Demo Abstract: A HIL Emulator-Based Cyber Security Testbed for DC Microgrids

Mengxiang Liu, Zexuan Jin, Jinhui Xia, Mingyang Sun, Ruilong Deng, and Peng Cheng

***Abstract*—In DC microgrids (DCmGs), distributed control is becoming a promising framework due to prominent scalability and efficiency. To transmit essential data and information for system control, various communication network topologies and protocols have been employed in modern DCmGs. However, such communication also exposes the DCmG to unexpected cyber attacks. In this demo, a scalable cyber security testbed is established for conducting hardware-in-the-loop (HIL) experiments and comprehensively investigating the security impact on DCmGs. Specifically, the testbed employs a Typhoon HIL 602+ emulator, which is professional in power electronics system emulation, to demonstrate four (12 at most) distributed energy resources (DERs). The communication network is implemented through the self-loop RS-232 interface. Based on the testbed, we systematically investigate the impact of two kinds of typical cyber attacks (i.e., false data injection and replay attacks). Experimental results show that both attacks will deteriorate the point-of-common coupling (PCC) voltages of the DERs and jeopardize the stability of the whole DCmG.**

I. Introduction

In recent decades, DC microgrids (DCmGs) have obtained widespread attentions for the advantages in accommodating distributed energy resources (DERs) through converters. To improve the scalability and efficiency of DCmG control, the distributed control framework has become an attractive alternative of the conventional centralized control. However, the integrated information and communications technology (ICT) utilized among the DERs in distributed control may introduce cyber security threats to the DCmG.

False data injection (FDI) and replay attacks are two typical cyber security issues that may threaten the DERs in DCmGs. The FDI attack injects well-designed malicious values into communication links, and the replay attack replaces the transmitted data with the previously recorded data. Numerous research has been conducted to address the cyber security issue of DCmGs, and below we review two representative literatures in this aspect. Sahoo *et al.* [1] proposed a cooperative vulnerability factor framework for each DER to identify the malicious DER that injects balanced false data into communication links. Gallo *et al.* [2] designed a distributed watermarking scheme for each DER to perceive the existence of replay attacks. However, existing literatures investigate the security impact on DCmGs through either impractical simulation studies or unscalable testbeds. There still lacks a scalable and practical cyber security testbed to conduct experimental experiments and comprehensively investigate the security impact on DCmGs. Towards this end, based on the Typhoon hardware-in-the-loop (HIL) 602+ emulator, which is specialized in the ultra-low-latency, ultra-high-fidelity, real-time emulation of power electronics enabled microgrids [3], we establish the DCmG testbed consisted of four (12 at most) DERs for the demonstration of the security impact of unexpected cyber attacks.

This work was supported in part by the National Key Research and Development Program of China 2020YFB1708700; in part by the National Natural Science Foundation of China under Grants 62073285, 61833015, and 61903328; and in part by the Fundamental Research Funds for the Central Universities (Zhejiang University NGICS Platform). The authors are with the State Key Laboratory of Industrial Control Technology and the College of Control Science and Engineering, Zhejiang University, Hangzhou 310027, China. (E-mail: lmx329@zju.edu.cn)

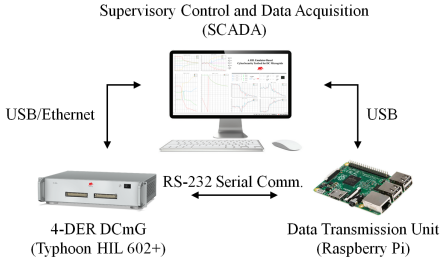

Fig. 1. Implementation overview of the DCmG testbed.

II. Testbed Implementation

The implementation overview and system diagram of the DCmG testbed is shown in Figs. 1 and 2.

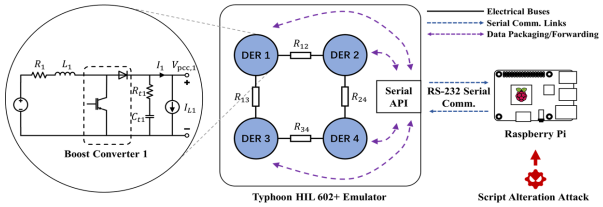

Fig. 2. System diagram of the DCmG testbed.

A. DCmG Implementation

As observed in Fig. 2, each DER adopts a boost converter for DC/DC power transmission in DCmG. Therein, the DC voltage source represents the generic renewable energy resources. Through providing appropriate switching signals for the IGBT, the point-of-common (PCC) voltage of the converter could be tuned to follow the reference voltage. The HIL emulator is equipped with a Xilinx Virtex-6 FPGA processor, wherein up to 12 converters could be discretized and emulated. Such emulation outputs are measurable analog signals that have been scaled down by the SCADA. Since the Typhoon emulator only provides one communication interface for the DCmG testbed, we utilize the self-loop RS-232 serial communication to implement the communication network in the DCmG.

B. Cyber Attacks Implementation

We implement two typical cyber attacks, i.e., FDI and replay attacks, by altering the data transmission script on the Raspberry Pi.

1) FDI Attacks: The FDI attack injects malicious values designed by the attacker into communication links. For the communication link $1 \rightarrow 2$ under FDI attacks, the output current of DER 1 received by DER 2 can be expressed as $I_{2,1}^{\text{fdi}}(t) = I_1(t) + \phi_{2,1}(t)$ with $\phi_{2,1}(t)$ being the injected value.

2) Replay Attacks: The replay attack replaces the original data with the previously recorded data transmitted in the communication link. For the communication link $1 \rightarrow 2$ under replay attacks, the output current of DER 1 received by DER 2 can be expressed as $I_{2,1}^{\text{rep}}(t) = I_1(t-\tau), \forall t \in (t_s^{\text{rec}}+\tau, t_e^{\text{rec}}+\tau)$, where $(t_s^{\text{rec}}, t_e^{\text{rec}})$ denotes the duration of the recorded data.

III. Experimental Results

In this section, the impact of FDI and replay attacks on the DCmG will be evaluated using the HIL-based experiments. Therein, the load currents of the DERs are set to 1.3A, 1.1A, 0.9A, and 0.7A, respectively, and the corresponding reference PCC voltages of the DERs are all 48V. During normal operations of the DERs, output currents and the average of PCC voltages will finally reach 1A and 48V, respectively.

A. FDI Attacks

Two kinds of FDI attacks (i.e., single and coordinated FDI attacks) that inject malicious values into the communication links of the DCmG have been considered in this demo.

1) Single FDI Attack: In the single FDI attack, we inject a constant value $\phi_{1,2} = 0.5$A into the communication link $2 \rightarrow 1$ at $t = 20$s. According to Fig. 3, under the single FDI attack, all output currents of DERs deviate from their sharing values (1A), and the average of PCC voltages increases monotonically.

2) Coordinated FDI Attack: In the coordinated FDI attack, we inject $\phi_{1,2}(t) = 0.25(t-20), t \in (20\text{s}, 24\text{s})$; $\phi_{1,2}(t) = 1\text{A}, t \geq 24\text{s}$ and $\phi_{3,2}(t) = -t+20, t \in (20\text{s}, 21\text{s})$; $\phi_{3,2}(t) = -1\text{A}, t \geq 21\text{s}$ into communication links $2 \rightarrow 1$ and $2 \rightarrow 3$ at $t = 20$s, respectively. As observed in Fig. 4, under the coordinated FDI attack, all output currents deviate from the sharing values, and the PCC voltages will re-converge towards new values. Compared with the single FDI attack, the coordinated FDI attack has the capability of causing specific and directional PCC voltage deviations ($\pm$1V).

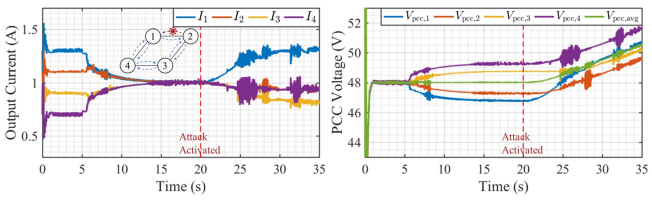

Fig. 3. Security impact of the single FDI attack.

B. Replay Attacks

Similarly, two kinds of replay attacks (i.e., single and multiple replay attacks) have been launched in the experiments.

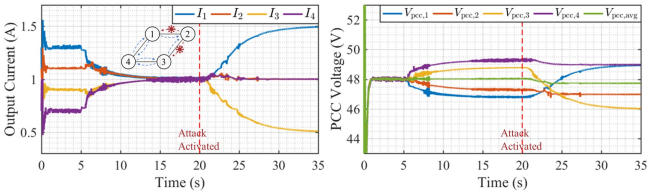

Fig. 4. Security impact of the coordinated FDI attack.

1) Single Replay Attack: In the single replay attack, for $t \in (20\text{s}, 26\text{s})$, we replace the data transmitted in the communication link $2 \rightarrow 1$ with the data recorded during $t \in (1\text{s}, 2\text{s})$. As shown in Fig. 5, the output currents deviate from their original values when the attack is enabled, and recover after the attack is stopped. The average PCC voltage slightly deviates from the desired value after the attack is activated. Since replay attacks simply replace the data with previously recorded data, the security deterioration of such attacks is not as severe as the FDI attack.

2) Multiple Replay Attack: In the multiple replay attack, for $t \in (20\text{s}, 26\text{s})$, we replace the data transmitted in communication links $2 \rightarrow 1$ and $2 \rightarrow 4$ with the data recorded during $t \in (1\text{s}, 2\text{s})$. According to Fig. 6, the security impact caused by the multiple replay attack can be considered as the sum of each single replay attack.

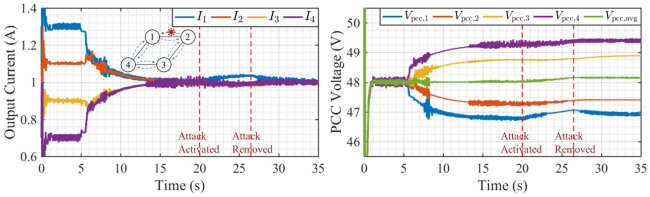

Fig. 5. Security impact of the single replay attack.

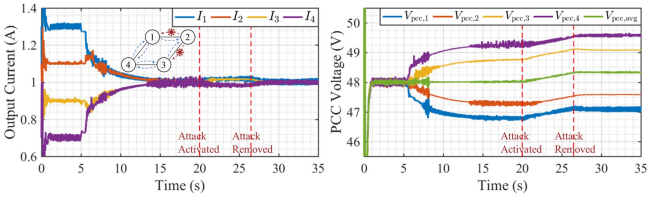

Fig. 6. Security impact of the multiple replay attack.

IV. Conclusion and Future Work

In this demo abstract, we have illustrated the implementation of a HIL emulator-based cyber security testbed for DCmGs. It can be concluded from the experimental results that attackers could easily construct the coordinated FDI attack such that the PCC voltages and the output currents of DERs will deviate significantly from their desired values. The multiple replay attack can also cause non-trivial PCC voltage deviations, which are comparable to those induced by the coordinated FDI attack.

References

[1] S. Sahoo, S. Mishra, J. C. H. Peng, and T. Dragičević, "A stealth cyber-attack detection strategy for dc microgrids," *IEEE Transactions on Power Electronics*, vol. 34, no. 8, pp. 8162–8174, 2018.

[2] A. J. Gallo, M. S. Turan, F. Boem, G. Ferrari-Trecate, and T. Parisini, "Distributed watermarking for secure control of microgrids under replay attacks," *IFAC-PapersOnLine*, vol. 51, no. 23, pp. 182–187, 2018.

[3] P. Maloney, "Building a better microgrid with hardware in the loop," Microgrid Knowledge White Paper Library, Tech. Rep., 2019.