S. S. Biswas, R. Zamora, and A. K. Srivastava, “Real-time implementation of intelligent reconfiguration algorithm for microgrid,” *IEEE Transactions on sustainable energy*, vol. 5, no. 2, pp. 598–607, 2014.
[26] J. Leonard, R. Hadidi, and J. C. Fox, “Real-time modeling of multi-level megawatt class power converters for hardware-in-the-loop testing,” in *2015 International Symposium on Smart Electric Distribution Systems and Technologies (EDST)*. IEEE, 2015, pp. 566–571.
[27] D. Watson, C. Hastie, and M. Rodgers, “Comparing different regulation offerings from a battery in a wind r&d park,” *IEEE Transactions on Power Systems*, vol. 33, no. 3, pp. 2331–2338, 2017.
[28] D. Watson, T. Chakraborty, and M. Rodgers, “The need for scada communication in a wind r&d park,” *Sustainable Energy Technologies and Assessments*, vol. 11, pp. 65–70, 2015.

Authorized licensed use limited to: Texas A M University. Downloaded on May 10,2022 at 21:51:22 UTC from IEEE Xplore. Restrictions apply.