A Security Assessment Model for Electrical Power Grid SCADA System

Qais Qassim, Norziana Jamil, Maslina Daud, Norhamadi Ja'affar, Hafizah Che Hasan, Mohamad Afendee Mohamed

Abstract*—Due to the wide application of SCADA systems in national critical infrastructure, their cyber security issues and vulnerabilities have been a primary concern; whereas, the impact and consequences of cyber-attacks to these systems have the potential to result in catastrophic consequences in the physical domain. Therefore, estimating possible attack impacts and identifying system vulnerabilities are major concern in SCADA management and operations. However, it is quite difficult to plan, execute and review vulnerability analysis in critical infrastructure systems as well as in industrial control systems (such as SCADA system) due to its complexity, large-scale and heterogeneity. Consequently, a consistent domain-specific conceptual model is required to establish a generic framework for cyber security analysis to examine and investigate security threats on cyber-physical systems, the role of the entities within the system as well as system operations. The main contribution of this work is to present a multi-facets model to support cyber security analysis practices such as penetration testing, vulnerability assessment and risk analysis. The proposed model presents a common insight among different SCADA configurations, implementations and the employed protocols to handle its complexity, heterogeneous and scale. To demonstrate the usability as a proof of concept and applicability of the proposed model, the paper also presents an example illustrating how the proposed model can be employed to carry out security vulnerability assessment.

Index Terms: Critical infrastructure systems, cyber-attack, SCADA, testbed, vulnerability assessment.

I. INTRODUCTION

Supervisory Control and Data Acquisition (SCADA) systems have been widely used for monitoring and controlling industrial and critical infrastructure functions such as the power generation, transmission and distribution control systems as well as oil and gas production and distribution [1]. They collect data from remote substations about the state of the physical process and send back commands to execute further actions to adjust its performance to meet a desired output response creating a feedback monitor and control loop. SCADA systems are designed to provide information in real-time and to take corrective actions when needed as an attempt to prevent significant system failures [2]. A typical SCADA composed of three main elements namely a central station housing number of specialized computer servers running SCADA software that manages number of geographically distributed field sites [3]. Several remotely located local control systems or devices which interact directly to control and automate the process equipment. Moreover, a communication links that connect the computer servers at the central station to those at the remote field sites.

Todays, SCADA system is becoming highly interconnected with other corporate networks and cloud-based services through the Internet [4]. Moreover, SCADA systems have become highly dependent on the use of Commercial-Off-The-Shelf (COTS) IT products and open communication standards to significantly cut down implementation costs and decrease the effort of maintenance and integration [5]. This becomes great challenges in protecting national critical infrastructure. That the cyber-threat landscape continuously growing, the security of SCADA systems and their underlying architecture is a must and well-equipped with strong protection mechanisms to withstand various cyber-attacks [6]. In order to understand the impending security risk and to identify possible attacks, potential security vulnerabilities should be identified and analysed. However, due to the scale and complexity of ICS systems and the communication technologies that they are associated with, making planning, executing and reviewing cyber and physical vulnerability assessments become a substantially challenging problem [7]. Consequently, establishing a consistent domain-specific conceptual model should be the starting point in any security analysis practice to provide a systematic and generic methodology for the security assessment of various implementations of SCADA systems [8]. As a result, a SCADA conceptual model has been proposed in this paper to efficiently and systematically model SCADA systems in the electrical power domain. The proposed model can be extended to model various domains. The model describes the architectural information and provides a guide to handle its complexity, heterogeneity and scale. Moreover, the proposed model transforms the security vulnerability assessment procedure to a systematic process.

The followings are the structure of this paper: Section 2 exposes reader to an introduction of electrical power grid based on SCADA systems. Section 3 demonstrates existing SCADA modelling approaches and highlights the needs for a new conceptual model for SCADA security assessment practices. Section 4 describes the proposed model, its layers as well as the use of viewpoints from security-related perspective to make intersections through the layers to handle the complexity exists within the SCADA system. To further expose the applicability of the proposed conceptual

Revised Manuscript Received on September 14, 2019.

Qais Qassim, Institute of Informatics and Computing in Energy, Universiti Tenaga Nasional, Malaysia and Institute of Informatics and Computing in Energy, Universiti Tenaga Nasional, Malaysia.

Norziana Jamil, Institute of Informatics and Computing in Energy, Universiti Tenaga Nasional, Malaysia.

Maslina Daud, CyberSecurity Malaysia.

Norhamadi Ja'affar, CyberSecurity Malaysia.

Hafizah Che Hasan, CyberSecurity Malaysia.

Mohamad Afendee Mohamed, Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Terengganu, Malaysia.

Retrieval Number: L113210812S219/2019©BEIESP
DOI: 10.35940/ijitee.L1132.10812S219

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

model, Section 5 discusses an example of its usage in the context of vulnerability assessment process. Lastly, Section 6 concludes the study and point out future works.

II. ELECTRICAL POWER GRID SYSTEM

Modern SCADA systems are distributed Cyber-Physical Systems (CPS) which encompass the transfer of data between multiple remote sites and a master control centre via a network of communication links [9]. Fig. 1 shows a typical CPS view of an electric power system. The cyber part of the CPS includes several substation automation networks (remote sites) connected to a main control centre (master control centre) through wired or wireless connections [10]. On the other hand, the physical part consists of electronic field devices such as sensors, actuators and relays.

SCADA systems vary among implementations, whereas several designs and technologies have been employed to setup mission-critical data and control systems that perform remote monitoring and control of physical systems. However, a typical SCADA system consists of control centre, communication links and remote sites. The master control centre houses the Master Terminal Unit (MTU), the Human Machine Interface (HMI), data historian and engineering workstations [11], [12]. A SCADA control centre monitors and controls one or more geographically distributed field sites [13]. The later are equipped with special field automation devices such as Programmable Logic Controllers (PLCs) or Remote Terminal Units (RTUs). The automation devices control and monitor the on-site system's physical components such as machines, generators or circuit breakers. Moreover, it periodically sends information about the state of the field equipment to the control centre for monitor, control and further analysis [10].

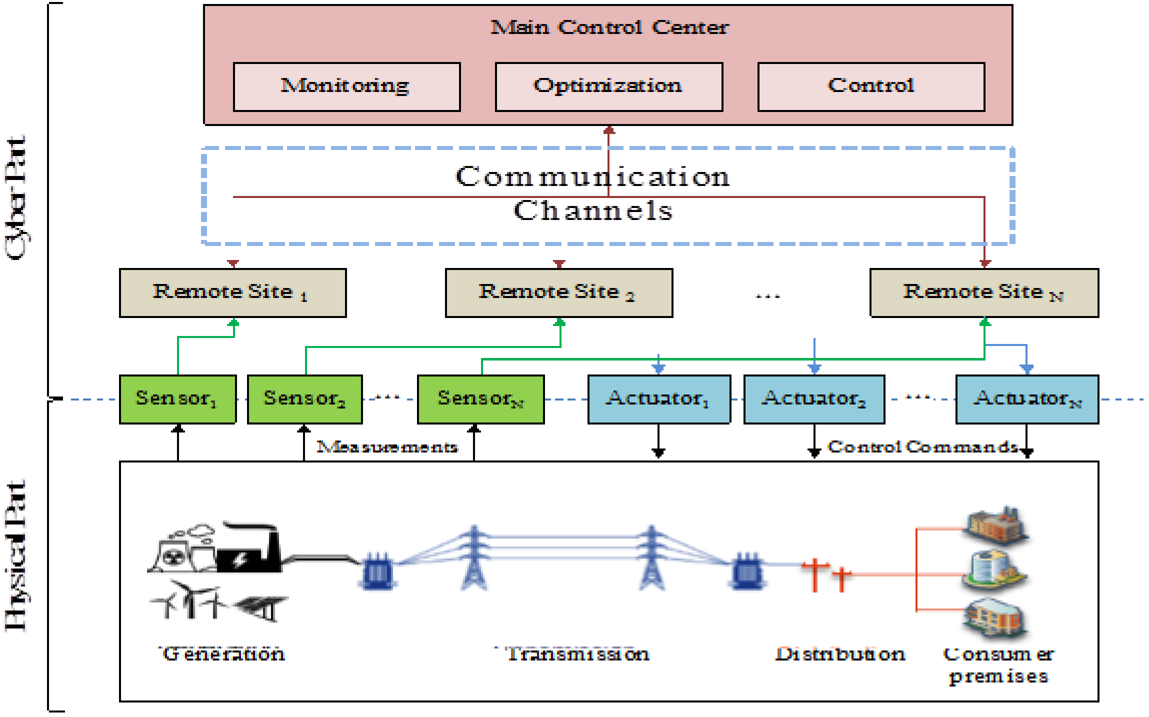

Fig. 1: General architecture of a SCADA system

The SCADA network communication channels act as the medium for data transmission between the operation centre and field sites. Back then, the networks operate in isolation from other networks by employing a dedicated links and proprietary communication protocols [14]. However, due to the growth in demands for geographically distributed substations, the systems have no choice but to connect to the Internet enabled devices and other open communication standards for the purpose of cutting down implementation costs and increase ease of maintenance as well as the integration compatibility with other manufacturers. Moreover, for providing real-time decision making, SCADA network has been incorporated to their enterprise networks to unify their operations [15]. Consequently, modern SCADA systems are facing different types of security threats and vulnerabilities that are associated with hardware and software, and communication and control protocols [16]. Therefore, identifying the security vulnerabilities and threats, applying the most appropriate security measures along with protecting SCADA systems are of vital importance. However, being a large-scale in nature and the heterogeneity of the systems and communication technologies of SCADA systems make planning, executing, and reviewing cyber and physical vulnerability assessments quite difficult. Therefore, a systematic and comprehensive modelling of the aforementioned SCADA system is required. This can be achieved through the use of a conceptual reference model.

III. RELATED WORKS

There have been several approaches to model SCADA systems from security perspective; one of the commonly used approach is based on modelling the SCADA systems in accordance with their network topologies. In this approach a

Retrieval Number: L113210812S219/2019©BEIESP
DOI: 10.35940/ijitee.L1132.10812S219

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

typical SCADA model consists of field devices network connected to a supervisory and control network, and further connected to a corporate network. This modelling approach have been adapted by [17] for developing a SCADA testbed for security analysis. In [1], [18], we can find similar topological view of the architecture. A relevant architectural modelling approach is proposed by the U. S. National Institute of Standards and Technology (NIST). NIST had proposed a set of guidelines in carrying out security assessment on SCADA systems [19]. NIST suggested that a SCADA architectural model consists of the following operational networks: The control centre network, the communication link network, the field devices and the physical process itself to understand and manage the complexity of SCADA systems and to identify the security vulnerabilities.

Another SCADA system modelling approach is proposed based on IEC/TS 62264 technical specification for industrial communication networks (formerly referred to as "ISA-99"). The ISA-99 introduced the concepts of “zone” and “conduit” as a way to segment and isolate the various subsystems in a control system. Moreover, ISA-99 had introduced a hierarchical logical framework (known as the Purdue logical framework) which utilizes the "zone" concept to subdivide an enterprise and SCADA networks into several logical segments whereas every zone is comprised of SCADA elements that perform similar functions. The Purdue logical framework defines six-levels of operations including [20]: Process level, basic control, area supervisory control, site management control, site business planning and the enterprise level. Another reference model called VIKING introduced by [21] focuses on the software services within SCADA systems. The VIKING reference architecture is used to demonstrate services and dataflow, as well as their relationship with the network topology. The VIKING reference architecture includes three components: A set of reference services of SCADA systems that represents common services and functions in SCADA, a set of reference dataflow between the SCADA services and a set of reference zone architectures. A slightly different approach is to describe the SCADA system and its environment and contexts using architectural layers. In [22] proposed a layered architectural view by grouping and re-organizing SCADA components into different technological layers of abstraction.

A SCADA reference model presented by Berg and Stamp make use of Object-Role Modelling [23] to model industrial control data, functionality and their internal interdependencies. The Object-Role model considered objects to represent both system entities features and properties in addition to the role annotates the relationship between these objects. The reference architecture model categorized the SCADA objects into four levels based on a mixture of function and network topologies namely; infrastructure equipment, field equipment, systems and control centres, as well as automation oversight. Object-Role model separates SCADA infrastructure and its control and communication networks into separate layers such that their analysis can be made more efficient. However, the relationship between the objects (roles) might be a peer-to-peer relationship between one object to another, or they may be implied through the relationship of two objects to a third (or others) making modelling complex SCADA architectures more challenging and tedious task.

Based on the reviewed related works, it can be concluded that, existing approaches of SCADA reference models lack proper representation that provides a consistent and comprehensive view of SCADA system suitable for cyber security assessment. For example, the architectural modelling approach presented by NIST does not show the interdependencies among different SCADA networks and electrical power grid system. On the other hand, IEC/TS 62264 modelling approach provides a comprehensive modelling of the interdependencies among SCADA networks but does not properly model SCADA services and dataflow among different SCADA layers. Similarly, SCADA modelling approaches presented by [21], [22] were carefully model services, dataflow and their relationship with the network topology. However, their modelling approaches do not consider isolating the SCADA system into several management levels which makes SCADA modelling a complex task. Therefore, this paper presents a proposal of a new conceptual model that suits the requirement of cyber-physical security analysis.

IV. ELECTRICAL POWER GRID CONCEPTUAL MODEL

A SCADA system uses a broad range of components and software applications from different vendors configured in various ways. Therefore, defining a standard architectural model that suits different SCADA implementations and domains is almost unfeasible. However, proposing a conceptual model that characterizes services of a typical SCADA system is vital for security assessment purposes. The proposed conceptual model is meant to be an architectural template representing all services, protocols and assets in different domains and operational levels. It aims at offering a support for cyber security analysis of the electric power grid systems with an architectural approach allowing for a representation of interdependencies among different operational layers and subsystems. It offers a support for both the current implementation of the electrical grid and future applications of the smart grid.

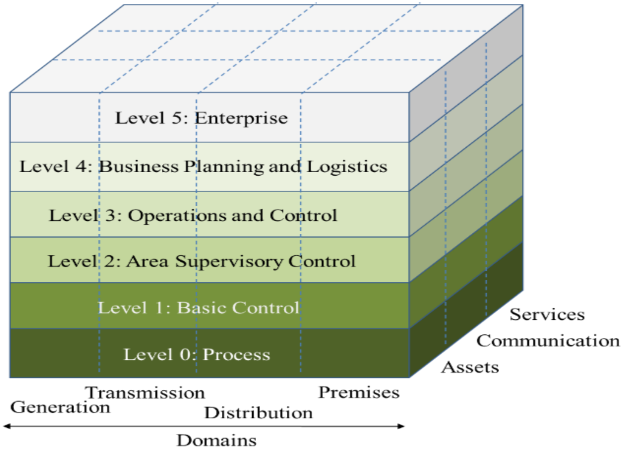

Fig. 2: SCADA multi-facets conceptual model

The proposed conceptual model is arranged into 3-dimensional structure; each dimension is intended to reflect a specific SCADA architectural view. The first dimension covers the complete electrical energy conversion chain, partitioned into four domains: Generation, transmission, distribution and customer's premises as have been defined by NIST Sp. 800-82, IEC 60870 and IEC 62351 standards. The second dimension represents the SCADA system based on its ICT resources which encompass assets, communication and services as proposed by [22]. Lastly, the third dimension forms six layers that map the functional components of SCADA systems as defined in the IEC 62264 reference model. Each layer covers an electric grid functional level, which extends over power grid domains and architectural abstraction of the SCADA system. This merge results in a multi-facets model which spans three dimensions as illustrated in Fig. 2.

A. The Power Chain Dimension

A typical electrical power grid includes several control centres to manage the generation, transmission, and distribution of power throughout the grid [24]. Therefore, the electric power critical infrastructure is highly interconnected, consisting of several utilities and distributed substations. The traditional hierarchical model of top-down electric power production chain splits the infrastructure into several substations including generation, transmission, distribution, and customer service systems. The generation substation houses the power plants which is responsible for generating electric power by electromechanical generators from sources of primary energy such as kinetic energy nuclear, natural gas and petroleum as well as other types of energy including solar photovoltaic energy, tidal power and other energy sources [25]. The generated electricity is transmitted over long distances to different distribution substations in the electrical power grid system through multiple transmission substations.

The transmission substation contains transmission lines, circuit breakers, as well as protection and control equipment [25]. The transmission lines symbolize the high voltage power lines that run over long distance area transporting electrical energy from the generation facilities to the areas of consumption. In transmission substations high-voltage circuit breaker are used to disconnect faulty transmission lines and isolate flawed electric network [26]. Different kinds of protection and control equipment can be located within the transmission substation such as relays and voltage regulators that ensure the reliability of the transmitted power. Power transmission substations can range from simple to complex; a simple substation can be a basic transmission line with few circuit breakers and voltage meters [27].

The distribution substations responsible for delivering the electrical power to customer promises consist of a primary distribution system and several secondary distribution subsystems [28]. The typical distribution substations consist of several power feeders emanating from the substation and supply power to one or more smaller distribution substations; that in turn, serves from one to several power feeder circuits, whereas a typical feeder circuit can serve numerous loads of all types [29]. The final stage of the electric power production chain is the customer service systems (or customer premises) that represent the system's end users. The premises include industrial, commercial buildings such as factories, airports, shopping malls and residential houses.

B. SCADA Functional Levels Dimension

The power grid functional levels has adapted IEC 62264 reference model which was largely based on Purdue model for control hierarchy logical framework to subdivide SCADA network into several logical segments comprised of systems that perform similar functions. Layer segregating allows the mapping the functional components into six different layers (denoted as level 0 to level 5) which represent the fundamental categorization in view of functionality, interconnectivity, nature of operations and integrative approach as illustrated in Fig. 3.

The first level (level 0) concerns with field instruments such as the sensors, actuators, protection relays which has direct connection to the industrial processes. These instruments are managed by devices structured in Level 1. Whereas, Level 1 includes several control equipment that receives monitoring data from field sensors, processes sensors' data by using control algorithms, and sends out control commands when a response or intervention is needed. Devices in this level include Distributed Control Systems (DCS), Programmable Logic Controllers (PLC), and Remote Terminal Units (RTU). Commonly, the devices of this level run vendor-specific operating systems and facilitate a remote access to be programmed and configured from engineering workstations.

Meanwhile, level 2 includes equipment related to the manufacturing operations for an individual substation. Typically level 2 includes: human machine interfaces and control room workstations. SCADA components at level 2 communicate with devices in Level 1. Additionally, a Demilitarized Zone (DMZ) may be used to interface operation systems at the enterprise zone with SCADA equipment of this layer.

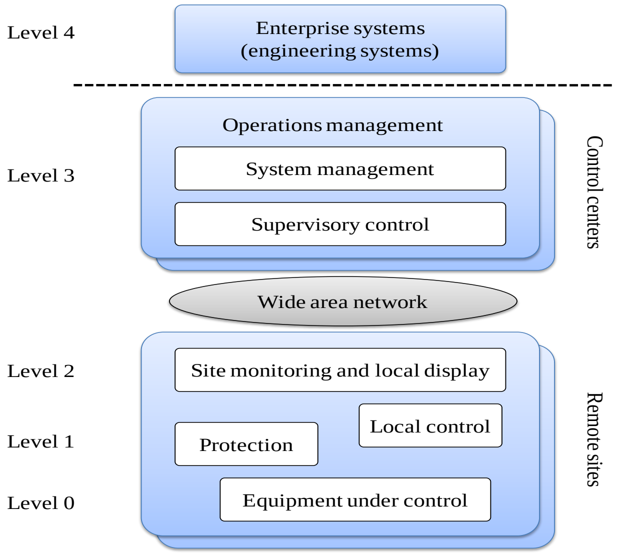

Fig. 3:IEC 62264 reference model

Manufacturing zone (Level 3) is where the sites' operations and control take place. SCADA components at this level are often responsible for control and monitor plant's operations. From assets and services perspective, this level may include production reporting and scheduling systems, engineering workstations as well as network file servers. The enterprise zone is allocated at SCADA functional level 4 which functions as site business planning and logistics operations. Level 4 houses number IT-specific systems. At this level, system operators are responsible for reporting, scheduling, inventory management, capacity planning, operational and maintenance management. Lastly, the corporate IT infrastructure systems and applications zone is at the functional level 5. Direct communication between systems in the enterprise zones and the ICS environment is usually done through a DMZ to manage access and restrict access to critical assets.

C. ICT Resource Dimension

From the architectural perspective, SCADA components is generally divided into two layers (as previously illustrated in Section 2) and possibly be extended into three layers: Physical, cyber and operational layers to reduce complexity and scale of the cyber-physical system. Similar approach has been proposed by [22] as an attempt to propose a layered architectural view for security analysis of SCADA system. The architectural view consists of four interrelated layers: Assets, communication, services and organization layer. Comparing the available modelling approaches in term of security perspective, it is evident that the second approach enables the detailed elicitation of SCADA system components as well as describing how data may flow in SCADA system. Therefore, the concept of representing SCADA systems in a layered architecture has been utilized in the proposed conceptual model to systematically identify and analyse ICT resources across different functional levels and power system domains. In this work, SCADA system is presented as assets, communication and services.

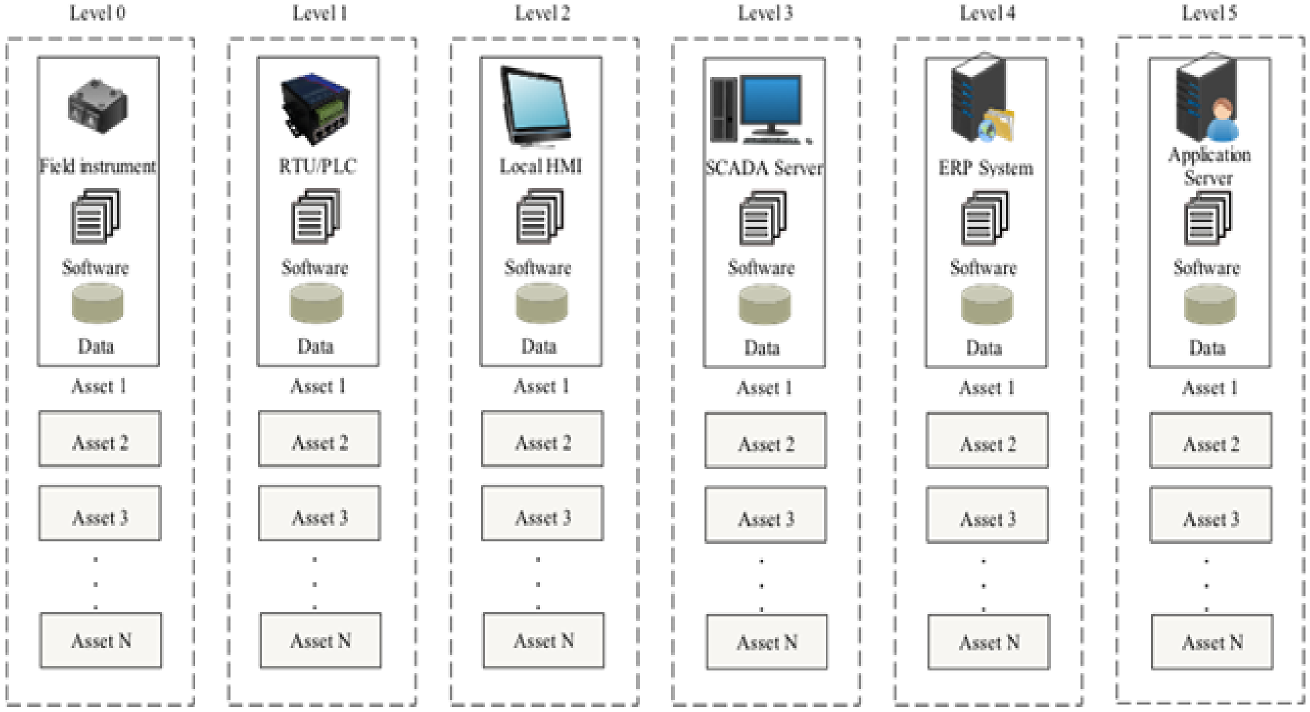

Fig. 4:Asset layer

Asset Layer: The layer typically consists of elements of SCADA system such as hardware, software and data. Hardware entities encompass broad range physical devices. The physical devices in a typical SCADA system can include computation, data storage and control units as well as field instruments; computation units include various computer systems those perform general or specific operations for example operations related to general, commercial and organizational processes such as desktop and laptop computers and hand held devices, and those related to enterprise networks such as workstations and servers. Other computer system assets are related to network system security and protection such as Intrusion Detection Systems (IDS). Moreover, SCADA control equipment such as PLC, RTU and Phasor Measurement Unit (PMU) can be considered as physical assets that control industrial processes of a physical plant. SCADA field instruments comprise of equipment to protect power lines and sensors, monitor meter readings and equipment status in addition to control the process of the power system. Field devices involve sensors, actuators and protection relays as well as bay controller and wide range of intelligent electronic devices. The asset layer also includes software such as operating systems, databases, and application software. Moreover, it includes data which involves all information used and transmitted among different SCADA physical devices. For simplicity, within this layer, software and data shall be associated to the hardware device that utilize, handle and transmit them. A simple asset layer across the functional levels is shown in Fig. 4.

Communication Layer: The layer is responsible for modeling the data transmission using various network devices, its software and protocols among different SCADA assets. From cyber security analysis perspective, modelling data communication and understanding data flow within SCADA system is essential in determining the remote reachability to critical assets and identify internal and external entry points that an attacker may exploit system vulnerabilities.

During the process of vulnerability assessment, SCADA communication model is advantageous in identifying vulnerabilities in different functional levels and power system domains. In this work, the communication model is designed to house various communication devices (will be referred to as gateways) and communication protocols (both network and control protocols) as illustrated in Fig. 5. The end points are entities that send and receive data which represents SCADA hardware assets that have been identified and analysed in the asset layer.

Communication devices (gateways) describe the data flow through the SCADA system. This layer houses various networking nodes like hubs, switches and routers as well as their software firmware. Firewalls can be considered as elements of the communication layer as they can restrain the flow of data through the SCADA systems; additionally, firewalls can be embedded into modern network routers. In addition to the various communication devices, the communication layer also models the wide range of protocols. As an example, ubiquitous protocol TCP/IP is used in enterprise networks. Whereas for control networks, different SCADA communication protocols including MODBUS, Distributed Network Protocol version 3 (DNP3) and IEC 60870-5-101/104 are used. The communication layer also considers the medium that encompasses links that connect various SCADA assets together. It may be wired or wireless. Wired networks may use dial-up telephone, leased line, power line, category 5 or 6 cable, serial cable, and/or fiber optic cable. Wireless networks may use standardized communication systems such as IEEE 802.11, Bluetooth and/or radio. Moreover, wireless links may include very long distance solutions such as satellite and microwave links.

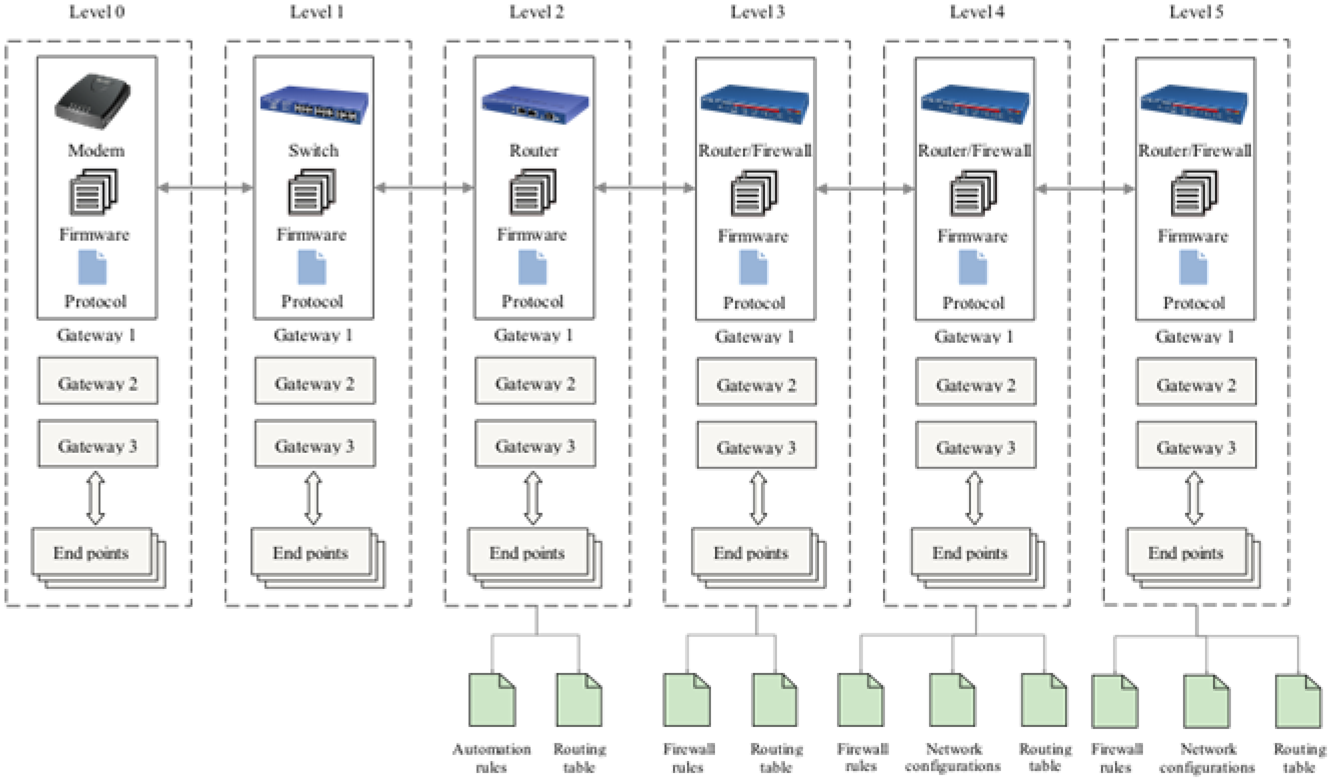

Fig. 5:Communication layer

In [22] has suggested enumerating on three main attributes at the stage of communication layer modelling in order to provide an insight on how data is travelled within the SCADA system. The authors have suggested considering the network and sub-network addressing layout of the system, the communication and control protocols and services to be used. Additionally, the state is also associated to these protocols and services. Identifying SCADA network addressing layout in terms of network and subnet address ranges is valuable to identify the scope of each entry point and furnish an indication on how the system can be penetrated. Additionally, identifying protocols and services that are in use, as well as their state is helpful in planning for vulnerabilities remediation during the security vulnerability assessment procedures.

Service Layer: In this work, service layer highlights functions or processes performed by various physical and communication devices in a SCADA system. Service layer presents an abstraction of SCADA devices and their interconnectivity as an attempt to provide a detailed model of the services provided. In other words, the service layer models various types of services as well as the data exchanged between services. In this work a service is referred to any functionality provided by a software or hardware component of a SCADA system. At this end, we consider databases, authentication servers, Web servers and application servers as services. An example of service layer is depicted in Fig. 6.

The arrows presented in the figure represent the data exchanges among the services. For example, services such as sensor and actuator send measurement data and receive control commands to and from SCADA control centre or industrial automation system through the front end SCADA service. Another example is the HMI, where the HMI provide services such as providing an interface of the operators to the SCADA server. Additionally, the historian archives monitor and control data of the control centre while proving audit logs for all activity across the SCADA network. It also provides an interface with the corporate network through a web-based application to allow management principals accessing these data for further analysis. It is worth to mention that; the service layer enables the modelling of factors that are not considered in the asset layer or the communication layer. For example, communication server permits remotely located client to gain terminal access to SCADA server for the purpose of operation and maintenance. From vulnerability analysis perspective, modelling SCADA system as services with encapsulated functions allows a better understanding of SCADA architecture. Furthermore, it enables modelling of SCADA systems with legacy and proprietary software components.

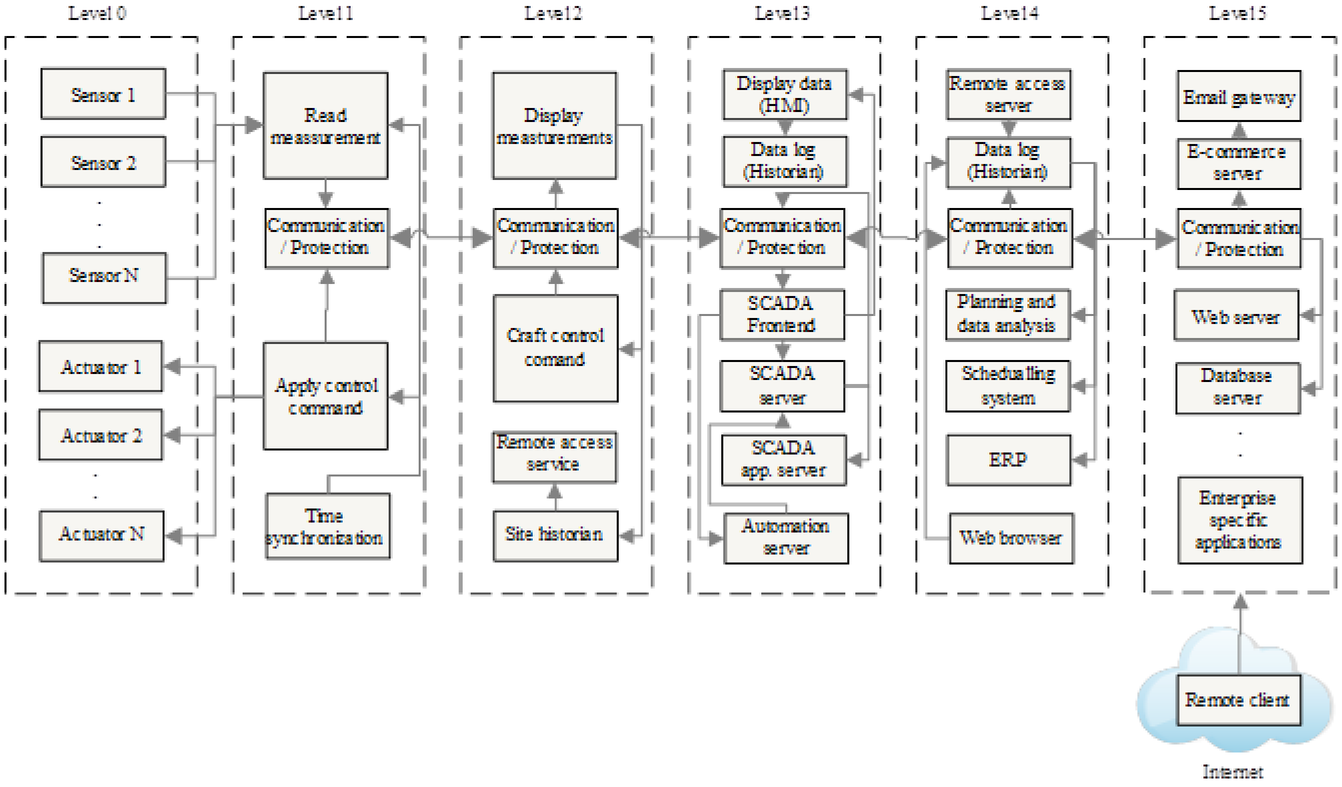

Fig. 6:Service layer

V. CONCEPTUAL MODELS' VIEWPOINTS

A viewpoint is defined as an abstraction technique using a selected set of architectural concepts in order to concentrate on specific concerns found in the system. To address the scalability and complexity of SCADA systems, the proposed conceptual model facilitates the use of viewpoints to provide an arbitrary view of SCADA system by making intersections through the layers when applying a particular security-related analysis such as vulnerability assessment and risk analysis.

For example, in security vulnerability assessment process, viewpoint can be used to systematically discover SCADA entities (such as hardware, software and data) associated with each operational zone within a power system domain and identify their interdependencies.

A viewpoint is used to segregate the conceptual model into either one or two dimensional views. One-dimensional view enables a comprehensive study of each fundamental dimension individually. On the other hand, two-dimensional view reveals the cross-discipline landscape of the SCADA system. It partitions the conceptual model either horizontally aligned to a functional level or vertically intersects different levels. The former assists in identifying various ICT resources of a specific domain within the selected functional level as illustrated in Fig. 7 (b). On the other hand, viewpoints that vertically intersect different functional level enable the investigation of SCADA dataflow and interdependencies among the functional levels within specific domain as depicted in Fig. 7 (c). Alternatively, it may represent an architectural layer of ICT resources within a specific domain as in Fig. 7 (d).

Viewpoints can be arbitrarily defined based on the security process that is being carried out. For example, a security team may wish to understand the cyber security vulnerabilities associated with integrating the marketing division with SCADA control centre. Moreover, a security team may wish to perform risk assessment of a particular aspect of the SCADA system such as the risk of critical assets within a substation of a specific domain. Additionally, the interdependencies and other relationships between

Retrieval Number: L113210812S219/2019©BEIESP
DOI: 10.35940/ijitee.L1132.10812S219

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

entities from different layers can be easily determined; for example, by defining a viewpoint that cut across all the power grid domains, resources and functional layers which can reveal how SCADA system is implemented in terms of system's services.

VI. CONCEPTUAL MODELS UTILIZATION& RESULTS

One of the intended uses of the proposed conceptual model is to provide a systematic approach in discovering SCADA system resources and model interdependencies among different functional levels for cyber-physical security related studies. For example, the proposed model can assist in finding out potential security vulnerabilities associated with its cyber and physical components. Additionally, it helps in identifying possible future cyber and/or physical attacks that can target the critical infrastructure system. To demonstrate the uses of the proposed model, this section presents an example to show how a vulnerability assessment might take place using the proposed conceptual model.

Typically, vulnerabilities are discovered in system resources that have not been fully inspected and checked for reliability and weaknesses and have not met the optimal security requirements. In conjunction with the proposed conceptual model, SCADA security vulnerabilities are tightly associated with the ICT resources layers of the conceptual model. As pointed out in earlier sections, SCADA ICT resources incorporate hardware and software assets, network communication and protocols as well as SCADA services. Therefore, a domain-wise viewpoint that vertically intersect the functional-levels for every power system domain is considered; consequently, SCADA resources can be systematically identified at each functional-level (i.e. SCADA resources of specific functional-level in a precise electric power system are identified) and their vulnerabilities are discovered. Table 1 presents a number of possible SCADA security vulnerabilities associated with each functional level of the proposed model. It is worth to mention that, SCADA resources and their security policies vary in every functional-level based on their security requirements as illustrated in Table 1.

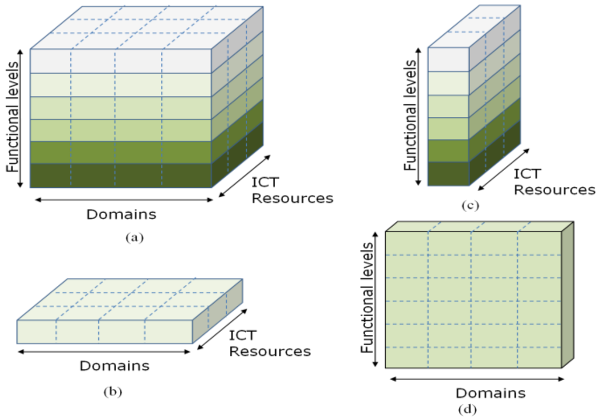

Fig. 7: Viewpoints of the conceptual model

Table 1: List of possible vulnerabilities associated with SCADA assets in different functional levels

Level	Resources	Possible Component	Possible Vulnerabilities
Level 5	Assets	Hardware: Workstations, servers, printers	No formal ICS security training and awareness program; lack of administrative mechanisms for security policy enforcement; improper protection of computer system's ports such as USB or Ethernet; untrained users setting up unauthorized workstations and networks; physically insecure locations.
		Software: Web, business and accountant software applications	Un-patched or old versions of operating systems, firmware or third-party applications; improper credential management; improper access/authorization control; use of unevaluated third party control software; missing encryption of sensitive data.
	Communication	Entities: Routers, switches and firewall	Improper network design; poorly configured access points; unprotected wireless networks; weak firewall rules; failure to physically secure network devices; improper authentication and authentication bypass issues.
		Protocol: Ethernet, IEEE802.11	Implementation flaw allows remote attackers to execute arbitrary code or obtain sensitive information; no configured security or poor security; lack of network monitoring and MAC address filtering; cryptographic issues; default or poorly configured SNMP protocol.
	Service	DNS, email and database	Web, email, DNS and database vulnerabilities; improper input validation; implementation flaw allows a remote user can cause denial of service conditions on the target device.

Level 4	Assets	Hardware: Workstations, servers, computer systems and printers	Inadequate security policy for the ICS; lack of adequate authentication policy; improper monitoring and protection of physical components; authentication bypass issues; improper access restrictions; improper protection of computer system's ports such as USB or Ethernet.
		Software: Planning, email, inventory management and ERP	Un-patched or old versions applications; insufficient verification of data authenticity; improper credential management; improper access/authorization control; use of unevaluated third party control software; missing encryption of sensitive data; use of proprietary software that have not been tested against security vulnerabilities.
	Communication	Entities: Routers, switches and firewall	No security perimeter defined; lack of integrity checking for communications; inadequate authentication between wireless clients and access points; physically insecure locations and no set physical boundaries; untrained users setting up unauthorized workstations and networks.
		Protocol: Ethernet and IEEE 802.11	Incorrectly specified destination in a communication channel; insufficient control of network message volume; improper restriction of communication channel to intended endpoints; cryptographic issues.
	Service	Email, print, ERP and database	Improper credential management; improper input validation; improper handling of permission, privileges and access control; programming errors and implementation flaws.
Level 3	Assets	Hardware: Workstations, servers, personal computers and printers	Lack of adequate access control policy; no formal ICS security training and awareness program; lack of administrative mechanisms for security policy enforcement; improper monitoring and protection of physical components; improper access restrictions; improper protection of computer system's ports such as USB or Ethernet.
		Software: SCADA, HMI, Historian and production management	Improper code quality; improper input validation; use of unevaluated third party control software; missing encryption of sensitive data; use of an inappropriate cryptographic algorithm; insufficiently protected credentials; improper security configuration.
	Communication	Entities: Routers, switches and firewall	Insufficiently protected credentials; improper system configuration; using weak or factory default passwords; no security perimeter defined; lack of network segmentation; lack of functional DMZs; firewalls non-existent or improperly configured.
		Protocol: Ethernet, IEC60870-101 and DNP3	Weaknesses in the implementation stack; predictable TCP sequence numbers allow spoofing; DNS resolver uses predictable IDs, allowing a local user to spoof DNS query results; Use of Insufficiently Random Values
	Service	Front end, HMI, SCADA	Improper credential management; improper input validation; improper handling of permission, privileges and access control; missing encryption of sensitive data; use of an inappropriate cryptographic algorithm.
Level 2	Assets	Hardware: Workstations	Lack of redundancy for critical components; improper monitoring and protection of physical components; improper access restrictions; no security perimeter defined; insecure architecture with little consideration for the potential security impacts.
		Software: HMI and industrial automation software application	Improper code quality; use of unevaluated third party control software; missing encryption of sensitive data; use of an inappropriate cryptographic algorithm; insufficiently protected credentials; improper security configuration.

	Communication	Entities: Routers, switches and firewall	Insufficiently protected credentials; improper system configuration; using weak or factory default passwords; no security perimeter defined; lack of network segmentation; lack of functional DMZs; firewalls non-existent or improperly configured.
		Protocol: IEC60870-101 and DNP3	Improper packet filtering allows remote attackers to send crafted packets to execute arbitrary code and cause Buffer Overflow; insufficient control of network message volume.
	Service	HMI, monitoring services	Missing encryption of sensitive data; use of an inappropriate cryptographic algorithm.
Level 1	Assets	Hardware: RTU and PLC	Improper monitoring and protection of physical components; lack of adequate access control policy; no formal ICS security training and awareness program; improper access restrictions; improper protection of computer system's ports such as USB or Ethernet.
		Software: Industrial specific operating systems and software applications	Use of unevaluated third party control software; missing encryption of sensitive data; insufficiently protected credentials; improper security configuration.
	Communication	Entities: Routers, switches and firewall	Insufficiently protected credentials; improper system configuration; using weak or factory default passwords; no security perimeter defined; lack of network segmentation; lack of functional DMZs, firewalls non-existent or improperly configured; firewall bypassed
		Protocol: IEC60870-101, Modbus and DNP3	Denial of service due to weak security considerations
	Service	Controller and gateway	Improper packet filtering allows remote attacker to carry out a TCP replay attack to execute arbitrary command; implementation error; improper security configuration.
Level 0	Assets	Hardware: Sensors, actuators and protection relays	Improper installation; lack of secure and backup power suppliers; unsecured physical ports; improper authentication implementation and bypass issues; improper measurement/command validation.
		Software: Propriety software applications	Missing encryption of sensitive data; use of an inappropriate cryptographic algorithm; insufficiently protected credentials; improper security configuration.
	Communication	Entities: Propriety communication links	Inadequate data protection between sensors and RTU, missing encryption of sensitive data.
		Protocol: IEC60870-101, Modbus and DNP3	Denial of service due to weak security considerations; lack of integrity checking form communications.
	Service	Measurement and process	Implementation error; improper security configuration.

VII. CONCLUSION

This work presented a multi-facets conceptual model to support the implementation of security analysis, as an attempt to model the SCADA system and describe the architectural information and to handle its complexity, heterogeneous and scale. The proposed multi-facets conceptual model is structured into a 3-dimensional view; each dimension is intended to reflect a specific SCADA architectural view from different perspective. One dimension covers complete electrical energy conversion chain, partitioned into four domains: Generation, transmission, distribution and customer's premises. The second dimension covers the ICT resources used to implement the SCADA system and the third dimension forms six layers that map the functional components of SCADA systems as defined in the IEC 62443 reference model. Each layer covers an electric grid functional level, which is spanned by power grid domains and architectural abstraction of the SCADA system. To make use of the proposed architecture, the concept of viewpoint is utilized which cut cross through the layers to provide a focused view on a subset of the system of interest when they are applied to specific security-related analysis such as vulnerability assessment and risk analysis. In summary, the proposed conceptual model is an attempt to establish and maintain a consistent view on the system architecture during security processes.

There are several directions for our future work: The validity and reliability of the proposed conceptual model will be investigated to show its feasibility in modelling complex SCADA systems. The conceptual model will also be used in planning for standard procedures in identifying SCADA resources as an essential step in the vulnerability assessment and risk analysis tasks. Tool support for efficient network vulnerability scanning and discovery of the SCADA will be another objective in our future work.

VIII. ACKNOWLEDGMENT

This work was supported by Ministry of Science, Technology and Innovation, Malaysia, CyberSecurity Malaysia and Tenaga Nasional Berhad (TNB) Seed Fund.

REFERENCES

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

2 E. Korkmaz, A. Dolgikh, M. Davis, and V. Skormin, “Industrial control systems security testbed,” 11th Annual Symposium on Information Assurance, 2016, pp. 13–18.

3 B. Zhu, A. Joseph, and S. Sastry, “A taxonomy of cyber attacks on SCADA systems,” IEEE 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., 10(1), 2012, pp. 58–66.

5 D. Cotroneo, A. Pecchia, and S. Russo, “Towards secure monitoring and control systems: Diversify!,” IEEE Int. Conf. Dependable Syst. Networks, pp. 4–5, 2013.

6 Industrial Control Systems Cyber Emergency Response Team, NCCIC/ICS-CERT industrial control systems assessment summary report. 2015, Available: https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/FY2015_Industrial_Control_Systems_Assessment_Summary_Report_S508C.pdf.

7 C. C. Sun, C. C. Liu, and J. Xie, “Cyber-physical system security of a power grid: State-of-the-art,” Electronics, 5(3), 2016, pp. 1-18.

8 C. Neureiter, D. Engel, and M. Uslar, “Domain specific and model based systems engineering in the smart grid as prerequesite for security by design,” Electronics, 5(2), 2016, pp. 1-42.

9 H. He, and J. Yan, “Cyber-physical attacks and defences in the smart grid: A survey,” IET Cyber-Physical Syst. Theory Appl., 1(1), 2016, pp. 13–27.

10 E. Chikuni, and M. Dondo, “Investigating the security of electrical power systems SCADA,” IEEE AFRICON, 2007, pp. 1–7.

11 K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, Guide to Industrial Control Systems (ICS) security. 2015, Available: http://www.gocs.com.de/pages/fachberichte/archiv/164-sp800_82_r2_draft.pdf.

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

13 W. Knowles, D. Prince, D. Hutchison, J. F. P. Disso, and K. Jones, “A survey of cyber security management in industrial control systems,” Int. J. Crit. Infrastruct. Prot., 9, 2015, pp. 52–80.

14 K. Stouffer, J. Falco, and K. Kent, Guide to Supervisory Control and Data Aquisition (SCADA) and industrial control systems security. 2006, Available: https://www.dhs.gov/sites/default/files/publications/csd-nist-guidetosupervisoryanddataccquisition-scadaandindustrialcontrolsystemssecurity-2007.pdf.

15 S. Sridhar, A. Hahn, and M. Govindarasu, “Cyber-physical system security for the electric power grid,” Proceedings of the IEEE, 100(1), 2012, pp. 210–224.

16 H. P. Singh, “Cyber security trend in substation network for automation and control systems,” IEEE Int. Conf. Comput. Intell. Comput. Res., 2013, pp. 1-3.

17 C. Queiroz, A. Mahmood, and Z. Tari, “SCADASimA framework for building SCADA simulations,” IEEE Trans. Smart Grid, 2(4), 2011, pp. 589–597.

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., 441, 2014, pp. 79–91.

19 K. Stouffer, J. Falco, and K. Scarfone, Guide to Industrial Control Systems (ICS) Security. NIST Special Publication 800-82, Maryland: National Institute of Standards and Technology, 2011.

20 T. M. B. Singer, Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS. New York: 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,” 2nd International Symposium on Resillient 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,” 1st International Symposium for ICS and SCADA Cyber Security Research, 2012, pp. 1-7.

23 M. Berg, and J. Stamp, A reference model for control and automation systems in electric power. Technical report SAND2005-1000C, Albuquerque: Sandia National Laboratories, 2005.

24 I. Nai Fovino, L. Guidi, M. Masera, and A. Stefanini, “Cyber security assessment of a power plant,” Electr. Power Syst. Res., 81(2), 2011, pp. 518–526.

25 T. Morrisa, A. Srivastavab, B. Reavesa, W. Gaoa, K. Pavurapua, and R. Reddi, “A control system testbed to validate critical infrastructure protection concepts. International Journal of Critical Infrastructure Protection, 4(2), 2011, pp 88-103.

26 L. L. Grigsby, Electric Power Engineering Handbook. England: Taylor and Francis, 2018.

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, B. M. Buchholz and Z. Styczynski,Eds. Berlin: Springer Berlin Heidelberg, 2014, pp. 61–119.

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

29 R. R. Shoults, and L. D. Swift, “Power system loads,” in Electric Power Generation, Transmission, and Distribution, L. L. Grigsby, Ed. Florida: CRC Press, 2018, pp. 1-12