Real-Time Hardware-in-the-Loop Distributed Energy Resources System Testbed using IEEE 2030.5 Standard

Jinsan Kim[1], Kyuchan Park[1], Bohyun Ahn[2], Jinchun Choi[2], Youngtae Noh[1], Dongjun Won[1], and Taesic Kim[2*]
[1]Electrical and Computer Engineering, Inha University, Incheon, 22212 South Korea
[2]Electrical Engineering and Computer Science, Texas A&M University-Kingsville, Kingsville, TX, 78363 USA
jskim@nsl.inha.ac.kr, 22171363@inha.edu, bohyun.ahn@students.tamuk.edu, jinchun.choi@tamuk.edu, ytnoh@inha.ac.kr,
djwon@inha.ac.kr, taesic.kim@tamuk.edu

Abstract—**IEEE 2030.5 standard is drawing special attention among communication protocols for smart inverters and distributed energy resources (DER). Moreover, California Rule 21 mandates new DER must be ready to communicate to a host utility using the IEEE 2030.5 standard. Therefore, development of an effective real-time simulation method for managing DER using IEEE 2030.5 network is crucial. This paper presents a real-time hardware-in-the-loop (HIL) DER system testbed using the IEEE 2030.5 standard. The proposed real-time co-simulation testbed consists of a DER physical system simulation using OPAL-RT real-time simulator and a cyber system simulation including DER gateways and a DER management system (DERMS) cloud server. Custom-built client and server programs are developed to meet the compliant with IEEE 2030.5-2018 standard and implemented in the DER gateways and a DERMS server, respectively. The feasibility of the proposed testbed for DER systems is validated by experiments.**

Keywords—co-simulation, hardware-in-the-loop testbed, cybersecurity, distributed energy resources, distributed energy resources management system

I. INTRODUCTION

Penetrations of distributed energy resources (DER) such as renewable energy systems, energy storage systems, electric vehicles in electric power systems has been rapidly growing [1], [2]. Due to the ever-increasing number of DER, the current power grid is undergoing a transition. Geographically, broadly dispersed DER can make the electric power grid resilient with monitoring and control [3]-[7]. For example, a group of DER can act as a virtual power plant [5] providing grid services such as demand response [6] and mitigating renewable energy oversupplies [7]. However, standardizing communication protocols for interoperability between power system operators and DER equipment is crucial [8]).

In efforts of standardization, DER equipment requires to have either an IEEE 2030.5 (Smart Energy Profile 2.0 (SEP2), IEEE 1815 (DNP3), or SunSpec Modbus communication interface in a revision to the US interconnection and interoperability standard, IEEE Std. 1547 (i.e., IEEE 1547-2018 [8]). Moreover, the California Public Utility Commission (CPUC) Electric Rule 21 [10] defines IEEE 2030.5 as the default application network protocol for Investor Owned Utilities (IOU) communications to DER [11], effective in early 2019. It is anticipated that the adoption of IEEE 2030.5 for DER will soon be expanded to other states in U.S. and nations due to the advanced features such as internet protocol (IP)-based interoperability and security mechanism for securely exchanging application messages via internet among communication protocols.

With an awareness of special attention to IEEE 2030.5, a few researchers have recently adopted the protocol as a standard of smart grids. A network protocol compliant with IEEE 2030.5 standard is applied for private message exchange between a transactive agent and a home energy management system for transactive demand response for residential customers [12]. In [13], the authors proposed a two-way smart grid communication system compliant with IEEE 2030.5 standard between a transformer agent attached to a neighborhood's electric transformer and customer agents attached to each house. Sandia National lab assessed network-based defense techniques for DER in a virtualized co-simulation environment where SunSpec-compliant PV inverters are deployed as virtual machines and interconnected to simulated communication network equipment and a local DER management system (DERMS) monitors and controls the PV inverters [8]. However, the testbed does not fully investigate and implement IEEE 2030.5 standard for DER systems. Therefore, it is necessary to design a DER system testbed using a network protocol compliant with IEEE 2030.5 standard.

This paper proposes a real-time hardware-in-the-loop (HIL) DER system testbed using IEEE 2030.5 standard. The proposed real-time DER co-simulation testbed consists of a DER physical system simulation using a real-time simulator and a cyber system simulation including DER gateways and a DERMS cloud server. The proposed testbed provides a comprehensive real-time cyber system modeling and HIL capability that captures the cyber-physical impacts of the DER using the IEEE 2030.5 profile. As a result, researchers can analyze the complex interactions in a cyber-physical environment, which is required for studying on cyber-physical DER systems such as optimizing DERMS and defending cyber-attacks. Experimental studies are conducted to validate the feasibility of the proposed testbed for DER systems.

II. DER NETWORK USING IEEE 2030.5 STANDARD

IEEE 2030.5 standard defines an application protocol which provides an interface between the smart grid and users via internet and enables to manage the end user energy environment such as demand response, load control, price communication [14]. IEEE 2030.5 was previously named the SEP and based on Zigbee Alliance as a metering communication solution for building energy devices. In 2013, SEP2 was originally developed after adopted and ratified by IEEE (i.e., IEEE 2030.5-2013). In 2016, CPUC chose this

---

This research was supported by the Department of Energy (DOE) under award No. DE-EE0009026 and by Republic of Korea's MSIT (Ministry of Science ICT), under the High-Potential Individuals Global Training Program (Task No. 2020-0-01540), supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation).

2021 IEEE PES Innovative Smart Grid Technologies - Asia (ISGT Asia) | 978-1-6654-3339-6/21/$31.00 ©2021 IEEE | DOI: 10.1109/ISGTASIA49270.2021.9715595

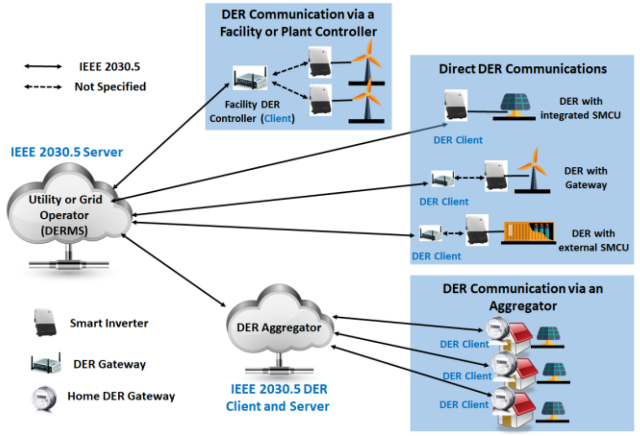


Fig. 1. Utility-to-DER communication architecture using IEEE 2030.5.

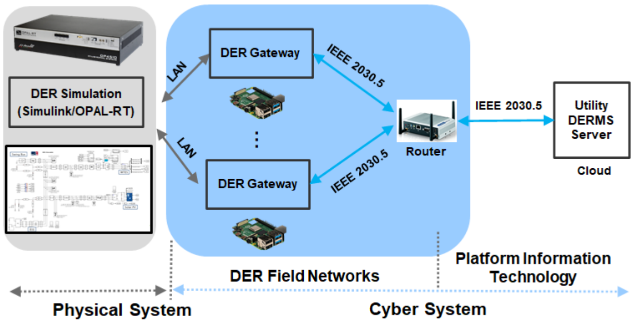


Fig. 2. A diagram of the proposed HIL DERMS testbed using IEEE 2030.5 standard.

protocol as the default protocol for Rule 21. The revision, IEEE 2030.5-2018, provides an expanded feature set that supports all controls in IEEE 1547-2018.

Fig. 1 shows examples of utility-to-DER communication architecture using IEEE 2030.5 where the DER is simply composed of a communication module and a smart inverter. IEEE 2030.5 applies to communications between the utility and DER systems through connections via DER facility controller, or an aggregator or direct connections [15]. In direct DER communications, either the smart inverter control unit (SMCU) or a separate gateway/control unit will be the IEEE 2030.5 client. The DER aggregator manages small DER as an IEEE 2030.5 server and communicates with DERMS as a client.

Technical components of IEEE 2030.5-2018 mapping to Open Systems Interconnection (OSI) layer include: 1) IP-based network mixing various link layer technologies (i.e., Wi-Fi, ZigBee) to promote interoperability; 2) transport layer security (TLS) v1.2 with a strong cipher suite (e.g., TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 unless otherwise indicated by utility interconnection obligations) for secure communication including the encryption, authentication, and key management; 3) representation state transfer (REST) HTTP architecture over TCP/IP for a client-server interaction; 4) extensible markup language (XML) schema to describe resources; 5) multicase DNS (mDNS) for host discovery on a local area network (LAN) and DNS-SD for resource discovery (standard DNS for host discovery is acceptable as well); and 6) providing application profile sources elements to direct support for DER controls defined in IEEE 1547-2018 (or other existing standards such as IEC 61968 and IEC 61850). Clients and servers perform mutual authentication using digital certificates (i.e., X.509 v3) during handshake through verification with the Root-CA. RESTful protocols allow HTTP actions. Common Smart Inverter Profile (CSIP) defines the operation of IEEE 2030.5 in the California Rule 21 use case. For example, POST (create) and DELETE (remove) can be used to create or remove DER end-devices or DER controllers.

III. PROPOSED REAL-TIME HIL DER TESTBED USING IEEE 2030.5-2018

Fig. 2 shows an overview of the real-time HIL DER testbed using IEEE 2030.5-2018 standard. This testbed including 1) a real-time DER physical system simulator using a grid simulator and 2) a real-time cyber system testbed consisting of DER gateways and a DERMS cloud server.

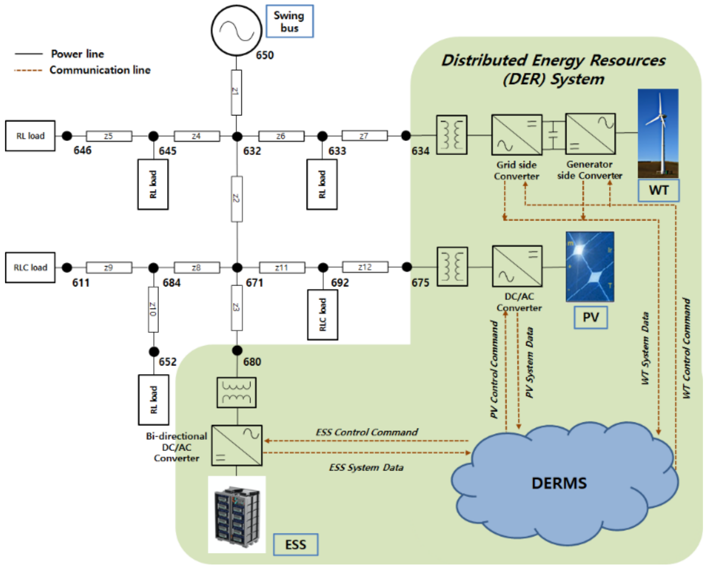


Fig. 3. A DER system in IEEE 13 node test feeder circuit, monitored and controlled by a DERMS.

A. DER System Modeling and Grid Simulation

Fig. 3 illustrates a DER system in IEEE 13 Node Test Feeder circuit where the DER system consists of multiple smart inverters, a swing bus, a wind turbine (WT), a Photovoltaic (PV), an energy storage system (ESS) and loads. The system bus frequency is 60Hz and the nominal voltage is 4.16kV. Smart inverters of WT and PV perform maximum power point tracking (MPPT) controls. The WT of the 634 bus is applied with the permanent magnet synchronous generator (PMSG) model and the rated power is 2.2 MVA. The PV is located on bus 675 and the rated output is 1MW. The ESS capacity of bus 680 is 1 MWh and a lithium-ion battery model is used. Except for the bus where the generators are connected, the resistive, inductive, and capacitive loads are evenly connected to the other buses, where the real power demand of the distribution system is 3.5 MW; the reactive power demand of inductive loads is 2.102 MVAR; and the reactive power demand of capacitive loads is 0.7 MVAR. The impedance values between the buses are chosen based on the IEEE 13 bus system. The DER system model is implemented in MATLAB/Simulink.

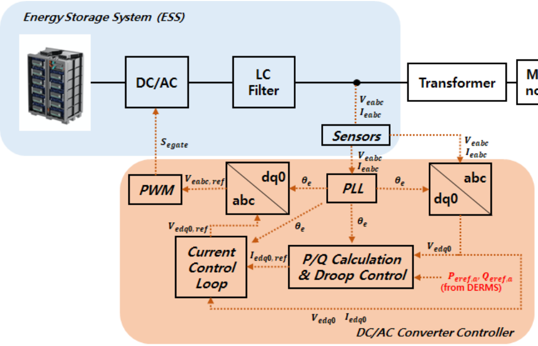


Fig. 4. ESS control model in IEEE 13 node test feeder circuit.

DERMS implemented in a cloud server monitors the DER system data and sends control commands to the DER devices as described in CSIP. A real-time power grid simulator (e.g., OPAL RT's OP4510) simulates the DER system modeled in MATLAB/Simulink.

Due to the page limit, this paper only provides the ESS converter control. Fig. 4 illustrates the ESS converter control model in IEEE 13 node test feeder circuit. The ESS converter controller receives the control commands such as active power reference ($P_{eref,a}$) and reactive power reference ($Q_{eref,a}$) from the DERMS. A droop control method is used for a primary control of the controller. Using combination of active/reactive (P/Q) calculation and the droop control, $I_{edq0,ref}$ (= $I_{ed,ref}$ and $I_{eq,ref}$) are determined, which is expressed as follows:

$$I_{ed,ref} = \frac{2}{3}\frac{P_{eref}}{V_{ed}} \tag{1}$$

$$I_{eq,ref} = -\frac{2}{3}\frac{Q_{eref}}{V_{ed}} \tag{2}$$

where P_{eref} and Q_{eref} are the active and reactive power references, respectively, and V_{ed} denotes the measured line voltage. Through the P/Q calculation and droop control, P_{eref} and Q_{eref} are computed as follows:

$$P_{eref} = P_{eref,a} + \Delta P_{edroop} \tag{3}$$

$$Q_{eref} = Q_{eref,a} + \Delta Q_{edroop} \tag{4}$$

$$\Delta P_{edroop} = -\frac{f - f_0}{K_{eP}} \tag{5}$$

$$\Delta Q_{edroop} = -\frac{V - V_0}{K_{eQ}} \tag{6}$$

where ΔP_{edroop} and ΔQ_{edroop} are variations of P and Q, respectively; f_0 and V_0 are nominal frequency and voltage of the DER system; f and V are measured frequency and voltage, respectively; and K_{eP} and K_{eQ} are droop coefficients. The output of the inner current control loop is calculated as:

$$V_{ed,ref} = V_{ed} + k_{pi}(I_{ed,ref} - I_{ed}) + \frac{k_{ii}(I_{ed,ref} - I_{ed})}{s} - \omega L_f I_{eq} \tag{7}$$

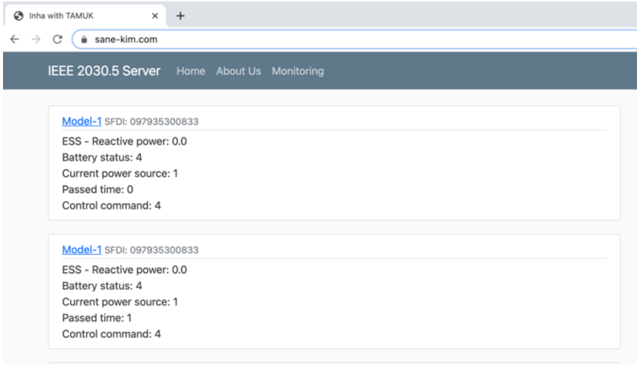
$$V_{eq,ref} = V_{eq} + k_{pi}(I_{eq,ref} - I_{eq}) + \frac{k_{ii}(I_{eq,ref} - I_{eq})}{s} + \omega L_f I_{ed} \tag{8}$$

where k_{pi} and k_{ii} are parameters of the proportional integral (PI) of the inner current loop; ω is an angular frequency (= $2\pi f$); and L_f is the inductance value of the LC filter.

B. Cyber System Simulation using IEEE 2030.5-2018

A cyber system testbed using IEEE 2030.5-2018 standard consists of DER Gateways (i.e., IEEE 2030.5 client), a router, and a DERMS cloud server (i.e., IEEE 2030.5 server). DER gateways in network layers are implemented by using internet of things (IoT) devices. Each gateway is connected to each component (i.e., WT, PV, ESS) of DER devices simulated by the real-time simulator. The DER client in the DER Gateway receives the DER system data and sends them to the cloud server. Although IEEE 2030.5-2018 standard recommends TLS v1.2 for secure communication. Latest TLS v1.3 also can be used once the cipher suite of TLS v1.3 meets all of the security features of IEEE 2030.5-2018. These cryptographic protocols are designed and implemented using OpenSSL. The Root-CA public key can be provided from third-party CA. It used to validate the certificate chains of communicating devices as part of the TLS handshake process.

Fig. 5. Shows the custom-built DERMS cloud server web page. DERMS server is implemented on a virtual private server. The server runs on Ubuntu 18.04 and uses Apache2 HTTP server project to host the server. Python 3.6.9 and



Model-1 SFDI: 097935300833
ESS - Reactive power: 0.0
Battery status: 4
Current power source: 1
Passed time: 0
Control command: 4

Model-1 SFDI: 097935300833
ESS - Reactive power: 0.0
Battery status: 4
Current power source: 1
Passed time: 1
Control command: 4

Fig. 5. DERMS cloud server web page.

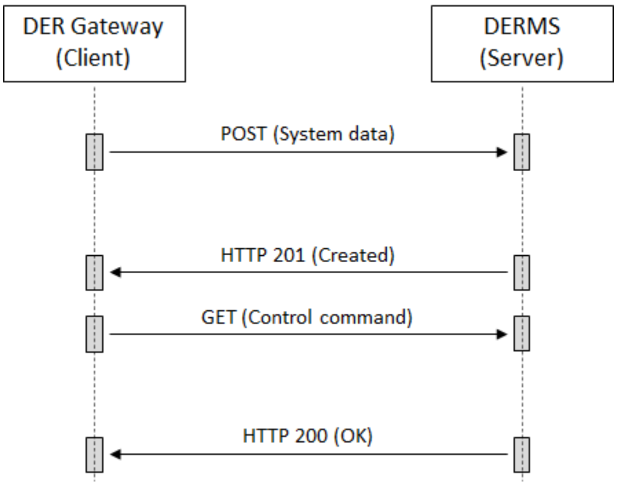


Fig. 6. An example of communication hierarchy using IEEE 2030.5 between DER Gateway and DERMS.

Django REST Framework are used to meet the technical components of IEEE 2030.5-2018 standard as mentioned in section II. In server, real-time DER system data such as reactive power and power factor are stored in local SQLite3 database. Such data are linked with identification using Short-Form Device Identifier (SFDI). These data are visualized in server as a graph in real time using Python library named pyplot from matplotlib.

C. DER Operation

The IEEE 2030.5 DER clients and the DERMS server perform CSIP operations once the TLS network is established. Server sends control commands to the DER clients such as autonomous function (e.g., vol-var, volt-watt, and freq-watt), immediate control (e.g., active power curtailment, fixed reactive power, and fixed power factor), and protection setting (e.g., high/low voltage ride-through and high/low frequency ride-through). DER clients send system information to the DERMS server such as DER nameplate ratings and settings, DER alarms and status, and DER measurements (e.g., active power, reactive power, voltage, current, power factor, and frequency). Fig. 6 describes an example of IEEE 2030.5 messaging sequence via RESTful commands for XML files when DER Gateway sends DER system data to the DERMS and receives control commands from the DERMS.

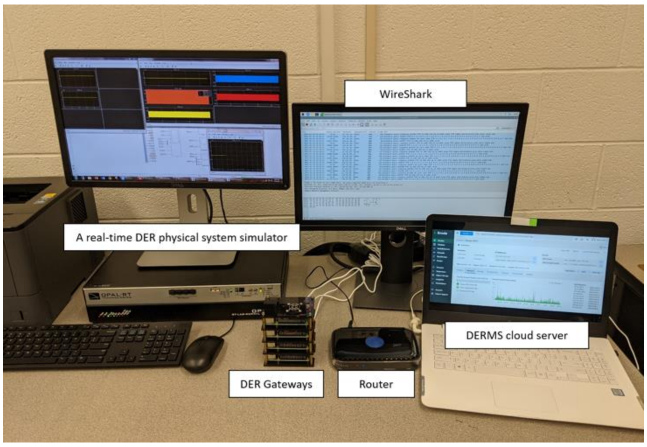
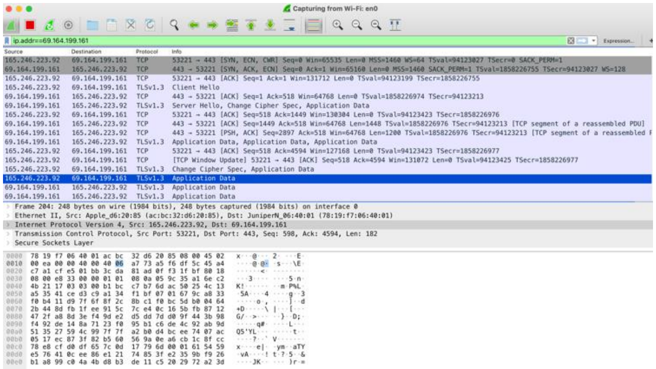


Fig. 7. Experimental setup



```
ip.addr==69.164.199.161
Source          Destination     Protocol Info
165.246.223.92  69.164.199.161  TCP      53221 → 443 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=94123027 TSecr=0 SACK_PERM=1
69.164.199.161  165.246.223.92  TCP      443 → 53221 [SYN, ACK, ECN] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=1858226755 TSecr=94123027 WS=128
165.246.223.92  69.164.199.161  TCP      53221 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=94123199 TSecr=1858226755
165.246.223.92  69.164.199.161  TLSv1.3  Client Hello
69.164.199.161  165.246.223.92  TCP      443 → 53221 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=1858226974 TSecr=94123213
69.164.199.161  165.246.223.92  TLSv1.3  Server Hello, Change Cipher Spec, Application Data
165.246.223.92  69.164.199.161  TCP      53221 → 443 [ACK] Seq=518 Ack=1449 Win=130304 Len=0 TSval=94123423 TSecr=1858226976
69.164.199.161  165.246.223.92  TCP      443 → 53221 [ACK] Seq=1449 Ack=518 Win=64768 Len=1448 TSval=1858226976 TSecr=94123213 [TCP segment of a reassembled PDU]
69.164.199.161  165.246.223.92  TCP      443 → 53221 [PSH, ACK] Seq=2897 Ack=518 Win=64768 Len=1200 TSval=1858226976 TSecr=94123213 [TCP segment of a reassembled P
69.164.199.161  165.246.223.92  TLSv1.3  Application Data, Application Data, Application Data
165.246.223.92  69.164.199.161  TCP      53221 → 443 [ACK] Seq=518 Ack=4594 Win=127168 Len=0 TSval=94123423 TSecr=1858226977
165.246.223.92  69.164.199.161  TCP      [TCP Window Update] 53221 → 443 [ACK] Seq=518 Ack=4594 Win=131072 Len=0 TSval=94123425 TSecr=1858226977
165.246.223.92  69.164.199.161  TLSv1.3  Change Cipher Spec, Application Data
165.246.223.92  69.164.199.161  TLSv1.3  Application Data
69.164.199.161  165.246.223.92  TLSv1.3  Application Data
69.164.199.161  165.246.223.92  TLSv1.3  Application Data
> Frame 204: 248 bytes on wire (1984 bits), 248 bytes captured (1984 bits) on interface 0
> Ethernet II, Src: Apple_d6:20:85 (ac:bc:32:d6:20:85), Dst: JuniperN_06:40:01 (78:19:f7:06:40:01)
> Internet Protocol Version 4, Src: 165.246.223.92, Dst: 69.164.199.161
> Transmission Control Protocol, Src Port: 53221, Dst Port: 443, Seq: 598, Ack: 4594, Len: 182
> Secure Sockets Layer
0000  78 19 f7 06 40 01 ac bc  32 d6 20 85 08 00 45 02   x···@···2· ···E·
0010  00 ea 00 00 40 00 40 06  a7 73 a5 f6 df 5c 45 a4   ····@·@··s···\E·
0020  c7 a1 cf e5 01 bb 3c da  81 ad 0f f3 1f bf 80 18   ······<·········
0030  08 00 e8 33 00 00 01 01  08 0a 05 9c 35 a1 6e c2   ···3········5·n·
0040  4b 21 17 03 03 00 b1 bc  c7 b7 6d ac 50 25 4c 13   K!········m·P%L·
0050  a5 35 41 ce d3 c9 a1 34  f1 bf 07 01 67 9c a8 33   ·5A····4····g··3
0060  f0 b4 11 d9 7f 6f 8f 2c  8b c1 f0 bc 5d b0 04 64   ·····o·,····]··d
0070  2b 44 8d fb 1f ee 91 5c  7c e4 0c 16 5b fb 87 12   +D·····\|···[···
0080  47 2f a8 8d 3e f4 9d e2  d5 dd 7d d0 9f 44 3b 98   G/··>·····}··D;·
0090  f4 92 de 14 8a 71 23 f0  95 b1 c6 de 4c 92 ab 9d   ·····q#·····L···
00a0  51 35 27 59 4c 99 7f 7f  a2 b0 d4 bc ee 74 07 ac   Q5'YL········t··
00b0  05 17 ec 87 3f 82 b5 60  56 9a 0e a6 cb 1c 8f cc   ····?··`V·······
00c0  78 e8 cf d0 df 65 7c 0d  17 79 6d 00 01 61 54 59   x····e|··ym··aTY
00d0  e5 76 41 0c ee 86 e1 21  74 85 3f e2 35 9b f9 26   ·vA····!t·?·5··&
00e0  b1 a8 99 c0 4a 4b d8 b3  de 11 c5 20 29 72 a2 3d   ····JK····· )r·=
```

Fig. 8. Encrypted traffic with TLS v.13 captured by WireShark.

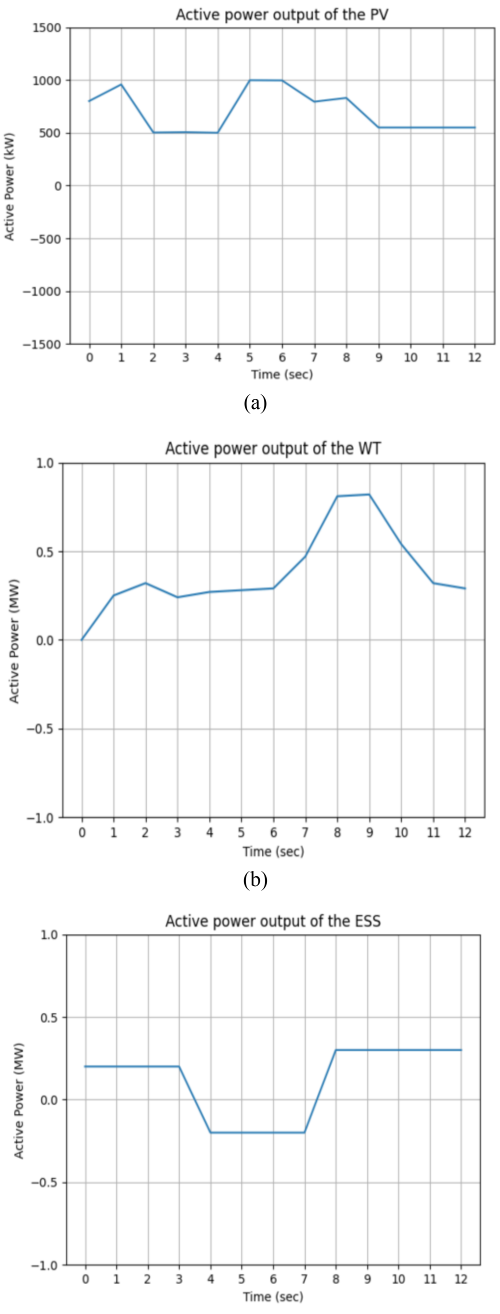
IV. VALIDATION

Fig. 7 shows the experimental setup to perform experiments to validate the proposed testbed which is described in Section III. To build a real-time DER physical system simulator and gateway OPAL-RT's OP4510 and Raspberry pi 4B are used. A DERMS cloud server is built in cloud provided by Linode [16]. The Root-CA public key is provided by Let's Encrypt [17]. Three test cases are performed: 1) TLS encryption and its performance using Wireshark to monitor in-transit DER network data; 2) real-time DER system data monitoring by DERMS server; 3) and impact of control command provided by DERMS.

Fig. 8 shows that the screenshot of the encrypted exchanging data between them by TLS 1.3 in WireShark. We can see all the communication data are encrypted and just shown as Application Data. Also, it is expected that TLS v1.3 provides fast processing time than TLS v1.2 since the number of round trips has been reduced in TLS v1.3. Fig. 9 shows real-time active power data from PV, WT, ESS with one second sampling rate via DER gateways. It is observed that the DERMS server can monitor the real-time DER system data using secured TLS networks. Fig. 10(a) illustrates reactive power change in ESS shown in the real-time simulator due to a received control command provided by DERMS and Fig. 10(b) shows the reactive power data monitored in DERMS. The control command changing reactive power of ESS from 0 VAR to 0.5 MVAR is received at 5 second, and then the controller of ESS changed the reactive power. The ESS operation change is available in the next sampling period (i.e., one second) in DERMS. Therefore, the proposed testbed can simulate both cyber events and impact of dynamics of DER system using the realistic IEEE 2030.5 standard.

V. CONCLUSION

This paper proposes a real-time HIL DER system testbed using IEEE 2030.5 standard. The proposed testbed provides a co-simulation of DER cyber system and physical system using DER system simulator, gateways and a DERMS cloud server. The proposed testbed will be used to analyze the complex interactions in a cyber-physical environment with IEEE 2030.5 for studying on cyber-physical DER systems such as optimizing DERMS and defending cyber cyber-attacks. Future works include detailed network performance analysis, adding more optimal control and security functions in DERMS.



(a)

(b)

(c)

Fig. 9. Real-time active power data monitoring in DERMS cloud: (a) PV, (b) WT, and (c) ESS.

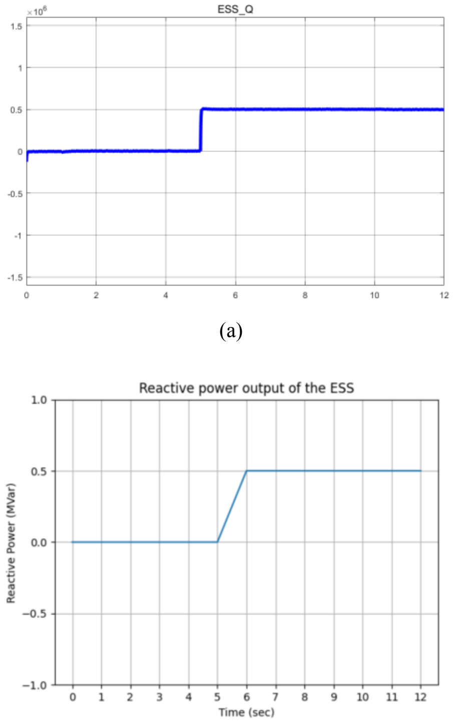
REFERENCES

[1] Solar Energy Industries Association and GTM Research, "U.S. solar market insight Q3 2018," Technical Report, Sept. 12, 2018.

[2] U.S. Energy Information Administration, "U.S. battery storage market trends," May 2018.

[3] [Online]. Available: https://www/energy.gov/eere/solar/solar-integration-and-grid-services-basics

[4] B. Kroposki, et. al, "Achieving a 100% renewable grid: Operating electric power energy systems with extremely high levels of variable renewable," *IEEE Power and Energy Magazine*, vol. 15, no. 2, pp. 61–73.



(a)

(b)

Fig. 10. ESS Reactive power change command sent by DERMS: (a) reactive power change in OPAL-RT and (b) monitoring data in DERMS.

[5] K. O. Adu-Kankam and L. M. Camarinha-Matos, "Toward collaborative virtual power plants: Trends and convergence," *Sustainable Energy, Grids and Networks*, vol. 16, pp. 217-230, Dec. 2018.

[6] Expanding PV Value: lessons learned from utility-led distributed energy resource aggregation in the united states, Technical Report, NREL, Nov. 2018.

[7] [Online]. Available: https://www.sce.com/business/demand-response

[8] J. Johnson, I. Onunkwo, P. Cordeiro, B. J. Wright, N. Jacobs, C. Lai, "Assessing DER network cybersecurity defences in a power-communication co-simulation environment, *IET Cyber Physical System*, Mar. 2020.

[9] IEEE Std. 1547-2018: 'IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces', (Institute of Electrical and Electronics Engineers, Inc.), New York, NY, 15 Feb 2018.

[10] [Online]. Avaliable: https://www.cpuc.ca.gov/Rule21/

[11] SunSpec Alliance, Common Smart Inverter Profile: IEEE 2030.5 'Implementation Guide for Smart Inverters, Version 2', Mar. 2018.

[12] J. Fattahi, M. Samadi, M. Erol-Kantarci, and H. Schriemer, "Transactive demand response operation at the grid edge using the IEEE 2030.5 standard," Engineering, vol. 6, pp. 801-811, June 2020.

[13] M. Ghalib, A. Ahmed, I. Al-Shiab, Z. Bouida, M. Ibnkahla, "Implementation of a smart grid communication system compliant with IEEE 2030.5," in *Proc. 2018 IEEE Int. Conf. Comm. Workshops*, Kansas City, MO, USA, May 20-24, 2018, pp.1-6.

[14] "IEEE Standard for Smart Energy Profile Application Protocol," in *IEEE Std 2030.5-2018 (Revision of IEEE Std 2030.5-2013)*, pp.1-361, 21 Dec. 2018.

[15] J. Obert, P. Cordeiro, J. Johnson, G. Lum, T. Tansy, M. Pala, and R. Ih, "Recommendations for trust and encryption in DER interoperability standard," Sandia Report SAND2019-1490, Feb. 2019.

[16] [Online]. Available: https://www.linode.com

[17] [Online]. Available: https://letsencrypt.org/