Cyber-Physical Security Testbed for Substations in a Power Grid

Junho Hong, Ying Chen, Chen-Ching Liu, and Manimaran Govindarasu

Abstract. The physical system of the power grids relies on the cyber system for monitoring, control, and operation. As a result, the reliable operation of power grids is highly dependent on the associated cyber infrastructures. The integrated cyber and physical system of power grids creates a large and complex infrastructure. Due to the high penetration of Information and Communications Technology (ICT), Supervisory Control And Data Acquisition (SCADA) systems are highly interconnected with one another, resulting in higher vulnerability with respect to cyber intrusions. Recent reports indicate that cyber-attacks are increasingly likely for the critical infrastructures, e.g., control centers, nuclear power plants, and substations. These attacks may cause significant damages on the power grid. Cyber security research for the power grid is a high priority subject for the emerging smart grid environment.

Substations in the power grid are critical as they are installed with power system components such as transformers, busbars, circuit breakers, and Intelligent Electronic Devices (IEDs). Measurements from substations are used as input to Energy Management System (EMS) software applications, including state estimation and optimal power flow. These cyber and physical devices can be physically or electrically connected. For example, a protection and control unit of a transformer is connected to the user-interface via the substation local area network.

Junho Hong
ABB US Corporate Research Center, Raleigh, NC, USA

Junho Hong · Ying Chen · Chen-Ching Liu
Washington State University, Pullman, WA, USA

Chen-Ching Liu
University College Dublin, Dublin, Ireland

Ying Chen
Tsinghua University, Beijing, China

Manimaran Govindarasu
Iowa State University, Ames, IA, USA

S.K. Khaitan, J.D. McCalley, and C.-C. Liu (eds.), *Cyber Physical Systems Approach to Smart Electric Power Grid*, Power Systems, DOI: 10.1007/978-3-662-45928-7_10

Remote access to substation networks is a common way for maintenance of substation facilities. However, there are many potential cyber security issues including remote access connection. Simultaneous cyber intrusions to important substations may trigger multiple, cascaded sequences of events, leading to a blackout. As a result, it is crucial to enhance the cyber security of substations and analyze cyber and physical security as one integrated structure in order to enhance the resilience of power grids. The mitigation strategy is vital to cyber-physical security of substations in order to stop the attack, disconnect the intruder, and restore the power system to a normal state. Mitigation methods can be taken on the cyber (ICT) side and physical (power system) side. The key to cyber mitigation is to find anomaly activities or malicious behaviors, and disconnect or stop the intrusion.

A cyber-physical testbed is critical for the study of cyber-physical security of power systems. For reason of security by power companies, real measurements (e.g., voltages, currents and binary status) and ICT data (e.g., communication protocols, system logs, and security logs) are not available. A testbed is a good alternative to acquire realistic cyber (i.e., ICT data) and physical (i.e., power system measurements) system data for research and demonstration purposes. The cyber-physical testbed provides a realistic environment to study the interactions between a complex power system and the ICT system. It is important to study the cause-effect relationships of cyber intrusions, vulnerability and resilience of power systems, as well as the performance and reliability of applications in a realistic environment provided by a testbed.

1 Introduction to Cyber and Physical System in a Power Grid

Power grids are complex cyber and physical systems [1]. The physical system of power grids includes power plants, substations, and transmission and distribution systems [2]. Electric power is produced by generators, while substations convert Alternating Current (AC) voltage from a voltage level to another for delivery from power plants to the load. Transmission systems deliver electric power to distribution substations through transmission networks. Distribution systems deliver electric energy to customers. The physical system of power grids relies on the cyber system for monitoring, control, and operation. The cyber system of power grids is formed by the Information and Communications Technology at the substations and the SCADA system at the control center [3]. The SCADA system supports the EMS that includes a number of power system software applications. Measurements (e.g., current and voltage) from Current Transformers (CTs) and Voltage Transformers (VTs) at the substations are delivered to control centers through ICT networks, e.g., TCP/IP based wide area networks. Control commands, such as opening of a Circuit Breaker (CB), can be sent from the SCADA system at a control center to the Remote Terminal Units (RTUs) or gateways in the substations. The integrated cyber and physical systems of power grids create a large and complex infrastructure.

SCADA systems have evolved from independent systems to networked-systems [4]. The first SCADA systems were isolated from other systems. As the requirements for data points are increased, more ICT networks are implemented in the substations and SCADA systems. Due to the high penetration of ICT systems, modern SCADA systems are highly interconnected with one another and, as a result, become more vulnerable than before with respect to cyber intrusions. Unsecured web servers in the user-interfaces, default passwords of IEDs and mis-configured firewalls are among the potential cyber vulnerabilities [5].

Substations in the power grid are critical since it has power system components such as transformers, bus bars, circuit breakers and IEDs, and the measurements from substations are used for input to EMS applications, e.g., state estimation and optimal power flow. The traditional power grid is designed based on the N-1 security criterion[1] [6]. However, a well coordinated cyber attack may compromise multiple substations. Therefore, simultaneous cyber intrusions to important substations may trigger multiple, cascaded sequences of events, leading to a power grid blackout. As a result, it is crucial to enhance the cyber security of substations and analyze cyber and physical security as one integrated structure in order to enhance resilience of power grids.

Cyber security concerns and potential threats to the power infrastructures have been reported by governments and other organizations, e.g., General Accounting Office (GAO), National Institute of Standards and Technology (NIST) or NISTIR (NIST Internal Reports) and Department of Energy (DOE) [7, 8, 9]. North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) published reliability standards 002-009 that covers the security of critical cyber assets, physical and cyber security, electronic security perimeters as well as personnel training and security management [10].

There are different cyber-physical systems in a smart grid, e.g., substation automation system, distribution automation system, advanced metering infrastructure, and electricity market. Moreover, many other critical infra structures, e.g., transport, health, water, gas, are critically dependent on ICT systems. Due to the vulnerability of these critical systems, a successful cyber intrusion may cause serious damages to the cyber system or physical components.

This chapter is concerned with cyber security of substations. A real-time cyber-physical security testbed is proposed for simulation of potential cyber intrusions and validation of cyber and physical mitigation methods. In the remaining of this chapter, Section III provides the concepts and design of the cyber-physical system. Section IV describes the IEC 61850 standard and multicast messages in a substation automation system. In Section V, vulnerabilities and hypothesized intrusion and mitigation scenarios of substation automation systems are explained. Section

[1] The power system has to be designed to absorb a loss of one or more system elements that occurs first, e.g., loss of a single generator or a transmission line. However, the expression "-1" may refer the failure of multiple elements since there could be physically or electrically linked elements as one, e.g., multiple feeders that are connected to one transformer.

VI provides architectures and components of the proposed cyber-physical security testbed and mitigation strategies. Simulation results involving cyber attacks and intrusion detection in the testbed environment are reported.

2 Cyber-Physical System Testbeds

By gradual deployment of advanced information and power technologies, the power system is in transition to a smart grid. This important transition creates the need for Research and Development (R&D) on the enabling technologies, such as integrated communication, advanced metering infrastructure (AMI), demand response, distribution automation and integration of large scale renewable devices. However, recent reports indicate that cyber attacks are increasingly likely for the critical infrastructures (e.g., control centers, nuclear power plants, and substations). Therefore, cyber security research for the power grid is an important priority for the emerging smart grid [11]. The work of [52, 53] show the survey of cyber-physical security research of power grid for researchers and system operators.

Advanced communication technologies and integration of a large number of Phasor Measurement Units (PMUs) enable the reliable and dependable Wide-Area Monitoring, Protection and Control (WAMPAC) system of the power grids. This system has the potential to analyze the power system condition, predict problems that may arise, and prevent worsening system conditions. The Automatic Generation Control (AGC) and Automatic Voltage Regulator (AVR) are representative applications that use the WAMPAC system. For instance, AVR uses measurements from substation RTUs periodically (e.g., 10 seconds or 2 minutes). It also sends control commands from the control center to the substation RTUs in order to increase or decrease the reactive power output of the generators, turn on/off switches of the capacitor banks, and change the positions of On-Load Tap Changers (OLTCs). The information is managed by the application in EMS. However, the performance of WAMPAC depends on the ICT networks. It also generates a lot of measurements and control messages to the ICT network (Specially, PMUs accumulate large amounts of data into the wide-area communication network between substations and control centers). All measurements and controls are transferred, stored and managed by the same ICT system in order to reduce the operation and implementation costs. As a result, there are potential threats and cyber security concerns for the EMS applications that are supported by ICT systems. These problems can be analyzed by the cyber-physical security testbed.

The cyber attack and defense studies cannot be conducted on the real systems due to the potential risk of service disruption. Furthermore, communication data in a substation and a control center may not be available for the cyber security research. As a result a realistic testbed is the best alternative for study of cyber security for power systems. The conventional power system simulation software or hardware tools do not incorporate the ICT systems (e.g., communication protocols and SCADA). Similarly, communication simulation tools do not support power system simulations (e.g., power system stability analysis and optimal power flow).

In order to analyze the cause- effect scenarios of the cyber and physical system (e.g., what is the consequence and impact to a power grid upon a successful cyber attack to a substation), integration of the cyber and physical system is needed. Therefore, a cyber-physical testbed is required for study of cyber-physical security of power systems. This testbed can be used for complex power system analysis with ICT systems and also provide a methodology to study the interaction between a power system and the ICT system that cannot be performed by a traditional power system testbed [11].

Several testbeds for cyber-physical security of power systems have been developed by a number of institutions. Idaho National Laboratory (INL) developed a National SCADA Testbed (NSTB) that can be used to identify and mitigate existing vulnerabilities [12, 13, 14]. The Virtual Control System Environment (VCSE) is developed by Sandia National Laboratory (SNL) that can be used to model and simulate cyber-physical system security [15], [16]. Iowa State University established the PowerCyber testbed using Real Time Digital Simulators (RTDS), and ISEAGE WAN emulation [1]. The Virtual Power System Testbed (VPST) was developed by the University of Illinois with the PowerWorld power system simulator and a Real-Time Immersive Network Simulation Environment (RINSE) [17]. The work of [18] proposes anomaly-based intrusion detection on the SCADA Control Systems (TASSCS) at the University of Arizona. The CRUTIAL testbeds are proposed to analyze the ICT resilience of power control systems in Europe [19], [20]. The testbed at the University College Dublin (UCD) has the capability to simulate cyber attacks and its impact on the power grids. This testbed is based on the commercial EMS and DIgSILENT power system simulator [21]. Royal Melbourne Institute of Technology (RMIT) developed the SCADASim testbed for testing of different attack and security solutions on actual devices and applications using a simulated environment [22].

In Sections 3.1, the common architecture and research applications of cyber-physical power system testbeds will be presented. Then the common design of a Cyber-Physical Substation Testbed (CPST) will be introduced in Section 3.2.

2.1 Common Framework and Applications of the Cyber-Physical Testbeds

As described in the last Section, there are various types of cyber-physical testbeds. Although the components and configurations of the testbeds are different, they do share some similarity. The figures 1 ~ 4 will explain the common modeling and simulation platforms of the cyber-physical testbeds and their applications.

The integrated system is composed of cyber (ICT systems) and physical (power system elements) systems as shown in Fig. 1. The cyber-physical system can be divided into three parts, i.e., control center with EMS and SCADA system, substations with critical devices (e.g., transformers, buses, generators, feeders, capacitors) and ICT systems that link them.

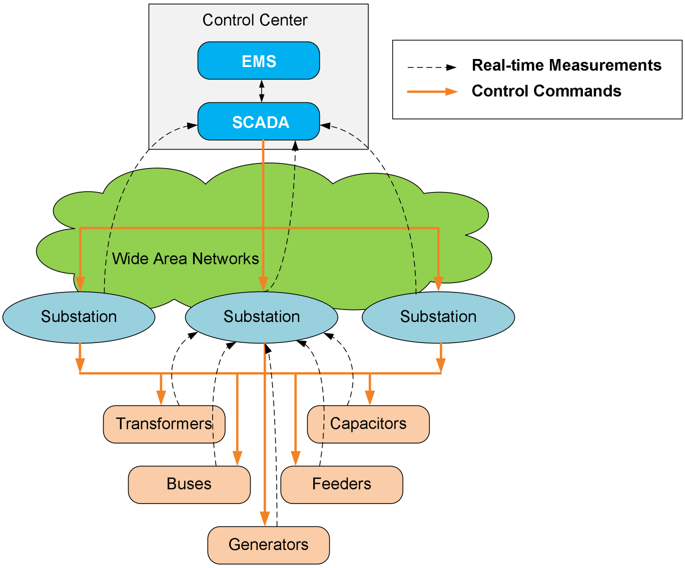


Fig. 1 General structure of the integrated system

The power flow snapshots can be obtained in two ways, i.e., acquired raw data and results from the state estimation software. Generally, the power flow snapshot from the raw data provides enough information to dispatchers to enable basic operations, e.g., monitoring and emergency warning. However, if dispatchers need to determine the controls for reconfiguring the power system, they need to use a credible power flow snapshot from the state estimation. The optimal or contingency dispatch strategies are generated by EMS in order to optimize the operation of the power system or prevent outages that are caused by power system faults and disturbances. These actions are performed by predefined algorithms or experienced dispatchers. Control commands are sent to the gateways or RTUs in the substations to operate the appropriate devices.

To enhance the robustness of a power system, double layered control systems are proposed as shown in Fig. 2. Remote controls are used to enhance the efficiency and stability of the power system whereas local controls are designed to maintain the integrity of the devices and reliability of the power system. Some local controls, e.g., excitation and governor controls for the generators, are responsible for enhancing the steady and dynamic stability of the power system.

Fig. 3 is an illustration of a typical structure of the cyber-physical testbed. Each module represents a simulation software package, hardware device or routine program. The functional modules include four features, i.e., the physical system, ICT, cyber system and system management module.

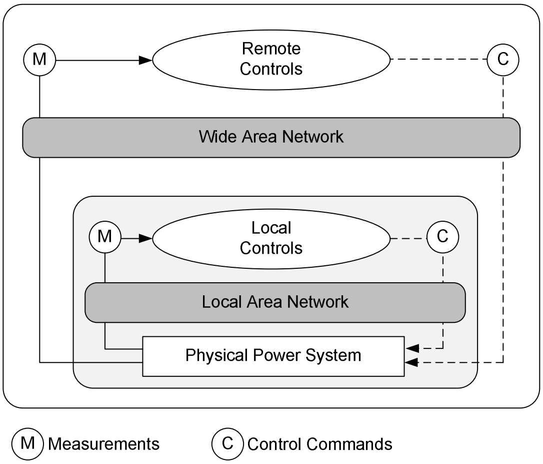


Fig. 2 Double layered controls within cyber-physical system

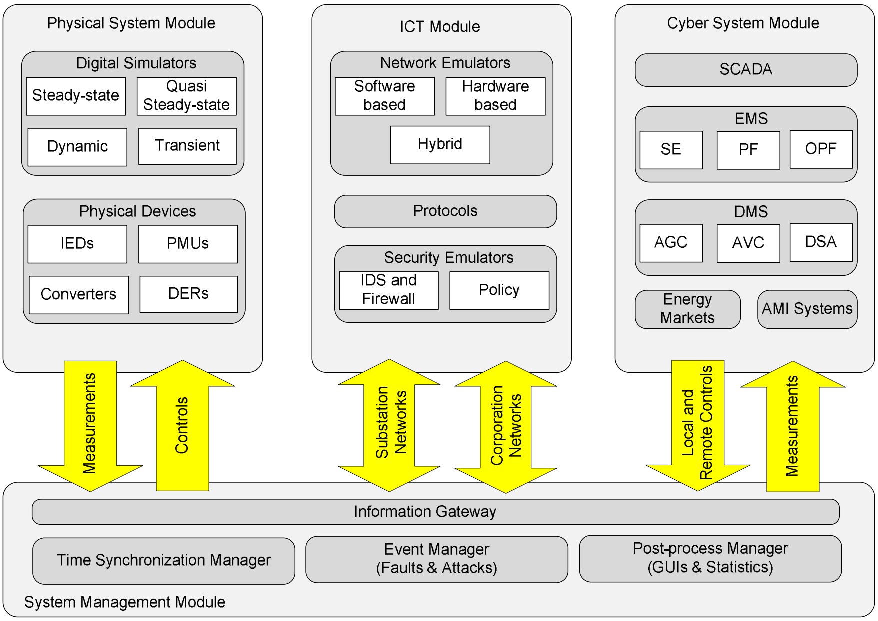


Fig. 3 Typical structure of the cyber-physical testbed

Each module's functions and interfaces are described in the following:

Physical System Module: This module is to simulate the complex power system behaviors accurately and efficiently. The cyber-physical testbed needs to have the capability to simulate various power system operating conditions, e.g., steady state, quasi-steady state (i.e., time series analysis based successive power flow), dynamic and transient simulations with small or large-scale power system models as shown in Fig. 3. Thus, it provides various measurements such as active and reactive powers, currents and voltages as well as binary status of switches and lines before/after control actions to other modules. The transient simulation produces detailed dynamics of power systems within microseconds. However, it is not feasible to represent the entire power system due to the modeling complexity and heavy computational burden. It is important to determine the tradeoffs between different levels of modeling and simulation methods.

In general, the hardware-in-loop refers to hybrid simulations that combine hardware devices and digital simulators. Hardware devices (e.g., IEDs, PMU and converters) need input data from the digital simulators to process its own algorithms. Digital simulators have to finish all calculations within a data sampling period. For instance, if PMU required 30 data samples every second, the digital simulator has to calculate the input data within 0.033 [mesc] and send it to the PMU. Otherwise, this cyber-physical testbed will lose the accuracy of the simulation result. Time synchronization between hardware devices and digital simulators can be done by implementation of time tags, e.g., creating time tags for measurements and controls.

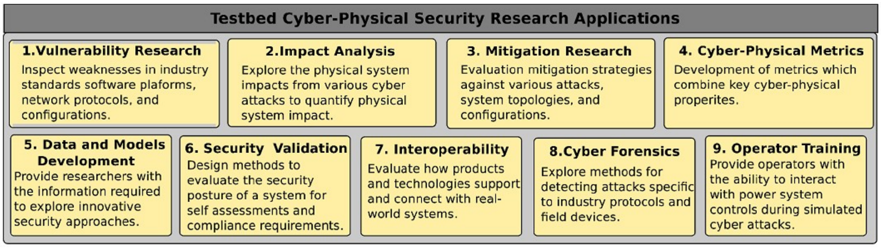
ICT Module: There are three sub-modules in the ICT module, i.e., network emulator, communication protocols, and security emulator that can be used to simulate local and wide area controls in power systems. In order to connect the cyber and physical system modules, the network emulator is used to evaluate the performance, stability, or functionality of communication networks. The network emulator can be computer software that performs a communication network simulation, a hardware based device or hybrid simulator that includes both of them. There are some benefits for using network emulators compared to hardware based devices. For instance, network emulators are smaller, cheaper and more flexible than the hardware options; they can provide more detailed information (e.g., packet delays, losses, network errors and latency). There are many industrial communication protocols, such as Modbus, Distributed Network Protocol (DNP), International Electrotechnical Commission (IEC) 60870-5 and IEC 61850 based protocols, in the power grids. They may not be suited for evaluation of cyber related intrusions since they do not adopt up to date security measures. False data injection attacks may lead to wrong control or protection actions. Large scale denial of service attacks may cause disruptions to the communication networks. Potential cyber threats, attack models and its mitigations have to be studied using a proper cyber-physical testbed. Security emulators can be used to detect network anomalies and malicious behaviors with predefined rules or algorithms. The Intrusion Detection System (IDS) and firewall are representative security devices in the ICT systems. The Intrusion Prevention System (IPS) can disconnect or stop the intruders whereas a passive IDS will trigger an alarm to the operators. The ICT module has two interfaces, substation and corporate networks. The time synchronized measurements are sent from the physical system module to the cyber system module whereas time synchronized controls come from the cyber system module to the physical system module through the ICT module, as depicted in Fig. 3.

Cyber System Module: This module includes software, applications and systems that are developed for a study of the management, operation, and control of power systems in the cyber-physical testbed, e.g., EMS, Distribution Management System (DMS), AMI and energy markets. A solution to enable the cyber system module is to deploy commercial products from industry vendors. In fact, most of existing cyber-physical power system testbeds follow this approach since the commercial products provide both simplified ICT networks integration and a general level of system-in-the-loop tests. On the other hand, the cost of this solution is a barrier. In addition, it is hard to implement customized or developed algorithms into the commercial products since vendors may not allow users to access or modify their source code. Open source code based emulators can be customized and incorporated into existing platforms. They are suitable for cyber-physical security research where it is desirable to evaluate security algorithms or applications against cyber intrusions or threats. Examples include the impact of cyber attacks on the secured state estimation, security enhanced automatic generation controls and automatic voltage regulations, and analysis of resilience of power systems against cyber attacks. The measurements and controls have to be synchronized by the time synchronization manager as shown in Fig. 3.

System Management Module: This module is in charge of the overall operation of cyber-physical power system testbeds. The responsibilities include maintaining time synchronization between modules, managing all events and attacks that are generated from external sources, and analyzing/visualizing the test steps and results on the Graphic User Interfaces (GUIs). An important part in building the cyber-physical testbed is to balance between the physical power grid module and communication network and cyber system module. The physical power grid module produces continuous dynamic data (i.e., measurements), whereas the communication network and cyber system module generates discrete dynamic data (i.e., controls). The information gateway can create, add, delete and query all exchanged data in the system by the key-value mapping scheme. As all data and information that are generated from four modules (e.g., the physical system module, ICT module, cyber system module, and system management module) are exchanged at the information gateway, time synchronization becomes the only feature that determines the consistency of these interactions. Therefore, significant effort has been made by researchers to design and model the proper time synchronization mechanism and function modules in order to build a cyber-physical testbed. There are three types of synchronization mechanisms that can serve to provide the backbone time line for data exchange such as Global Positioning System (GPS) signal for real-time simulation, virtual-time stamp for off-line simulation or hybrid simulation that includes both of them. If the power system simulation tool (physical system module) calculates the power flow and sends measurements to the state estimation (cyber system module), this system can be synchronized by a combination of real-time and virtual-time mechanisms after ignoring the power flow calculation time at the power system simulation tool. Recently, the Functional Mock-up Interface (FMI) protocol standard has been proposed by the FMI research group. This independent standard is a tool to support both model exchange and co-simulation of dynamic models using a combination of xml-files and compiled C code. Moreover, it can reduce the system configuration times and efforts by offering the synchronized Function Mock-up Unit (FMU) that contains descriptions of interface data and functionalities [23].

The cyber-physical testbeds generate a large amount of data so it is important to manage and analyze all information and results by the post-process manager, as shown in Fig. 3. GUI can manage the global inputs and outputs of the testbed, configuration of physical, and ICT and cyber system modules. It can also be used for the external events due to cyber attacks, abnormal weather conditions, intensive fluctuation of loads and physical device failures. If there is an uncertain event, the statistical application will calculate the probability distributions to be used for stochastic analysis. Data mining techniques are used to perform the multi-round tests with different parameters and scenarios.

A cyber-physical testbed consists of various types of components such as software, hardware, ICT networks, emulators, and communication protocols. As shown in Fig. 4, the research of [1] identifies various applications of cyber-physical security testbed for power grids. The cyber-physical testbed is beneficial as a realistic platform for modeling and simulation of the power system and ICT applications, as well as the attack and defense strategies.



Testbed Cyber-Physical Security Research Applications

1.Vulnerability Research
Inspect weaknesses in industry standards software plaforms, network protocols, and configurations.

2.Impact Analysis
Explore the physical system impacts from various cyber attacks to quantify physical system impact.

3. Mitigation Research
Evaluation mitigation strategies against various attacks, system topologies, and configurations.

4. Cyber-Physical Metrics
Development of metrics which combine key cyber-physical properites.

5. Data and Models Development
Provide researchers with the information required to explore innovative security approaches.

6. Security Validation
Design methods to evaluate the security posture of a system for self assessments and compliance requirements.

7. Interoperability
Evaluate how products and technologies support and connect with real-world systems.

8.Cyber Forensics
Explore methods for detecting attacks specific to industry protocols and field devices.

9. Operator Training
Provide operators with the ability to interact with power system controls during simulated cyber attacks.

Fig. 4 Testbed applications [1]

2.2 Design of the Off-line Cyber-Physical Testbed

This section provides details of cyber-security testbed with examples of the actual implementation, e.g., off-line testbed. The off-line testbed has been used for the cyber security of AVR applications between substations and control centers. In the off-time testbed, all components are synchronized with a virtual-time stamp. The proposed off-line testbed requires more time and effort compared to the real-time testbed since this testbed does not use commercial products. It uses only freely available software. The ability of this testbed is limited since it can only perform the off-line based simulations and tests. However, it can produce reliable results and the implementation cost is low. The figures 5 ~ 9 will explain the framework and architecture of the off-time testbed for cyber security of the substations.

As shown in the Fig. 5, the testbed consists of open-source software packages and interfaces for physical, ICT, and cyber modules. Since this testbed adopted off-line testbed with the virtual time stamp, it can simulate large-scale power grids and ICT systems for the cyber-physical security research.

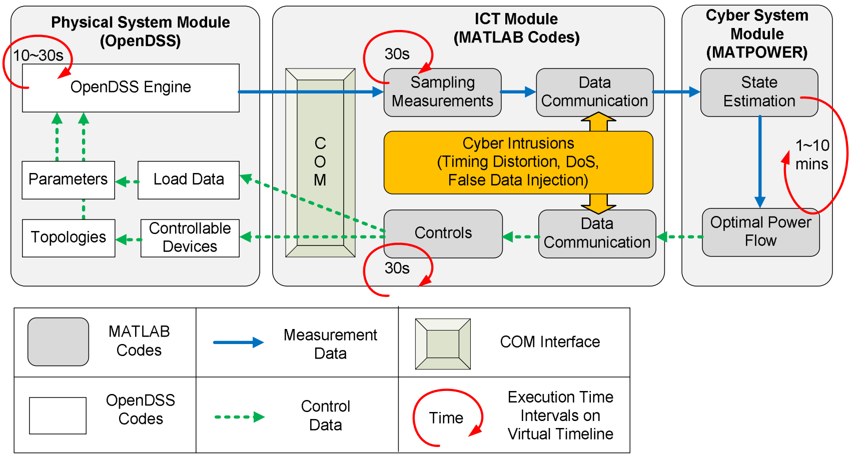


Fig. 5 Application flow of the off-line testbed

Physical System Module: Wide area control applications in SCADA systems can significantly affect the dynamics of a power system. Therefore, this testbed uses the OpenDSS[2] simulation tool to model the physical power systems. The OpenDSS (The Open Distribution System Simulator) is a toolbox for power system simulation, especially for the simulation of distribution networks with

[2] The OpenDSS is a comprehensive electrical power system simulation tool primarily for electric utility power distribution systems. It supports nearly all frequency domain (sinusoidal steady-state) analyses commonly performed on electric utility power distribution systems [24].

DER integrations. The functions of the OpenDSS include power flow, successive power flow with controls and load variations, common multi-phase circuit analysis, distributed generator analysis, harmonic analysis, and solar energy analysis. In this testbed, the OpenDSS is used as a simulation engine to generate quasi-steady dynamics of the power system. As shown in Fig. 6, the time series of system states are obtained by successive power flow calculations with inputs of the controls and load variations, where T is the current time, T_{end} is the end of simulation time, and Δt is the time difference between the previous and the current power flow.

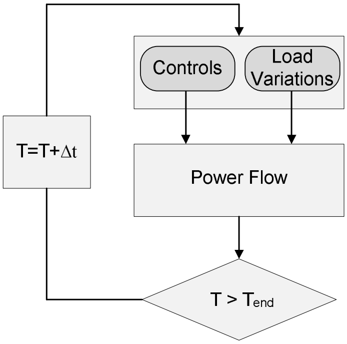
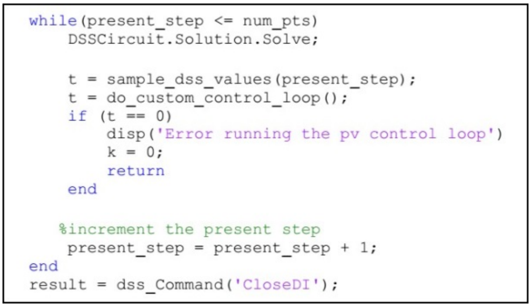


Fig. 6 Successive power flows

For the integration between the power system simulation engine and external modules, the Component Object Model (COM) interface is used, which is a built-in feature of OpenDSS and can be executed by MATLAB and Python languages. Through the COM interface, MATLAB can access the power flow results and adjust the parameters of the OpenDSS data (e.g., load data and status of devices). Fig.7 shows an example of the MATALB source code that controls the time-based simulation in OpenDSS. Therefore, MATLAB is acting as the wide area ICT module that connects the cyber system and physical system modules.



```
while(present_step <= num_pts)
    DSSCircuit.Solution.Solve;

    t = sample_dss_values(present_step);
    t = do_custom_control_loop();
    if (t == 0)
        disp('Error running the pv control loop')
        k = 0;
        return
    end

   %increment the present step
    present_step = present_step + 1;
end
result = dss_Command('CloseDI');
```

Fig. 7 Pseudo codes for the time-based simulation in Matlab

ICT and Cyber System Module: MATLAB is used for the ICT module. For the cyber system module, Matpower[3] has been used to simulate the EMS applications, including optimal power flow and state estimation. There are six steps for the ICT and cyber system module, e.g., sampling measurements, data communications, state estimation, optimal power flow, controls and cyber intrusions, as shown in Fig. 5. First, every 30 seconds, the function of measurement sampling has the responsibility to obtain all required measurements from the OpenDSS engine, such as the three phase voltages of all buses, power injections on each side of branches and transformers, and outputs of the generators. Measurements are tagged with time stamps, and they will be stored at the measurement data pool (i.e., database). Then, the data communication function will transfer time synchronized measurements to the state estimation function in the cyber system module. During this process, the network latency will be tagged to each time stamp according to the predefined configurations of communication channels. Also, the state estimation function imports the latest measurements from the data pool to produce the power flow snapshot. For every predefined time interval, if there is any limitation violation, the optimal power flow function will be executed using the data from state estimation. The optimal power flow results provide the necessary control commands, which are tagged with time stamps to controllable devices. Finally, the data communication function will transfer all controls from the optimal power flow function to the control function. Again, all control commands will be handled by the data communication function, which will create time tags and network latency information and store them in the command data pool. The control function will check the commands from the optimal power flow function periodically. Once it receives a new command, the control function changes the status of the corresponding devices, which are modeled in the OpenDSS engine via the COM interfaces.

Cyber Intrusion Module: In order to study cyber-security of the power system with wide area control applications, the cyber intrusion module is modeled and implemented in the testbed. Although there are numerous possibilities of attacks on the cyber system, the impact of these cyber attacks is related to three important features such as function integrity, service availability, and information confidentiality. The consequences caused by the availability and integrity attacks on the ICT module are explored with proper models and simulations. Note that if the testbed has a simulation function of the power system market, it can also simulate information confidentiality attacks on electricity market prices.

[3] MATPOWER is a package of MATLAB M-files for solving power flow and optimal power flow problems. It is intended as a simulation tool for researchers and educators. MATPOWER is designed to give the best performance possible while keeping the code simple to understand and modify [25].

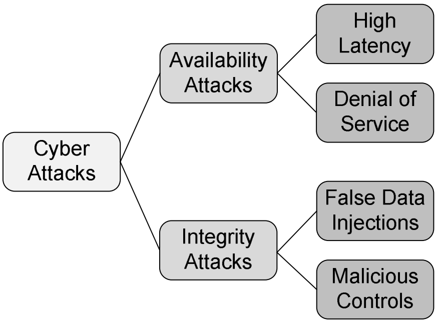


Fig. 8 Classification of cyber attacks

As shown in Fig. 8, wide area networks of a power system can be jammed by a large amount of data requests or injections as an attempt to reduce the availability of the cyber system. Moreover, if the ICT network links and communication protocols are compromised , the integrity of the wide area control systems can be damaged by injecting false data. Moreover, attackers may generate fabricated control messages to critical devices such as generators, transformers and breakers to create large scale outages. To model the cyber attacks, three dimensions are given, e.g., time, space, and style as illustrated in Fig. 9.

The execution time intervals for each function are shown in Fig. 5. They represent the operation period of each module. For example, the OpenDSS engine performs power flow calculations to generate measurements of the power system every 10 ~ 30 seconds. Since the proposed testbed is working in the off-line mode, the virtual timeline can be manipulated by adding, removing or adjust events. The operation periods of each module are important parameters for the study of wide area control cyber-security since it can influence the performance of EMS applications. Therefore, the off-line testbed is suitable for the parameter sensitivity analysis of the cyber-physical system security of power systems.

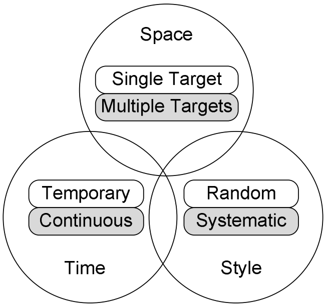


Fig. 9 Implementation strategies of cyber attacks

3 Substation Automation System

The concept and design of substation automation system was proposed by the IEC Technical Committee (TC) 57, Working Group (WG) 10. IEC TC 57 published IEC 61850 which is a standard for the design of substation automation system. The main purposes of IEC 61850 standard can be divided into four parts, (1) Lower configuration and installation cost, (2) Multi-vendor interoperability, (3) Long term stability, and (4) Minimal impact to the existing system.

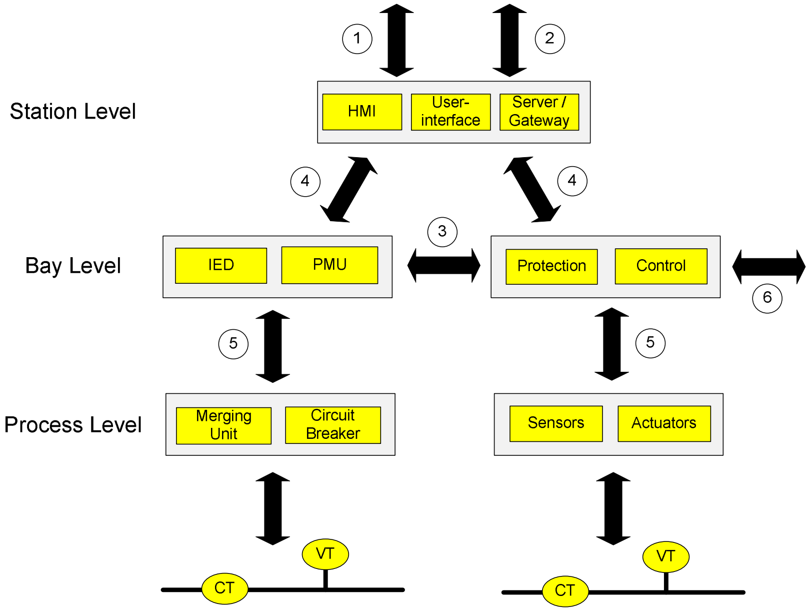


Fig. 10 Communication topology of the substation automation system (cyber system)

The installation and engineering cost of IEC 61850 based devices are drastically reduced since all hardwired connections from CTs and VTs to relays are changed to Ethernet based communications using Sampled Measured Value (SMV) messages which contain sampled data of currents and voltages. The Generic Object Oriented Substation Event (GOOSE) enables IEC 61850 based devices to quickly exchange critical data (e.g., a trip signal to a circuit breaker), i.e., less than 4 [msec], over the Ethernet based communication. This also significantly reduces the cost of wire installation. The Substation Configuration Language (SCL) contains device configuration information. Therefore, IEC 61850 based devices do not need any manual configurations; they import the configured SCL file through the ICT network. Standardized communication protocols and logical nodes enhance multi-vendor interoperability. Therefore, substation operators can use IEDs and user-interfaces from different vendors in a substation. The concept of IEC 61850 is extended to Distributed Energy Resources (DERs) and distribution automation. Hence, IEC 61850 enables devices from different manufacturers to exchange information in the substation level as well as system level [26]. The ICT technologies have been fast evolving over the last decade and the trend is continuing. However, the evolving cycle of power substation functions and software applications are slow compared to that of ICTs. The long term stability allows upgrading of ICT at a substation without re-engineering of the entire substation system. Since multi-vendor interoperability significantly reduced the gaps of device configuration between different vendors, substation engineers can add or remove existing devices at a lower cost. For instance, substation engineers can set up new devices and applications in a substation by sending SCL files via the ICT network [27].

Fig. 10 shows the three levels of the substation automation system, i.e., the station, bay, and process levels. The station level is where the user-interface, Human Machine Interface (HMI), substation server and gateway are located. The server and gateway exchange data coming from/to substation, e.g., remote access points (interface 1), control centers (interface 2) using DNP 3.0 or IEC 60870-5 [28]. The protective devices exchange critical data, e.g., interlocking (interface 3), between bays using GOOSE messages. Control and protection data are exchanged between the station and bay level using Manufacturing Message Specification (MMS) message (interface 4). Measurements such as currents and voltages are sent to the station level from the process level to bay level whereas control data are sent from the bay level to process level (interface 5) using SMV and GOOSE, respectively. Interface 6 shows the remote control and protection features between substations [29].

A substation includes various types of critical physical equipment, e.g., transformers, circuit breakers (52), bus bars, disconnect switches, and feeders, as shown in Fig. 11. The substation in Fig. 11 has two main transformers, and single busbars. When a fault occurs at a transformer or a busbar, the faulted area can be isolated by switching actions. The substation equipment will be protected by different types of protective relays. For instance, the transformer and busbar are protected by differential relays while the feeder is protected by overcurrent relays.

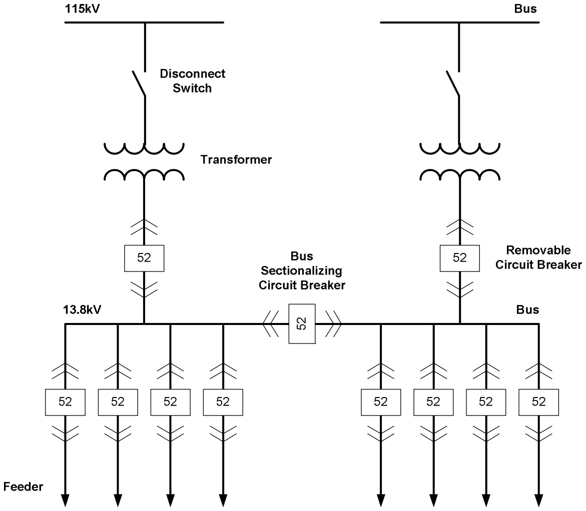


Fig. 11 The one line diagram of a substation (physical system) [30]

3.1 IEC 61850 Standard

The IEC 61850 is divided into 10 sections and 7 sub-sections as shown in Table I. Part 1 is an overview of the IEC 61850 standard series, basic interface and reference model of a substation automation system. Part 2 provides an explanation of the abbreviations and terms that are used in IEC 61850 series. Part 3 describes the general requirements of the ICT networks and guidelines for environmental conditions and recommendations. Part 4 is concerned with the system and project management with respect to the engineering process, life cycle of the overall system and supporting tools for engineering and testing. The scope of part 5 covers the communication requirements of the functions that are performed in the substation automation system. It also explains the Logical Nodes (LNs) for each function, e.g., PTOC is an AC time overcurrent relay that is able to trip the circuit breaker when the input current exceeds the predetermined threshold. The IED related configuration languages are shown in part 6, e.g., SCL, IED Capability Description (ICD), System Exchange Description (SED), Instantiated IED Description (IID), System Specification Description (SSD) and Configured IED Description (CID) that are based on the Extensible Markup Language (XML). Part 7 deals with the basic communication structure for substation and feeder equipment. Part 7-1 explains the principles of the modeling method, communication and information models that are used in IEC 61850-7-x. The definition and structure of Abstract Communication Service Interface (ACSI) communication in substations are introduced in part 7-2. Part 7-3 provides details of the layered substation communication architecture. The ICT models of functions and devices that are related to substation automation are described in part 7-4. Specially, this part of the standard includes details of logical node names and data names for communication between substation devices, e.g., IEDs and user-interfaces. Part 8-1 describes a method for data exchange between ACSI and MMS communication. Finally, part 9-1 and part 9-2 explain the structure and mapping of the SMV. Part 10 covers the subject of conformance testing for IEC 61850 systems.

Table 1 Sections of IEC 61850 standards

Section	Title
IEC 61850-1	Introduction and overview
IEC 61850-2	Glossary
IEC 61850-3	General requirements
IEC 61850-4	System and project management
IEC 61850-5	Communication requirements for functions and device models
IEC 61850-6	Configuration language for communication in electrical substations related to IEDs
IEC 61850-7	Basic communication structure for substation and feeder equipment
├ IEC 61850-7-1	├ Principles and models
├ IEC 61850-7-2	├ Abstract communication service interface (ACSI)
├ IEC 61850-7-3	├ Common Data Classes
└ IEC 61850-7-4	└ Compatible logical node classes and data classes
IEC 61850-8	Specific communication service mapping (SCSM)
└ IEC 61850-8-1	└ Mappings to MMS (ISO/IEC9506-1 and ISO/IEC 9506-2)
IEC 61850-9	Specific communication service mapping (SCSM)
├ IEC 61850-9-1	├ Sampled values over serial unidirectional multidrop point to point link
└ IEC 61850-9-2	└ Sampled values over ISO/IEC 8802-3
IEC 61850-10	Conformance testing

3.2 Multicast Messages in a Substation Automation System

The communication protocols in IEC 61850 can be classified into seven types. Due to the requirement of type 1, 1A and 4 messages, e.g., GOOSE and SV, they use three communication stacks, i.e., physical, data link and application layer as shown in Fig. 12. GOOSE supports critical data exchange such as interlocking between IEDs, trip messages from IED to circuit breakers or the status of circuit breakers to IED. The basic concept of information exchange is that a publisher writes values in a GOOSE packet and subscriber receives and reads the values from the GOOSE packet. GOOSE uses Media Access Control (MAC) address for the multicast[4] scheme. Due to the real-time requirement, GOOSE applies a re-transmission[5] scheme in order to achieve the appropriate level of communication speed and reliability. As shown in Fig. 10, the merging unit receives voltage and current values from CT and VT through the hard wire. Then the merging unit sends measured current and voltage values to protection IEDs using SMV messages. A merging unit can send SMV messages to multiple IEDs since SMV supports the multicast scheme. There are three types of resolution (bits) amplitude for SMV messages such as bits (P1 class), 16 bits (P2 class) and 32 bits (P3 class) [31].

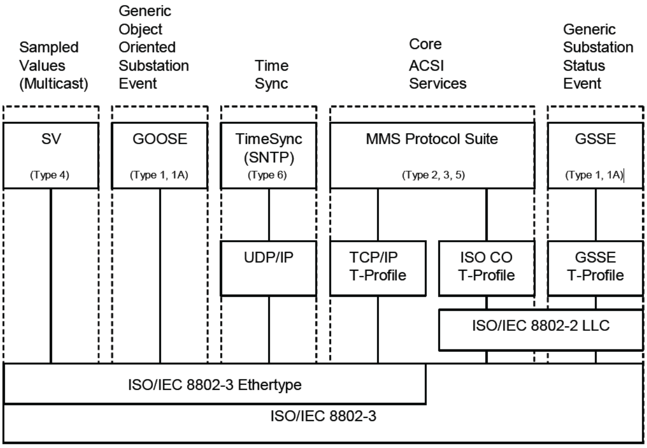


Fig. 12 Communication protocols in IEC 61850 [32]

- Type 1: Fast messages
- Type 1A: Trip
- Type 2: Medium speed messages
- Type 3: Low speed messages
- Type 4: Raw data messages
- Type 5: File transfer functions
- Type 6: Time synchronization messages

[4] Multicast is the delivery of data or information in a single host to multiple receivers simultaneously.

[5] The receiver does not send any response to the sender.

4 Vulnerability, Intrusion and Mitigation Scenarios of the Substations

The cyber security of substations has been recognized as a critical issue since it consists of various types of critical physical and cyber devices as explained in Section 3. They can be physically or electrically connected, e.g., a protection and control unit of a transformer is connected to user-interface via the substation local area network. The remote access to substation networks, e.g., IED or user-interface, is a common way for maintenance of the substation facilities. However, there are many potential cyber security issues, such as: (1) Well-trained intruder(s) compromise the remote access points for cyber attacks, (2) Standardized communication protocols allow intruders to analyze the substation communications, (3) Unencryptable multicast messages (e.g., GOOSE and SMV) due to the requirements, (4) Mis-configured firewalls, and (5) IEDs and user-interfaces with default passwords. .

4.1 Substation Vulnerabilities

4.1.1 Unsecured Industrial Protocols

Communication protocol is an important element for the operation of a power grid. The protocol must not be modified, fabricated or monitored except by system operators. Despite their importance, cyber security features are not included in most industrial protocols since cyber security was not a major concern when industrial communication protocols were published, e.g., DNP 3.0, IEC 61850, IEC 60870-5 and Inter-Control Centre Communication Protocol (ICCP). Therefore, IEC TC 57 WG 15 established the IEC 62351 standard. The primary objective is to develop standards for security of the communication protocols defined by IEC TC 57. The GOOSE and SMV messages contain critical information and use the multicast scheme as explained in Section 3. The multicast scheme has potential cyber vulnerabilities, e.g., group access control and group center trust. Most encryption schemes or other cyber security features that delay the transmission time are not applicable for these protocols since the performance requirement of GOOSE and SMV messages is within 4 [msec]. Therefore, IEC 62351 standard recommends an authentication scheme with a digital signature using Hash-based Message Authentication Code (HMAC) for GOOSE and SMV. However, the performance test to apply the authentication scheme to GOOSE and SMV is yet to be performed. The existing intrusion and anomaly detection systems do not normally support IEC 61850 based protocols since they are more focused on general cyber intrusions such as Distributed Denial of Service attack (DDoS). In order to mitigate the communication based cyber attacks to substation automation networks, the work of [33] proposed an Intrusion Detection System (IDS) for IEC 61850 based substation automation system. An intrusion detection system for serial communication based MODBUS and DNP3 in the substations is proposed in [34]. Reference [35] proposes a temporal anomaly detection method and [36] reports an integrated anomaly detection method for detecting malicious activities of IEC 61850 based multicast protocols (e.g., GOOSE and SMV) in the substation ICT network.

4.1.2 Remote Access Points

Power system components are located in wide-spread and remote sites. Remote access to substation networks using Virtual Private Network (VPN), dial-up or wireless is a common way to monitor and maintain the substation. The main problem of the remote access point is that remote access points may not be installed with adequate security features, e.g., poorly configured firewall, weak ID and password policy, bad key management for cryptography, and use of un-secured external memory (e.g., USB flash drive). Therefore, substation security managers have to consider the following actions in order to enhance the cyber security: (a) Check firewall policies and logs periodically to identify security breaches, (b) Change ID and password frequently and enhance the password policy (e.g., including numerical digits and special characters), (c) Enhance security of the key server against attacker(s), and (d) Provide security practice education for operators.

4.1.3 Default Password and Built-in Web Server

A typical substation may have a number of IEDs and it is difficult to manage the different passwords for each IED. Therefore, substation operators may use the default or same password for all IEDs. In addition, some IEDs and user interfaces have a built-in web server and hence it may be vulnerable to cyber intrusions, e.g., remote configuration change and control with default passwords. Substation security managers have to check the security and system logs of IEDs and user-interface to detect unauthorized access.

4.2 Hypothesized Intrusion Scenarios to Substations

Security threats to the substation automation system can be divided into two parts based on the physical and cyber assets. The physical assets are the hardware components, e.g., GPS (A4), IED (A5) and circuit breaker (A8), whereas cyber assets include physical and cyber resources, e.g., firewall (A2), communication network (A3) and software applications in the user-interface (A6), as illustrated in Fig. 13. Mitigation actions against security threats have to consider both physical and cyber intrusions. More details about the mitigation will be discussed in Section 5.

Security threats to substations can be inadvertent events as well as deliberate attacks. Inadvertent events include animal intrusions, equipment failures and natural disasters [37]. Animal intrusion is a major concern for substation operators [38]. A significant amount of research has been undertaken over the last decade concerning monitoring of the health condition for substation components.

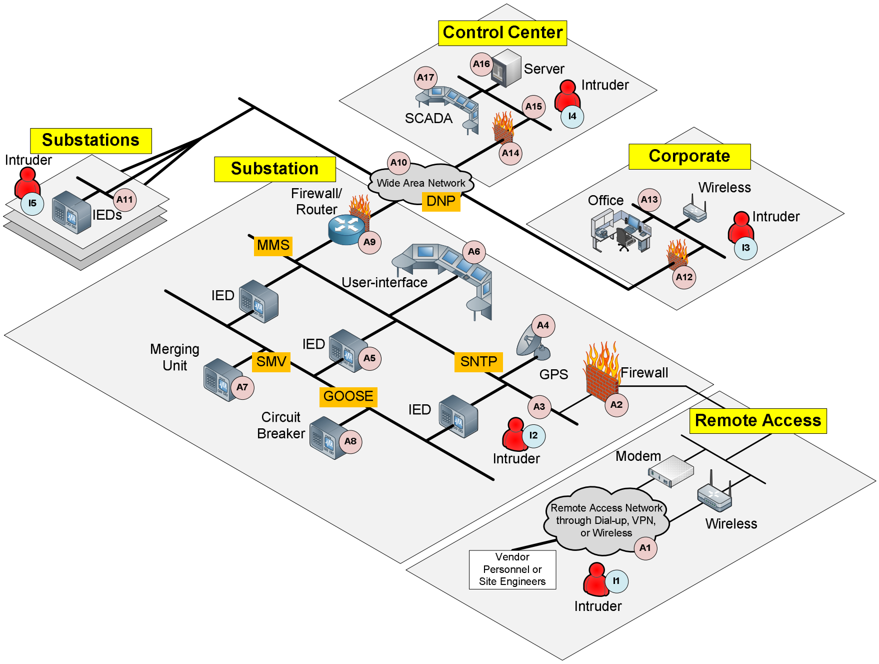


Fig. 13 Overview of substation ICT network diagram and security threats

Natural disasters such as flood, volcanic eruption, earthquake and tsunami, are rare but, in a severe scenario, can lead to cascading events and catastrophic outages. The work of [39] proposes weather-related power outages and enhancement of the system resiliency. Deliberate threats can be caused by disgruntled employees, cyber attackers, and malwares. Disgruntled employees can be threats for the substation security as they are familiar with the substation systems. The threats of cyber attacks are higher than before since substations need remote access connections for maintenance. *Stuxnet* is a relevant example of cyber threats (malwares) that are aimed at control systems of critical power infrastructure [40].

4.2.1 Single Substation Attack

As shown in Fig. 13, potential cyber security threats and locations of intruders in a substation automation network include:

A1: Compromise remote access points (e.g., dial-up, VPN and wireless)
A2/A9/A12/A14: Compromise firewall
A3: Gain access to substation network
A4: Interrupt GPS time synchronization
A5: Gain access to bay level devices or change protective device settings
A6: Gain access to user-interface
A7: Compromise process level devices (e.g., merging unit)

A8: Change the status of circuit breaker (e.g., close to open or vices versa)
A10: Gain access to wide area network (e.g., DNP 3.0)
A11: Gain access to neighbor substation network
A13: Gain access to corporate network
A15: Gain access to control center network
A16: Compromise the server in a control center
A17: Compromise the user-interface in a control center

I1: Intruder from outside of substation network via remote access points
I2: Intruder from inside of substation network
I3: Intruder from outside of substation network via corporate network
I4: Intruder from outside of substation network via control center network
I5: Intruder from outside of substation network via neighbor substation network

As depicted in Fig. 13, possible intrusions to the substation local area network can originate from outside or inside a substation network.

The following combinations represent the possible intrusion paths from outside to a local area network at a substation. Intrusions can originate from remote access points (A1) or neighbor substation network (A11) or corporate network (A13) or control center network (A15) all the way to the substation local area network (A3), e.g.,

from A1-A2-A3;
from A11-A10-A9-A3;
from A13-A12-A10-A9-A3;
from A15-A14-A10-A9-A3

Cyber attacks from inside the substation can originate from the substation network (A3) or user-interface (A6) then gain access to other facilities in the substation. An inside attack can be performed by social engineering [41]. One of the realistic examples of this attack is that intruder(s) send an email to substation operators that appears to come from a credible source. However, this email contains a fabricated website link or malware software so once operators open this email, their desktops or laptops will be infected. After that, this malware will infect the external flash drive that plugged into compromised devices. Finally, operator(s) may use the infected flash drive at the substation network to copy documentation. Then this malware will find a path to external communication, and send all information to intruder(s) or change the setting of the protection devices (e.g., IEDs).

It is crucial to protect the substation automation ICT network against cyber attacks as a successful cyber intrusion can cause significant damages on the power grid. Once an intruder can access the substation communication network, (s)he can access other facilities in the substation. For instance, the result of cyber attack, A4, may disrupt time synchronization of all communication protocols in the substation ICT network, and operators may lose the availability of substation communications. Upon successfully cracking an user name and a password and gaining an access to the user-interface (A6), the intruder may control or modify the settings of the IEDs (A5). Then they can operate circuit breakers through the connection of IEDs. Another possibility is to gain access to the ICT network of a neighbor substation, e.g., from A9-A10-A11, then multiple cyber attacks can be carried out. More details about simultaneous cyber attacks to the multiple substations will be discussed in Section 5.2.2.

4.2.2 Simultaneous Attacks to Multiple Substations

Each substation has a different level of importance in a power grid. Since generally, a high voltage substation carries more power. The level of cyber security is also different at each substation. For instance, substation A uses firewall, IDS and cryptography features for cyber security mitigation whereas substation B only uses firewalls. In this example, the security level of substation A is higher than substation B whereas the cost of security implementation at substation B is lower. By analyzing the security level of each substation and importance in a power grid, an intruder may find the optimal combination (considering cost-benefit model) of target substation(s) that can trigger a sequence of cascading events, leading to a system blackout. Therefore, the impact of simultaneous cyber attacks to multiple substations can be much higher than that of a single substation attack.

Table 2 Cost for cyber intrusion

Substation	Cyber security level	Physical importance	Cost for attack
1	Low	Medium	5
2	Medium	Medium	4
3	High	High	10
Successful attack combinations		(1, 2), (3), (1, 3), (2, 3), (1, 2, 3)	

For instance, there are 3 substations in the power system shown in Table II. If an attacker knows the cyber security level, physical importance, costs of an attack, and attack combinations that lead to a power system collapse, they may find the optimal attack combination. In this example, the lowest cost combination that can cause a collapse of the power system is (1, 2). Therefore, the attacker is likely to choose this combination to achieve the goal.

4.2.3 Attack Tree

In the field of computer science and information technology, attack trees have been used to analyze potential threats and attack paths against cyber attacks [42, 43, 44]. However, the concept of attack trees is broadened and applied to other systems, e.g., cyber security of power systems [45, 46]. Although there are numerous concepts and definitions of attack trees, the most commonly occurring concepts are nodes (root or leaf), edges, connectors and attributes [47]. Fig. 14 shows a simplified attack tree for the substation automation system. Root node (T1) is the ultimate goal (i.e., open circuit breakers) with combinations of leaf nodes (T3) that do not have any predecessor. Leaf nodes (T3) contain sub goals or steps to archive the final goal (T1). Edges (T2) are connectors for all nodes. There are two types of connectors (T4) in Fig. 14, "AND" and "OR." AND connector shows different steps (nodes) toward achieving the same goal. For instance, an intruder has to complete two steps, *Social Engineering* and *Compromise Operator Laptop*, in order to achieve *Obtain ID and Password*. Attributes represent features or properties relevant for numerical analysis of security models, e.g., attack probability and cost of an attack. Fig. 14 shows an example model of cost of an attack. If the first priority is to minimize the attack cost, the combination of (9)-(10)-(5)-(2) is the best way to achieve the final goal. However, if the priority of attack is to minimize attack steps, (4)-(1) is the best way to open circuit breakers.

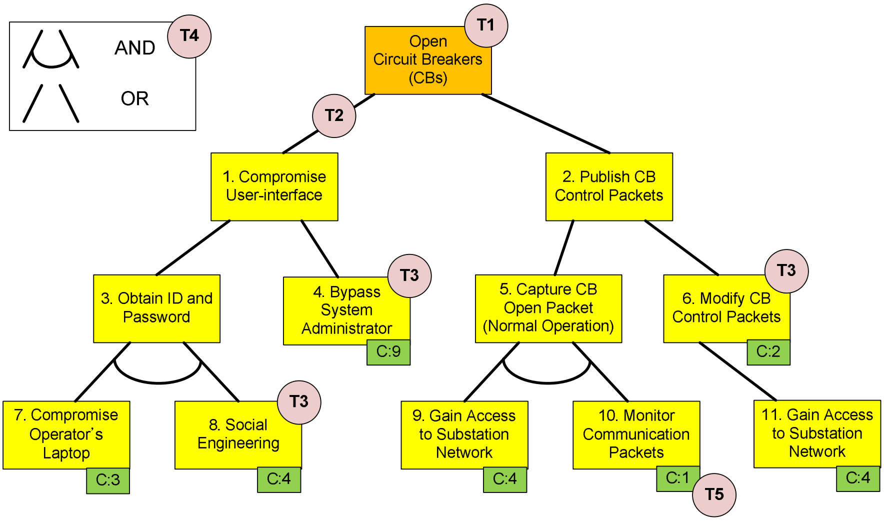

AND
OR
T4
Open Circuit Breakers (CBs)
T1
T2
1. Compromise User-interface
2. Publish CB Control Packets
3. Obtain ID and Password
4. Bypass System Administrator
T3
C:9
5. Capture CB Open Packet (Normal Operation)
6. Modify CB Control Packets
T3
C:2
7. Compromise Operator's Laptop
C:3
8. Social Engineering
T3
C:4
9. Gain Access to Substation Network
C:4
10. Monitor Communication Packets
C:1
T5
11. Gain Access to Substation Network
C:4

Fig. 14 Attack tree diagram for substation automation systems

4.3 Mitigation Strategies That Include Cyber and Physical Aspects

The mitigation strategy is vital to cyber-physical security of substations in order to stop the attack, disconnect the intruder, and restore the power systems to a normal state. Mitigation methods can be divided into two sides, e.g., cyber (ICT) and physical (power system) side. On the cyber side, real-time network monitoring, intrusion detection system, encryption, authentication and enhanced firewall are common practices in industry. The key to cyber mitigation is to find anomaly activities or malicious behaviors, and disconnect or stop the intrusion. A remedial action for mitigation can be performed on the physical side. For example, the Optimal Power Flow (OPF) algorithm, with an objective function that minimizes load shedding, can be used to calculate the mitigation actions. Substation operators need to determine an optimal cost-benefit solution. For instance, they can implement new security measures at important substations (e.g., high voltage substations).

4.3.1 Framework

Confidentiality, Integrity and Availability (CIA) are essential concepts in information security [48]. Confidentiality is to prevent access to data or information by unauthorized individuals. Communication data in a substation network must be protected since any successful eavesdropping attack can capture critical packets that contain important information to be used for an attack. Integrity refers to the ability to maintain authenticity, accuracy and provenance of recorded and reported information over its life cycle, i.e., data cannot be modified by an unauthorized person [49]. Upon successfully modification of fabrication of control messages (e.g., circuit breaker control or transformer tap change) in a substation network, an attacker may trigger an outage of the power system. Availability refers to the timely delivery of functional capability. Communications from/to a substation must be available all the time. A Denial-of-service (DoS) attack to a substation network can disrupt the communication for controls and measurements from/to the control center. Therefore, these security objectives (i.e., CIA) must be met.

Fig. 15 shows a framework of mitigation strategies based on the status of intrusion, i.e., before, on-going, and after a cyber intrusion. Before an attack is encountered at the substations, security managers and operators need to analyze potential vulnerabilities using the system and security logs, penetration test, etc. Encryption is needed for non-time critical messages, e.g., MMS and DNP in order to enhance the confidentiality. Authentication is used for time critical messages, e.g., GOOSE and SMV, for the enhancement of integrity. Transient stability and contingency analysis will be performed to check whether the power system can maintain stability when it undergoes hypothesized cyber attacks. During the intrusions, it is important to find the intrusion point and type of attack. Then the intruder(s) can be disconnected from the substation network through an IDS and a firewall. The impact analysis will be performed to find the most critical attack that can cause the worst case damage to the power grid. Once intruders are blocked or disconnected from the substation network, the security manager has to analyze the security breach using security and system logs.

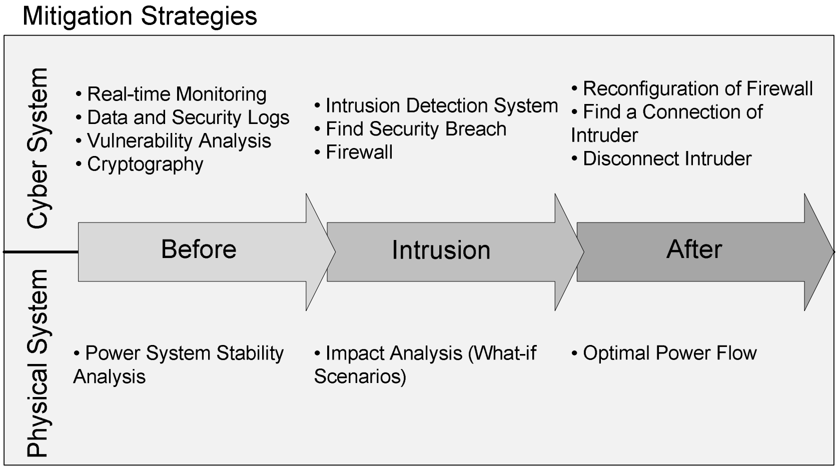


Fig. 15 The framework of mitigation strategies

5 Real-time Testbed for the Cyber Security of the Substations

5.1 Objectives and Requirements

As mentioned in previous Sections, a cyber-physical power system testbed is helpful for the study of the cause-effect relationships of cyber intrusions, resilience of power systems, as well as the performance and reliability of applications in a realistic environment. In a real-time testbed, all components that include software, hardware, communications and emulators are synchronized with GPS or time protocol. Real-time dynamics of communication and information processing are required when cyber intrusions, detections and mitigations are studied. The following Section explains the framework and architecture of a real-time testbed for cyber security of substations.

5.2 Architecture and Components

The work of [50] proposes a Real-time monitoring, Anomaly detection, Impact analysis, and Mitigation strategies (RAIM) framework. Real-time monitoring allows tracking of activities on the cyber-power system. The objective of Anomaly detection is to identify the events on cyber systems that indicate potential cyber intrusions. The tasks of impact analysis are to evaluate the intrusion behaviors and consequences on the power system operating condition. Impact analysis can be achieved by computer simulations in a way similar to the contingency evaluation for online security assessment. The mitigation module serves to illustrate the preventive, remedial or restorative actions to mitigate potential damages caused by cyber intrusions. Analytical techniques can be evaluated on a software based cyber-power system testbed with the control center and substation models.

As shown in Fig. 16, the testbed consists of real-time substation ICTs and the SCADA system from a commercial vendor, while the digital simulator is adopted for the physical power system. There are a couple of products that produce analog and digital values, e.g., the Real-time Digital Simulator (RTDS) and HYPERsim. They are widely used for hardware testing and power system simulation. However, it has a limitation to produce analog and digital values per hardware board so software simulators are more suitable for large scale power grids in a hybrid or an off-line mode.

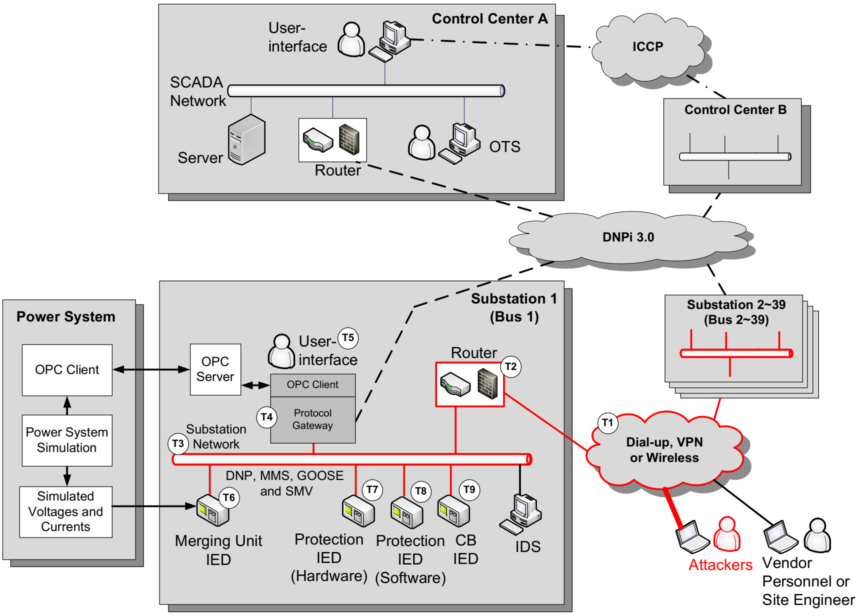


Fig. 16 Real-time testbed for cyber-physical substations

Physical System Module: This testbed comprises two control centers and thirty nine substations, as shown in Fig. 16. The DIgSILENT power factory is a suite of software simulation tools for power systems incorporating applications for system dynamics, transient analysis, optimal power flow, and state estimation. It is used as a real-time simulator for power systems in this testbed. Institute of Electrical and Electronics Engineers (IEEE) 39-bus system has been modeled and implemented in the power factory for research on cyber security of substations and transmission systems. In fact, the power factory is not a real-time simulator. However, it can be used to generate real-time simulation results that include electromechanical transient dynamics of a small system (e.g., IEEE 39-bus) by advanced multi-core based microprocessors and fast Solid-State Drivers (SSDs). Four types of IEDs are installed at the substation networks such as merging unit IED, hardware type protection IED, software type protection IED and circuit breaker IED. Both hardware and software types of IEDs have the capability to deliver control commands (GOOSE messages) of a circuit breaker whereas the circuit breaker IED is designed to subscribe to GOOSE messages, and publish the status (open/close) to software type protection IED. The merging unit IED can send calculated currents and voltages values to software type protection IED. The IDS is designed to detect anomalies and malicious behaviors in a substation automation system [51].

ICT Module: ICCP is used for communication between control centers. Each control center belongs to a different power company. Therefore, control center A only monitors the measurements of control center A but control center A does not have the jurisdiction to control devices supervised by control center B. DNPi (DNP over TCP/IP) protocol enables communications between control centers and substations. All measurements are sent from substations to control centers whereas control commands come from the control centers to substations via DNPi protocol. Object Linking and Embedding for Process Control (OPC) enables the communications between the physical and cyber systems. As illustrated in Fig. 16, all measured status data and analogue values from the power system simulator (i.e., powerfactory) are mapped with the OPC client and linked to an OPC server. The gateway is also mapped with an OPC client and connected to server. Therefore, the control center user interface is able to supervise and control the power system. IEC 61850 based protocols (e.g., SMV, MMS and GOOSE) have been implemented for the substation's communication network using SISCO MMS EASE Lite which can be used to simulate real-time substation automation communication. As described in Section 3, MMS messages are used for the communication between the user-interface and IEDs; SMV messages that include currents and voltages are sent from MU IED to the software type protection IED; GOOSE messages are used for communications between IEDs and circuit breakers, i.e., when an IED sends a tripping signal to CB, and CB sends a status to an IED. The role of the gateway is to convert different communication protocols in a substation network, e.g., convert DNPi to MMS and vice versa. The integrated IDS and firewalls are deployed for cyber security measures. In order to evaluate cyber intrusions from remote access points to substation networks, the IDS and routers need to be connected to the same ICT network. There are three types of remote access points (e.g., dial-up, VPN or wireless) in the testbed environment.

Cyber System Module: SCADA systems can collect, store and visualize the measurements and events on multiple screens. A commercial SCADA system is installed to maximize the accuracy of data and enhance interoperability between devices. The SCADA system consists of network devices, computer servers, databases, user interfaces and the Operator Training Simulator (OTS). The OTS enables operators to simulate and analyze how realistic cyber intrusions can cause damages to a power system and how to defend against the intrusions. Therefore, it can help operators to be prepared for emergency situations. The EMS supports power system applications such as state estimation and optimal power flow.

5.3 Case Study

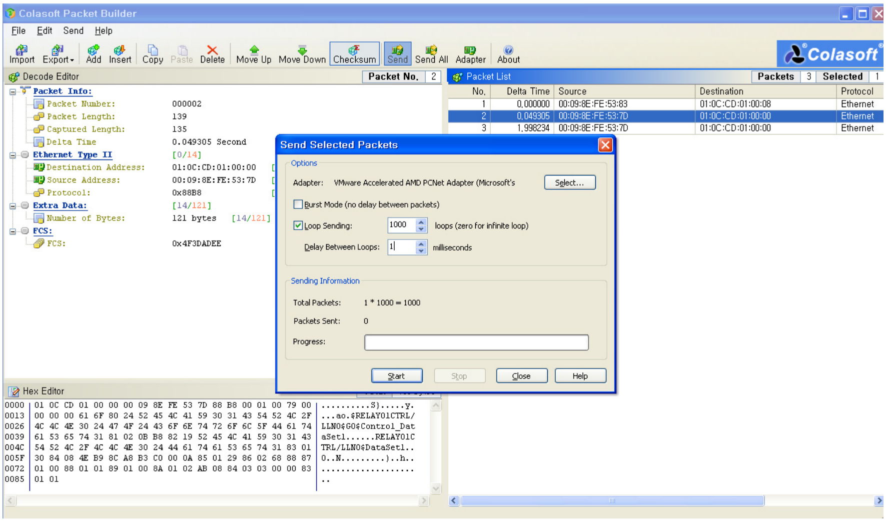
A real-time cyber-physical testbed enables users to study realistic scenarios of cyber attacks and defense strategies. In this Section, scenarios that include possible intrusion paths to the substation systems and cyber attacks that compromise the substation will be discussed.

Table 3 Cyber intrusions and mitigations

No.	Intrusions	Results	IT mitigations
1	GOOSE replay attack	Open CB	Network based IDS
2	GOOSE data modification	Open CB	Network based IDS
3	DoS attack using GOOSE	Lost availability of protection IEDs and CB	Network based IDS
4	Generate fabricated GOOSE packets	Open CB	Network based IDS
5	SMV replay attack	Open CB	Network based IDS
6	SMV data modification	Open CB	Network based IDS
7	DoS attack using SMV	Lost availability of protection IEDs and MU	Network based IDS
8	Generate fabricated SMV packets	Open CB	Network based IDS
9	Modify control values at gateway	Open CB / change transformer tap position	Host based IDS
10	Modify measurement values at gateway	Send wrong data to control center	Host based IDS
11	Man-in-the-middle attack	Lead wrong operation action	Network / host based IDS
12	Compromise user-interface	Change password / open CB / change transformer tap position	Host based IDS
13	Compromise protection IED	Change protection setting / open CB	Host based IDS

As depicted in Fig. 16, a possible intrusion path is from the remote access point (T1) to the substation systems (T2-9). This intrusion path is protected and monitored by security enhanced firewalls with confidential security rules. However, once an intruder successfully compromises the site engineer computer, (s)he can install back door software and is able to acquire the user name and password of the VPN (T1) connection. Using a legitimate ID and password, the firewall (T2) cannot detect the intruder. Once they access the substation network (T3), all network devices can be detected by ping and port scanner software tools that are publicly available. Therefore, intruders can find the substation's user interface (T5), IEDs (T6~9) and protocol gateway (T4). Unfortunately, these critical devices are sometimes mis-configured or improperly protected against cyber intrusions since they may be perceived as part of an isolated communication network. It has been reported that many computer servers and systems use default user IDs and passwords, and operators may not know the configurations of their firewalls. Through these security breaches, the intruder could compromise the substation system. After compromising the substation system, attacks can be launched based on their scenarios as follows.

(1) The intrusion scenario, GOOSE replay attack, is to capture the normal operation of GOOSE packets that contain a CB trip signal, and then retransfer them to the substation network without any modification using free available software, as shown in Fig. 17. The software has the capability to capture and retransfer packets from/to chosen network. This attack can open the circuit breaker (T9).



Packet No. 2

```
Packet Info:
  Packet Number:          000002
  Packet Length:          139
  Captured Length:        135
  Delta Time              0.049305 Second
Ethernet Type II          [0/14]
  Destination Address:    01:0C:CD:01:00:00
  Source Address:         00:09:8E:FE:53:7D
  Protocol:               0x88B8
Extra Data:               [14/121]
  Number of Bytes:        121 bytes   [14/121]
FCS:
  FCS:                    0x4F3DADEE
```

Packets 3 Selected 1

No.	Delta Time	Source	Destination	Protocol
1	0,000000	00:09:8E:FE:53:83	01:0C:CD:01:00:08	Ethernet
2	0,049305	00:09:8E:FE:53:7D	01:0C:CD:01:00:00	Ethernet
3	1,998234	00:09:8E:FE:53:7D	01:0C:CD:01:00:00	Ethernet

Options

Adapter: VMware Accelerated AMD PCNet Adapter (Microsoft's

☐ Burst Mode (no delay between packets)

☑ Loop Sending: 1000 loops (zero for infinite loop)

Delay Between Loops: 1 milliseconds

Sending Information

Total Packets: 1 * 1000 = 1000

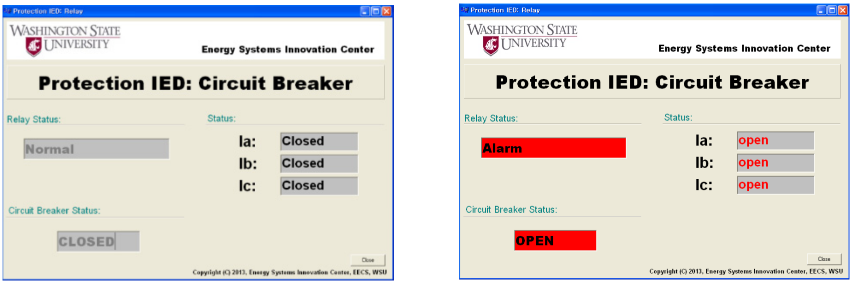
Packets Sent: 0

Progress:

```
0000 | 01 0C CD 01 00 00 00 09 8E FE 53 7D 88 B8 00 01 00 79 00 | ..........S}.....y.
0013 | 00 00 00 61 6F 80 24 52 45 4C 41 59 30 31 43 54 52 4C 2F | ...ao.$RELAY01CTRL/
0026 | 4C 4C 4E 30 24 47 4F 24 43 6F 6E 74 72 6F 6C 5F 44 61 74 | LLN0$GO$Control_Dat
0039 | 61 53 65 74 31 81 02 0B B8 82 19 52 45 4C 41 59 30 31 43 | aSet1......RELAY01C
004C | 54 52 4C 2F 4C 4C 4E 30 24 44 61 74 61 53 65 74 31 83 01 | TRL/LLN0$DataSet1..
005F | 30 84 08 4E B9 8C A8 B3 C0 00 0A 85 01 29 86 02 68 88 87 | 0..N.........)..h..
0072 | 01 00 88 01 01 89 01 00 8A 01 02 AB 08 84 03 03 00 00 83 | ...................
0085 | 01 01                                                    | ..
```

Fig. 17 Retransfer captured GOOSE packet to the substation network

(2) Fig. 18-(a) shows an HMI of the circuit breaker before the attack. In this status, the circuit breaker is closed, and status of relay is normal. After the GOOSE data modification attack, the circuit breaker is opened with the associated relay alarm status as shown in Fig. 18-(b). This alarm indicates that no overcurrent is sensed by the relay but the circuit breaker is tripped.



Protection IED: Relay

WASHINGTON STATE UNIVERSITY

Energy Systems Innovation Center

Protection IED: Circuit Breaker

Relay Status: Normal

Status:

Ia:	Closed
Ib:	Closed
Ic:	Closed

Circuit Breaker Status: CLOSED

Copyright (C) 2013, Energy Systems Innovation Center, EECS, WSU

(a) Before attack

Protection IED: Relay

WASHINGTON STATE UNIVERSITY

Energy Systems Innovation Center

Protection IED: Circuit Breaker

Relay Status: Alarm

Status:

Ia:	open
Ib:	open
Ic:	open

Circuit Breaker Status: OPEN

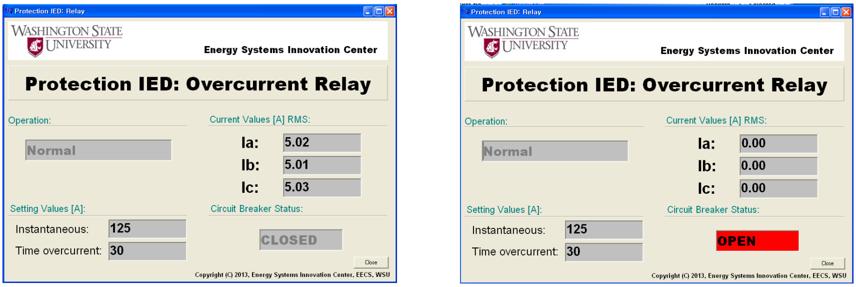
Copyright (C) 2013, Energy Systems Innovation Center, EECS, WSU

(b) After attack

Fig. 18 Consequence of a GOOSE related cyber attack to the circuit breaker

(3) The intrusion scenario, DoS attack using GOOSE, is to generate a huge amount of GOOSE packets into the substation network. This attack can disrupt the availability of substation ICT network so operators will lose controls and measurements.

(4) The attack scenario, generate fabricated GOOSE packets, is to capture, modify, and transfer fabricated GOOSE packets to the substation ICT network. This attack can open the circuit breaker (T9). As shown in Fig. 19-(a), this relay has the overcurrent protection function with instantaneous (125 [A]) and time overcurrent (30 [A]) settings. It can also monitor the status of the circuit breaker. As illustrated in Fig. 19-(b), it shows the consequence of a GOOSE modification attack since the overcurrent relay does not sense any fault current but the circuit breaker is opened by cyber intrusion. The relay sensed a change of the circuit breaker status (from closed to open) without an overcurrent condition.



Protection IED: Relay

WASHINGTON STATE UNIVERSITY

Energy Systems Innovation Center

Protection IED: Overcurrent Relay

Operation: Normal

Current Values [A] RMS:

Ia:	5.02
Ib:	5.01
Ic:	5.03

Setting Values [A]:

Instantaneous:	125
Time overcurrent:	30

Circuit Breaker Status: CLOSED

Copyright (C) 2013, Energy Systems Innovation Center, EECS, WSU

(a) Before attack

Protection IED: Relay

WASHINGTON STATE UNIVERSITY

Energy Systems Innovation Center

Protection IED: Overcurrent Relay

Operation: Normal

Current Values [A] RMS:

Ia:	0.00
Ib:	0.00
Ic:	0.00

Setting Values [A]:

Instantaneous:	125
Time overcurrent:	30

Circuit Breaker Status: OPEN

Copyright (C) 2013, Energy Systems Innovation Center, EECS, WSU

(b) After attack

Fig. 19 Consequence of GOOSE related cyber attack to overcurrent relay

(5) The intrusion scenario, SMV replay attack, is to capture normal SMV packets when a fault occurred, and then retransfer them to the substation network without any modification. This attack will execute the overcurrent protection (since captured SMV packets contain overcurrent data) and relay (T8) will trip the circuit breaker (T9).

(6) The intrusion, SMV data modification, is to capture normal SMV packets from substation ICT network, modify the measurement data (e.g., low current value to high current value), and then retransfer them to the substation ICT network.

This attack will execute the protection functions at relay (T8), and open the circuit breaker (T9).

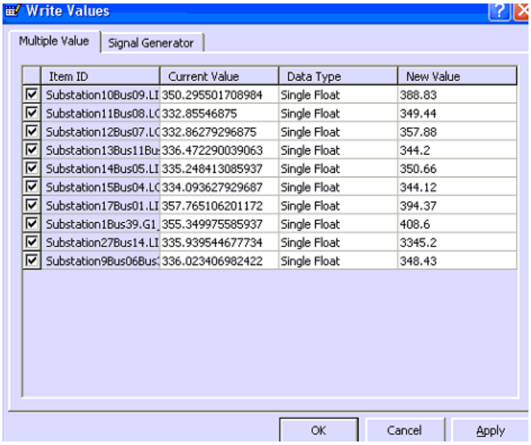
(7) The scenario, DoS attack using SMV, is to generate a large amount of SMV packets into the substation network. This attack can disrupt the availability of a substation network so operators will lose controls and measurements of network connected devices.

(8) The scenario, generate fabricated SMV packets, is to capture, modify, and transfer fabricated SMV packets to the substation ICT network. This attack will execute the protection functions at relay (T8) and open the circuit breaker (T9).

(9) The intrusion scenario, modify control values at gateway, involves compromising the substation gateway (T4). An attacker can monitor, modify and generate all measured analog and status values using the compromised gateway. A false signal is generated and a trigger open (T7 and T8) command is sent to substation circuit breaker (T9).

(10) The scenario, modify measurement values at gateway, is to generate a forged CB status at the gateway. As a result, control center operators will be presented with fabricated data for the CB status or current and voltage values. However, the actual status has not changed.

(11) The attack scenario, man-in-the-middle attack, is to generate fabricated analog values to the control center using a man-in-the-middle attack. Once an intruder successfully compromises the substation Local Area Network (LAN) (T3) or OPC client, (s)he is able to monitor and capture all measured data from field devices. Attackers send fabricated data to the control center as illustrated in Fig. 20. Once data passes through the SCADA system, system operators will observe an operational emergency. As a result, operators may take emergency controls such as reducing voltage set points at generators, while the power system is actually in a normal operation condition. In the worst case, these (logical) actions based on fabricated data can drive the system into a sequence of cascading events, leading to a power outage.



	Item ID	Current Value	Data Type	New Value
☑	Substation10Bus09.LI	350.295501708984	Single Float	388.83
☑	Substation11Bus08.LC	332.85546875	Single Float	349.44
☑	Substation12Bus07.LC	332.86279296875	Single Float	357.88
☑	Substation13Bus11Bu	336.472290039063	Single Float	344.2
☑	Substation14Bus05.LI	335.248413085937	Single Float	350.66
☑	Substation15Bus04.LC	334.093627929687	Single Float	344.12
☑	Substation17Bus01.LI	357.765106201172	Single Float	394.37
☑	Substation1Bus39.G1_	355.349975585937	Single Float	408.6
☑	Substation27Bus14.LI	335.939544677734	Single Float	3345.2
☑	Substation9Bus06Bus	336.023406982422	Single Float	348.43

Fig. 20 Generating fabricated analog values to the control center

(12) The attack scenario, compromise user-interface, is to find and compromise the substation user-interface. If an attacker has sufficient knowledge about the substation automation system, they may find all network connected devices using ping and port scanner. Once intruders compromise (i.e., find user name and password) the substation user-interface, they may change the password of user-interface, execute opening command to circuit breaker, or change the transformer tap position.

(13) After compromising the substation protection IED, intruders can access the IED with authorized user name and password, and then change the protection settings to execute the system protection functions.

Mitigation actions are needed for the substation IT as well as the power grid. For IT mitigation, a host-based and network-based IDS have been proposed [51]. The host-based IDS uses an anomaly detection algorithm based on the logs of temporal events whereas the network-based IDS monitors malicious behaviors that violates the predefined rules as illustrated in Fig. 21 and 22.

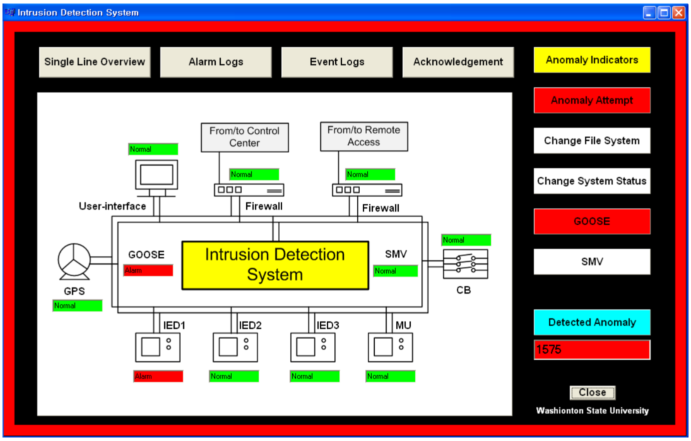


Fig. 21 HMI of intrusion detection system

As shown in Fig. 22, the network-based intrusion detection system has 6 types of anomaly indicators, i.e., predefined logics, data violation, security constrains, detected intrusions, alarm data, and event data. The host-based intrusion detection system has 8 anomaly indicators, i.e., temporal anomaly detection, unauthorized control actions, intrusion attempt, change of the file system, change of IED setting, change of system status, alarm data, and event data. These modules monitor all system activities or the network traffic in order to find anomalies or abnormal behaviors. For the communication protocol based attacks, e.g., replay, packet modification and generation, the attacker's behaviors will violate the predefined security rules. For instance, replay attack will violate the time synchronization since the attacker will use previously captured control messages that contains an incorrect time stamp. When the attacker tries to access the substation gateway which is on the user interface, logs of intrusion attempts (user interface) will be generated. Any intrusion that attempts to change of the target system's status (e.g., circuit breaker status and change settings of IED) will generate system logs. For the gateway intrusion scenario, the attacker will create logs of changes of the file system (gateway) and intrusion attempts (user interface). In the user-interface intrusion scenario, the attacker triggers logs of intrusion attempts (user interface) and changes of file system logs. The host-based IDS is able to detect the intrusions by analyzing the log files. The proposed collaboration scheme between IDS and the firewall is able to disconnect intruders from the substation network.

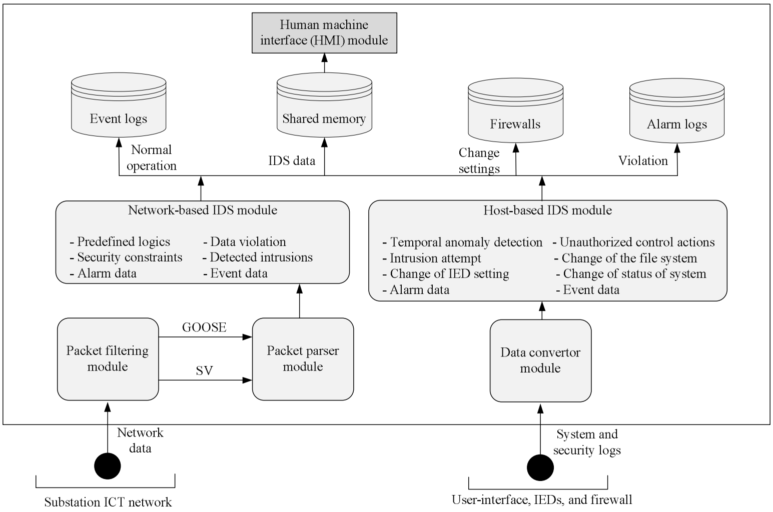


Fig. 22 Host- and network-based intrusion detection system

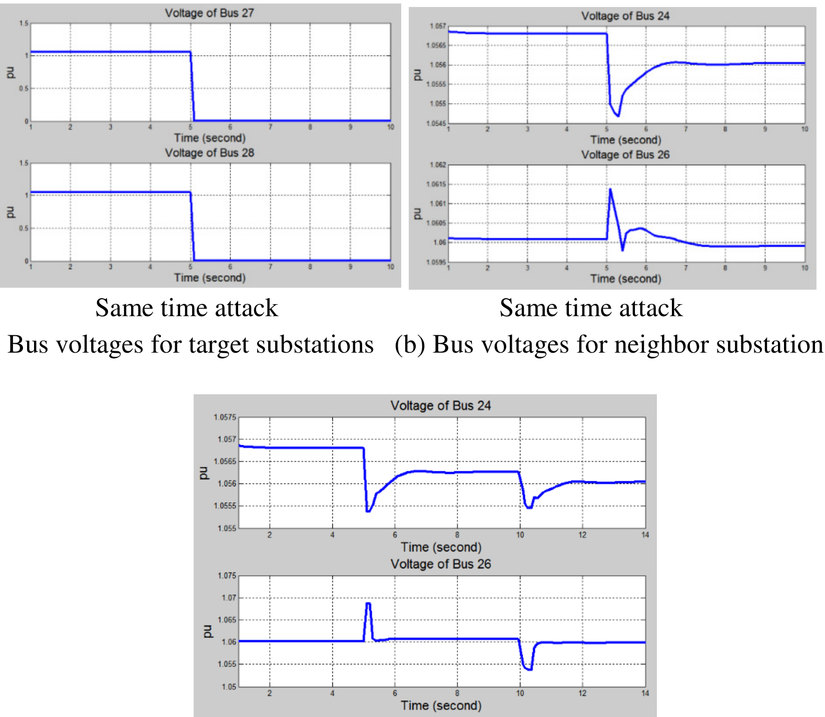
The IDS has been validated under different types of attack packet intervals, e.g., 1, 10, 20 and 30 [msec], in order to check the performance of IDS. The false negative ratio (FNR) is defined as the number of misclassified abnormal packets divided by the total number of abnormal packets. Table IV shows the mean value of FNR of each test case: 1 ms: 0.95%, 10 ms: 0.62%, 20 ms: 0.29% and 30 ms: 0.11%, respectively. The FNR performance of the proposed intrusion detection system depends on the interval between packets. This is due to the fact that IDS may lose packets when the interval between packets is too small [36]. The false positive ratio (FPR) is defined as the number of misclassified normal packets divided by the total number of normal packets. As shown in Table IV, the mean value of FPR of each test case are 1 ms: 0.79%, 10 ms: 0.56%, 20 ms: 0.18% and 30 ms: 0.027%, respectively.

Emergency control actions are taken to mitigate the effects of cyber intrusions as an attempt to restore the system back to a normal condition. Fig. 23-(a) and 23-(b) show the consequence of multiple cyber attacks to substation 27 and 28 at the

Table 4 False ratio of the substation intrusion detection system

Attack packet interval	1 [msec]	10 [msec]	20 [msec]	30 [msec]
False negative ratio	0.95 %	0.62 %	0.29 %	0.11 %
False positive ratio	0.79 %	0.56 %	0.18 %	0.027 %

same time (attack time is at 5 second) whereas Fig. 23-(c) shows the results of different time (attack times are at 5 and 10 second, respectively) based cyber intrusions. Both attacks consider the worst case scenario such as opening all circuit breakers at a substation as shown in Fig. 24. After compromising substations 27 and 28, intruders open all circuit breakers at target substations. As the consequence of this attack, the voltages of substations 27 and 28 dropped to 0 pu. In the mean time, the voltages of neighbor substations, e.g., substations 24 and 26, dropped dramatically. However, Optimal Power Flow (OPF), with an objective function that minimizes load shedding and constraints that include generator maximum and minimum allowable P and Q, executed as a physical mitigation. At 5.5 second, the voltages at buses 24 and 26 recover by the mitigation actions.



Same time attack

(a) Bus voltages for target substations

Same time attack

(b) Bus voltages for neighbor substations

different time attacks

(c) Bus voltages for neighbor substations

Fig. 23 Consequence of cyber attacks on IEEE 39 bus system

Fig. 23-(c) and Fig. 24 illustrate how voltages of neighbor substations vary after multiple cyber intrusions (substation 27 at 5 second and substation 28 at 10 second, respectively). The first cyber intrusion is executed at 5 second which leads to a voltage drop, and then physical mitigation (i.e., OPF) leads to the sharp voltage rise. Another 5 seconds later, the second attack on substation 28 is executed, and then the amount of load shedding is determined by OPF and power systems are back to a normal status.

The time domain dynamic calculation has been used for the case study. For power grid mitigation, an optimal power flow based generation control with an objective function that minimizes the network losses is used for power system recovery after cyber attacks. Coordination between mitigations in the cyber and physical systems enhances the security of a substation.

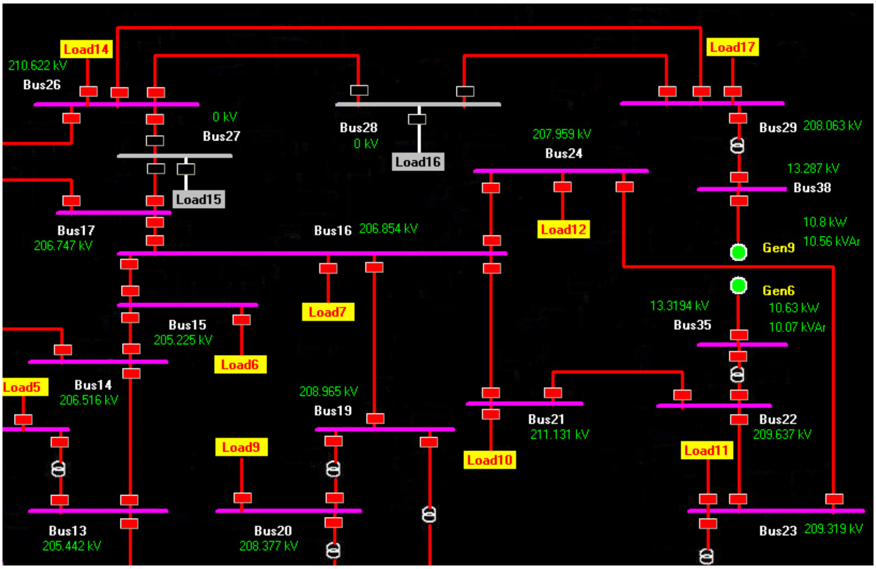


Fig. 24 Consequence of physical system after simultaneous cyber attacks to multiple substations on the IEEE 39-bus system (buses 27 and 28)

Acknowledgement. This research is sponsored by U.S. National Science Foundation, "Collaborative Research: Resiliency Against Coordinated Cyber Attacks on Power Grid," EECS-1202229. This work is partially sponsored by National Natural Science Foundation of China, Grant No. 51277104, and Tsinghua University.

References

[1] Hahn, A., Ashok, A., Sridhar, S., Govindarasu, M.: Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid. IEEE Trans. on Smart Grid 4(2), 847–855 (2013)

[2] Glover, J.-D., Sarma, M.-S., Overbye, T.-J.: Power system analysis and design. Thomson (2011)

[3] Li, F., Qiao, W., Sun, H., Wan, H., Wang, J., Xia, Y., Xu, Z., Zhang, P.: Smart Transmission Grid: Vision and Framework. IEEE Trans. Smart Grid 1(2), 168–177 (2010)

[4] Igure, V.-M., Laughter, S.-A., Williams, R.-D.: Security Issues in SCADA Networks. Computers & Security 25(7), 498–506 (2006)

[5] Liu, C.-C., Stefanov, A., Hong, J., Panciatici, P.: Intruders in the Grid. IEEE Power Energy Magazine 10(1), 58–66 (2012)

[6] Milano, F., Canizares, C.-A., Invernizzi, M.: Voltage Stability Constrained OPF Market Models Considering Contingency Criteria. Electric Power Systems Research 74(1), 27–36 (2005)

[7] Govindarasu, M., Hann, A., Sauer, P.: Cyber-Physical Systems Security for Smart Grid. Future Grid Initiative White Paper, PSERC (February 2012), http://www.pserc.wisc.edu/documents/publications/papers/fgwhitepapers/Govindarasu_Future_Grid_White_Paper_CPS_May_2012.pdf

[8] GAO-11-117, Electricity Grid Modernization: Progress Being Made on Cyber Security Guidelines, but Key Challenges Remain to be Addressed. Government Accountability Office (GAO) (January 2011), http://www.gao.gov/new.items/d11117.pdf

[9] Guidelines for Smart Grid Cyber Security, National Institute for Standards and Technology (August 2010), http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf

[10] North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standards 002-009, http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

[11] Govindarasu, M., Liu, C.-C.: Cyber Physical Security Testbed for the Smart Grid: Fidelity, Scalability, Remote Access, and Federation. Position Paper to National CPS Energy Workshop (2013)

[12] National SCADA test bed: Fact sheet, Idaho National Laboratory, INL (2007)

[13] Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL NSTB Program, Idaho National Laboratory (INL) (November 2008)

[14] Rohde, M.-R.-P.: Cyberassessment Methods for SCADA Security. Instrumentation, Systems and Automation Society (ISA), Tech. Rep. (2005)

[15] McDonald, M.-J., Conrad, G.-N., Service, T.-C., Cassidy, R.H.: Cyber Effects Analysis Using VCSE. Promoting Control System Reliability, Sandia National Laboratories, SAND, 2008-5954 (September 2008)

[16] McDonald, M.-J.: Modeling and Simulation for Cyber-Physical System Security Research. Development and Applications, Sandia National Laboratories, SAND2010-0568 (February 2010)

[17] Bergman, D.C., Jin, D., Nicol, D.M., Yardley, T.: The Virtual Power System Testbed and Inter-Testbed Integration. In: Proc. 2nd Workshop Cyber Security Exp. Test (August 2009)

[18] Mallouhi, M., Al-Nashif, Y., Cox, D., Chadaga, T., Hariri, S.: A Testbed for Analyzing Security of SCADA Control Systems (TASSCS). In: Proceedings of IEEE PES Innov. SmartGrid Technol. (ISGT) (January 2011)

[19] Dondossola, G., Garrone, G., Szanto, J., Deconinck, G., Loix, T., Beitollahi, H.: ICT Resilience of Power Control Systems: Experimental Results from the CRUTIAL Testbeds. In: Proceedings of IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN), pp. 554–559 (July 2009)

[20] Dondossola, G., Deconinck, G., Garrone, F., Beitollahi, H.: Testbeds for Assessing Critical Scenarios in Power Control Systems. In: Setola, R., Geretshuber, S. (eds.) CRITIS 2008. LNCS, vol. 5508, pp. 223–234. Springer, Heidelberg (2009)

[21] Hong, J., Wu, S.-S., Stefano, A., Fshosha, A., Liu, C.-C., Gladyshev, P., Govindarasu, M.: An Intrusion and Defense Testbed in a Cyber-power System Environment. In: IEEE Power and Energy Society General Meeting (July 2011)

[22] Queiroz, C., Mahmood, A., Tari, Z.: SCADASim A Framework for Building SCADA Simulations. IEEE Trans. Smart Grid 2(4), 589–597 (2011)

[23] Blochwitz, T., Otter, M., Akesson, J., Arnold, M., Clauß, C., Elmqvist, H., Friedrich, M., Junghanns, A., Mauss, J., Neumerkel, D., Olsson, H., Viel, A.: Functional Mockup Interface 2.0: The Standard for Tool independent Exchange of Simulation Models. In: Proceedings of 9th International Modelica Conference, Munich (2012), https://www.fmi-standard.org/start

[24] Simulation Tool - OpenDSS, Smart Grid Resource Center, Electric Power Research Institute (EPRI), http://www.smartgrid.epri.com/SimulationTool.aspx

[25] MATPOWER, A MATLAB Power System Simulation Package, Power Systems Engineering Research Center (PSERC), http://www.pserc.cornell.edu//matpower/

[26] Vyatkin, V., Zhabelova, G., Higgins, N., Schwarz, K., Nair, N.C.: Towards Intelligent Smart Grid Devices with IEC 61850 Interoperability and IEC 61499 Open Control Architecture. In: IEEE PES Transmission and Distribution Conference (April 2010)

[27] Mackiewicz, R.E.: Overview of IEC 61850 and Benefits. In: IEEE PES Transmission and Distribution Conference, pp. 376–383 (May 2006)

[28] Clarke, G., Reynders, D., Wright, E.: Practical Modern SCADA Protocols, IDC technologies (2004)

[29] Communication Networks and Systems for Power Utility Automation, IEC 61850-90-1 Standard: Use of IEC 61850 for the Communication between Substations, 1st edn. (March 2010)

[30] Electrical Single Line Diagram - Part Two, Electrical Knowhow, http://www.electrical-knowhow.com/2012/12/electrical-single-line-diagram-part-two.html

[31] Communication Networks and Systems in Substations, IEC 61850-5 Standard: Communication Requirements for Functions and Device Models, 1st edn. (July 2003)

[32] Specific Communication Service Mapping (SCSM), IEC 61850 8-1 Standard: Mapping to MMS (ISO/IEC9506-1 and ISO/IEC 9506-2), 1st edn. (May 2004)

[33] Premaratne, U.-K., Samarabandu, J., Sidhu, T.-S., Beresh, R., Tan, J.-C.: An Intrusion Detection System for IEC 61850 Automated Substations. IEEE Trans. Power Del. 25(4), 2376–2383 (2010)

[34] Morris, T., Pavurapu, K.: A Retrofit Network Transaction Data Logger and Intrusion Detection System for Transmission and Distribution Substations. In: IEEE International Conference on Power and Energy (PECon), pp. 958–963 (November 2010)

[35] Ten, C.-W., Hong, J., Liu, C.-C.: Anomaly Detection for Cybersecurity of the Substations. IEEE Trans. Smart Grid 2(4), 865–873 (2011)

[36] Hong, J., Liu, C.-C., Govindarasu, M.: Detection of Cyber Intrusions Using Network-Based Multicast Messages for Substation Automation. In: Proceedings of IEEE Innovative Smart Grid Technologies (ISGT) Conference (2014)

[37] Power Systems Management and Associated Information Exchange - Data and Communications Security, IEC TS 62351-1 Standard: Part 1: Communication Network and System Security - Introduction to Security Issues, 1st edn. (May 2007)

[38] Pender, T.: When Power Goes Out, a Squirrel is Likely to Blame, The Record (October 2013), http://www.therecord.com/news-story/4164925-when-power-goes-out-a-squirrel-is-likely-to-blame/

[39] Campbell, R.-J.: Weather-Related Power Outages and Electric System Resiliency, Congress Research Service 7-5700, http://www.fas.org/sgp/crs/misc/R42696.pdf

[40] Kushner, D.: The Real Story of Stuxnet. IEEE Spectrum 50(3), 48–53 (2013)

[41] Orgill, G.-L., Romney, G.-W., Bailey, M.-G., Orgill, P.-M.: The Urgency for Effective User Privacy-Education to Counter Social Engineering Attacks on Secure Computer Systems. In: Proceedings of the 5th Conference on Information Technology Education (CITC5), pp. 177–181 (2004)

[42] Schneier, B.: Attack Trees: Modeling Security Threats. Dr. Dobb's Journal (December 1999)

[43] Dawkins, J., Hale, J.: A Systematic Approach to Multi-stage Network At-tack Analysis. In: Second IEEE International Information Assurance Workshop, pp. 48–56 (April 2004)

[44] Moore, A.-P., Ellison, R.-J., Linger, R.-C.: Attack Modeling for Information Security and Survivability. Survivable Systems, Technical Note CMU/SEI-2001-TN-001 (March 2001)

[45] Ten, C.-W., Liu, C.-C., Govindarasu, M.: Vulnerability Assessment of Cybersecurity for SCADA Systems Using Attack Trees. In: IEEE Power and Energy Society General Meeting (June 2007)

[46] North American Electric Reliability Corporation, Cyber Attack Task Force, Final Report (May 2012), http://www.nerc.com/docs/cip/catf/12-CATF_Final_Report_BOT_clean_Mar_26_2012-Board%20Accepted%200521.pdf

[47] Kordy, B., Pietre-Cambacedes, L., Schweitzer, P.: DAG-Based Attack and Defense Modeling: Don't Miss the Forest for the Attack Trees. arXiv preprint arXiv:1303.7397 (2013)

[48] Ericsson, G.N.: Management of Information Security for an Electric Power Utility-On Security Domains and Use of ISO/IEC17799 Standard. IEEE Transactions on Power Delivery 20(2), 683–690 (2005)

[49] Bayuk, J.-L., Healey, J., Rohmeyer, P., Sachs, M.-H., Schmidt, J., Weiss, J.: Cyber Security Policy Guidebook. Wiley (2012)

[50] Hong, J., Stefano, A., Liu, C.-C., Govindarasu, M.: Cyber-Physical Security in a Substation. In: IEEE Power and Energy Society General Meeting (July 2012)

[51] Hong, J., Liu, C.-C., Govindarasu, M.: Integrated Anomaly Detection for Cyber Security of the Substations. IEEE Trans. Smart Grid 5(4), 1643–1653 (2014)

[52] Khaitan, S.K., McCalley, J.D.: Cyber physical system approach for design of power grids: A survey. In: IEEE Power and Energy Society General Meeting (July 2013)

[53] Khaitan, S.K., McCalley, J.D.: Design Techniques and Applications of Cyber-physical Systems: A Survey. IEEE Systems Journal (2014)