ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 10(26), DOI: 10.17485/ijst/2017/v10i26/116775, July 2017* ISSN (Online) : 0974-5645

A Survey of SCADA Testbed Implementation Approaches

Qais Qassim[1], Norziana Jamil[1], Izham Zainal Abidin[1], Mohd. Ezanee Rusli[1], Salman Yussof[1], Roslan Ismail[1], Fairuz Abdullah[1], Norhamadi Ja'afar[2], Hafizah Che Hasan[2] and Maslina Daud[2]

[1]Centre for Information and Network Security Universiti Tenaga Nasional (UNITEN) Kajang – 43000, Selangor, Malaysia; qaisj3@gmail.com, norziana@uniten.edu.my, izham@uniten.edu.my, ezanee@uniten.edu.my, salman@uniten.edu.my, roslan@uniten.edu.my, fairuz@uniten.edu.my
[2]Cyber Security Malaysia Seri Kembangan – 43300, Selangor, Malaysia; norhamadi@cybersecurity.my, hafizah@cybersecurity.my, maslina@cybersecurity.my

Abstract

Objectives: SCADA systems are turning into the central nerve system of the electric power system critical infrastructure. With the increasing availability and use of computer networks and the Internet as well as the convenience of cloud computing, SCADA systems have increasingly adopted Internet-of-Things technologies to significantly reduce infrastructure costs and increase ease of maintenance and integration. However, SCADA systems are obvious targets for cyber attacks that would seek to disrupt the critical infrastructure systems thus are governed by a SCADA system. **Methods/Statistical Analysis:** Cyber attacks exploit SCADA security vulnerabilities in order to take control or disrupt the normal operation of the system. Analyzing security vulnerability and loopholes are critical in developing security solutions for such systems. It is also equally important to test security solutions developed to protect SCADA systems. **Findings:** Experimenting on live systems is generally not advisable and impractical as this may render the system unstable. Such situation calls for the need of an experimental setup equivalent or quite close to the real scenario for developing and testing security solutions. **Application/Improvements:** This paper reviews common SCADA implementation approaches utilized in previous related works.

Keywords: Cyber Attacks, Industrial Control, Power Systems, SCADA Systems, Security, Testbed

1. Introduction

Supervisory Control and Data Acquisition (SCADA) systems are widely used in electrical power generation, distribution and transmission.[1] They have been utilized to carry out and perform a wide variety of functions which are essential to the day-to-day running of the electrical power utility. These functions include load management, automatic generation and transmission control, identifying and isolating faults and restoring service, to name a few.[2] Due to the advances in telecommunication technologies and the needs for improved functionality and effectiveness with cost minimization in industrial control systems, SCADA systems have been incrementally evolved to adapt the Internet-of-Things and cloud computing technologies.[3] As a result, SCADA systems are obvious targets for cyber attacks.[4] These cyber attacks can disrupt and damage critical infrastructural operations, cause major economic losses, contaminate ecological environment and even more dangerously, claim human lives.[5]

With the constantly evolving technology and the ever-present threat of cyber attacks, tools are needed to support the early detection and timely reporting of cyber incidents. Generally, there are three countermeasures to secure and protect SCADA systems:[6] one is to identify known security incidents at the perimeter of the system using security tools such as intrusion detection systems and firewalls; the second approach is to model the normal data flows and control operations within the

* *Author for correspondence*

SCADA system to detect anomalies caused by attempts to change or damage the system; lastly, which is an essential approach, is to eliminate the vulnerabilities in the control system designs and implementations by performing technical auditing tests (e.g. penetration tests).

Analyzing security vulnerability and loopholes are essential and critical in developing and testing security solutions for such systems.[7] However, experimenting on live critical infrastructure systems is generally not advisable and impractical as this may render the system unstable.[8] Therefore, an experimental setup equivalent or quite close to the real scenario is required for development and testing of the SCADA security. To identify the assessment requirements and design needs and challenges, this work reviews commonly used testbed implementation approaches that have been proposed for scientific researches.

2. Introduction to SCADA

Supervisory Control and Data Acquisition (SCADA) systems gather and analyze data from industrial field instruments for real-time control and management. They are the core of many modern industries and critical infrastructures, including: power generation, transmission and distribution, manufacturing, oil and gas, transportation and water distribution.[9] SCADA systems improve the performance of the operation of the industrial critical system as well as provide better protection to the utilized equipment. Moreover, it improves productivity of the personnel. SCADA systems provide reliable detection and immediate alarm annunciation to the monitoring station by utilizing a certified monitoring platform, advanced communications, and a supporting array of state-of-the-art sensors.

A SCADA system encompasses the collecting of the information via a Remote Terminal Unit (RTU), transferring it back to the Master Terminal Unit (MTU), carrying out any necessary analysis and control and then displaying that information on a number of operator screens or displays namely Human Machine Interface (HMI). The required control actions are then conveyed back to the process. In the control centre, dedicated SCADA software is used to manage the field instruments' readings and graphically represent it to the user. Moreover, the SCADA software logs information about who runs reports and the data that is used. Various computer software applications are integrated with the SCADA software including billing and inventory management applications to manage corporate and business functions. Usually, data exchange among these software applications is done with software interface standards (e.g. OPC), database interaction (e.g. ODBC) or through an API.[10,11] Various data protection and recovery mechanisms are commonly used in SCADA systems such as intrusion detection systems and real time data backup to prevent interception or loss of critical telemetry data.

SCADA systems monitor and control industrial processes that exist in the physical world. SCADA systems control processes range from raising and lowering device's temperature to controlling energy-generating and distribution networks including nuclear, traffic systems and rail networks.[12] Thus, it is not hard to comprehend that the impacts of cyber attacks on these systems can be disastrous and a successful attack would be an attractive goal for both individual hackers and state-sponsored organisations. Therefore, SCADA system's security and protection are extremely important as well as of national concern. Recent cyber attacks on SCADA systems draw attention to the need of a SCADA security testbed, which can be used to model real SCADA systems in order to perform a proper vulnerability assessment and to study the effects and the consequences of SCADA cyber-attacks.[13]

The U. S. National Institute of Standards and Technology (NIST) had suggested a set of guidelines in carrying out security assessment on SCADA systems.[14] It is recommended that, a SCADA testbed should consider four general areas: the control centre, the communication architecture, the field devices and the physical process itself to understand and manage the complexity of SCADA systems and to identify the security vulnerabilities. Therefore, this paper broadly divided the SCADA system into four functional interconnected layers: process layer, bay layer, communication layer, and station layer. Figure 1 illustrates a general architecture of SCADA system and its components.[15] Modelling SCADA system as a layered structure is beneficial in identifying possible threats and the source of cyber attacks based on each level. The functional layers are also advantageous in proposing and developing SCADA security testbed, as each layer can be modelled separately.

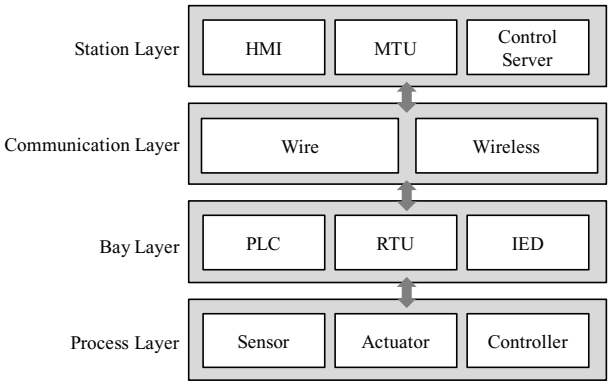

Figure 1. General architecture of a SCADA system.[13]

SCADA's station layer includes the functions involved in monitoring and controlling the physical process, general deployment of services such as HMI, control station and historian.[12] The communication layer includes the physical communication networks which may be wired or wireless. Wired networks may use leased lines, category 5 or 6 cables, serial cables, and/or fiber-optic cables.[16] Wireless networks may use standardized communication systems such as IEEE 802.11 or may include very long distance solutions such as satellite and microwave links. Beyond the physical components, this layer also encompasses network protocols such as TCP/IP. On the other hand, the bay layer comprises of process control devices and protocols which gathers data from all the process level devices and provides the data to the station layer. There are many standards for SCADA communication including MODBUS, Distributed Network Protocol Version 3 (DNP3) and IEC60870-5-101.[17] Finally, process level is the actual physical process. It includes the sensors, actuators, and controlled process/controlled object directly connected to the process and process equipment.

3. SCADA Assessment Approaches

In this work, existing SCADA assessment approaches have been reviewed to identify the current state-of-the-art and explore existing challenges to establish a set of requirements in constructing improved SCADA platform for cyber security assessment. Generally, performing vulnerability assessment and security evaluation on a running SCADA system is technically difficult to audit without compromising its reliability and performance.[18] Therefore, security and electrical engineering researchers attempt to clone the SCADA systems in isolated environments, also called testbeds, where experiments can safely be performed.[19] However, constructing a SCADA testbed is a challenge and tedious process even with the aid of the advanced modern computing technologies; it can be difficult to obtain a realistic testbed scale and configuration.[12] The review of existing SCADA testbed implementations has identified a number of approaches that can be categorized into: physical replication, simulated testbed constructed by modelling technologies, virtualized testbed constructed by emulation technologies and virtual-physical replication (hardware-in-the-loop).[14] The identified approaches were originally used to implement one or more SCADA layers illustrated in Figure 1.

3.1 Physical Replication Testbed

Physical replication testbed is an experimental environment developed based on replicating the existing SCADA system and the industrial utility. It represents a clone of the real system with identical devices and information systems. The National SCADA Testbed (NSTB) implemented by the United States department of energy is one of the well known examples of physical replication testbed.[20] Carrying out a penetration test and evaluate existing vulnerabilities and loopholes on an identical replica of a real-world system provides the highest degree of fidelity.[21] However, it is difficult to reconfigure and maintain real hardware and software in a testbed, especially given the presence of software exploits that have the potential to damage the systems; not to mention establishing a valid testbed scale due to the costs involved.[19]

The national SCADA testbed implemented in Idaho National Labs (INL) is a large scale SCADA testbed developed for cyber security assessment, communication standards improvement and training.[22] The testbed include a full scale electrical power grid having a 61 mile 128KV transmission loop, 13.8KV distribution lines, and seven substations with more than 3000 monitoring and control points in the system. At the communication level, the testbed supports various network and industrial protocols such as IP, ATM, 802.11, GSM as well as ICCP, MODBUS, DNP3. Moreover, it supports testing of firewalls and virtual private networks. The National SCADA Testbed

was the experimental tool to identify taxonomies of common industrial control vulnerabilities and security assessments controls reported in the presented article.[23]

3.2 Software Simulated Testbed

An alternative to physical replication is to employ computer software simulation through modelling the existing system to develop a software-based experimental environment, that provides similar functions and behaviours of SCADA system.[2] Generally, simulation models are easy to reconfigure, maintain and can provide an extensive testbed scale.[24] However, it is difficult to obtain high fidelity from simulation models, especially when software exploits and cyber attacks need to be considered.[25] This is because software simulators effectively model computer networks in their normal operations but incapable to capture the way computer networks fail.[26]

An example of software based simulated testbed is presented in the presented article.[2] The study has introduced SCADASim, a framework for building SCADA simulations. The SCADASim framework developed at the Royal Melbourne Institute of Technology, Melbourne, Australia, provides predefined modules for building SCADA simulations, employing the OMNET++ discrete event simulation engine to recreate typical SCADA components while providing an underlying inter-model communications layer. In the presented article a model of electric power system has presented by integrating the PowerWorld simulator, simulated network clients, simulated control and power system measurement information, and the Real-time Immersive Network Simulation Environment for Network Security Exercises (RINSE) to simulate network traffic and cyber security attacks.[27] The PowerWorld simulation tool is a commercially available application for simulating the operations of large scale power distribution systems.[27] The study demonstrated three attack scenarios and showed the vulnerability of the network client to a DDOS attack and the ability of filtering to mitigate the attacks where the attacks have prevented data from being transmitted across the network, causing the control display to display incorrect data.

Another example of integrating PowerWorld simulator and RINSE is presented in the article.[28] The study presented a simulation-based SCADA testbed dedicated for cyber security analysis. PowerWorld was used to model the electric generation, transmission, and load while the RINSE network simulator was used to simulate the control network and configured to simulate DNP3 over TCP protocol.

3.3 Virtualization Testbed

Virtualization is the concept of executing software in an environment that minimizes or eliminates the software's dependence on the hardware on which it runs.[29] To overcome the limitations presented by the physical replication and software simulation, the virtualization technique turn out to be advantageous in developing SCADA testbeds for security purposes.[10] Virtualization is a technology which concerns isolating computer software in a means that enables layers of abstraction between software and hardware.[25] Generally, virtualization technique provides an easy way to configuring systems' components and network links and devices using software scripts; it also isolates activities in the testbed from the physical systems as well as external systems.[19,30]Usually multiple systems are configured and operated from a single computer hardware using actual software and protocols rather than simulated equivalents. Virtualization of SCADA system potentially allow large-scale realistic testbeds with low-cost, replicable and reliable vulnerability assessment and cyber threat identifications as well as execute live cyber attacks to identify security weaknesses and study potential effect.[30] Virtual systems can be simpler to develop and have practically no maintenance costs. Scaling of a virtualized system, altering or adding new features does not require much effort.

An example of virtual SCADA testbed is presented in the article.[24] The study have presented a virtualization-based SCADA testbed designed to assist in the development of innovative security and protection techniques for SCADA based control systems against a wide range of cyber attacks. The developed testbed consists of simulated electrical grid, HMI, PLC, communication networks (include process control network, demilitarized zone network and corporate network) and an anomaly intrusion detection system to detect and protect against any cyber attack that can be lunched on SCADA systems and their networks. The testbed uses the PowerWorld simulation system to simulate the operations of segments of the electrical power grid, OPNET tool to simulate computer networks, and MODBUS client and server to

simulate HMI and PLC respectively. The historian server has been located within the demilitarized zone network to collect data from various devices in SCADA network and logs to a database.

The PowerWorld tool has been used to simulate the impacts of cyber attacks on the operations of the electrical grid. The PLC is simulated using MODBUS Server that is interfaced with the power grid simulator using SimAuto application and to the control network through an Ethernet modem. The control network is simulated using OPNET modeller that simulates the large scale wide area network that interfaces the HMI to the control process over TCP/IP protocol.

Another example of virtual SCADA testbed is presented in the article.[10] The proposed SCADA testbed considered virtualization of all the real hardware devices using software, and model the main behaviour of all the field devices to maintain the re-configurability, standardization and scalability. The authors have divided the SCADA system into four parts: HMI, Communication protocols, SCADA master server and field sensors. The entire platform was run on a computer running 64-bit version of Windows 7/Windows 8. iFix was used as HMI of the Virtual SCADA infrastructure. iFix is a software package developed by General Electric that offers a robust SCADA engine, rich set of connectivity options, open architecture, and a highly scalable and distributed networking model. MatrikonOPC Server was used as a SCADA master control server. The relational database capability of iFix (HMI) that works with MatrikonOPC software allows them to exchange readings. The design structure allows iFix to receive information from the MatrikonOPC server running on a central server, and then display this information on the iFix GUI. Power System Simulator for Engineering (PSS/E) software was used to simulate the power system. PSS/E is a power system software package designed by Siemens, which provides both steady state and dynamic power system simulations.

3.4 Virtual-Physical Replication (Hardware-in-the-Loop)

In Hardware-In-the-Loop (HIL) emulation technique, either the physical part of a machine or the entire critical infrastructure can be replaced by a computer-model in real-time emulation.[8] In other words, HIL components simulate portions of the environment which the SCADA systems are designed to control. This approach provides cost-cutting measure for the design and testing of a wide variety of systems including power system control. The HIL approach offers a superior solution to test critical infrastructure systems with a virtualized model prior the integration of the untested system into the physical environment. HIL usually involves connecting control devices (e.g. PLCs or RTUs) with data acquisition and control components.

HIL control systems have a number of advantages compared to simulated and virtual systems. Typically, the measurement data is more realistic and reflect the data that would be found in an actual process control system.[31] Moreover, the communication patterns and latencies will be more accurate and not vulnerable to inaccuracies in simulated variables like OS scheduling load.[30] From the cyber attack perspectives, vulnerability analysis and behaviour-based monitoring are more feasible than simulated testbed.

In recent research activities, real-time emulators with the capability of HIL have been widely used to facilitate developing cost efficient, reliable and safe laboratory experiments. OPAL-RT devices are the most common digital simulator used for such purposes.[32] It provides power system real-time simulation platforms that meet the power system requirements. An example of virtual-physical testbed is presented in the article, the study have presented an HIL SCADA testbed developed at USF Smart Grid Power System lab.[8] The testbed was constructed to test energy management schemes, power grid cyber attack detection and prevention strategies. On the process level, phasor management units were used to capture data from real smart grid system as well as a simulated power network in Opal-TR's real time simulator. PI-system have been used for real-time data management and visualization.[33]

3.5 Hybrid Testbed

To overcome the disadvantages of existing SCADA assessment approaches stated earlier, recent SCADA security researchers have introduced a new approach for testbed development which enables the creation of a SCADA system using simulated, virtualized, emulated and physical devices in a single hybrid experiment.[12] In this approach, SCADA components have either been replicated physically, virtualized, emulated or simulated. This is to present a realistic testbed for cyber security

purposes.[25] The architecture provides a high degree of fidelity and is also cost effective.

An example of hybrid SCADA testbed is presented in the article, the study have presented hybrid SCADA testbed for power system. The testbed consists of traffic generator, remote terminal units, master terminal unit, human machine interface and communication channel which is wrapped around industrial communication protocols such as IEC-60870-5-101 and DNP3. The study presented the SCADA testbed as a three layered architecture: process layer, bay layer and station layer. The process layer represents power system sensors and actuators. It is responsible for aggregation of process variables from industrial operations and forwarding the data to the bay layer. On the other hand, the bay layer comprises of process control devices such as RTUs and PLCs. Finally, the station layer consists of MTU and HMIs. The main objective of the presented testbed is to perform power flow analysis. Therefore, power flow feature is used for the simulation purpose. In the process layer, PSAT (Power System Analysis Toolbox was used to simulate the electrical power system. PSAT is power system simulation software which offers various types of power analysis including such as load flow analysis, continuation/optimal power flow analysis, small-signal stability analysis and time-domain simulations. Five virtual remote terminal units were used in this testbed, where selected values from the output of power flow are fetched to the respective RTUs based on the configuration of each RTU. Every virtual RTU was deployed in a computer system and has a configurable number of analogue and digital I/O. After aggregation of data from the simulated power system, a protocol adapter wraps up the data into an industrial control protocol i.e. DNP3 or IEC- 60870-5-101. The wrapped data is forwarded to the station layer where a virtual MTU is executed on a computer system. The virtual MTU collects data from all of the five virtual RTUs and the corresponding values are displayed on the HMI. A simple and basic user interface was used to view the data and to send commands.

4. Evaluation of SCADA Testbed Approaches

According to, developing a SCADA testbed for cyber security analysis requires ensuring the support of the following requirements: fidelity for construction of realistic scenarios from the operators' point of view, repeatability for statistically consistent results while reiterating experiments for different configurations, measurement accuracy for analysing tests processes with no interference to the outcomes and safe execution for risk free experiments.[34] SCADA testbed should also be cost-effective, reliable and scalable for large-scale power grid experiments. Table 1 illustrates an evaluation of existing SCADA testbed approaches based on the identified set of requirements. The SCADA testbed requirements were rated based on the scale of excellent, high, moderate, low or poor, where excellent represents absolute support for a specific requirement, high represents great support with some limitations and moderate denote a fair support. On the other hand, low and poor depict limited and weak support respectively.

Physical replication approach intended to construct a copy of a real system with the same physical devices and information systems.[25] Therefore, physical replication demonstrates an excellent representation of the exact physical system with remarkable reliability. However, due to the need to have stacks hardware components, scalability is a great issue in physical replication testbed approach.[35] Moreover, the cost of deploying a similar installation limits its practical application.[36]

Simulation and virtual representation of the system are comparable approaches; both are based on software applications which use modelling methodologies instead of actual physical devices. Such a testbed is low-cost and provides safe execution solutions for research focused on attacks on industrial control systems and the development of security strategies.[2] However, due to the absence of real components and devices and simulated components cannot reflect the real situations in the real SCADA system, the approach provides low fidelity and reliability.[15] On the other hand, software models are easy to reconfigure, maintain and scale. Therefore, repeatability and scalability requirements can easily be met.[25] Virtual testbed components utilize standalone computer system for each respective SCADA component. Therefore, virtualization of SCADA systems is more advantageous. Virtualization offers enhanced fidelity and reliability as it eliminates the software's dependence on the hardware on which it runs. Moreover, virtualized testbed is considered as a controlled environment, as a result it improves repeatability and safety execution.[34]

Table 1. Evaluation of SCADA Testbed approaches

Testbed Approach	Fidelity	Repeatability	Accuracy	Safety	Cost-effective	Reliability	Scalability
Physical replication	Excellent	Poor	Moderate	Poor	Poor	Excellent	Poor
Simulated	Low	Moderate	Poor	Excellent	Excellent	Poor	High
Virtual	Moderate	High	Moderate	Excellent	Moderate	Moderate	Moderate
Virtual-Physical	High	High	Excellent	Excellent	Low	High	Moderate
Hybrid*	High	High	Excellent	High	Moderate	High	Moderate

* Rated based on selecting the optimal approach

Virtual-physical replication is used to overcome the limitations of both virtualization and physical replication to construct a realistic testbed. This approach generally improves overall testbed requirements' factors other than the cost-effectiveness as illustrated in Table 1.[37] Lastly, hybrid testbed approaches incorporate replicated devices and systems as well as software models.[35] It is considered as an effective method to create a SCADA security experimentation platform. Hybrid approach utilizes the most suitable approach for each layer in the SCADA architecture.

Table 1 showed that compared to physical replication approach as a reference, hybrid testbed approaches offers higher repeatability, safety, and more cost-effective with excellent accuracy. Hybrid approaches are reliable with high fidelity in the case of utilizing virtual-physical (HIL) devices for modelling. Therefore, hybrid testbed approach with dedicating HIL is considered for the proposed SCADA testbed framework.

5. Conclusion

In order to protect the SCADA system and its control networks, potential vulnerabilities should be identified and mitigated and propose suitable countermeasures to identify possible malicious attacks. However, it is unpractical to perform security testing and evaluation on an active SCADA system. Therefore, SCADA testbeds is indispensable to assess vulnerabilities and identify possible loophole before deploying the amendments on the critical infrastructure. Researchers typically implement exploits and attack the systems in the testbed to understand the implications of the vulnerability.

The integration of digital components and the physical nature of industrial control systems present several challenges in the design and operation of SCADA testbed. Review of some previously proposed SCADA testbeds have identified three challenges that must be tackled in order to enhance control systems security representation. The first challenge addresses the testbed's scale since the testbed is a scaled down model of the actual physical industrial control system. The second challenge addresses the fidelity, where the testbed must accurately represent the control system in order to support the protocols and standards as well as to generate accurate data. Lastly, the experiments carried out by the proposed testbed should be repeatable and be able to produce the same or statistically consistent results.

This work has reviewed several approached utilized in implementation SCADA testbed intended for cyber security assessment. Future works include developing and implementing a hybrid SCADA testbed utilizing HIL technologies for cyber security assessment and other different applications, analyse different cyber attack scenarios to study the impact of cyber attacks on industrial control infrastructures and integrating anomaly intrusion detection module to protect the SCADA system and prevent future attacks.

6. References

1. Chen B, Pattanaik N, Goulart A, Butler-Purry KL, Kundur D. Implementing attacks for modbus/TCP protocol in a real-time cyber physical system test bed. Proc CQR 2015 IEEE Int Work Tech Comm Commun Qual Reliab; 2015.
2. Queiroz C, Mahmood A, Tari Z. SCADASimA framework for building SCADA simulations. IEEE Trans Smart Grid. 2011; 2(4):589–97. Crossref
3. Stoian I, Ignat S, Capatina D, Ghiran O. Security and intrusion detection on critical SCADA systems for water management. 2014 IEEE Int Conf Autom Qual Testing Robot; 2014. p. 1–6. Crossref
4. Do VL, Fillatre L, Nikiforov I, Antipolis S. Cyber-Physical Attacks. University of Technology of Troyes. CNRS ICD / LM2S UMR 6281 10004 Troyes Cedex; France; 2015. p. 2301–5.
5. Zhu B, Joseph A, Sastry S. A taxonomy of cyber attacks on SCADA systems. Proc of 2011 IEEE Int Conf Internet Things Cyber Phys Soc Comput; 2011. p. 380–8. Crossref

6. Drias Z, Serhrouchni A, Vogel O. Analysis of Cyber Security for Industrial Control Systems. Int Conf Cyber Secur Smart Cities Ind Control Syst Commun; 2015. p. 1–8. Crossref
7. Anwar Z, Shankesi R, Campbell RH. Automatic security assessment of critical cyber-infrastructures. Proc Int Conf Dependable Syst Networks; 2008. p. 366–75. Crossref
8. Aghamolki HG, Miao Z, Fan L. A hardware-in-the-loop SCADA testbed. 2015 North Am Power Symp (NAPS); 2015. p. 1–6.
9. Queiroz C, Mahmood A, Hu J, Tari Z, Yu X. Building a SCADA security testbed. NSS 2009 Netw Syst Secur; 2009 Jan. p. 357–64. Crossref
10. Dayal A, Deng Y, Tbaileh A, Shukla S. VSCADA: A Reconfigurable Virtual SCADA Test- bed for Simulating Power Utility Control Center Operations; 2015. p. 1–5.
11. Chikuni E, Dondo M. Investigating the security of electrical power systems SCADA. IEEE AFRICON Conference; 2007. Crossref
12. McLaughlin S, Konstantinou C, Wang X, Davi L, Sadeghi A, Maniatakos M, Karri R. The Cybersecurity Landscape in Industrial Control Systems. Proc IEEE. 2016 May; 104(5):1039–57. Crossref
13. Li W, Xie L, Liu D, Wang Z. False logic attacks on SCADA control system. Proc 2014 Asia Pacific Serv Comput Conference (APSCC 2014); 2015. p. 136–40.
14. Stouffer K, Falco J, Scarfone K. Guide to Industrial Control Systems (ICS) security: Supervisory Control and Data Acquisition (SCADA) systems Distributed Control systems (DCS) and other control system configurations such as Programmable Logic Controllers (PLC); Gaithersburg, MD; 2011 Jun.
15. Gao H, Peng Y, Jia K, Dai Z, Wang T. The design of ICS testbed based on emulation physical and simulation (EPS-ICS Testbed). Proc 2013 9th Int Conf Intell Inf Hiding Multimed Signal Process (IIH-MSP); 2013. p. 420–3. Crossref
16. Gao W, Morris T, Reaves B, Richey D. On SCADA control system command and response injection and intrusion detection. Gen Members Meet eCrime Res Summit eCrime; 2010.
17. Nai Fovino I, Coletta A, Carcano A, Masera M. Critical state-based filtering system for securing SCADA network protocols. IEEE Trans Ind Electron. 2012; 59(10):3943–50. Crossref
18. Singh P, Garg S, Kumar V, Saquib Z. A testbed for SCADA cyber security and intrusion detection. 2015 International Conference on Cyber Security of Smart Cities Industrial Control System and Communications (SSIC); 2015. p. 1–6. Crossref
19. Bergman DC, Jin D, Nicol DM, Yardley T. The Virtual Power System Testbed and Inter-Testbed Integration; 2003 Aug.
20. Inl T. National SCADA Test Bed Substation Automation Evaluation Report; 2009.
21. Hahn A, Member S, Ashok A, Member S. Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid. 2013; 4(2):847–55.
22. Queiroz C, Mahmood A, Hu J, Tari Z, Yu X. Building a SCADA security testbed. NSS 2009 Netw Syst Secur; 2009. p. 357–64.
23. Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL NSTB Program. U.S. Department of Energy Idaho National Engineering and Environmental Laboratory; 2008. p. 18–27.
24. Mallouhi M, Al-Nashif Y, Cox D, Chadaga T, Hariri S. A testbed for analyzing security of SCADA control systems (TASSCS). IEEE PES Innov Smart Grid Technol Conf Eur ISGT Eur; 2011. p. 1–7. Crossref
25. Holm H, Karresand M, Vidström A, Westring E. A Survey of Industrial Control System Testbeds. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). S. Buchegger and M. Dam Eds; Springer. 2015; 9417:11–26.
26. Siaterlis C, Genge B. Cyber-Physical Testbeds: Scientific Instruments for Cyber Security Assessment of Critical Infrastructures; 2012.
27. Davis CM, Tate JE, Okhravi H, Grier C, Overbye TJ, Nicol D. SCADA cyber security testbed development. 2006 38th Annual North Am Power Symp NAPS-2006 Proc; 2006. p. 483–8. Crossref
28. Bergman DC. Power Grid Simulation Evaluation and Test Framework; 2010.
29. Daniels J. Server virtualization architecture and implementation. Crossroads. 2009; 16(1): 8–12. Crossref
30. Reaves B, Morris T. An open virtual testbed for industrial control system security; 2012. p. 215–29.
31. Mehta BR, Reddy YJ. SCADA Systems. Industrial Process Automation Systems; 2015. p. 237–300.
32. Mets K, Ojea JA, Develder C. Combining Power and Communication Network Simulation for Cost-Effective Smart Grid Analysis. IEEE Commun Surv Tutorials. 2014 Jan; 16(3):1771–96, Jan. 2014. Crossref
33. The PI System OSI soft [Internet]. Crossref
34. Siaterlis C, Genge B. Cyber-physical testbeds. Commun ACM. 2014; 57(6):64–73. Crossref
35. Gao H, Peng Y, Dai Z, Wang T, Han X, Li H. An industrial control system testbed based on emulation, physical devices and simulation. IFIP Adv Inf Commun Technol. 2014; 441:79–91. Crossref
36. Benzel T, Braden R, Kim D, Newnan C, Joseph A, Sklower K, Ostrenga R, Schwab S. Experience with deter: A testbed for security research. 2nd Int Conf Testbeds Res Infrastructures Dev Networks Communities (TRIDENTCOM). 2006; 2006:379–88. Crossref
37. Wertzberger N, Glatter C, Mahoney W, Gandhi R, Dick K. Towards a Low-Cost SCADA Test Bed: An Open-Source Platform for Hardware-in-the-Loop Simulation. 2011 International Conference on Security and Management Special Track on Mission Assurance and Critical Infrastructure Protection (STMACIP); 2011.