Designing An IEC 61850 Based Power Distribution Substation Simulation/Emulation Testbed for Cyber-Physical Security Studies

Eniye Tebekaemi * and Duminda Wijesekera†
Volgenau School of Engineering
George Mason University
Fairfax, USA
Email: *etebekae@gmu.edu, †dwijesek@gmu.edu

***Abstract*—The present traditional power grid system is slowly migrating to an interactive, intelligent power grid system (smart grid or future grid) driven by information and communication technology. The smart grid functions are expected to improve the reliability, efficiency, operations and control of the electric power grid. The smart grid functions are realizable through power communication networks that interface with traditional computer networks often connected to the Internet. This situation makes cyber-physical security a serious concern in the design, development, and implementation of smart grid functions in power grid systems. Understanding the physical behavior, cyber security challenges, physical security challenges, impact of cyber/physical security breaches, and security requirements of time-critical cyber-physical systems like the smart grid is critical in designing a robust security solution that ensures its safe and reliable operation. This work focuses on the design and implementation of a simulation testbed that would support extensive analysis of communication protocols, cyber-physical security functions, intelligent electronic device (IED) vulnerabilities, network configuration, and physical security requirements of an IEC 61850 based power distribution substation.**

Keywords–Cyber Security; Communication Protocols; Simulation Testbed; Cyber-Physical Systems; Smart Grid; Power Substation Automation.

I. INTRODUCTION

Simulation of cyber-physical systems is fast becoming a popular method for analyzing the behavior of hybrid systems and testing out new functionalities before deployment in the real world. In power systems, simulation testbeds have been used extensively for fault analysis, testing of protection and control functions, and in the testing and analysis of new technologies. The future grid (or smart grid) represents one such new technology that incorporates data communication network into existing power networks to provide a more efficient and resilient power grid system. Simulating the smart grid functions for cyber-physical security studies requires three major parts: 1) Simulation of the physical power system, 2) Simulation of the communication network, and 3) The interaction between the physical power system and the communication network. There exist several power systems simulation software used for the design, evaluation, and analysis of powers systems that supports real-time simulation, discrete event simulation, and hardware in the loop (HIL) simulation. Most research work focuses on the use of network simulators to simulate network communication between components, and either implement the smart grid functions in the simulated network nodes or as functions in the power system simulator. This approach helps researchers to determine suitable network topology and configuration that supports the real-time communication requirements for the smart grid. For cyber security studies, the approach helps in studying the effects of packet delay, packet loss, packet injection and data manipulation on the simulated power systems.

The major objective of this work is to expand the scope of cyber-physical security studies using simulation testbeds to perform real-time analysis of smart grid communication network and security protocols, analyze the impact of physical disturbance (deliberate and accidental), provide a realistic environment for implementing and testing new and existing smart grid functions through virtual IEDs, perform vulnerability analysis of physical IEDs used in smart grid systems, test new Internet of Things (IoT) services, and analyze security protocols and security controls for the smart grid. To achieve this, the physical system, IEDs and communication network must be independent and support relevant standards and protocols to ensure interoperability when implementing smart grid functions. Implementing IEDs as nodes in network simulators or as procedures in power system simulators in the smart grid simulation testbed makes it tough to perform studies that meet our objectives.

In this work, we make use of virtual IEDs, which are computing units implemented as either virtual machines (VMs) or standalone computers with full network support capabilities. The virtual IEDs can be connected through a physical, simulated or software-defined network (SDN). The virtual IEDs depending on the smart grid function they implement, can read values from the simulated power system, communicate with other IEDs through the communication network, and write control instructions to the simulated power system. Fig. 1 shows the high-level graphical representation of the simulation testbed.

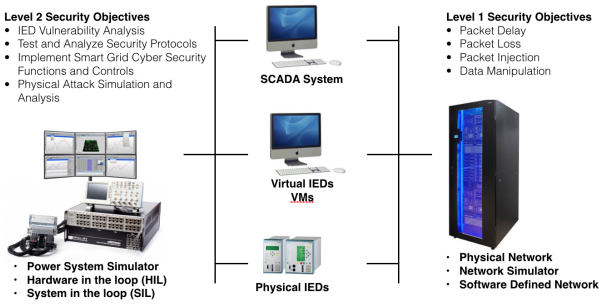

Figure 1: High-level representation of the proposed testbed

The simulation testbed presented in this work enables cyber-physical security research objectives at level 2. Some of the other advantages of this model include:

 ISBN: 978-1-61208-512-8

1) *Modular Design* - The modular structure used in our testbed enables components to be easily replaced with newer and more efficient components, making it easy to test new technologies, upgrade and replace existing components, and perform scale up operations seamlessly.
2) *Scalability* – The testbed can easily be scaled out to support more smart grid functions, HIL co-simulations, distributed simulations, and remote IoT operations.
3) *Cost* – Using virtual IEDs makes it cheap and convenient to implement practical smart grid functions. The testbed can be set up on a small scale in a purely virtual environment, using a single host computer with multiple VMs costing a few hundred dollars; or large scale using real-time HIL simulators such as RTDS Simulator and OPAL-RT Simulator with real IEDs and actual communications and networking equipment.
4) *Ease of Setup and Use* – Both network and power simulators come with APIs written in a specific programming language that must be learned to use the simulator. Using these network simulators means that one can hardly take advantage of already existing smart grid libraries when using network simulators. Our testbed allows users to implement smart grid functions using libraries, programming languages, and applications they are comfortable with in the virtual IEDs.
5) *Interoperability* - The testbed is based on IEC 61850 standards and related protocols, which makes it relatively easy to perform system in the loop (SIL) and HIL simulations with systems and devices that support IEC 61850.

The remainder of this work is organized as follows: Section II discusses the cyber and physical vulnerabilities of the smart grid, and related work is discussed in Section III. Section IV reviews related smart grid standards, software, and tools that are frequently used in designing simulation testbeds. In Section V, we present our simulation testbed model. Section VI focuses on the implementation of the model and presentation of some of our results. We conclude in Section VII by discussing the accomplishments and limitations of this work, and potential future work.

II. Cyber and Physical Vulnerabilities of Smart Grid

Over the years, we have seen series of cyber-attacks of massive scale against government organizations and private companies alike. Cyber-Physical systems like the smart grid, are vulnerable to both cyber and physical acts that could critically impact their safe and reliable operation. Also, the high availability, tight coupling of components, and time sensitive communication requirements of power systems make them even more vulnerable.

A. Physical Vulnerabilities

Attacks on Physical Components - Power systems have components distributed over a large geographical area, and some of their components are installed in areas where it is difficult to guarantee physical security. An attacker can physically attack sensors, actuators and other components that may result in faulty measurements causing errors in the system state estimation and control operations [1], [2].

Faults and Failure of Components - Devices may fail during operation. These failures could be caused by some accumulated faults or the device reaching its end of life. In most cases, power system components degenerate progressively giving facility managers enough time to respond and in some cases, failure is abrupt with little or no indication.

Accidents and Acts of Nature - Severe weather conditions could cause instability in power systems and power disruption. Power systems frequently suffer from trees falling on power lines, storms, lightning and thunder strikes destroying power installations and causing power outages.

B. Cyber Vulnerabilities

Software and Firmware Bugs - IEDs rely on software to provide the much-needed functionality. Software often comes preinstalled which determines the (primary) behavior of the IED without any need for human interaction (firmware and drivers), while others can be installed by the user to extend the functionality of the smart device. Since software is written by humans, we cannot rule out errors in the implementation, and attackers look for such errors to exploit the system [3]. An example of this was the Heartbleed vulnerability of 2014 caused by bugs in the OpenSSL implementation of the secure sockets layer (SSL) protocol [4].

IED and Network Misconfiguration - Misconfiguration of network components and IEDs are huge security risks to the smart grid. Some of these misconfigurations include: 1) Using default settings and default passwords even when the device is operational, 2) poorly maintained security and software patches, 3) using short and guessable passwords, 4) poorly configured firewall [5], or some other configuration issues. All these can put the network at risk.

Data Manipulation and Falsification - Data manipulation and falsification attacks border on data integrity. By altering certain bits of the signal, an attacker alters the meaning of the control signal. An attacker with knowledge of how the system works can generate packets or replay previously recorded packets to change the correct behavior of the system. Data manipulation attacks are countered by proper application of cryptographic controls in the authentication and integrity checks of communicating nodes and data.

Malware and Advanced Persistent Threat (APT) - Malware are pieces of software with malicious intent. Malware could open covert communication channels to the remote attacker so that the attacker can take control of the host, send vital information about the system to a remote attacker, or just perform preprogrammed malicious actions [6]. APTs are unique forms of malware and attacks that use various stealthy techniques to gain remote access while staying undetected on the host system for a long time.

Communication Channel - power systems are distributed and span multiple locations requiring communication links between the various parts of the system. This communication network can be wired or wireless, although the wireless connection is most often used. One weakness of wireless communication is that of visibility. Anyone in proximity to the wireless network and operating on the same frequency and

 ISBN: 978-1-61208-512-8

channel can see the network traffic. Power systems rely on the timeliness of communication packets to operate (e.g., interlocking and switching functions in power distribution systems) and a mere delay or loss of packets may yield undesired results. Typical attacks include signal jamming, wormhole attacks, and signal diversion attacks.

C. Coordinated Cyber-Physical Attacks

Another possibility is a coordinated cyber-physical attack, exploiting both the physical and cyber vulnerabilities of the power system in a contemporary way to maximize the impact. This kind of attack could be a collusion between an insider with access to the physical power system components, and a cyber attacker at a remote location with knowledge of the power communication network working together to cause cascading failures and service disruption.

III. Related Work

There are a few substation simulation testbeds designed primarily for cyber-physical security related research. These testbeds are either too expensive to reproduce or lack the capability for level 2 cyber security work. This is a significant setback for researchers who need a realistic simulation testbed for cyber-physical security studies in power systems but do not have a large budget. Other issues are the lack of implementation of existing information security standards, which means these information security protocols cannot be evaluated for vulnerabilities and possible impact on the substation. For example, the IEC 62531-9 uses the group domain of interpretation (GDOI) protocol for key management, but what happens if the key management server is down or compromised? Hahn et al. [7] developed the PowerCyber testbed at Iowa State University that supports level 1 and 2 cyber security objectives. In their work, they use the RTDS Simulator platform and the PowerFactory power simulation software to simulate the physical power system. The RTDS Simulator provides real-time HIL simulation and interfaces directly with the IEDs, while the PowerFactory is used mainly for non-realtime analysis and connects to the RTDS Simulator through the open platform communications (OPC) protocols. The IEDs are either actual physical IEDs or virtual machines (VMs), and they communicate with remote terminal units (RTUs) that aggregate their data and send it to the controller. For the communication network part, they use the Internet-Scale Event and Attack Generation Environment (ISEAGE), a multimillion-dollar research at Iowa State University dedicated to designing a security testbed to emulate the Internet for the purpose of researching, designing, and testing cyber defense mechanisms.

Yang et al. [8] presented a testbed that simulates the power system using the RTDS Simulator, actual IEDs and communication devices. Using only real IEDs makes it difficult to implement and analyze new substation security protocols and functions, and gives little room for scalability. Liu et al. [9] designed a reconfigurable testbed for analyzing the impact of specific cyber-attacks on the power systems. They implemented their substation testbed using RTDS Simulator to simulate the power system, and used network simulator 3 (NS3) and the defense technology experimental research laboratory (DeterLab) to simulate the communication network. Their testbed was not implemented according to the IEC 61850 standards, and their controllers were modeled as nodes in the network simulator. Koutsandria et al. [10] simulated the power system with Matlab/Simulink and used simulated and actual programmable logic controllers (PLC) for control. They also used an actual local area network (LAN) setup for the network communication part. Their objective was to validate the continuous, reliable operation of network intrusion detection systems (NIDS) in exposed network environments.

Jarmakiewicz et al. [11] used labVIEW software to simulate the power system and used real IEDs connected to a real LAN. Hong et al. proposed in [12] a cyber-physical security testbed to simulate attacks and validate security controls. Their proposed testbed although not yet implemented, would be based on RTDS and support HIL simulations. Deng et al. in [13] designed their testbed to test the operation, control and protection functions of the substation using RT-LAB, actual and virtual IEDs. Their testbed is not intended for cyber security analysis and lacks an appropriate communication network model. Chen et al. [14] used RTDS and OPNET to simulate the power system and communication network respectively, but implemented the bay-Level IEDs as functions in RTDS and the station-level IEDs as nodes in OPNET, and not as standalone devices. The works [15]–[19] all have similar software based testbeds. The major differences are in their choice of software combination used in the co-simulation of power and communication network systems. The IEDs used in their simulation is either modeled as nodes in the network simulator or as functions in the power system simulation.

IV. Review of Standards, Libraries and Tools

Understanding the standards for substation automation necessary to set up a simulation testbed for research in power systems could be daunting, as it requires one to have adequate knowledge of both the power systems and communications network domain. The international organization for standardization (ISO) and the international electrotechnical commission (IEC) are the two primary organizations that define standards for power systems. In this section, we will discuss the IEC 61850 Standards (communication networks and systems for substations), the ISO/IEC 9506 (MMS – Manufacturing Message Specification), the IEC 62351 (Information Security for Power System Control Operations), the RFC 6407 (GDOI - Group Domain of Interpretation) and the relevant parts of the open systems interconnection (OSI) communication model.

IEC 61850 (Communication Networks and Systems in Substations) is the most popular internationally accepted standard for substation automation. It describes the structure, functions, and interface for substation devices, as well as the communication protocol for process-level, bay-level, and station-level communication necessary for substation automation.

ISO/IEC 9506 (MMS – Manufacturing Message Specification) is an application layer messaging standard based on the OSI communication model. MMS is designed for controlling and monitoring devices remotely through remote terminal units (RTU) and programmable logic controllers (PLC). It defines functions common across distributed automation systems and acts as a concrete object to implement the abstract IEC 61850 standards.

IEC 62351 (Information Security for Power Systems Control Operations) is the current security standard and defines the end to end cyber security requirements for securing power

 ISBN: 978-1-61208-512-8

management networks. It specifies the security requirements for secure data communication and processing in power systems in regards to data confidentiality, data integrity, authentication, and non-repudiation.

RFC 6407 (GDOI - The Group Domain of Interpretation) is the internet engineering task force (IETF) protocol used to provide group key management for secure group communications. The IEC 62351 standard specifies the use of the GDOI for managing security associations and distributing security transforms in power systems.

Open Systems Interconnection (OSI) Model is the communication model that standardizes the communication functions necessary for computer network communication. The OSI model consists of 7 abstraction layers and defines communication functions and requirements for each layer. It serves as an abstract structure through which network communication protocols are defined.

A. Intelligent Electric Devices (IEDs)

Understanding how the IEC 61850 standard defines the naming structure, data structures, services, and command sets for read, write, and control is necessary to design virtual IEDs. Substation automation consists of functions that facilitate monitoring, protection, and control in the substation. Each substation automation function performs dedicated tasks and is referred to as a logical node in the IEC 61850 standard. A logical node (LN) is defined as the smallest part of the IED that exchanges data and performs some functions [20]. An IED is composed of one or more LNs and must implement all the necessary data structures, services, and interfaces to support each LN it contains. LNs are the building blocks for IEDs and have standardized names, data structures, abstract service interfaces, and behavior models.

1) Naming Structure: LNs exchange data by reading and writing values to memory locations referenced to by their data attribute (DA). The IEC 61850 standard uses a hierarchical naming convention that uniquely identifies each DA in the substation. The first letter of the LN name identifies the group to which the LN belongs, and suffixes can be used to identify each instance of the LN in the IED. An IED name is unique within the substation, and LN name is unique within the IED. Using Fig. 2, we can determine the status value (stVal) of the switch position (Pos) of the circuit breaker Relay1 by referencing *"Relay1/XCBR2.ST.Pos.stVal"*, where "2" represents an instance of the circuit breaker LN (XCBR) in "Relay1", "X" identifies its LN group as switchgear, and "ST" represents the functional constraint (FC) for status value.

2) Data Structure: The compatible data class (CDC) template specifies the data type of each data attribute (DA) allowed for the given data object (DO). For example, if the CDC specifies that the controllable double point (DPC) template be used for the Relay1/XCBR1.Pos data object, then the data attribute for Relay1/XCBR1.ST.Pos.stVal will have a type "coded enum" with four possible states intermediate-state, off, on, bad-state [21]. The timestamp attribute "t" referenced by Relay1/XCBR2.ST.Pos.t will have a data type of either int32 or unsigned int24 based on the chosen time quality [22]. Both IEC 61850-7-2 and IEC 61850-7-3 should be consulted for the detailed definition of all data types and recommended values used in the CDC template.

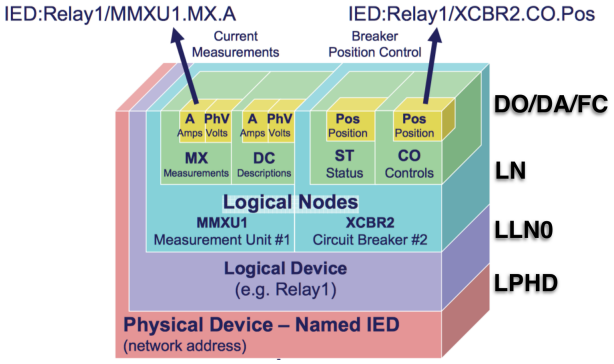

Figure 2: Structural Composition of an IEC 61850 based IED

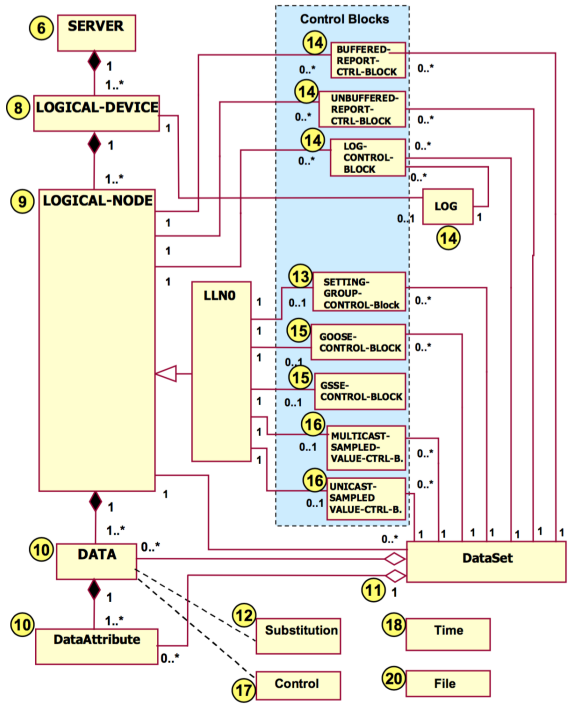

Figure 3: Conceptual service model of the ACSI [22]

3) Services and Interfaces: IEC 61850-7-2 defines an abstract communication service interface (ACSI) for IEC 61850 based IEDs. All IEDs must implement some of the services and interfaces defined by the ACSI if they require real-time cooperation in the substation. ACSI defines abstract interfaces for client/server remote communication that supports real-time data access, remote control, event reporting and more. It also defines the subscriber/publisher communication abstract interface for fast and reliable system-wide event distribution and transmission of sampled values. Interfaces represent communication points, IEDs communicate with one another using these interfaces. Services are activities that run on interfaces, the kind of interface an IED supports determines the type of service the IED can provide.

Fig. 3 summarizes all the abstract interfaces available defined in [22]. IEDs can implement all or a subset of interfaces. The type of interface an IED implements determines the kind

 ISBN: 978-1-61208-512-8

of services it can provide and the type of communication protocol it can use. For example, an IED needs to implement the Generic Object Oriented Substation Event (GOOSE) control block interface to use the GOOSE communication protocol to send GOOSE messages.

B. Protocol for Data Communication

Communication protocols are necessary for IEDs to send and receive messages in a power communication network. IEC 61850 based IEDs rely on the 7-layer OSI reference model which specifies the functional requirements for each layer. The IEC 61850 standard groups the seven abstract OSI layers into two profiles; 1) the ISO application profile (A-Profile) composed of the three upper layers, and 2) the ISO transport profile (T-Profile) composed of the four lower layers. It is important to draw the distinction between an application program and an application protocol. An application program provides a set of functions and an interface through which users can interact with the application, while an application protocol provides a communication structure through which applications interact with other applications irrespective of their internal system representation. Application protocol provides interoperability and universality, which means that application programs can be written in different programming languages, run on different operating systems and still be able to communicate as long as the implement the same application protocol.

The IEC 61850 standard defines all requirements needed to design IED application programs, but not application protocols. Instead, it relies on existing application protocols, and defines mappings from ACSI services to the communication protocol (A-Profile and T-Profile). [23] and [24] describe in detail the mappings from ACSI to MMS, ACSI to Generic Substation Events (GSE/GOOSE), ACSI to Generic Substation State Event (GSSE), and ACSI to sampled value (SV) for both application and transport profiles (A-Profile and T-Profile).

C. Data and Communication Security

Information security is a grave concern for power management systems. Many standards have been proposed over the years, and the IEC 62531 standard [25] is the only globally accepted standard for securing power management systems. The IEC 62531 standard suite defines information security requirements for the various communication profiles used in substation automation necessary to provide confidentiality, integrity, availability, and non-repudiation. The IEC 62531 standard identifies potential threats and vulnerabilities for power automation systems, and other aspects of information security relevant to power automation systems.

1) TCP Profile: IEC 62531-3 specifies the use of transport layer security (TLS) 1.0 or higher to protect TCP/IP profiles and provides protection against eavesdropping through encryption, spoofing through Security Certificates (Node Authentication), replay through TLS encryption, and man-in-the-middle security risk through message authentication [25]. It mandates the support for Rivest, Shamir, and Alderman (RSA) and digital signature standard (DSS) signature algorithms with RSA key length of 2048 bits and also mandates the support for regular and ephemeral Diffie-Hellman key exchange with a key length of 2048 bits. For authentication, it mandates the use of the X.509 certificates with support for multiple certificate authority (CA). As observed by Schlegel et a. [26], IEC 62531-3 can protect against rogue certificates but not against already compromised IEDs which would have valid certificates.

2) MMS Profile: IEC 62531-4 defines the security requirements for all profiles that include MMS. It provides authentication through the use TLS based X.509 certificates but does not cover message integrity and confidentiality. If encryption is to be employed then IEC 62531-3 should be used. The IEC 62531-4 by itself only protects against unauthorized access to information.

3) GOOSE and SV: IEC 62531-6 defines the security requirements for IEC 61850 communication profiles. GOOSE and SV profiles use multicast and non-routable messages that run on the substation LAN, and must be transmitted within 4ms. IEC 62531-6 does not recommend the use of encryption or certificate based authentication as it may increase the transmission time and add more processing overhead. For GOOSE profile, encryption can be used only if the processing and transmission time is less than 4ms. For message authentication and integrity protection of GOOSE and SV messages, the IEC 61850 supports the use of HMAC digital signatures.

4) Access Control and Certificate Management: IEC 62531-8 specifies the use of role-based access control (RBAC) for power systems. RBAC defines roles and set of rights associated with each role. Users/Entities are assigned to roles, and they inherit all the rights associated with that role. The IEC 62531-8 standard defines a list of roles and associated rights for power systems. For certificate/key management, the IEC working group is currently working on the IEC 62351-9 standards, which will specify the use of the Group Domain of Interpretation (GDOI) protocol (RFC 6407).

D. Libraries, Software and Tools

In this section, we will discuss IEC 61850 libraries, network and power simulation software, and other tools frequently used to simulate substation automation functions.

1) IEC 61850 Libraries and Tools: Software libraries are a collection of prepackaged functions and resources used to help reduce the time and effort needed to implement applications that share common properties. Since IEDs implement IEC 61850 services, libraries have been developed by individuals and organizations for some or all of the IEC 61850 services. The libiec61850 [27] and the OpenIEC61850 [28] are two of the most popular open source IEC 61850 libraries in use. The libiec61850 is a c library written by Michael Zillgith under the GPLv3 license and provides a server and client library for the IEC 61850/MMS, IEC 61850/GOOSE, and IEC 61850-9-2/Sampled Values communication protocols. It supports the static implementation and dynamic creation of IED models using substation configuration language (SCL) files or through API calls. It also provides full ISO protocol stack on top of TCP/IP, and publisher and subscriber models used for GOOSE and SV applications. The OpenIEC61850 is an open source implementation of IEC 61850 standard suite written in Java under the Apache 2.0 license. OpenIEC61850 provides IEC 61850/MMS client and server libraries but does not provide native support for the subscriber/publisher model based GOOSE and SV communication protocol. Organizations like Systemcorp, Xelas Energy, SISCO, and SmartGridware all have their implementation of the IEC 61850 standard suite available for purchase.

 ISBN: 978-1-61208-512-8

Development IEC 61850 based IED models could be a complicated process. Creating virtual IEDs requires the application developer to have a thorough understanding of data objects (DO), data attributes (DA), compatible data classes (CDC), interfaces, and services that apply to all the LNs to be implemented in the IED. IED modeling applications such as IEDModeler and OpenSCLTools amongst others, help reduce the complexity and programming errors associated with designing IEDs by visualizing the IED modeling process and generating the corresponding IED Capability Description (ICD) files. Like most of the other IEC 61850 libraries, the libiec61850 library suite has individual tools that parse ICD files into c classes corresponding to the IED model.

2) Power Simulation Software: IEDs implement substation automation functions (protection, monitoring, and control) used inside substations as part of the power management ecosystem. There are several applications used to simulate power systems, some of them are MATLAB/Simulink, GridLab-D, and PSS/E amongst others. MATLAB/Simulink produced by Mathworks is one of the most popular simulation software used for power system simulation experiments today. MATLAB/Simulink uses a very intuitive, graphical component-based code generation process to create models of systems. For power systems simulation, MATLAB/Simulink has a specialized toolbox called Simscape Power Systems (SimPowerSystem). SimPowerSystem provides component libraries and tools for modeling and simulating physical power systems. GridLAb-D is an open source multi-agent based power system distribution simulation and analysis tool developed by the U.S. Department of Energy (DOE). Gridlab-d is very useful in power simulations that involve distributed energy resources (DER), distribution automation, and retail markets interaction and evolution. PSS/E is a power system planning and analysis tool used primarily for power transmission systems [29].

Other popular platforms for power systems simulation are the specialized real-time digital simulators like those produced by RTDS [30] and OPAL-RT [31] Technologies. These are custom hardware and software solutions specialized for continuous real-time digital simulations. They can be used to design, test, analyze and optimize control systems and support personal computer and field programmable gate array (PC/FPGA) based real-time HIL simulations.

3) Communication Network Simulation Software: IEC 61850 based IEDs exchange messages over data communication networks. OPNET, NS2, NS3, OMNET++, and NetSim are some of the most popular network simulation and analysis application used in simulating the communication network part of the power systems automation network. Siraj et al. [32] give a comprehensive analysis of these network simulators, their features, advantages, and disadvantages.

V. Testbed Model

Our testbed model consists of the power model, IED model, communication model, and attack model. The power model for this work is a single bay power distribution substation as shown in Fig. 4.

A. IED Model

IEDs have physical properties such as names, network interfaces, and ON/OFF states. IEDs also have logical behavior which aggregates the behavior of the all the LN's functions that make up the IED. IEC-61850 mandates all IEDs to implement the two system LNs; 1) the physical device LN (LPHD), which abstracts the physical properties of the IEDs, and 2) the Logical node zero (LLN0), which aggregates all the mandatory DAs of the LNs in the IED to provide a single consistent point of access/update. These two system LNs are mandatory for all IEDs whether they are process-level, bay-level or station-level devices as shown in Fig. 2.

1) Process Level:

Switchgear Devices - Make use of circuit breaker LNs (XCBR) and circuit switch LNs (XSWI) that directly control power systems actuators to open or close the breakers and isolators. XCBR and XSWI are process-level devices and subscribe to switch controller (CSWI) for open or close instructions. Each instance of XCBR or XSWI represents one circuit breaker or isolator and controls the operations of that breaker or isolator. Switchgear devices communicate with bay-level IEDs through GOOSE messages and support the GOOSE communication protocol with keyed-hash message authentication code (HMAC) for authentication and integrity protection. All devices in the substation connected to the same process bus share a single group key. The group key is managed by the key management server and must be changed periodically.

Measurement Devices - Make use of current transformer LNs (TCTR) and the voltage transformer LNs (TVTR) to obtain current and voltage measurements from the power system. Each instance of TCTR or TVTR represents one phase measurement from the current or voltage instrumentation transformer in the power system. The TCTRs and TVTRs are aggregated into merging units (MU) that operates a publisher/subscriber service. Merging units support SV multicast communication protocol and transmit voltage and current measurements to subscribers. Merging units also support HMAC for authentication and integrity protection, and TLS protected MMS connection for key management services.

2) Bay Level:

Control IEDs - Control operations like bay-level interlocking functions, fault isolation functions, load management switching functions, voltage/VAR control, frequency control, and power quality control functions are all designed as control IEDs and form part of the "Bay Controller." At the minimum, all control IEDs implement the switch controller LN (CSWI), and sometimes implement the bay-level interlocking LN (CILO) if interlocking functions are to be provided at the bay level. The CSWI controls the operations of switchgear devices (XCBR and XSWI), and the CILO provides the bay-level interlocking rules.

Protection IEDs - Make use of protection function LNs like the time overcurrent protection (PTOC), time overvoltage protection (PTOC), instantaneous overcurrent protection (PIOC), and distance protection (PDIS). Protection IEDs subscribe to the MU and monitoring IEDs to obtain necessary data values needed to make protection decisions. Protection IEDs also implement CSWI for controlling switchgear operations in response to protection decisions. *Monitoring IEDs* - Make Use of sensor-based monitoring LN like the monitor and diagnostics for arc LN (SARC) that monitors gas volumes of gas insulated switchgear devices. Monitor IEDs obtain information from sensors that monitor power system equipment to obtain their state information.

 ISBN: 978-1-61208-512-8

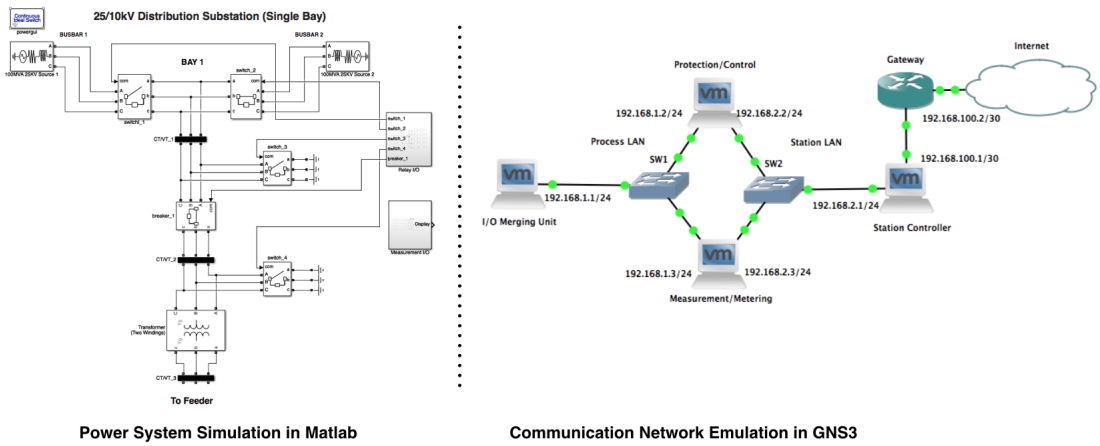

Figure 4: Single Bay IEC 61850 Power Distribution Substation Simulation Testbed

Bay-level IEDs could also implement measuring and metering LNs (MMXU and MMTR), and other LNs to provide additional functionalities that may be required at the bay level. Bay-level Control IEDs support GOOSE and SV protocols for communication with the process and bay-level devices, and MMS protocol for communication with the station-level devices.

3) Station Level: Station-level devices provide monitoring, control, and remote terminal functions for the substation. Functions at this level include human machine interface LN (IHMI), group control/key server (GCKS), remote terminal unit (RTU), and supervisory control and data acquisition (SCADA) services. Station-level devices support TLS protected MMS communication with devices at the station and bay level.

B. Communication Model

The communication model consists of the process network and the station network. Each bay has a dedicated process network, which is a switched or hub-based 10/100Base-T LAN, that supports GOOSE and SV multicast/broadcast protocols and isolate from that of other bays in the substation. The substation has one station network connecting all the bay-level devices and the station-level devices. The substation network is a switched 10/100Base-T LAN redundantly configured.

C. Attack Model

Attacks on the smart power grid could be physical-based, cyber-based, or both physical and cyber based.

1) Physical Attack Model: - There are two types of physical attacks; 1) the incremental attack where the attack occurs slowly and is spaced over time, and 2) the abrupt attack where the impact is sudden. Let C_i be the current state of the device, X be the set of all normal operating states, and Y be the set of faulty states and $Y = \bar{X}$, then we can model an abrupt attack as

$$C_1 = \{C_0 + A\} \in Y \tag{1}$$

Where A is the attack value, and C_0 is the state of the device just before the start of the attack. If A is spread over n duration such that $a = A/n$ be the attack value for each iteration, then we can model the incremental attack as

$$C_i = \{C_{i-1} + a\} \in X \mid 0 \leq i \leq n-1\} \quad and \quad \{C_0 + a.n\} \in Y \tag{2}$$

2) Network Attack Model: An attacker may be able to access the substation network from the process LAN, station LAN, or from a remote network. The type of traffic at each access level is different, and requires different attack strategies for each access level. *Process-Level Attacks* - We assume that the attacker can gain physical access to the process LAN, and the network traffic is predominantly broadcast and multicast GOOSE and SV packets. *Station-Level Attacks* - We assume that the attacker can gain physical access to the substation LAN, and the network traffic is a mixture of multicast GOOSE and unicast MMS packets. *Remote Attacks* - These are attacks that seek to compromise the substation RTUs, IDS, and firewall to gain access to the station network.

VI. Implementation and Results

Our testbed is implemented as shown in Fig. 4, and consists of a single bay with the associated substation devices. The simulation testbed runs on an Intel corei7 MacBook Pro computer, with a processor speed of 2.5ghz, 16GB of RAM, and 512GB SSD.

A. Implementation Details

1) Physical Power System: The power substation system is simulated in Matlab/Simulink. The substation consists of a single bay (Bay1) connected to two three-phase power transmission lines from two different power generation sources using two busbars (Busbar1 and Busbar2). The busbars are controlled by isolator switches (switch_1 and switch_2), and the bay is protected by a circuit breaker (breaker_1). The Bay also has two earthing switches (switch_3 and switch_4) and three three-phase voltage/current measurement units. The simulated power system uses two functions; Measurement I/O, and Relay to send and receive messages from the communication network system through UDP ports. The measurement I/O function receives voltage and current measurements from all the measurement units, converts them into a data communication compatible format and sends them to the communication

 ISBN: 978-1-61208-512-8

network. The relay function receives switchgear control messages from the communication network and converts them into control signals for the simulated switchgears.

2) Process-Level IEDs: At the process-level, we implemented a single VM (I/O Merging Unit) that performs the measurements merging and switchgear control functions. The measurements merging function is composed of nine TVTR and nine TCTR corresponding to each phase in the three three-phase voltage/current measurements received from the measurement I/O. The switchgear control function consists of four XSWI and one XCBR necessary to control the switches and the circuit breaker in the simulated power system.

3) Bay-Level IEDs: We implemented two VMs at the bay level. The first VM (Protection/Control) consists of five CSWIs, two MMXUs, and two CILOs. The CSWIs are configured to publish their status information to all the XSWI and XCBR subscribers in the I/O merging unit using the GOOSE control blocks. The MMXUs subscribe to the TVTRs and TCTRs in the I/O merging unit VM using SV message blocks. The two CILOs contain state and interlocking information about the two isolator switches. The second VM (Measurement/Metering) consists of three MMXUs and subscribes to the TVTRs and TCTRs in the I/O merging unit using SV message blocks.

4) Station-Level Devices: At the station-level, we have the offline CA server VM (not shown in Fig. 4) and the station controller VM. The station controller runs the CSWI client applications for all the switchgear devices and connects to the bay-level IEDs through MMS. The CA server is run offline and its only function is to issue certificates.

5) Communication Network: The communication network simulation comprises of 4 VMs that are identically configured (Ubuntu 14.04.4LTS 1GB RAM, 1 Core Processor, 20GB HDD), the process LAN, and the station LAN. The IEC 61850 standard is implemented using the libiec61850 API modified to support MMS over TLS. The process and station LAN infrastructure are simulated using the GNS3 network emulator. The GNS3 is a network emulation software that emulates network devices (switches and routers) to use VMs without modification as shown in Fig. 4.

6) Attacker: The attacker is implemented as a Kali VM (not shown in Fig. 4). Kali is an advanced penetration testing Linux distribution tool used for penetration testing, hacking, and network security assessments. The Kali VM comes preinstalled with applications frequently used in network security testing and exploitation. The Kali VM is configured to have access to the process and station LAN.

B. Preliminary Results

We tested the testbed against some well-known network attacks at the process and network LAN.

1) Process LAN Attacks: Process-level traffic is predominantly multicast/broadcast and publisher/subscriber ethernet messages. An attacker having access to the process LAN can read and write GOOSE and SV messages. Using wireshark and tcpreplay from the attacker VM, we were able to capture and replay GOOSE messages from the protection/control VM to the I/O merging unit VM. By observing the stNum (status number) and sqNum (sequence number) of the goose messages for switchgear control, we were able to create custom GOOSE messages using scapy (a packet manipulation tool) to control the switchgear devices.

2) Station LAN Attacks: At the station level our single bay implementation only supports MMS unicast client-server messages. To gain access to the network traffic, we did a man-in-the-middle attack by spoofing the ARP messages of the station controller and protection/control VMs. Then we configured our attacker VM to intercept and forward the MMS messages between the station controller and protection/control VMs using the ettercap tool.

The attacks were first performed when the IEC-62531 standard was not implemented, and then when the IEC-62531 standard was implemented. The attacks were not successful when the IEC 62531 standard was implemented. However, the attacker can still see the process LAN messages in plain text, and can learn useful information concerning the behavior of the system.

VII. Conclusion

Cyber-physical systems have both physical and cyber components, and any security solution for cyber-physical systems must take this into consideration. Building an IEC 61850 based substation simulation testbed for cyber-physical security studies requires independence between the physical system, the IEDs, and the communication network to realistically represent the IEC 61850 power substation. This work presents a cost effective testbed model that can be easily implemented and scaled according to budget constraints. Our modular and independent design enables various IEC 61850 functions and configurations that supports security to be implemented and tested using virtual IEDs. Our model enables testing and tuning of network configuration to enhance security and performance, and study the effects of physical attacks and disturbances on the security posture of the substation network.

In our future work, we would expand our substation testbed to use real IEDs, and implement multiple bays like actual substation with full SCADA functions using IEC 61850 standards. We would also simulate physical attacks to study its effects on the security posture of the substation network, analyze existing and proposed smart grid security protocols and controls, and develop cyber-physical security solutions that would take into consideration the physical and cyber behavior of intelligent power systems.

References

[1] R. Smith, “Assault on California power station raises alarm on potential for terrorism,” Wall Street Journal, vol. 5, 2014.

[2] E. I. Bilis, W. Kröger, and C. Nan, “Performance of electric power systems under physical malicious attacks,” IEEE Systems Journal, vol. 7, no. 4, 2013, pp. 854–865.

[3] Y. Li, J. M. McCune, and A. Perrig, “Sbap: Software-based attestation for peripherals,” in International Conference on Trust and Trustworthy Computing. Springer, 2010, pp. 16–29.

[4] Z. Durumeric, J. Kasten, D. Adrian, J. A. Halderman, M. Bailey, F. Li, N. Weaver, J. Amann, J. Beekman, M. Payer, and V. Paxson, “The matter of heartbleed,” in Proceedings of the 2014 Conference on Internet Measurement Conference, ser. IMC ’14. ACM, 2014, pp. 475–488.

[5] C.-C. Liu, A. Stefanov, J. Hong, and P. Panciatici, “Intruders in the grid,” IEEE Power and Energy magazine, vol. 10, no. 1, 2012, pp. 58–66.

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

 ISBN: 978-1-61208-512-8

[7] 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, June 2013, pp. 847–855.

[8] Y. Yang et al., "Cybersecurity test-bed for IEC 61850 based smart substations," in 2015 IEEE Power & Energy Society General Meeting. IEEE, July 2015, pp. 1–5.

[9] 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, Sep. 2015, pp. 2444–2453.

[10] G. Koutsandria et al., "A real-time testbed environment for cyber-physical security on the power grid," in Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and Privacy, ACM. ACM Press, 2015, pp. 67–78.

[11] J. Jarmakiewicz, K. Maślanka, and K. Parobczak, "Development of cyber security testbed for critical infrastructure," in 2015 International Conference on Military Communications and Information Systems (ICMCIS). IEEE, May 2015, pp. 1–10.

[12] J. Hong et al., "Cyber-physical security test bed: A platform for enabling collaborative cyber defense methods," 2015. [Online]. Available: http://taocui.info/docs/TestBed.pdf

[13] W. Deng, W. Pei, Z. Shen, and Z. Zhao, "IEC 61850 based testbed for micro-grid operation, control and protection," in 2015 5th International Conference on Electric Utility Deregulation and Restructuring and Power Technologies (DRPT). IEEE, Nov. 2015, pp. 2154–2159.

[14] B. Chen, K. L. Butler-Purry, A. Goulart, and D. Kundur, "Implementing a real-time cyber-physical system test bed in RTDS and OPNET," in North American Power Symposium (NAPS), 2014. IEEE, Sep. 2014, pp. 1–6.

[15] M. A. H. Sadi, M. H. Ali, D. Dasgupta, and R. K. Abercrombie, "OPNET/simulink based testbed for disturbance detection in the smart grid," in Proceedings of the 10th Annual Cyber and Information Security Research Conference, ACM. ACM Press, 2015, pp. 1–4.

[16] D. Bian, M. Kuzlu, M. Pipattanasomporn, S. Rahman, and Y. Wu, "Real-time co-simulation platform using OPAL-RT and OPNET for analyzing smart grid performance," in 2015 IEEE Power Energy Society General Meeting. IEEE, July 2015, pp. 1–5.

[17] J. Nivethan, M. Papa, and P. Hawrylak, "Modeling and simulation of electric power substation employing an IEC 61850 network," in Proceedings of the 9th Annual Cyber and Information Security Research Conference, ser. CISR '14, ACM. ACM Press, 2014, pp. 89–92.

[18] A. Razaq, B. Pranggono, H. Tianfield, and H. Yue, "Simulating smart grid: Co-simulation of power and communication network," in Power Engineering Conference (UPEC), 2015 50th International Universities. IEEE, Sep. 2015, pp. 1–6.

[19] K. Mets, J. A. Ojea, and C. Develder, "Combining power and communication network simulation for cost-effective smart grid analysis," IEEE Communications Surveys & Tutorials, vol. 16, no. 3, 2014, pp. 1771–1796.

[20] IEC 61850-5:2003, "Communication networks and systems in substations - part 5: Communication requirements for functions and device models," first Edition. [Online]. Available: https://webstore.iec.ch/publication/20075

[21] IEC 61850-7-3:2003, "Communication networks and systems in substations - part 7-3: Basic communication structure for substation and feeder equipment - common data classes," first Edition. [Online]. Available: https://webstore.iec.ch/publication/20075

[22] IEC 61850-7-2:2003, "Communication networks and systems in substations - part 7-2: Basic information and communication structure - abstract communication service interface (ACSI)," first Edition. [Online]. Available: https://webstore.iec.ch/publication/20075

[23] IEC 61850-8-1:2004, "Communication networks and systems in substations - part 8-1: Specific communication service mapping (SCSM) - mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3," first Edition. [Online]. Available: https://webstore.iec.ch/publication/20075

[24] IEC 61850-9-2:2004, "Communication networks and systems in substations - part 9-2: Specific communication service mapping (SCSM) - sampled values over ISO/IEC 8802-3," first Edition. [Online]. Available: https://webstore.iec.ch/publication/20075

[25] IEC TS 62351-1:2007, "Power systems management and associated information exchange - data and communications security - part 1: Communication network and system security - introduction to security issues." [Online]. Available: https://webstore.iec.ch/publication/6903

[26] R. Schlegel, S. Obermeier, and J. Schneider, "Assessing the security of iec 62351," in Proceedings of the 3rd International Symposium for ICS & SCADA Cyber Security Research, ser. ICS-CSR '15. Swinton, UK, UK: British Computer Society, 2015, pp. 11–19.

[27] Michael Zillgith. libIEC61850 | open source library for IEC 61850. [Online]. Available: http://www.libiec61850.com/libiec61850/ (2016)

[28] Stefan Feuerhahn, Marco Mittelsdorf, Dirk Zimmermann, Albrecht Schall, Philipp Fels. OpenIEC61850 | open source library for IEC 61850. [Online]. Available: https://www.openmuc.org/index.php?id=35

[29] SIEMENS. PSS®E - Power Transmission System Planning Software. [Online]. Available: http://w3.siemens.com/smartgrid/global/en/products-systems-solutions/software-solutions/planning-data-management-software/planning-simulation/Pages/PSS-E.aspx (2016)

[30] RTDS Technologies. RTDS - Real Time Digital Simulation. [Online]. Available: https://www.rtds.com (2016)

[31] OPAL-RT Technologies. OPAL-RT - PC/FPGA Based Real-Time Digital Simulators. [Online]. Available: http://www.opal-rt.com (2016)

[32] S. Siraj, A. Gupta, and R. Badgujar, "Network simulation tools survey," International Journal of Advanced Research in Computer and Communication Engineering, vol. 1, no. 4, 2012, pp. 199–206.

 ISBN: 978-1-61208-512-8