Towards Automated Generation of Smart Grid Cyber Range for Cybersecurity Experiments and Training

Daisuke Mashima, Muhammad M. Roomi,
Bennet Ng, Zbigniew Kalbarczyk
Illinois at Singapore Pte Ltd
{daisuke.m,roomi.s,bennet.ng,kalbarcz}@adsc-create.edu.sg

S.M. Suhail Hussain, Ee-chien Chang
National Cybersecurity R&D Lab
National University of Singapore
suhail@ieee.org, changec@comp.nus.edu.sg

***Abstract*—Assurance of cybersecurity is crucial to ensure dependability and resilience of smart power grid systems. In order to evaluate the impact of potential cyber attacks, to assess deployability and effectiveness of cybersecurity measures, and to enable hands-on exercise and training of personals, an interactive, virtual environment that emulates the behaviour of a smart grid system, namely smart grid cyber range, has been demanded by industry players as well as academia. A smart grid cyber range is typically implemented as a combination of cyber system emulation, which allows interactivity, and physical system (i.e., power grid) simulation that are tightly coupled for consistent cyber and physical behaviours. However, its design and implementation require intensive expertise and efforts in cyber and physical aspects of smart power systems as well as software/system engineering. While many industry players, including power grid operators, device vendors, research and education sectors are interested, availability of the smart grid cyber range is limited to a small number of research labs. To address this challenge, we have developed a framework for modelling a smart grid cyber range using an XML-based language, called SG-ML, and for "compiling" the model into an operational cyber range with minimal engineering efforts. The modelling language includes standardized schema from IEC 61850 and IEC 61131, which allows industry players to utilize their existing configurations. The SG-ML framework aims at making a smart grid cyber range available to broader user bases to facilitate cybersecurity R&D and hands-on exercises.**

***Index Terms*—Smart grid, cyber range, testbed, IEC 61850, cybersecurity**

I. Introduction

Emerging cyber threats against smart grid systems is one of the biggest concerns for ensuring dependable and trustworthy operation of our nations' critical infrastructure. In the last decades, we have witnessed a number of real-world incidents, such as Stuxnet attack in 2010 [1], Ukraine power plant attacks in 2015 and 2016 [2], hacking against the US utility's control room in 2018, Venezuela blackout caused by cyber attacks in 2019 [3], ransomware attack against K-Electric in Pakistan [4]. In order to counter and respond to such incidents, it is imperative to intensively evaluate the impact of various attack vectors, robustness of the system against these vectors, and to design response and recovery procedures.

While it would be ideal to conduct such exercises and evaluations in the real system environment, it is impossible to avoid any potential impact on the availability and stability of the power grid operation. An alternate solution is to develop an isolated testbed using the same hardware as the real system, e.g., Electric Power and Intelligent Control (EPIC) testbed [5]. However, such a hardware-based approach has inherent limitation in initial and operational cost, reconfigurability, scalability, and accessibility. Setting up and maintaining such a testbed is rather costly and hence may not be feasible for most organizations. Moreover, the system configuration and topology are fixed and difficult to modify or extend. In addition to these challenges, even in such an isolated testbed, experiments with high risk are often not permitted. For example, it would never be allowed to do the experiments similar to Aurora generator test done by Idaho National Lab researchers to demonstrate that cyber-originated attacks could physically destroy generators [6].

Due to these reasons, high-fidelity, virtual environment for conducting interactive cybersecurity experiments and exercises, often called cyber range, has attracted interest from both industry and academia. Smart grid cyber range is a virtual system that emulates cyber and physical systems of a smart grid, and can interact with human users in a real-time manner for conducting various experiments. Numerous efforts have been made to develop cyber range for smart grid systems in the recent years. Numerous efforts have been made to develop a cyber range for smart grid systems in recent years. Some of the efforts, such as [7], have limitations in terms of fidelity while others are designed to emulate one specific system or designed in one-off, in-house manner [8]–[15], resulting in very limited accessibility.

To address these challenges and facilitate industry players and academic researchers to have their own cyber range on premise, we have developed a framework for automated smart grid cyber range generation, called *SG-ML* (Smart Grid Modelling Language) [16]. SG-ML defines XML-based modelling language for defining configurations of smart grid cyber range and provides the toolchain, *SG-ML Processor*, for parsing the models and, like a compiler, instantiating a cyber

range according to the configuration. This paper focuses on the description of the SG-ML Processor toolchain. SG-ML is defined by using standardized models, such as IEC 61850 SCL (System Configuration description Language) [17], [18] that power grid operators already have. Thus users in the power grid industry can utilize their existing assets to generate a digital replica of their smart grid, which can be, for instance, utilized for a red-team exercise to identify vulnerabilities without affecting the production system. Moreover, the XML-based model can be shared and customized in the open-source community. As a result, even users in other sectors can develop their own cyber range or reproduce it with minimal power grid expertise and engineering efforts. [1]

Different types of smart grid security testbeds (physical, hybrid and virtual) are developed over the years for research, training and experiment applications [7], [15], [19]–[23]. Although these testbeds have different advantages and are utilized for different applications, limitations are found in one or multiple of deployability, configurability, scalability, and reproducibility. In particular, none of the existing efforts considers automated generation of smart grid cyber range to minimize user's burden on designing and implementing the system. To our knowledge, the SG-ML framework we have developed is the first to largely automate the generation of smart grid cyber range based on user-defined models.

Automated generation of cyber range from user-defined, standard-based models benefit industry players and practitioners in multiple ways. First, by generating a replica of the smart grid infrastructure, it can be utilized to assess potential vulnerabilities through extensive red-team testing without affecting the real system. Besides cybersecurity, such a cyber range can be utilized to evaluate compatibility and correctness of the power grid configuration (e.g., consistency among IED's (intelligent electronic devices) protection functions and PLC (programmable logic controllers) logics). Cyber range can also be used to conduct hardware-in-the-loop testing of PLCs and IEDs before deployment. Last but not the least, cyber range can be valuable resource for the cybersecurity hands-on training and education for technicians.

II. Smart Grid Cyber Range Architecture

We first summarize the components that are involved in a typical smart grid cyber range found in the literature, which is to be modelled and generated by the SG-ML framework. The high-level architecture is shown in Figure 1.

Typically, cyber range for cyber-physical systems is implemented as a combination of cyber system emulation and a physical plant simulation. In a smart grid cyber range for a flexible and interactive cyber attack experiments, the cyber side of the system should be implemented with a virtual network running a number of (virtual) smart grid devices, namely SCADA HMI (supervisory control and data acquisition human-machine interface), PLCs , and IEDs . SCADA HMI is a user interface for human operators to see the status of the power grid system and, when necessary, sends control commands to the plant. IEDs work as sensors and actuators to collect power grid measurements (e.g., power, voltage, frequency, etc.) and operate on the physical devices, such as circuit breakers (CBs) and transformers. IEDs also implement protection function (e.g., over current / voltage protection) to protect the physical equipment from damage. IEDs communicate with other IEDs, PLCs, and/or SCADA HMI, using standard communication protocols, such as IEC 61850 [17]. PLCs are often utilized in smart grid system to implement automated control. PLCs collect measurements from one or multiple IEDs and then execute pre-configured control logic based on those inputs and sends control commands to IEDs. Control logic for the PLC is often programmed according to IEC 61131 standard [24].

The aforementioned cyber-side components interact with the power system simulator in real-time. For instance, when a virtual IED receives a control command to open a circuit breaker, it should take effect on the power flow status shortly after the receipt. The near-realtime interface between the cyber side and physical side can be implemented in multiple ways. Some commercial power system simulators have interactive API, and thus it can be utilized when the emulated virtual IEDs receives control commands. Alternatively, database or networking can be utilized. A cyber range discussed in [14] utilizes database as the bi-directional (read/write) interface, and [15] utilizes publisher-subscriber communication to interact with the power system simulator. As the cyber range is mainly intended for interactive cyber attack exercise and experiments, all of these options are regarded sufficient in practice. Besides, power system simulation models can be configured according to some scenarios, such as contingency, disruptions, as well as abnormal load profiles.

III. Automated Smart Grid Cyber Range Generation Framework

The automated smart grid cyber range generation framework utilizes the XML-based modelling schema proposed by us, called SG-ML [16]. SG-ML is used to define cyber and physical configuration of smart grid cyber range, and the set of XML files are used as the input for the SG-ML Processor. SG-ML Processor processes the model files and generate an operational cyber range (Figure 2).

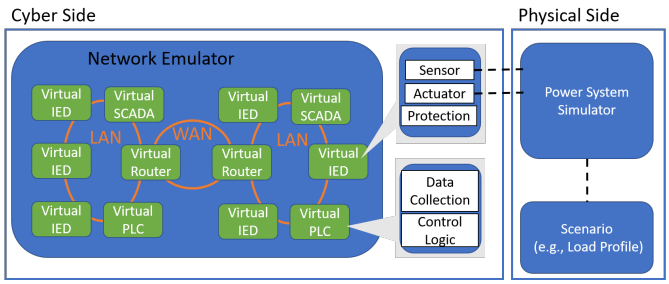


Fig. 1. Typical Architecture of Smart Grid Cyber Range

[1] SG-ML framework is open-sourced, along with the specification document and demo videos, at https://github.com/smartgridadsc/CyberRange

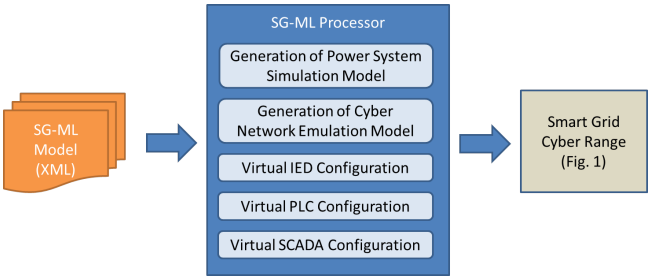


Fig. 2. Overview of SG-ML Framework

TABLE I
TYPES OF IEC 61850 SCL (SYSTEM CONFIGURATION DESCRIPTION LANGUAGE) FILES AND DESCRIPTION

Type of SCL File	Description
SSD (System Specification Description)	Contains the overview of the substation structure as a single line diagram, voltage levels, bay levels, and functions of the substation.
SCD (System Configuration Description)	Contains complete description of the process including configuration for all IEDs present in a substation, structure or layout of the substation and a communication configuration section.
ICD (IED Capability Description)	Contains an overview of functionalities and engineering capabilities of an IED. It also contains the logical nodes (LNs) and the corresponding data types associated with the IED capability.
SED (System Exchange Description)	Contains information about the electrical connection between the two substations and the communication network information, and semantics of IEDs involved in inter-substation communication.

A. SG-ML Specification

SG-ML is the modelling language for configuring smart grid cyber range and is defined as a set of XML schemas. Thus, the SG-ML model is both human and machine friendly. In other words, SG-ML models can be processed by software while human users can also write and modify them. We have decided to utilize standardized models used in the power grid sector, namely IEC 61850 SCL (System Configuration description Language) and IEC 61131-3 PLCopen XML, as well as the supplementary XML schema defined by us. IEC 61850 SCL schema is used in different kinds of configuration files for the IEC 61850 compliant substation systems (Table I). This design choice allows power grid operators to recycle their own IEC 61850 SCL files corresponding to their own systems to generate a virtual replica for experiments and exercises. While we admit that preparing IEC 61850 SCL files from scratch is not trivial for users from other domains, this can be overcome by sharing a wide range of examples, including ones contributed by power grid experts, in a public repository. Since SCL files are well-structured XML files and well documented, customization of such template is not difficult. Moreover, such templates allows users to reproduce the same virtual environment for experiments, benchmarking and so forth.

Based on our study, most of the static configuration of the smart grid can be derived from SCL files. For instance, an SSD file can be used to generate power flow simulation model while an SCD file can be used for cyber network topology to be emulated. An ICD file contains necessary information to define functionality of virtual smart grid devices, namely IEDs. An SED file defines cyber and physical connectivity between substations, and thus can be used to generate multi-substation topology. SG-ML framework can, in an unified way, support modelling and instantiation of various smart grid systems that differ in terms of the number of substations and the number of devices and topology involved in each substation.

PLCs are the crucial component for automated control in industrial control systems, and they are often used in smart power grid systems. PLCs read measurements from power grid and then execute pre-configured control logic to initiate actuation. Such configuration are defined in IEC 61131-3 PLCopen XML [24], which expresses the control logic and variable definitions.

While the standardized models provide us with useful information for characterizing a cyber range, they are not sufficient. For instance, dynamic behaviour of the system, e.g., load profile and disturbance scenarios, cannot be configured in the SCL files. Thus, we have defined supplementary XML schema (*Power System Extra Config XML*). Besides, parameters for IEDs' protection functions (described in Table II), such as alarm and trip thresholds, and the mapping between the cyber-side devices and physical-side device or information (e.g., which IED is measuring or controlling which transmission lines) are not included in the SCL files. Thus, we defined *IED Config XML* to incorporate the missing parameters. In addition, data sources and data points for SCADA HMI are not part of the SCL files. Hence, these can be defined in another supplementary XML schema *SCADA Config XML*. In order to ensure user-friendliness, supplementary XML schemas are defined in a simple, straightforward format [16]. Usage of the supplementary XML files will be illustrated in Figure 3.

B. SG-ML Processor

SG-ML Processor is a toolchain to parse SG-ML files that are used to generate cyber and physical model to be emulated in the cyber range. The components of the SG-ML Processor is illustrated in Figure 2 (the middle section).

Generation of Power System Simulation Model: An IEC 61850 SSD file contains information such as a single-line diagram of the power grid topology in a substation. Thus, SG-ML parses the SSD file and then generates a power system simulation model. In the current version, SG-ML Processor generates a simulation model for Pandapower [25], an open-source power system simulator. While an SSD file only contains topology in a single substation, it is often desired to simulate a larger system model consisting of multiple-substations. In such a case, IEC 61850 SED files, along with SSD files of the substations, are used. Typically, an SED file contains connectivity between a pair of substations. Our toolchain first combines multiple SSD files into a consolidated SSD file based on the connectivity derived from SED files. Then the consolidated SSD file is processed using the same tool to generate a multi-substation power grid physical model (see also Table I). In order to run the power system simulation for the cyber range, we further need to provide information such

TABLE II
PROTECTION FUNCTIONS ON VIRTUAL IED

IEC 61850 Standard Logical Node Name	Description	Thresholds in IED Config XML File
PTOC (Time Over-current protection)	Opens a circuit breaker when the amount of power flow exceeds the threshold.	Threshold limit for current, generally 3 to 4 times the nominal current
PTOV (Over-voltage protection)	Opens a circuit breaker when the voltage on a bus exceeds the threshold	Threshold limit on bus voltage
PTUV (Under-voltage protection)	Opens a circuit breaker when the voltage on a bus goes below the threshold	Lower limit of bus voltage
PDIF (Differential Protection)	Opens a circuit breaker when the current measurements at the 2 connected substations are different beyond the threshold	Threshold limit for differential current between two substations
CILO (Interlocking)	Prevents a circuit breaker to be closed when a certain circuit breaker is open	-

as load profile and simulation scenarios. Simulation scenarios include disturbance and contingency, such as generator loss, line loss, etc. In order to incorporate these, the Power System Config Extra XML file is used. The XML file specifies the amount of load and circuit breaker status in a time series for each component in the simulation model. The power system simulator in the cyber range reads these parameters at each step of the simulation.

Generation of Cyber Network Emulation Model: For each substation, cyber network model can be derived from IEC 61850 SCD file. An SCD file contains network addresses (including IP address and MAC address) of nodes, and connectivity between nodes (e.g., node-switch, switch-switch connections, etc.). These parameters are used to configure the network emulator. In the current version, we use Mininet [26] for the cyber network emulation. Similar to SSD files, each SCD file contains information about a single substation. Thus, to produce multi-substation cyber network model, we need to combine multiple SCD files. Typically, substations are connected through wide area network (WAN). The toolchain of the current version simplifies the emulation of WAN, and it is abstracted as a single switch connected to all substations.

Virtual IED Configuration: Virtual IEDs are implemented as an application written in C language using libiec61850 library [27]. A virtual IED implements communication using IEC 61850 protocols, including MMS (Manufacturing Message Specification), GOOSE (Generic Object Oriented Substation Event), R-GOOSE (Routable GOOSE) and R-SV (Routable Sampled Value). IEC 61850 MMS is utilized for communication between SCADA HMI and IEDs and PLCs and IEDs for conveying interrogation and control commands. GOOSE and R-GOOSE are utilized among IEDs to exchange device status information, while R-SV is used for sending power grid measurements among IEDs. Virtual IEDs also implements popular protection functions, which are listed in Table II. Each virtual IED is instantiated by an IEC 61850 ICD file by enabling features defined in it. For instance, if the ICD file contains definition of logical node PTOV, over-voltage protection function is enabled. Moreover, if inter-substation protection function (logical node CILO) is defined in the ICD file, communication module for R-GOOSE and R-SV protocols are enabled. However, an ICD file alone is not sufficient because actual threshold for each protection function is not specified in the ICD file. Thus, to provide supplementary information, we have introduced IED Config XML. Virtual IEDs are connected to the power system simulator through an open-sourced MySQL database. This works as a "cache" storing a set of key-value pairs, for reading power grid measurements (voltages, power flow, etc.) and executing control (e.g., opening/closing circuit breakers). As it is necessary for each virtual IED to know the mapping between the naming of data item in the ICD file and the power system simulation output, such information is also part of self-defined IED Config XML [16].

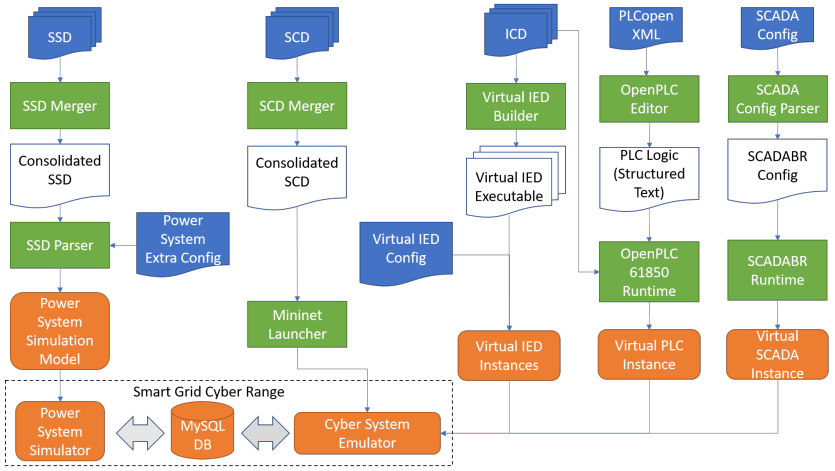
Virtual PLC Configuration: Our cyber range uses an open-source PLC software, namely OpenPLC61850 [31], for emulating a PLC. OpenPLC61850 supports Modbus communication protocol (for interacting with SCADA) and IEC 61850 MMS protocol towards IEDs. OpenPLC61850 requires a set of ICD files corresponding to the IEDs that it interacts with, as well as an IEC 61131-3 PLCopen XML file that contains control logic. According to the configuration found in the SCD file explained earlier, OpenPLC61850 is started on nodes that run PLCs.

Virtual SCADA Configuration: A SCADA system offers an user-interface for a human user to monitor the system status and trigger manual control on a physical plant. Our cyber range utilizes an open-source software, called SCADABR [30]. The settings on data source (e.g., PLCs) and data points has to be configured in SCADABR according to the user-defined model. We have implemented a script to translate the SCADA Config XML into a JSON format that SCADABR can import.

The overall procedure of SG-ML Processor and the placement of each module (green rectangular) are found in Figure 3.

C. Limitation

A cyber range generated by SG-ML relies on open-source tools for the sake of broader accessibility. One limitation caused by this decision is that the power system simulation is not completely real-time or capable of simulating dynamics. Pandapower [25] simulator we employed is a steady-state power flow simulation software, and it is a one-time solver that provides a snapshot of power grid status. Therefore, our cyber range runs it periodically (e.g., every 100ms) with the updated configuration and load profile. This implies that change of power grid status happens with this time granularity in a discrete manner. On the other hand, cyber range is intended



Module Name	Description
SSD Merger	For multi-substation model, combine multiple SSD files into a consolidated SSD file
SCD Merger	For multi-substation model, combine multiple SCD files into a consolidated SCD file
SSD Parser	Generate power system simulation model from SSD
Mininet Launcher	Generate cyber topology from SCD and start virtual network
Virtual IED Builder	Configure and compile virtual IED instance based on ICD
OpenPLC Editor / OpenPLC61850	Open-source PLC runtime and configuration tool [28], [29]
SCADA Config Parser	Parse SCADA Config XML to generate JSON that can be imported to SCADABR
SCADABR	Open-source SCADA HMI for monitoring power grid status [30]

Fig. 3. SG-ML Processor Toolchain Flowchart and Module Description

for human-interactive cyber attack exercise and experiments, and SCADA HMI and PLCs are collecting data usually with second-level granularity. Thus, the time granularity and real-timeness of this degree are still acceptable in practice.

IV. Demonstration of SG-ML and Cyber Range

A. Generation of EPIC Testbed Cyber Range

EPIC [5], [32] is a state-of-the-art smart grid security testbed hosted by Singapore University of Technology and Design. This testbed is utilized for research and training to design a safe and secure critical infrastructure. Therefore, we consider EPIC testbed for our demonstration. The topology and configuration are available at [5], [32]. EPIC testbed consists of 4 segments, namely generation, transmission, microgrid, and smart homes. The power generation is performed through two generators (in generation segment) and PV and batteries (in microgrid segment). This combined generation reflects the modern-day power grid with conventional power sources and renewable energy sources (RES). The smart homes consist of controllable loads. Each of these segments include multiple IEDs connected the power grid devices and is monitored by a SCADA HMI. While the original EPIC testbed includes multiple PLCs, in the cyber range we consider one PLC that mediates communication between SCADA HMI and IEDs (called CPLC). In the real power grid, these segments belong to different substations. However, following the EPIC testbed setting, we consider all belong to a single substation.

The SCL files can be generated with any tool or can be obtained from the real system or an open-source community. Our toolchain conducts the preparation tasks in a largely automated manner, such as generation of the power system simulation model, cyber network emulation model, and/or virtual IED, PLC, and SCADA HMI instances (Figure 3).

The cyber topology of the EPIC testbed model is shown in Figure 4. The scripts in our toolchain parse an SCD file (consolidated SCD, in case of multi-substation model) and then extract necessary information into an intermediate JSON file, which is then passed to the script to configure and start the Mininet emulator. The same script also launches virtual IED executables on the specified virtual nodes on the Mininet.

After the Mininet emulator is started, the virtual PLC and a SCADA HMI is started on the respective virtual node on Mininet. As open-source tools (OpenPLC61850 [31] and SCADABR [30]) are used, the starting process has to be done manually. The user can access the command-line terminal and/or web interface of the corresponding virtual node and then start the necessary program. PLC logic in Structured Text format can be uploaded to the OpenPLC runtime and then started. The main responsibility of CPLC in the EPIC testbed is to mediate the communication between IEDs and SCADA HMI. Therefore, we also configured the virtual PLC accordingly. Note that OpenPLC61850 also requires ICD files of IEDs that the PLC interacts with. Regarding SCADABR, after starting up, the user can upload the SCADABR Config JSON data that defines data sources and data points.

After confirming the communication among the virtual devices, we can start the power flow simulator. We utilize Pandapower simulator, and the topology is automatically defined according to the SSD file. Our script generates the topology by parsing the SSD file, and then, by using the information from the configuration file, a sequence of power system simulation models is created (Figure 5). The models in the sequence are executed at a designated time slot (e.g., 100ms interval).

Our toolchain can support smart grid system including multiple substations, beyond the scale of the EPIC model. Cyber and physical connectivity among substations and communication models are defined by using IEC 61850 SED files (see Table I). Based on our experiments, a commodity desktop PC with Intel Core i9 Processor and 16GB RAM can host a 5-substation model including 104 virtual IEDs with 100ms power flow simulation interval. It is also possible to define a cyber range spanning over multiple nodes to scale up further.

B. Cyber Attack Case Studies

As the main purpose of a cyber range is to conduct interactive cyber attack experiments and exercises, in this

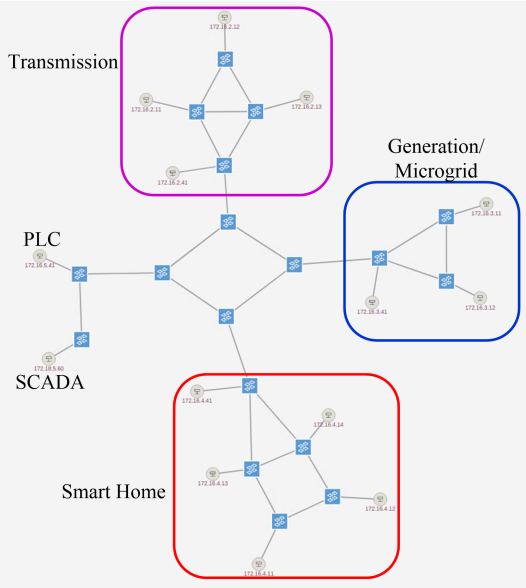


Fig. 4. Generated Cyber Network Topology on Mininet (EPIC Model) generated using ONOS [33]. Rounded rectangles show mapping to the EPIC testbed.

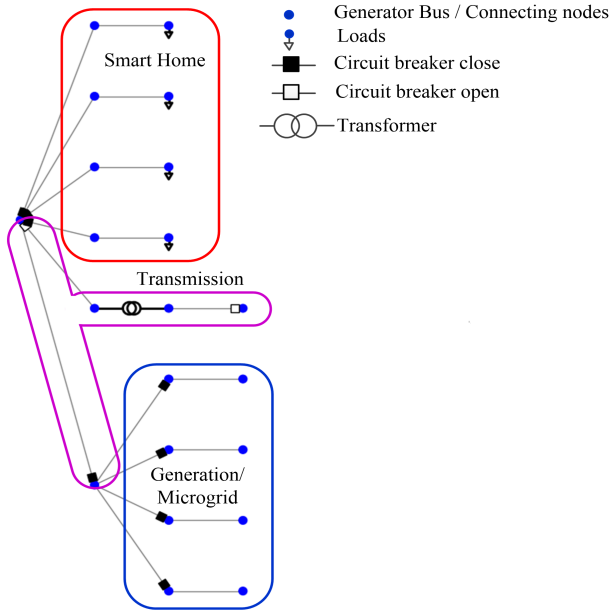


Fig. 5. Generated Power System Topology on Pandapower (EPIC Model). Rounded rectangles show mapping to the EPIC testbed.

section we discuss how the cyber attack case studies can be conducted on the cyber range. Owing to the limitation of space, we leave the demonstration to the demo video found at https://github.com/smartgridadsc/CyberRange.

Among a wide range of attack vectors, we focus on false command injection and man-in-the-middle attacks. The former can cause direct and immediate impact on power grid stability as demonstrated in the 2015 Ukraine incident [34], and the latter is a versatile building block for mounting a wide range of attacks, such as false data injection and alarm suppression. We note that attacks that can be experimented are not limited to these two. Users can utilize any penetration testing tool like Nmap and Metasploit on a virtual node of the cyber range or on their own devices connected to the cyber range.

False Command Injection (FCI) Attack: Assuming that the attacker has compromised one of the nodes in the system and run malwares like CrashOverride [35] to transmit fake IEC 61850 MMS commands. Attack of this sort can be experimented by running an IEC 61850 MMS client (e.g., IEC61850bean [36]) on a node in the cyber range to emit standard-compliant command messages. Once the IED receives a circuit breaker (CB) open command, for instance, the corresponding CB is operated, and the power flow change is calculated by the power flow simulator.

Man-in-the-middle (MITM) Attack: Typically man-in-the-middle (MITM) attack is mounted by using a strategy called ARP (Address Resolution Protocol) spoofing. This confuses the mapping between a device's logical (IP) address and physical address. Using ARP spoofing, an attacker can mislead the traffic to itself for interception and manipulation. As a consequence, the attacker could possibly mislead the SCADA HMI or the PLC to confuse the plant control (Figure 6).

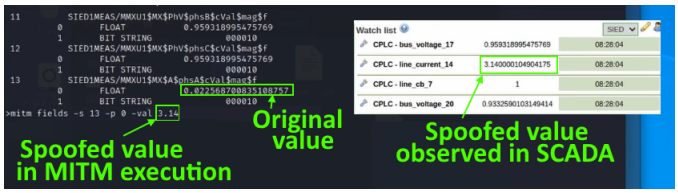


Fig. 6. MITM Attack on a Power Grid Measurement

V. Conclusions

We introduced a novel framework for modelling and automated generation of smart grid cyber range, called SG-ML. SG-ML framework makes a smart grid cyber range accessible to broader user base, including power grid industry, smart grid device vendors, education sectors, and academia. In particular, power grid operators can use our tool to generate a virtual replica of the real infrastructure to conduct intensive red-team testing, validation of configurations, compatibility testing, and so forth. We have open-sourced the tool along with example models for getting real-world feedback for future enhancement. Enhancement of flexibility by using other virtualization technologies, such as Docker, is part of our future work. We also plan to develop a cloud-based cyber range service based on our framework for enhanced accessibility and scalability.

Acknowledgment

This research is supported in part by the National Research Foundation, Singapore, Singapore University of Technology and Design under its National Satellite of Excellence in Design Science and Technology for Secure Critical Infrastructure Grant (NSoE_DeST-SCI2019-0005), and in part by the National Research Foundation, Prime Minister's Office, Singapore under its Campus for Research Excellence and Technological Enterprise (CREATE) programme.

REFERENCES

[1] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49–51, 2011.

[2] D. U. Case, "Analysis of the cyber attack on the ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, vol. 388, pp. 1–29, 2016.

[3] "Venezuela's maduro: Blackout due to cyber-attack, infiltrators," [Online]. Available at https://www.aljazeera.com/news/2019/3/10/venezuelas-maduro-blackout-due-to-cyber-attack-infiltrators.

[4] "Hackers leak files stolen in pakistan's k-electric ransomware attack," [Online]. Available at https://www.bleepingcomputer.com/news/security/hackers-leak-files-stolen-in-pakistans-k-electric-ransomware-attack/.

[5] iTrust, Available at https://itrust.sutd.edu.sg/testbeds/electric-power-intelligent-control-epic/.

[6] J. Weiss, "Aurora generator test," *Handbook of SCADA/Control Systems Security*, vol. 107, 2016.

[7] P. Gunathilaka, D. Mashima, and B. Chen, "Softgrid: A software-based smart grid testbed for evaluating substation cybersecurity solutions," in *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy*, ser. CPS-SPC '16. New York, NY, USA: Association for Computing Machinery, 2016, p. 113–124.

[8] M. Annor-Asante and B. Pranggono, "Development of smart grid testbed with low-cost hardware and software for cybersecurity research and education," *Wireless Pers Commun*, vol. 101, p. 1357–1377, 2018.

[9] M. Mallouhi, Y. Al-Nashif, D. Cox, T. Chadaga, and S. Hariri, "A testbed for analyzing security of scada control systems (tasscs)," in *ISGT 2011*, 2011, pp. 1–7.

[10] E. Hammad, M. Ezeme, and A. Farraj, "Implementation and development of an offline co-simulation testbed for studies of power systems cyber security and control verification," *International Journal of Electrical Power & Energy Systems*, vol. 104, pp. 817–826, 2019.

[11] 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.

[12] G. Elbez, H. B. Keller, and V. Hagenmeyer, "A Cost-efficient Software Testbed for Cyber-Physical Security in IEC 61850-based Substations," in *IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2018.

[13] D. Mashima, D. Kok, W. Lin, M. Hazwan, and A. Cheng, "On design and enhancement of smart grid honeypot system for practical collection of threat intelligence," in *13th USENIX Workshop on Cyber Security Experimentation and Test (CSET 20)*, 2020.

[14] M. M. Roomi, P. P. Biswas, D. Mashima, Y. Fan, and E.-C. Chang, "False data injection cyber range of modernized substation system," in *2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, 2020, pp. 1–7.

[15] N. K. Kandasamy, S. Venugopalan, T. K. Wong, and L. J. Nicholas, "Epictwin: an electric power digital twin for cyber security testing, research and education," *arXiv preprint arXiv:2105.04260*, 2021.

[16] M. M. Roomi, S. S. Hussain, D. Mashima, E.-C. Chang, and D. Nicol, "SG-ML: SMART GRID CYBER RANGE MODELLING FRAMEWORK SPECIFICATION (Version 0.9)," [Online]. Available at https://github.com/smartgridadsc/CyberRange.

[17] R. E. Mackiewicz, "Overview of iec 61850 and benefits," in *2006 IEEE Power Engineering Society General Meeting*. IEEE, 2006, pp. 8–pp.

[18] I. TC57, "Iec 61850: Communication networks and systems for power utility automation," *International Electrotechnical Commission Std*, vol. 53, p. 54, 2010.

[19] A. A. Smadi, B. T. Ajao, B. K. Johnson, H. Lei, Y. Chakhchoukh, and Q. Abu Al-Haija, "A comprehensive survey on cyber-physical smart grid testbed architectures: Requirements and challenges," *Electronics*, vol. 10, no. 9, p. 1043, 2021.

[20] I. N. Fovino, M. Masera, L. Guidi, and G. Carpi, "An experimental platform for assessing scada vulnerabilities and countermeasures in power plants," in *3rd International Conference on Human System Interaction*. IEEE, 2010, pp. 679–686.

[21] K. Barnes and B. Johnson, "National scada test bed substation automation evaluation report," Idaho National Lab.(INL), Idaho Falls, ID (United States), Tech. Rep., 2009.

[22] M. McDonald, J. Mulder, B. Richardson, R. Cassidy, A. Chavez, N. Pattengale, G. Pollock, J. Urrea, M. Schwartz, W. Atkins *et al.*, "Modeling and simulation for cyber-physical system security research, development and applications," *Sandia National Laboratories, Tech. Rep. Sandia Report SAND2010-0568*, 2010.

[23] M. M. Roomi, S. S. Hussain, D. Mashima, E.-C. Chang, and T. S. Ustun, "Analysis of false data injection attacks against automated control for parallel generators in iec 61850-based smart grid systems," *IEEE Systems Journal*, 2023.

[24] A. Otto and K. Hellmann, "Iec 61131: A general overview and emerging trends," *IEEE Industrial Electronics Magazine*, vol. 3, no. 4, pp. 27–31, 2009.

[25] L. Thurner, A. Scheidler, F. Schäfer, J.-H. Menke, J. Dollichon, F. Meier, S. Meinecke, and M. Braun, "pandapower—an open-source python tool for convenient modeling, analysis, and optimization of electric power systems," *IEEE Transactions on Power Systems*, vol. 33, no. 6, pp. 6510–6521, 2018.

[26] "Mininet," Available at http://mininet.org/.

[27] "Open source libraries for iec 61850 and iec 60870-5-101/104," [Online]. Available at https://libiec61850.com/.

[28] "OPENPLC," [Online]. Available at https://openplcproject.com/.

[29] "OpenPLC61850," [Online]. Available: https://github.com/smartgridadsc/OpenPLC61850.

[30] "ScadaBR," Available at https://www.scadabr.com.br/.

[31] M. M. Roomi, W. S. Ong, D. Mashima, and S. S. M. Hussain, "OpenPLC61850: An IEC 61850 MMS compatible open source PLC for smart grid research," *SoftwareX*, vol. 17, p. 100917, 2022.

[32] A. Siddiqi, N. O. Tippenhauer, D. Mashima, and B. Chen, "On practical threat scenario testing in an electric power ics testbed," in *Proceedings of the 4th ACM Workshop on Cyber-Physical System Security*, 2018, pp. 15–21.

[33] "Open Network Operating System (ONOS)," [Online]. Available at https://github.com/opennetworkinglab/onos.

[34] K. Zetter, "Inside the cunning, unprecedented hack of ukraine's power grid," http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/, 2016.

[35] "Crashoverride malware," [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA17-163A, (Date last accessed on Aug. 18, 2017).

[36] "Iec61850bean," [Online]. Available: https://www.beanit.com/iec-61850/, (Date last accessed on Nov. 28, 2022).