Threat Assessment Model in Electrical Power Grid Environment

Qais Saif Qassim¹, Norziana Jamil², Mohammed Najah Mahdi², Fiza Abd Rahim², Zaihisma Che Cob², and Lariyah Mohd Sidek³

¹University of Technology and Applied Sciences-Ibri, Sultanate of Oman.
²College of Computing and Informatics, Universiti Tenaga Nasional, Malaysia.
³Institute of Energy Infrastructure, Universiti Tenaga Nasional, Malaysia.

E-mail: qassim@qq.org

Abstract. At the heart of every critical national infrastructure, there is a SCADA system. The wide range of supported applications has made this life-saving management system the key element of every industrial control infrastructure in various sectors. The complexity and sophistication of SCADA systems have been increased dramatically over the last few years. Various cyberattacks have targeted these systems by exploiting zero-day vulnerabilities or targeting a nearby Internet-enabled appliance or computer system. To this end, many efforts have been proposed previously to model the threats on SCADA systems to eliminate potential danger and diminish the catastrophic consequences in the physical domain. The main contribution of this work is to present a multi-facets threat assessment model to aid security teams to systematically perform various cybersecurity analysis practices such as penetration testing, vulnerability assessment and risk analysis.

1. Introduction

All power generation, transmission and distribution facilities around the world are being supervised and managed by SCADA systems. SCADA: Supervisory Control and Data Acquisition systems, are remote monitoring and controlling structures used to collect data, from remote sites, together into a centralised unit. The collected data will be used for managing the remote sites and perform various analytical studies. SCADA systems are broadly used in various industrial and critical infrastructure facilities, including electrical power, oil and gas production, and distribution [1]. Data reflecting the status of physical processes are being collected from remotely distributed substations on a timely basis. The collected data are transmitted using various communication medium and communication protocols to central control stations for further analysis and execute necessary actions. The actions are generated as a response to the monitored physical device’s current status to adjust or improve its performance. This harmony establishes a feedback monitor and control loop to meet the desired system performance.

The underlying systems of SCADA, including its communication protocols and various physical devices, were designed to transfer the data and control commands back and forth in semi-real-time. Fast information exchange is one of the most important and crucial requirements of these systems. This assists concerned units in identifying issues when they arise and taking appropriate corrective measures to avoid major device errors or disastrous effects. [2]. In order to achieve this task, a SCADA system is usually built using heterogeneous and diverse physical
devices, communication channels and communication protocols. This has widened the attack surface, making the industrial infrastructure more vulnerable to a wider range of cyberattacks. Thus, SCADA and the supporting infrastructure should be protected from various malicious activities and should be equipped with diverse resilient countermeasures to withstand various cyber-attacks [6]. However, due to these systems’ size and sophistication, performing adequate preparation, execution, and analysis of cyber and physical risk evaluations has proven to be a significant challenge [7].

To this end, creating a coherent domain-specific conceptual model should be the first step in every security research practice in order to provide a structured and generic approach for assessing the security of different SCADA framework implementations [8]. As a result, this paper proposes a SCADA mathematical model for modelling SCADA structures in the electrical power domain in an optimal and structured manner. The suggested model can be used to model a wide range of domains. The model defines architectural data and offers a framework for dealing with its complexity, variability, and size. Furthermore, the suggested model turns the method of assessing security vulnerabilities into a systematic process. The following sections are organised as follows; an overview of SCADA systems in electrical power grid has been presented in Section 2. A review of existing SCADA model approaches has been demonstrated in Section 3. In Sections 4 and 5, we describe the proposed model in details. Section 6 illustrates how the proposed model can be applied in the context of the vulnerability assessment process. At the end, Section 7 concludes the study and point out future works.

2. Electrical Power Grid SCADA System

A typical SCADA system comprises three main elements: a central station that houses several industrial computer servers running SCADA software, geographically distributed field sites and communication channels [3]. Many remotely located spatial control systems or computers communicate directly with the physical machines to monitor and automate the operation. Modern SCADA systems use a network of communication links to transmit data from several remote locations and a master control centre [9]. Figure 1 illustrates a typical view of an electric power system. On the right side of the SCADA system, several substation automation networks (remote sites) are wired or wirelessly linked to the main control centre (master control centre) [10].

The SCADA system can be viewed as a cyber-physical system where electronic field instruments such as sensors, actuators, and relays make up the physical component. On the other hand, the cyber component consists of computer networks and networking protocols that are used to transmit data and commands.

Referring back to Figure 1, the main units of a SCADA system are as follows: the central/master control unit, the remote substations and the in-between communication channels and protocols. The Master Terminal Unit (MTU), the Human Machine Interface (HMI), the data historian, and engineering workstations are all housed in the master control centre [11], [12]. The remote substations consist of several geographically distributed field sites equipped with special fields automation devices including the Programmable Logic Controllers (PLCs) and the Remote Terminal Units (RTUs) [13]. One of the main goals of the automation system is that it regulates and tracks the operation of the on-site system’s physical components, such as machines, generators, and circuit breakers. Furthermore, it sends reports about the status of the field equipment to the control centre on a regular basis for monitoring, control, and review [10]. Lastly, the SCADA network communication channels and protocols provide the medium by which data and control commands can be transferred between the main control centre and field sites.

For many years back, SCADA systems are used to operate in an isolated environment using special and dedicated networks and proprietary communication protocols [14]. In contrary to the
modern SCADA system where Internet-enabled devices and open communication protocols are in use. Therefore, modern SCADA systems face new types of security threats and vulnerabilities. These threats and vulnerabilities are originated from the cyber and the physical devices, as well as software and communication and control protocols [16].

3. Related Works
This section reviews several approaches previously proposed as an attempt to simplify the complexity of the SCADA system, especially from the security and safety perspectives. One of the well-known and commonly used models is illustrated in Figure 1, where the SCADA system is considered distributed field devices connected to a central control station. Many studies have adopted this modelling approach. For instance, Queiroz [17] has utilised this model for constructing a SCADA testbed for various security analysis. A similar topological view of the architecture is also used in [1], and [18].

Similarly, the National Institute of Standards and Technology (NIST) of the United States, had proposed an architectural modelling approach. The model has a projected set of rules, and action plans to help carrying out security assessment procedures on SCADA systems [19]. The key disadvantage of this modelling technique is that it fails to depict the interdependencies between various SCADA networks and the electrical power grid structure.

An alternative SCADA modelling approach was proposed based on the IEC/TS 62264 technical specification (previously known as "ISA-99"). The concepts of "zone" and "conduit" have been introduced here [20]. The "zone" term was used to separate an organisation and SCADA networks into several logical sectors, such as SCADA elements that perform similar functions grouped together in one sector (zone) The model defined six levels of operations, including: process level, basic control, area supervisory control, site management control, site business planning and the enterprise level. Similarly, Giani [21] have suggested a model for SCADA systems that focuses on software services called VIKING. The VIKING reference architecture is used to demonstrate services and data flow and their relationship with the network topology. Another modelling approach uses architectural layers to characterise the SCADA scheme, its environment, and its contexts has proposed by Ma [22]. The author has presented a layered architectural view via the utilisation of new grouping and re-organising SCADA modules into various technical levels of abstraction.

An object-role modelling approach was also utilised in SCADA systems; an object-role based
SCADA modelling was proposed by Berg and Stamp [23]. The authors have shown that the object-role approach can model all industrial control processes and functions as well as the underlying internal interdependencies. The object-Role model has been presented to segregate the SCADA infrastructure and its underlying control and communication networks into several layers. Layered modelling usually makes the system analysis more approachable. However, one drawback can be identified here, which is the limited scope of the relationships between the objects.

In conclusion, it can be observed that the reviewed SCADA modelling approaches are commonly lacking comprehensive and inclusive view capabilities, which are two essential parameters for cybersecurity analyst and penetration testers. Therefore, this paper presents a new conceptual model that ensembles the needs and demanding requirements of the security analysis of cyber-physical systems.

4. The Proposed Conceptual Model

As we have deliberated in the previous section, modern SCADA implementations utilise a broad range of software and hardware modules from various vendors. Therefore, each and every component have to be configured variously. For that reason, defining a unified model (architectural or logical) that fits all SCADA implementations in various domains is impractical. Therefore, many studies have suggested proposing a reference model in which all processes and functionalities can be addressed. This is essential for security assessment purposes because considering all potential resources and modules is important to understand better what can go wrong.

In this work, a security-specific SCADA model has been proposed. The proposed model was designed to help security assessors use a flexible instrument representing all SCADA assets, protocols, services, and processes. The flexibility is achieved via the viewpoint concept, which is the main feature of the proposed model. The model has been designed with security in mind. Therefore, it supports all security analysis practices starting from vulnerabilities identification to threat and risk assessment. Moreover, the proposed model is designed to model various domains and, more specifically, the electrical power grid domain. Furthermore, it is expandable in such a way that it suits the current implementations as well as it can be supporting future power grid applications as well including smart grid, green energy and electricity trading.

The proposed model has been designed by incorporating three existing modelling approaches. All three modelling approaches were projected on each other to eliminate their existing drawbacks and optimise their advantages. Therefore, this results in a 3-dimensional model and each dimension representing the model. The complete electrical energy chain was among the three dimensions, while the second dimension represents the IEC62264 reference model, which segregates the SCADA system into various functional levels. Finally, to model the hardware, software, services and processes of the SCADA systems, the ICT resources have been considered and projected into the proposed model. This fusion produces a three-dimensional model as illustrated in Figure 2.

4.1. Power Chain Dimension

The electrical power ecosystem is divided into several functional divisions, including power generation, power transmission, and power distribution [24]. Each division has its control systems and functions. Therefore, the operations of the electrical power grid system and functionalities are highly interconnected. One of the well-known traditional and yet effective power grid modelling approaches is the hierarchical model in which the power chain is segregated into four domains, namely, generation, transmission, distribution, and customer service domains [25]. The generation domain accommodates the power plants, including all sensors, actuators, machinery and operation protocols and processes. The transmission domain is responsible for
transmitting the generated power to the intended destination, where the distribution domain is mapped. Normally, the generated electricity is sent through a large number of various transmission substations over long distances. Typically, transmission cables, circuit breakers, and safety and control systems are all used in the transmission substation [25].

Figure 2. SCADA multi-facets conceptual model

Generally, the electrical power transmission lines accommodate high voltage power lines, high-voltage circuit breakers, relays and voltage regulators. The high voltage power lines are used to transmit power over long distances from when it has been generated to where it will be consumed. The circuit breakers also are essential components of this domain, especially when a fault has been identified. They are used to isolate and disconnect faulty electric network, or transmission lines [26]. The circuit breakers play an important role in remote managing the electrical power system. They are the main concern of cyber attackers, where they can control the power supply on different areas by redirecting or isolating potential power networks. This type of attack is possible and has been occurred before in several countries, including in Ukraine in 2015 [27].

The third domain of the power system chain is the distribution substations which are responsible for supplying the demanded electrical power to customer promises. Usually, this domain is divided into a primary subsystem, and several secondary units [28]. Switch gears, transformers, fuses and feeders are among the various devices that can be seen in this domain. Due to its closeness to the consumer and billing system, this domain is also considered a hot target for many malicious activities.

The last domain of the electric power system is the customer service domain (or customer premises). As the name suggests, this domain represents the system’s end users. It encompasses a wide variety of promises, from manufacturing and urban structures, including warehouses, airports, shopping centres, and private homes. With this wide range of consumers comes a serious responsibility towards their confidentiality and privacy as well as the reliability and integrity of their billing in addition to the availability of the electricity service provided.

4.2. SCADA functional levels dimension

The IEC has proposed a reference model reflecting the hierarchical levels of SCADA systems in the electrical power grid domain. The IEC 62274 reference model has been carefully implemented
to represent the functions of the SCADA system in various management layers. The IEC 62274 reference model have suggested to map the functional units of the SCADA systems into six functional layers, as illustrated in Figure 3.

The lowest layer (level 1) of the model adjacent to the physical system level is associated with field instruments, including the sensors, actuators, protection relays and other instrumental elements that are directly connected to the industrial processes. The second layer (level 2) includes several control devices which are responsible for communicating with the sensors and actuators on the first layer. The main purpose of the devices hosted in this layer is to manage the reading collection and control command deployment to and from the first layer. Common devices seen in this level include the Programmable Logic Controllers (PLC) and the Remote Terminal Units (RTU). The cyber-part of the cyber-physical system can be noticed in level 3 and the adjacent levels.

At level 3, various computer and network devices can be found, which introduce different types of vulnerabilities to the SCADA system. Moreover, in level 4 where the enterprise network is located, which responsible for site business plans and logistics. Finally, there are the applications and software that make up the corporate IT architecture. have been mapped in level 5. The main security challenge drawn from the last two levels is how to keep all interconnected tools and applications of business planning and logistic operations away from the SCADA network.

![SCADA functional levels dimension](image)

**Figure 3.** SCADA functional levels dimension
4.3. ICT resources dimension

In any information and communication technology system, there are two major dimensions; the computation part and the communication part. In this work, we are proposing a third dimension, namely the services and operations. A similar approach has been proposed by [22] as an attempt to present a layered architectural view for security analysis in SCADA. As a result, in this work, the SCADA system is presented as assets, communication and services. The asset dimension shall include all hardware, software, and human resources assets, including SCADA data.

On the other hand, the communication layer models the mechanism in which the SCADA data are being transmitted through various devices in a wide range of place. Typically, this dimension shall model all communication links and communication protocols. From a cybersecurity analysis perspective, understanding how the data is transmitted and what systems are processing or routing these data is essential in determining the reach-ability of critical assets from remote networks and identifying internal and external entry points attacker may exploit system vulnerabilities.

The last dimension is the service layer, in which highlights the functions and processes carried out by the different computer and communication systems in a SCADA system as well as the various industrial and physical systems. Looking at the service layer alone will show an abstraction layer of interconnected services and functions performed by various modules of the SCADA system. Figure 4 illustrates an example of how the SCADA system can be modelled using the service layer across all the management levels.

Figure 4. Viewpoints of the conceptual model

5. Conceptual Models’ Viewpoints

To deal with the scale and sophistication of SCADA systems and to analyse the system from different perspectives, an abstraction technique has been defined here called viewpoint. Basically, the key principle is to create an arbitrary view of the SCADA structure by intersecting the various layers identified by the proposed conceptual model. The viewpoints can serve as a
way to look at the SCADA systems from different angles based on the requirements and the type of analysis to be performed. A viewpoint, for example, can be used to systematically discover SCADA objects (such as hardware, software, and data) associated with each operating zone within a power system domain and define their interdependencies during the security vulnerability assessment process.

The conceptual model is divided into two-dimensional and one-dimensional views using viewpoints. A one-dimensional view allows for a detailed examination of each fundamental dimension separately. The two-dimensional view, on the other hand, shows the SCADA system’s multi-disciplinary landscape. It divides the conceptual model horizontally into functional levels or vertically into levels that intersect.

Within the chosen functional level, the functional levels assist in defining different ICT tools of a given domain, as illustrated in Figure 5 (b). Viewpoints that intersect different functional levels vertically, on the other hand, allow for the investigation of SCADA dataflow and interdependencies among functional levels within a domain as depicted in Figure 5 (c). Alternatively, it may represent an architectural layer of ICT resources within a particular environment as in Figure 5 (d).

Figure 5. Viewpoints of the conceptual model

Viewpoints can be defined in any way that is appropriate for the security process at hand. A security team, for example, might be interested in learning about the cybersecurity risks associated with integrating the marketing division with the SCADA control centre. A security team may also want to conduct a risk assessment of a specific aspect of the SCADA system, such as the risk of critical assets within a particular domain’s substation. Furthermore, the interdependencies and other interactions between actors in the different layers can be easily determined; for example, by identifying a perspective that spans all power grid realms, properties, and functional layers, revealing how the SCADA structure is applied in terms of system services.

6. The Conceptual Model Utilisation

One of the proposed conceptual model’s intended uses in cyber-physical security research is to provide a systemic approach to finding SCADA device tools and modelling interdependencies across different functional levels. The proposed model, for example, will aid in identifying possible security flaws associated with its cyber and physical elements. It also aids in the
detection of any future cyber and/or physical threats on sensitive infrastructure systems. This section provides an example of how the current conceptual model might be used to conduct a risk evaluation.

Vulnerabilities are typically found in device services that have not been thoroughly tested and reviewed for compatibility and flaws, as well as those that do not meet the highest security standards. SCADA vulnerability issues are closely linked to the conceptual model’s ICT resources layers in accordance with the proposed conceptual model. SCADA ICT tools include hardware and software properties, network connectivity and protocols, and SCADA facilities, as mentioned in previous pages. As a result, with each power system domain, a domain-wise perspective that vertically intersects the functional levels is considered; as a result, SCADA resources can be routinely defined at each functional level (i.e. SCADA resources of particular functional-level in a precise electric power system), and their weaknesses found.

7. Conclusions and Future Works
This paper proposed a multi-faceted computational model to aid in the implementation of security analysis, with the goal of modelling the SCADA system and describing architectural detail, as well as dealing with its complexity, heterogeneity, and size. The proposed multi-faceted conceptual model is organised into a three-dimensional view, with each axis reflecting a single SCADA architectural view from a different angle. The entire electrical energy conversion chain is covered by one dimension and is divided into four domains: generation, transmission, distribution, and consumer premises. The second dimension is made up of six layers that map the practical components of SCADA systems as specified by the IEC 62443 reference model. The third dimension is made up of six layers that map the ICT services required to execute the SCADA framework. Each layer represents a practical level of the electric grid, which is spanned by power grid domains and the SCADA system’s architectural abstraction. When applying to basic security-related analyses such as vulnerability evaluation and risk analysis, the idea of perspective is used to allow sense of the proposed framework, which cuts cross through the layers to provide a concentrated view on a subset of the system of concern.

In conclusion, the suggested conceptual model aims to provide and preserve a coherent vision of the system architecture during security phases. Our future work could go in a number of directions: The proposed computational model’s validity and reliability would be examined in order to demonstrate its applicability in modelling complex SCADA structures. The computational model can also be used to prepare standard protocols for defining SCADA tools, which is an important step in vulnerability evaluation and risk analysis. Another aim of our future work will be to provide tool support for effective network vulnerability scanning and SCADA discovery.

Acknowledgement
This research is supported by Transdisciplinary Research Grant Scheme (TRGS) 2020, Ministry of Higher Education Malaysia, under the project 'Cyber Threat Modeling and Advanced Persistent Threat Detection for a Resilient Dam Control System Using Context-based Approach and Ensemble Method of Machine Learning Models With Discrete Probability Distribution.'

References
[1] V. Urias, B. Van Leeuwen, and B. Richardson, "Supervisory Command and Data Acquisition (SCADA) system cybersecurity analysis using a live, virtual, and constructive (LVC) testbed," Proc. - IEEE Mil. Commun. Conf. MILCOM, no. Lvc, pp. 1–8, 2012.
[2] E. Korkmaz, A. Dolgikh, M. Davis, and V. Skormin, "Industrial Control Systems Security Testbed," in 11th Annual Symposium on Information Assurance (ASIA ’16), 2016, pp. 13–18.
[3] B. Zhu, A. Joseph, and S. Sastry, "A Taxonomy of Cyber Attacks on SCADA Systems," in 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, 2011, pp. 380–388.

[4] C. C. Liu, A. Stefanov, J. Hong, and P. Panciatici, "Intruders in the grid," IEEE Power Energy Mag., vol. 10, no. 1, pp. 58–66, 2012.

[5] D. Cotroneo, A. Pecchia, and S. Russo, "Towards secure monitoring and control systems: Diversify!," Proc. Int. Conf. Dependable Syst. Networks, pp. 4–5, 2013.

[6] "NCCIC/ICS-CERT Industrial Control Systems Assessment Summary Report," 2015.

[7] C.-C. Sun, C.-C. Liu, and J. Xie, "Cyber-Physical System Security of a Power Grid: State-of-the-Art," Electronics, vol. 5, no. 3, p. 40, Jul. 2016.

[8] C. Neureiter, D. Engel, and M. Uslar, "Domain Specific and Model Based Systems Engineering in the Smart Grid as Prerequisite for Security by Design," Electronics, vol. 5, no. 2, p. 24, May 2016.

[9] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: a survey," IET Cyber-Physical Syst. Theory Appl., vol. 1, no. 1, pp. 13–27, Dec. 2016.

[10] E. Chikuni and M. Dondo, "Investigating the security of electrical power systems SCADA," in AFRICON 2007, 2007, pp. 1–7.

[11] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "Guide to Industrial Control Systems (ICS) Security," Gaithersburg, MD, Jun. 2015.

[12] Y. Zhang, L. Wang, and W. Sun, "Investigating the impact of cyber attacks on power system reliability," 2013 IEEE Int. Conf. Cyber Technol. Autom. Control Intell. Syst., pp. 462–467, 2013.

[13] W. Knowles, D. Prince, D. Hutchinson, J. F. P. Disso, and K. Jones, "A survey of cyber security management in industrial control systems," Int. J. Crit. Infrastructure. Prot., vol. 9, pp. 52–80, Jun. 2015.

[14] K. Stouffer, J. Falco, and K. Kent, "Guide to Supervisory Control And Data Acquisition (SCADA) and industrial control systems security," Recomm. Natl. Inst. . . . , p. 155 pp, 2006.

[15] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," in Proceedings of the IEEE, 2012, vol. 100, no. 1, pp. 210–224.

[16] H. P. Singh, "Cyber security trend in Substation Network for automation and control Systems," 2013 IEEE Int. Conf. Comput. Intell. Comput. Res. IEEE ICCIC 2013, pp. 0–2, 2013.

[17] C. Queiroz, A. Mahmood, and Z. Tari, "SCADASimA framework for building SCADA simulations," IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 589–597, 2011.

[18] H. Gao, Y. Peng, Z. Dai, T. Wang, X. Han, and H. Li, "An industrial control system testbed based on emulation, physical devices and simulation," IFIP Adv. Inf. Commun. Technol., vol. 441, pp. 79–94, 2011.

[19] K. Stouffer, J. Falco, and K. Scarfone, "Guide to Industrial Control Systems (ICS) Security," Gaithersburg, MD, Jun. 2011.

[20] T. M. B. Singer, Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS. Auerbach Publications, 2011.

[21] A. Giani, S. Sastry, K. H. Johansson, and H. Sandberg, "The VIKING project: An initiative on resilient control of power networks," in 2009 2nd International Symposium on Resilient Control Systems, 2009, pp. 31–35.

[22] Z. Ma, P. Smith, and F. Skopik, "Towards a Layered Architectural View for Security Analysis in SCADA Systems," Nov. 2012.

[23] M. Berg and J. Stamp, "A Reference Model for Control and Automation Systems in Electric Power," 2005.

[24] I. Nai Fovino, L. Guidi, M. Masera, and A. Stefanini, "Cyber security assessment of a power plant," Electr. Power Syst. Res., vol. 81, no. 2, pp. 518–526, Feb. 2011.

[25] T. Morrisa, A. Srivastavab, B. Reavesa, W. Gaosa, K. Pavurapua, and R. Reddi, "A Control System Testbed to Validate Critical Infrastructure Protection Concepts," 2011.

[26] L. L. Grigsby, Electric Power Engineering Handbook. Taylor & Francis Group, 2006.

[27] B. M. Buchholz and Z. Styczynski, "Modern Technologies and the Smart Grid Challenges in Transmission Networks," in Smart Grids – Fundamentals and Technologies in Electricity Networks, Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 61–119.

[28] P. Mohajerin Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, "Cyber attack in a two-area power system: Impact identification using reachability," Proc. 2010 Am. Control Conf., pp. 962–967, 2010.