International Journal of Advances in Scientific Research and Engineering (ijasre)

E-ISSN : 2454-8006

DOI: 10.31695/IJASRE.2022.8.5.1

Volume 8, Issue 5
May - 2022

Evaluating the Security Posture and Protection of Critical Assets of Industrial Control Systems in Zambia

Lukumba Phiri[1], and Simon Tembo[1]

[1]Department of Electrical and Electronic Engineering

School of Engineering, University of Zambia,

Lusaka, Zambia

ABSTRACT

The number of successful attacks on vital infrastructure has increased, as has the sophistication of the attacks. Many cybersecurity strategies include traditional best practices, but they frequently overlook organizational circumstances and unique critical infrastructure protection requirements. The goal of this qualitative multiple case research was to look into the cybersecurity tactics employed by IT managers and compliance officers to protect critical infrastructure from cyber threats. The participants in this study were IT managers and compliance officials from four Zambian case organizations. The conceptual framework was based on the routine activity theory published by criminologists Cohen and Felson in 1979. Interviews with two IT managers, three compliance officers, and 25 papers relating to cybersecurity and policy governance were used to gather data. Four significant themes emerged from data triangulation: the need for a robust worker training program, prioritizing infrastructure resiliency, the importance of security awareness, and the importance of organizational leadership support and investment. This research uncovered essential tactics that can help OT and compliance professionals enhance their cybersecurity strategy, which can help reduce successful assaults on critical infrastructure. The study findings will contribute to positive social change through an exploration and contextual analysis of cybersecurity strategy with situational awareness of OT practices to enhance cyber threat mitigation and inform business processes.

Keywords: Industrial Control Systems, ICS, SCADA, Operational Technology, OT, CPS, Cyber Security.

1. INTRODUCTION

Industrial Control Systems (ICS) form the backbone of modern-day infrastructure, responsible for the delivery of services considered critical from a societal perspective [1]. Due to their criticality, the Zambian government recently imposed new legislation in the form of Cyber Security, mandating that operators of critical national infrastructure (CNI) conform to a set of baseline principles. This acknowledgment of the threat posed to ICSs from a cyber security perspective comes after several years of high-profile attacks [2],[3], and an increasing number of identified vulnerabilities in common components and software [4],[5].

1.1 Motivation

The Zambian government proposes the formation of national cyber security advising and coordinating council (NCSACC**)** in its Cyber Security and Cyber Crimes Act, 2021[6]. For example, the NCSACC is now advising critical infrastructure operators on how to comply with cybersecurity audits. Furthermore, the act requires that the controller of a critical information infrastructure establish mechanisms and processes, per information security standards, as may be required for the detection of a cyber security

threat concerning its critical information infrastructure [6]. The National Cyber Security Policy [7] was implemented in 2021 by the Ministry of Transportation and Communications to foster effective mechanisms and a well-coordinated governance framework on cybersecurity by creating a secure, reliable, and trustworthy cyber environment that boosts confidence. This is where academia can help the most, by doing research and providing feedback on regulations and related recommendations, thereby improving operators' ability to protect against attacks. This, however, is not without its difficulties. Because of the crucial nature of these systems, access is extremely limited, creating a roadblock for anyone looking to do practical research.

1.2 Problem Statement

The rapid growth in the use of internet-based technologies has resulted in various organizations being subjected to cyberattacks. The classical security measures, such as a firewall, have proved to be inadequate, as hackers deliberately avoid firewall protection. It is, therefore, of paramount importance to find effective solutions that can dynamically and adaptively defend the network systems [2],[3].

There is no or limited information available as to the current state of ICS in Zambia including the factors influencing ICS and how they are governed. This study examined present ICS practices and the environment in Zambia to establish a consolidated ICS cybersecurity framework tailored to Zambia's needs, taking into account new and existing legislation. (Lubobya and Mwila, 2020) [8] and (Chinyemba and Phiri, 2018) [9] have done generic studies on Cybersecurity in Zambia, therefore this study addresses that gap and focuses on ICS.

1.3 Goals of the Research Work

In this study, we use a survey to advance Design Science Research by gathering requirements [10] for a cyber threat modeling and mitigation framework for ICS. The goal of this research is to evaluate the security of a SCADA system and create a Domain-specific language (DSL) that can be used to create a threat model for a single SCADA instance. The objective of this study is to address the current cyber security maturity levels as regards the ICS-SCADA protection in Zambia. We can attain our objective by concentrating on two factors;

a. Identify, at the Zambian level, the thematic areas/indicators of maturity and lessons learned from the ICS-SCADA security practices in critical sectors; and

b. The issuance for policymakers and decision-makers a collection of high-level and context-specific future suggestions that will aid in the process of creating resilient ICS/SCADA in Zambia.

1.4 Research Question

The project focuses on building the threat modeling language for SCADA. In this work, we ask the following research question:

• What is the state of Security in Industrial Control Systems in Zambia?

The sub-questions are as follows:

a. Who is in charge of the procedures?

b. What are the security threats and factors that influence them?

c. What security controls and techniques have been implemented?

d. What strategies do you have to address the convergence of information and operational technologies?

e. Who is in charge of your company's security budget for control systems?

1.5 Main Contributions

This work was conducted in the domain of operation and maintenance related to ICS. The focus of the work was on the provision of insights and artifacts to improve the availability of control systems through enhanced cybersecurity implemented solutions. The major contributions of the work are the following:

a. Identification of cybersecurity issues and challenges – The research contributes by identifying various cybersecurity issues and challenges in ICS operation and maintenance through vast state-of-the-art.

b. Cybersecurity maturity level – The research contributes to information assurance by estimating the existing cybersecurity maturity levels in ICS organizations. The estimation can be used to make recommendations for necessary actions to improve the overall system availability.

DOI: 10.31695/IJASRE.2022.8.5.1

c. A cybersecurity framework – The work proposes a proactive approach to ICS cybersecurity. It formulates a holistic cybersecurity framework to facilitate proactive cybersecurity and enhances cybersecurity resilience. The framework facilitates threat intelligence sharing by organizations so they can remain updated on the latest cyber threats.

The rest of the work is organized as follows; Chapter 2 provides the background information to make a reader familiar with the notions used in this work. Chapter 3 gives information about the methodology applied. Chapter 4 presents and discusses the survey results. And finally, the paper is completed by a conclusion and perspectives in Chapter 5.

2.0. STATE OF THE INDUSTRIAL CONTROL SYSTEMS

In the past, cyberattacks against industrial control systems have occurred all across the world [2]-[9]. The oriental pipelines are described in this chapter, as well as the widely reported 2015 attack on a Ukrainian distribution system operator (DSO), a case of a self-inflicted incident in the Austrian transmission system operator (TSO) system due to a cross-border miscommunication, a case of malware targeting industrial control systems, and a case in Zambia. It also examines the impact of cyber-attacks before concluding with a survey of relevant literature.

2.1 Industrial Control Systems (ICS) Cyber Security: Critical and Exposed

According to TXOne [11], cyber attackers' techniques will shift dramatically in 2021, with more advanced and devastating supply chain attacks than ever before. These new cybercrime developments have created a climate of dread, which is pushing cyber defense research and the discovery of ICS-related Common Vulnerabilities and Exposures (CVEs). Current cybercriminal operations have progressed to the point that a service industry has evolved with a similar business model – ransomware-as-a-Service, according to a timeline of the year's major OT and ICS cyber events (RaaS). Users who want to carry out illicit projects might use a customized platform provided by RaaS service providers. They market their services using a variety of payment schemes, including affiliate programs that provide special offers - for example, if the provider generally takes 25% of the ransom, they might agree to take a reduced amount if the client requests a much greater ransom. RaaS organizations have increased ransom demands in this fashion.

Maze, Lockbit, REvil, and DarkSide are known recently active ransomware gangs, however, their activity levels can fluctuate. For example, the Maze ransomware gang announced its retirement in November 2020 [12]. REvil and DarkSide landed on the wrong side of the US government in the middle of 2021 when their service was used to launch two of the year's most severe ransomware assaults, the Colonial Pipeline cyber disaster, and the Kaseya supply chain attack.

DarkSide's RaaS platform [14] was used in the Colonial Pipeline attack [13], which resulted in a $4.4 million payoff to attackers. REvil's service was used to launch the Kaseya supply chain assault, which exploited CVE-2021-30116 [15], a "zero-day authentication bypass" vulnerability. The REvil organization claimed to have infected over a million machines when they demanded a $70 million ransom [16]. Following these two attacks, both DarkSide and REvil went silent, with REvil reappearing in October as a result of increasing government and law enforcement attention. However, further RaaS development, including new RaaS platforms that incorporate capabilities from prior systems, is possible. The Darkside, REvil, and LockBit 2.0 ransomware families, for example, use tools and strategies from the BlackMatter ransomware [17]. Our investigators suspect, but cannot confirm, that BlackMatter is the DarkSide rebranding. Emotet and Conti resurfaced in December 2021, this time with a stronger exploit of the Log4Shell vulnerability to achieve their objectives.

According to Trend Micro, supply chain attacks will continue to be a major trend in 2022, with attackers employing "quadruple extortion," in which they "hold the victim's critical data for ransom, threaten to leak the data and publicize the breach, threaten to go after the victim's customers, and attack the victim's supply chain or vendors" [18].

2.2 Case studies of known incidents in ICS

In this section, some of the risks associated with the cyber-security aspects of the current industrial manufacturing industry will be put into perspective. These risks are unique in the sense that although the OT platforms typically utilized in the industry are widely familiar, they pose certain cyber-security risks that are different from those encountered in an IT environment. Consequently, these risks have not been considered as such until now. First, a few case studies of historic cyber-physical attacks are briefly introduced to put into perspective the true nature of such attacks on industrial control systems networks. While a comprehensive study into the details of how these attacks work is beyond the scope of this article, some key aspects in terms of the associated security vulnerabilities can still be identified to formulate more clearly defined cyber-physical security problem statements. Putting these security aspects into perspective, they can be contextualized to identify and formulate solutions to the problems.

DOI: 10.31695/IJASRE.2022.8.5.1

2.2.1. Colonial Pipeline: The DarkSide Colonial Pipeline Strikes

On May 8, 2021, the Colonial Pipeline Company [11] announced that it had halted pipeline operations due to a ransomware attack, disrupting the crucial supply of gasoline and other refined products across the East Coast. This attack was similar to a ransomware attack on a pipeline in 2020, which resulted in the pipeline being shut down as well.

According to the study [11], attackers gained access to the Colonial Pipeline network by using an exposed password for a VPN account. Many businesses utilize a virtual private network (VPN) to enable secure, encrypted remote access to their corporate network. A Colonial Pipeline employee who was not publicly identified during the hearing presumably used the same password for the VPN in another location, according to the report.

2.2.2 Destructive Industrial Control System Malware Targeted at Saudi Arabia Energy Infrastructure in 2017

In December 2017, FireEye revealed [19] that it had recently dealt with an industrial operator whose facility had been targeted by a new type of ICS malware known as TRITON (also known as TRISIS or Hatman by other groups) [20]. The hack reprogrammed the facility's SIS controllers, causing them to reach a failed condition and forcing the industrial process to shut down automatically. The hacking effort was discovered during the inquiry that followed the shutdown.

The SIS that was attacked was a Triconex Safety Instrumented System from Schneider Electric, and the target location was later identified as a Saudi Arabian petrochemical manufacturing complex [20]. This form of SIS is frequently used and is commissioned in a consistent manner across numerous sectors [20].

TRITON is one of just a few malware strains capable of interrupting the physical processes of an industrial control system. The attack began with a network breach that was carried out using well-documented and easily detectable attack methods. To get access to the OT (Operational Technology) network, the attackers employed systems that were available in both environments [21].

After gaining access to the OT network, the threat actors were able to infect the SIS system's engineering workstation, which was typically placed in a separate network segment. The infection was most likely spread via social engineering, with the engineer obtaining or downloading a program with a genuine file name, such as "trilog.exe." The dropper file (TRIconex LOGging filename) [21] is a basic program that interacts with Triconex and its logging capabilities, as the name implies.

The main goal of the dropper file was to deliver the malicious script to the target, in this case the SIS controller. Shortly after the execution, the dropper attached to the targeted Triconex and injected the legitimate malware code into its memory [21].

The malware payload was stored in two binary files called inject.bin and imain.bin. Reading, injecting, and executing these files into the Tri-memory conex's were among the dropper's actions [21].

• inject.bin contained code that exploited a specific zero-day vulnerability to execute the contents of the file "imain.bin."

• imain.bin contained the final code that allows a remote user to entirely operate the SIS device.

The dropper, which was written in Python, was compiled using the trilog.exe application. It comprises a reverse-engineered version of the TriStation protocol, which is used to communicate with the targeted device [21].

2.2.3 Attack on the Ukraine distribution system operator in 2015

The electric power sector was forced to take a more aggressive approach to cybersecurity following the 2015 attack on the Ukrainian power grid, affecting 27 substations and approximately 225,000 end customers. The target was the Ukrainian electricity distribution company Kyivoblenergo. The attack can be classified as an advanced persistent threat (APT) and resulted in a disruption of service and blackout.

The attackers used targeted emails carrying weaponized visual basic for application (VBA) Microsoft Word and Excel attachments. Opening the files by employees installed a specific remote access tool (RAT) / malware, BlackEnergy3, on the workstations [22].

From there the attackers got access privileges for at least 6 months until they fully deployed specially crafted malware to the SCADA and field system enabling them to affect multiple substations. Finally, they were able to open a series of breakers of multiple substations, triggering the blackout. Seven 110 kV and twenty-three 35 kV substations were disconnected. This incident received global attention and helped spread public awareness of the vulnerabilities of electric power systems. A subsequent attack in

DOI: 10.31695/IJASRE.2022.8.5.1

December 2016 further exasperated industry concerns, with the country's power grid quickly becoming a testbed of sorts for cyberattacks [22].

2.2.4 Self-inflicted Information Overload of the Austrian Control center due to Cross-Border Miscommunication in 2013

A single counter-value inquiry from the Bavarian gas system caused an overload or temporary non-availability of the Austrian control center's critical operations in 2013, due to a misconfiguration in the Austrian electrical transmission grid operator's control system. The incident was caused by a misinterpretation of a data signal at the intersection of two domains in two different energy sectors, which resulted in the temporary non-availability of critical system functions [22].

More specifically, a status request command packet, which was broadcast from a German gas company as a test for their newly installed network branch, found its way into the systems of the Austrian energy power control and monitoring network. Due to misinterpretation, the data message from the gas system-generated thousands of reply messages in the power system, which generated even more data packages, which in turn flooded the control network. To stop this self-inflicted Distributed-Denial-of-Service (DDoS) 'attack', part of the monitoring and control network had to be isolated and disconnected. Fortunately, the situation was resolved without any power outages [22].

2.2.5 Shamoon (Saudi Aramco and RasGas)

On August 15, 2012, harmful spyware infiltrated Saudi Aramco's computer systems, making it the world's largest energy business. The attackers meticulously chose the one day of the year when they knew they could do the greatest damage: the day that more than 55,000 Saudi Aramco employees remained home from work to prepare for Lailat al Qadr, or the Night of Power, which commemorates the revelation of the Quran to Muhammad [23].

When the Shamoon malware was triggered, it overwrote data on over 30,000 computers with an image of a burning American flag. Shamoon was an information-stealing malware, which also included a destructive module. Shamoon renders infected systems unusable by overwriting the Master Boot Record (MBR), the partition tables, and most of the files with random data. Once overwritten, the information is not recoverable [25].

Symantec described the malware on their social media blog on August 16, 2012 [24]. On August 27, 2012, the Sha-moon malware hit its second target, the Qatari natural gas company RasGas, which is one of the world's largest liquefied natural gas (LNG) firms [25].

There was no evidence that Shamoon had any direct impact on ICS or SCADA systems at either Saudi Aramco or RasGas. Once a system is infected with the Shamoon malware, it attempts to spread itself to other devices on the local network. C2 communications are used to control the operation of the attack but are not necessary if the threat actor has programmed a time for disk destruction before delivering the malware [25].

Shamoon supports the ability to download and execute arbitrary executables from the C2 server, giving the attacker the ability to potentially spread the infection or download additional tools on the victim's device for network traversal [25].

2.3 Selection of Cyber Threats in the Industrial Control Systems

The danger landscape for utilities has grown to include a wider range of threats from a wider range of players. Infrastructure providers have been increasingly targeted by nation-state actors and other smart players as part of bigger campaigns. Furthermore, fraudsters profit from utilities and other vital infrastructure players. This section examines some recent criminal operations that have targeted ICS. Because the target of such attacks is no longer limited to IT networks [2-3], a paradigm shift in the content eminent risks that cyberattacks pose to ICS systems is required.

DOI: 10.31695/IJASRE.2022.8.5.1

Table 1 Threats in the energy system

SN	Title	Description	System Impacted
1	Infection through intrusion detection system (IDS)	To infect the general ICT protection systems of power system equipment enables the attacker to get access rights for all crucial elements and subsystems of the infected system, e. g. substation or generation unit. A threat agent exploits the security vulnerability in out-facing interfaces of a protection measure (e.g. firewall or IDS) to gain access to the internal network. Access then is extended laterally throughout the distribution or transmission grid operators' enterprise network. This scenario is an instance of a general type of scenario where the (often necessarily) higher access rights of protection software and devices make them an interesting entry vector to compromise the control system of the system operator	ICT System
2	Virus/Trojan infiltrates industrial control system	In this scenario, the attacker infiltrates the equipment using a virus, worm, or trojan. An existing virus, worm, or trojan that isn't built for industrial control systems (ICS) infects the system, disrupting or threatening to disrupt the process and seize control of the targeted equipment.	IT/OT System
3	Social engineering: phishing employees on enterprise-level propagates to field level manipulation or introducing a remote access tool kit to the human-machine interface	In this indirect attack, the attacker first infiltrates the general office ICT-System of the network operator or manufacturer and secondly gets access to the control systems of the attacked organization. This attack does not address individual power system equipment but allows access to all control systems of the organization. Remote Access Toolkits (RAT) are injected into workstations in the Enterprise Zone through spear-phishing employees through emails carrying weaponized attachments (e.g. scripts embedded in text processor macros). The attacker then laterally extends its foothold in the Enterprise Zone and collects intelligence on access codes and the structure of the company network. This information is then used to vertically extend access by deploying RAT in the Operations and Field Zone using legitimate credentials. The threat agent operates an external command and control service to execute control on the infected devices. The gained access is then used to change the behavior of field devices, e.g. to disrupt power or gas distribution or to damage equipment.	Office ICT System (affecting OT-System)
4	Malicious update to firmware in the field to influence single substation	This scenario focuses on the security of the manufacturers/supply chain and affects all equipment having regular firmware updates. A threat agent uses access to the update service for OEM firmware to inject malicious code to influence, by injection of communication to the field bus, the behavior of other devices at the substation of the power system. The attacker may aim at damaging individual devices by blocking (i.e. jamming) communication for protection functions or disrupting service by issuing single commands.	Substation OT-System
5	Cross-sector, cross-border message flooding	A misconfiguration in the control system of the electricity transmission grid operator can to the situation where a single counter value query from the gas system triggers a domino effect and an overload or temporary non-availability of the crucial services of the control center. The incident to misinterpretation of a data signal at the interface of two domains in different energy sectors can result in temporary non-availability of relevant system functions	Control Centre (TSO,DSO)
6	Compromise equipment through SCADA apps	This scenario focuses on the security of regular maintenance via so-called SCADA apps (business clients) and smart home applications (end consumers). Most generation units are affected in this scenario. A threat agent exploits the established relationship between a (legitimate) SCADA app on a dual-use (private and business) smartphone of a control room engineer to gain privileged access to a distribution SCADA system (e.g. of a generation unit or transformer station) and estab-	IT/OT System

DOI: 10.31695/IJASRE.2022.8.5.1

		lishes persistent remote access there	
7	Advanced persistent threat (APT) to DSO flexibility management system	A threat agent performs reconnaissance of utility communications and electrical infrastructure, and ancillary systems to identify critical feeders and electrical equipment. The threat agent gains access to selected elements of the utility distribution management system (DMS) - which includes all distribution automation systems and equipment in control rooms, substations, and on pole tops - via remote connections. After gaining the required access, the threat agent manufactures an artificial cascade through sequential tripping of select critical feeders and components, possibly causing automated tripping of distribution level generation sources due to power and voltage fluctuations. A blackout of varying degrees and potential equipment damage ensues. Remote connections to the DMS might be established using a variety of methods or a combination of methods.	DSO (IT/OT Conveegence threat)
8	Plant tripped off-line through a compromised vendor (software update by manufacturer) and remote connection to generation unit or equipment	This scenario focuses on the security of the communication channel of the manufacturer to upload software updates on power system equipment in the field (in general generation units) per remote access. A threat agent uses compromised authorization credentials to access a secured remote maintenance network interface. The interface provides access to a vendor-maintained asset controllable through a distributed control system (DCS). The network access must correlate with a separate call from the vendor to the utility to open a conduit to the interface. The threat agent then drops a modified system file that further attacks the local DCS network, either by flooding the network or by compromising further devices within the network. To affect a large area, multiple similar attacks have to be executed in parallel. The threat otherwise affects only a single DCS and all attached assets. A variant of the scenario establishes a foothold in a DCS and uses this access to further progress into different parts of the system. The elevated trust potentially assigned to a utility's "own" devices is exploited and used to access larger control structures, for example through an uplink to a control room. The threat might also be the first stage of a coordinated load-changing attack that potentially affects the whole system.	Generation
9	Compromised distribution grid management through supply chain vulnerabilities	Lifecycle attacks against equipment (in general generation units) during development, production, shipping, and maintenance can introduce deliberate errors that will fail under special conditions. For example, a threat agent might upload modified firmware in a relay during production that introduces a back door for changing relay settings and set points. This could render the relay inoperable or cause it to operate unexpectedly. The functional integrity of digital systems is based on functional assumptions of the whole hardware and software stack. This implies, that the whole supply and maintenance chain, starting from the design process, is protected against code injections. Any modification potentially has a catastrophic impact that not be detected for a long time. The recently publicized vulnerabilities "Meltdown" and "Spectre", which affected the whole design series of microcontrollers, provide an example of the possible scale of the number of involved devices in case of such issues. Large-scale industrial installations are considered vulnerable if they rely on a very limited number of manufacturers of parts and sub-parts of the system.	Supply Chain
10	Unauthorized Mass Remote Disconnect Through Firmware update	A threat agent prepares smart meter firmware containing malware and manually installs it on a target smart meter in each neighborhood. The single insertion point in each neighborhood becomes the botmaster for a smart meter-based botnet. The botmaster acquires the IP address for the neighborhood's headend at the utility and spoofs that address. As other smart meters attempt to connect to the headend, the botmaster sends a firmware update command to the smart meters and transmits the malicious firmware to each victim. Individual bots propagate the malicious firmware throughout the neighborhood and use them to achieve a mass remote dis-	Smart Meter

DOI: 10.31695/IJASRE.2022.8.5.1

		connect scheduled at the same time.	

Source:[22]

2.4 Related Works

In this section, we critically evaluate the major surveys on the topic of industrial control systems (ICSs) and their security, arguing that more research is needed.

This research, written by Pen et al. [26], focuses on a comprehensive security understanding of the SGs framework, assault scenarios, detection/protection mechanisms, estimation, and control tactics from both the communication and control perspectives. In addition, several potential obstacles and solutions for dealing with SG threat issues are presented. Finally, some findings are offered, as well as future study directions. The authors of [27] look at the design goals and functionalities of the smart grid communication system, as well as the communication requirements in depth. There are also discussions on some of the most current innovations in smart grid communication technologies. In this paper [28], Mrabet et al. summarize the cyber security requirements and the possible vulnerabilities in smart grid communications and survey the current solutions for cyber security for smart grid communications. However, both these works lack the survey based on primary data which is the main focus of this current research.

Authors in [29] review state the art in cybersecurity risk assessment of Supervisory Control and Data Acquisition (SCADA) systems. Knowles et al.[30] have surveyed the cyber-security of ICSs and the risk management aspects of it. The related standard in this domain are discussed and how the current systems lack built-in security considerations.

Kriaaa et al. [31] conducted a thorough investigation into the safety and security of industrial control systems. The distinction between these two ideas (ICS safety and security) has been established. Different methods to these difficulties proposed in the literature are also classified as generic or non-generic. A review by Sajid et al. [32] focuses on the security challenges of cloud-based ICS systems. Additional issues following cloud integration, as well as the general security flaws of SCADA systems, are mentioned. However, a more thorough security examination is required, particularly for the applicability of the machine learning methodologies that we will develop in later papers.

Authors in [33] have provided a survey on the developed distributed filtration and control of ICSs using mathematical methodologies The differential dynamic models are the main focus, with a short component dedicated to security controls. For the security of these systems, it is necessary to design mod-el-based techniques. Molina and Jacob [34] examined existing cyber-security techniques for industrial settings based on software-defined networking solutions. However, they are more concerned with the general concept of cyber-physical systems than with ICSs in particular.

The available approaches for intrusion detection systems (IDSs) deployed in ICSs were investigated by Zeng and Zhou [35]. There is also a taxonomy of the relevant vulnerabilities in these systems. They explore machine learning-based solutions as well as various forms of intrusion detection systems.

3. RESEARCH DESIGN AND METHODS

This chapter describes the research design process followed in this research publication.

3.1 Research Design

Yin (2017) defines five main research strategies: experiment, survey, archival analysis, history, and case study (Table 2). The choice of a research strategy depends on three conditions (Yin, 2017): the type of research question; the control of behavioral events; and a focus on contemporary events.

Table 2. Research strategies (Yin, 2017)

Research Strategy	Type of Research Question	Requirement of Behavior control	Focuses on contemporary events
Experimental	How, Why	Yes	Yes
Survey	Who, What,	No	Yes

DOI: 10.31695/IJASRE.2022.8.5.1

	Where, How many, How much		
Archival Analysis	Who, What, Where, How many, How much	No	Yes/No
History	How, Why	No	No
Case Study	How, Why	No	Yes

Source: [36]

In this research RQ1 focus on 'what'; while the sub-questions are ' How' and 'who'.The possible strategies for this research could be experiment, survey, archival, history, or case study. However, the experiment strategy cannot be applied since it requires control of behavioral events. Furthermore, the focus of the studied domain, i.e. cybersecurity in ICS, highlights current and existing technologies, thus favoring contemporary events. Hence, according to the criteria given by [37], the most appropriate strategy to answer RQ1 is a survey and a case study (see Table 2).

3.2 Study Area or Site

Zambia is the study area, considering the following towns as the study baseline: Chikankata, Chingola, Kitwe, Livingstone, Lusaka, Namalundu, and Siavonga.

3.3 Study Population

The term "population" refers to a complete group of people (subjects or occurrences) with similar features in which the researcher is interested, according to studies by [37]. The population in this example refers to the overall number of people who will be chosen to participate in the survey. ICS security personnel and employees from ZESCO, CEC, Kafue Gorge Lower, and Kafue Gorge Upper make up the majority of those in Kafue.

3.4 Study Sample and Sampling Techniques

There are numerous approaches, incorporating many different formulas, for calculating the sample size for categorical data. We will use Yamane's finite equation [38]

- n = N / (1 + Ne^2) (1)

Where:

n is the required sample size, N is the percentage occurrence of a state or condition, and E is the percentage maximum error required.

- Taking the population of specialized personnel to be 200 across all the targeted organizations and precision be 95%,
- Then, n = 200 / 1 + 200 (0.05^2)
- n = 170
- The Sample size for the questionnaires is anticipated to be a minimum of 170 people across various professional organizations and companies running ICS/SCADA systems to help elicit requirements for the model.

The sample study includes Chief Information Security officers, information security professionals, Cybersecurity professionals, Network Administrators, IT Auditors, Computer Engineers, End Users, and other related professionals who are directly involved in the administration and management of cybersecurity, Top management, Finance, Legal, and Training.

DOI: 10.31695/IJASRE.2022.8.5.1

3.5 Data Collection and Data Analysis

Data collection (Kothari 2011) [39] is the process of gathering information from a range of sources to answer a question. Primary and secondary data are the two types of data [39]. The phrase "primary data" refers to information gathered by the researcher for the study [39]. Secondary data is information obtained by someone other than the researcher before it is used by the researcher [39]. The majority of the data in this study comes from primary sources because it is based on a case study. Interviews and questionnaires were used to get this information. Secondary data was gathered through the use of literature, technical studies, and industry standards.

3.5.1 Literature Study

The review includes literature on different theories and practices used for cybersecurity in ICS operation and maintenance. The relevant literature from journals, conference proceedings, theses, technical reports, and standards provided information on ongoing cybersecurity activities in the railway, statistics of cyberattacks within the ICS, and estimates of applied cyber-security capability maturity models. The literature study was also used to select models to detect cyberattacks. In addition, it helped in the formulation of a holistic cybersecurity framework to enable proactive cybersecurity in ICS.

3.5.2 Interviews

The objective of the interviews held was to consider the opinions of the personnel and experts involved in railway cyber-security to complement the literature review and data analysis. The outcomes of the literature review and the data analysis were the basis for the interviews. The main issues discussed in the interviews were practical ones, i.e., cybersecurity in ICS operation and maintenance and interpretation of the results of the data analysis. The interviewees were involved in the on-going ICS projects and experienced practitioners in the field of cybersecurity. They also provided valuable and applicable documents.

3.5.3 Questionnaire

A questionnaire is a structured framework consisting of a set of questions and scales designed to generate primary data [40]. The thesis used Google Forms (an online survey tool) to develop and administer an online survey. A questionnaire using a series of questions based on a modified SANS 2021 Survey: OT/ICS Cybersecurity [41] was prepared and sent to the participating ICS organizations. Experienced practitioners in the field of cybersecurity answered the questionnaire.

In our research, we shall use a focus group in one of the surveys to determine the understanding of subjects when applying the vulnerability modeling method and get their reflection on our proposed method.

4.0 RESULTS AND DISCUSSIONS

The findings of the RQ research are presented in this chapter (s). I) identification of cybersecurity issues and challenges in ICS operation and maintenance; II) evaluation of cybersecurity maturity level in ICS; III) development of ICS Defender Kill Chain to defend against cyberattacks; IV) development of cybersecurity framework to predict, prevent, detect, and respond to cyberattacks are the main outcomes of the thesis.

4.1. Security Roles and Responsibilities

Individuals came from a variety of industries, including energy/utilities, business services, oil and gas (production or delivery), engineering services and control system equipment manufacturers, control system services, and hand chemical production, among many others. Forty-nine percent (49%) of the sample came from industries that are easily recognizable as using control systems as critical enablers of company operations.

4.1.1 Focus of Role

13.5 percent of respondents indicated their role as process control engineers, while 12.6 percent listed their role as security administrators or security analysts, which roughly matched the target audience demography. Process control engineers, control system operators, operations or plant directors, or production engineering managers are among the few (6%) who hold responsibilities specifically related to ICS activities. Despite this, 27% stated that ICS operations are their top priority. Another 31% divide their time evenly between IT/business operations and ICS operations, while the rest do not consider

DOI: 10.31695/IJASRE.2022.8.5.1

ICS security to be a top priority. More than a third (37%) of respondents with an ICS-related certification or certificate spend at least half of their time on ICS cyber security, with the majority (25%) focusing almost entirely on it. See appendix A.

4. 2. General SCADA or Distributed Control System (DCS) Information.

Figure 1 reveals that 95% of respondents agreed that some type of monitoring system had been implemented. Furthermore, the data indicate that ICS deployment is gaining traction, with a total of 80% (see figure 2) of respondents adopting some type of SCADA and remote monitoring in the last ten years.

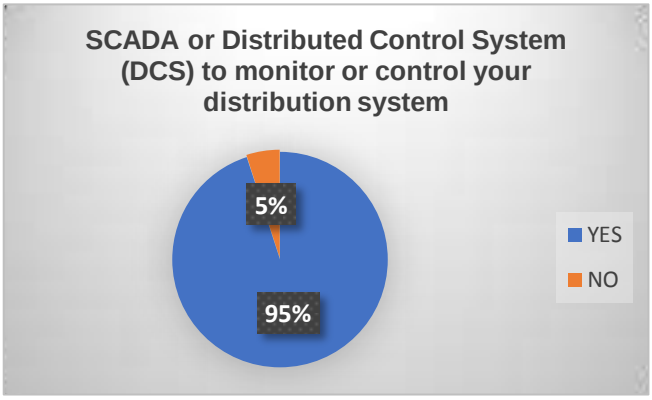


Figure 1. SCADA or DCS Implementation

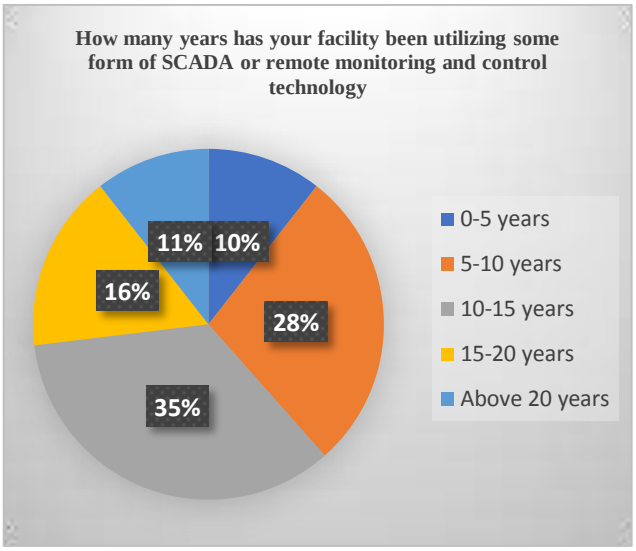


Figure 2. Years of utilizing some form of SCADA or remote monitoring and control technology

DOI: 10.31695/IJASRE.2022.8.5.1

Windows (98 percent) was the preferred platform for some SCADA software systems, including SCADATA (40 percent), Honeywell (38 percent), Siemens (36 percent), Rockwell (23 percent), NARI (24 percent), and ABB (26 percent). See figure 3.

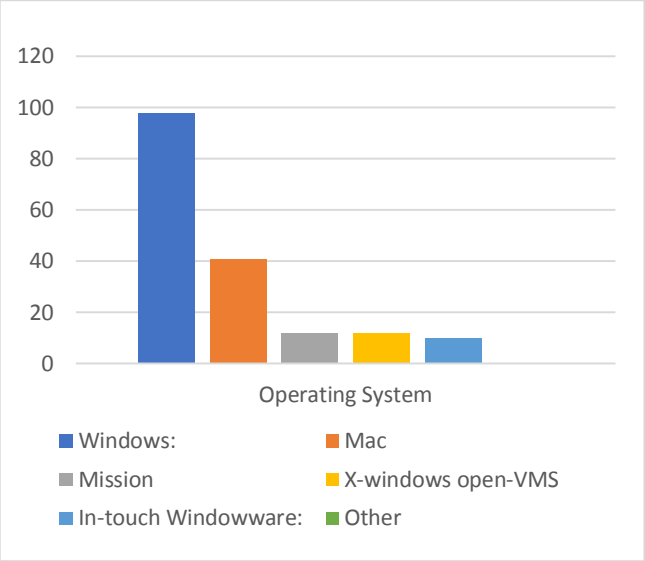


Figure 3. Prefered Operating System Platform.

4.3 Security Threats and Drivers

The major business concern of survey respondents about control system security was assuring the dependability and availability of control systems (92.70 percent).

Preventing information leakage came in second with 83.3 percent of the vote. At 79.80 percent, controlling information leakage was the third most critical priority.

Control system availability and reliability are frequently seen to be at odds with efforts to safeguard those systems, and this topic has recently attracted attention. With the growing use of IP-based technologies in control system contexts, well-known security concerns have arisen. Unfortunately, in the ICS environment, the methodologies and technologies that have been in use for a long time in IT can be extremely disruptive. New technologies and solutions are being developed in response to the requirement for nondisruptive approaches to safeguard control systems without having to wait for their rare shut-downs. A ranking of corporate concerns can be found in Figure 4.

DOI: 10.31695/IJASRE.2022.8.5.1

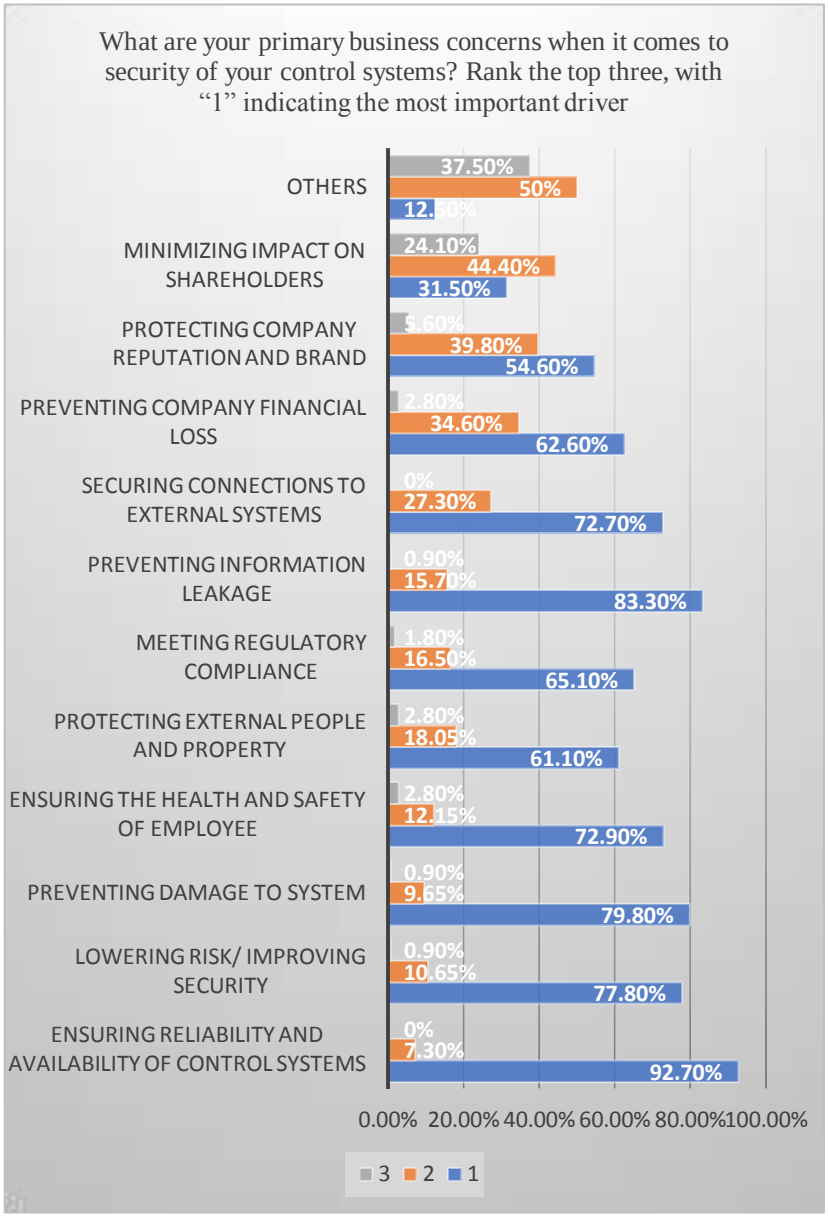


Figure 4. Ranking of Business Concerns

4.3.1 Risk Perception

Because penetration and assessment teams frequently use corporate IT to get access to control system networks, it's no surprise that the connectivity of office networks to internal systems is the top priority for 87 percent of respondents. 75 percent of respondents believe network hardware including firewalls, switches, and routers is the second most vulnerable to attack. Despite the proliferation of attack kits aimed at industrial control systems, penetration testers know that the quickest way into an ICS network is through connected business systems. Figure 5 illustrates this.

DOI: 10.31695/IJASRE.2022.8.5.1

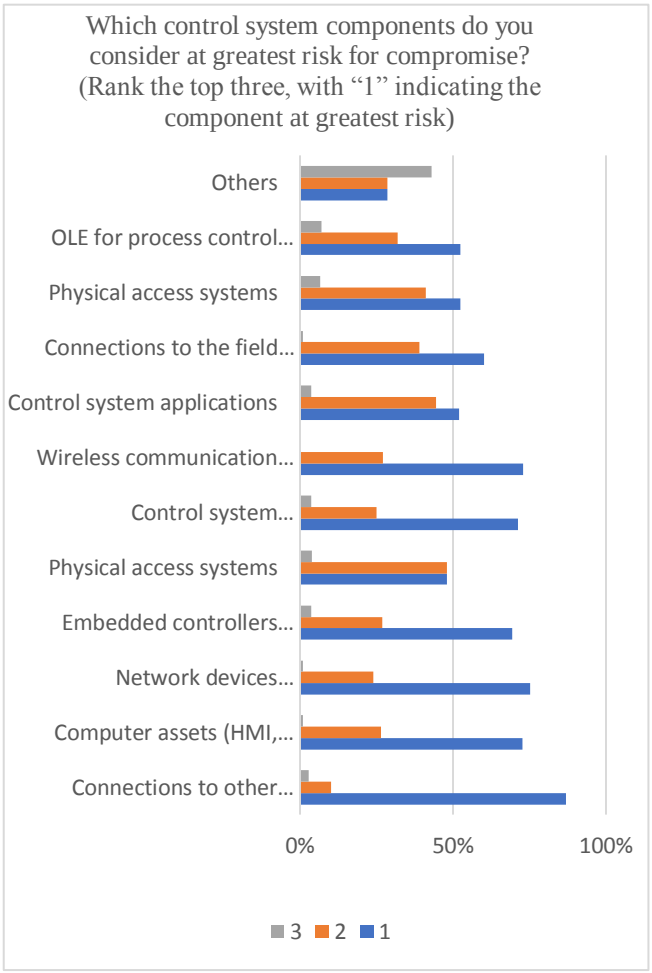


Figure 5. Components at Greatest Risk for Compromise

4.3.2 Incident Detection

Figure 6 shows that more breaches are occurring, with 45 percent of respondents admitting breaches in the last 12 months, 25 percent being suspicious but unable to prove it, 14 percent not knowing and having no idea, and 9 percent certain of not being infiltrated, and 7 percent unsure

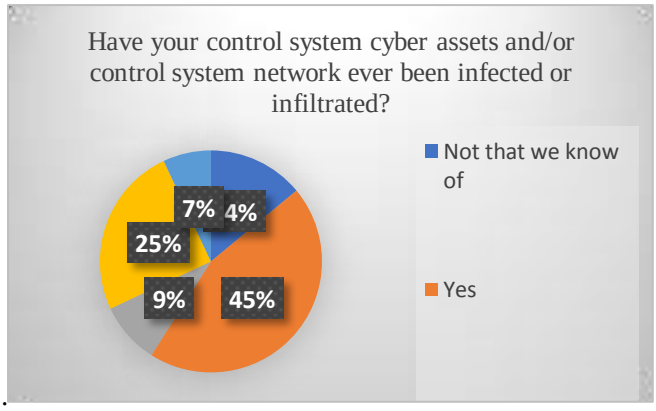


Figure 6. Have your control systems been breached?

DOI: 10.31695/IJASRE.2022.8.5.1

4.4. Security Control and Methodologies

The most widely utilized security components in practitioners' toolboxes were access controls and vulnerability scanning, which were used by 91.9 percent and 89.90 percent of respondents, respectively. The next most popular security control strategy was monitoring and log analysis (86.1 percent). According to the respondents, communication whitelisting (84 percent), anomaly detection (81.5 percent), asset identification (79.60 percent), and control system upgrades (78 percent) are among the top additional security techniques. Such findings could imply that several asset owners and operators are applying standard IT security methods to ICS/OT networks, which is a less effective method of securing control systems. Figure 7 illustrates this.

4.4.1 Systems Procurement

While it is unavoidable to secure existing assets and systems, a full life-cycle approach also includes security in the purchase. We find the results (44.4%) positive because it shows that more respondents are considering cybersecurity as part of their automation system procurement process. The group that says it doesn't consider cybersecurity in the automation systems procurement process (5.4 percent) is a bad sign. Those who were "slightly" hopeful were at 10.80 percent, while those who were "somewhat" hopeful were at 26.1 percent. Figure 8 illustrates this.

DOI: 10.31695/IJASRE.2022.8.5.1

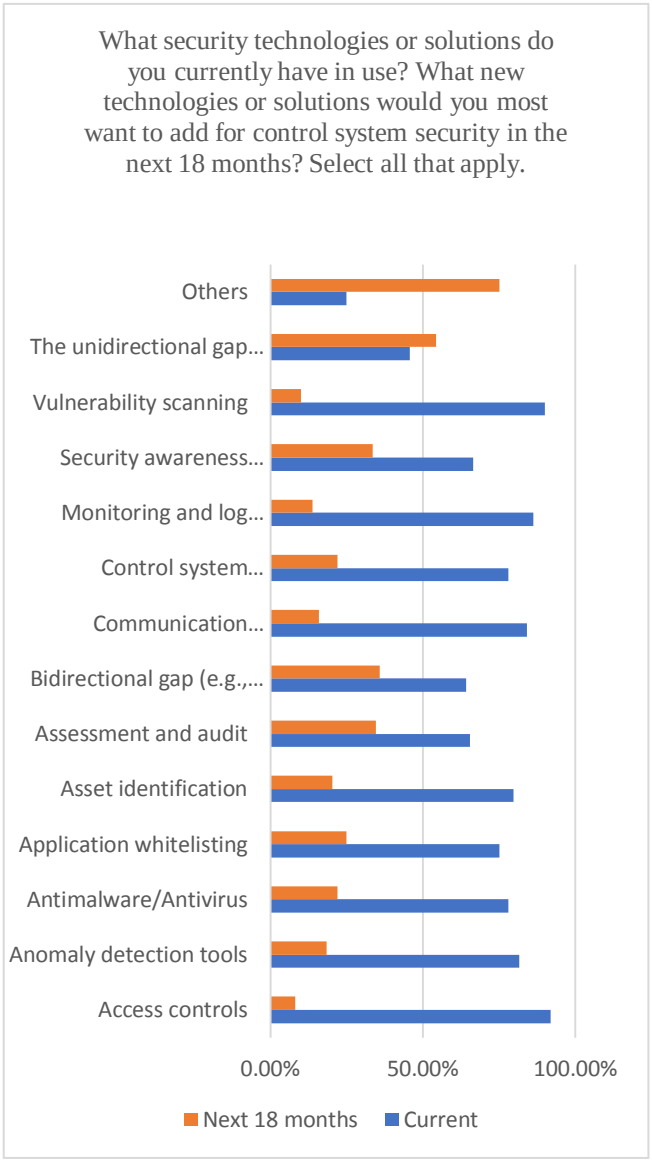


Figure 7. Technologies in Use to Protect Control Systems

DOI: 10.31695/IJASRE.2022.8.5.1

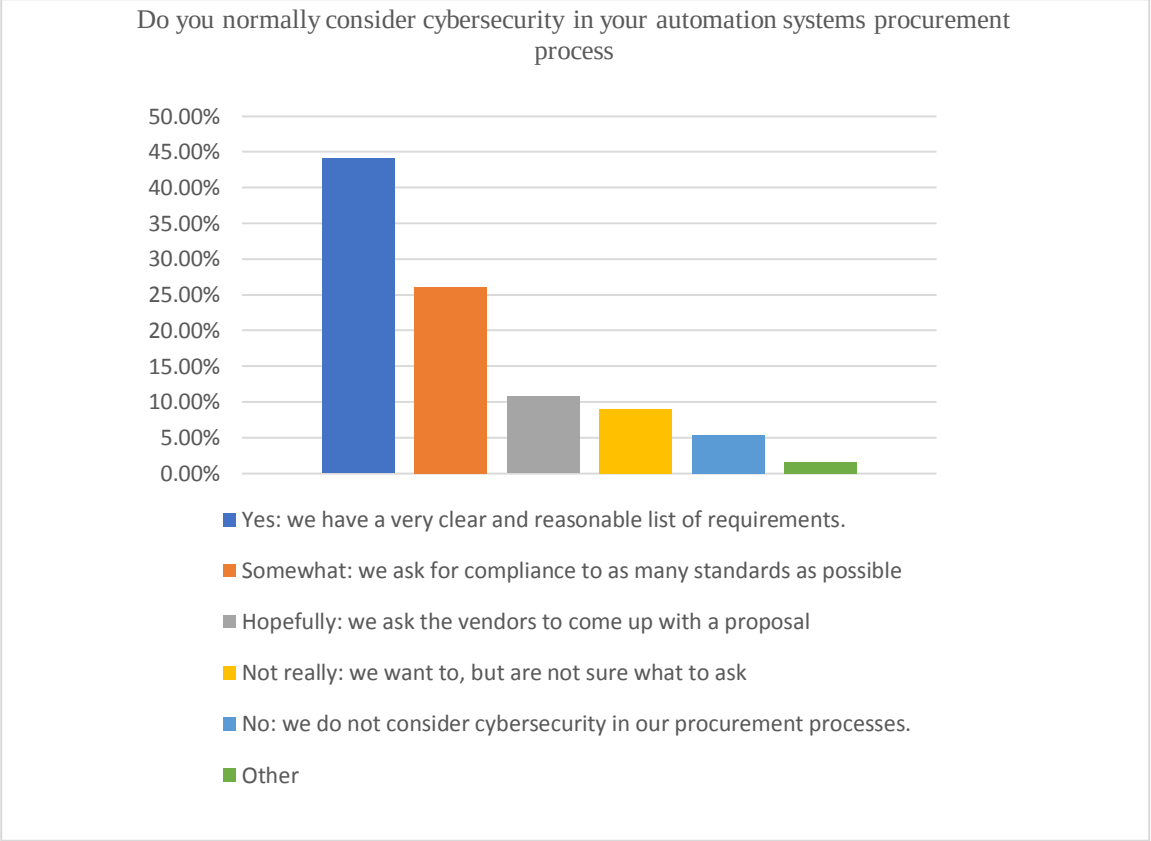


Figure 8. Consideration of Cybersecurity in the Procurement Process

4.5 IT-ICS Convergence

The continuous integration of commercial operating systems (Windows, Linux, UNIX) and open communication protocols into control system networks prompted us to investigate how participants are dealing with this convergence of technology. We asked if participants have a plan as general-purpose devices and IP-based technologies continue to develop within control and automation system contexts, given the enormity of the changes that are driving the trend [42]. The majority of respondents (80%) agree that having a security strategy in place to meet the convergence of information and operational technologies is critical. Unfortunately, as demonstrated in Figure 9, only 40% of people have a strategy.

DOI: 10.31695/IJASRE.2022.8.5.1

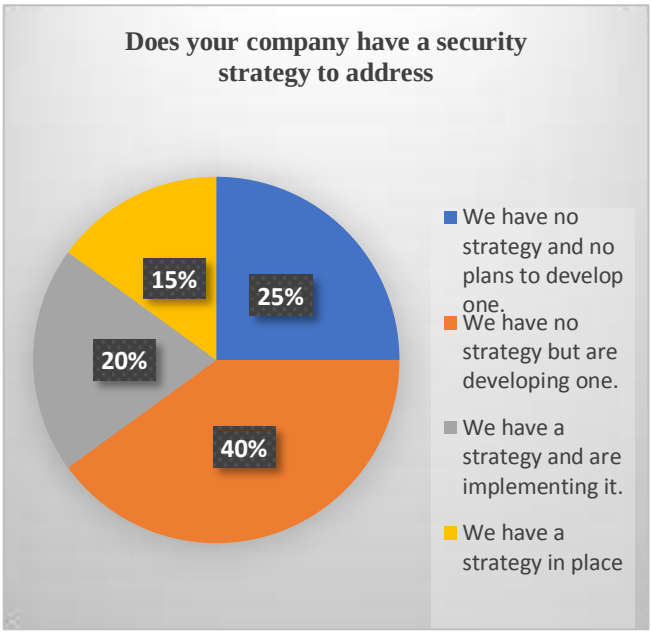


Figure 9. Strategies for IT-ICS Convergence

4.6 Security Budgets

Another encouraging trend is that, as shown in Figure 10, IT and operations jointly handle the control systems security budget in 45 percent of respondent organizations. This should encourage people to recognize their common goals and work together even more.

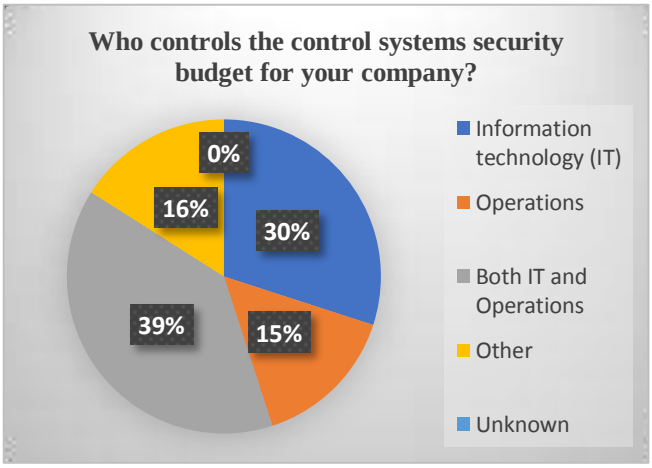


Figure 10. Control of the Control Systems Security Budget

The fact that 84 percent of respondents said they had some knowledge of the budget is promising. This is encouraging because it shows that folks in the trenches are at least somewhat involved in the budgeting process, which most certainly includes participation in priority determination. Unfortunately, this means that another 16% of respondents are unaware of the budgets. Figure 11 depicts the respondents' current understanding of control system security budgets.

DOI: 10.31695/IJASRE.2022.8.5.1

Figure 11. Control Systems Security Budgets

5.0 CONCLUSIONS

This chapter draws important conclusions from the results of the research study.

To effectively defend OT environments, a complex and integrated approach is needed that takes into account internal and external risks, analyzes vulnerability to those risks, and prioritizes risk mitigation measures using people, processes, and technology. This strategy necessitates a thorough grasp of the current state of affairs across similar entities as well as critical internal collaborations, particularly with IT security teams and peers from other firms.

The gaps and challenges that the ICS community needs to address include:

• Better understanding of the threat landscape, with enhanced sharing of incidents to improve collective defense

• Understanding the process-related impacts of incidents

• Correlating process control telemetry with cybersecurity telemetry for root cause analysis

• Meeting current ICS security hygiene fundamentals improved asset identification and connectivity management

• Improving OT/ICS endpoint visibility as key technologies continue to mature

The ICS community faces an inflection point. We continue to see investments and outcomes from OT security efforts increase, but risk drivers do not remain static. OT security dominates the national cyber conversation in ways not previously imagined. Although the ICS/OT security community has made great strides, we still have hard work ahead.

ACKNOWLEDGEMENT

The authors would like to acknowledge the contribution and hard work of the many security and facility professionals who participated in this research. Without their contributed time out of their busy schedules, the research could not have been achieved.

REFERENCES

[1] Candell R, Zimmerman T, Stouffer K. NISTIR 8089: An Industrial Control System Cybersecurity Performance Testbed. 2015http://nvlpubs.nist.gov/nistpubs/ir/ 2015/NIST.IR.8089.pdf.

DOI: 10.31695/IJASRE.2022.8.5.1

[2] Phiri, Lukumba & Tembo, Simon. (2022a). Petri Net-Based (PN) Cyber Risk Assessment and Modeling for Zambian Smart Grid (SG) ICS and SCADA Systems. 10.5923/j.computer.20221201.01.

[3] Phiri, Lukumba & Tembo, Simon. (2022b). Cyberphysical Security Analysis of Digital Control Systems in Hydro Electric Power Grids. Computer Science and Engineering. 12. 15-29. 10.5923/j.computer.20221201.02.

[4] Trend Micro April, et al. "An in-Depth Look at ICS Vulnerabilities Part 3." Trend Micro, 6 Apr. 2022, https://www.trendmicro.com/en_us/research/22/d/an-in-depth-look-at-ics-vulnerabilities-part-3.html.

[5] "Threat Landscape for Industrial Automation Systems. Vulnerabilities Identified in 2019: Kaspersky ICS CERT." Kaspersky ICS CERT | Kaspersky Industrial Control Systems Cyber Emergency Response Team, 14 Dec. 2021, https://ics-cert.kaspersky.com/publications/reports/2020/04/24/threat-landscape-for-industrial-automation-systems-vulnerabilities-identified-in-2019/.

[6] The Cyber Security and Cyber Crimes Act, 2021.

[7] "National Cyber Security Policy Approved." MISA Zambia, 27 Jan. 2021, https://zambia.misa.org/2021/01/27/national-cyber-security-policy-approved/. FLEXChip Signal Processor (MC68175/D), Motorola, 1996.

[8] Mwila, Kingston & Lubobya, Charles. (2019). An Assessment of Cyber Attacks Preparedness Strategy for Public and Private Sectors in Zambia. 8. 10.15680/IJIRSET.2019.0812041.

[9] Chinyemba, Melissa K. & Phiri, Jackson. (2018). An Investigation into Information Security Threats from Insiders and how to Mitigate them: A Case Study of Zambian Public Sector. Journal of Computer Science. 14. 1389-1400. 10.3844/jcssp.2018.1389.1400.

[10] Shadi Moradi Seresht. 2009. A Methodology for Software Requirements Elicitation and Analysis: Semi-Automatic Assistance in Elicitation and Analysis of Textual User Requirements. VDM Verlag, Saarbrücken, DEU.

[11] https://www.txone-networks.com/blog/content/txone-networks-2021-cybersecurity-report

[12] CISO MAG, "Are We Really Out of the Maze? The Ransomware Gang Announces Retirement", Nov. 3, 2020

[13] Colonial Pipeline: The Darkside Strikes - Congress. https://crsreports.congress.gov/product/pdf/IN/IN11667.

[14] Associated Press, "Colonial Pipeline confirms it paid $4.4m ransom to hacker gang after the attack", The Guardian, May 20, 2021

[15] Shaun Nichols, "Kaseya ransomware attacks: What we know so far", TechTarget, July 6, 2021

[16] Lance Whitney, "Kaseya supply chain attack impacts more than 1,000 companies", TechRepublic, July 6, 2021

[17] Pedro Tavares, "A full analysis of the BlackMatter ransomware", Infosec, Nov. 10, 2021

[18] Trend Micro Research, "Toward a New Momentum: Trend Micro Security Predictions for 2022", Trend Micro, Dec. 7, 2021

[19] FireEye, "Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure"," 14 December 2017. [Online]. Available: https://www.fireeye.com/blog/threat-research/2018/06/totally-tubular-treatise-on-triton-and-tristation.html.

[20] T. W. S. Journal, "New Type of Cyberattack Targets Factory Safety Systems," 19 January 2018. [Online]. Available: https://www.wsj.com/articles/hack-at-saudi-petrochemical-plant-compromised-a-safety-shut-off-system-1516301692.

[21] Alessandro Di Pinto, Younes Dragoni, Andrea Carcano, TRITON: The First ICS Cyber Attack on Safety Instrument Systems Understanding the Malware, It's Communications, and Its OT Payload

[22] OFFIS e.V. "Home." OFFIS E.V., https://www.offis.de/en/offis/publication/study-on-the-evaluation-of-risks-of-cyber-incidents-and-on-costs-of-preventing-cyber-incidents-in-the-energy-sector.html.

[23] N. Perlroth, In cyberattack on Saudi rm, U.S. sees Iran firing back,The New York Times, (www:nytimes:com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us:html),October 23, 2012.

DOI: 10.31695/IJASRE.2022.8.5.1

[24] Symantec, The Shamoon attacks, Symantec, (www:symantec:com/connect/blogs/shamoon-attacks), August 16, 2011.

[25] Kevin Hemsley, & Ronald E. Fisher, History of Cyber Incidents and Threats to Industrial Control Systems

[26] C. Peng, H. Sun, M. Yang and Y. -L. Wang, "A Survey on Security Communication and Control for Smart Grids Under Malicious Cyber Attacks," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, no. 8, pp. 1554-1569, Aug. 2019, doi: 10.1109/TSMC.2018.2884952.

[27] Yan, Ye & Qian, Yi & Sharif, Hamid & Tipper, David. (2012). A Survey on Cyber Security for Smart Grid Communications. Communications Surveys & Tutorials, IEEE. 14. 998-1010. 10.1109/SURV.2012.010912.00035.

[28] Zakaria El Mrabet, Naima Kaabouch, Hassan El Ghazi, Hamid El Ghazi, Cyber-security in smart grid: Survey and challenges, Computers & Electrical Engineering, Volume 67,2018, Pages 469-482, ISSN 0045-7906, https://doi.org/10.1016/j.compeleceng.2018.01.015.

[29] Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., Stoddart, K., 2016. A review of cyber security risk assessment methods for SCADA systems. Comput. Secur. 56, 1–27.

[30] Knowles, W., Prince, D., Hutchison, D., Pagna Disso, J.F., Jones, K., 2015. A survey of cyber security management in industrial control systems. Int. J. Crit. Infrastruct. Protect. 9, 52–80.

[31] Kriaaa, S. , Pietre-Cambacedes, L. , Bouissou, M. , Halgand, Y. , 2015. A survey of approaches combining safety and security for industrial control systems. Reliab.Eng. Syst. Saf. 139, 156–178

[32] Sajid, A. , Abbas, H. , Saleem, K. , 2016. Cloud-assisted IOT-based SCADA systems security: a review of the state of the art and future challenges. IEEE Access 4,1375–1384

[33] D. Ding, Q. L. Han, Z. Wang, and X. Ge, "A Survey on Model-based Distributed Control and Filtering for Industrial Cyber-Physical Systems," IEEE Transactions on Industrial Informatics, vol. 15, no. 5, pp. 2483-2499, May 2019.

[34] E. Molina, E. Jacob, "Software-Defined Networking in Cyber-Physical Systems: A Survey," Computers & Electrical Engineering, vol. 66, pp. 407-419, February 2018.

[35] P. Zeng and P Zhou, "Intrusion Detection in SCADA System: A Survey," Springer Singapore, pp. 342-351, 2018.

[36] Yin, R. K. (2017). Case study research and applications: Design and methods. Sage publications.

[37] Fraenkel, J.R. & Wallen, N.E. (2002). How to design and evaluate research in education (5th Ed.). Boston: McGraw Hill.

[38] Hamed Taherdoost. Sampling Methods in Research Methodology; How to Choose a Sampling Technique for Research. International Journal of Academic Research in Management (IJARM), 2016, 5. hal-02546796

[39] Kothari, C. R. (2011). Research methodology and techniques Delhi: New Age International Limited Publishers.

[40] Hair, J. F., Money, A. H., Samouel, P., & Page, M. (2007). Research methods for business.Education+ Training.

[41] Survey options based on CISA's critical infrastructure sector definitions, with some modifiers for ICS-specific elements, www.cisa.gov/critical-infrastructure-sectors

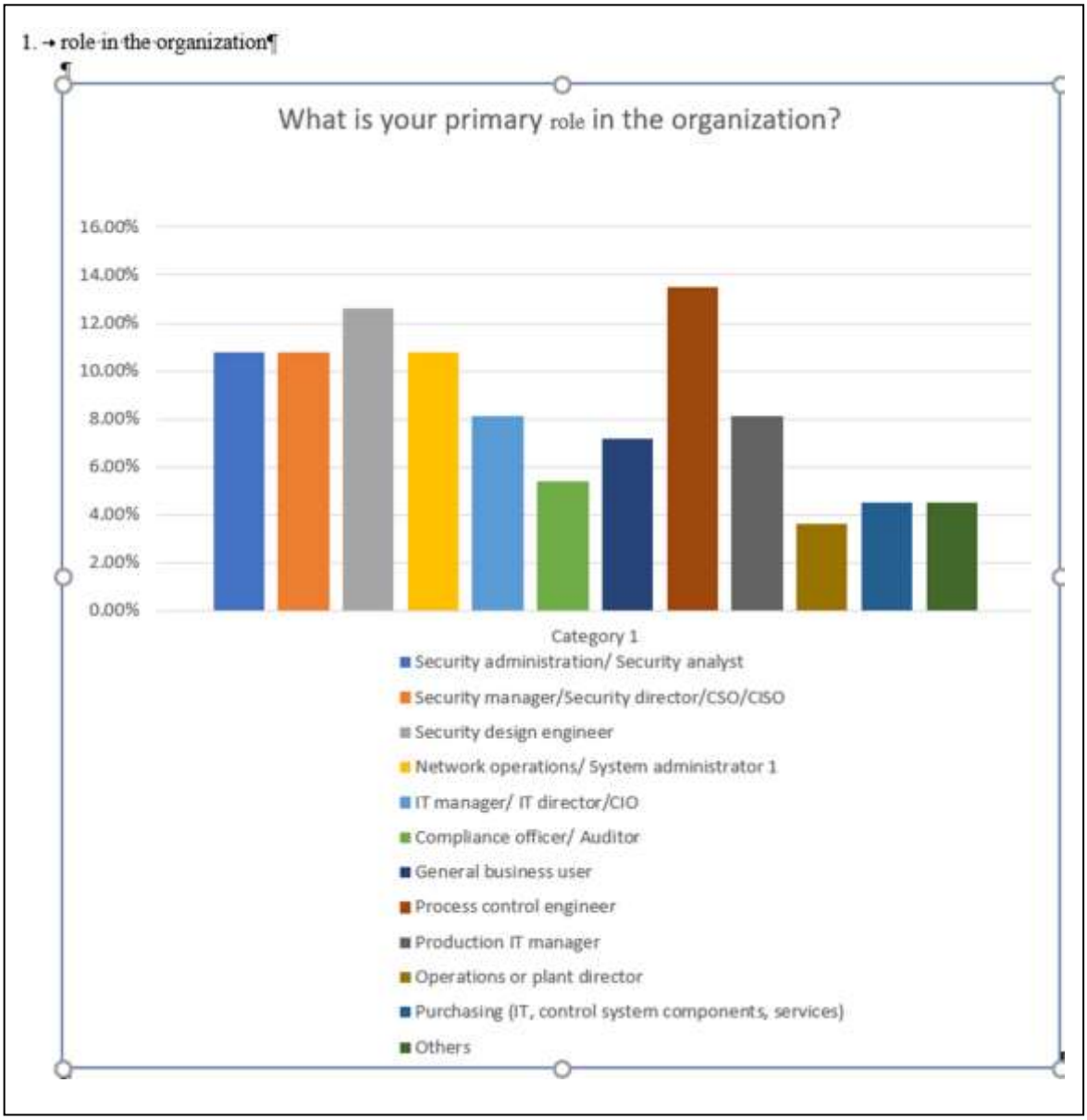
[42] www.intelligentutility.com/article/13/09/fusion-it-and-ot-utilities-.

DOI: 10.31695/IJASRE.2022.8.5.1

APPENDICES

A. Questionnaire Responses for Q1.

1. → role in the organization¶



DOI: 10.31695/IJASRE.2022.8.5.1