5-2019

A Taxonomy-based Analysis of Attacks on Industrial Control Systems

Kahawalage Kanchana Tikirikumari Lankatilake
St. Cloud State University, chana522k@gmail.com

A Taxonomy-based Analysis of Attacks on Industrial Control Systems

by

Kahawalage Kanchana Tikirikumari Lankatilake

A Starred Paper

Submitted to the Graduate Faculty of

St. Cloud State University

in Partial Fulfillment of the Requirements

for the Degree of

Master of Science

in Information Assurance

May, 2020

Starred Paper Committee:
Changsoon Sohn, Chairperson
Erich Rice
Balasubramanian Kasi

Abstract

Most critical infrastructure depends on industrial control and automation systems to manage their processes. However, industrial control and automation systems were found to have many vulnerabilities owing to their design. They were initially designed to operate as air-gapped systems. However, with the evolution and the expansion of the industry, they are increasingly being targeted by attackers. Thus, preventative methods must be implemented to minimize/ prevent ICSs from being compromised by patching the vulnerabilities and addressing possible attack vectors. In order to prepare to defend against forthcoming attacks on critical infrastructure, it is vital to understand how past attacks have been carried out. This study analyzed and cataloged cases of attacks against ICSs to form a taxonomy that can be used as a tool to analyze the nature of ICS attacks. The taxonomy developed by this study can aide interested parties to determine potential attack vectors an attacker may choose, based on the attributes discussed in the study. Moreover, this paper also serves as a resource for the interested parties to understand ICSs.

Table of Contents

Page

List of Figures

Figure Page

List of Tables

Chapter I: Introduction

1.1 Introduction

Security of Critical Infrastructure is vital to the wellbeing of a nation. Legacy ICSs (Industrial Control Systems) such as SCADA (Supervisory Control and Data Acquisition) are widely used in Critical Infrastructure due to their robustness and proven performance. However, the legacy network security solutions such as airgaps and obscurity appear to be ineffective at shielding these systems from cyber-physical attacks.

The introduction of network protocols such as TCP/IP, GSM and the use of conventional operating systems and software within SCADA and other ICSs has resulted in these systems being less secluded from the cyberspace (Kube, 2013). Thus, their vulnerabilities can be exploited by hackers, terrorists and others will malicious intentions. For example, during 2016 the Sandworm hackers successfully executed a cyber-physical attack on the power grid of Ukraine causing a blackout that affected many people (Gavin, 2018).

To minimize ICSs from being compromised an understanding of past attacks are necessary. Thus, this study discussed past cases of attacks on ICSs and clarified them by their attributes such as Target Industry, Vulnerabilities, Vector, payloads, attacker and Motivation. These attributes were organized into a taxonomy which will facilitate the analysis of these attacks on ICSs with their target industries, target vulnerabilities and attacker profiles. Moreover, this taxonomy will clearly explain the nature of these attacks and how they may be carried out in the future.

1.11 Industrial control Systems

ICS (Industrial control system) refers to the wide array of control systems and equipment used to electronically manage an industrial process, *Figure 1*. The most common types of ICS are SCADA (Supervisory Control and Data Acquisition) and DCS (Distributed Control System). Also, some of the components that ICSs use are PLCs (Programmable Logic Controllers), RTUs (Remote Terminal Units) and HMIs (Human Machine Interfaces).

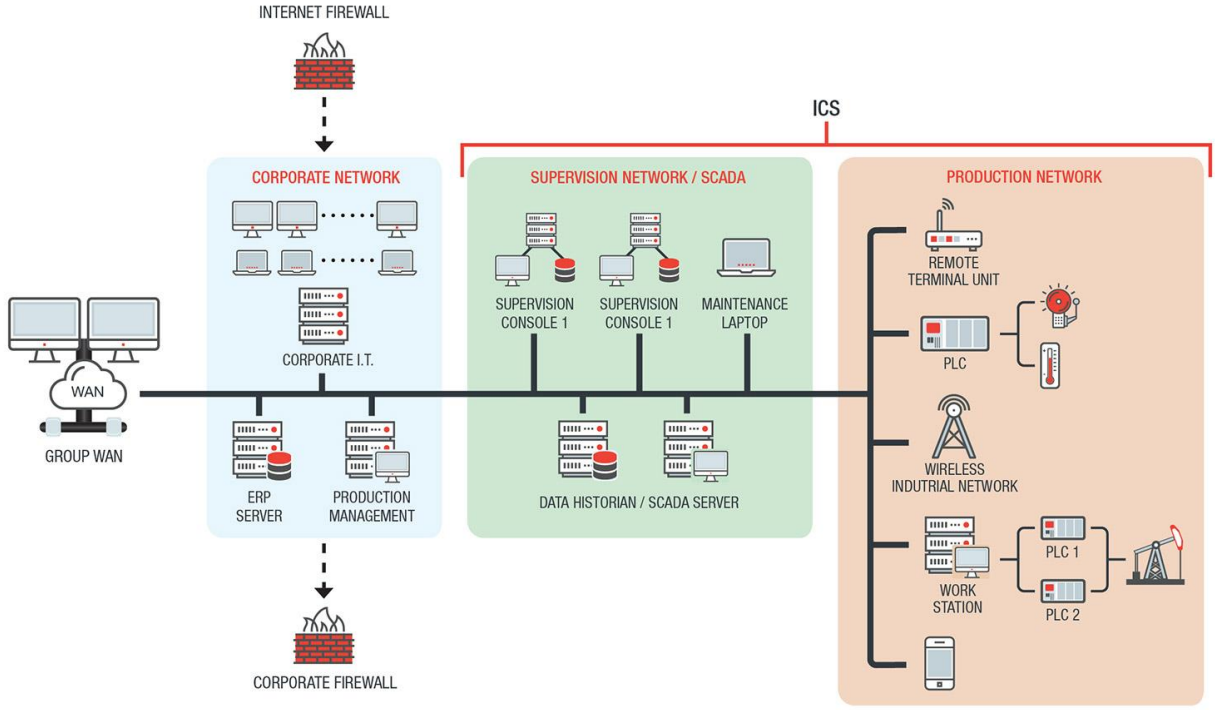

Figure 1. The layout of an ICS. From Industrial Control System, Courtesy of TREND MICRO (TREND MICRO, n.d.)

SCADA and DCS are a combination of software and hardware elements that provide supervisory control and data acquisition over long distances. The software works in tandem with equipment such as HMIs, PLCs and RTUs to provide operators with a centralized control system. The centralized control system controls the field devices such as valves, motors, and pumps via PLCs and RTUs. The HMIs present the operator with a display to monitor the process. It also enables the operator to configure setpoints, adjust control parameters and address alarms.

Prior to the advent of ICS such as SCADA and DCS, most industrial plants consisted of manual controls and analog systems. Consequently, they required multiple operators to be on site, where they would monitor gauges and operate manual controls. The technological advances during and after the mid-1900s enabled the automation of these plants thus, transferring the manual controls to ICS.

1.2 Problem Statement

ICSs such as SCADA was introduced in the 1960s and relied on air gaps and obscurity to be insulated from attacks. With the growth of the cyberspace, ICSs that critical infrastructure rely upon, are increasingly becoming internet facing systems due to the integration of operational technology (OT) and IT. Hence, they are vulnerable to attacks. Thus, preventative methods must be implemented to minimize ICSs from being compromised by patching the vulnerabilities and addressing the possible attack vectors. In order to prepare to defend against forthcoming attacks against critical infrastructure, it was vital to understand how these attacks had been carried out. However, tools available for Interested parties that enable them to easily understand the nature of potential attacks are limited.

1.3 Nature and Significance of the Problem

The Natanz nuclear facility in Iran, operates many centrifuges to extract enriched Uranium to the displeasure of many nations such as Israel and the United States of America. The facility was facing multiple technical issues during the years of 2009 and 2010. Their centrifuges were having catastrophic failures and the safety systems designed to protect the centrifuges were malfunctioning. The engineers working at the site were unable to locate the root cause until later it was revealed to be the work of a malware called Stuxnet (also known as Olympic Games), designed specifically to target the PLCs (programable logic controllers) employed at Iranian nuclear enrichment facilities.

The attack carried out at Natanz, rumored to be orchestrated by state actors, revealed the vulnerabilities of SCADA (Supervisory Control and Data Acquisition) and other ICSs (Industrial Control Systems). The use of ICSs such as SCADA is prolific in critical infrastructure such as power plants, water treatment facilities, petroleum refining and chemical processing. Thus, widespread grief including loss of life can be brought onto to large populations if a successful attack was to target critical infrastructure, since they have a direct physical impact such as power outages, pipe explosions, malfunctions in the water and sewage management. It is therefore vital to understand the nature of past attacks and how they have been carried out against critical infrastructure, in order to prepare to defend against future attacks.

A Threat landscape developed by Monyai (2018), *Figure 2*, illustrates the global impact of attacks against ICSs.

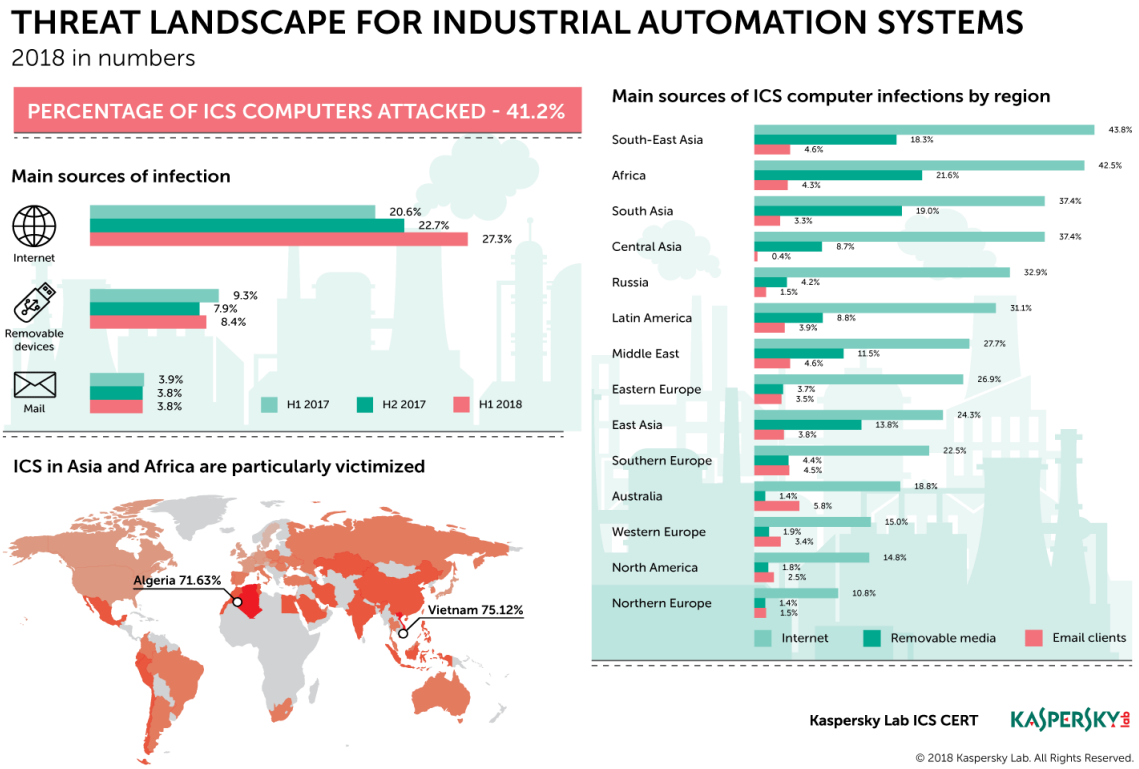

Figure 2. "Threat landscape for Industrial Automation Systems", (Monyai, 2018)

Attacks on ICSs have been reported since the turn of the millenia, *Figure 3*. The rapid growth of the cyber-space can only mean, an increase in such attacks.

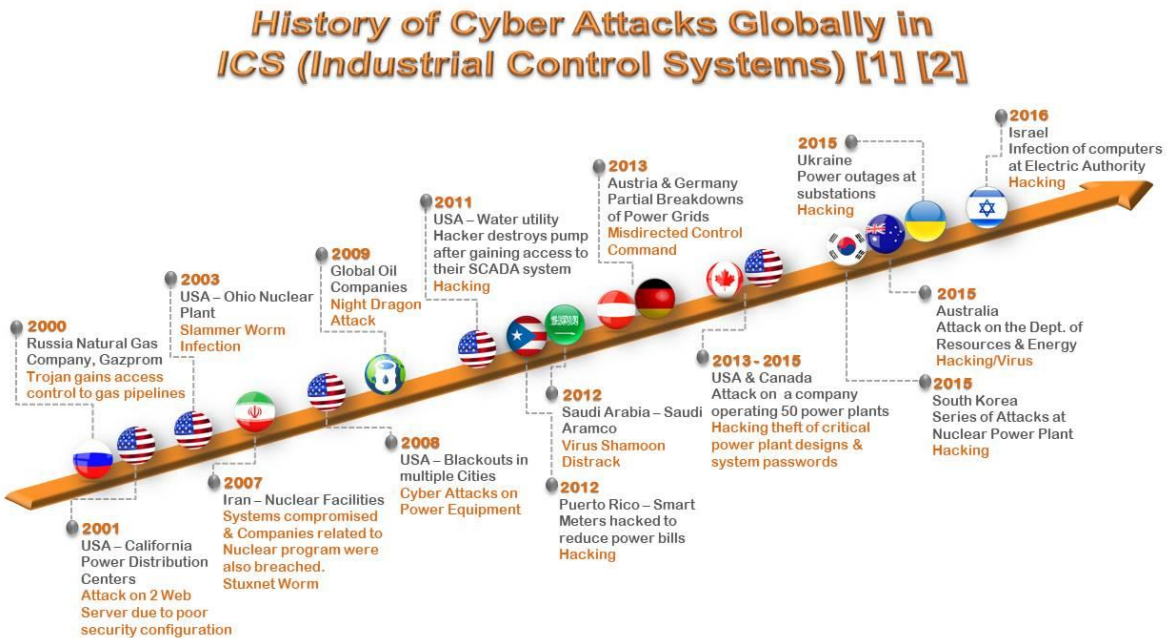

Figure 3. Trend of cyber-attacks on ICS (Cyber Immunity, a holistic view for Industrial Control Systems, 2017)

1.4 Objective of the Study

To understand the nature of the attacks on ICSs, to identify the key attributes of the attacks, to recognize the key vulnerabilities common to most ICSs and to develop a taxonomy that presents the effects of an attack. Moreover, the goal of this study is to present a tool that allows to recognize the nature of the past attacks on industrial control systems and how they may be carried out in the future.

1.5 Study Questions/Hypotheses

1. How to analyze the nature of the attacks on Industrial Control systems?

2. What are the key attributes of the attacks on Industrial Control systems?

3. What vulnerabilities are common to most ICSs?

4. How to forecast the possible attacks on ICS?

1.6 Limitations of the Study

This study will not introduce new solutions to the vulnerabilities that exist in ICSs. It will be limited to providing the reader with solutions that are already published and practiced.

1.7 Definition of Terms

PLC: Programable logic controller, is an industrial computer that is used to control field devices such as valves, motors and pumps. It consists of many I/O (inputs and outputs) that helps it to transmit and receive simple ON/OFF signals as well as analog

control signals such as 4-20 mA and 0-10 VDC signals. It is built to be rugged in order to withstand electrical noise, vibration and large temperature ranges. Moreover, it is capable of networking either through serial communication protocols such as RS-232 or through ethernet. Thus, it can communicate with SCADA software via a LAN (local area network).

RTU: A Remote Terminal Unit is very similar to a PLC in function. However, unlike a PLC, an RTU is designed and built to be extremely rugged and operate in remote areas and in withstand harsh environments (offshore oil rigs, mountain tops, mining etc.).

HMI: A Human Machine Interface is a programable display device that are normally touchscreen. It provides the operator with a graphical user interface (GUI), that facilitates the communication between the operator and control devices in the ICS environment.

IIOT: IIOT, stands for industrial internet of things. This can be understood as the result of the natural evolution of operational technology such as PLCs, RTUs and SCADA systems. The fourth industrial revolution, which we are in the midst of have contributed significantly to the IIOT development. Self-driving vehicles, highly automated production facilities and even more efficient renewable energy systems such as smart grids owe their success to IIOT.

Airgaps: Airgap is a method of assuring the network security by physically isolating it from external connections such as the internet to prevent unauthorized access.

1.8 Summary

The critical infrastructure that supports the modern lifestyle of many is under threat from cyberattacks, especially with the escalation of cyberwarfare. The expansion of the

cyberspace and the integration of conventional IT technologies into ICSs are assumed to be the main reason behind this.

This study analyzed and cataloged cases of attacks against ICSs to form a taxonomy that can be used as a tool to analyze the nature of historical ICS attacks. The taxonomy can aide interested parties to determine potential attack vectors an attacker may use, based on the attributes discussed in the study. Moreover, this paper also serves as a resource for the interested parties to understand ICSs.

Chapter II: Background and Review of Literature

2.1 Introduction

In this chapter various sources of information were used to expand the understanding of the vulnerabilities in ICSs and potential solutions available. The sources ranged from articles published in reputed media, vendor websites, research papers and journals. Different sources presented different aspects of ICSs and their vulnerabilities, but they were all in tune when discussing the potential impacts of a successful attack.

In addition to sources pertaining to ICSs and their vulnerabilities, the review of literature also includes sources used to model the data collection and the analysis. This data was sourced from a wide array of disciplines, as the primary focus was identifying various methodologies that can be used to conduct this study. Due to the affinity of this study towards a qualitative approach, sources elaborating qualitative studies were considered.

2.2 Background Related to the Problem

There were many studies that outline the potential vulnerabilities of ICSs. However, the studies that map vulnerabilities of ICSs to other attributes were scarce. Thus, this study aims to provide IT professionals with a classification of security incidents that expresses the relationship between attacks and their attributes.

The study of attacks on ICSs appeared to gain a significant momentum after the Stuxnet virus and the damage it caused was disclosed. Many researchers were concerned about vulnerability assessments of ICSs. This was due to the realization that obscurity and isolation are not effective means of protecting such systems.

A significant contribution to the understanding of the vulnerabilities and how the ICSs are targeted was provided by cyber security firms such as Trend Micro and Kaspersky. However, the data expressed in such sources are directed at an audience who are expected to be proficient in the area. Hence, many research articles were geared towards simplifying the information to be used by IT Professionals.

2.3 Literature Related to the Problem

An ICS network security vendor website, Trend Micro, discusses three primary motivations for an attack, these are financial gain, political cause and military objectives. Based on the level of motivation and resources at the attacker's disposal, it may be near impossible to shield a system from attack as seen in the case of Natanz nuclear enrichment facility. At Natanz, the worm created for the attack was extremely sophisticated with four zero-day vulnerabilities and the ability to seek out and attack very specific equipment (Karnouskos, 2012).

Trend Micro describes attacks on an ICS as a step-by-step process. Firstly, the attacker will gather information regarding the target ICS by surveying the environment. Next, the attacker will attempt to find ways to anchor into the network, after which potential vulnerabilities in the system would be analyzed. Once these steps are complete, the attacker will use malware or intrude into the network to cause the desired damage. The complexity of an attack ranges from simple (denial-of-service attacks) to complex (manipulating the control systems undetected).

As noted, Stuxnet virus brought attention to the vulnerabilities in critical infrastructure. The main concern behind the attack was with the nature in which it was used. Stuxnet was the launch of the first digital weapon and it unveiled a new theater of

war, cyberwarfare (Zetter, An Unprecendented Look at Stuxnet, the World's First Digital Weapon, 2014). Zetter (2014) details the order of events that ultimately led to the detection and the realization of the impacts of the virus. The article details the sophistication of the attack that allowed the infiltration to go undetected for an extended period, all the while attacking components vital to the process.

ICSs such as SCADA are responsible for many industrial processes such as production, power generation, water management and wind farms (Karnouskos, 2012). Karnouskos (2012), explains the realization of the vulnerabilities of what was thought of as systems impervious to cyber-attack was the lasting impact of Stuxnet. The author emphasizes on the importance of enforcing rules generally used in IT networks such as timely installation of security patches, better regulated and well defended networks. These measures are emphasized despite the increase in the overhead and the continuous maintenance demanded.

Attacks on ICSs have been reported in the past, however, the frequency of attacks especially on targets like power grids are on the rise, possibly inspired by Stuxnet. A carefully planned attack that prompts a cascading failure is possible (Che, Liu, Ding, & Li, 2019). A cascading failure occurs when certain parts of the power grid are overloaded, causing other parts to fail as a result. Generally, such occurrences are rare but cyber attackers can use a False Data Injection (FDI) attack to initiate them (Che, Liu, Ding, & Li, 2019). The authors describe and FDI attack as an act of intruding a network and falsifying the data received by the controllers, causing them to respond incorrectly. The simulations carried out in the study reveal the risks imposed by attackers targeting the control systems of the power grid and other critical infrastructure.

The advancements in technology such as Cloud-based SCADA has unearthed many advantages. For instance, a petroleum company located in Canada brought more than 300 wells online within a month by using offsite SCADA (Gavin, 2018). As described in the article, if the company opted to use onsite SCADA systems, bringing the wells online would have consumed more time and capital.

With the digitization of ICSs, the number of vulnerabilities and the targets available for attack has also grown (Gavin, 2018). Gavin (2018), highlights recent attacks such as the attack on Ukrainian power grid that caused blackouts for more than half a million people by the Sandworm hackers, the Shamoon virus that affected Saudi Arabian oil companies and the WannaCry ransomware that not only spread to hospital computer systems, but also to their equipment such as MRI scanners and blood testing devices. The author also highlights the fears within the industry that prevents them from modernizing their systems, and the opportunity cost of it.

The National Institute of Standards and Technology (NIST) has published a guide to secure ICSs (Stouffer, Pillitteri, Lightman, Abrams, & Hahn, 2015). Based on the guide, there are many potential avenues an ICS may experience disruptions. These disruptions can be due to troubles with the information flow, unauthorized manipulation of operational parameters and equipment, faulty data transmission, malware, neutralizing safety systems and commanding equipment to operate in self-destructive manner.

Stouffer, Pillitteri, Lightman, Abrams, & Hahn (2015) outlines the importance of restricting access to the ICS, both physically and logically. Access could be restricted logically by employing DMZs (Demiliterized Zones), minimizing traffic from the internet reaching into the ICS network. In addition to these measures, they recommend to take

measures such as installing safety patches (after testing for compliancy), use antivirus software and provide users with only the necessary privileges. These measures are aimed at insulating individual components of the ICS from being exploited.

The possibility of the ICS being compromised is inevitable (Stouffer, Pillitteri, Lightman, Abrams, & Hahn, 2015). Thus, contingency plans must be in place to recover the system in the shortest possible time. Moreover, the authors describe the need for redundancies for all critical components and the elimination of possibilities for cascading events.

Paridari, et al. (2018) discusses the need of a system-level security methods in order to protect ICSs. This idea was reached because of the “tight integration between the controlled physical environment and the cyber system” (Paridari, et al., 2018, p. 114). The authors also introduce the idea of attack detection (such as man-in-the-middle) by using data analytics and visualization.

Attacks on ICSs can come from many sources, such as, non-IT /process automation employees, IT /process automation employees, vendors /contractors and hackers/ external entities (Theron, 2014). Theron (2014) identifies the primary motivations for attacks as wanting to cause damage, tarnishing the reputation, siphoning data and financial gain. The analysis showed the existance many attack vectors, e.g. malware, USBs, network and email.

Common attack vectors for targeting a PLC or a SCADA system are man-in-the-middle, DoS, spoofing, packet injection and reconnaissance (Ponomarev & Atkison, 2016). Ponomarev & Atkison (2016) state that most attacks on SCADA systems target data packets sent to the SCADA system. They would send PLC values into the network

by falsely identifying themselves as an authorized engineer. Using this method, an attacker can present the operator with misinformation.

During the past 3-4 decades control system technology had advanced at being effective at controlling industrial processes (Kube, 2013). However, the security of such systems has dwindled when considering the threats. The primary reason for this was the reliance of industrial systems to on air-gaps. The drive to boost the performance of these systems has resulted in them being tethered to transport protocols such as TCP/IP (Kube, 2013). This has opened many critical infrastructures to be targets to even some unsophisticated attacks.

A risk assessment proves whether a cyber-physical system (CPS) can operate safely (Wu, Kang, & Li, 2015). Wu, Kang and Li (2015) presents a strategy to quantify the risk of a cyber-attack. In order quantify the risks, the attacks were classified into “physical availability, cyber availabilty, cyber integrity and cyber confidentiality attacks” (Wu, Kang, & Li, 2015).

Older ICSs may require patches and careful monitoring until they are phased out. On the contrary, new ICSs must be designed to circumvent all forecasted threats within its operational period (Mishina, Takaragi, & Umezawa, 2018). The remedy proposed by Mishina, Takaragi and Umezawa (2018) was to use a Fault Tree-Attack Tree (FT-AT) developed using vulnerability databases.

In the paper, “A tiered security analysis of Industrial Control System Devices”, authors Vargas, Langfinger and Vogel-Heuser (2017) dissects the components of an ICS and discusses vulnerabilities. The components were separated into hardware layer, firmware layer, and the programming layer (Vargas, Langfinger, & Vogel-Heuser, 2017).

This facilitates the recognition and the classification of vulnerabilities. For instance, most ICSs embed RTOs in their systems to provide the required level of reliability, speed and ruggedness (Vargas, Langfinger, & Vogel-Heuser, 2017). However, they are much more vulnerable when compared to typical operating systems used.

The document from the Homeland Security's Control Systems Security Program in the National Cyber Security Division explicitly states: "The strength, growth, and prosperity of this nation are maintained by key resources and a functioning and healthy infrastructure. Much of that infrastructure is sustained by a variety of industrial control systems." (Homeland Security, 2009). Homeland Security emphasizes the importance of enhancing the cyber incident response. This is because, and incident may cause data breaches or a compromised web site touting content to embarrass an organization shifting the public concern. However, a more serious attack that may have physical consequences such as changing the chemical composition of the water supply or a release of untreated sewage would instill a severe distrust on the organization that may take a long time to forget (Homeland Security, 2009).

Having a calculated and coordinated response to ICS attacks allows for a rapid deployment of preventative methods (Homeland Security, 2009). For this purpose, Homeland Security had put forth multiple automated approaches. These include Networks Intrusion Detection Systems (NIDS), Protocol-based Intrusion Detection System (PIDS), Host-based Intrusion Detection System (HIDS), Intrusion Prevention System (IPS), Network and Device Logging and the Configuration of Data Generators (Homeland Security, 2009).

2.4 Literature Related to the Methodology

Many studies have been conducted using a variety of methodologies to study the vulnerabilities and how they compromise ICSs. As noted, only a handful of these studies propose solutions to eliminate or mitigate the effects of these vulnerabilities. Upadhyay & Sampalli (2019), provided a table (Table 1) listing vulnerabilities of SCADA software along with recommendations to mitigate them.

Table 1

Courtesy of (Upadhyay & Sampalli, 2019)

SCADA product/software vulnerabilities and recommendations.

Vulnerability	Recommendation
Improper Input Validation (INFOSEC; Department of Energy 2008; Chaffin and Nelson 2011; Homeland Security 2015)	
Buffer overflow	1. Coding practice should incorporate length validation according to inputs; 2. Size of a buffer should not be identified by user inputs; 3. Sanity and integrity checks need to be implemented to avoid fuzzy attempts to crash the network or server by DOS.
Lack of index validation	1. Programmers should be trained to implement secure code by adopting index validation in practice; 2. To avoid network traffic intercept index value check needs to be implemented.
OS & SQL injections	1. Create static function calls for external commands; 2. Use library calls implementation technique in programming; 3. Use strict validation rules to accept input strings; 4. Use prepared statement, parameterized or stored function to process SQL queries.
Cross-Site Scripting	1. A web server should be tested and validated thoroughly for malformed inputs; 2. Developers can add an extra layer of protection using open source libraries which automatically detect the encoding of the data which must be filtered to prevent the system from XSS attacks; 3. Implement alerts and intrusion detection system for web browser and email security.
Directory path traversal	1. Specify strict acceptable inputs in a list; 2. Input string should be transformed into acceptable input before being validated.
Poor Code Quality (Quinn et al. 2009; Pauna and Moulinos 2013)	
Invalid function calls	1. The custom application should be implemented using security features; 2. Code review should perform during each iteration of testing; 3. SCADA protocols should integrate integrity check and authentication.
Improper resource shutdown of release	1. Product deployed into SCADA environment should also be passed through security check; 2. During the procurement process, asset owners should explicitly understand the security features of a product.
Null pointer dereferences	1. Null pointer dereferences can be prevented using a sanity check method before all pointers are modified.
Improper Control of Resource (NERC 2005; DHS and CSSP 2008; Pauna and Moulinos 2013)	
Poor patch management and security configuration	1. Management policies should include below mentioned elements in patch management program: 1.1 Configuration & patch management Plan 1.2 Incident responses plan 1.3 Vulnerabilities notification plan 1.4 Risk assessment plan 1.5 Backup/Archive plan 1.6 Disaster recovery plan 1.7 Complete and unified control system asset inventory plan 2. Consider below key points to maintain documentation of patch related alerts: 2.1 Keep all the records of relevant patch alerts 2.2 Define proper cataloging of patch related alerts 2.3 Maintain test results of the specific alert 2.4 List out possible solutions for each alert 2.5 Label best practices for patch management/configuration 3. Vendors should support in patch testing; 4. Vendors should provide the service for patch upgrades based on findings; 5. Vendors should always follow the latest version of the third-party software and update the current version by add-ins before delivering the product.

Kim, Heo, Zio, Shin, & Song, (2019), conducted a similar study for cyber attacks on the digital environment in nuclear power plants. They have developed a taxonomy for cyber-attacks on nuclear power plants where they used classifications such as attack procedure, attack vector, attack concequence, vulnerability and countermeasures. The attack procedure was further branched into “gathering information, acquiring access rights, command and control, and action and exfiltration” (Che, Liu, Ding, & Li, 2019). Furthermore, they subdivided the attack vector “into physical access and network access” (Che, Liu, Ding, & Li, 2019). Finally, the consquences were subdivided into two sub-catogories and they were sabotach and unauthorized removal of nuclear material.

Qualitative studies are most suited for understanding the nature of attacks against ICSs. Qualitative researches are conducted to “understand, explain, explore, discover, and clarify situations, feelings, perceptions, attitudes, values, believes and experiences”, (Kumar, 2011). Owing to this reason, study designs constructed qualitatively employ deductive logic instead of inductive logic. Moreover, these study designs are agile, non-linear and unorganized in their implementation (Kumar, 2011).

Qualitative research allows the researcher dive deep into acumens on vague topics. This is possible because, qualitative research is expressed in words. Thus, it enables the understanding of “concepts, thoughts or experiences”, (Streefkerk, 2019). Studies that require the investigation of specific attributes and consequences find case study to be a suitable research design. This is because, case studies allow the researcher to probe real world subjects and obtain a thorough “concrete, contextual and in depth knowledge”, (McCombes, How to do survey research, 2019). Furthermore, “if a study

contains more than a single case then a multiple-case study is required", (Baxter & Jack, 2008). This is comparable to a study with multiple experiments.

According to Church (2002), data collected indirectly by means of the work conducted by other researches are known as secondary data. Russell states, "secondary data analysis may be based on the published data or it may be based on the original data", (Church, 2002). Moreover, Streefkerk (2019) explains that the use of secondary data allows for a holistic view of the topic.

Non-probability sampling methods suite researches that are conducted to develop a preliminary understanding of a small population (McCombes, Understanding different sampling methods, 2019). This is because, such studies are focused on exploring and expanding the topics rather than testing a specific hypothesis for a large population (McCombes, Understanding different sampling methods, 2019). Moreover, according to Setia (2016) and McCombes (2019), a non-probability sampling study allows the researcher to simply include the data that are most accessible. Hence, such studies cannot produce generalized results (McCombes, Understanding different sampling methods, 2019).

The objective of a qualitative content analysis is to provide solutions to the research questions. Thus, a qualitative content analysis allows the researcher to be selective of the data (Hashemnezhad, 2015). Hsieh and Shannon (2005) list three distinct approaches to content analysis, they are "conventional, directed or summative", (Hsieh & Shannon, 2005). Although these are three distinct approaches, they all "adhere to the naturalistic paradigm", (Hsieh & Shannon, 2005) because the text data were used to interpret meaning. Moreover, Hsieh and Shannon (2005) defined qualitative content

analysis as “a research method for the subjective interpretation of the content of text data through the systematic classification process of coding and identifying themes or patterns”, (Hsieh & Shannon, 2005).

Joshi, Singh and Tarey (2015) explains that a taxonomy is a useful tool when “performing a systematic security assessment of a system”, (Joshi, Singh, & Tarey, 2015). Maria Kjaerland from the Faculty of Social Sciences, University of Stavanger, Norway has developed a taxonomy that is limited to cyber intrusions. The aspects for the taxonomy based on CERT/CC were “Source sectors, Method of Operation, Impact, Target Sectors”, (Kjaerland, 2006). These aspects were comparable to “Attackers, Tools, Access, and Results” developed by Maria.

In the article “A taxonomy of network and computer attacks”, by Hansman and Hunt (2005), a taxonomy was made and the correlations between the dimensions were made. For instance, a correlation between an attack and a vulnerability may reveal seemingly unrelated attacks may share common dimensions (Hansman & Hunt, 2005). This can then open new paths of research.

2.5 Summary

The literature reviews contained in this chapter describes similar studies conducted in the past. The studies provide a broader understanding of the vulnerabilities within ICSs and how attackers target them. The studies also provide a foundation to the method described in the following chapter. The literature review in this chapter was extensively used to frame the methodology that was used to collect and analyze data pertaining to past ICS security compromise incidents.

Chapter III: Methodology

3.1 Introduction

This chapter discusses the methodology of the study. The study was a qualitative multi-case study employing a non-probability convenience sampling technique to select data samples for the study. Secondary qualitative descriptive data was collected through literature reviews and case studies that were published in news articles, cybersecurity case studies, and prior research papers. Gathered data were analyzed through content conventional analysis from which a taxonomy was developed to present the results of the study.

3.2 Design of the Study

By nature, this study is a qualitative study. Therefore, the study used a qualitative approach based on three considerations. These three considerations were the study being: expressed in words, used to understand concepts and experiences and gathering in-depth insights on topics. The flexibility of the qualitative study approach allowed the study to be flexible throughout the study.

> Qualitative data collects information that seeks to describe a topic more than measure it. Think of impressions, opinions, and views. A qualitative survey is less structured: It seeks to delve deep into the topic at hand to gain information about people's motivations, thinking, and attitudes. While this brings depth of understanding to your research questions, it also makes the results harder to analyze (Survey Moneky, n.d.).

“Qualitative research is expressed in words. It is used to understand concepts, thoughts or experiences. This type of research enables you to gather in-depth insights on topics that are not well understood.” (Streefkerk, 2019)

> Qualitative research methods start from questions which tend to be more “open” and additional ideas for data collection can emerge during the data collection phase. Data can be gathered using a range of methods, including interviews, focus groups, or observations. Analysis of these data tends to be text-based (Boeren, 2018).

“The ‘power-gap’ between the researcher and the study population in qualitative research is far smaller than in quantitative research because of the informality in structure and situation in which data is collected.” (Kumar, 2011) “Because of flexibility and lack of control it is more difficult to check researcher bias in qualitative studies.” (Kumar, 2011)

Based on the characteristics established by the researcher of this study, attacks on ICSs from 2003 to 2017 with a physical aspect was constituted as the study population of this study. “A complete set of elements (persons or objects) that possess some common characteristic defined by the sampling criteria established by the researcher” (Populations and Sampling, n.d.).

Secondary data type was used in this study for data collection. The secondary data type was selected because it was easier and faster to access, larger and more diverse, flexible and conductible with small samples, and can be gathered from the study subject without intervening.

Due to the qualitative nature of the study, multi-case study approach was used as the study design. “Case study design is a very useful design when exploring an area

where little is known or where you want to have a holistic understanding of the situation." (Kumar, 2011) "Case study design is of immense relevance when the focus of a study is on extensively exploring and understanding rather than confirming and quantifying. It provides an overview and in-depth understanding of a case(s)." (Kumar, 2011)

> In this Case study design [our] attempt is not to select a random sample but a case that can provide you with as much information as possible to understand the case in its totality. When studying an episode or an instance, [our] attempt to gather information from all available sources so as to understand it in its entirety (Kumar, 2011).

"If a study contains more than a single case then a multiple-case study is required." (Baxter & Jack, 2008). Thus, the study had successfully adopted the multi-case. Nonprobability convenience sampling technique had to be used to determine the target sample of this study because the number of elements in the population was unknown and the data was gathered through the most accessible cases. Also, it was an easy and inexpensive way to gather the initial data. "non-probability sampling methods where the sample population is selected in a non-systematic process that does not guarantee equal chances for each subject in the target population." (Elfil & Negida, 2017)

10 cases of attacks on ICSs between 2003 and 2017 were selected as the sample size for this study. This sample was chosen because it was deemed to be the most representatives of the target population. In this study the number of related cases were decided in advance. However, the available data was collected until the data saturation point was reached.

“In qualitative research, you do not have a sample size in mind. Data collection based upon a predetermined sample size and the saturation point distinguishes their use in quantitative and qualitative research.” (Kumar, 2011) “In a non-probability sample, individuals are selected based on non-random criteria, and not every individual has a chance of being included. This type of sample is easier and cheaper to access.” (McCombes, Understanding different sampling methods, 2019) “Convenience sampling (also known as availability sampling) is a specific type of non-probability sampling method that relies on data collection from population members who are conveniently available to participate in study.” (Dudovskiy, n.d.)

3.3 Data Collection

Data for this study were sourced from the websites of cybersecurity firms, news articles, online magazines, scholarly articles and case studies. The articles were then vetted for credibility, relevance (presence of physical harm) and for the available content. The selection of secondary data for this study expanded the scope of the study and it was cost and time efficient.

There were no limits set on the number of ICS attacks considered for this study. However, based on the convenience sampling technique data were derived from ICS attacks that happened from 2003 to 2017.

3.4 Data Analysis

The textual data compiled from literature reviews, news media, case-studies, research papers and cybersecurity publications were analyzed to derive the attribute data from the attacks. The material compiled from these sources were analyzed using content

analysis. The derived attribute data was then organized into categories also known as dimensions.

> By using the Content analysis method, [the study] [was] able to analyze the data without the direct involvement of participants, so our presence as a researcher doesn't influence the results. Also, [the study] [was] able to followed a systematic procedure that could easily be replicated by other researchers, and produced results with high reliability. Due to the high flexibility of this method [the study] could conduct [the] data analysis at any time & in any location at low cost by accessed to the appropriate sources (Luo, 2019).

There are three types of content analysis, and they are; conventional content analysis, directed content analysis and summative content analysis. This study began with observation and the codes derived from data were defined during the data analysis. Therefore, a conventional content analysis was employed.

"In conventional content analysis, coding categories are derived directly from the text data.With a directed approach, analysis starts with a theory or relevant research findings as guid-ance for initial codes." (Hsieh & Shannon, 2005)

The data analysis was followed using the steps in *Figure 4*.

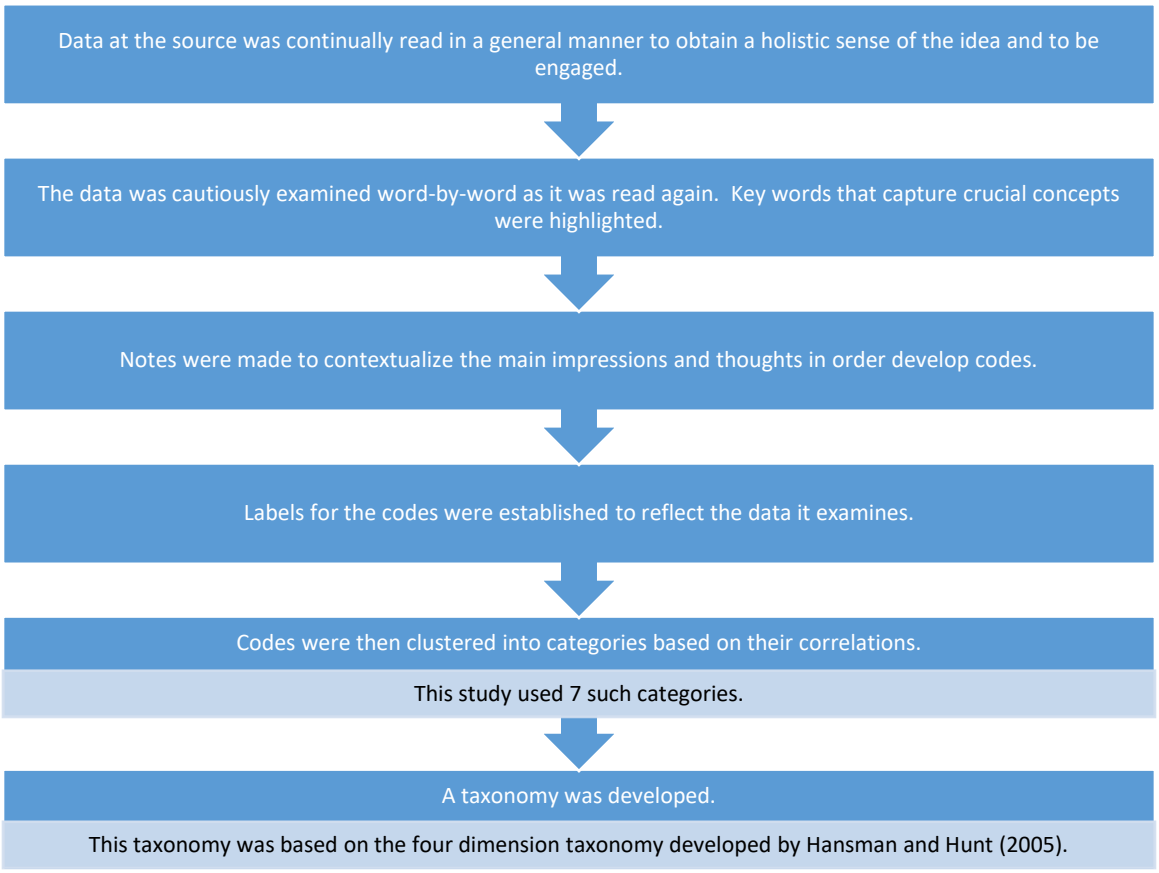

Figure 4. Steps for data analysis

3.5 Summary

This chapter described the methodology employed to collect and analyze the data obtained for selected 10 number of cases of attacks on ICSs from 2003 to 217. The methodology used, was a qualitative multi-case study and it employed a non-probability convenience sampling technique to select data sample from the population for the study. This methodology used employed a conventional content analysis on the secondary qualitative descriptive data collected through literature reviews and case studies that were published in news articles, cybersecurity case studies, and prior research papers.

Chapter IV: Data Presentation and Analysis

4.1 Introduction

This chapter presents the 10 cases considered for the study as the sample of study. Each case was introduced and explained utilizing the secondary data sourced from news articles, research papers, cybersecurity firms and case studies. The data presented and the subsequent analysis was detailed in this chapter.

4.2 Data Presentation

4.2.1 Saudi Arabian Petrochemical Plant Attacked, 2017

Triton is a rare caliber of malware because its creators had the intention of targeting safety systems of their victims. These safety systems are the last line of defense against serious accidents. Safety systems actively monitor, warn and act against any impending accidents. Therefore, malfunctions in these systems can compromise the safety of the facility as well as its employees and nearby residents (Giles, 2019). For example, in 1984, the leak of highly toxic Methyl Isocyanate (MIC) from the Union Carbide India Limited (UCIL) in Bhopal, India killed 3,787 victims.

The malware, Triton, discovered in a Saudi Arabian petrochemical plant, if deployed without bugs, would allow the attacker to take control over the plant's safety systems (Giles, 2019). Triton targets a vulnerability (this vulnerability has since been patched) in the Triconex safety controllers that were offered by Schneider Electric (Giles, 2019). Triconex safety systems are widely used in the industry and they can be found in safety applications ranging from water treatment facilities to nuclear power plants (Giles, 2019).

A bug in the cyberweapon caused two shutdowns of the petrochemical plant. The initial outage was thought to be due to a mechanical glitch, however, due to a second shutdown, industrial cybersecurity specialists from FireEye and Dragos were dispatched to investigate before the plant was brought online again. The investigation revealed the attackers had been able to infiltrate the company's corporate IT network since 2014.

The investigators speculate, a poorly configured firewall may have allowed the hackers to access the plant's network. Moreover, an unpatched windows vulnerability or by intercepting a worker's login credentials would have gotten them access to an engineering workstation with a communication link to the safety systems used at the plant.

The hackers having access to the engineering workstation learned about the safety layout of the facility. This revealed to them, the use of the Triconex safety controller. Thus, they most likely acquired a controller of their own and probed it for its vulnerabilities and communication protocols. This would have presented them with the zero-day-vulnerability in the controller that would have given them full control of the safety system.

The hackers of this attack were unquestionably targeting the specific sites the malware was found. Thus, this attack was a highly sophisticated one, and may have the involvement of nation states. Giles (2019), compares this attack to the Stuxnet attack, in terms of the commitment from the hackers and their capability. However, Giles (2019) distinguishes this cyberweapon from the one used at Natanz nuclear enrichment facility due the moral inaptness of the Saudi Arabian petrochemical plant hackers in their blatant disregard for human life.

4.2.2 Ukraine Power Grid, 2016

The attack on the Ukrainian power grid during the month of December in 2016 was the second such attack on Ukraine's power grid. The target of the attack was a substation north of Kiev, and it triggered a blackout that lasted for about an hour (Greenberg, 2017). The attack was well-coordinated and carried over some DNA from the 2015 attack e.g. the telephone denial-of-service (TDoS) for the call centers was repeated in this attack (Hemsley & Fisher, 2018).

Two cybersecurity firms ESET and Dragos Inc. were dispatched to analyze the attack. Based on their findings, this was the second case where a malware was written to target a specific hardware component (Greenberg, 2017). The malware, "Crash Override", or also known as "Industroyer" was found to be modular and be adapted to a range of attacks against electricity utilities (Greenberg, 2017).

Unlike the previous attack, this attack was fully automated (Greenberg, 2017). This can therefore be a force multiplier for the attackers. The Crash Override malware was able to find and communicate with grid equipment using obscure protocols. Thus, once the malware was deployed, probably using phishing attacks, the malware can command grid equipment to turn on or off without significant human intervention. This means, attacks can be planned out quickly and with smaller teams.

Based on ESET's analysis, the malware can cause physical damage to power equipment. In the case of this specific attack, the malware seemingly sought after a vulnerability in a Siemens hardware named Siprotec digital relay (Greenberg, 2017). The device was designed to open circuit breakers if power levels exceed certain limits. However, if the device receives a specific string of data, it disables itself until it is

physically rebooted, thus, causing major issues. Manipulating these breakers would allow the attackers to cause significant damage to power lines, transformers and other grid components. These damages would ultimately extend blackout periods.

The attackers can also orchestrate a cascading outage using this type of attack. This is because multiple points can be attacked simultaneously in a choreographed manner. This will cause multiple regions to face blackouts at the same time making it difficult for administrators to handle the issue (Greenberg, 2017).

4.2.3 Kemuri Water Company, 2016

Kemuri Water Company (KWC), is a fictional designation given to a water utility by Verizon Security solutions. The water utility company experienced an attack on its ICS/ SCADA by a Syrian hacktivist group. The attackers were able to manipulate the chemicals added to the water supply by gaining control of the PLCs used (Hemsley & Fisher, 2018). They were reportedly accomplished this by employing low level technics such as and SQL injection (Leyden, 2016).

KWC was home to many vulnerabilities (Brocklehurst, 2017). Firstly, the internet payment application webserver used a single factor authentication. Secondly, it was directly connected to the AS400 server. Thirdly, the AS400 server's IP address was listed in the application server in simple text format. However, the most dangerous network decision that was made was having KWC's OT network directly tethered to the AS400 server.

The single administrator responsible for the AS400 server lacked any oversight. This allowed the malpractices such as using same login credentials by the administrator for the remote access of the AS400 and payment application webserver go unnoticed. Thus, allowing the threat actors easy paths to infiltrate.

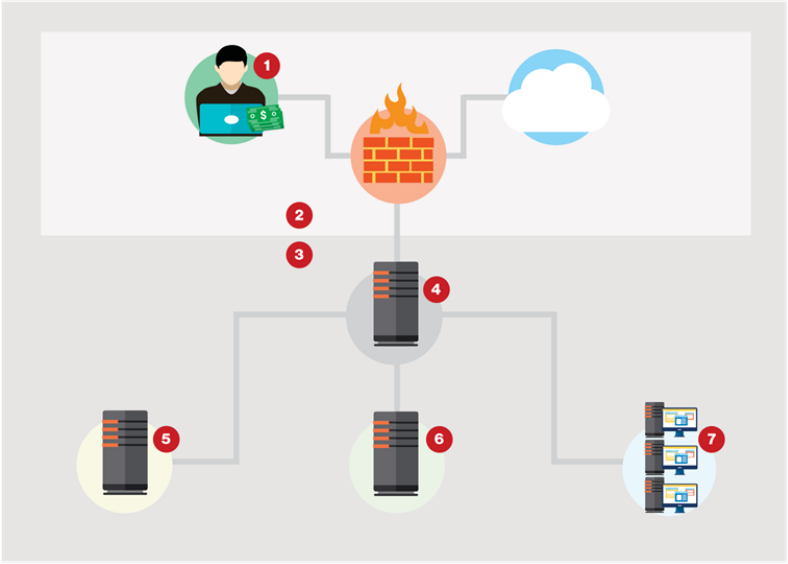

Figure 2

1. Customer access to payment system
2. External (Internet)
3. Internal (Corporate access)
4. AS400
5. PLC management
6. Finance access (PII access)
7. IT management

Figure 5: Poor network framework of Kemuri water company (Verizon, 2016)

The “hacktivist” group stole 2.5 million unique records, but they were interested in causing public harm by adjusting chemical level and flow rates (Brocklehurst, 2017). The hacktivists happened to have a limited knowledge of the ICS/SCADA. Hence, KWC was able to adjust the chemical levels and flow rates back to what it should be (Verizon, 2016).

4.2.4 Ukraine Power Grid, 2015

The first known example of interrupting the functionality of a power grid occurred at Ukraine during the December of 2015. The logistical sophistication of the attack was very high, because unlike the attack later in 2016, this attack was driven manually. Also, the attack was against a hardened target, with many safety precautions.

The result of the attack impacted more than 230,000 residents, and they were without power for more than 6 hours during winter. This attack was speculated to be sponsored by a nation state, motivated by political retaliation.

The hackers used spear-phishing to gain access to the cooperate network. They sent Microsoft Word files with a Trojan (BlackEnergy3), that gets activated when the unwitting user authorizes the Word files to run macros. They were unable to navigate to the SCADA networks directly from the cooperate network due to the presence of firewalls. Thus, they hijacked VPNs to access the SCADA network remotely.

The attackers strategized the attack after learning about various components of the ICS used by the power distributor. Leading to the attack, the uninterruptible power supplies (UPSs) used at the site were disabled. Additionally, malicious software was written to overwrite the firmware of the serial-to-ethernet convertors. This was to prevent the power company from remotely accessing them to close the breakers again. Finally, they injected a logic bomb with a payload (KillDisk) to cover their tracks. This would overwrite the data in important system files causing the computers crash and unable to boot again.

At 3:30 PM on December 23rd, 2015, the attack was executed. The plan was executed flawlessly, and as an added measure, they triggered a TDoS attack right before bringing down the power. This would prevent the customers from phoning into report the outage. The outage lasted up to 6 hours and the breakers that were remotely opened by the attackers had to be manually closed because of the damage done to their serial-to-ethernet convertors. However, their plan exfil without a trace failed because the firewall and system logs accrued allowed the security experts in Ukraine and the United States of America reconstruct the attack (Zetter, Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid, 2016).

4.2.5 German Steel Plant Attack, 2014

An undisclosed German steel plant suffered a major cyber-attack based on a report published by the German Federal Office for Information Security (BSI), (Tend Micro, 2015). The attack was described as an advanced persistent threat (APT) attack (Lee, Assante, & Conway, 2014). Based on the report, the plant's furnace was physically damaged after plant controls failed.

The information provided by BSI, indicates the attackers to have used spear-phishing to get into the corporate network. However, information describing their intrusion into the OT/ ICS is unavailable. Nevertheless, they were able to infiltrate the ICS demonstrating their expertise with ICSs. Once, they were there, they were able to cause significant damage, specifics of which are not disclosed.

4.2.6 Bowman Avenue Dam, 2013

Bowman avenue dam is a small dam located in New York. In 2013, Iranian hackers gained unauthorized access to the SCADA systems of the dam which allowed them to have visibility of sensor data such as water levels and temperatures. They would have also been able to control the flood gates and cause flooding. However, it is noted that at the time of attack this would not have been possible due the sluice gate being under repair and hence offline (Berger, 2016).

One of the attackers identified, Hamid Firoozi, had apparently used an unsophisticated method, namely, "Google Dorking" to identify the vulnerability (Nation-E, 2016). He then implemented more advanced maneuvers and technologies to successfully intrude. This attack highlights the importance of eliminating a lax attitude towards network security. Moreover, such dams and infrastructures are dotted all around

the United States, and thus, a consorted effort at targeting such soft targets may lead to substantial damages to the economy. Hence, all ICSs that have a path to the internet must practice a high level of network security.

4.2.7 Honeypot, 2013

Honeypot is a cybersecurity tool that is used to collect data on attackers. They are commonly implemented by cybersecurity vendors. Honeypots entice attackers by emulating internet facing ICSs and SCADA systems. They often present attackers with vulnerabilities and observe the attack vectors hackers use. The data gathered by honeypots allow researches and cybersecurity specialists to learn about the threat landscape and implement preventative methods.

Trend Micro is a major cybersecurity firm that conduct such tests. They use high interaction honeypots to mimic physical ICS devices like PLCs and low interaction honeypots to mimic production systems (Wilhoit, 2013). These honeypots were then deployed strategically around the world. For the 2013 honeypot study, the honeypots were set to operate separately, hence, no communications were established within one another. Moreover, the honeypots were made to appear local using language and local customs.

As a precursor to most attacks, hackers performed recon on the honeypots using ShodanHQ. They also use text sharing platforms Pastebin and Pastie. Attackers while masking their IP address using software and services akin to Tor, would scan the netblock and the ports of the subnets surrounding the target. Moreover, to identify potential vulnerabilities, they try to determine OSs using fingerprinting and exfiltrate data such as Virtual Private Network (VPN) configuration files.

The study did not consider superficial attacks such as SQL injections as “attacks”. Trend Micro was primarily interested in targeted attacks. Based on their definition of attacks, 74 attacks from 16 countries were logged on 7 of their honeypots. Of these 11 were considered critical as they had the potential of causing catastrophic failure of the ICS device.

The definition of critical attacks here would not include DDoS attacks. The attacks that were deemed critical included Modbus traffic modification, water pump CPU fan speed modification and setpoint modification. An example of an attack on a honeypot located at Japan is illustrated in *Figure 6*.

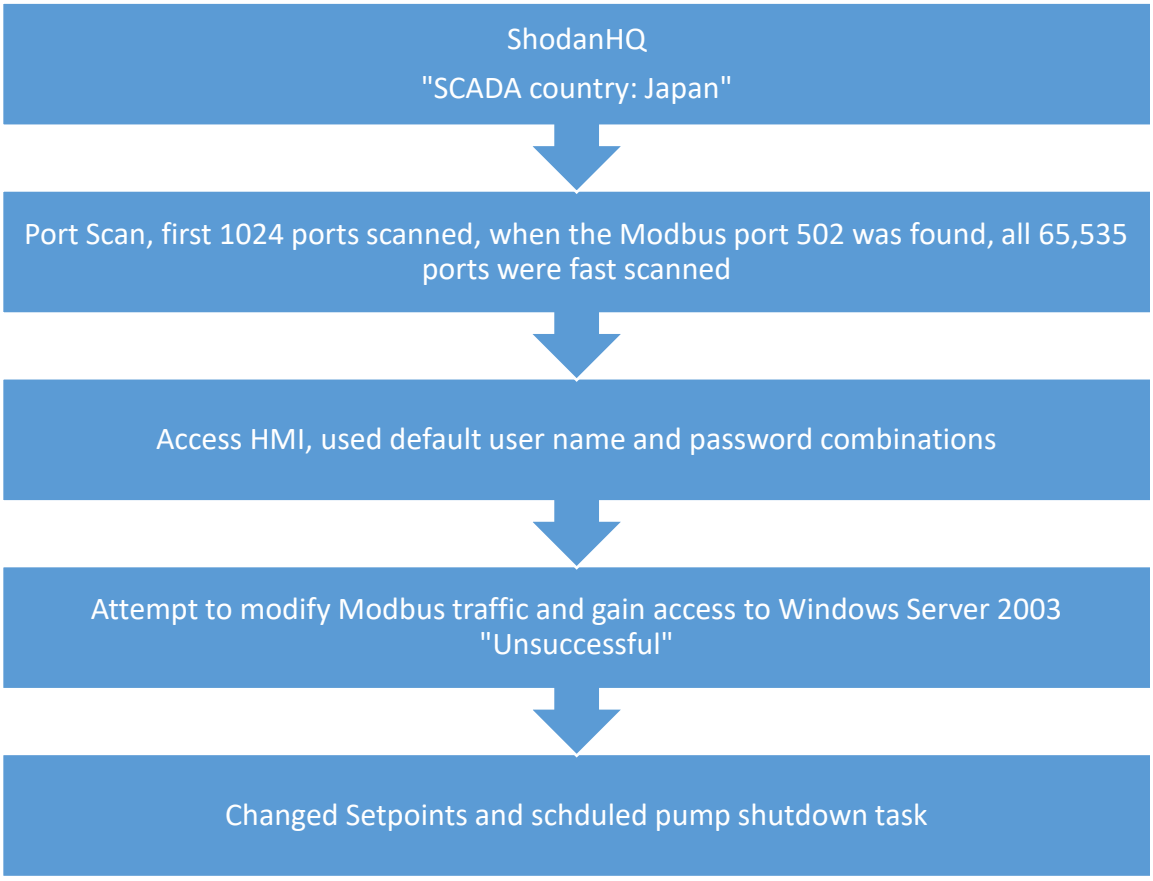

Figure 6. Sample honeypot attack

4.2.8 Attack on Natanz Nuclear Enrichment Facility, 2010

The attack on Natanz nuclear enrichment facility in Iran with the cyberweapon Stuxnet was the first of its kind. It was one of the most daring and sophisticated attacks accomplished. The attack blurred the boundaries of the cyber domain of warfare as it introduced a new element, “sabotage” into this domain. Up until that point, cyber domain of warfare consisted of espionage, propaganda and economic disruption.

Stuxnet provided the blueprint and the inspiration for a whole range of malware e.g. Duqu (2011), Flame (2012), Havex (2013), Industroyer (2016) and Triton (2017) (McAfee, n.d.). These malwares, or also known as cyberweapons, follow the same suite as Stuxnet. They were most likely sponsored by nation states and executes their tasks with surgical precision.

Stuxnet was rumored to be in use, even before the centrifuges at Natanz spun into their destruction. It would have depended on a rogue employee at the facility in order to jump the air gap for most of its life. However, significant modifications to the malware code, such as including four zero-day vulnerabilities, allowed the weapon to find its way into the facility by infecting the computers of contractors that service the facility.

The payload of the malware sought after a specific model of a PLC manufactured by Siemens. Meanwhile, the worm would appear to lay dormant, all the while it logged communications between the PLC and the SCADA system. If the PLC was connected to specific drives that were commanded to spin at a certain frequency. Then, Stuxnet would overwrite the programs and cause the centrifuges to damage themselves. Meanwhile, Stuxnet would replay logged data to the SCADA systems keeping operators blind to the destruction happening to the centrifuges (Fruhlinger, 2017).

4.2.9 LA Traffic Light Hack, 2006

Films are often credited with being predictors of the future. Fictional action scenes in films such as “Live Free or Die Hard” and “The Italian Job”, have made us spectators to possibilities of cyber-attacks when unleashed in a physical arena (Aaronson, 2014). The LA traffic light hacking incident on 2006 may prove the reality is not far from fiction.

Two traffic engineers from Los Angeles made the fiction a fact on 2006, when they decided to hack the city’s traffic control system. The two engineers, Kartik Patel and Gabriel Murillo accessed the system remotely and modified the light sequences in four intersections of the city. Their actions were akin to a hacktivist as they had acted in support of a labor union protest, and it ultimately resulted in a severe traffic jam that went on for multiple days.

The traffic engineers most likely had classified knowledge on how they could access the traffic light control system remotely. However, this attack clearly illustrates the vulnerabilities created by bringing infrastructure such as traffic lights online. Few years later, it was reported that a security expert was able to hack into the New York’s traffic control system by just using $100 hardware hitting the issue home (Aaronson, 2014).

4.2.10 Davis-Besse Nuclear Plant, 2003

In the January of 2003, Davis-Besse Nuclear Plant located in Ohio experienced an infection by the worm named Slammer that was designed to attack MS-SQL. The worm successfully penetrated the private-computer network (Poulsen, 2003). This incapacitated the safety monitoring system known as the Safety Parameter Display System (SPDS), for almost five hours.

The SPDS provides indicators for coolant systems, core temperatures and external radiation sensors. Having an SPDS failure was more concerning at the time of the incident because a large hole in the reactor head was discovered along with other significant safety issues, leading to an extended shutdown (March 2002 – March 2004). Had the safety concerns were not found, and the plant continued its operations. The SPDS system would have been one of the last lines of defense in communicating any anomalies to the operators.

The worm found its way into the nuclear plant complex by means of a contractor's network. The cooperate network of Davis-Besse Nuclear Power Plant had an active firewall (Poulsen, 2003) but a T1 line from the contractor's unsecured network bypassed the firewall. In addition to this T1 line, investigators had found many other entry points into the plant bypassing the firewall.

The worm was able then spread to the plant network via the previously infected cooperate network. Due to the extreme use of the CPU power and network bandwidth by the worm, it crashed the Safety Parameter Display System (Holloway, 2015). Thus, causing the plant operators to rely on unaffected analog systems for almost five hours.

Nuclear power plants had since been enhanced security wise. Many plants have implemented stringent security measures and the likelihood of a stray worm or a virus entering mission critical systems at a nuclear power plant is next to impossible.

4.3 Data Analysis

Following the initial scanning of the content and the word-by-word conventional content analysis of the data sources, yielded the codes; victim, attack vector, attack tools,

target, payload, vulnerable hardware, attack identified, physical impact, initial response, vulnerabilities found, attacker profile, motivation and attack inception.

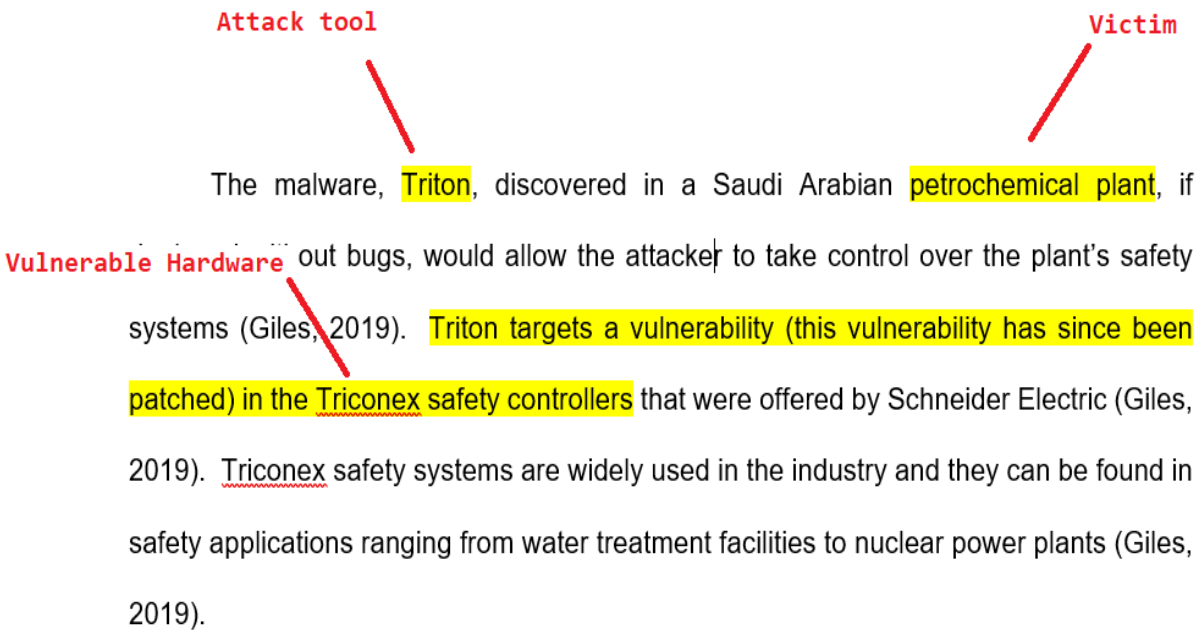

Figure 7. Coding method

Two examples, the case of the Saudi Arabian Petrochemical Plant, and the Ukrainian Power Grid Attack 2 are provided below, in order to demonstrate how the codes were generated.

Table 2

Coding of the Saudi Arabian petrochemical plant incdent

Content	**Code**
Petrochemical Plant	Victim
Malware	Attack Vector
Triton	Attack tool
Safety Systems	Target
Triconex by Schneider electric	Vulnerable Hardware
2014, Coorporate IT network	Attack inception
2017	Attack identified
Plant shutdown due to safety malfunction caused by attackers gaining control of the safety system	Physical impact
Mechanical glitch assumed	Initial response
Poorly configured firewall	Vulnerabilities
Unpatched windows vulnerability	Vulnerabilities
Potential interceptability of employee login credentials	Vulnerabilities
Sustained communication link between the work station and the safety system	Vulnerabilities
Zero-day-vulnerability in Triconex	Vulnerabilities
Targeted attacks	Attacker profile
High sophistication	Attacker profile
High commitment	Attacker profile
Non-resource constrained	Attacker profile
Disregard to human life	Attacker profile

Table 3

Coding of the Ukrainian Power Grid Attack 2

Content	**Code**
Power distributor	Victim
Utility	Victim
Malware	Attack Vector
Phishing	Attack Vector
Crashoverride	Attack tool
Industroyer	Attack tool
Remotely operated breaker switch	Target
Siprotec digital relay by Siemens	Vulnerable Hardware
2016	Attack Inception
2016	Attack Identified
Power blackout due to attackers taking control of the breaker switch	Physical Impact
Cyber attack assumed	Initial response
Power restoration through manual swithching	Initial response
Susceptatbility to phishing attacks	Vulnerabilities
Network allowing the unauthorized communication with critical components	Vulnerabilities
Targeted attacks	Attacker profile
Highly sophisticated	Attacker profile
High coordination	Attacker profile
Non-resource constrained	Attacker profile
Innovative	Attacker profile

After generating codes for all cases as shown above, the common codes that were found between most cases were categorized into the following seven groups: These seven groups were considered as the attributes of the attacks on ICSs.

Table 4

Code grouping

Group	**Code**
Attack Description	Attack Identified, Victim
Target Industry	Target
Vulnerability	Vulnerabilities found, Vulnerable hardware
Nature of The Attack	Attack tools, Attack vector
Payload and The Physical Impact	Payload, Physical impact
Attacker Profile	Attacker profile
Motivation	Motivation

Based on the groups a six-dimension taxonomy was developed, where the attack description was not considered to be a dimension. The attack description will be used for attack identification only.

The six dimensions that were used to base the taxonomy are expressed in the Table 5.

Table 5.

Six dimensions of the taxonomy

Dimension 1	Dimension 2	Dimension 3	Dimension 4	Dimension 5	Dimension 6
Target Industry	Vulnerability	Nature of the Attack	Payload & the Physical Impact	Attacker Profile	Motivation

The six-dimension taxonomy developed based on the six attributes of attacks on ICSs as below.

Table 6

The derived taxonomy model

Attack Description		Attributes of Attacks on ICS							
		Target Industry	Vulnerability		Nature of The Attack		Payload and The Physical Impact	Attacker Profile	Motivation
Year	Title		Vulnerability type	Description	Attack Vector	Attack Tool			

4.4 Summary

The data was analyzed using a conventional content analysis technique. This yielded codes that were clustered into seven groups, and these groups were considered as the attributes for the ICSs attacks. The seven attributes were used to develop a taxonomy which can be used as a tool to analyze the nature of historical ICS attacks. Of the seven attributes six were considered as dimensions and the remaining attribute was used as the attack identifier.

Chapter V: Results, Conclusion, and Recommendations

5.1 Introduction

This chapter presents the study results of the data analysis of selected sample 10 cases of attacks on ICS from 2003 to 2017. A taxonomy was developed to present the analyzed data on the study. The attributes derived from the attacks on the ICSs were represent the 6-dimension of the taxonomy.

5.2 Results

The methodology used in the study was a qualitative multi-case study and employed a non-probability convenience sampling technique to select data samples for the study. This methodology used employed a conventional content analysis on the secondary qualitative descriptive data collected through literature reviews and case studies that were published in news articles, cybersecurity case studies, and prior research papers.

The data was analyzed using a conventional content analysis technique. This yielded codes that were clustered into seven groups, and these groups were considered as the attributes for the ICSs attacks. The seven attributes were used to develop a taxonomy which can be used as a tool to analyze the nature of historical ICS attacks. Of the seven attributes six were considered as dimensions and the remaining attribute was used as the attack identifier. The resulting taxonomy from this study is illustrated in the Table 7 (Attacker profile, vulnerability and attack vector are elaborated in the appendix).

Table 7

The taxonomy of ICS attacks incident analysis

Attack Description		Target Industry	Vulnerability		Nature of The Attack		Payload and The Physical Impact	Attacker Profile	Motivation
Year	Title		Vulnerability type	Description	Attack Vector	Attack Tool			
2017	Saudi Arabian Petrochemical Plant Attacked	Petroleum	Implementation Configuration Design Design	Triconex Safety controller Firewall Windows security update not done ability to intercept worker login credentials	Malware	Triton	Take full control of the safety systems	Nation State	Economic Impact Put the facility and its employees at risk
2016	Ukraine Power Grid Attack 2	Utilities, Power Grid	Implementation	Siprotec digital relay from Siemens disables in response to a specific input	Malware Phishing	Crash Override, Industroyer Telephone DoS attack	Seek , communicate and command grid equipment. Disable grid equipment	Nation State Hackers	Disrupt activities Political
2016	Kemuri Water Company	Utilities, water supply	Design Configuration Implementation	Network connecting internet payment server (IPS) to AS400 server, OT network tethered to the AS400 Single factor authorization, AS400 IP address listed in plain text in the (IPS) AS400 Admin lacking any oversight	SQL Injection Phishing		Manipulate chemical additives and flow rates Data exfiltration	Hacktivist	Do harm to the public as a part of their activism
2015	Ukraine Power Grid Attack 1	Utilities, Power Grid	Configuration	Attackers were able to hijack the VPNs	Phishing Trojans Network attacks Malware Logic bombs Denial of service attacks	Trojan, BlackEnergy3 Overwrite firmware of serial-to-ethernet convertors KillDisk Telephone DoS attack	Disable the UPSs at the control center Make the Serial-to-ethernet convertors unusable Crash all the computer systems	Nation State	Political Retallation Disrupt activities
2014	German Steel Plant Attack	Industrial	Implementation	An employee was tricked into opening a malicious file	Phishing		Disable the plant	APT	Disrupt functions
2013	Bowman Avenue Dam	Flood Management	Design	Internet facing OT network	Google Dorking		Take control of the SCADA system	Nation State	Political
2013	Honeypot	NA	Design Configuration Implementation	Intentional lapses in security for design Intentional lapses in security for configuration Intentional lapses in security for implementation	SQL Injection Denial of service attacks OT (Modbus, Profibus etc.) Traffic Modification CPU Fan Speed Modification	Not a serious concern in this context Not a serious concern in this context Serious attack Serious attack	Set points when changed would harm processes the ICS is responsible for Modbus Traffic Modification allows attackers to take over SCADA systems CPU Fan speed modification can cause hardware to fail	Nation State Hacktivist Hackers	Economic Impact Cause disruptions Political
2010	Attack of Natanz Nuclear Enrichment Facility	Nuclear Enrichment	Implementation Implementation	The worm was able to hitchhike on a contractor's computer or USB drive The high reliance on airgaps and obscurity does not work anymore	Setpoint modification Worms OT (Modbus, Profibus etc.) Traffic Modification Spyware	Serious attack Stuxnet is a worm that can easily spread from one device to another Stuxnet can hijack communications Stuxnet can remain undetected and log data	Seek Siemens PLCs and evaluate their performance connections If pre-determined conditions are matched, execute a sabotage sequence of operations	Nation State	Political Sabotage Cause disruptions
2006	LA Traffic Light Hack	Traffic Control	Configuration	The traffic engineers were able to access the network remotely and while not on site		Remote access	Cause major disruptions to the flow of traffic	Insider	Activism
2003	David-Besse Nuclear Plant	Utility, Nuclear Power Generation	Configuration Design	While a firewall was present, it did not matter because a T1 line bypassed it when connecting to a contractor The worm was able to infect the OT network once the IT network was infected	Worms	Slammer	Spread, slow down and crash computers. Unintentionally, crashed the safety system	Unknown	Unintentional

Based the results of the study the study questions have been successfully answered as follows:

1. How to analyze the nature of the attacks on Industrial Control systems?

   This study presents six attributes to analyze the nature of attacks on Industrial Control Systems. By using the taxonomy presented in this study, interested parties can clearly understand the nature of those attacks and how they may be carried out in the future.

2. What are the key attributes of the attacks on Industrial Control systems?

   I. Target industry
   II. Vulnerability type
   III. Nature of the attack (attack vector and attack tool)
   IV. Payload and the physical impact
   V. Attacker profile
   VI. Motivation

3. What vulnerabilities are common to most ICSs?

   Vulnerabilities common to most ICSs are vulnerabilities in implementation, configuration and design.

4. How to forecast the possible attacks on ICS?

Using the proposed taxonomy in this study as a tool, interested parties can identify the vulnerabilities of a specific ICS and predict the most common types of attacks carried out against such vulnerabilities.

5.3 Conclusion

The use of ICSs such as SCADA is prolific in critical infrastructure such as power plants, water treatment facilities, petroleum refining and chemical processing. With the growth of the cyberspace, ICSs that critical infrastructure rely upon, are increasingly becoming internet facing systems (IIOT). Hence, they are vulnerable to cyber-physical attacks and these vulnerabilities heighten the risk of disruptions and safety concerns to the society.

Widespread grief including loss of life can be brought onto to large populations if a successful attack was to target critical infrastructure, since they have a direct physical impact such as power outages, pipe explosions, malfunctions in the water and sewage management. To minimize/ prevent ICSs from being compromised an understanding of past attacks are necessary. Thus, this study's primary objective is to address this necessity.

This study discussed past cases of attacks on ICSs and clarified them by their attributes. In order to accomplish this study, a qualitative multi-case study was employed. Attacks on ICSs from 2003 to 2017 were selected as the population for this study. 10 cases have been selected from the population as the sample for this study by non-probability convenience sampling technique. Data were collected from literature reviews, case studies, past research etc. and by using conventional content analysis the data were analyzed and through that six attributes from attacks on ICSs were derived. Based on

those attributes the study presented a six-dimension taxonomy that can be used as a tool to analyze the nature of historical ICS attacks and forecast characteristics of future attacks.

5.4 Recommendations

Based on the study, the following recommendations were made:

- Security patches must be piloted and installed in ICSs when every they become available. If the security patch is incompatible with the ICS, then an understanding of the vulnerability must be developed, and heightened safety measures must be implemented until a suitable patch becomes available.
- Any development in an ICS environment that is out of the ordinary must be treated as an attack and remedial measures must be implemented.
- Network architecture must mask OT systems from the internet, and all communication must be managed through firewalls, managed switches and protocols.
- Tunnels such as VPNs must be disabled when not in use, and onsite control systems must always be preferred despite cost premiums.

5.5 Contributions of the study

The primary contribution of this study is the taxonomy developed to aide interested parties with the understanding of various types of attacks on industrial control systems used in critical infrastructure. The summary of attacks in the recent past that are included in the taxonomy will provide the reader with a good understanding on how the attack was

carried out, how the victim was selected, the motivations behind the attacks and the tools used or developed for these attacks.

This paper is also written to serve as a starting point for researchers who are interested in industrial control systems and their vulnerabilities. This is because, this paper has sourced and summarized a wealth of information from a diverse set of sources. These sources range from articles published by cyber security experts such as Kaspersky and Trend Micro to journalistic articles published such those in the Wired magazine.

5.6 Future Work

The taxonomy developed can be further expanded with additional dimensions and data.

References

Aaronson, X. (2014, May 22). *How LA's Traffic System Got Hijacked*. Retrieved from VICE: https://www.vice.com/en_us/article/3dkk8k/how-las-traffic-system-got-hacked-5886b6f8f672c2456362f36b

Baxter, P. , & Jack, S. (2008). Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. *NSU Florida CAHSS JOURNALS*. Retrieved from https://nsuworks.nova.edu/tqr/vol13/iss4/2/

Berger, J. (2016, March 25). *A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case*. Retrieved from The New York Times: https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html

Boeren, E. (2018). The Methodological Underdog: A Review of Quantitative Research in the Key Adult Education Journals. *SAGE Journals*. Retrieved from https://journals.sagepub.com/doi/pdf/10.1177/0741713617739347

Brocklehurst, K. (2017, February 22). *U.S. Water Utility Breach and ICS Cyber Security Lessons Learned*. Retrieved from Belden: https://www.belden.com/blog/industrial-security/u-s-water-utility-breach-and-ics-cyber-security-lessons-learned

Che, L., Liu, X., Ding, T., & Li, Z. (2019, September 24). Revealing Impacts of Cyber Attacks on Power Grids Vulnerability to Cascading Failures. *IEEE Transactions on Circuits and Systems II: Express Briefs, 66*(6), 1058-1062.

Church, R. M. (2002). The Effective Use of Secondary Data. *Elsevier*, 32-45.

Cyber Immunity, a holistic view for Industrial Control Systems. (2017, November 22). Retrieved from is5communications: https://is5com.com/uncategorized/nov-22-2017-cyber-immunity-a-holistic-view-for-industrial-control-systems/

Dudovskiy, J. (n.d.). *Convenience sampling*. Retrieved from research-methodology.net: https://research-methodology.net/sampling-in-primary-data-collection/convenience-sampling/

Elfil, M., & Negida, A. (2017, Jan 14). Sampling methods in Clinical Research; an Educational Review. *National Center for Biotechnology Information*. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5325924/

Fruhlinger, J. (2017, August 22). *What is Stuxnet, who created it and how does it work?* Retrieved from CSO: https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html

Gavin, R. (2018, August). Cybersecurity for cloud-based SCADA. *CONTROL ENGINEERING*, 50-52.

Giles, M. (2019, March 5). *Triton is the world's most murderous malware, and it's spreading*. Retrieved from MIT Technology Review: https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/

Greenberg, A. (2017, 06 12). *'Crash Override': The Malware That Took Down a Power Grid*. Retrieved from WIRED: https://www.wired.com/story/crash-override-malware/

Hansman, S., & Hunt, R. (2005, January 28). A taxanomy of network and computer attacks. *Computers & Security*. ELSEVIER.

Hashemnezhad, H. (2015). Qualitative Content Analysis Research: A Review Article. *Journal of ELT and Applied Linguistics (JELTAL), 3*(1), 54-62.

Hemsley, K. E., & Fisher, R. E. (2018). *History of Industrial Control System Cyber Incidents.* Idaho Falls: Idaho National Laboratory.

Holloway, M. (2015, July 16). *Slammer Worm and David-Besse Nuclear Plant*. Retrieved from Standford: http://large.stanford.edu/courses/2015/ph241/holloway2/

Homeland Security. (2009). *Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability.* Retrieved from US-Cert.gov: https://www.us-cert.gov/sites/default/files/recommended_practices/final-RP_ics_cybersecurity_incident_response_100609.pdf

Hsieh, H.-F., & Shannon, S. E. (2005, November). Three Approaches to Qualitative Content Analysis. *QUALITATIVE HEALTH RESEARCH, 15*(9), 1277-1288.

Joshi, C., Singh, K. U., & Tarey, K. (2015). A Review on Taxonomies of Attacks and VUlnerability in Computer and Network System. *International Journal of Advanced Research in Computer Science and Software Engineering, 5*(1), 742-747.

Karnouskos, S. (2012, January 3). Stuxnet Worm Impact on Industrial Cyber-Physical System Security. *IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society*. IEEE Xplore.

Kim, S., Heo, G., Zio, E., Shin, J., & Song, J.-g. (2019, November 1). Cyber attack taxonomy for digital environment in nuclear power plants. Retrieved from https://doi.org/10.1016/j.net.2019.11.001

Kjaerland, M. (2006). A taxonomy and comparison of computer security incidents from the commercial and government sectors. *ELSEVIER*, 522-538.

Klein, M. (2017, May 19). *SCADA LIFE CYCLE – A LOOK BACK AND AHEAD*. Retrieved from CONCENTRIC INTEGRATION: http://goconcentric.com/resources/scada-life-cycle-a-look-back-and-ahead/

Kube, N. (2013, February). Cybersecurity And SCADA In Critical Infrastructure. *Pipeline & Gas Journal, 240*, N46-47.

Kumar, R. (2011). In R. Kumar, *Research Methodology* (3 ed., p. 123). SAGE Publications Ltd.

Lee, D. (2012, May 28). *Flame: Massive cyber-attack discovered, researchers say*. Retrieved from BBC: https://www.bbc.com/news/technology-18238326

Lee, R. M., Assante, M. J., & Conway, T. (2014). *ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper – German Steel Mill Cyber Attack.* SANS ICS.

Leyden, J. (2016, March 24). *Water treatment plant hacked, chemical mix changed for tap supplies*. Retrieved from The A Register: https://www.theregister.co.uk/2016/03/24/water_utility_hacked/

Luo, A. (2019, July 18). *What is content analysis and how can you use it in your research?* Retrieved from scribbr: https://www.scribbr.com/methodology/content-analysis/

McAfee. (n.d.). *What Is Stuxnet*. Retrieved from McAfee: https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html

McCombes, S. (2019, August 20). *How to do survey research*. Retrieved from Scribbr: https://www.scribbr.com/methodology/survey-research/

McCombes, S. (2019, September 19). *Understanding different sampling methods*. Retrieved from scribbr: https://www.scribbr.com/methodology/sampling-methods/

Mishina, Y., Takaragi, K., & Umezawa, K. (2018). A Method of Threat Analysis for Cyber-Physical System using Vulnerability Databases. Tokyo, Japan: IEEE.

Monyai, R. (2018, September 7). *More than 40% of ICS computers were attacked in H1 2018*. Retrieved from AVeS: https://aves.co.za/ics-computers-attack-statistics-h1-2018/

Nation-E. (2016, August 4). *Cyber-Attack Against the Bowman Avenue Dam*. Retrieved from Nation-E: http://www.nation-e.com/blog/new_page_759

Paridari, K., O'Mahony, N., El-Din Mady, A., Chabukswar, R., Boubekeur, M., & Sandberg, H. (2018, January). A Framework for Attack Resilient Industrial Control Systems: Attack Detection and Controller Reconfiguration. *Proceedings of the IEEE, 106*(1), 113-128.

Ponomarev, S., & Atkison, T. (2016). Industrial Control System Network Intrusion Detection by Telemetry Analysis. *IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, 13*(2), 252-260.

Populations and Sampling. (n.d.). Retrieved from http://www.umsl.edu/: https://www.umsl.edu/~lindquists/sample.html

Positive Technologies. (2019, April 11). *ICS vulnerabilities: 2018 in review*. Retrieved from Positive Technologies: https://www.ptsecurity.com/ww-en/analytics/ics-vulnerabilities-2019/

Poulsen, K. (2003, August 19). *Slammer worm crashed Ohio nuke plant network*. Retrieved from SecurityFocus: https://www.securityfocus.com/news/6767

ProfileTree. (n.d.). *What Is Content Analysis? Quantifying the Qualitative*. Retrieved from Profiletree: https://profiletree.com/what-is-content-analysis/

Setia, M. S. (2016). Methodology Series Module 5: Sampling Strategies. *Indian Journal of Dermatology, 65*(5), 505-509.

Stephanie. (2015, June 26). *Convenience Sampling (Accidental Sampling): Definition, Examples*. Retrieved from statisticshowto: https://www.statisticshowto.com/convenience-sampling/

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015, May). Guide to Industrial Control Systems (ICS) Security. *NIST Special Publication 800-82(2)*. National Institute of Standards and Technology.

Streefkerk, R. (2019, April 12). *Qualitative vs. quantitative research*. Retrieved from www.scribbr.com: https://www.scribbr.com/methodology/qualitative-quantitative-research/

Survey Moneky. (n.d.). *The difference between quantitative vs. qualitative research*. Retrieved from surveymonkey: https://www.surveymonkey.com/mp/quantitative-vs-qualitative-research/?program=7013A000000mweBQAQ&utm_bu=CR&utm_campaign=71700000059189232&utm_adgroup=58700005410222818&utm_content=39700049736551245&utm_medium=cpc&utm_source=adwords&utm_term=p49736551245&u

Tend Micro. (2015, January 12). *German Steel Plant Suffers Significant Damage from Targeted Attack*. Retrieved from Trend Micro:

https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/german-steel-plant-suffers-significant-damage-from-targeted-attack

Theron, P. (2014, November). Case Studies for the Cyber-security of Industrial Automation and Control Systems. Ispra, VA, Italy: Joint Research Center.

TREND MICRO. (n.d.). *Industrial Control System*. Retrieved from trendmicro: https://www.trendmicro.com/vinfo/us/security/definition/industrial-control-system

Upadhyay, D., & Sampalli, S. (2019, November 13). SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. *Computers & Security*, 1-18.

Vargas, C., Langfinger, M., & Vogel-Heuser, B. (2017). A tiered security analysis of Industrial Control System Devices. Munich, Germany: IEEE.

Verizon. (2016). Smoke on the Water [plant]. *Data breach digest*, 39-42.

Wilhoit, K. (2013). *The SCADA That Didn't Cry Wolf.* Retrieved from Trend Micro: https://www.trendmicro.fr/media/wp/the-scada-that-didnt-cry-wolf-whitepaper-en.pdf

Wu, W., Kang, R., & Li, Z. (2015). Risk Assessment Method for Cybersecurity of Cyber-Physical Systems Based on Inter-Dependency of Vulnerabilities. Beijing, China: IEEE.

Zetter, K. (2014, October 3). *An Unprecendented Look at Stuxnet, the World's First Digital Weapon*. Retrieved from wired: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

Zetter, K. (2016, March 3). *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*. Retrieved from Wired: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

Appendix A: The four-dimension taxonomy proposed by (Hansman & Hunt, 2005)

The First Dimension	**The second dimension**	**The third dimension**	**The fourth dimension**
Classification in the first dimension consists of two options: If the attack uses a single attack vector, categorize by the vector. Otherwise find the most appropriate category, using the descriptions for each category	The second dimension covers the target(s) of the attack. As an attack may have multiple targets, there may be multiple entries in this dimension.	The third dimension covers the vulnerabilities and exploits that the attack uses.	The fourth-dimension deals with attacks having payloads or effects beyond themselves

Appendix B: Attack Vectors in ICS

Attack Vector	
Virus	“Self-replicating program that propagates through some form of infected files”, (Hansman & Hunt, 2005)
Worms	“self-replicating program that propagates without using infected files; (Usually propagate through network services on computers or through email.)” (Hansman & Hunt, 2005)
Trojans:	“a program made to appear benign that serves some malicious purpose”, (Hansman & Hunt, 2005)
Buffer overflows:	“a process that gains control or crashes another process by overflowing the other process’s buffer”, (Hansman & Hunt, 2005)
Denial of service attacks:	“an attack which prevents legitimate users from accessing or using a host or network”, (Hansman & Hunt, 2005)
Network attacks:	“attacks focused on attacking a network or the users on the network by manipulating network protocols, ranging from the data-link layer to the application layer”, (Hansman & Hunt, 2005)
Physical attacks:	“attacks based on damaging physical components of a network or computer”, (Hansman & Hunt, 2005)

Password attacks:	“attacks aimed at gaining a password”, (Hansman & Hunt, 2005)
Information gathering attacks:	“attacks in which no physical or digital damage is carried out and no subversion occurs, but in which important information is gained by the attacker, possibly to be used in a further attack”, (Hansman & Hunt, 2005)
Malware	Malicious programs scripted by attackers to carry out malicious activities on victims
Phishing	Emails or other forms of communications used to spoof unassuming victims in order to gain access into their networks.
Logic bombs	Malicious programs designed to execute a task after a delay.
Spyware	Malicious software designed to stealthily exfil data from a victim

Appendix C: Vulnerabilities in ICS

Vulnerability	
Vulnerability in implementation	The design of the system is secure, but the implementation fails to meet the design and thus vulnerabilities are introduced. Buffer overflows often exploit such vulnerabilities, for example a program may be designed securely, but its implementation contains bugs that can be exploited. Also zero-day-vulnerabilities and vulnerabilities in hardware would be considered under implementation.
Vulnerability in design	The fundamental design of the system is flawed, so that even a perfect implementation will have vulnerabilities. For example, a system which allows users to choose weak passwords will have a vulnerability in its design.
Vulnerability in configuration	The configuration of the system introduces vulnerabilities. The system itself may be secure but if configured incorrectly, renders itself vulnerable. An example would be installing a secured operating system and then opening a number of vulnerable ports.

Appendix D: Attacker Profiles in ICS

Attacker Profile	
Nation State	These attackers are sophisticated and well-funded. They can be described as to be engaged in cyberwarfare. Their goals are multifaceted. They try to create incidents to disgruntle citizens of a country. They also try to conduct espionage and sabotage against. Propaganda.
Hacktivist	Hacktivists can be motivated many different reasons. Their primary goal is to send a message or take revenge.
Hackers	Hackers are diverse. More specifically known as Blackhat hackers have mal-intentions and are usually financially motivated. They conduct their operations primarily for a monetary gain.
Insider	Disgruntled employees are usually the what fits this category. They use their insider knowledge to intrude in their own company and cause damage or conduct unauthorized activities.