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

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

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

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 realtime 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:

- 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.
- 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



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

umber	560	-	_	ind By Number	Point Type	Counts		_
ame			-	Find By Name	binary in	1 3 0	nary Out	
tal Daia	, 20				Analog In	18 A	nalog Out 2	
Darie Darie	ud Multinline I				Counter In	0		
eculte a	nd Control All	Points Binary	In Points Analo	To Points Cour	ter In Points	Binary Out Point		• 1
	Outstation	Object Type	Object ID By	Field Name	Value	Point Type		-
	Number		Number					
1	560	Branch	5047 TO 5260	STATUS	1.000	Binary Input		
2	560	Branch	5260 TO 5045	STATUS	1.000	Binary Input		
3	560	Branch	5261 TO 5260	STATUS	1.000	Binary Input		
4	560	Branch	5262 TO 5260	STATUS	1.000	Binary Input		
5	560	Branch	5263 TO 5260	STATUS	1.000	Binary Input		
6	560	Branch	5317 TO 5260	STATUS	1.000	Binary Input		
7	560	Branch	5261 TO 5246	STATUS	1.000	Binary Input		
8	560	Gen	5262 #1	STATUS	1.000	Binary Input		
9	560	Gen	5263 #1	STATUS	1.000	Binary Input		
10	560	Branch	5047 TO 5260	MWFROM	-1123.818	Analog Input		
11	560	Branch	5047 TO 5260	MVARFROM	118.991	Analog Input		
12	560	Branch	5260 TO 5045	MWFROM	-1415.104	Analog Input		
13	560	Branch	5260 TO 5045	MVARFROM	100.882	Analog Input		
14	560	Branch	5261 TO 5260	MWFROM	-79.823	Analog Input		
15	560	Branch	5261 TO 5260	MVARFROM	7.186	Analog Input		
16	560	Branch	5262 TO 5260	MWFROM	1211.658	Analog Input		
17	560	Branch	5262 TO 5260	MVARFROM	42.988	Analog Input		
18	560	Branch	5263 TO 5260	MWFROM	1024.040	Analog Input		
19	560	Branch	5263 TO 5260	MVARFROM	32.867	Analog Input		
20	560	Branch	5317 TO 5260	MWFROM	-2432.885	Analog Input		
21	560	Branch	5317 TO 5260	MVARFROM	137.132	Analog Input		
22	560	Branch	5261 TO 5246	MWFROM	79.823	Analog Input		
23	560	Branch	5261 TO 5246	MVARFROM	-7.186	Analog Input		
24	560	Gen	5262 #1	MW	1211.658	Analog Input		
25	560	Gen	5262 #1	MVAR	42.988	Analog Input		
26	560	Gen	5263 #1	MW	1024 040	Analog Input		

Figure 2. Outstation Information Dialog

Point Object ID (also used	for pasting and aux files) Branch '4042' '4041' '1'
Change Point Obje	ct
Point Type Binary Input Analog Input Counter Input Binary Output Analog Output	Point Field (Depends on Object Type) STATUS Event Class
√ <u>o</u> ĸ	Save Cancel ? Help Print

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



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 cyberphysical 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



Figure 5. One-Line Diagram of Substation GLEN ROSE1

synthetic 2000-bus Texas case [19] to configure the Power-World 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.

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

PowerWorld_RTAC_S	560_DNP						×
Other, Client - Ethe	ernet [DNP Protocol]				Advar	nced Settings 🔲	
Settings	Setting	Value	Range	Description	Comment		
Binary Inputs	Communications						
Double Bit Inputs	Transport Protocol	TCP	TCP,UDP	Use TCP or UDP as the ethernet transport protocol.			
Taxa Calman	Client IP Port	20010	23,1024-65534	Local RTAC IP port for this DNP client session.			
bnary outputs	Client UDP Broadcast Port	20010	1-65534	Remote UDP port to which this DNP clent transmits UDP broadcast messages.			
Counters	Server IP Address	172.168.2.10	Valid IPv4 Addr	IP address of the remote DNP server connection.			
Analog Inputs	Server IP Port	20000	23,1024-65534	IP port of the remote DNP server connection.			
Analog Outputs	Date-Time						
Datasets	UTC Offset	0	-720 to 840 (mi	Local Time offset from Universal Time			
	DST Enabled	True	True,False	Enable Daylight Savings Time			
HOU HIN Settings	DNP						
Custom Requests	Client DNP Address	559	0-65519	DNP source address. The local address of this RTAC client session. Addresses 65520			
Tags	Server DNP Address	560	0-65519	DNP destination address. The address of the remote IED poled by this client session.			
Controller	Integrity Poll Period	60000	0, 100-1000000	Class 1,2,3,0 integrity pol period. Set to 0 to disable.			
	Class 1,2,3 Polling Period	5000	0, 100-1000000	Class 1,2,3 Poling Period. Set to 0 to disable.			
	Pol Timeout	7000	100-65535 (mili	Time allowed for attached DNP Server to respond to a poll. If time is exceeded, this D			
	Number of Poll Retries	1	0-255	The number of poll retries before the connected DNP Server is considered offline.			
	1 of 13 🚺 🗐 🗐 🗐						>

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

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 7. Client PowerWorld_RTAC_560 Controller

Summar Conne Valid S	y cted Clients cans	1	Vali Sim	d Com ulatior	mano n Eve	ls Re	eive	d	0							~	Close				
Input Co	intingency Act	ions	Simulation Actions	Simu	lation	Ever	nts	Serv	er Lo	9 C	onne	cted	Clien	ts E	NP3	Log	Options				
🔽 Log	Outgoing DN	PS Me	essages 🔽 Log	Encomi	ing D	NPS	lessa	ages													
	Time		Source	Τ					_			Hea	Da	ta				 Т	-	 	^
58				E8	C9	01	3C	02	06	3C	03	06	3C	04	06	7D	AD				
59	11:16:43	PM	Outgoing	05	64	0A	44	2F	02	30	02	48	C0								
60				C0	C9	81	00	00	5B	DF											
61	11:16:48	PM	Incoming	05	64	11	C4	30	02	2F	02	CE	63								
62				E9	CA	01	3C	02	06	3C	03	06	3C	04	06	08	7A				
63	11:16:48	PM	Outgoing	05	64	A 0	44	2F	02	30	02	48	C0								
64				C0	CA	81	00	00	1A	D5											
65	11:16:53	PM	Incoming	05	64	11	C4	30	02	2F	02	CE	63								
66				EA	CB	01	3C	02	06	3C	03	06	3C	04	06	D6	14				
67	11:16:53	PM	Outgoing	05	64	a 0	44	2F	02	30	02	48	C0								
68				C0	СВ	81	00	00	F2	17											~

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

lame		-		Find By Nu	mber	Point	Type C	ounts	_			_
	Ë		-	Find By N	ama	Binary	/ In	9	Binar	y Out	9	
			<u>.</u>	T Ind by Iv	ame	Analo	g In	18	Analo	g Out	2	_
otal Points	s 3	18				Cours	-	0	_			
can Period	d Multipli	er 1	=			court	ler m	0				
eculte an	d Contro	All Pointe Bin	any To Pointe An	alog In Points	low	nter In Po	inte Ì B	inary Out	Pointe]	Analog ()ut Pointe	,1
courto un	a contra		ally information		1000		1	indi y Out	roma p	and og v	Juction	· I
	Numb	er Index	ed Object lyp	Numb	D By Der	Field N	ame	Analog	alue			
1		560	0 Branch	5047 TO	5260	MWFRO	м	-112	3.811			
2		560	1 Branch	5047 TO	5260	MVARFR	OM	11	8.990			
3		560	2 Branch	5260 TO	5045	MWFRO	M	-141	5.102			
4		560	3 Branch	5260 TO	5045	MVARFR	ом	10	0.885			
5		560	4 Branch	5261 TO	5260	MWFRO	M	-3	9.822			
0		560	5 Branch	5261 10	5260	MVARFR	ОМ	101	7.186			
0		560	7 Pranch	5262 10	5260	MUNPRO		12	1.075			
0		560	8 Branch	5262 TO	5260	MW/ERO	M	103	4 005			
10		560	9 Branch	5263 TO	5260	MVARER	ОМ	102	2.873			
11		560	10 Branch	5317 TO	5260	MWFRO	M	-24	2.873			
12		560	11 Branch	5317 TO	5260	MVARFR	ом	13	7.137			
13		560	12 Branch	5261 TO	5246	MWFRO	M		9.822			
14		560	13 Branch	5261 TO	5246	MVARFR	ОМ		7.186			
15		560	14 Gen	5262 #1		MW		121	1.673			
16		560	15 Gen	5262 #1		MVAR		4	2.978			
17		560	16 Gen	5263 #1		MW		102	4.005			
her, Client - Eth	hernet [DNP	Protocol]										S
her, Client - Eth ettings	hernet (DNP	Protocol]										প্র
her, Client - Eth ettings inary Inputs	hernet (DNP	^p rotocol] umn header here to group I	by that column		Cont No. or b	ur Tan Tuna	Tan Alar	Crather Value	Test Marrih da	Marribula	Daadhard	हो। रस्क
her, Client - Eth ettings inary Inputs ouble Bit Inputs	brag a col Enable	Protocol] Imin header here to group 1 Tag Name PowerWinds RTAC 560 DNP	by that column	2 17 5260 1 MM/FBOM	Font Numb	er Tag Type	Tag Alias	Status Value	Inst Magnitude	e Magnitude	Deadband	رچ Zero I
her, Client - Eth ettings inary Inputs ouble Bit Inputs inary Outputs	hernet (DNP Drag a col Enable True	Protocol] Imm header here to group 1 Tag Name PowerWorld_RTAC_560_DNP. PowerWorld_RTAC_560_DNP.	by that column AI_Substation_560_Branch_504 AI_Substation_560_Branch_504	12 17_5260_1_MWFROM 17_5260_1_MWFROM	Point Numb	er Tag Type 0 MV 1 MV	Tag Alias	Status Value	Inst Magnitude	e Magnitude 0	Deadband 0 10 0 10	Zero I 0
her, Client - Eth ettings inary Inputs ouble Bit Inputs inary Outputs outputs	hernet [DNP Drag a col Enable True True True	Protocol] Imm header here to group I Tag Name PowerWorld_RTAC_560_DNP. PowerWorld_RTAC_560_DNP. PowerWorld_RTAC_560_DNP.	by that column AI_Substation_560_Branch_504 AI_Substation_560_Branch_504 AI_Substation_560_Branch_526	2 7_5260_1_MWFROM 17_5260_1_MWFROM 10_5045_1_MWFROM	Foint Numb	er Tag Type 0 Mr 1 Mr 2 Mr	Tag Alias	Status Value	Inst Magnitude	e Magnitude 0 0	Deadband 0 10 0 10 0 10	Zero I 0 0
her, Client - Eth ettings inary Inputs ouble Bit Inputs inary Outputs ounters salard Insyste	hernet [DNP Drag a col Enable True True True True	Protocol] Imm header here to group 1 Tag Name PowerWorld (RTAC_560_DNP. PowerWorld (RTAC_560_DNP. PowerWorld (RTAC_560_DNP.	by that column Al Substaton 560 Branch 504 Al Substaton 550 Branch 504 Al Substaton 550 Branch 526 Al Substaton 560 Branch 526	2 17_5260_1_MIXAFROM 17_5280_1_MIXAFROM 10_5045_1_MIXAFROM 10_5045_1_MIXAFROM	Point Numb	er Tag Type 0 MV 1 MV 2 MV 3 MV	Tag Alias	Status Value	Inst Magnitude	Magnitude 0 0 0 0	Deadband 0 10 0 10 0 10 0 10 0 10	2ero 1 0 0 0
her, Client - Eth ettings inary Inputs iouble Bit Inputs inary Outputs iounters nalog Inputs palog Octouts	hernet (DNP Drag a col Enable True True True True True	Protocol] Tag Name PowerWorld, RTAC_560_DNP. PowerWorld, RTAC_560_DNP. PowerWorld, RTAC_560_DNP. PowerWorld, RTAC_560_DNP.	by Host column Al Substaton 560 Branch 504 Al Substaton 560 Branch 504 Al Substaton 560 Branch 526 Al Substaton 560 Branch 526	2 77,5260,1,MWFROM 17,5260,1,MWFROM 10,5045,1,MWFROM 10,5045,1,MWFROM 11,5280,1,MWFROM	Font Numb	er Tag Type 0 Mr 1 Mr 2 Mr 3 Mr 4 Mr	Tag Alas	Status Value	Inst Magnitude	Magnitude 0 0 0 0 0 0	Deadband 0 10 0 10 0 10 0 10 0 10 0 10 0 10	2ero 1 0 0 0 0
ther, Client - Eth ettings inary Inputs touble Bit Inputs inary Outputs iounters nalog Inputs inalog Outputs	bring a col Enable True True True True True True	Protocol] Tag Name PowerWorld, RTAC, 560, DIVP. PowerWorld, RTAC, 560, DIVP. PowerWorld, RTAC, 560, DIVP. PowerWorld, RTAC, 560, DIVP. PowerWorld, RTAC, 560, DIVP.	by that column Al Substation 560 Branch 504 Al Substation 560 Branch 524 Al Substation 560 Branch 526 Al Substation 560 Branch 526 Al Substation 560 Branch 526	3 75,5260_1_WWFROM 175,5260_1_WWFROM 10_5045_1_WWFROM 10_5045_1_WWFROM 11_5260_1_WWFROM	Font Numb	Tag Type 0 MV 1 MV 2 MV 3 MV 4 MV 5 MV	Tag Alas	Status Value	Inst Magnitude	Magnitusia 0 0 0 0 0 0 0 0	Deadband 0 100 0 100 0 100 0 100 0 100 0 100	2ero 1 0 0 0 0 0
ther, Client - Eth ieitings ilinary Inputs Souble Bit Inputs ilinary Outputs Counters nalog Inputs knalog Outputs Jatasets	bernet (DNP Drag a col Enable True True True True True True True Tru	Protocol] Tag Name Power Viord, ETAC, 560, DAP- Power Viord, ETAC, 560, DAP- Power Viord, ETAC, 560, DAP- Power Viord, RTAC, 560, DAP-	ky that column Al Substaton (50) Branch (54 Al Substaton (50) Branch (54 Al Substaton (50) Branch (55 Al Substaton (50) Branch (55 Al Substaton (50) Branch (55 Al Substaton (50) Branch (55) Al Substaton (50) Branch (55)	22 47_5260_1_MWR0M 47_5280_1_MWR9R0M 40_5045_1_MWR9R0M 40_5045_1_MWR9R0M 41_5280_1_MWR9R0M 41_5280_1_MWR9R0M 42_5280_1_MWR9R0M	Foint Numb	rer Tag Type 0 Mr 1 Mr 2 Mr 3 Mr 4 Mr 5 Mr 6 Mr	Tag Alias	Status Value	Inst Magnitude	Magnitude 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Deadbend 0 100 0 100 0 100 0 100 0 100 0 100 0 100	Image: Second
thes, Client - Eth Settings Snary Inputs Souble Bit Inputs Souble Bit Inputs Sinary Outputs Counters nalog Snputs Analog Outputs Volu Pin Settings	hernet (DNP Drag a col Enable True True True True True True True Tru	https:// Tagitame PowerWork #145_560_DHP- PowerWork #145_560_DHP- PowerWork #145_560_DHP- PowerWork #145_560_DHP- PowerWork #145_560_DHP- PowerWork #145_560_DHP- PowerWork #145_560_DHP- PowerWork #145_560_DHP- PowerWork #145_560_DHP-	y that column AL Substaton, 560 Janut, 544 AL Substaton, 560 Janut, 544 AL Substaton, 560 Janut, 554 AL Substaton, 560 Janut, 554 AL Substaton, 560 Janut, 554 AL Substaton, 560 Janut, 554 AL Substaton, 560 Janut, 555 AL Substaton, 560 Janut, 555 AL Substaton, 560 Janut, 555	22 47_5260_1_MINFROM 47_5260_1_MINFROM 40_5045_1_MINFROM 40_5045_1_MINFROM 41_5260_1_MINFROM 42_5260_1_MINFROM 42_5260_1_MINFROM 42_5260_1_MINFROM 42_5560_1_MINFROM	Foint Numb	Tag Type 0 Mr 1 Mr 2 Mr 3 Mr 4 Mr 5 Mr 5 Mr 7 Mr 8 Mr	Tag Alias	Status Value	Inst Magnitude	Magnitude 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Deadband Deadband Deadband Data	
her, Client - Eti ettings inary Inputs iouhle Bit Inputs iouhle Bit Inputs iouhler Bit Inputs iouhlers ouhlers nalog Outputs latasets OU Pin Settings Juston Requests	hernet (DNP Drog a col Enable True True True True True True True Tru	httocol] min headen kenet to group 1 Tog Name PowerWork (FIAC, 560, DIP. PowerWork (FIAC, 560, DIP.	ly that column M. Schraten, 500 (Sendi, 504) M. Schraten, 500 (Sendi, 504)	2 7,5260_1,MNFROM 17,5260_1,MNFROM 10,545_1,MNFROM 10,5451_1,MNFROM 11,5260_1,MNFROM 12,5260_1,MNFROM 12,5260_1,MNFROM 13,5260_1,MNFROM 13,5260_1,MNFROM 13,5260_1,MNFROM	Foint Numb	Tag Type 0 Mr 1 Mr 2 Mr 3 Mr 4 Mr 5 Mr 5 Mr 6 Mr 7 Mr 8 Mr 9 Mr	Teg Alies	Status Value	Inst Magnitude	Magnitude 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Deadband Deadband Do Do D0	2ero D 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
ther, Client - Bt ettings inary Inputs isouble Bit Inputs isoury Outputs iounters nalog Inputs inalog Outputs latasets OUP in Settings Justion Requests lags	hernet [DNP Drag a col Endole True True True True True True True Tru	Instruction Tag Name Tag Name PowerWork (FLAC_560_DPR- PowerWork (FLAC_560_DPR-	y that column Al Schotaton 500 Brands 504 Al Schotaton 500 Brands 504	2 7, 5260 MIRFOM 6, 5045 MIRFOM 6, 5045 MIRFOM 6, 5045 MIRFOM 6, 5045 MIRFOM 6, 5260 MIRFOM 12, 5260 MIRFOM 13, 5260 MIRFOM 13, 5260 MIRFOM 13, 5260 MIRFOM	Foint Numb	Tag Type 0 Mr 1 Mr 2 Mr 3 Mr 4 Mr 5 Mr 6 Mr 7 Mr 8 Mr 7 Mr 8 Mr 9 Mr 20 Mr	Teg Allas	Status Value	Inst Magnitude	Magnitusk 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Deadband 0 100 0 100 0 100 0 100 0 100 0 100 0 100 0 100 0 100 0 100 0 100 0 100 0 100 0 100 0 100	
ther, Client - BH ettings inary Inputs isouble BI: Inputs isoury Outputs iounters nalog Inputs inary Outputs latasets OUP in Settings Justion Requests lags isotroller	benet (DNP Drag a col Endole True	hetecol in the back to be to group b Tag lates PowerWork (FLL, Sol D.H.P. PowerWork (FLL, Sol D.H.P.	by that column 41 Substaton, 560 Jiranh, 504 41 Substaton, 500 Jiranh, 504 41 Substaton, 500 Jiranh, 536 41 Substaton, 500 Jiranh, 537 41 Substaton, 500 Jiranh, 537 41 Substaton, 500 Jiranh, 537	2 7 530 J WIROM 7 530 J WIROM 8 596 J WIRFOM 8 596 J WIRFOM 1 530 J WIRFOM 8 530 J WIRFOM 3 530 J WIRFOM 3 530 J WIRFOM 7 530 J WIRFOM	Foint Numb	Tag Type 0 Mr 1 Mr 2 Mr 3 Mr 4 Mr 5 Mr 6 Mr 7 Mr 8 Mr 7 Mr 8 Mr 9 Mr 20 Mr 11 Mr	Tag Alias	Status Value	Inst Magnitude	Magnitude Magnitude 0 0 0 0 0 0 0 0 0 0 0 0 0	Deadband 0 100 0 100 0 100 0 100 0 100 0 100 0 100 0 100 0 100 0 100 0 100 0 100 0 100 0 100 0 100 0 100 0 100 0 100	Image: 2ero D 0
her, Client - Et/ ettings inary Inputs iouble Bit Inputs iounters nalog Inputs inary Outputs iounters nalog Outputs istasets OU Prin Settings Justom Requests lags jontroller	hernet [DNP Drag a col Endble > True	Telescol Taplane Taplane PowerWork (FLC, 560, DPA- PowerWork (FLC, 560, DPA-	by Ibalt column Al Solotation, 560, Brench, 594 Al Solotation, 560, Brench, 514 Al Solotation, 560, Brench, 514 Al Solotation, 560, Brench, 514	2 7 (160),UMIRO 7 (260),UMIROM 8 (94),UMIROM 8 (94),UMIROM 8 (150),UMIROM 8 (150),UMIROM 8 (150),UMIROM 8 (150),UMIROM 9 (150),UMIROM 7 (150),UMIROM 7 (150),UMIROM	Font Numb	Tag Type 0 MV 1 MV 2 MV 3 MV 4 MV 6 MV 6 MV 7 MV 8 MV 9 MV 90 MV 11 MV 12 MV	Tag Alias	Status Value	Inst Magnitude	Magnitude Magnitude 0 0 0 0 0 0 0 0 0 0 0 0 0	Deadband 0 10 0 10 0 10 0 10 0 10 0 10 0 10 0 10 0 10 0 10 0 10 0 10 0 10 0 10 0 10 0 10	Zero I 0
her, Client - Et/ ettings inary Inputs iouble Bit Inputs iouble Bit Inputs iounters analog Inputs inalog Outputs atlasets OU Phi Settings Justom Requests aga jontroller	hernet [DNP Drag a col Endble > True	Telescol Tag New Constraints of the State	by Balt Column H. Schetaton, 560 (Janob, 594 H. Schetaton, 560 (Janob, 594 H. Schetaton, 500 (Janob, 504 H. Schetaton, 500 (Janob, 504) H. Schetaton, 500 (Janob, 504) H. Schetaton, 500 (Janob, 504)	2 7 (320) J. M. MR 7 (320) J. M. MR 8 (340 J. M. MR 8 (350 J. M. MR 9 (350 J. M. MR) 9 (350 J. M. MR 9 (350 J. M. MR 9	Font Numb	 Tag Type Mv 	Tag Alas	Status Value	Inst Magnitude	Magnitude 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Deadband 0 10 0 10 0 10 0 10 0 10 0 10 0 10 0 10 0 10 0 10 0 10 0 10 0 10 0 10 0 10 0 10 0 10 0 10	 Zero I Zero I D <lid< li=""> D D <li< td=""></li<></lid<>
her, Client - Eti ettings inary Irputs iouble Bit Inputs iounters analog Inputs analog Inputs analog Upputs attasets OU Pin Settings USE Pin Settings app iontroller	hernet [DNP Drag a col Endole True True True True True True True Tru	hetecol Tay lane Tay lane Tay lane Tay lane Howerhold, STLC, Sob (JPR- Newerhold, STLC, Sob (JPR- Newerhold	IV that column A Substatum, 540 Sensin, 544 Substatum, 540 Sensin, 544 Substatum, 540 Sensin, 554 Substatum, 550 Sensin, 556 Substatum, 5	2 7) 550 _ J.W.REK 70 _ 550 _ J.W.REK 70 _ 550 _ J.W.REK 70 _ 550 _ J.W.REK 71 _ 550 _ J.W.REK 71 _ 550 _ J.W.REK 70 _ J.W.REK 70 _ J.W.REK 70 _ J.W.REK 70 _ J.W.REK 70 _ J.W.		Tag Type 0 MY 1 MY 2 MY 3 MY 4 MY 5 MY 5 MY 6 MY 9 MY 9 MY 90 MY 90 MY 11 MY 12 MY 11 MY 13 MY	Teg Ales	Status Value	Inst Magnitude	Magnitude 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Desident 0 300 0 100	Image: second
ther, Client - Bi Settings Sinary Inputs Sounders Sounders Sounders Sounders OUI Pri Settings Custom Requests Fags Controller	Prog a col Prog a col Endole True True True True True True True Tru	Instructor) Toy Inner PowerWork (J. K.G. 500, Die- NeuerWork (J. K.G. 500, Die-	ly that column Al Substatum, 560 (Jamob, 504) Al Substatum, 500 (Jamob, 504) Al Substatum,	7 (1991) (MIRON 9 (290) (MIRON 9 (200) (MIRON 9 (MIRON		Tag Type 0 Mv 1 Mv 2 Mv 3 Mv 4 Mv 5 Mv 6 Mv 7 Mv 8 Mv 7 Mv 8 Mv 10 Mv 11 Mv 12 Mv 11 Mv 12 Mv 13 Mv 14 Mv	Teg Alles	Status Value	Inst Magnitude	Magnitude Magnitude	 Deadband 0 100 0 <li< td=""><td>Zero D Zero D D</td></li<>	Zero D Zero D D
ther, Client - Et lettings lineny Inputs lineny Outputs Dounters nalog Inputs Sounters OU Pin Settings Juston Requests lings Sontroller	hernet (DNP Drog a col Enable True	heated Toylors Tayl	ly that column Al Schetzen, 500 Jennin, 504 Al Schetzen, 500 Jennin, 505 Al Schetzen, 500 Jennin, 504 Al Schetzen, 500 Jennin, 504 Al Schetzen, 500 Jennin, 504 Al Schetzen, 500 Jennin, 504 Jennie Jennie Je	27,530,1,44000 77,530,1,44000 77,550,1,44000 70,945,1,44000 70,950,1,440000 70,950,1,44000000000000000000000000000000000	Fort Numb	Tag Type 0 MV 1 Mr 2 MV 4 MV 4 MV 5 MV 5 MV 7 MV 8 MV 9 MV 9 MV 10 MV 11 Mr 11 Mr 12 MV 13 MV 13 MV 15 MV 15 MV	Teg Ales	Status Value	Inst Magnitude	Magnitude Magnitude	 Deadband 0 100 0 <li< td=""><td>Cerro C Cerro C C</td></li<>	Cerro C C
ther, Client - Bi Settings Binary Inputs Double Bit Inputs Double Bit Inputs Sinary Outputs Counters Analog Outputs Datasets OUI Pin Settings Justion Requests Tags Sontroller	hernet (DIA) Drog a col Endole Probe True	Hentroll Testime Testime Testime Hentrold 214C, 300, 244 November 214, 246, 240, 244 November 214, 240, 240, 240 November 214, 240,	y that column Al Substate, 560 Janob, 544 Al Substate, 560 Janob, 544 Al Substate, 560 Janob, 544 Al Substate, 560 Janob, 554 Al Substate, 560 Janob, 554 Al Substate, 550 Janob, 555 Al Substate, 550 Janob, 550	27 (360) (MARGM 77 (350) (MARESON 97 (350) (MARESON 90	Fort Numb	Tag Type 0 Mr 1 Mr 2 Mr 3 Mr 4 Mr 5 Mr 6 Mr 9 Mr 12 Mr 12 Mr 13 Mr 14 Mr 15 Mr 16 Mr 17 Mr	Teg Alas	Status Value	Inst Magnitude	Magnitude O	Deadband 0 100	2ero D 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
her, Client - Eb ettings inary Inputs isouble Bit Inputs isoury Outputs isoury Outputs isatasets OUP in Requests ago iontroller	Incent (DIV) Ince I color Ince I color In	Hereined Toyland Bancel Lang Lang, 2013 Toylande Toyl	ly that column Al Schertston, 560 Janesh, 594 Al Schertston, 580 Janesh, 594 Al Schertston, 590 Janesh, 594 Al Schertston, 590 Janesh, 534 Al Schertston, 590 Janesh, 535 Al Schertston, 590 Janesh, 535 Al Schertston, 590 Janesh, 538 Al Schertston, 590 Janesh, 538 Al Schertston, 590 Janesh, 538 Al Schertston, 590 Janesh, 538 Al Schertston, 590 Janesh, 538	100MW 100WW 100MW 100WW	Sint hund	Tag Type 0 Mr 1 Mr 2 Mr 3 Mr 4 Mr 5 Mr 6 Mr 7 Mr 8 Mr 9 Mr 10 Mr 12 Mr 13 Mr 14 Mr 15 Mr 17 Mr	Teg Alas	Status Value	Inst Magnitude	Magnitude O	Descharting 0 100	I Zero D 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

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

WHO HURD_KIAU_						
Uther, Client - Eth	emet [UNP Protocol]					
Settings	Expression	Туре	Value	Prepared value	Address	Cr^
Rinary Innuts	🗉 🍯 PowerWorld_RTAC_560_DNP.A1_Substation_560_Branch_5047_5260_1_MVARFROM	MV				
	🛊 instMag	REAL	118.990372			
Double bit inputs	🖗 mag	REAL	118.990372			
Binary Outputs	🖗 range	RANGE_T	normal			
Counters	⊟ ≬ q	quality_t				
Inales Insuite	🌶 validity	VALIDITY_T	good			
A long a poo	🗉 🏚 detailQual	detaiQual_t				
Analog Outputs	🛊 source	SOURCE_T	process			
Datasets	👂 test	BOOL	FALSE			
POUPIn Settings	operator8locked	BOOL	FALSE			
	H #1	timeStamp_t				
Oustom Requests	🛊 db	REAL	100			
Tags	🛊 zeroDb	REAL	2			
Controller	* 🛊 rangeC	rangeConfigReal_t				
	PowerWorld_RTAC_560_DNP.AI_Substation_560_Branch_5047_5260_1_MWFROM	MV				
	PowerWorld_RTAC_560_DNP.A1_Substation_560_Branch_5260_5045_1_MVARFROM	MV				
	PowerWorld_RTAC_560_DNP.A1_Substation_560_Branch_5260_5045_1_MWFROM	MV				
	PowerWorld_RTAC_560_DNP.AI_Substation_560_Branch_5261_5246_1_MVARFROM	MV				
	PowerWorld_RTAC_560_DNP.A1_Substation_560_Branch_5261_5246_1_MWFROM	MV				

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

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

PowerWorld_RTAC_	560_DNP					×
Other, Client - Eth	ernet [DNP Protocol]					
Settings	Expression	Туре	Value	Prepared value	Address	Cr^
Binary Innuts	🗏 📓 PowerWorld_RTAC_560_DNP.BI_Substation_560_Branch_5047_5260_1	SPS				
	stVal	800L	TRUE			
Dorpie sit tubrita	H 🖗 q	quality_t				
Binary Outputs	validity	VALIDITY_T	good			
Counters	🗷 🛊 detaiQual	detaiQual_t				
And a Treate	source	SOURCE_T	process			
Analog Inputs	< test	800L	FALSE			
Analog Outputs	operatorBlocked	800.	FALSE			
Datasets	H Øt	timeStamp_t				
DOLLDIA Cattleast	PowerWorld_RTAC_560_DNP.BI_Substation_560_Branch_5260_5045_1	SPS				
Fourinsetungs	PowerWorld_RTAC_560_DNP.BI_Substation_560_Branch_5261_5246_1	SPS				
Custon Requests	PowerWorld_RTAC_560_DNP.BI_Substation_560_Branch_5261_5260_1	SPS				
Tags	PowerWorld_RTAC_560_DNP.BI_Substation_560_Branch_5262_5260_1	SPS				
Controlar	PowerWorld_RTAC_560_DNP.BI_Substation_560_Branch_5263_5260_1	SPS				
CONTORO	PowerWorld_RTAC_560_DNP.BI_Substation_560_Branch_5317_5260_1	SPS				
	PowerWorld_RTAC_560_DNP.BI_Substation_560_Gen_5262_1	SPS				
	* 📓 PowerWorld_RTAC_560_DNP.BI_Substation_560_Gen_5263_1	SPS				
	PowerWorld_RTAC_560_DNP.80_Substation_560_Branch_5047_5260_1	DNPC				
	* 📓 PowerWorld_RTAC_560_DNP.B0_Substation_560_Branch_5260_5045_1	DNPC				

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

PowerWorld_RTA	C_560_DNP					
Other, Client - E	themet [DNP Protocol]					
Settings	Expression	Туре	Value	Prepared va	lue Address	Cr
Binary Inputs	🗉 🙆 PowerWorld_RTAC_560_DNP.AO_Substation_560_Gen_5262_1_MWSETPOINT	APC				
	= 🖉 oper	oper APC				
Double bit input	s 🖉 🖉 setMag	REAL	() 1000			
Binary Outputs	trigger	BOOL	🕒 TRU			
Counters	⊞ @ q	quality_t				
tealer levete		timeStamp_				
Hand a boo	🗏 🧳 origin	originator_t				
Analog Outputs	🗏 🌒 status	MV				
Datasets	🖲 🌒 origin	originator_t				_
POU Pin Setting	PowerWorld_RTAC_560_DNP.AO_Substation_560_Gen_5263_1_MWSETPOINT	APC				
	PowerWorld_RTAC_560_DNP.81_Substation_560_Branch_5047_5260_1	SPS				
Custom keques	PowerWorld_RTAC_560_DNP.81_Substation_560_Branch_5260_5045_1	SPS				
Tags	PowerWorld_RTAC_560_DNP.81_Substation_560_Branch_5261_5246_1	SPS				
Controller	PowerWorld_RTAC_560_DNP.81_Substation_560_Branch_5261_5260_1	SPS				
	* Powerworld_RIAC_560_DNP261_Substation_560_Branch_5262_5260_1	SPS				
	PowerWorld_RIAC_560_DNP35_Substation_560_Branch_5263_5260_1	SPS				
	* Polienwond KIAL Sou DWP/81 Substation Sou Branch SS1/ S260 1	995				_
PowerWorld_RTA	IC_SED_DNP					
Other, Client - E	themet [UNP Protocol]					
Settings	Expression	Туре	Value	Prepared value	Address	Comment
Discourt Instalts	* 🗿 PowerWorld_RTAC_560_DNP.A1_Substation_560_Gen_5262_1_GENMVAR	W				
onely signs	B 🗿 PowerWorld_RTAC_560_DNP.A1_Substation_560_Gen_5262_1_GENMW	W				
Double Bit Input	s 🖉 🛊 instMag	REAL	1004.40973			
Binary Outputs	🛊 mag	REAL	1015.82452			
Counters	() range	RANGE_T	normal			
	= = • q	quality_t				
Analog Inputs	≕ ∲ q ∲ validty	quality_t VALIDITY_T	good			
Analog Inputs Analog Outputs	☐ Ø q Ø volidty ₩ Ø detaiQual	quality_t VALIDITY_T detaiQual_t	good			
Analog Inputs Analog Outputs Datasets		quality_t VALIDITY_T detaiQual_t SOURCE_T	good process			
Analog Inputs Analog Outputs Datasets POLI Din Satting	= Ø validity # Ø detalQual Ø source Ø text	quality_t VALIDITY_T detaiQual_t SOLRCE_T BOOL	good process FALSE			
Analog Inputs Analog Outputs Datasets POU Pin Setting	in € € Ø vildty # Ø desilgud Ø Source Ø Ø text Ø Ø operatorBlockad Ø	quality_t VALIDITY_T detaiQual_t SOURCE_T BOOL BOOL	good process FALSE FALSE			
Analog Inputs Analog Outputs Datasets POU Pin Setting Custom Request	 ⇒ 4 slidy ⇒ 6 datilya ⇒ 6 datilya ⇒ sora ⇒ fost ⇒ fost ⇒ spectoficidad ≥ 4 	quality_t VALIDITY_T detalQual_t SOURCE_T BOOL BOOL timeStamp_t	good process FALSE FALSE			
Analog Inputs Analog Outputs Datasets POU Pin Setting Custom Request Tags	□ 0 widty □ □ deallgual □ 0 text □ 0 text □ □ operation □ □ text □ □ operation □ □ text □ □ text □ □ text □ □ text	quality_t VALIDITY_T detalQual_t SOURCE_T BOOL BOOL timeStamp_t REAL	good process FALSE FALSE			
Analog Inputs Analog Outputs Datasets POU Pin Setting Custom Request Tags Controller	□ 0 □ 0 □ 0 □ 0 □ 0 □ 0 □ 0 □ 0 □ 0 □ 0 □ 0 □ 0 □ 0 □ 0 □ 0	quality_t VALDITY_T deta(Qual_t SOURCE_T BOOL BIONEStamp_t REAL REAL	good process FALSE FALSE 100 2			
Analog Inputs Analog Outputs Datasets POU Pin Setting Custom Request Tags Controller	□ 0 siddy □ □ deallyal □ 0 istic □ istic 0 □ istic 0	quality_t VALIDITY_T detaiQual_t SOURCE_T BOOL bmeStamp_t REAL REAL rangeConfigReal_t	good process FALSE FALSE 100 2			
Analog Inputs Analog Outputs Datasets POU Pin Setting Oustom Request Tags Controller	E 0 V 9	quality_t WALDDTY_T detaiQual_t SOURCE_T BOOL BOOL BrinsStamp_t REAL REAL rangeConfigReal_t W/	good process FALSE FALSE 100 2			

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

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-theloop 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

in an	Everyon	Type	Value	Prenared va	lue Address	0
ungs	E Constitued OTAC SEA DAD DI Orbetaliza SEA Cas C202 1	iype coo	ianae	Prepareo va	IDE MUUIES	
ary Inputs	PowerWorld_RTAC_550_DAP.0[_30512001_501_501_3250_1	342				
ble Bit Inputs	Powerworkd_stat	UNPC				
u Outrade	 V operate V deset trickles 	operand				
ay 00603	 P operation P operation 	operand				
inters		opersec.				
log Inputs	a deal	operand Book	O TOUS			
no Outraits		BUUL and the t				
	- v q	quarty_t	and			
tasets	Velocy R A desilout	VALIDUT_1	good			
U Pin Settings	* V DECATQUA	oetalQua_t				
store Recturest	V source	SURCE_I	process			
	y itsi A asustatifadad	8000	FALSE			
15	operatorbiobase	BUOL	FALSE			
ntroler	a et al a substantes	tmestamp_				
	* pusecong	pulseConfig	3			
	* ¢ ongn	originator_t				
	* Ø operLiose	operSPC				
	a a status	202				
ierWorld_RTA her, Client - E	A Browning Bran Star Star DWB RD Substation SSS Brann STAS SS45 1 S50 pre bernet [DNP Protoco]]	DADC.				Ø
erWorld_RTA ner, Client - E	A distance of the SSE Tray Bit Coloration SSE Branch Chill Sold 1 SSE 1 S	Туре	Value	Prepared value	Address	(comment)
erWorld_RTA her, Client - E ettings	A Description of STAT SEE PAREAR Sector SEE Brands SEE Sector	Type	Value	Prepared value	Address	Comment
erWorld_RTA her, Client - E ettings hery Inputs	All Reconfloct 21% SEL DB RO Schetzers SEL Reuch DBE DBE 1 CSD 31% CSD 31% February 2000 Selection Selection Selection Selection February 2000 Selection Selection Selection Selection Selection Selection Selection Selection Selection Selection Selection	Type APC SSS	Value	Prepared value	Address	Comment
erWorkl_RTM Ier, Client - E ttings Iary Inputs uble Bit Input	Compared PTZ SIX TAPRA Schemen SIX Rank SIX SIX 1 Compared PTZ SIX TAPRA Schemen SIX Rank SIX SIX 1 Compared PTZ SIX TAPRA Schemen SIX SIX 1 Posteriol Posteriol STX SIX TAPRA Schemen SIX SIX SIX 1 Posteriol STX SIX TAPRA Schemen SIX SIX SIX 1 Posteriol STX SIX TAPRA Schemen SIX SIX SIX 1	Type APC SPS BOD	Value	Prepared value	Address	Comment
erWorld_RTM rer, Client - E ttings rery Inputs uble Bit Input	Constructed FD2 444 704811 Ochement 448 Revuel 1544 546 1 C10(5) 70 C10(5) 70 Detected Dependent (DDP Photocol) Dependent (DDP Photocol) Dependent (DDP Photocol) Statistical Statistical Statistical Statistical Statistical Statistical Statistical Phonetholog(STAC) Statistical Statistical Statistical Statistical Phonetholog(STAC) Statistical Statistical Statistical Statistical Statistical Phonetholog(STAC) Statistical Statistical Statistic	Type APC SPS BOOL	Value	Prepared value	Address	Comment
erWorld_RTA ner, Client - E ettings nery Inputs suble Bit Input nery Outputs		Type APC SPS BOOL Quality_t MINITY_T	Value	Prepared value	Address	Comment
erWorld_RTA her, Client - E tttings hery Inputs ouble Bit Input hery Outputs sunters		Type APC SPS BOOL Quality_t VALIDITY_T detail/usi t	Value FALSE good	Prepared value	Address	Comment
erWorld_RTA ner, Client - E tttings nery Inputs suble Bit Input nery Outputs sunters salog Inputs		Type APC SPS BOOL quality_t VALIDITY_T detaQual_t SCIENCE T	Value FALSE good	Prepared value	Address	Comment
erWorld_RTA ner, Client - E tttings nery Inputs suble Bit Input nery Outputs sunters salog Inputs nalog Outputs		Type APC SPS BOOL Quality_1 VALIDITY_T detaiQual_1 SOURCE_T BOOL	Value FALSE good process	Prepared value	Address	Comment
erWorki_RTM her, Client - E titings hary Inputs buble Bit Inputs hary Outputs halog Inputs halog Outputs		Type APC 995 BOOL quality_1 vuLDITy_T detailud_1 SOURCE_T BOOL BOOL	Value FALSE good process FALSE	Prepared value	Address	Comment
erWorki_RTM her, Client - E titings hary Inputs buble Bit Inputs hary Outputs halog Inputs halog Outputs stasets		Type APC SPS BOOL Quality_1 VALIDITY_T detailQual_1 BOOL BOOL BOOL BOOL	Value FALSE good process FALSE FALSE	Prepared value	Address	Comment
er Work J str A ttings try Inputs uble Bit Inputs alog Inputs alog Cutputs tasets U Pin Settings		Type APC 955 800L quality_1 4talQual_1 SOURCE_T 800L 90L 90L 90L 90L 90L 90L 90L 90L 90L	Value FALSE good process FALSE FALSE	Prepared value	Address	Comment
er Worki jstrA tings tings any Inputs able Bit Inputs alog Inputs alog Cutputs alog Cutputs tasets U Pin Settings storn Request		Type APC 995 BOOL quality_1 VALIDTY_T BOOL BOOL BOOL BOOL BOOL BOOL BOOL BOO	Value FALSE good process FALSE FALSE	Prepared value	Address	Comment
erworki RTA ker, Client - E ttings whe Bit Inputs whe Bit Inputs any Outputs alog Dutputs alog Outputs itasets NU Pin Settings stom Request	a Reserved STAC SHI 2008 R. Solvention SHI Reach. SHI 5 Hit Stream [DDR Protoci] Eperation a Provemoid STAC, SHI 2009 R. Solvention, SHI Send, SHI 1 a Provemoid STAC, SHI 2009 R. Solvention, SHI Send, SHI 2009 R. a Provemoid STAC, SHI 2009 R. Solvention, SHI Send, SHI 2009 R. a a b a c a c a c a a a b a c a a a b a b a b a c a c a c a c a c a c a c a c a c a c a c a c a c a c a <td< td=""><td>Type APC 955 BOOL aukity_t VULUTV_T detalQual_t SOUKE_T BOOL BOOL BOOL BOOL BOOL BOOL BOOL BOO</td><td>Value FALSE good prorzes FALSE FALSE</td><td>Prepared value</td><td>Address</td><td></td></td<>	Type APC 955 BOOL aukity_t VULUTV_T detalQual_t SOUKE_T BOOL BOOL BOOL BOOL BOOL BOOL BOOL BOO	Value FALSE good prorzes FALSE FALSE	Prepared value	Address	
erworki grrA er, Client - E ttings ary Inputs uble Bit Input ary Outputs alog Dutputs alog Outputs alog Outputs tasets U Pin Settings stom Request 35	Compared TEX SHA TARRA Schemens SHA Reach SHA SHA 1 CONCOMP Permit Permit P	Type A/C 95 800L quality_1 vuLitrY_T 800LCE_T 800L 800L 800L 955 95 95 95 95 95 95	Value FLSS good FLSS FLSS FLSS FLSS	Prepared value	Address	Comment
er World RTM er, Client - E ttings ary Inputs uble Bit Input ary Outputs alog Inputs alog Outputs alog Outputs tasets U Pin Settings storn Request js ntroller	a Reserved FIZ SML TAREA Sciences SML Reach, SML SML 1 Copy Dr Experime termed [DRF Protoci] Experime Experime Proverviced STAC, SML DAVAD, Schenzen, SML Send, SML SML 1 a Proverviced STAC, SML DAVAD, Schenzen, SML Send, SML SML 1 a Proverviced STAC, SML DAVAD, Schenzen, SML Send, SML SML 1 a Proverviced STAC, SML DAVAD, Schenzen, SML Send, SML SML 1 a a a Proverviced STAC, SML DAVAD, Schenzen, SML Send, SML SML 1 a a b a b a b a b a b a c a c a c a c a c a c a c a c a c a c a c a c a c a c a	Type APC 95 800L quality_1 detaQual_t 50LRCE_T 800L 800L 800L 905 95 95 95 95 95 95 95 95	Value F1152 pood process F1152 F1152	Prepared value	Address	
er World RTM er, Client - E trings ery Inputs uble Bit Input any Outputs alog Inputs alog Outputs tasets U Pin Settings storn Request ps ntroller	Comparison of TUP SHA TAPRA Schemen SHA Rand, SHA SHA 1 COMPARISON OF SHA Schemen SHA Rand, SHA SHA 1 COMPARISON Province Province STAC SHA TAPRA Schemen SHA Send SHA 1 Province STAC SHA TAPRA Schemen SHA Send SHA SHA 1 Province STAC SHA TAPRA Schemen SHA Send SHA SHA 1 Province STAC SHA TAPRA Schemen SHA Send SHA SHA 1 Province STAC SHA TAPRA Schemen SHA Send SHA SHA 1 Province STAC SHA TAPRA Schemen SHA Send SHA SHA 1 Province STAC SHA TAPRA Schemen SHA Send SHA SHA 1 Province STAC SHA TAPRA Schemen SHA Send SHA SHA 1 Province STAC SHA SCHEME SHA Send SHA SHA 1 Province STAC SHA SCHEME SHA SHA SHA SHA SHA 1 Province STAC SHA SCHEME SHA SHA SHA SHA SHA SHA 1 Province STAC SHA SCHEME SHA	Type 44C 955 800L quality.1 VALIDITY.7 800L 800L 800L 800L 805 805 955 955 955 955 955 955 955 9	Value FALSE good FALSE FALSE	Prepared value	Address	Commen
erWorld_RTA ker, Client - E ttings any Inputs uble Bit Input any Outputs alog Inputs alog Outputs rtasets IU Pin Settings storn Request ps ntroller	a Reamond RTLC SML TARRAS Sciences SML Reach, SML SML 1 Stream CDR Protocil Experime Provermidel, STAC, SML DARAS, Sciences, SML, Send, SML, SML 1 a Provermidel, STAC, SML DARAS, Sciences, SML, Send, SML, SML 1 a Provermidel, STAC, SML DARAS, Sciences, SML, Send, SML, SML 1 a Provermidel, STAC, SML DARAS, Sciences, SML, Send, SML, SML 1 a a a a b a b a b a c a a a b a b a c a c a c a c a c a c a c a d a d a d a d a d a d a d a d a	7996 7996 AFC 975 900L 0488/9.1 900L 900L 900L 900L 900L 900L 900L 905 995 995 995 995 995 995 995 995	Value FLSE process FLSE FLSE	Prepared value	Address	
etWorld_RTA err, Client - E ttings erry Inputs uble Bit Inputs alog Duputs alog Duputs alog Cuputs itasets XU Pin Settingi storn Request 35 mitroller	Compared ETAC SHIL SHARE Schemenes Mill Reach, SHIL SHIL 1 Compared ETAC SHIL SHARE Schemenes Mill Reach, SHIL SHIL 1 Experiment Free-Wind ETAC SHIL SHARE Schemenes SHIL Reach, SHIL SHIL 1 Foreither SHIL SHIL SHIL SHARE SCHEME SHIL Reach, SHIL SHIL SHIL SHIL SHIL SHIL SHIL SHIL	7904 7004 7004 905 9001 9001 9001 9001 9001 9001 9001 9001 905 905 905 905 905 905 905 905	Value FALSE pood process FALSE FALSE	Prepared value	Address	

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

Summary Connected Clients Valid Scans	1 0	Valid Commands Received 0 Simulation Events 2	✓ Close	
Input Contingency Acti	ions Simulation	Actions Simulation Events Server Log Connec	cted Clients DNP3 Log Options	
Time (Seconds)	Model Type	Object	Description	Level
1 1894.5000 A	AC Line I	MANSFIELD 0 TO GLEN ROSE 1 0 CKT 1	Open	Info
2 1929.8750 0	Sen (GLEN ROSE 1 2 #1	Generator MW value changed to 1000.000	Info

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 realtime 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

- 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. 20181231–170401, 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.