International Journal of Cryptology Research 8(2): 39 - 60 (2018)

Electrical Power SCADA Testbed for Cyber Security Assessment

Norziana Jamil[*1], **Qais Qassim**[1,2], **Maslina Daud**[3], **Norhamadi Jaaffar**[3], **Izham Zainal Abidin**[4], and **Wan Azlan Wan Kamarulzaman**[5]

[1]*Institute of Informatics and Computing in Energy, Universiti Tenaga Nasional, Malaysia*
[2]*Information Technology Department, Ibri College of Technology, Oman*
[3]*CyberSecurity Malaysia, Malaysia*
[4]*Collage of Engineering, Universiti Tenaga Nasional, Malaysia*
[5]*Tenaga Nasional Berhad, Malaysia*

E-mail: norziana@uniten.edu.my
[*]*Corresponding author*

ABSTRACT

The cyber-security and protection of Supervisory Control and Data Acquisition (SCADA) has been an active topic of research for the past few years for their catastrophic consequences and significant risk to the health and safety of human lives, serious damage to the physical and industrial environments, and financial issues such as production losses and negative impact to a nations economy. The security measures of SCADA systems are mostly relying on the basis of security through obscurity via controlled access environment. However, the growing interconnectedness with enterprise systems and the trend to use the Internet as the communication medium exacerbates the problem of securing these systems. Therefore, it is vital to identify the vulnerabilities of SCADA system and pinpoint potential cyber-attacks as well as it is essential to enhance

the security measures and protection techniques of these systems. However, performing a real penetration test and vulnerability assessment in a real critical infrastructure system is infeasible and unlikely to happen because an unintended consequence that might occur can propagate its effect to a wider scale. On the other hand, a replicated system is also infeasible due to the high cost and huge effort required. Therefore, developing a realistic SCADA testbed is the best available option for the cyber-security exercise to take place. This paper describes in-detail a scalable and reconfigurable SCADA testbed for cyber-security analysis.

Keywords: SCADA, Testbed, Cyber Security, Vulnerability Assessment

1 INTRODUCTION

Supervisory Control and Data Acquisition (SCADA) system controls and monitors public infrastructures such as electrical power, oil and gas, manufacturing and transportation networks as well as industrial processes (Stouffer et al., 2015). A SCADA system gathers and analyses data from industrial field instruments for real-time control and management to improve the performance of the industrial critical system operations as well as to provide a better protection to the utilised equipment (Stefanov et al., 2015). Due to its wide range of applications, many attacks have been targeting SCADA systems because the failure-to-operate could cause great financial loss and have serious impacts on public safety and the environment (He and Yan, 2016) and (Lin et al., 2017).

A typical SCADA system incorporates three main components: a centralized control station, remote substations and communication networks that connect the substations to their corresponding control centre (Miller and Rowe, 2012). SCADAs control centre is responsible for managing and supervising the overall system, stores processes and system information in addition to,in some cases, serves as a gateway between the corporate network, which supports business operations, and the resources on the industrial network (operation network). Due to the critical functions provided by the control centre, any downtime or compromise of its processes can have disastrous consequences for

the economy, public safety and national security (Nazir et al., 2017). Therefore, any external access or interface with other networksmust be secured and protected. Moreover, a maximum security measurements should be applied using various security tools including firewalls, demilitarized zones (DMZs), intrusion detection systems (IDSs), and anti-malware software programs (Ramachandruni and Poornachandran, 2015).

Prior to the Internet connectivity revolution in SCADA domain and cloud-based SCADA applications as well as the trend of real-time business information systems, SCADA systems were relatively isolated from other networks and external access (Ani et al., 2017). Additionally, proprietary communication protocols and industrial devices were used which promote the security-by-obscurity concept. Therefore, cyber-security was never a key issue to these systems; rather the issues were about developing a reliable, real-time and safe industrial control system. Nonetheless, today's technological trends and the advent of real-time information sharing and analysis have paved way for internetworking capabilities of the enterprise and business networks with the SCADA systems (Krotofil and Gollmann, 2013). This interconnectivity allowed for more efficient remote control, management, and monitoring of industrial processes within the supervised system. The downside to this integration is that a large number of security threats have been introduced to the industrial domain. Consequently, new security vulnerabilities have been enabled (Nazir et al., 2017). Moreover, the interconnection with corporate and business networks made systems' vulnerability accessible and exploitable by malicious parties (Tawde et al., 2015). These problems were not considered in SCADA systems in the past (Ani et al., 2017), (Nazir et al., 2017).

Due to modern SCADA systems' technological trends in addition to the increasing number of successful breaches and cyber-attacks that caused catastrophic and devastating consequences during the past few years on various critical infrastructures, industries and dependant economies, as it has been witnessed by the popular Stuxnet attack, SCADA security has turned a critical concern. Therefore, SCADA needs to be secured and protected against possible cyber sabotages with new security methods and detection/prevention mechanisms to sustain existing relevance within an evolving society. Stuxnet attack incident demonstrated that the security by obscurity concept is no longer a valid approach for such systems (Karnouskos, 2010). Stuxnet attack crossed

both the cyber and physical world by manipulating the control system of the critical infrastructure. During the last few years, a number of security incidents targeted highly sensitive facilities such as the cyber-attack that induced power outage in Ukraines power grid in 2015 by compromising the corporate networks using spear-phishing emails with BlackEnergy malware (Liang et al., 2017), and the attack on German steel plant in late 2014 where hackers successfully took control of the production software and caused significant material damage to the site (Lee et al., 2014).

These incidents have raised concern among cyber-security researchers. Therefore, many cyber-security agencies, providers and researches have taken substantial initiatives to address SCADA systems vulnerabilities and their security loopholes as an effort to protect these systems and their control from security threats, attacks and malware (Stoian et al., 2014). However, activities that help in identifying security vulnerabilities and potential breaches, and investigating the effect of attack on an actual system is neither recommended due to the unintended consequences, nor feasible on a replicated system due to the cost and effort involved (Hahn et al., 2010), (Singh et al., 2015). Therefore, SCADA cyber-security researchers mostly rely on developments of SCADA-specific cyber-security testbed which imitate a realistic SCADA system through emulating, virtualising or simulating SCADA devices, software and communication infrastructure to analyse the security and defence countermeasures of these systems. Such testbed would help researchers to build a better and a more resilient SCADA network architecture, to find methods to do penetration testing on live systems, to build tools to check intrusion, malware, and other vulnerabilities etc. The testbed is also aimed at training engineers with hands-on exercises on how to secure their SCADA systems.

SCADA communication protocols are seen as the weakest link in the cyber security analysis of these systems (Pidikiti et al., 2013), where protocol security is crucial for the functioning of the SCADA systems (Maynard et al., 2014). Security researchers urge on that, protecting data in-transit should be essential part of system protection strategy since data will be moved back and forth from many locations (Baalbaki et al., 2013). Whereas, any disruption or modification occur to the communication link may result in loss of availability and/or integrity of the entire system. That suggests vulnerability in the protocol implementation in the SCADA system may compromise the en-

tire system. Therefore, cyber-security analysis for SCADA-specific protocols should be considered. In the work, the proposed SCADA testbed was designed to utilise one of the commonly used communication protocols namely: IEC 60870-5-104. This protocol was intentionally chosen because it is crucial for the communication between the control stations and distribution stations in many electrical power facilities around the world. For example, a simple search for IEC 80670-5-104 devices using Shodan service reveals that about 584 SCADA servers are connected to the Internet and are remotely accessible. The rest of this paper is organised into the following sections. Section 2 provides an overview of the electrical power grid SCADA system. Section 3 presents research works related to SCADA testbed implementation and design. Section 4 describes the SCADA testbed requirements. In Section 5 the proposed SCADA testbed for cyber-security analysis is presented. Finally, Section 6 concludes the work.

2 ELECTRICAL POWER GRID SCADA SYSTEM

Electrical power systems have been early adopters of SCADA systems for their operations, making them one of the earliest cases of cyber-physical systems. They were designed to provide voltage and current levels, circuit breaker status information and other field related indicators in a real-time to identify problems as they occur and to take corrective actions when assistance is needed as an attempt to prevent significant system failures. In electrical power systems, SCADA is used to remote control and monitor the flow of electricity from generators to customer premises and factories through transmission and distribution subsystems. SCADA systems enable an efficient power production and distribution of electric systems through the use of automated data collection and equipment control (Spellman, 2016). It improves the overall efficiency of the system for optimising, supervising and controlling the generation and transmission systems. SCADA function in the power system network provides greater system reliability and stability for integrated grid operation.

The architecture of electrical power SCADA system can be envisaged as three main areas as shown in Fig. 1. At the field devices area; sensors, relays and actuators provide an interface for control and monitoring of the physical

process. Remote Terminal Unit (RTU) and Programmable Logic Controllers (PLC) are also reside in this area where they aggregate control (acting as master) for many field devices by passing commands and responses through the communications network to the SCADA server. On the other side, a dedicated control centre to govern the entire control and monitor process. The control centre commonly consists of SCADA application servers for process monitoring and control, database servers for historical record storage and in some cases interoperability servers for interconnecting SCADA software and hardware from different vendors. Moreover, the system's operator monitors the process state through Human-machine Interface (HMI) and controls the process by activating commands as required.

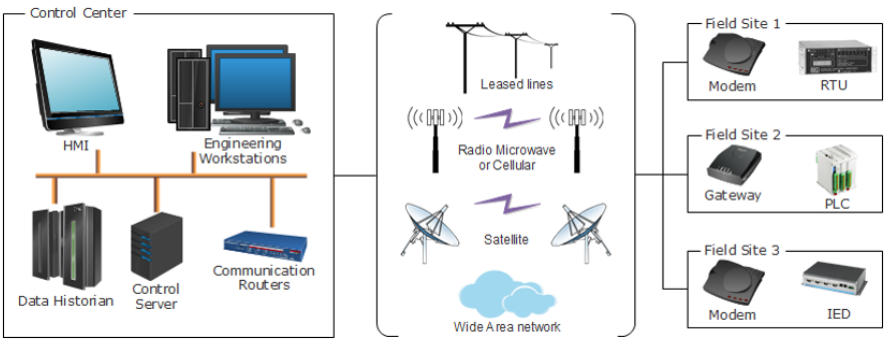

Figure 1: General architecture of a SCADA system

Generally, SCADA system could have multiple supervisory systems, PLCs, RTUs, HMIs, process and control instrumentation, sensors and actuator devices over a large geographical area, interconnected through a communications network. The communication network is intended to provide the means by which data can be transferred between the main control centre and field sites. Historically, SCADA networks have been isolated from other networks through the use of dedicated communication links and proprietary communication protocols (Stouffer et al., 2008). However, with the increased deployment of geographically distributed substations and economical consideration, SCADA systems are becoming increasingly interconnected, rapidly adapt internet enabled devices as well as open communication standards to significantly reduce infrastructure costs and increase ease of maintenance and inte-

gration (Urias et al., 2012), (Chalamasetty et al., 2016). Moreover, for better decision making and provide real-time updates utility companies have integrating their SCADA network with their enterprise networks (such as business and corporate networks) to streamline operations (Sridhar et al., 2012). Consequently, SCADA systems have to face different types of vulnerabilities and threats that are associated with cyber and physical devices, software as well as communication and control protocols (Singh, 2013). Therefore, identifying the vulnerabilities and threats and protecting SCADA systems is of vital importance.

3 RELATED WORKS

As mentioned in previous sections, the security of SCADA system is a critical issue. Therefore, the SCADA system has to be tested thoroughly for security related faults, vulnerabilities and loopholes. However, conducting security tests such as vulnerability and penetration testing on a production system is technically difficult to audit without compromising and/or impact its reliability and performance (Poudel et al., 2017). Therefore, security researchers attempt to clone the SCADA systems in isolated environments where experiments can safely be performed. SCADA testbed allows cyber-security researchers and system engineers to at first investigate cyber-security vulnerabilities on functional control systems, then implement exploits to attack the systems in the testbed to understand the implications of the vulnerability. In this section, relevant published literature in terms of SCADA simulation and testbed implementation for SCADA cyber-security research is surveyed. Table 1 illustrates a summary of the reviewed related works.

Several SCADA testbeds have been developed at various entities such as national labs, universities and research centres for purpose of studying the consequences associated with these cyber-physical threats and mitigate those consequences. At the national laboratories level, the Department of Energy, US, in 2003 has established a SCADA testbed at Idaho National Laboratory called National SCADA testbed (Ralston et al., 2007) and (Idaho National Laboratory, 2011), it aims to provide testing, research and training facilities to help improve the security of SCADA control systems.

Testbed	Sponsor	Approach	Location	Aim
National SCADA Testbed	U.S. Department of Energy	Physical replication	Idaho National Lab. U.S.	To provide testing, research and training facilities.
Sandia National SCADA Testbed	U.S. Department of Energy	Simulation	Sandia National Lab. U.S.	To discover critical vulnerabilities and threats to the energy sector.
TASSAS	University of Arizona	Simulation	University of Arizona, U.S.	To implement and test an anomaly-based intrusion detection system.
SCADA Security Lab.	Mississippi State University	Simulation and HIL	Mississippi State University, U.S.	To simulate common power system contingencies.
SCADASim	Royal Melbourne Institute of Technology University	Simulation	Royal Melbourne Institute of Technology University	To analyse the impact of malicious attacks on power system.
Cyber-Physical Security Testbed	University College Dublin	Simulation	University Collage Dublin	To analyse the impact of malicious attacks.
SCADA Testbed for Security Analysis	Department of Energy, US	Simulation	Washington State University	To simulate man-in-the-middle and denial-of-service attacks.
HIL based SCADA Testbed	South Dakota State University	Virtualization	South Dakota State University	To study the cyber security and voltage stability control of power grid.

Table 1: Summary of reviewed SCADA testbed implementations

Another effort developed by a national lab is by Sandia National Laboratory (Parks, 2007) which uses hybrid modelling and simulation architecture in order to understand the possible impact of particular cyber threats, cyber defence training and exploring power system vulnerabilities. Comparable efforts have been made by Universities and research laboratories in the design and deployment of a realistic and reliable SCADA testbed for various applications especially in electrical power control system. For instance, a SCADA testbed has been developed at University of Arizona using PowerWorld simulation tool to simulate the operations of large scale power distribution systems to implement and test an anomaly-based intrusion detection system (Mallouhi et al., 2011).

Another SCADA testbed example is implemented at power and energy research laboratory of Mississippi State University (Adhikari et al., 2012). The testbed was used for simulation of common power system contingencies (generator loss, transmission loss and sudden load loss), and event detection using data mining of phasor measurement unit data. Similarly, at Royal Melbourne Institute of Technology University, a SCADA testbed has been developed for building SCADA simulations which support combination of network simulation and real device connectivity (Queiroz et al., 2011).

Furthermore, University College Dublin have implemented a SCADA testbed for cyber-security practices using computer networks and power grids simulators (Stefanov and Liu, 2014). The testbed provides a tool for analysing cyber-physical vulnerabilities, allows monitoring of the dynamic behaviour of power system as response to cyber-attacks (impact analysis), and mitigation of cyber-attacks. The simulations of cyberattack were performed with IEEE 39-bus system and three attack scenarios including unauthorised access to control assets such as RTUs and Intelligent Electronic Devices (IEDs), denial of service by flooding the SCADA network, man-in-the-middle by modifying packets carrying measurements and control commands, configuration change of protective relays.

One more SCADA testbed for cyber-security analysis was developed at Washington State University (Liu et al., 2015). The developed testbed was used to study the impact of three types of real-life cyber-attacks on IEEE 14-bus test system controlled by SCADA. The testbed was designed using an inte-

grated cyber-power modelling and simulation tools such that a real-time modelling of end-to-end cyber-power systems have been developed with hardware-in-the-loop capabilities. Real-time digital simulator, synchro-phasor devices, DeterLab, and network simulator-3 (NS-3) were utilised. The testbed was used to simulate Man-in-the-middle and denial-of-service attacks which were modelled in DeterLab.

Recently, a real-time hardware-in-the-loop based SCADA testbed were developed at South Dakota State University, US (Poudel et al., 2017). The testbed was developed to study the cyber-security and voltage stability control of power grid SCADA systems. The testbed utilises SEL-351S protection system with OPAL-RT including control functions and communications to build a cyber-physical environment. The study presented two different mitigation strategies using optimal power flow for system reconfiguration in order to restore normal or next steady state operating condition after failures. Additionally, different reconfiguration plans were presented for avoiding the cascading failures following any kind of cyber-attack.

4 SCADA TESTBED REQUIREMENTS

A trustworthy and accurate simulation results require a testbed that is able to reproduce the real system as accurately as possible. The fidelity concept defined by Siaterlis and Genge (2012) ensures the implementation of an adjustable level of realistic SCADA testbed through the use of real hardware devices when its really required rather than emulators, simulators or other abstraction methods. Another key requirement for a reliable testbed design is repeatability (Gao et al., 2013). This requirement reflects the need to repeat the experiment and to obtain the same or statistically consistent results. Prior to conducting the experiment, the researcher has to define clearly and in-detail the experiments initial and final states as well as all events in between the two states. According to Hahn et al. (2010), a reliable testbed requires accurate measurements; an accurate conduct of experiment should be maintained. In other words, researchers should not interfere with the experiment in such a way that they might alter the experiments outcome.

Requirement	Description
Fidelity	Reproduced as accurately as possible the real system under study
Repeatability	Redundant assessments show similar or statistically consistent outcomes.
Measurement accuracy	Assessments should not interfere with the outcome.
Reconfigurable	The combination ofsoftware flexibility with the high performance of hardware offers very flexible and high-speed computing fabrics.
Safe execution of tests	Cybersecurity evaluations commonly embed adversaries that exploit systems with malicious software. As determining the outcomes of the activities at prior may be challenging, the evaluations must ascertain that the activities in the testbed are isolated.

Table 2: SCADA testbed requirements

Safe execution of tests is another requirement defined by Siaterlis and Genge (2014) and has been a focus area for most of the testbeds intended for cyber-security exercise Holm et al. (2015). In most of the cases, the experiments for cyber-security exercise assume the presence of an adversary who utilises malicious software and injects malicious code and command or traffic into the testbed to reach the desired goal. The effect of these activities can be unpredictable as it is difficult to predict the outcome of these activities beforehand which may have disruptive effects on physical systems. Such cases need to be carried out in an isolated and controlled environment to ensure the safety of physical devices as well as to protect security researchers from potential danger resulting from simulating an attack or executing a malicious activity. Qassim et al. (2019) have summarized the five important needs that a cybersecurity testbed should fulfil, as listed in Table 2.

In the previous work by Qassim et al. (2017), several SCADA testbed implementation approaches were evaluated based on the SCADA testbed requirements. The study showed that, to address the given requirements and to come

up with a realistic testbed for cyber-security exercise, SCADA testbed should utilise a combination of both virtualisation and physical replication in a hybrid environment that ensures a high degree of fidelity. Therefore, virtual-physical replication is used to overcome the limitations of both virtualisation and physical replication approaches.

5 IMPLEMENTATION OF THE PROPOSED SCADA TESTBED

This section describes the architecture of the proposed electrical power SCADA testbed. The experimental setup is as shown in Fig. 2. It includes several SCADA key components such as real-time digital simulator to emulate the power system, master and local HMI for monitoring and control, an RTU to control the emulated physical system and several engineering workstations for testing and analysis purposes. As illustrated in Fig. 2, four functional levels (or zones) have been considered in the design of our SCADA testbed, which are: process, bay, communication and stations levels. The functional levels denote for the hierarchical levels of power system management based on IEC-62264 reference model for industrial communication networks. The following subsections highlight the testbed components at the different functional levels.

5.1 Implementation of process level

In this testbed, OPAL-RT model OP5600 is used to simulate the electrical power system. OPAL-RT is a versatile and high-performance real-time digital simulator; it is a platform equipped with analoge and digital I/O that provides the capability to perform real-time experiments by interfacing with real hardware devices such as RTUs, IEDs and protection relays. In demonstrating this testbed, the IEEE 39-bus electrical network test system is used to validate the implemented testbed and provide a meaningful example for other researches, experiments and applications of this infrastructure. The IEEE 39-bus electrical network is simulated by OPAL-RT to offer a real-time response and feedback. The IEEE 39-bus network consists of 10-generators, and 46-transmission lines

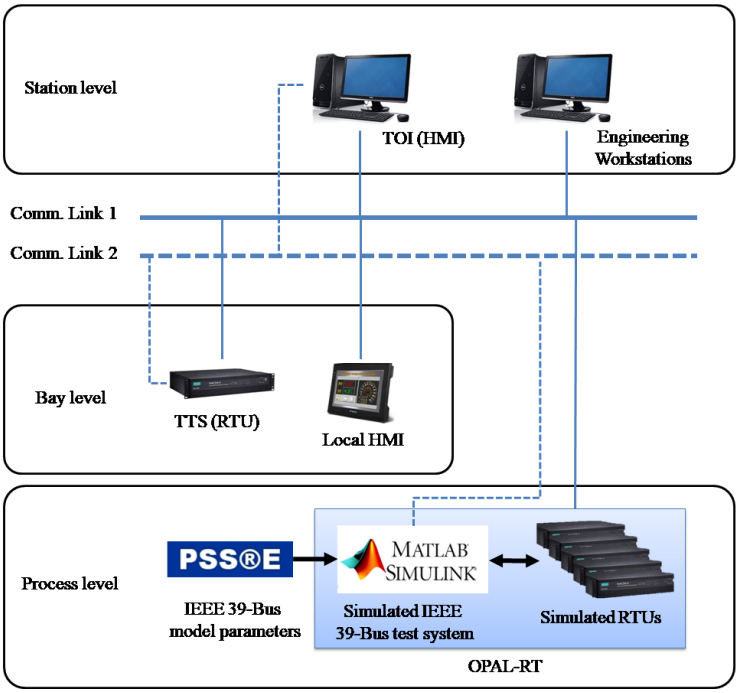

Figure 2: The implemented SCADA testbed

as shown in Fig. 3. This particular network is chosen because it is a standard based network used by power system researchers all over the world and serves as a benchmark in result comparison. The electrical network is modelled in Power System Simulator for Engineering (PSS/E or PSSE) software to obtain a simulation parameters to be loaded into MathWorks Simulink software application.

PSS/E is a software tool used by power system engineers to simulate electrical transmission networks in steady-state conditions as well as over timescales of a few seconds to tens of seconds. PSS/E is used by most power system utilities around the world to run and test their power system network. It has the ability to run from basic power flow simulations right up to complex dynamic simulations. However, the software requires huge computing power to run large scale dynamic simulations. Hence the reason why OPAL-RT was cho-

sen as the computing engine to enable this. For the IEEE 39-Bus network to run in the OPAL-RT environment, the configuration files are loaded up into the OPAL-RT Solver which is integrated with MathWorks Simulink software application. The OPAL-RT Solver serves as the engine to run the power system network. Since OPAL-RT is configured to run on multiple processors, this enables it to run the real-time digital simulation with ease.

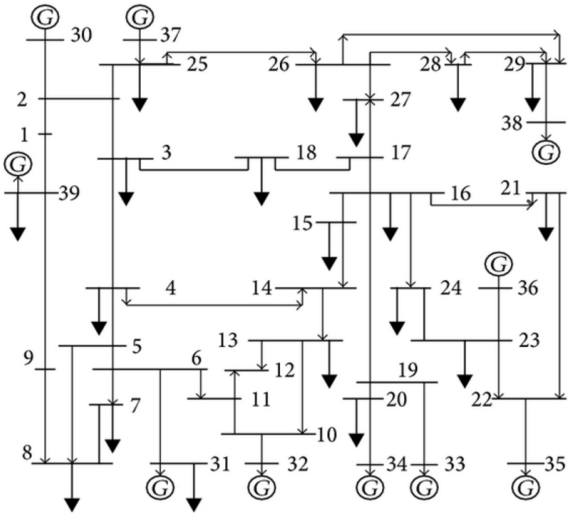

Figure 3: IEEE 39-bus test system network

5.2 Implementation of bay level

For the SCADA testbed, a new proprietary software application were developed called Tenaga Terminal Simulator (TTS). The TTS is used for modelling and simulating an industrial control system device such as an RTU. Instead of having a physical RTU to be attached to the testbed, the RTU will be replaced with the TTS software which can produce data as if it is an RTU. At the heart of the TTS architecture is a Real-time Database (RTDB), which is an in-memory, event-driven, real-time database. The RTDB can run on any Portable Operating System Interface (POSIX) compliant operating system. RTDB consists of

freely configurable tag items that can be associated with different drivers for communication and applications usage. Among the communication protocols supported by RTDB are:

- C37.118 (for communication with synchro-phasor)
- IEC 60870-5-101 (for communication with SCADA devices such as RTU)
- IEC 60870-5-104 (for communication with SCADA devices such as RTU over TCP/IP network)
- IEC 61850 (for communication with IEDs in substation automation environment)

5.3 Implementation of communication link

The communication network for controlling and monitoring the power system, namely the SCADA network has to be simulated as close as possible to the real substation SCADA network. In this work, the SCADA testbed was designed to simulate the IEC-60870-5-104. IEC 60870-5-104 (also known as IEC104) is one of the IEC 60870 set of international standards released by the IEC (International Electrotechnical Commission) which define systems used for tele-control in electrical engineering and electrical power system automation applications (Chalamasetty et al., 2016). It specifies a communication profile for sending basic tele-control messages between two systems over standard TCP/IP network. The usage of TCP/IP network offers simultaneous data transmission between several devices and services. Apart from this, the security of IEC 60870-5-104 has been proven to be problematic, according to recent security advisories (Ralston et al., 2007) and (Idaho National Laboratory, 2011), multiple issues in this protocol such as the lack of proper data encryption could allow an unauthenticated, remote attacker to spoof network communications or exploit input validation flaws on vulnerable systems using the affected protocol. IEC has published a security standard (IEC 62351), the security of IEC tele-control protocol series that implements authentication of data transfer and end-to-end data encryption. The implementation of IEC 62351 would prevent

common cyber-attacks such as replay, man-in-the-middle and packet injection attacks. However, due to the increase in complexity and the limited processing capabilities of existing SCADA devices, vendors are reluctant to employ these countermeasures on their devices and/or networks.

5.4 Implementation of station level

At the station level, a web-based application platform have been developed to simulate the function of a SCADA HMI. Tenaga Operator Interface (TOI) is the codename of our HMI software application. TOI is a real time interface system that collects and displays information about power system parameters to the substation operators. It also offers control capability whereby immediate action can be taken should there be anomalies detected in the power system. TOI provides various communication ports for fast communication and convenient control of a diverse range of machines, systems and facilities. The TOI was developed for real-time visualisation and control of power system network. Warning alarms can be visualised in dynamic symbols or retrieved in tabular format. TOI increases operational awareness of substation operators in a manned substation allowing pre-emptive corrections to be performed to avert catastrophe. TOI complements the SCADA network control centres capability by monitoring operations of substation equipment remotely as well as locally.

5.5 Simulation process

The integration of OPAL-RT, TOI and TTS, which involves ensuring data are communicated properly between all three systems, is tested by simulating a case following these steps: The IEEE 39-bus model is loaded into OPAL-RT.

1. Once the loading and initialization process is successful, simulation is executed which will generate all the system parameters reflecting the power system condition.
2. These parameters are then sent to TTS and TOI machine via TCP/IP protocol.

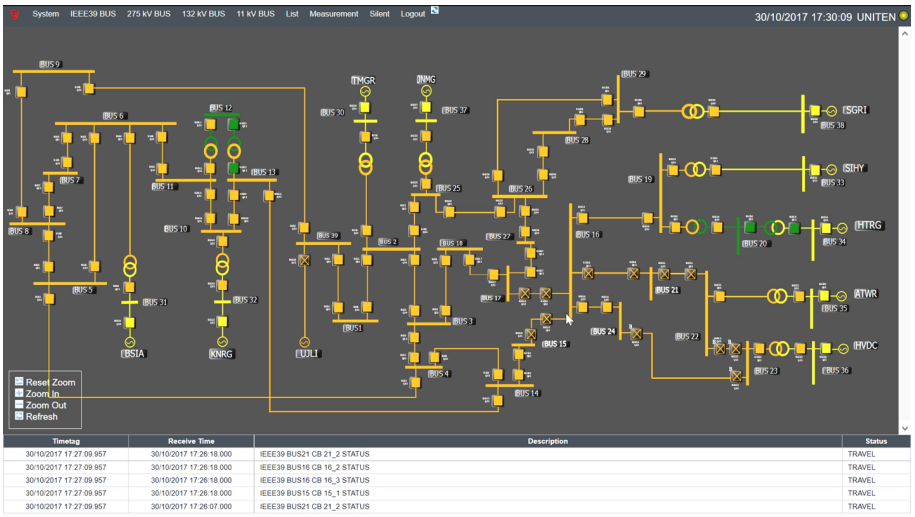

Figure 4: Tenaga operator interface

3. The Tenaga operator interface will show the status of the power system i.e. breaker open, breaker close and the analog parameters such as voltage, frequency etc.

4. Any changes made either in OPAL-RT itself, or through system control in TOI, or external injected data via TTS will be reflected in TOI display and OPAL-RT console. For example, if the breaker is closed, the box in Figure 4 at the affected bus will turn to empty box, highlighted box or crossed-box to notify status of open, closed and traveling (error status), respectively.

6 CONCLUSION

The proposed testbed in this work offers highest fidelity and accuracy. This is because the real-time simulator offers an excellent representation of the actual power system with the support of a reconfigurable environment. Moreover, the testbed has been designed to host several substations to accurately model the

scale of real electric power grid system. An operator shall control the emulated substations from separate computer system through Ethernet based network to mimic real SCADA system implementation.

The proposed testbed supports a wide range of experimental applications such as security related studies including vulnerability assessment, risk analysis, cyber-security evaluation and digital forensic investigation as well as other control related applications. This is due to the scalability feature of the proposed testbed environment. The proposed testbed also supports repeatability in order to obtain the same or statistically similar results. A researcher/tester could easily reproduce a previously tested experiment since the initial state and set up of the testbed environment is fixed at the start of each simulation and is a user-defined choice. In addition to the power system security, the proposed testbed is capable of conducting control experiments in real time. Therefore, it is a valuable tool for simulating different events in the realistic cyber-physical environment. In future works, the implemented testbed will be used to demonstrate the impact of the cyber-attack on the physical power grid in terms of voltage stability and loss of generation.

ACKNOWLEDGMENTS

This research study is supported by Ministry of Science, Technology and Innovation, Malaysia through DSTIN project 2016-2018.

REFERENCES

Adhikari, U., Morris, T. H., Dahal, N., Pan, S., King, R. L., Younan, N. H., and Madani, V. (2012). Development of power system test bed for data mining of synchrophasors data, cyber-attack and relay testing in RTDS. In *2012 IEEE Power and Energy Society General Meeting*, pages 1–7, San Diego, CA, USA. IEEE.

Ani, U. P. D., He, H. M., and Tiwari, A. (2017). Review of cybersecurity issues

in industrial critical infrastructure: manufacturing in perspective. *Journal of Cyber Security Technology*, 1(1):32–74.

Baalbaki, B. A., Al-Nashif, Y., Hariri, S., and Kelly, D. (2013). Autonomic Critical Infrastructure Protection (ACIP) system. *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*.

Chalamasetty, G. K., Mandal, P., and Tzu-Liang Tseng (2016). Secure SCADA communication network for detecting and preventing cyber-attacks on power systems. In *2016 Clemson University Power Systems Conference (PSC)*, pages 1–7. IEEE.

Gao, H., Peng, Y., Jia, K., Dai, Z., and Wang, T. (2013). The design of ICS testbed based on emulation, physical, and simulation (EPS-ICS Testbed). *Proceedings - 2013 9th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP 2013*, pages 420–423.

Hahn, A., Kregel, B., Govindarasu, M., Fitzpatrick, J., Adnan, R., Sridhar, S., and Higdon, M. (2010). Development of the PowerCyber SCADA security testbed. *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research - CSIIRW '10*, page 1.

He, H. and Yan, J. (2016). Cyber-physical attacks and defences in the smart grid: a survey. *IET Cyber-Physical Systems: Theory & Applications*, 1(1):13–27.

Holm, H., Karresand, M., Vidström, A., and Westring, E. (2015). A Survey of Industrial Control System Testbeds. In Buchegger, S. and Dam, M., editors, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 9417, pages 11–26. Springer.

Idaho National Laboratory (2011). Vulnerability Analysis of Energy Delivery Control Systems (Report No. INL/EXT-10-18381). Technical report, Idaho National Laboratory, Idaho Falls, Idaho.

Karnouskos, S. (2010). Stuxnet Worm Impact on Industrial Cyber-Physical System Security. In *IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society*, pages 4490–4494.

Krotofil, M. and Gollmann, D. (2013). Industrial control systems security: What is happening? In *2013 11th IEEE International Conference on Industrial Informatics (INDIN)*, pages 664–669. IEEE.

Lee, R. M., Assante, M. J., and Conway, T. (2014). German Steel Mill Cyber Attack. Technical report, SANS Industrial Control Systems.

Liang, G., Weller, S. R., Zhao, J., Luo, F., and Dong, Z. Y. (2017). The 2015 Ukraine Blackout: Implications for False Data Injection Attacks. *IEEE Transactions on Power Systems*, 32(4):3317–3318.

Lin, C.-T., Wu, S.-L., and Lee, M.-L. (2017). Cyber attack and defense on industry control systems. In *2017 IEEE Conference on Dependable and Secure Computing*, pages 524–526. IEEE.

Liu, R., Vellaithurai, C., Biswas, S. S., Gamage, T. T., and Srivastava, A. K. (2015). Analyzing the Cyber-Physical Impact of Cyber Events on the Power Grid. *IEEE Transactions on Smart Grid*, 6(5):2444–2453.

Mallouhi, M., Al-Nashif, Y., Cox, D., Chadaga, T., and Hariri, S. (2011). A testbed for analyzing security of SCADA control systems (TASSCS). *IEEE PES Innovative Smart Grid Technologies Conference Europe, ISGT Europe*, pages 1–7.

Maynard, P., McLaughlin, K., and Haberler, B. (2014). Towards Understanding Man-In-The-Middle Attacks on IEC 60870-5-104 SCADA Networks. In *2nd International Symposium for ICS & SCADA Cyber Security Research 2014*. BCS Learning & Development.

Miller, B. and Rowe, D. (2012). A survey SCADA of and critical infrastructure incidents. In *Proceedings of the 1st Annual conference on Research in information technology - RIIT '12*, page 51.

Nazir, S., Patel, S., and Patel, D. (2017). Assessing and augmenting SCADA cyber security: A survey of techniques. *Computers & Security*, 70:436–454.

Parks, R. C. (2007). Guide to Critical Infrastructure Protection Cyber Vulnerability Assessment (Report No. SAND2007-7328). Technical report, Sandia National Laboratories, Albuquerque, New Mexico: Sandia National Laboratories.

Pidikiti, D. S., Kalluri, R., Kumar, R. K. S., and Bindhumadhava, B. S. (2013). SCADA communication protocols: vulnerabilities, attacks and possible mitigations. *CSI Transactions on ICT*, 1(2):135–141.

Poudel, S., Ni, Z., and Malla, N. (2017). Real-time cyber physical system testbed for power system security and control. *International Journal of Electrical Power & Energy Systems*, 90:124–133.

Qassim, Q., Jamil, N., Daud, M., and Hasan, H. C. (2019). Towards implementing Scalable and Reconfigurable SCADA Security Testbed in Power System Environment. *International Journal of Critical Infrastructures*, 15(2).

Qassim, Q., Jamil, N., Zainal Abidin, I., Ezanee Rusli, M., Yussof, S., Ismail, R., Abdullah, F., Ja'afar, N., Che Hasan, H., and Daud, M. (2017). A Survey of SCADA Testbed Implementation Approaches. *Indian Journal of Science and Technology*, 10(26):1–8.

Queiroz, C., Mahmood, A., and Tari, Z. (2011). SCADASimA framework for building SCADA simulations. *IEEE Transactions on Smart Grid*, 2(4):589–597.

Ralston, P., Graham, J., and Hieb, J. (2007). Cyber security risk assessment for SCADA and DCS networks. *ISA Transactions*, 46(4):583–594.

Ramachandruni, R. S. and Poornachandran, P. (2015). Detecting the network attack vectors on SCADA systems. *2015 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2015*, pages 707–712.

Siaterlis, C. and Genge, B. (2012). Cyber-Physical Testbeds : Scientific Instruments for Cyber Security Assessment of Critical Infrastructures. *Communications of the ACM*.

Siaterlis, C. and Genge, B. (2014). Cyber-physical testbeds. *Communications of the ACM*, 57(6):64–73.

Singh, H. P. (2013). Cyber security trend in Substation Network for automation and control Systems. *2013 IEEE International Conference on Computational Intelligence and Computing Research, IEEE ICCIC 2013*, pages 0–2.

Singh, P., Garg, S., Kumar, V., and Saquib, Z. (2015). A testbed for SCADA cyber security and intrusion detection. In *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, pages 1–6. IEEE.

Spellman, F. R. (2016). *Energy Infrastructure Protection and Homeland Security*. Bernan Press.

Sridhar, S., Hahn, A., and Govindarasu, M. (2012). Cyber attack-resilient control for smart grid. *2012 IEEE PES Innovative Smart Grid Technologies, ISGT 2012*, pages 1–3.

Stefanov, A. and Liu, C.-C. (2014). Cyber-Physical System Security and Impact Analysis. *IFAC Proceedings Volumes*, 47(3):11238–11243.

Stefanov, A., Liu, C.-C., Govindarasu, M., and Wu, S.-S. (2015). SCADA modeling for performance and vulnerability assessment of integrated cyber-physical systems. *International Transactions on Electrical Energy Systems*, 25(3):498–519.

Stoian, I., Ignat, S., Capatina, D., and Ghiran, O. (2014). Security and intrusion detection on critical SCADA systems for water management. *2014 IEEE International Conference on Automation, Quality and Testing, Robotics*, pages 1–6.

Stouffer, K., Falco, J., and Kent, K. (2008). Guide to Industrial Control Systems (ICS) Security Recommendations of the National Institute of Standards and Technology. *Nist Special Publication*, 800(82).

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., and Hahn, A. (2015). Guide to Industrial Control Systems (ICS) Security. Technical report, National Institute of Standards and Technology, Gaithersburg, MD.

Tawde, R., Nivangune, A., and Sankhe, M. (2015). Cyber security in smart grid SCADA automation systems. In *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, pages 1–5. IEEE.

Urias, V., Van Leeuwen, B., and Richardson, B. (2012). Supervisory Command and Data Acquisition (SCADA) system cyber security analysis using a live, virtual, and constructive (LVC) testbed. *Proceedings - IEEE Military Communications Conference MILCOM*, pages 1–8.