Computer Science and Engineering 2022, 12(1): 15-29
DOI: 10.5923/j.computer.20221201.02

Cyberphysical Security Analysis of Digital Control Systems in Hydro Electric Power Grids

Lukumba Phiri*, Simon Tembo

Department of Electrical and Electronic Engineering, School of Engineering, University of Zambia, Lusaka, Zambia

Abstract The use of hydro energy to generate electric power is crucial to meet the increasing energy demand of a modern economy and maintains the stability of power supply for unstable sources of power like solar, and wind. In newly constructed hydropower plants (HPPs), the trend among control systems is to adopt contemporary digital and cyber-based systems at the expense of obsolete analog hard-wired systems. Therefore, cyber-physical security is a critical issue in reliability-constrained HPPs. In this paper, we present different levels/layers of protection to manage cyber security. We adopt generalized stochastic Petri nets to quantitatively evaluate the intrusion probability. We then propose a new cyber framework and show that the proposed framework conforms to NIST cybersecurity regulations. Finally, we discuss dependability through three metrics, i.e., reliability, maintainability, and availability. A case study is presented to demonstrate that the proposed cyber framework is highly dependable through analyzing steady-state probabilities.

Keywords Control networks, Control systems, Cyber-physical security, Dependability analysis, Generalized stochastic Petri nets (GSPNs), Hydropower plants, National Institute of Standards and Technology (NIST)

1. Introduction

Hydropower is the main renewable resource in Africa with over 37GW of installed capacity. The African continent also has the highest untapped hydropower potential in the world, with only 11% utilized. Hydropower amounts to 17% of electricity generation in Africa, with this share potentially increasing to more than 23% by 2040, as part of many African countries' ambitious proposals for creating a lower-carbon energy system, and universal energy access in Africa. Hydropower provides a free and clean fuel source - water, renewed by rainfall. It can supply large amounts of electricity and, when combined with storage (a reservoir), can be despatched to provide baseload power or to smooth out the intermittency of other renewables in an energy system - meaning it is one of the most flexible and reliable forms of renewable energy [1,2].

In Zambia, energy sources include renewable sources such as water, solar, wind, and biomass; as well as fossil fuels such as petroleum. Given the substantial unexploited reserves of renewable sources, Zambia has the potential to be self-sufficient in energy, except for petroleum that is wholly imported into the country. Despite the diversity of these energy sources, however, water remains the main energy source in Zambia. It is estimated that Zambia possesses 40 percent of the water resources in the SADC region and has a hydropower potential above 6,000MW out of which about 2,354MW has been developed. The national installed capacity of electricity stood at 2,981.23 MW as of 30th June 2020. With regards to the installed capacity by technology, hydro generation accounted for 80.5 percent followed by coal at 10.1 percent. Further Heavy Fuel Oil (HFO) generation was at 3.7 percent, while Diesel and Solar were at 2.8 percent and 3.0 percent, respectively. The large hydropower projects under feasibility studies are over 2,800MW situated on the major rivers of Zambia. For this reason, it would be advisable to formulate optimal generation plans that are centered around hydropower [3,4,5].

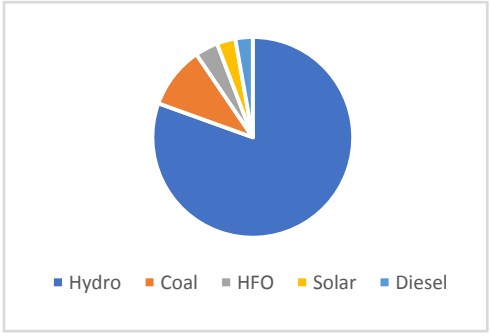

Figure 1. Power Generation Summary

Zambia's energy sector is dominated by the Zambia Electricity Supply Corporation (ZESCO). ZESCO is the vertically integrated national utility that generates transmits, distributes, and supplies electricity to national and regional

* Corresponding author:
phirilukumba@gmail.com (Lukumba Phiri)
Received: Feb. 22, 2022; Accepted: Mar. 7, 2022; Published: Mar. 15, 2022
Published online at http://journal.sapub.org/computer

markets. There are two other major players, namely: the Copperbelt Energy Corporation (CEC) which is a transmission company that purchases electricity from ZESCO at high voltage and distributes it to the mining industry in the Copperbelt region; and the Lunsemfwa Hydro Power Company. There are also two rural concessions: Zengamina Hydro Power Company (ZHPC) which runs a remote rural network in the Northern Province and North West Energy Corporation which distributes electricity to a rural mining community that is not on the ZESCO grid [6].

The regulation of the sector is undertaken by the Energy Regulation Board (ERB). The ERB was created under the Energy Regulation Act of 1995 Chapter 436 of the Laws of Zambia following the issuance of Statutory Instrument number 6 of 1997, the Energy Regulation Act (Commencement Order) of 27th January 1997 [6].

In recent times the major power utility operator in Zambia has experienced large-scale power outages, some even spanning the entire country. The Energy Regulation Board (ERB), a regulatory board is mandated to investigate and document such critical incidences. And as such, in 2021 ERB recently reported national power blackouts in August, October, and November respectively. This has on several occasions been attributed to systems disturbances, although ERB is yet to issue a report on the 2021 blackouts [7]. With the advent of cyber-attacks on critical infrastructure, it's imperative that the reliability analysis on power grids shifts from physical-based (contingency) to cyber-physical analysis.

As a result, a myriad amount of efforts have been put into the research of security issues in the smart grid. Various reactive (acting against the past) and proactive (acting in anticipation) methodologies are proposed to reduce the risk of threats, increase the ability to detect and identify system anomalous behavior, and initiate mitigation countermeasures quickly to restore the system operations. Since the nature of threats and vulnerabilities is constantly changing, the applications of current best security practices are necessary but not sufficient [8]. The authors in [9] proposed an original resilience analysis framework for a complex gas pipeline transmission network, considering the cybernetic interdependence of the physical gas pipeline network with the SCADA system, critical insights on the resilience model were obtained through a systematic sensitivity analysis (SA) framework. Cho, Chi-Shiang et al. [10] adopted generalized stochastic Petri nets to quantitatively evaluate the intrusion probability for a Nuclear Power Plant. We approach our work as in our earlier publications [8] and [10], although our focus will be on the cyber aspect of a Hydro Power Plant. Authors in [11-15] analyzed the integrated safety and security for cyber-physical harm scenarios. [11] posited a method called coined Uncontrolled Flows of Information and Energy (UFoI-E), a distinct theoretical foundation rooted in accident causation models and a framework to design diagrammatic representations of CPSs during the analysis. Lu T, Guo X, Li Y, et al. [13] focused on cyber-physical security for industrial control systems based on Wireless Sensor Networks (WSN), while [14] and [15] conducted a comprehensive survey on the state-of-the-art research to enhance the physical and cyber security in a smart grid environment.

Authors in [16], [17], [18], [19], and [20] conducted analyses on testbeds and surveyed literature but their work didn't propose a framework applicable to the digital control systems in electric power grids.

The main contribution of this paper is to propose a novel model (i.e., GSPNs) to elucidate security of digital control systems in HPPs, to obey smart grid regulations. We propose a new cyber framework to comply with the NISTIR 7628 and NERC CIP cybersecurity regulation, Through a case study, we demonstrate that the proposed framework is feasible for the security analysis of control networks in HPPs.

The remainder of this paper is organized as follows.

Section II analyzes the cyber-physical security issues of control systems in HPPs. We discuss and model intrusions into the control networks in Section III. Section IV discusses and compares cybersecurity standards applicable to Industrial Control Systems (ICS). To comply with the NIST framework, we present a new cyber framework in this section. In Section V, we analyze a case study to demonstrate that the enhanced cyber framework can be applied to determine the reliability, availability, and maintainability (RAM) metrics of a digital control system. Section VI gives the conclusion and future works.

2. Security of Digital Control Systems in HPPS

2.1 Overview of Main Control and Automation System in Hydroelectric Power

The main control and automation system in a hydroelectric power plant are associated with the start and stop sequence for the unit and optimum running control of power (real and reactive), voltage, and frequency. Data acquisition and retrieval are used to cover such operations as relaying plant operating status, instantaneous system efficiency, or monthly plant factor, to the operators and managers. The type of control equipment and levels of control to be applied to a hydro plant are affected by such factors as the number, size, and type of turbine and generator. The control and monitoring equipment for a hydropower plant includes control circuits/logic, control devices, indication, instrumentation, protection, and annunciation at the main control board and the unit control board for generation, conversion, and transmission operation, grid interconnected operation of hydro stations including small hydro stations. These features are necessary to provide operators with the facilities required for the control and

supervision of the station's major and auxiliary equipment. In the design of these features, consideration must be given to the size and importance of the station to other stations in the power system, location of the main control room to the pieces of equipment to be controlled, and all other station features which influence the control system. The control system of a power station plays an important role in the station's rendering of reliable service; this function should be kept in mind in the design of all control features. Basic control functions in a modern hydroelectric station require all equipment (generating unit, auxiliaries, switchyard equipment, and hydraulic control e.g. spillway gates, etc.) to be connected to the plant control system by electrically actuated element for automatic control, protection, and monitoring.

The digital control systems for an HPP are depicted in figure 2 above. ICS is led by device vendors and integrators and is not as standardized as IT systems. ICS in different industries and regions are very different, their architecture, types of equipment, and protocols are different. Establishing a reference model is the primary means of addressing these variations. Purdue Enterprise Reference Architecture (PERA) is currently widely used in the industry [23]. PERA was developed in 1993 by Theodore J. Williams and members of the Industry-Purdue University Consortium for Computer Integrated Manufacturing. This model was adopted by ISA- 99 (ISA/ IEC 62443) [24] and other industry security standards, and used as the basis for ICS network segmentation. As shown in Fig. 3, the network of enterprises can be separated into six levels across three zones [25].

Level 4/5 – Enterprise: This is typically the IT network as we know it today, where the primary business functions occur. This is the level that provides business direction and orchestrates manufacturing operations. Enterprise resource planning (ERP) systems drive plant production schedules, material use, shipping, and inventory levels. Popular ERP systems include offerings from Oracle, SAP, Microsoft, and Epicor. Any disruptions at this level can lead to days or even weeks of downtime, creating the potential for significant revenue loss with downstream processes delayed or stopped [25].

Level 3.5 – Demilitarized zone (DMZ): A recent addition over the last decade, this level includes security systems, such as firewalls and proxies, used to separate or air gap the IT and OT worlds. This is where the IT and OT worlds "converge," increasing the attack surface for the OT systems. Many plants either do not have this layer or have very limited capabilities. The rise of automation leading to higher efficiencies has created an increased need for bidirectional data flows between OT and IT systems. This OT-IT convergence is ultimately creating a formidable competitive advantage for companies that are accelerating digital transformation [25].

Level 3 – Manufacturing operations systems: This is where the production workflow is managed on the manufacturing floor. Customized systems based on operating systems, such as Windows, are used to perform batch management, record data, and manage operations and plant performance. The systems at this level are called manufacturing execution systems (MES) or manufacturing operations management systems (MOMS). MES/MOMS are specific to the products being processed/manufactured. This layer also consists of databases or historians to record the operations data. The communication between the enterprise level and manufacturing level typically occurs through a dedicated backhaul network to the main data center or headquarters. Like the enterprise level, any disruptions at the manufacturing level can lead to hours or days of downtime, with enormous potential for revenue loss, as it impacts the entire manufacturing plant [25].

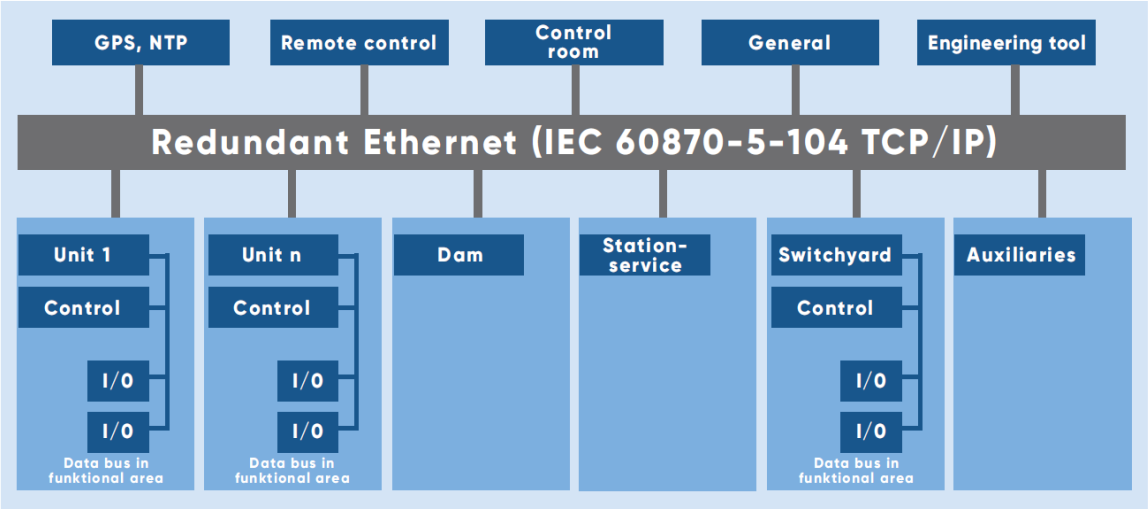

Figure 2. Architecture for Digital Control Systems

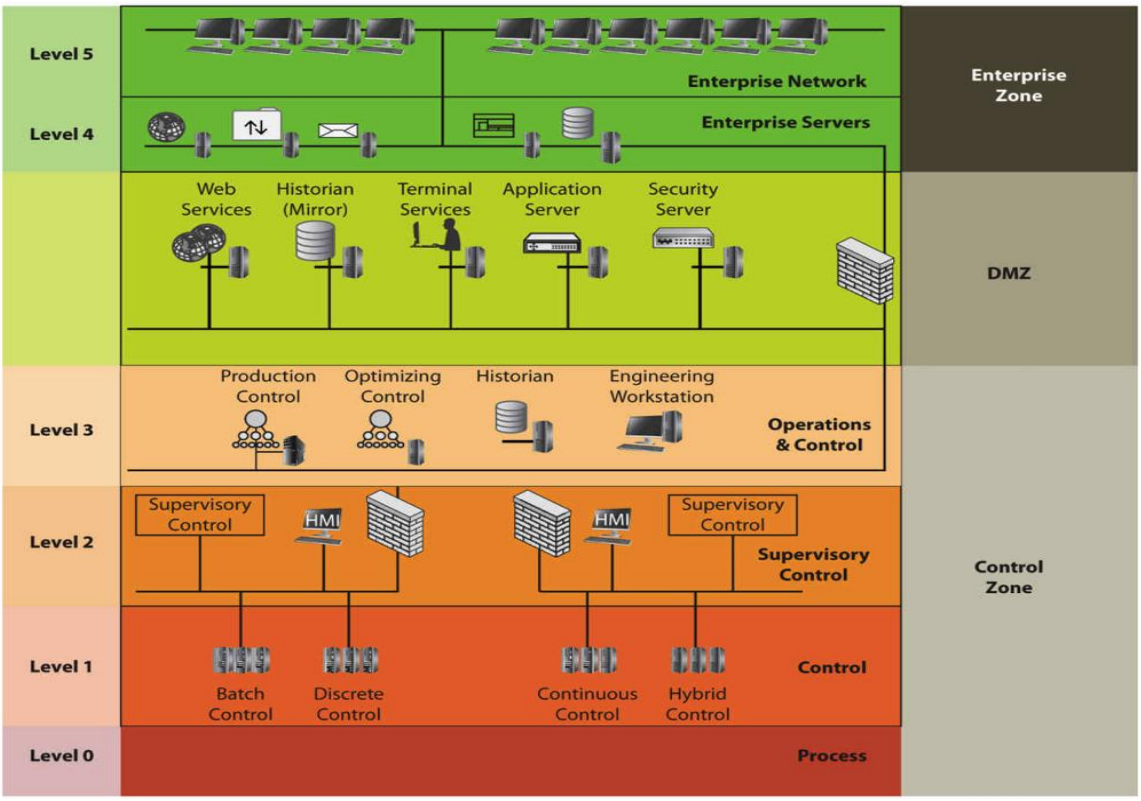

Figure 3. Purdue Enterprise Reference Architecture

Level 2 – Control systems: Supervisory control and data acquisition (SCADA) software is used to supervise, monitor, and control physical processes. SCADA can manage systems over long distances from the physical location of the plants, while the distributed control system (DCS) and programmable logic controllers (PLCs) are usually deployed within the plant. The human-machine interface (HMI) connected to DCS and PLCs allows for basic controls and monitoring, while the SCADA systems aggregate data and send it upstream for recording by the historian in level 3. PLCs typically do not have keyboards and monitors. Remote Terminal Units (RTUs) allow operators to log in to the SCADA systems. Siemens, Schneider Electric, ABB, GE Digital, and Rockwell Automation are some of the major providers of SCADA systems. Devices and strategies at this layer typically communicate over the Modbus and DNP3 protocols, and data diodes can help bolster security [25].

Level 1 – Intelligent devices: Sensing and manipulating physical processes occurs at this level with process sensors, analyzers, actuators, and related instrumentation. To drive efficiencies, sensors are increasingly communicating directly with their vendor monitoring software in the cloud via cellular networks [25].

Level 0 – Physical process: Defines the actual physical processes.

2.2. Cyberphysical Security Accidents in HPPs

The European Network of Transmission System Operators for Electricity (ENTSO-E) became the latest power sector organization to have fallen victim to a cyberattack [26].ENTSO-E – which represents 42 European transmission system operators in 35 countries – said on 9 March 2020 it had recently "found evidence of a successful cyber intrusion into its office network", and was introducing contingency plans to avoid further attacks. According to French think-tank Institut Français des relations internationals (IFRI) [27], the power sector has become a prime target for cyber-criminals in the last decade, with cyberattacks surging by 380% between 2014 and 2015. Motives include geopolitics, sabotage, and financial reasons. The US Department of Energy (DoE) [28] reported 150 successful attacks between 2010 and 2014 that targeted systems holding information regarding electricity grids. In June 2019, the New York Times [29] reported that the US launched cyberattacks into the Russian power grid [30]. According to the newspaper, US military hackers used American computer code to target the grid as a response to the Kremlin's disinformation campaign, hacking attempts during the 2018 midterm elections, and suspicions of Russia hacking the energy sector. The story was condemned by President Trump, who said it was fake news, and experts, while the Kremlin said it was a possibility. According to the 2018 National Defence Authorisation Act, government hackers are permitted to carry out "clandestine military activities" to protect the country and its interests [31]. Saudi Aramco became the target of cyberattacks in 2017 when hackers targeted the safety system in one of the company's petrochemical plants. Experts believe that, despite the plant shutting down, an incident could have taken place. According to a report by the Independent [32], a plant

official said that the attack aimed not only to shut down the plant or wipe out data but also sent a political message. Experts traced the attack to a Russian Government-owned laboratory. The 2016 cyberattack on Ukraine was the second in less than a year. Hackers left customers in parts of Kyiv without electricity for an hour, after disabling an electricity substation. The BBC [33] said that the loss of electricity amounted to a fifth of Kyiv's power consumption for that night. The attack was attributed to Russian hackers, with some experts suggesting that the attack aimed to physically damage the power grid. Hackers got into the system of a western Ukrainian power company, cutting power to 225,000 households. A US report into the blackout concluded that a virus was delivered via email through spear-phishing – a technique that sends key employees detailed messages, using information gathered from social media. The report did not name any perpetrators but experts suggested it was linked to a group of Russian hackers. South Korean nuclear and hydroelectric company Korea Hydro and Nuclear Power (KHNP) was hacked at the end of 2014 [34]. Hackers stole and posted online the plans and manuals for two nuclear reactors, as well as the data of 10,000 employees. The US pinned the attack on North Korea but South Korean authorities traced the IP addresses to Shenyang, a city in northeast China.

2.3. Digital Control Systems (SCADA-specific) Communication Protocols

The communication protocols are regulations for the data depiction and exchange over a communication link. [18]. SCADA communication protocols play a pivotal role in MTU-RTU interactions. At first, instruments and protective relays permitted remote communications using local RS232 associations or using a dial-up modem interface. But due to scalability issues, they have moved to more advanced protocols [19].

As the SCADA system is a composition of many components, if each component uses a vendor-specific protocol, it will not be able to communicate with other components. Each vendor-specific SCADA protocol has its own rules and procedures of communication which can vary from data presentation and conversion, assignment of addresses to command generation, and status information. Therefore, to support interoperability and cost efficiency, some open standards were presented. To encourage open protocols, the Open System Interconnection (OSI) model was introduced in 1984 [20]. The OSI model shows the data communications process composed of seven independent layers, and each of the layers describes how the data is handled in the different stages of transmission. Open protocols increase the availability of the device, interoperability, vendors independence, optimized cost, easy technical support, etc.

A study of various communication protocols is done below.

A. Modbus: The Modbus transmission protocol, an application layer messaging protocol was developed by Gould Modicon for their Modicon programmable controller [21]. It is the most commonly used protocol for connecting electronic devices due to being openly published and easy to use. Moreover, it is used for the interactions between MTU and RTUs. A typical Modbus network supports one master and a maximum of two hundred forty-seven slaves. RTUs only reply to messages targeted to them but avoid responding to the broadcasts [22]. It uses four types of communication messages to request/respond to messages to/from MTU, acknowledgment messages for the successful delivery of the message at the MTU and RTUs. MTU can send messages to the slaves and also assign an address to each of the slaves which varies from 1 to 247. Modbus/TCP, an enhanced variation of Modbus is also available which focuses on reliable communication over the Internet and Intranet. It follows TCP/IP's error detection methods to detect the errors. Modbus plus protocol is proposed to overcome the master terminal vulnerability issues. It is a token-based protocol. Modbus protocol assembles the request message transmitted from the remote terminal to the master terminal into PDU which is an amalgam of the data request and a function code. PDU changes over into an application information unit by including function code fields at the OSI layer. Similarly master terminal will send a reply to the remote terminal. However, due to extra cable and other communication issues, it is not preferred for real-time communication.

B. DNP3: Distributed Network Protocol (DNP) protocol is based on the Enhanced Performance Architecture (EPA) model. EPA is a streamlined type of OSI layer architecture. It was developed by Harris, Distributed Automation Products [35]. The motive for DNP3 protocol development was to obtain open and standards-based interoperability between RTUs, MTU, and Programmable Logic Controller (PLC). Datalink layer convention, transport functions, application conventions, and data link library are the core components of the DNP3 protocol. A user layer is appended to the EPA architecture which is responsible for multiplexing, data fragmentation, prioritization and error checking, etc. In the layered architecture of the DNP3 protocol, the application layer details the packet design, services, and procedure for the application layer. This message is then forwarded to the pseudo-transport layer which forwards the segmented data unit to the data link layer [37]. It further forwards the message to the physical layer [41]. It supports multiple-slave, peer-to-peer (P2P), and multiple-master communication.

C. IEC 60870-5 Protocol: The International Electro-Technical Commission (IEC) 60870-5 protocol also follows the EPA model. The application layer is included as an additional top layer of EPA architecture which indicates the functions related to the telemetry-control framework. Telecontrol framework-based variations e.g. T101, T102, T103, T104 characterize diverse particulars, data objects, and function codes at the application convention level [42]. For efficient transmission, the DNP3 layer stack adds a pseudo-transport layer, but it is not used in IEC 60870-5.

D. Foundation Fieldbus Protocol: This protocol was presented by FieldComm Group [43]. The user, application,

data link, and physical, the four-layer stack is used in Foundation Fieldbus. The architecture of Foundation Fieldbus follows the OSI layer model in which the user layer is added as an additional top layer of the application layer. The user layer acts as a gateway between software programs and field devices. Easy process integration, multifunctional devices, open standard, decrease massive wire cost features superior it from other protocols.

E. Profibus Protocol: Process Field Bus (Profibus) protocol was promoted by BMBF (Germany). The communication of data between MTU and RTUs is a cyclic process. MTU reads RTUs input data and writes RTUs output data. Field Bus Message Specification (FMS), Distributed Peripheral (DP), and Profibus Variations (PA) are the three versions of the Process Field Bus (Profibus) protocol. Profibus is most popularly used in discrete manufacturing and process control [35].

F. IEC 61850 Protocol: The International Electro-Technical Commission (IEC) 61850 protocol was developed by the IEC Technical Committee 57 [44]. A group of manufacturers (ABB, Alstom, Schneider, SEL, Siemens, Toshiba, etc.) proposed this protocol to improve the interoperability of equipment [45]. This protocol differs from other OSI reference models in the sense that it also describes how data is executed and stored apart from how it is sent and received. The source and destination addresses are 48 bits each [46]. IEC 61850 is generally used in electrical substations for communication among intelligent electronic devices [44]. Moreover, IEC 61850 abstract data models can be mapped to many other protocols, e.g. MMS, GOOSE, and SMV [47].

SCADA communication conventions have advanced from restrictive to business/open-source conventions. SCADA framework's unwavering quality relies on its correspondence conventions. A brief and comparative analysis of communication protocols available for SCADA is in Table 1. Since DNP3, IEC 60870-5-101, and Foundation Fieldbus are open Standards [30]. These protocols are more widely used. DNP3 and IEC 60870-5-101 focus on providing the first-level solutions of Data Acquisition Interoperability. These are required to communicate outside the substation [23]. DNP3 allows SCADA systems to poll at different frequencies while IEC 60870-5-101 poll at the same frequency which helps it is a case of limited bandwidth. The packet size in DNP is larger than IEC 60870-5-101. Hence for long-distance DNP3 protocol is favored. Modbus is, for the most part, utilized for applications where the volume of information exchange is low [19]. It is a quick and safe convention, and a ton of data is loaded in one message [18].

Modbus is a single-layer protocol while DNP3, Foundation Fieldbus uses four-layer architecture. Modbus is mainly targeted for low-volume data applications. Only DNP3-SA and Profibus support encryption and authentication control, while Modbus is an insecure communication protocol. IEC-6870-5-101 and IEC 61850 do not support encryption but allow authentication control. Many factors affect the protocols selection for communication, for example, the utility of the system, location where the SCADA system will be implemented. Choosing the best protocols ensures that if needed the developed system will have good potential for scalability. Systems should have the flexibility to incorporate security in communication protocols.

Table 1. ICS Communication Protocols

Attribute	Modbus	DNP3	IEC 60870-5-101	Foundation Fieldbus	Profibus	IEC 61850
Year	1979	1993	1995	2004	1989	2005
Organization	Gould Modicon	Harris, Distributed Automation Products	IEC	FieldComm Group	Promoted by BMBF (Germany)	EC Technical Committe57
Number of Layers	1	4	3	4	3	3
Addressing	8-bit address	16-bit source and destination addresses	0,8,16-bit addresses are supported	8,16, 32-bit addresses are supported	7-bit address (0-3 address are used by master and the rest by slaves)	48-bit source and destination addresses
Users	Target low data application	China, North America, and Australia	Europe, China	America and France	All over the World	All over the World
Source	Open-source	Open-source	Commercially Available	Open-source	Commercially Available	Open-source
Security State	No encryption and authentication control	DNP3-SA Supports encryption and authentication control	No encryption and authentication control	No encryption and authentication control	Supports encryption and authentication control	No encryption and authentication control

Apart from these traditional communication protocols, in IIoT based SCADA other IoT protocols, e.g. Zigbee, Bluetooth Low Energy (BLE), Long Range (LoRA), etc. are used for communication.

1. Zigbee: Zigbee, an IEEE 802.15.4 based communication protocol, is developed by Zigbee alliance. Zigbee was standardized in 2003 and revised in 2006. The range of Zigbee communication is between 10 to 100 meters line-of-sight depending on environmental characteristics. Zigbee architecture includes three types of devices, i.e. Fully Functional Device (FFD) (act as a router), Reduced Functional Device (RFD), and a coordinator. It enables Wireless Personal Area Networks (WPAN) and provides a communication protocol with low-power digital radios. In short, it is a low data rate, low-power, and low communication range wireless ad hoc network which is secured by 128-bit symmetric encryption keys and a data rate of 250 kbps.

2. Bluetooth: Bluetooth special interest group developed with a motive to decrease the power consumption as compared to classic Bluetooth technology. The protocol stack in BLE is the same as in classic Bluetooth. BLE supports a quick transfer of small data packets with a 1 Mbps data rate. It does not support data streaming. It follows master-slave architecture. Masterbehave is like a central device that connects to many slaves, resulting need for these devices power-efficient. The energy is saved by keeping the slave nodes in sleep mode by default and waking up these nodes periodically to send data packets to the master node and receive control packets from the slave node. BLE is 2.5 times more energy-efficient than Zigbee [48].

3. LoRA: LoRA, a long-range communication protocol, was developed by Cycleo of Grenoble, France. In 2012, it was acquired by Semtech. It supports long-range communication up to 10 Km and a data rate less than 50kbpsnwith low power consumption. It is most suitable for non-real-time applications which is fault-tolerant. It works in the physical layer combined with Long Range Wide Area Network, in the upper layers.

Apart from this device-to-device communication protocol, other application layer protocols e.g. MQTT, Constrained Application Protocol (CoAP), and Message Queue Telemetry Transport (MQTT) is developed for IoT environment as HTTP, HTTPs is not suitable due to resource constraints.

1. CoAP: CoAP, a specialized Internet Application Protocol, is a replacement of HTTP for resource constraint IoT-based devices [49,50]. Low overhead, multicast, and ease to use are the basic pillar for IoT devices. IoT devices have much less memory and power supply in comparison to traditional Internet devices. It uses an Efficient XML Interchanges (EXI) data format that leads to a more space-efficient protocol. It also supports resource discovery, message exchange, auto-configuration, built-in header compression, etc. It uses four types of message, i.e. confirmable, non-confirmable, acknowledgment and reset. Confirmation messages are used for reliable communication; acknowledge message is used for the successful delivery of the message. By default, CoAP is bound to User Datagram Protocol (UDP), and security is provided using Datagram Transport Layer Security.

2. MQTT: MQTT, a publish-subscribe-based messaging protocol, was developed by IBM. It is client/server protocol, where clients act as a publisher or subscribers and the server behaves like a broker. The information is arranged in a topics hierarchy. Topics names are generally in text format, which increases the overhead. A client sends a control message to the server when it wants to publish a message. The server distributes the message to the subscribers later. Neither publisher nor subscribers need to share their configurations, location. MQTT is supported over Transmission Control Protocol (TCP), which restricts its use for all types of IoT devices. MQTT control message size varies between 2 bytes to 256 megabytes. It supports 14 control messages to manage publisher-broker-subscriber communication [51].

Apart from MQTT, a few extensions, e.g. MQTT-S/ MQTT-SN are proposed which specifically focus on cost and power-effective solutions. These include replacing topic text with topic Ids, buffering procedure for nodes in sleep mode, etc. MQTT-SN is proposed to use over UDP or Bluetooth.

The communication network protocols do not support security features. Therefore, they are prone to cyber-attacks. In the next section, we discuss the inherent vulnerability of SCADA systems by looking at reported attacks.

3. Intrusions into the Control Networks

In this paper, we discuss and model cyber intrusions into the control networks launched from outside the network as shown in Fig. 4.

State-space-based approaches, i.e., Markov chains and PNs, are powerful to quantitatively model security as well as dependability measures.

However, the state space grows exponentially as the number of components increases, which makes it difficult to compute the steady-state probability. This paper is focused on steady-state analysis using the state-space-based modeling tool, i.e., GSPNs. Before discussing intrusions into the control networks, we will briefly introduce PNs and their extension, GSPNs, which will be used throughout this paper. Detailed explanations can be found in [21], [52], and [53].

3.1. Petri Nets and GSPNs

A PN also called a place transition net, is a pictorial mathematical model of information flow named after its developer, Petri [54]. A PN comprises a set of places drawn by circles, a set of transitions drawn by bars, and a set of directed arcs. Places and transitions are connected by arcs from places to transitions and from transitions to places. Places may contain tokens, which are drawn as black dots residing in the circles. A transition is enabled if all of its input places contain at least one token. An enabled transition fires by removing one token in each input place

and generating one token in each output place. The execution of a PN is controlled by the movement of tokens, while the distribution of tokens over places is denoted by a marking corresponding to the notion of a state in a Markov chain. A PN is defined as follows [52].

Definition 1: A PN is a four-tuple (*P, T, A,* and *M*0), where:

1) P = {P1, P2, . . ., Pn} is a set of places;
2) T = {t1, t2, . . ., tm} is a set of transitions;
3) A ⊆ {P × T} ∪ {T × P} is an arc set;
4) M0 = (m01,m02, . . .,m0n) is the initial marking.

A GSPN defines two different classes of transitions: 1) immediate transitions (drawn as boxes) and 2) timed transitions (drawn as bars). In a GSPN, an enabled immediate transition fires immediately, whereas an enabled timed transition fires after an exponentially distributed firing time. The state space is then divided into two subsets, one containing vanishing states (markings), which enable at least one immediate transition, and the other containing tangible states (markings), which enable only timed transitions. A GSPN is said to be k-bounded if for any marking, the maximum number of tokens in any place is less than or equal to k. Therefore, a k-bounded GSPN is isomorphic to the continuous-time Markov chain and the quantitative analysis of GSPNs can be transferred to that of Markov models [53]. The definition of a GSPN is given as follows.

Definition 2: A GSPN is a four-tuple (PN, T1, T2, and λ), where:

1) PN = (P, T, A, M0) is the underlying place transition net;
2) T1 ⊆ T is a set of timed transitions;
3) *T*2 ⊂ *T* is a set of immediate transitions;
4) *T*1 ∩ *T*2 = *φ, T*1 ∪ *T*2 = *T*;
5) *λ = (λ*1, *λ*2, . . ., *λk)* is a set of nonnegative real numbers:
   a) *λi* denotes a firing rate if *ti* ∈ *T*1;
   b) *λi* denotes a firing weight if *ti* ∈ *T*2.

PNs and GSPNs are versatile and hence, find them been applicable in a variety of systems engineering.

3.2. Modeling Intrusions into the Control Networks

Motivated by the cryptography and FW protection against cyberintrusions proposed in our earlier work [8] and the password/FW models proposed in [54], in this paper, scenarios to model intrusions into the digital control networks in HPPs: the cyberattacks launched from the level 4 and the level 5 are modeled. As described in Section II, the cybersecurity level of the ICS architecture is five. The application workstation in level 3 can connect the terminal server (TS) residing in the plant's main control room through the remote desktop connection. However, if the malicious attacker intrudes into the supervisory control from the internet or external network and successfully logs into the TS, i.e., cracks the correct password, he can immediately penetrate the plant control networks and do severe damage. The intrusion scenario is thus illustrated in Fig. 4 by using a GSPN. The attacker from the Internet can intrude into the corporate WAN through the DMZ, if the attacker guesses the correct password then the attacker penetrates the corporate WAN successfully. Communications between WAN and LAN as well as between LAN and Control networks are protected by FWs. The attacker can penetrate the FWs if the malicious packets match the FW access control rules. Therefore, once the FWs are penetrated, the site LAN and the control network are intruded as well. The attacker then penetrates the plant control networks by logging into the TS as described in the scenario [8]. We depict the intrusion scenario by using a GSPN with 2 units of plant control networks, as shown in Fig. 4.

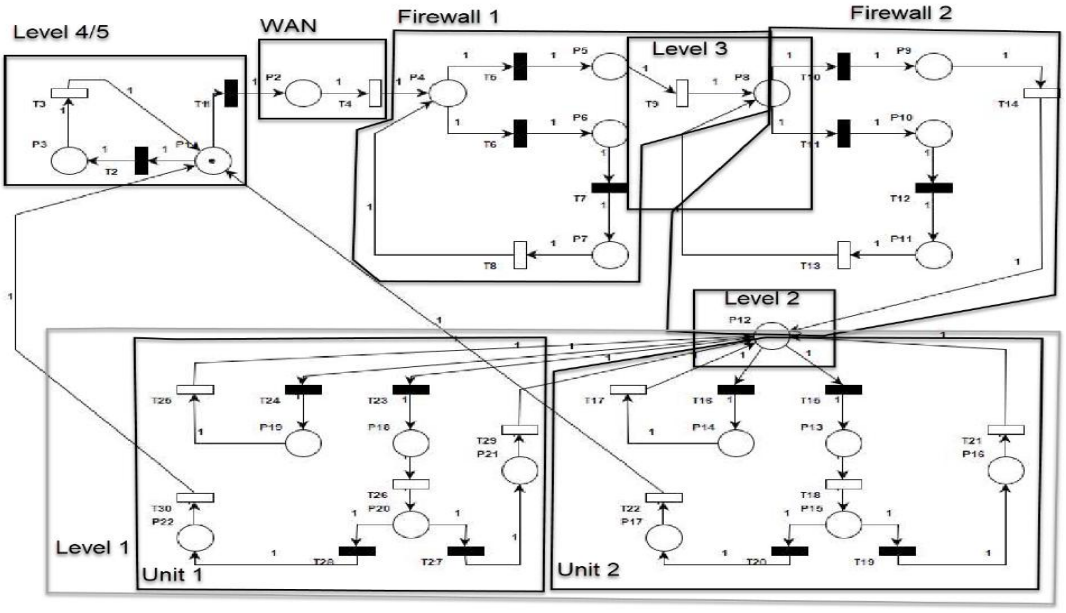

Figure 4. GSPN Model for ICS Architecture

3.2.1. Quantitative Analysis of Scenario

To quantitatively evaluate the intrusion probability of control networks launched from the enterprise network, we need to define the GSPN:

GSPN1 = (PN1, T1, T2, λ)

PN1 = (P, T, A, M0)

P = {P1, P2, P3, P4, P5, P6, p7, P8, P9, P10, P11, P12, P13, P14, P15, P16, P17, P18, P19, P20, P21, P22}

T = {t1, t2, t3, t4, t5, t6, t7, t8, t9, t10, t11, t12, t13, t14, t15, t16, t17, t18, t19, t20, t21, t22, t23, t24, t25, t26, t27, t28, t29, t30}

M0 = (1, 0, 0, 0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)

T1 = {t3, t4, t8, t9, t13, t14, t17, t18, t21, t22, t25, t26, t29, t30},

T2 = {t1, t2, t5, t6, t7, t10, t11, t12, t15, t16, t19, t20, t23, t24, t27, t28}

λ = {λ1, λ2, λ3, λ4, λ5, λ6, λ7, λ8, λ9, λ10, λ11, λ12, λ13, λ14, λ15, λ16, λ17, λ18, λ19, λ20, λ21, λ22, λ23, λ24, λ25, λ26, λ27, λ28, λ29, λ30 } (1)

Where P1 denotes the initiation of the password cracking of local SCADA systems, P2 denotes the successful login, p3 denotes the failed login to the local SCADA, P4 denotes the initiation of cracking of FW rule of DMZ, P5 denotes the success of cracking DMZ Firewall, P6 failure to crack DMZ FW, P7 denotes denial of attack on FW attack, P8 denotes the initiation of cracking of FW rule of levels 3 LAN, P9 denotes the success of cracking FW rule of level 3 LAN, P10 failure to crack FW rule of level 3 LAN, P11 denotes denial of attack on FW attack, P12 denotes initiation of the password cracking of local SCADA systems of units 1 to units N, P13, and P18 denotes the successful login to the local SCADA, P14, and P19 denotes the failed login to the local SCADA, P15 and P20 denotes the knowledge discovered from the SCADA, P17 and P22 denotes the executed disruptive sequence of switching attacks from the SCADA, and P16 and P21 denotes the failure to execute switches due to sequentially interlocking blocks.

We assume that the probability to guess the correct password is 0.01. The firing weights of λ1 = 0.01, λ2 = 0.99, We also assign the firing rates λ3 = λ4 = 10−6 and λ6 = 0.5×10−6 representing response delay times the rest of the rates are depicted in table 2, and as proposed in [8]. From the initial marking M0 (S0 in our case) and by a sequence of transition firings, we can obtain the reachability graph, as shown in Fig. 5. The GSPN is one-bound and contains 22 markings. Among these markings, S0, S3, S4, S7, S8, S11, S16, and S17 are vanishing, whereas S1, S2, S5, S6, S9, S10, S12, S13, S14, S15, S18, S19, S20, and S21 are tangible. Therefore, the transition matrix P can be composed into four submatrices for the set of vanishing markings (V) or adsorbing states ($\mathbf{n_a}$) and the set of tangible markings (T) or transient states ($\mathbf{n_t}$) for immediate and timed transitions respectively.

We begin our analysis by numbering the states in the MC such that the $\mathbf{n_a}$ absorbing states occur first and writing the transition probability matrix P as

$$P = \begin{bmatrix} \mathbf{C} & \boldsymbol{D} \\ \boldsymbol{E} & \boldsymbol{F} \end{bmatrix} \quad (2)$$

Where;

C := (cij), cij = Prob[Mi → Mj], Mi ∈ V and Mj ∈ V;

D := (dij), dij = Prob[Mi → Mj], Mi ∈ V and Mj ∈ T;

E := (eij), eij = Prob[Mi → Mj], Mi ∈ T and Mj ∈ V;

F := (fij), fij = Prob[Mi → Mj], Mi ∈ T and Mj ∈ T.

and T denotes the set of tangible states and V the set of vanishing states. C describes the transition probabilities between vanishing states and F specifies the probabilities between tangible states.

Once in an absorbing state, the process remains there, so C is the identity matrix with all elements $\mathbf{p_{ii}} = 1, 1 \leq i \leq \mathbf{n_a}$. E is the $\mathbf{n_t} \times \mathbf{n_a}$ matrix describing the movement from the transient to the absorbing states, and F is the $\mathbf{n_t} \times \mathbf{n_t}$ matrix describing the movement amongst transient states. Since it is not possible to move from the absorbing to the transient states, D is the $\mathbf{n_t} \times \mathbf{n_t}$ zero matrix.

By using the values described in Table 2 above, the transition matrix P formed is a 22 x 22 matrix. The dimensions of C, D, E, and F are 8 × 8, 8 x 14, 14 × 8, and 14×14, respectively.

The steady-state distribution $\tilde{\boldsymbol{\pi}}$ of the embedded Markov chain (EMC) is given by [52]

$$\tilde{\boldsymbol{\pi}} P = \tilde{\boldsymbol{\pi}} \text{ and } \sum_{\mathbf{Mi} \in \mathbf{T} \cup \mathbf{V}} \tilde{\boldsymbol{\pi}}_{\mathbf{i}} = 1 \quad (3)$$

Since an enabled immediate transition fires immediately, it is obvious that the time spent by each vanishing marking is zero. The matrix P can be reduced to a smaller matrix P' where only tangible markings for timed transitions are considered. The reduced matrix P' is thus obtained as follows [52]:

$$P' = F + E \times (I - C)^{-1} \times D. \quad (4)$$

Table 2. Transition firing rates

λ1	λ2	λ3	λ4	λ5	λ6	λ7	λ8	λ9	λ10
0.01	0.99	10E-6	10E-6	0.01	0.99	1	0.5E-6	10E-6	0.01
λ11	**λ12**	**λ13**	**λ14**	**λ15**	**λ16**	**λ17**	**λ18**	**λ19**	**λ20**
0.99	1	10E-6	0.5E-6	0.01	0.99	10E-6	10E-6	0.9987	0.0013
λ21	**λ22**	**λ23**	**λ24**	**λ25**	**λ26**	**λ27**	**λ28**	**λ29**	**λ30**
10E-6	0.5E-6	0.01	0.99	10E-6	10E-6	0.9987	0.0013	10E-6	0.5E-6

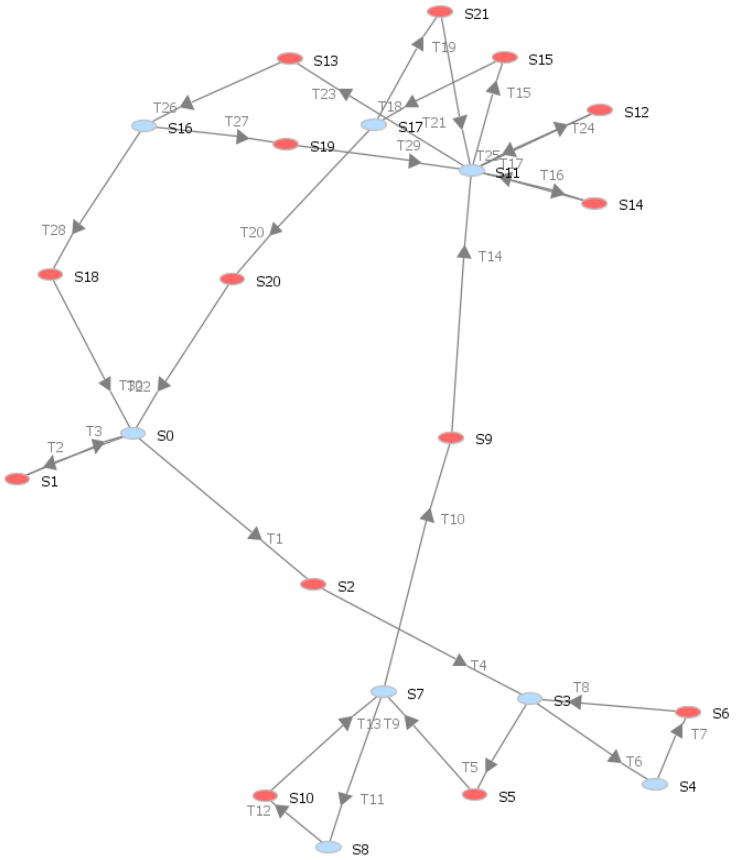

Figure 5. Reachability graph of modeling intrusions launched from Enterprise Network

Therefore, we formulate this problem with the continuous Markov chain instead of the semi-Markov chain. The steady-state distribution, π of the continuous-time Markov chain is expressed by the reduced EMC given by [52]:

$$\tilde{\boldsymbol{\pi}}P' = \tilde{\boldsymbol{\pi}} \text{ and } \sum_{\mathbf{Mi}\in\mathbf{T}} \tilde{\boldsymbol{\pi}}_{\mathbf{i}} = 1 \quad (5)$$

The steady-state probability πj can be calculated by the mean time spent in marking Mj divided by the mean cycle time [52]. The steady-state solution πj is given as

$$\boldsymbol{\pi_j} = \begin{cases} \frac{\{\tilde{\pi}_j \boldsymbol{X} (\sum_{k:tk\in ENT(Mj)} \lambda_k)^{-1}}{\{\sum_{Ms\in T} \tilde{\pi}_s \boldsymbol{X} (\sum_{k:tk\in ENT(Mj)} \lambda_k)^{-1}} \text{ if } M_j \in T \end{cases} \quad (6)$$

where $t_k \in EN(Mj)$ denotes that the transition t_k is enabled in marking Mj.

The steady-state distribution, $\tilde{\boldsymbol{\pi}}$, for the tangible markings after solving equations (5) and (6) is as follows:

$\tilde{\boldsymbol{\pi}}$ = (π_1 = 0.00998, π_2 =0.00181, π_5 = 0.00544, π_6 = 0.19958, π_9 = 0.23587, π_{10} = 0.00544, π_{12} = 0.02109, π_{13} = 0.02207, π_{14} = 0.02207, π_{15} = 0.02339, π_{18} = 0.01055, π_{19} = 0.21092, π_{20} = 0.01104, π_{21} = 0.22075.

4. Cybersecurity Standards and the Enhanced Cyberphysical Frameworks

There are many high-level risk assessment methods (or frameworks) that an organization can use to support the implementation of a cybersecurity risk assessment for the smart grid. Whilst these risk assessment methods are useful, they do not provide specific guidelines for the peculiarities of the smart grid. For example, in the smart grid, cyber-attacks can have physical impacts on the quality of energy supply or cause damage to power equipment. Furthermore, attacks could result in safety-related incidents happening, resulting in injury or loss of life. In this context, it would be helpful to provide specific guidance on how to assess these aspects.

4.1. IEC 62443 (ISA 99)

Represents a set of security standards for IACS prepared by the IEC technical committee. The goal of these standards is to provide a flexible framework that can address vulnerabilities in IACS and to apply required mitigations systematically. The concrete standard that was analyzed is IEC 62443-3-3:2013 System security requirements and security levels [55] that defines the security requirements for control systems related to the seven requirements defined in IEC 62443-1-1 and assigns system security levels to the system that is being constructed. The IEC 62443-3-3:2013 was selected since it represents the system level standard that can add diversity to the analysis.

4.2. ISO/IEC 27001 and 27002—ISO 27001

Represents one of the best-known IT security standards

that is recognized all around the world. The official title of the standard is ISO/IEC 27001:2013; Information technology—Security techniques—Information security management systems—Requirements [56]. Its supplementary standard is ISO 27002 [57] focuses on the information security controls that organizations might choose to implement and these controls are also listed in Annex A of ISO 27001. Although compliance with ISO 27001 standard alone would not be enough for securing the ICS ecosystem, this standard was selected as one general-purpose security standard that has the requirements that can be applied to different sectors.

4.3. NIST SP 800-53

Represents the guideline that is published by NIST with the official title: Special Publication (SP) 800-53 Recommended Security Controls for Federal Information Systems and Organizations (Revision 5). It is intended to be used as a toolbox containing a collection of safeguards, countermeasures, techniques, and processes to respond to security and privacy risks [58]. This guideline is versatile enough to be applied for the IT systems as well as ICS systems and even if originally aimed at systems that reside in the US, it is well recognized and applied worldwide. This publication is selected as a guideline representative.

4.4. NERC CIP

Represents the set of regulations that define how the bulk electric systems (BES) prepare for cyber and physical threats that can affect the reliability of the system. Policies are required for defining, monitoring, and changing the configuration of critical assets, as well as governing access to those assets. NERC is subject to oversight by the US Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada [59]. All North American bulk power system owners, operators, and users must comply with NERC CIP standards. NERC CIP was selected as one of the most respected representatives of the regulatory type of documents and the publication with the most occurrences during the literature review.

4.5. Proposed Enhanced Cyberphysical Frameworks

The coupling of the power infrastructure with complex computer networks substantially expands the current cyber-attack surface area and will require significant advances in cyber security capabilities. Strong security metrics are necessary to ensure security-based decisions accurately reflect a realistic understanding of cyber risk. NIST [58] specifically addresses this requirement and recommends research in tools and techniques that provide quantitative notions of risks, that is, threats, vulnerabilities, and attack consequences for current and emerging power grid systems.

The main goal of the framework is to depict all possible attack paths in the digital control network (smart grid architectures), evaluate the security level of the smart grid through security metrics, and assess the effectiveness of defense strategies. The proposed framework is shown in Figure 6 can be deployed in layer 3.5 of the Purdue architecture. There are five steps in the framework: i) preprocessing, ii) security model generation, iii) visualization and storage, iv) security analysis, and v) changes and updates.

We explain each step as follows:

In step 1, the security decision-maker provides inputs needed to construct a smart network. The inputs required are the total number of nodes, the network topology, and the vulnerability information for each node. The inputs are fed into the SG Generator. The smart grid Generator creates a smart grid network with a specified network topology consisting of levels and nodes with their vulnerability information. The network topology is fixed after the generation. The security decision-maker also selects the security metrics from a pre-defined metric pool which will be used as an input into the security analysis phase.

In step 2, the security model generation is performed. Our security model is developed based on the Purdue model in which five layers are used to represent the network reachability information at the uppermost level and the vulnerability information at the lower level, respectively. Specifically, the Security Model Generator takes the constructed network with topology and vulnerability information as inputs and automatically computes all possible attack paths in the SG network.

In step 3, the attack paths generated from the Security Model Generator are visualized in the form of a reachability / coverability graph, depicting the transient and absorbing states.

In step 4, the security analysis is carried out for the SG network. The attack vectors are taken as the input into the Security Evaluator along with the determined security metrics. Based on the metrics, the Security Analysts can perform one of the two options. One is to output the analysis results directly and the other is to generate a text file and import the file into the analytic modeling and evaluation tool named Platform Independent Petri net Editor (PIPE) [60] which computes the security analysis results. The security metric is selected from a pre-defined metric database.

In step 5, any changes caused by the defense strategies are captured to update model inputs. Based on the security analysis results, the security decision-maker knows which part of the SG is the most vulnerable, thus being able to decide proper defense strategies. The deployment of the defense strategy changes either the vulnerability information (e.g., eliminates a specific vulnerability in a smart grid node or mitigates the effect caused by the vulnerability) or the topology information, which should be updated and taken as the input to the Security Model Generator. When choosing the defense strategies, the security decision-maker can also assess the effectiveness of different strategies via the framework by using security metrics, comparing their effects, and choosing the best one among them.

5. Analysis

In this section, we present the dependability analysis method to evaluate industrial control systems with the proposed SPN model. We define three metrics of dependability and provide a detailed method to calculate them. We address the issue of state-space explosion in computing as well.

A. Metrics

In this paper, we consider three dependability metrics, i.e. reliability, availability, and maintainability for digital control networks in smart grid. Reliability is used to evaluate the capability to continuously provide services without failures [61]. In detail, it can be defined as the probability that the digital control networks work correctly during the period [0, t], i.e.,

$$R(t) = Pr\{X > t\} = e^{-\lambda t} \text{ and } R(0) = 1 \quad (7)$$

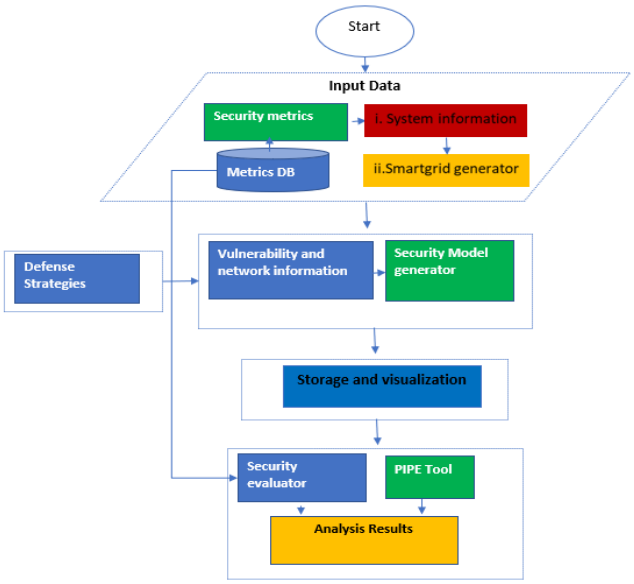

Figure 6. Proposed Framework

where the system is operational at time zero and the failure distribution is exponentially distributed with a constant failure rate λ. The steady-state probability of reliability (Rel) and mean time to failure (MTTF) are given as follows:

$$Rel = R(\infty) = 0 \text{ and } MTTF = 1/\lambda \quad (8)$$

Maintainability is defined as the probability that a failed system will be restored to an operable state within a specified downtime t and is given by [61]

$$M(t) = 1 - e^{-\mu t} \quad (9)$$

where t denotes the downtime (i.e., time to repair) and the repair distribution is exponentially distributed with a constant repair rate μ. The probability of maintainability (Mnt) as t approaches infinity and the meantime to repair (MTTR) is given by

$$Mnt = M(\infty) = 1 \text{ and } MTTR = 1/\mu \quad (10)$$

Availability is defined as the fraction of time that the system provides correct services during an observation period, and is dependent on reliability and maintainability [61]. MTTF reflects how good the reliability of each component is and MTTR reflects how good the maintainability is. To achieve high steady-state availability, the MTTF should be designed as high as possible and the MTTR as low as possible. Therefore, we are interested in the steady-state availability analysis that the system provides correct services of data transmission from the plant network to the enterprise network or vice versa. The steady-state availability is given as:

$$AVL = \sum_j \pi_j \quad (11)$$

Where πj is the steady-state solution corresponding to the state j where the system is available, i.e., providing correct services. The steady-state solution π can be calculated by using equations 1 to 6 defined above.

B. Model Analysis Results

In this subsection, we present the calculation results of the reliability and availability from the steady-state aspect. The proposed method involves two steps: the analysis of the equivalent continuous-time Markov chain and the computation of reliability and availability. Figure 7 depicts the steady-state probabilities for the tangible states of the Purdue equivalent Purdue model, it can be deduced that states P5, P12, and P14 corresponding to DMZ, level 2, and Unit LAN respectively have a high probability of an intrusion if the attack is initiated from the enterprise network, conversely, state P2 corresponding to a WAN is unlikely to be affected by an intrusion launched from the internet.

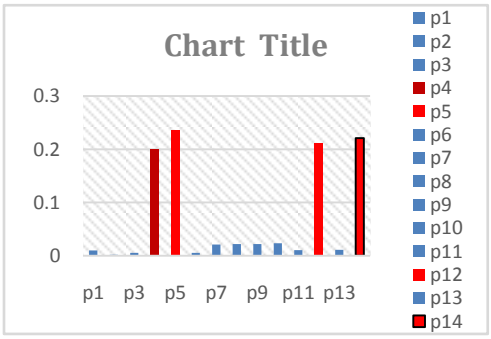

Figure 7. Steady state probability

Several parameters are needed in calculating the steady-state availability, namely the failure rates (λ) and repair rates (μ). The failure rates are given precisely according to the specification of each component, while the repair rates are approximated based on the maintenance procedures.

Having calculated the steady-state probabilities in section 4, we can compute the reliability and availability. For the reliability, it can be seen that only the initial state is reliable, and the rate of leaving the reliable state M0 is λ_1. Thus, we can have the steady-state reliability as:

$$R = e^{-0.99t}$$

Solving equation (11), assuming that the initial state (M0) is reliable and not susceptible to any intrusion, then:

Ava = 1 – (0.00181 + 0.00544 + 0.19958 + 0.23587 + 0.00544 + 0.02109 + 0.02207 + 0.02207+ 0.02339 + 0.01055 + 0.21092+0.01104+0.22075)

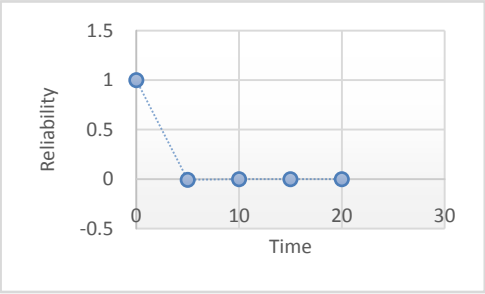

Figure 8. Steady state availability

Then steady-state availability is 0.99002. Therefore, we demonstrate that the proposed framework is highly dependable. We can further improve the steady-state availability by improving cybersecurity and maintenance policies.

6. Conclusions and Future Works

In this paper, we discuss the cyber-physical security and dependability issues of digital control systems in safety-HPPs.We also discuss and compare cybersecurity standards, We use GSPNs to model intrusions into digital control networks of HPPs. We then, propose the cyber framework, that conforms to the NIST framework. We also use GSPNs to evaluate the steady-state availability and show that the proposed framework is highly dependable. To reduce the computation complexity, a technique is employed by partitioning the set of transitions into timed and immediate transitions. The results show that mitigation measures are required in the DMZ, level 2, and local area networks in digital control networks of smart grids to enhance resilience to cyber attacks. In future work, we will use the datasets such as failure rates, repair rates, failed login attempts, and firewall rates from a working power plant in Zambia to model resiliency and propose mitigation to improve the RAM metrics. Furthermore, we shall propose an enhanced framework based on GSPNs and Bayesian Nets and compare the results with our current work.

ACKNOWLEDGEMENTS

I am grateful to the Lord God Almighty for the gift of life and His amazing grace. My family at large especially my little boy Salifyanji, thanks for accepting my absence to achieve this challenging mission. I also wish to acknowledge the guidance of my supervisor Dr. Simon Tembo, the University of Zambia School of Engineering, and all the contributors for making this lonely journey awesome.

REFERENCES

[1] Africa, https://www.hydropower.org/region-profiles/africa.

[2] IEA (2020), *SDG7: Data and Projections*, IEA, Paris https://www.iea.org/reports/sdg7-data-and-projections.

[3] "The National Energy Policy 2019." Ministry of Energy Integrated Resource Plan, 21 Oct. 2021, https://www.moe.gov.zm/irp/download/the-national-energy-policy-2019-2/.

[4] Final Report - Moe.gov.zm. https://www.moe.gov.zm/?wpfb_dl=45.

[5] "Home." Ministry of Energy Integrated Resource Plan, 1 Sept. 2021, https://www.moe.gov.zm/irp/.

[6] Energy Sector Report 2020 - Erb.org.zm. https://www.erb.org.zm/reports/esr2020.pdf.

[7] Press Statement - Erb.org.zm. https://www.erb.org.zm/press/statements/2021-11-26_PressStatement.pdf.

[8] Lukumba Phiri, Simon Tembo. Computer Science and Engineering, 2022 12(1), pp. 1-14 Published Online: January 21, 202210.5923/j.computer.20221201.01.

[9] Antonio Marino, Enrico Zio, A framework for the resilience analysis of complex natural gas pipeline networks from a cyber-physical system perspective, Computers & Industrial Engineering, Volume 162, 2021, 107727, ISSN 0360-8352, https://doi.org/10.1016/j.cie.2021.107727.

[10] Cho, Chi-Shiang et al. "Cyberphysical Security and Dependability Analysis of Digital Control Systems in Nuclear Power Plants." *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 46 (2016): 356-369.

[11] Nelson H. Carreras Guzman, Igor Kozine, Mary Ann Lundteigen, An integrated safety and security analysis for cyber-physical harm scenarios, Safety Science, Volume 144, 2021, 105458, ISSN 0925-7535, https://doi.org/10.1016/j.ssci.2021.105458.

[12] Ivo Friedberg, Kieran McLaughlin, Paul Smith, David Laverty, Sakir Sezer, STPA-SafeSec: Safety and security analysis for cyber-physical systems, Journal of Information Security and Applications, Volume 34, Part 2, 2017, Pages 183-196, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2016.05.008.

[13] Lu T, Guo X, Li Y, et al. Cyberphysical Security for Industrial Control Systems Based on Wireless Sensor Networks. *International Journal of Distributed Sensor Networks*. June 2014. doi:10.1155/2014/438350.

[14] Sun C-C, Liu C-C, Xie J. Cyber-Physical System Security of a Power Grid: State-of-the-Art. *Electronics*. 2016; 5(3):40. https://doi.org/10.3390/electronics5030040.

[15] Xie, Jing & Stefanov, Alexandru & Liu, Chen-Ching. (2016). Physical and cyber security in a smart grid environment. Wiley Interdisciplinary Reviews: Energy and Environment. 5. n/a-n/a. 10.1002/wene.202.

[16] Hawrylak, Peter J., Hale, John, Papa, Mauricio, Edgar, Thomas, Craig, Philip, Wall, Donald, and Hines, Corey. *Cyber Security Analysis for Nuclear Reactor Control Systems (Final Technical Report)*. United States: N. p., 2020. Web. doi: 10.2172/1650024..

[17] Yaacoub JA, Salman O, Noura HN, Kaaniche N, Chehab A, Malli M. Cyber-physical systems security: Limitations, issues and future trends. *Microprocess Microsyst*. 2020; 77: 103201. doi:10.1016/j.micpro.2020.103201.

[18] Uchenna D. Ani, Nneka Daniel, Francisca Oladipo & Sunday E. Adewumi (2018) Securing industrial control system environments: the missing piece, Journal of Cyber Security Technology, 2:3-4, 131-163, DOI: 10.1080/23742917.2018. 1554985.

[19] Yeboah-Ofori, Abel & Abdulai, Jamal-Deen & Katsriku, Ferdinand. (2018). Cybercrime and Risks for Cyber-Physical Systems: A Review. 10.20944/preprints201804.0066.v1.

[20] Kavallieratos, Georgios & Katsikas, Sokratis & Gkioulos, Vasileios. (2019). Towards a Cyber-Physical Range. 25-34. 10.1145/3327961.3329532.

[21] 30 years of GreatSPN Amparore, Elvio Gilberto and Balbo, Gianfranco and Beccuti, Marco and Donatelli, Susanna and Franceschinis, Giuliana," Principles of Performance and Reliability Modeling and Evaluation pages 227--254, 2016,. Springer.

[22] Automation Solutions for Hydropower Plants - Andritz. https://www.andritz.com/resource/blob/334010/ca47bd154c 713b3509acc9472cd134c5/hy-automation-en-data.pdf.

[23] T. J. Williams, "The Purdue enterprise reference architecture," ComputInd, vol. 24, no. 2-3, pp. 141-158, 1994.

[24] ISA, "ANSI/ISA-62443-1-1 (99.01.01)-2007 Security for Industrial Automation and Control Systems Part 1-1: Terminology, Concepts, and Models," in Part 1-1: Terminology, Concepts, and Models, ed, 2007.

[25] C. E. Bodungen, B. L. Singer, A. Shbeeb, S. Hilt, and K. Wilhoit, Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions: McGraw-Hill Education, 2016.

[26] Macola, Ilaria Grasso, et al. "The Five Worst Cyberattacks against the Power Industry since 2014." Power Technology, 24 Jan. 2022,https://www.power-technology.com/features/th e-five-worst-cyberattacks-against-the-power-industry-since2 014/.

[27] Desarnaud, Gabrielle. "Cyber Attacks and Energy Infrastructures: Anticipating Risks." Afficher La Page D'accueil Du Site, https://www.ifri.org/en/publications/etude s-de-lifri/cyber-attacks-and-energy-infrastructures-anticipati ng-risks.

[28] Cybersecurity for Energy Delivery Systems: DOE ... - Congress. https://crsreports.congress.gov/product/pdf/R/R44 939.

[29] Sanger, David E., and Nicole Perlroth. "U.S. Escalates Online Attacks on Russia's Power Grid." The New York Times, The New York Times, 15 June 2019, https://www.nytimes.com/2 019/06/15/us/politics/trump-cyber-russia-grid.html.

[30] "Russia Power Market Outlook to 2030, Update 2021 - Market Trends, Regulations, and Competitive Landscape." GlobalData Report Store, 1 Feb. 2022, https://store.globaldat a.com/report/russia-power-market-outlook-to-2030-update-2 021-market-trends-regulations-and-competitive-landscape/.

[31] Offensive Cyberspace Operations: A Gray Area in ... https://www.bu.edu/ilj/files/2020/08/10.-Article_Bailey.pdf.

[32] "A Cyber Attack in Saudi Arabia Failed to Cause Carnage, but the next Could Be Deadly." The Independent, Independent Digital News and Media, 21 Mar. 2018, https://www.independent.co.uk/news/long_reads/cyber-warf are-saudi-arabia-petrochemical-security-america-a8258636.h tml.

[33] "Ukraine Power Cut 'Was Cyber-Attack'." BBC News, BBC, 11 Jan. 2017, https://www.bbc.com/news/technology-38573 074.

[34] "Ukraine Power Cut 'Was Cyber-Attack'." BBC News, BBC, 11 Jan. 2017, https://www.bbc.com/news/technology-38573 074.

[35] A. Shahzad, S. Musa, A. Aborujilah, and M. Irfan. The SCADA review: System components, architecture, protocols, and future security trends. American Journal of Applied Sciences, 11(8): 1418–1425, 2014.

[36] Udara Perera. Comparisons of SCADA communication protocols for power systems, 2015.

[37] Muhammad Uzair. Communication methods (protocols, format & language) for the substation automation & control.

[38] Tom Sheldon. McGraw-Hill's Encyclopedia of Networking and Telecommunications. McGraw-Hill Professional, 2001.

[39] WINGPATH software development. Modbus protocol, 2004-2017.

[40] RDMS. What is Modbus?, 2016.

[41] Krushna Chandra Mahapatra and S Magesh. Analysis of vulnerabilities in the protocols used in SCADA systems. International Journal of Advanced Research in Computer Engineering & Technology, 4(3), 2015.

[42] IPCOMM. Iec 60870-5-102, 2004-2017.

[43] "Foundation Fieldbus." FieldComm, https://www.fieldcomm group.org/technologies/foundation-fieldbus. Date accessed 16 February 2022.

[44] "Customize Your engineering360 Experience." IEC 61850-8-2 - Communication Networks and Systems for Power Utility Automation – Part 8-2: Specific Communication Service Mapping (SCSM) – Mapping to Extensible Messaging Presence Protocol (XMPP) | Engineering 360, https://standards.globalspec.com/std/13127 190/IEC%2061850-8-2.

[45] Robert Czechowski, Pawel Wicher, and Bernard Wiecha. Cyber security in the communication of scada systems using iec 61850. 2015 Modern Electric Power Systems (MEPS), pages 1–7, 2015.

[46] "IEEE Power & Energy Society." Application Testing of IEC 61850 Based Systems (TR84), https://resourcecenter.iee e-pes.org/publications/technical-reports/PES_TP_TR84_PS RC_120720.html.

[47] Y. Yang, H. Q. Xu, L. Gao, Y. B. Yuan, K. McLaughlin, and S. Sezer. Multidimensional intrusion detection system for IEC 61850-based SCADA networks. IEEE Transactions on Power Delivery, 32(2):1068–1078, April 2017.

[48] Pallavi Sethi and Smruti R. Sarangi. Internet of things: Architectures, protocols, and applications. J. Electrical and Computer Engineering, 2017:9324035:1–9324035: 25, 2017.

[49] N. DeCaro B. Buta and V. Dobrota W. Colitti, K. Steenhaut. Evaluation of constrained application protocol for wireless sensor networks. 2011.

[50] K. Hartke Z. Shelby and C. Bormann. The constrained application protocol (coap). 2014.

[51] Pallavi Sethi and Smruti R. Sarangi. Mq telemetry transport (MQTT) v3. 1 protocol specification. 2010.

[52] F. Bause and P. S. Kritzinger, Stochastic Petri Nets: An Introduction to the Theory, 2nd ed. Braunschweig, Germany: Vieweg, 2002.

[53] Trivedi, Kishor S. "Probability and Statistics with Reliability, Queuing, and Computer Science Applications, 2nd Edition." Wiley.com, 28 Nov. 2001, https://www.wiley.com/en-us/ProbabilityandStatisticswithReliabilityQueuingandComputerScienceApplication2ndEdition-p-9780471333418Trivedi.

[54] K. Yamashita, C.-W. Ten, Y. Rho, L. Wang, W. Wei, and A. F. Ginter, (2020) Measuring systemic risk of switching attacks based on cybersecurity technologies in substations," IEEE Trans. Power Syst., vol. 35, no. 6, pp. 4206–4219, Nov. 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9078877.

[55] International Electrotechnical Commission (IEC). IEC 62443-3-3: 2013 Industrial Communication Networks — Network and System Security—Part 3-3: System Security Requirements and Security Levels. Available online: https://webstore.iec.ch/publication/7033 (accessed on 2 August 2021).

[56] ISO/IEC. ISO/IEC 27001:2013: Information Technology Security Techniques Information Security Management Systems Requirements; ISO: Geneva, Switzerland, 2013.

[57] ISO/IEC. ISO/IEC 27002:2013: Information Technology — Security Techniques—Code of Practice for Information Security Controls; ISO: Geneva, Switzerland, 2013.

[58] National Institute of Standards and Technology (NIST). NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations. Available online: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final (accessed on 3 August 2021).

[59] North American Electric Reliability Corporation (NERC). CIP Standards. Available online: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx (accessed on 3 August 2021).

[60] "Platform Independent Petri Net Editor 2." Platform Independent Petri Net Editor 2, http://pipe2.sourceforge.net/.

[61] Helerea, Elena. "Interconnections between Reliability, Maintenance and Availability." IFIP Advances in Information and Communication Technology, 19 Aug. 2016, https://www.academia.edu/27901809/Interconnections_between_Reliability_Maintenance_and_Availability.