ICSrank: A Security Assessment Framework for Industrial Control Systems (ICS)

Sulaiman Alhasawi

A thesis submitted in partial fulfilment of the requirements of
Liverpool John Moores University
for the degree of Doctor of Philosophy

August 2020

TABLE OF CONTENTS

ACKNOWLEDGEMENT

I would like to start by thanking God for creating me and for giving me endless gifts, knowledge, strength, support and guidance.

I would also like to thank my mom and dad. Thank you for supporting me all my life. You are the best thing in my life.

I would also like to thank my sister Tasneem. She is my spiritual supporter and healer. I would like to thank my sister Dr. Nouf for your academic advice.

I would also like to thank my wife and my kids Fouz, Ahmad and Amina. You are my world and my travel mates during my study in UK. I had a wonderful time with you in UK.

Finally, I would like to thank my supervisor Andy Laws for his support during my PhD research. I would like to thank Tricia and Lina for all the hard work they do, and all the administration help they have given me during my time at Liverpool John Moores University.

ABSTRACT

This thesis joins a lively dialogue in the technological arena on the issue of cybersecurity and specifically, the issue of infrastructure cybersecurity as related to Industrial Control Systems. Infrastructure cybersecurity is concerned with issues on the security of the critical infrastructure that have significant value to the physical infrastructure of a country, and infrastructure that is heavily reliant on IT and the security of such technology. It is an undeniable fact that key infrastructure such as the electricity grid, gas, air and rail transport control, and even water and sewerage services rely heavily on technology. Threats to such infrastructure have never been as serious as they are today. The most sensitive of them is the reliance on infrastructure that requires cybersecurity in the energy sector.

The call to smart technology and automation is happening nowadays. The Internet is witnessing an increase number of connected industrial control system (ICS). Many of which don't follow security guidelines. Privacy and sensitive data are also an issue. Sensitive leaked information is being manipulated by adversaries to accomplish certain agendas.

Open Source intelligence (OSINT) is adopted by defenders to improve protection and safeguard data.

This research presented in thesis, proposes "ICSrank" a novel security risk assessment for ICS devices based on OSINT.

ICSrank ranks the risk level of online and offline ICS devices. This framework categorizes, assesses and ranks OSINT data using ICSrank framework. ICSrank provides an additional layer of defence and mitigation in ICS security, by identification of risky OSINT and devices. Security best practices always begin with identification of risk as a first step prior to security implementation.

Risk is evaluated using mathematical algorithms to assess the OSINT data. The subsequent results achieved during the assessment and ranking process were informative and realistic. ICSrank framework proved that security and risk levels were more accurate and informative than traditional existing methods.

GLOSSARY

ICS:

The term Industrial Control Systems is used to describe different types of control systems and associated industrial instruments, including devices, systems, networks used to operate and/or automate industrial processes. ICS are built to function electronically and manage tasks depending on industries' different needs. Today ICS protocols are used in nearly every industrial sector and critical infrastructures such as the manufacturing, transportation, energy, and water treatment industries [176].

IoT:

The internet of things, commonly abbreviated as IoT, refers to the connection of computing, digital and mechanical devices in a system providing a unique identifier to each device and the ability to transfer data over a network without human intervention [177].

OSINT:

This acronym stands for Open Source Intelligence that is the insight gained from analysing and processing the publicly available media data sources like television, newspaper, radio, social media, and websites. These sources provide data in all its forms to be assessed and used by organizations. [178]

SCADA:

is an acronym that refers to Supervisory Control and Data Acquisition. SCADA is a computer system that monitors industrial processes. The main task for this system is to monitor industrial electrical assets scattered over large geographic areas [179].

SSL:

this is an acronym for Secure Sockets Layer. It is a standard protocol used to secure documents transmitted over the network. A secure link is created between the browser and the webserver for private data transmission [181].

TSL:

this is an acronym for Transport Security Layer. The protocol ensures a secure communication link between server and client communicating over the internet. It protects the data and ensures its integrity

and privacy between the internet nodes [182].

SQLi:

This is an acronym for SQL injection. This is a type of malicious computer attack that is embedded in software that is poorly designed then transferred to the backend databases. It then produces queries that should not be executed [183].

XSS:

This is an acronym for Cross-Site Scripting. It is a process where malicious code is added to a genuine website with the intention of gathering information from users. The attacks are also possible through vulnerabilities posed by web applications; they are commonly injected from the client-side [184].

CSRF:

Cross-Site Request Forgery (CSRF) is an exploitation of the website from a trusted user. It is done by issuing unauthorized commands from the user's browser to the trust of the website [188].

TCP:

Transmission Control Protocol (TCP) is a network communication protocol designed to send data packets over the network. The protocol connects remote computers, then transmits and ensures that the messages are delivered [187].

SMTP:

Simple Mail Transfer Protocol (SMTP) is the standard email transfer protocol on a TCP/IP network. It facilitates sending and receiving of email messages over the internet [186].

UDP:

User Datagram Protocol (UDP) is a protocol used to send short messages called datagrams for programs that run on various computers on a network [185].

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1.1 FOREWORD

Industrial Control Systems (ICS) are critical infrastructures for many organizations and countries. ICS are responsible for operating and maintaining industrial factories that produce assets such as gas, nuclear power, and water. The security of these systems is critical since their continuous operation is crucial to the well-being of industries and countries. Energy security has always been a high priority worldwide since attacks on ICS security systems (or their lack of security) can result in disastrous implications, both in terms of physical and financial damage.

In this chapter, ICS security methods are introduced, and security controls are discussed. This thesis also discusses research motivation and presents novel contributions to the field. Finally, the aims, objectives, methodology, and thesis layout are put forward.

1.2 CRITICAL INFRASTRUCTURE SYSTEMS

Critical Infrastructure Systems have grown to be one of the vital aspects of the operation of systems since they ensure security and reliability in operation. They are the key assets and systems (virtual or physical) of such importance to countries that their destruction or incapacity poses serious threats to security, the national public health and safety, the national economy or a sum of all of these issues. Therefore, systems are monitored and controlled to avoid disrupting

normal operations due to attacks, natural disasters or component faults. Such monitoring and control ensure continued operation after failure [189].

Supervisory Control and Data Acquisition (SCADA) systems are heavily used in important national infrastructures such as oil, gas and energy production, to name but a few. The main role of a SCADA system is to organize and control traffic data to manage infrastructure operations. A SCADA system is mainly composed of Master Terminal Units (MTUs) (sometimes called the Human Machine Interface (HMI)) which read and control data coming from field devices like Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs) and Intelligent Electronic Commands (IEDs). RTUs, PLCs and IEDs obtain readings (data) from meters, sensors and valves.

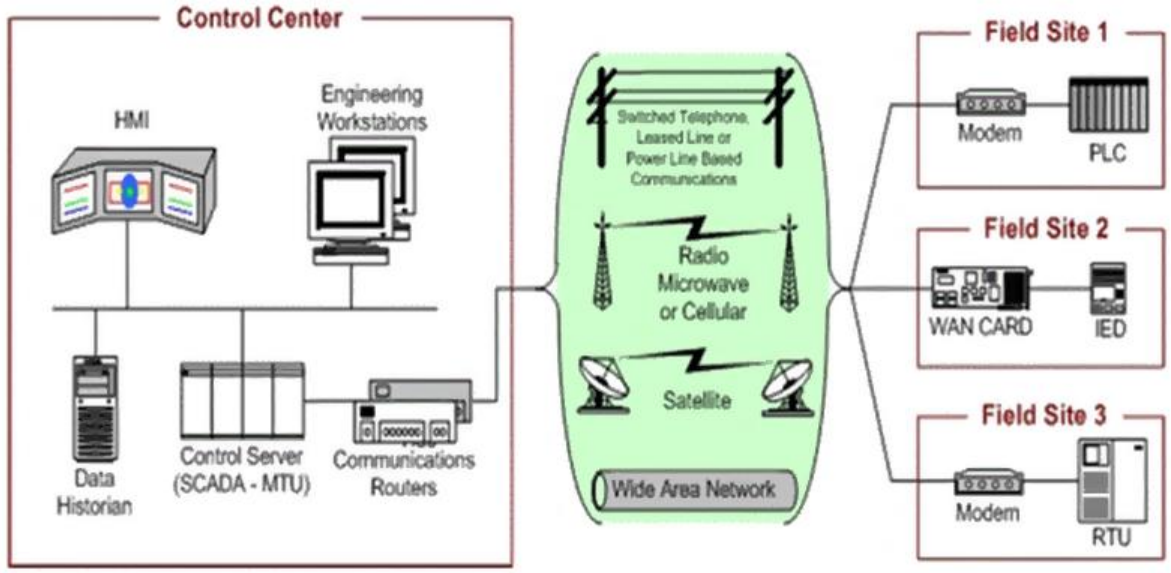


Figure 1:SCADA layout [1]

SCADA components such as MTUs and RTUs communicate through channels and protocols such as DNP3 [2], International Electro-technical Commission (IEC60870-6) (sometimes called Inter-Control Centre Communications Protocol (ICCP) or TASE.2[3], Modbus [4], Tristation (source)and Profinet IO [5] to name only some of the estimated 150-200 protocols identified by the American Gas Association[6]. SCADA protocols organize the interaction of SCADA components by issuing built-in functions designed specifically for each protocol. Most SCADA protocols were designed by proprietary vendors and are therefore considered closed-

source products (which are difficult to study). Nevertheless, there are some widely used, open-source protocols like Modbus and DNP3 that can be used to demonstrate SCADA protocol interactions (see Figure 2). Open-source software is a type of application, in which the source code is freely available to the public and hence modifiable; contrasting with a closed-source product where no source code is available. Open-source software benefits from mass cooperation by the open-source community, which enables the constant revision and improvement of code. This has a significant advantage over proprietary (closed) software as security and design errors could be fixed and improved faster (although clearly, open-source fixes are publicly visible). However, open-source protocols such as Modbus and DNP3 remain insecure and require a lot of improvement. Proprietary protocols such as Tristation also require security hardening In this thesis, the key focus is on the Tristation protocol security in chapter 6.

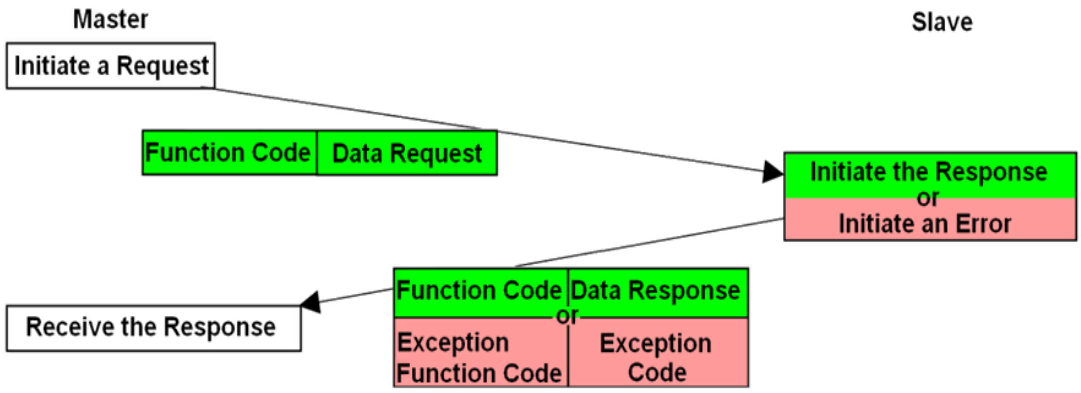


Figure 2: SCADA interactions using Modbus [7]

SCADA protocols and systems were designed to be closed systems in private networks. After the emergence of open protocols and networks such as TCP/IP and the Internet, SCADA systems were interconnected with open protocols and commercial off-the-shelf (COTS) software/hardware, thus becoming exposed to a variety of cyber risks and attacks. SCADA systems are especially vulnerable to cyber-attacks because security was not considered as an integral part of the original design of SCADA systems or open protocols and COTS systems. SCADA systems were designed principally for functionality purposes such as performance, reliability and availability.

1.2.1 ICS Security Issues

There have been many cyber-attacks on SCADA networks (Table 1). An example is the Australian sewage incident in Queensland's Maroochy district in the year 2000, during which an intruder had access to a weak SCADA network and released tons of sewage into the city [8]. The intruder was an employee for a company that installed the SCADA system for the council. He had applied for a job in the council but was rejected. Seeking revenge, he used his ex-employer's software installed on his laptop and issued radio commands near the council sewage system, which eventually caused the disastrous event. Another example that demonstrates the real risk and consequences of neglecting SCADA security is the Slammer worm that crashed a nuclear plant network in Ohio in 2003[9]. The source of the attack was an insider who accidentally installed unpatched Microsoft SQL on his laptop, which subsequently allowed his laptop to be infected by the worm. The worm spread the instant he was connected to the company's network reaching both corporate and control networks. Production was not affected. However, the company lost some historical data stored on its server.

Miller and Rowe [10] have listed 15 SCADA and control system incidents such as the Siberian Pipeline Explosion in 1982, caused by a Trojan implanted in the network. Another large Trojan incident was the 2010 Stuxnet attack against Iranian nuclear plants which aimed to disrupt and distort regular operations. The malware infected the control network through an employee's computer. The Stuxnet attack allowed a man-in-the-middle (MITM) attack to take place between the network's PLC controllers. MITM is an eavesdropping attack that an attacker can monitor or modify communication between two nodes [190]. However, the exact target was not revealed by the Iranian authority and is still unknown. The alleged objective was to intercept packets and change them [11]. Miller and Rowe classified the main methods of attacks that targeted ICS systems during a 20-year period (1982 – 2012) as the following:

- Misuse of operation [Explored in this thesis]
- User compromise.
- Compromise of root or administrator credentials. [Explored in this thesis]
- Trojan: [Explored in this thesis].
- Denial of service.

- Virus.
- Social engineering

Two of the above attacks are explained in depth in chapter 6. Misuse of operation is demonstrated in case study 1, 2 and 3. Case studies are built on the concept of system manipulation. Trojan attack is also the core study in chapter 6, where Trisis malware is examined Chapter 4 identifies the credential attack as part of OSINT collection process.

Their work has also explained the impact of SCADA attacks on targeted control systems and has provided a classification of targeted sectors into three types: government, commercial or international.

Table 1: Top 10 most critical SCADA vulnerabilities [12]

Vulnerability	SCADA Impact
Unpatched Published Vulnerabilities	Most Likely Access Vector
Web Human-machine Interface (HMI) Vulnerabilities	Supervisory Control Access
Use of Vulnerable Remote Display Protocols	Supervisory Control Access
Improper Access Control (Authorization)	Access to SCADA Functionality
Improper Authentication	Access to SCADA Applications
Buffer Overflows in SCADA Services	SCADA Host Access
SQL Injection	Data Historian Access
SCADA Data and Command Message Manipulation and Injection	Supervisory Control Access
Unprotected Transport of SCADA Application Credentials	SCADA Credentials Gathering
Use of Standard IT Protocols with Clear-text Authentication	SCADA Credentials Gathering

Because of these safety risks, the demand to protect digital and physical assets under SCADA control from cyber-attacks is escalating. It is becoming a priority for most countries and organizations to act towards understanding and protecting SCADA systems to mitigate or prevent risks. One crucial step towards securing SCADA systems is to understand the vulnerabilities and subsequent cyber-attacks that target SCADA protocol vulnerabilities[1].

1.2.2 ICS Protocols

1.2.2.1 MODBUS PROTOCOL

Modbus is an old protocol, designed and developed by Modicon Industrial Automation Systems (currently Schneider Electric) in 1979. It is the standard amongst other protocols in Industrial Control Systems (ICS). It is the oldest and most widely used industrial protocol by automation systems around the world and as such, it is of primary concern in ICS research (especially ICS cybersecurity) [24].

The Modbus protocol is vulnerable by design and lacks critical security features such as authentication, availability, confidentiality, integrity and non-repudiation. Authentication is neglected in the design of ICS protocols: no passwords are required to control access to stations, substations and sensors. However, in DNP3 there is a feature that allows the "masters" to identify themselves by issuing a "SELECT" command.

There are security features that must be available for every secure protocol:

- Availability is a vital and critical feature in industrial control systems and thus means that processes must be available in real-time and functioning continuously as required by the nature of these industries.
- Confidentiality is enhanced by ensuring that encryption is available to protect data flows in networks instead of a clear text format, thus preventing data sniffing.
- The integrity of data and processes remains unchanged in their original form without any alteration or manipulation.
- Finally, non-repudiation is a protection mechanism that aims at preventing attackers from manipulating packets between masters and slaves.

ICS protocols such as Modbus were designed for functionality and networking purposes such as performance, reliability and availability. These functionality features are important for industrial systems. However, they are not enough for the protocol to survive in the cyber age. Therefore, the demand to protect ICS systems from cyber-attacks and hence protect digital and physical assets is escalating. As such, it is becoming a priority for most countries and organizations nowadays to take action towards understanding and hardening ICS systems to mitigate or prevent risks. Securing ICS protocols is an important step to secure ICS's internal and external communications.

There has been a considerable amount of work done on Modbus security [15] – [31]. Huitsing has laid out a Modbus attack taxonomy [24], which extended the work done by DigitalBond[25] by identifying more attacks. However, his work (by his own admission) is incomplete as not all attacks that target Modbus are covered.

Fovino and Masera also contributed work towards Modbus security by increasing the number of analysed attacks [27], compared to the aforementioned study. For example, malware attacks on Modbus were tested experimentally [27]. In the report, 11 attacks against Modbus were identified [28]. Further work by these authors discussed developing Intrusion Detection Systems (IDS) that can detect malicious Modbus packets [29]. A platform was also developed for assessing SCADA vulnerabilities [26]. They also described a secure version of Modbus [31]. However, their secure Modbus was only a prototype and was only tested for performance and functionality (it was not tested for security issues). They admitted that the work did not demonstrate attack scenarios, which is essential for evaluating the effectiveness of a secure version. Furthermore, they have mentioned that their proposed protocol cannot protect the system if an intruder gains control over the master device (e.g. RTU or PLC). Our research considers this issue.

1.2.2.2 DNP3 PROTOCOL

DNP3 is a bidirectional protocol that allows devices to act as either master or slave (allowing the ability to change roles). DNP3 is very popular in SCADA networks [33]. With the advent of the internet, DNP3 was developed to support TCP connectivity to be able to connect with outstations at a distance. The complexity of DNP3 architecture introduces many vulnerabilities

[32] alongside a lack of main security features such as authentication and confidentiality, thus making DNP3 an insecure medium inside SCADA network.

East et.al. developed an attack taxonomy related to the DNP3 protocol [33], their work is similar to Huitsing's work on Modbus [24]. However, similar gaps to those of Huitsing's work such as missing attacks still exist. Both works are theoretical developments and thus remain untested. Some authors have focused on examining basic security features such as access control by demonstrating how the design of DNP3 is weak when protecting devices in the network [34]. The authors proposed a solution that protects those devices if a master device becomes compromised or when intruders by-pass other security solutions.

1.2.2.3 PROFIBUS I/O PROTOCOL

Profibus IO or Profinet I/O is one of the most commonly used protocols in SCADA systems. Along with most SCADA protocols, Profibus I/O lacks basic security characteristics. It also presents weak access control features that allow for breaches by the initialization of illegal packets [32]. An attacker can manipulate packets by changing the data or instructions that each packet contains.

Akerberg and Bjorkman demonstrated that physical nodes connected by Profinet I/O are vulnerable to attack without detection [35]. They have proposed a solution based on the concept of modules. The module is built on top of Profinet I/O protocol and thus provides basic security features such as integrity and confidentiality. They argue that the concept of modules is practical because it does not affect the transmissions inside the protocol. However, their proposal is still theoretical and has not been evaluated. In another work, Baud and Felser demonstrated a man-in-the-middle attack by emulating SCADA devices using Profinet I/O protocol as a medium [36]. The concept of emulation is adopted in our work. They proposed a guideline on how to develop emulated devices for security testing. For example, they show how to implement the behaviour of a PLC and demonstrate its vulnerability when targeted by a man-in-the-middle attack. This type of attack attempts to sniff or spy on communication channels.

1.2.3 IoT and the new generation of Industrial devices

Contemporary industrial control systems can now be integrated with smart devices such as sensors, meters, mobile phones and networks. This integration is called the Industrial Internet-of-Things (iIoT), a Web of Things (WOT), Industry 4.0 or Internet-of-devices [37]. ICS devices are becoming more exposed to the internet than ever before. It is estimated that the number of iIoT devices will reach 50 billion by 2020 [38]. This growth is explained by the need for smarter and faster automation. The trade-off is a larger exposure to internet attacks. This is the trade-off when performance is prioritized. It is common for ICS systems to choose performance (availability) characteristics over security. This puts iIoT devices in jeopardy.

Traditional ICS devices such as SCADA, PLC and HMI are the backbone of critical infrastructures. There is a need in this work to understand how these devices were designed and how they operate. This research also needs to understand the sequence of security feature priority for industrial devices. These devices are by no means like other traditional devices. Each device is composed of one or more software packages, they normally contain a firmware, application and a network protocol embedded in them. In brief, the more software used, the larger the chance for a vulnerability to exist. IIoT devices suffer from multiple weaknesses such as lack of physical protection, which leads to a physical attack. They are connected wirelessly which enables eavesdropping and makes it difficult to implement security solutions and other major security features such as authentication, data integrity [39], privacy, identity management, trust and resilience [40]. OWASP [41] has identified 10 major bugs for iIoT, which are analysed thoroughly in chapter two. Not all iIoT devices have the same level of security. The above factors contribute to the overall risk level. In chapter four an analysis of each device is demonstrated by considering every factor that affects its security.

It is a general fact that cyber risk has been a recurring issue with ICS devices since the day they were introduced to the internet. What made matters worse is that public search engines have managed to identify, locate and archive those devices. Everyone, especially attackers, has eas

y access to the wealth of information that search engines provide. In chapters three and four, this thesis shows the types of information that search engines can reveal. Also, an explanation of how to use that information to assess ICS devices is included. Such information can sometimes be critical.

Search engines are only a part of the general problem. There are other threats apart from attackers that can contribute to the insecurity of ICS devices. Free and public information and data about these devices are labelled as Open Source Intelligence (OSINT) [42]. Search engines are one source of OSINT. In chapter three, an outline of OSINT and its tools is presented in more depth. Attackers use this data to learn about a target and to spot weaknesses and thus prepare before attacking a target device. Therefore, knowing how attackers think is vital. Knowledge of critical information that an attacker can use is a major step to stop a threat and minimize risks. Our research takes this approach and proposes a framework that focuses on the security assessment of ICS devices using available information from OSINT resources (see below section 1.3).

According to project Shodan Intelligence Extraction "Shine" [43], there were 1,000,000 ICS devices connected to the internet in 2014 [44]. Today, there are probably many more devices. ICS devices could be part of a network that belongs to many industries, such as oil, gas, electricity, water, nuclear, etc. This could indicate the possibility that these ICS devices are connected to real physical systems. In our research, it is assumed that the targeted physical system is a gas industry. Questions such as How to get access to that device and even to the gas network? What would be the impact and cascading effects? are discussed. This thesis adopts ethical rules (See Chapter 4) throughout research, which prevents access to ICS devices; this inspired the author to build a gas cylinder model. The model allows to experiment with various scenarios. The methodology in this research links cyber threats (that were collected using this research's framework) with the gas model. To the best of author knowledge, this linkage is a new topic in this area. The relationship (cyber-physical) between iIoT security and a physical system is a new research area (see section 1.3 below).

1.3 MOTIVATION

Industrial control devices such as SCADA, PLC and RTU are heavily used in critical national infrastructures such as oil, gas and energy production, transmission and distribution, to name a few. ICS were designed to be closed systems in private networks. After the emergence of open protocols and networks such as TCP/IP and the Internet, ICS devices were interconnected with open protocols and commercial off-the-shelf (COTS) software/hardware, thus exposing them to a variety of cyber risks and attacks. ICS devices are specifically vulnerable to cyber-attacks because security was not considered as part of the design of ICS or open protocols and COTS

systems. ICS were designed principally for functionality purposes such as performance, reliability and availability.

There have been many cyber-attacks on ICS networks, a few will be listed. Some attacks originated from disgruntled insiders such as The Australian sewage incident in Queensland's Maroochy district in 2000 that was discussed earlier. Another example that demonstrates the real risk and consequences of neglecting ICS security is the Slammer worm that crashed a nuclear plant network in Ohio in 2003[9]. The attack source was from an insider who accidentally installed unpatched Microsoft SQL on his laptop that eventually became infected by the worm. The worm spread the moment the laptop was connected to the company's network, reaching both corporate and control networks. Production was not affected; however, the company lost some history data inside its server.

Miller and Rowe [10] listed 15 industrial control systems incidents, such as the Siberian Pipeline Explosion in 1982, caused by a Trojan implanted in the network. Another Trojan (the same as in the previous source) attack was the Stuxnet attack in 2010 against the Iranian nuclear plants to disrupt and distort normal operations. The malware infected the control network through an employee's computer. The impact of the Stuxnet attack was to allow a man-in-the-middle attack to take place between the network's PLC controllers. However, the exact target was not revealed by the Iranian authorities and is still unknown. The goal apparently was to intercept packets and change them [11].

1.3.1 The Growing ICS exposure

There has been a rapid growth in the number of ICS devices that need to be connected to the internet in order to be functional. This is especially true in the era of industry 4.0 and the emergence of the iIoT. A typical iIoT system is composed of ICS devices along with a cloud service and business applications [45]. Businesses are using IoT technology to help improve their day to day operations, cut costs, as well as to monitor, maintain and protect assets such as PLCs in real-time. Attack surfaces to ICS devices are increasing every day. Attack surfaces are different entry points of a system (e.g. device) which an attacker can use to get access or obtain data [191].

The wealth of sensitive information about those devices, their organizations and staff that is publicly available on the internet is threatening. OSINT sources that are available to the public and the dark web have made matters worse. With a click of the mouse, one can find a target ICS device exposed online with an accompanying information pack about it. Specialized search engines such as Shodan, Zmap and Censys are hunting and classifying ICS devices for use by security researchers and practitioners. However, there is a misuse of these services by notorious threat actors. They contribute generously to the leakage of private information about ICS victims such as credentials, a method of attack and device network details. There is a loud call for action to help reduce this exposure and minimize attack surface for ICS devices and IoT systems.

1.3.2 OSINT threats

Nowadays, smart technologies such as IoT have been strongly linked to ICS. IoT technologies have contributed to the improvement of automation, performance and production of ICS. The integration of ICS and IoT has resulted in the birth of new systems of ICS. These systems are indeed smarter. However, IoT design and security suffer from many weaknesses. Issues such as weak web interface, lack of privacy and leakage of sensitive information are too risky for industrial entities to ignore. The impact is severe and costly. To show an example in the energy field, BlackEnergy [46] (a Trojan) hit many energy companies in Ukraine in 2014. The Trojan, implanted in a Microsoft Office document, was specifically made for SCADA systems and was spread by a simple spear-phishing email. Spear-phishing email is an email sent to a targeted group of people from trusted sources that are familiar and related to those groups [192]. Social engineering was part of this attack because the document asked the receiver to carry out certain steps. Based on some Black Energy analysis, it was revealed that this malware was using a common practice when it comes to hosting an infected domain [47]. The free availability of information has made OSINT a powerful toolkit for both white and black hats. Many entities are attacked often because they were not aware of these threats. This lack of awareness about system threats is dangerous. Social media has, in turn, accelerated the growth of OSINT sources. One needs to have skills and tools to collect and filter OSINT information and convert it into useful intelligence. Most importantly, many entities do not know how to use this intelligence in the assessment of ICS devices. To minimize threats coming from OSINT, one needs to trace the source of leakage of information and remove its trails. Doing that requires

studying ICS device security in depth. In addition, there is also a need to develop techniques for collection and analysis of OSINT information regarding those devices.

1.3.3 Motivation Summary

This research is motivated by the real risk associated with ICS devices. The threats, combined with OSINT data, are alarming. Our research focuses on digital risks and their impact on physical systems such as gas pipelines.

The rising exposure of ICS devices on the internet brings many challenges to practitioners and academics. The mixture of IT and OT products has its benefits. However, the trade-off between benefits and security is steep. The leakage of digital data from ICS devices has recently accelerated the rate of cyber-attacks. This was due to the growth of social media services that made sharing information easy and increased the availability of tools that store ICS data such as search engines and databases.

1.4 AIMS AND OBJECTIVES

The following is a list of our aims:

- The identification of critical data of ICS devices using OSINT sources: To use available public OSINT that is related to ICS devices. This includes collection, categorization and identification of OSINT data, that can affect the security of online and offline ICS devices
- The analysis of OSINT data and its impact on ICS devices: Analysis of OSINT data categories based on this research framework. Furthermore, security assessment of this data to determine its security and relevance.
- Ranking the risk level of ICS devices using ranking algorithms: Application of these algorithm on collected and assessed OSINT data to determine its risk value and level.

Research Objectives

- Research into ICS vulnerability and risk assessment, methodologies and metrics.

- Investigating the impact of cyber threats on ICS devices
- Research into related work about ICS security in general.
- Research into IoT security.
- Research into OSINT techniques.
- Research into related work about industrial device security.
- Evaluation of current methodologies in risk analysis of ICS devices.
- Application of ICSrank framework on 3 case studies:
    - Case 1: Analysis of Triconex PLC using OSINT sources
    - Case 2: Analysis of Trisis malware using network data
    - Case 3: Analysis of research tools using “Gas cylinder filling “model
- Interviewing engineers from a gas company and development of “Gas cylinder filling “simulation model
- Evaluation of results.
- Proposal for mitigation and defence techniques
- Publication of research results.

1.5 APPROACH

Our aim is to develop a framework/methodology to assess ICS device security based on OSINT and to investigate the risk level of related OSINT information. To achieve this, the following is done:

- Collect OSINT sources that offer data about ICS devices.
- Collect filters and keywords that tell us about ICS devices, such as technology details including vendor and device name, type, version, etc.
- Prepare search engine operators that use our filters to scan and find devices.
- Gather all OSINT information and categorize it based on source and type.
- Develop a gas cylinder filling simulation to conduct case studies.

- Analyse and assess OSINT categories.
- Rank and evaluate OSINT categories using ICSrank algorithms.
- Rank ICS devices using ICSrank algorithms

Leverett [48] has investigated the presence of ICS devices on the internet. His goal was to debunk the myth that ICS devices are not connected to the internet. He has demonstrated techniques that help in assessing and visualizing ICS devices. However, his risk assessment technique depended on popular vulnerability databases. Current vulnerability databases use CVSS metric system to rank vulnerabilities. This thesis argues that CVSS has many weakness and inaccuracies [49][50], especially when it comes to ICS and IoT devices. It is important to consider other threats such as critical device information available in OSINT sources. In this research, a demonstration that OSINT can contribute to the cyber defence research for ICS devices and for ICS security in general is carried out.

1.6 NOVEL CONTRIBUTIONS

- Development of ICSrank a comprehensive security assessment framework- for industrial control systems based on OSINT. It's a qualitative quantitative metric. ICSrank is applied to internet-connected ICS devices and non-connected ICS devices. ICSRank consists of 3 stages OSITN data collection, assessment and ranking.
- Development of ranking algorithms that evaluates the risk level of ICS devices. The algorithms evaluate ICS devices using developed novel techniques that is based on OSINT categorization and assessment. The categorization and assessment of OSINT data that is based on type and security is unique.
- The application of ICSrank framework on different types of OSINT is novel too. A demonstration of how to apply ICSrank on online devices and offline devices is explained. Online devices are those that are discovered in the Internet and tend to have higher surface attack vulnerabilities than offline devices and normally require lower skills level to be exploited. Offline devices require higher skills and more OSINT knowledge. This research digs deeper to look at existing OSINT information especially for offline ICS devices. There are 3 perspectives when it comes to analyse OSINT data that are applicable to offline devices specially and online devices as well. This way of looking at OSINT data is a novel contribution. The types that are

presented in this research are as follows: comprehensive view of OSINT data, partial view and research concepts. The comprehensive and partial OSINT are device specific information. It means that information was built for existing devices. The research OSINT are information that were developed to provide design and conceptual applications and were not targeting real devices. This technique of OSINT analysis is a novel way to view vulnerabilities in the area of ICS security.

1.7 THESIS LAYOUT

The research in this thesis is divided into 8 chapters. A description for each of the chapters is provided in this segment.

CHAPTER 1

This chapter consists of a brief introduction, a description of the research motivation, aims and approach.

CHAPTER 2

Chapter 2 stands as a literature review. This is mainly a discussion of ICS devices' security. The second chapter discusses the vulnerabilities of and threats to ICS devices. This thesis mentions previous research that outlines threats and attacks that target ICS devices. It also provides a brief taxonomy of specific ICS targeted attacks as blueprinted in past studies. Related research topics such as ICS device metrics and assessments are scrutinized and explored in depth.

CHAPTER 3

The third chapter provides a comprehensive analysis of existed techniques of ICS/IoT vulnerability testing and evaluation. The goal in chapter 3 is to develop a ground for OSINT categories that would be used for the later chapters.

CHAPTER 4

In this chapter, a lay out of this thesis framework and methodology is discussed in depth. This thesis discusses how to use OSINT tools in vulnerability and risk assessments, how to categorize information gathered from OSINT, how to assess and quantify the risk level for collected information, and to demonstrate how to rank risk ICS devices based on ICSrank algorithms. This chapter also introduces a case study that serves as a proof of concept.

CHAPTER 5

In this chapter, a development of a novel ICS attacks taxonomy based on safety PLC in gas systems is presented. This thesis discusses the security of cyber-physical systems by linking the framework presented in chapter 4 with the gas cylinder model. This thesis demonstrates a threat model of how to attack an online ICS device

CHAPTER 6

The sixth chapter demonstrates an application of ICSrank on 3 ICS case studies that are related to Triconex PLC, Trisis malware and the gas cylinder model respectively. Chapter 6 provides A description of the gas cylinder model used in this research. This chapter explains how to apply ICSrsnk on 3 case studies that are classified as different types of OSINT. The application process includes all the steps that ICSrank framework follows.

CHAPTER 7

Chapter 7 is the academic conclusion to this thesis, and it serves as a conclusory section to all of the above. General conclusion and future work are put forward.

1.8 SUMMARY

Today, ICS devices are more exposed online than ever before. ICS devices and protocols suffer critical security flaws. To make matters worse, the devices are exposed online in new trendy technologies such as IoT, iIoT and industry 4.0. Unfortunately, Industry 4.0 and IoT are still using the same security features as the old ICS. Information sharing and OSINT is enormous nowadays. Academics, security analysts and criminals use industrial OSINT too. It made security, attack techniques, and exploits harder for asset owners to identify and to keep up with.

Motivated by those issues, this research took on the mission to research new ICS security ways and concepts that can contribute to the ICS community. This thesis argues that in order to secure ICS, it is important to study the security of ICS from a new perspective. This research considers new metrics to assess ICS security and takes careful consideration of OSINT. To sum up, this chapter is this research map and guide that lays out the aims, research approach and ideas. In the next chapter, it examines the core literature of ICS and IoT security in more depth.

CHAPTER 2

LITERATUR REVIEW I

2.1 ICS AND IIOT DEVICE SECURITY

2.1.1 Introduction

In this chapter, the literature review of general vulnerabilities that are inherent to ICS and IOT as well as their role in some well-known attacks are discussed. Indeed, both ICS and IOT share common characteristics, and these characteristics lead to possible exploitation. Many industrial systems have their own bugs and limitations; however, with new technology and the expansion of IoT devices, many ICS devices were converted and integrated with the web and smart devices (IOT), functionally making them iIoT themselves (see introduction). Thus, even these upgraded devices still have certain issues. This chapter will discuss these issues in light of how they have resulted in attacks in the past.

To appropriately assess the risk level of an iIoT device, a need to build an understanding of these devices and what they do (see Chapter 3 for a list of common ICS devices). For the present discussion, it is important to know the design and security features of ICS and IoT devices generally. Given the breadth of previous research that has discussed these devices and their inherent security shortcomings, here this research presents a brief list of the commonest and severest security issues of ICS and iIoT devices. Thus, the aim of this chapter is to present these issues and how they have resulted in previous attacks so that the general level of risk of a device can be better understood and assessed.

2.1.2 Common ICS Security Problems and Issues:

ICS systems, such as those commonly used in gas and oil systems, have many vulnerabilities. In Chapter 6, possible countermeasures and solutions that affect ICS security are discussed and proposed [51] [52]:

A major reason that ICS security is fragile is human ignorance. Most people who work in the industry and are most likely to use these devices lack security awareness. For example, the core focus of many industrial organizations is production and safety. However, cybersecurity is generally not presented as important and is almost certainly not a priority for the individuals most likely to interact with the ICS devices regularly. Unfortunately, this is a risky approach because the ICS devices are directly related to the core intentions of production and safety. The risk is too high to ignore these technological security issues. Indeed, managers and the individuals who are most likely to use the ICS devices need to be informed about these looming issues. Knowledge and awareness about how to secure ICS and cyber threats should be addressed for all members of an organization, not just for the individuals at higher levels of management [1]. Indeed, these individuals should know the limitations of ICS, the appropriate default configurations, and the risk of online exposure prior to having direct access to these devices. Active preparation is always more effective and will keep production and safety at the forefront of an organization's mission.

The second issue that many industrial companies face is remote working. Either a contractor or direct employees working remotely either on a temporary or a permanent basis could do this. A contractor might need to access ICS for regular maintenance or for specific patching of issues that arise. In this process of regular remote access, malicious threats (e.g. malware) might be brought inside the ICS network if the employee's computer is infected or their network is not secure from eavesdropping. An insider or direct employee, on the other hand, might experience the same issues as a contractor, but with far more severe consequences because normally insiders can access more critical locations within the network than a contractor. So, the same malicious threats can be presented to the organization's network and because of the deeper access allowed to the insider, have a far greater effect over time.

The third issue is using open source IT products or those made by 3rd parties. There are two specific issues with these products. Many IT products are not patched immediately following

a known issue and many have vulnerabilities that are incapable of being patched. The other issue is with open-source software. If the open-source product does not come with a large and active community, then it would be risky as it is highly unlikely that the software is regularly inspected for bugs or that known issues are patched competently or quickly. Another issue with open source software is the availability of source code. Having open-source code is often advantageous because it allows you to inspect it, fix it and improve it for your specific application over time. However, some attackers study such open-source code in order to write exploits that were not previously discovered by that software's community.

The fourth reason is the lack of security culture between partners. Partners should agree on security practices, and they should exchange information with each other regarding their products. They should cooperate to share known vulnerability disclosures, patching and security hardening. For example, if a vendor sells products to an industrial company, the vendor must inform the company about default configurations and credentials so that they can be changed and not let customers discover them after what would likely be a devastating attack.

The fifth reason is that data networks are not well separated. There are normally two networks in most companies: information technology and operational technology. There is a business network, sometimes called the information technology (IT) network. That network is where business tasks take place. The IT network is connected directly to the internet. The other network is called the operation technology (OT) network. This network is where industrial processes and production occurs, and which is supposed to be isolated from the IT network and the internet. This isolation is intended to protect the OT network, and thus by proxy the IT network, from malicious packets and cyber threats. Unfortunately, most companies do not follow these standard security practices, and thus have problems separating their information architectures.

The six and seventh reasons are the use of mobile devices and cloud storage. Specifically, it involves the data sharing between on and offshore or off-site facilities. In modern technologies, there is an increasing dependence on cloud services and cloud storage. This technology is advantageous because of the cheap cost of storage and the relative convenience of maintenance, updates, etc. However, when an ICS company saves data in a third-party location, then this can be a significant disadvantage. Cloud services suffer from many security issues such as loss of

device control, data integrity and encryption issues for both communication and files [193]. Together, these risks are simply too great for any ICS company to sustain.

The eighth reason is that many ICS devices suffer from weak physical security. Access to insecure physical hardware allows an intruder to insert removable media, such as flash drive, to the actual devices. This mobile media could be used to extract and steal data or to load malware or other malicious software onto the physical systems. In addition, although rare, an intruder could also damage the devices physically and thus render them inoperable.

The ninth reason is that many ICS companies use old and outdated systems. Many of those systems use software and hardware that is no longer patched or maintained by the original producer. These systems generally have limited computer resources and specifications. Thus, even if a company is still releasing patches when appropriate, these systems cannot handle the released patches without experiencing a performance decrease, which would then decrease the productivity of the overall system. It is a current fact that many industrial organizations prefer availability over security and choose productivity over adaptation [1].

Other reasons, such as the availability of a web interface for ICS devices, and relatively weak security support also affect ICS devices. Many ICS devices ship with a default web access. Unfortunately, many of these web interfaces contain many security flaws such as default configurations and credentials (see Chapter Four), lack of network encryption, and general susceptibility to other cyber-attacks.

2.2.2.1 CAUSES OF VULNERABILITIES:

According to [2], the main causes of these vulnerabilities in ICS devices are due to isolation. ICS devices are typically built and designed for the purpose of isolation. Typically, An ICS network is isolated from a business network or has little connectivity to it [1]. Security is not generally considered in the design process because the designers assume that the system will exist separately from any other systems. Indeed, the main concerns of the designers are safety and availability during production. However, when the connection to the internet became prominent, problems started to arise in these systems as the internet reduced the ability for isolation [1]. There is nothing necessarily wrong with connecting to the internet, but when the

default configuration and security mechanisms are weak, ICS devices are likely to be exposed to serious risks.

Another factor is the heterogeneity. Many ICS devices are really a mixture of different components; Commercial-of-the-shelf (COTS), third party and proprietary software. This could lead to serious issues as many COTS have bugs and their vulnerabilities to exploitation are available publicly on the internet. Individuals seeking to patch the issue typically describe these exploitations, but other communities also post the exploitations for nefarious reasons. The other issue is the mixing of different systems because these systems were not designed to work together securely. This could lead to leaks and the absence of any security mechanisms in software design, such as security and privacy configuration. The mixture of systems must work as one unit in order to be resistant to common threats. However, many systems are made up of many sub-systems that each have their own patches, work rounds, and other issues [1].

2.2.2.2 EXAMPLES OF FAMOUS INCIDENTS:

In the following table [53], a list of famous and registered incidents occurring in industrial systems is presented. The list spans more than 30 years and lists the impacts resulting from the incidents based on standard security metrics such as confidentiality, integrity and availability. In the ICS domain, availability is ranked as number one in priority as it directly affects functionality and production [1]. However, other IT systems place different emphasis on security principles.

Table 2: Famous ICS Incidents [53][213]

Year	Attack Description	Location
1982	Trans-Siberian Gas Pipeline	Russia
1994	Salt River Project	USA
2000	Maroochy Shire Sewage Plant	AUS
2000	Russian Gazprom	Russia
2001	Electricity Transmission Control System	USA
2003	SQL-Slammer Worm	USA
2003	Houston Ferry System	USA
2005	Zotob Worm	USA
2006	Browns Ferry Nuclear Power Plant	USA
2006	Harrisburg Sewage Treatment Plant	USA
2007	Canadian Water System	Can
2008	Suburban Railway System	Pol
2009	USA Power Grid invasion	USA
2010	Stuxnet, Iranian Nuclear System	Iran
2011	Water Supply ICS	USA
2011	Duqu Global Virus	International
2011	Night Dragon	International
2012	Flame Virus	Middle East
2012	Qatar-based Ras Gas Virus	Qatar
2012	Saudi Aramco Oil Company	Middle East
2014	Norway Oil Company Phishing	Norway
2014	Sony Pictures	International
2014	South Korea, Wolseong Nuclear Plant	South Korea
2014	Sandworm	Ukraine
2014	German Steel Mill	Germany
2014	Black Energy	Ukraine
2014	Dragonfly/Energetic Bear No. 1	Ukraine
2015	Ukraine Power Grid attack No. 1	Ukraine
2016	“Kemuri” water company	USA
2016	Return of Shamoon	Saudi Arabia
2016	Ukraine Power Grid attack No. 2	Ukraine
2017	CrashOverDrive	Ukraine
2017	APT33	Middle East
2017	NotPetya	Ukarine
2017	Dragonfly/Energetic No. 2	Ukraine
2017	TRITON/Trisis/HatMan	Saudi Arabia
2018	Raspite	Kuwait
2019	Kudankulam Nuclear Power Plant	India
2019	Norsk Hydro	Norway
2020	Wind turbines scada system	Azerbaijan
2020	Water treatment plants	Israel

2.1.3 Common iIOT Security problems and issues:

Chapter One explained that modern internet-connected ICS is classified as iIoT [196][37]. This research found that the OWASP classification of IoT is comprehensive and also applies to ICS devices (see below 2.1.4). Therefore, it will be considered as a benchmark to assess and analyse the security of iIoT devices. This section is similar to section 2.1.2, in that the common characteristics of iIoT are presented in light of ICS devices. The aim here is to show the similarities between the two with specific emphasis on what existing research has demonstrated about the security of these IoT devices and about the similarities and differences between these technologies.

OWASP has classified IoT issues into a Top 10 list [54].

- The first issue that IoT devices have is weak interface security. Most come with default credentials and weak password systems, and many users do not change these.
- Second, many of these devices lack strong authentication systems, such as two-factor authentication. Two-Factor authentication requires two methods of authentication for extra security, where a user has to provide his/her credentials and another method like a pin code or an id [196]. Indeed, many IoT devices do not have a proper access control mechanism.
- Third, most if not all, IoT devices do not have encryption in their network communications or applied to any produced data.
- Fourth, many IoT devices have network service issues such as unnecessary open ports and susceptibility to cyber-attacks.
- Fifth, IoT devices, due to the security issues discussed above can result in the leakage and collection of personal information. This is a major privacy issue.
- Sixth, many IoT devices integrate with cloud storage and processing. As discussed in section 2.1.2, cloud computing has many issues.
- Seventh, many IoT devices lack logging, monitoring and access control mechanisms.
- Eighth, many IoT devices lack regular updates to firmware and software without the user specifically instigating the update within the software.

- Also, the poor update mechanisms typically lack verification and encryption and thus are capable of being duped by malware.
- Lastly, susceptibility to physical threats and issues (similar to those identified for ICS in section 2.1.2) are an issue for IoT devices.

However, there are other issues that could affect iIoT devices and these make such devices weak and vulnerable. The largest of these are related to design issues [55][56]. If exploited, these issues could lead to potential threats. In addition, IoT devices have limited energy. Energy is the amount of battery or power an IoT has. Knowing that could lead an attacker to use methods that exploit it. Also, IoT devices are sensitive to time factors such as latency, and an exploitation of this could lead to an overall malfunction. Typically, IoT devices, especially industrial type, work on low latency, which means they respond in real-time with no delay. An attacker can exploit that sensitivity and cause delay by blocking IoT devices and causing a delay [55] [56] [57]. IoT devices have limited capabilities and resources and are not intended to handle large amounts of data or large packets. This exploitation is particularly true of IoT devices because their memory and CPU resources are limited. Lastly, most IoT devices are designed to exist in the same network with a multitude of other IoT devices. The combined vulnerabilities and behaviour of these devices can become risky over time (See section 2.2.1 for more information about COTS).

2.1.4 Commonalities between modern ICS and IoT:

From the above points (2.1.3), it can be concluded that IoT and ICS devices share common characteristics and issues. In general, they both suffer from design, privacy and security issues that make them very vulnerable when exposed to the internet. In Chapter 7, we discuss what should be done to address the above vulnerabilities based on best practices and standards. However, these devices also share similar features [57] and drawbacks (e.g. poor updating standards and practices). Eventually, this could lead to vulnerable devices rooted inside networks.

Device communication with one another is dynamic and explicit, making it hard to predict their behaviour if it becomes abnormal or risky. They cannot adapt to new security solutions because of poor and limited specs and resources. ICS may differ from IoT in that ICS devices have a

long lifespan. They can function for a long time without patching. Many ICS devices are old legacy devices.

Both ICS and IoT devices have physical security issues. They both have web-based access to their devices and have limited resources and computing abilities. Both are connected to the internet and to cloud services. Both have communications issues such as lack of encryption: weak security default configuration and credentials. Both suffer from weak, or lack of, authentication systems such as two-factor authentication. Both systems use COTS and heterogeneous software. Both lack security features such as logging and monitoring [56] [57].

2.1.5 How criminals gain access:

In Chapter 4, the various methods that can be used to gain access to ICS devices are discussed. However, attackers commonly use a few general approaches:

- IP exposure allows intruders to access the device through an IP/port [58].
- Connected to IoT devices makes attacking OT devices possible [59].
- Contractor: normally they could jeopardize the network if they carry infected machines or misconfigure the network.
- Remote working: remote connection could open the exposure to risks such as infection by malware or interception of connection.
- Backdoors (malware) through email fishing or employee devices, flash drives

2.1.6 Cyber attacks:

Based on reviewed literature, the common attacks that target ICS and iIOT devices are varied [60] [61] [62] [63] [64] [65] [66].This research uses (T4), (T11) , (T12),(T15) and (T20) in chapter 6 to demonstrate the Trisis case study and the gas model. The two case studies are an example of unauthorized access to an ICS network, exploitation of software and packet modification to affect system status. Data leak also happens the Crisis incident. Chapter 4 uses (T4), (T12) and (T20). In that case study, the attacker uses default credentials and leaked data to access the network and then exploit vulnerabilities.

Table 3: Common attacks that target ICS and iIOT

Attack Type	Description
Data impairment (T1)	Affecting signals through attenuation, noise and distortion
Data drop (T2)	The attacker can drop the exchanged data between network devices
Data counterfeit (T3)	An attacker can inject a malicious content inside the network through a compromised node
Data disclosure (T4)	The device could leak data or data could be leaked by an insider or outsider accidently or intentionally, like theft
Frequency jamming (T5)	The use of interference to cause network blockage.
Data collision (T6)	Collision raises errors leading to the stopping of receiving data.
Router Data Compromise (T7)	Attacking router vulnerabilities to open the door for other attacks such as (Sybil, wormholes and router spoofing)
Data flooding (T8)	Most IoT devices have low memory, therefore an attacker can flood the device with many data or requests, causing the device to stop functioning as intended.
Data eavesdropping and interception (T9)	Ease to read data through, affecting the privacy. Block and delay data/information. Keylogging is common here.
Denial of Service (DoS) (T10)	Similar to Data Flooding: the aim is to affect the availability of resources.
Data tempering (T11)	The modification of intercepted data. Or modification of memory, configuration, firmware. Deleting files, loss and removal
Unauthorised access (T12)	Having unauthorized access to the device, either through brute force, guessing or default credentials.
Data spoofing (T13)	Sending a corrupted data or false information from a fake source. Falsification of information.
Rouge Access point (T14)	An attacker plants a rogue node, in order to hunt other devices
Man in-the-middle (T15)	Spying on data exchanged between components with the ability to exploit vulnerabilities or data.
Data scrambling (T16)	Radio jamming, congesting and crashing
Removable media threat (T17)	They can be used to propagate viruses or steal information.
Physical security (T18)	Physical access to a device or destruction
Social engineering (T19)	Obtaining data about personnel using social skills or social media.
Software attacks (T20)	The exploitation of malware and virus on devices' systems vulnerabilities.
Faulty hardware (T21)	This could lead to cause physical issues and impact on dependable components.

2.1.7 Threat agents and goals/motives:

There are many different individuals who could, whether purposely or inadvertently, become an attacker on a system: [3] [67]

Insider:

A person who works in a plant or factory. This is the most dangerous threat because he has access to both the network and sensitive data.

Hacker:

An individual with computer hacking skills, their motives can vary from criminal to curiosity or fame.

Extremist group:

A gang of people with political or religious agendas. Their motives could be any of the five motives listed below

Terrorist group:

This group seeks to do espionage and cause chaos.

National level:

This level is composed mostly of serious, skilful and professional personnel. Their motive could be political or spying or cyber warfare.

2.1.7.1 MOTIVES OF ATTACKERS:

There are four major motives in cybercrime that can be categorized as the following [2]:

Criminal:

The main goal in this category is to cause damage and losses.

Political espionage:

The gathering of intelligence in conventional ways as happens between intelligence organizations for reasons such as reconnaissance of critical infrastructure.

Political cyber warfare:

Cyberwars between political powers or nations.

Financial:

It could be to cause financial gains or to cause losses for other entities.

2.1.8 Cyber Physical incidents and Impact:

In this section, a list of cyber impacts is shown that could result from previous vulnerabilities and attacks. In Chapter 5, these impacts are examined and translated into cyber-physical terms.

The table below (Table 4) is an example that shows the cyber impact of attacks on ICS that have already taken place. The table was adapted from [68]. The term ‘Int’l’ means international and outside of USA. ‘Comm’ means commercial. ‘Gov’ means government. User means an individual user. In Chapter 5 and 6, the physical impact of these security vulnerabilities and resulting attacks are discussed in depth.

Table 4: Potential Cyber Incidents and Impacts [68]

Year	Attack Description	Source Sector	Target Sector	Motive	Impact
1982	Trans-Siberian Gas Pipeline	Unknown	Int'l	Trojan	Distort
1992	Chevron Emergency Alert System	User	Comm	Misuse of Resources, Compromise of User	Disrupt
1994	Salt River Project	User	Gov	Compromise of Root, Trojan	Disclosure
1997	Worcester, MA Airport	User	Gov	Compromise of Root, Denial of Service	Disrupt
1999	Bellingham, WA Gas Pipeline	User	Comm	Misuse of Resources	Disrupt
2000	Russian Gazprom	Int'l	Int'l	Compromise of User, Trojan	Disrupt
2000	Maroochy Shire Sewage Plant	Int'l	Int'l	Misuse of Resources, Compromise of User	Disrupt
2001	California Electricity Transmission Control System	Int'l	Gov	Compromise of Root	Unknown
2003	Davis-Besse Nuclear Power Plant	Unknown	Comm	Worm	Disrupt
2003	CSX Corporation	Unknown	Comm	Virus	Disrupt
2007	Tehama Colusa Canal Authority	User	Gov	Misuse of Resources	Unknown
2010	Stuxnet, Iranian Nuclear System	Int'l	Int'l	Worm, Root Compromise, Trojan	Disrupt, Distort
2011	Night Dragon	Int'l	Int'l	Social Engineering, Compromise of User and Root	Disclosure
2011	Duqu Global Virus	Int'l	Int'l	Virus	Disclosure
2012	Flame Virus	Unknown	Int'l	Worm	Disclosure, Destruction

2.2 ICS DEVICES' SECURITY:

2.2.1 Introduction

The emergence of specialized search engines such as Censys [69], Masscan [70], Shodan [71] and Zmap [72], and their speciality in finding online devices, including ICS devices, has simplified the task of finding a target device enormously for an attacker. Matters are made worse by the fact that those search engines give so much information about devices. This has become a major issue for industrial organizations and academics.

The relationship between the above-mentioned search engines and the security of online devices has been the subject of much recent research [73] [74] [75] [76] [77]. In this section, existing research in this domain is summarised, as a foundation for this research.

2.2.1.1 FINDING ICS DEVICES ONLINE

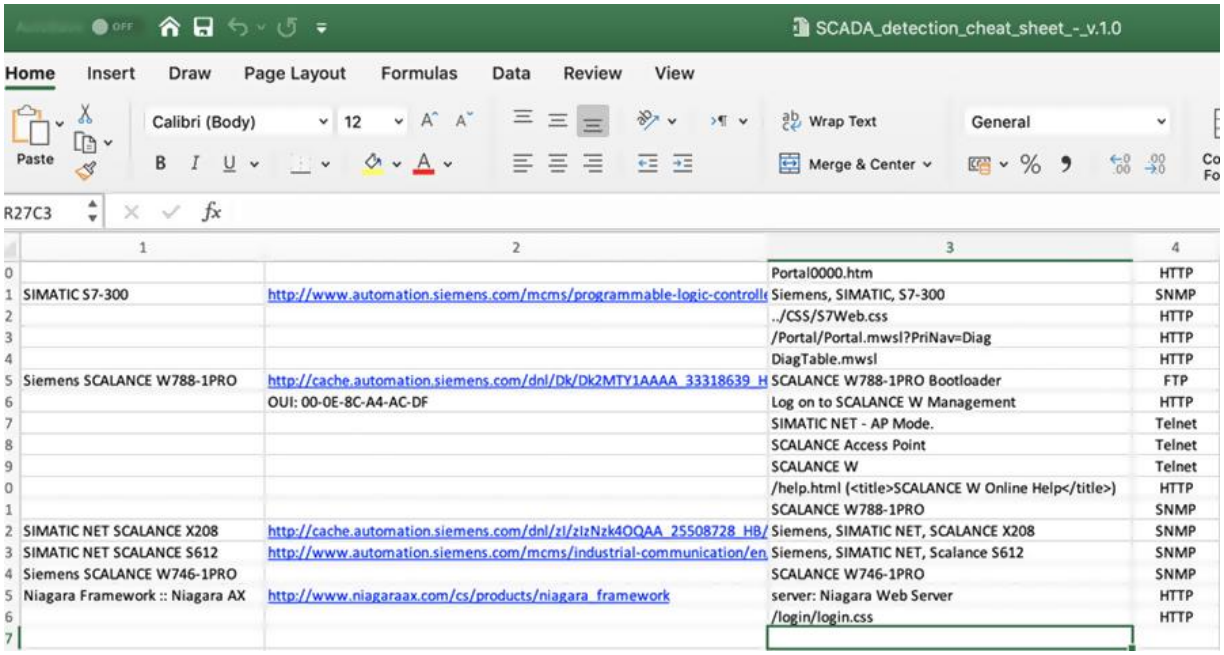
There are works that focus on the ability to find ICS devices through search engines. This research [73] developed a tool to scan for industrial devices using a modified version of the Zmap search engine. The tool name is WiScan, a low foot-printing scanner which does not affect the ICS device. A low footprint scanner collects little or passive information about a device, unlike active scanners where they can sometimes cause flooding by probing those devices with excess information. This tool targets SCADA ports. Their finding confirms the existence of SCADA systems online and that they can be discovered.

This paper [74] evaluated the functionality of Shodan on the listing, finding, querying and indexing a set of deployed PLCs. Their findings confirmed that their devices were positively found and identified.

This research published a methodology [75] to distinguish ICS devices from other devices in Shodan using PLC information; They managed to extract ICS devices that are connected to physical systems and classify them into what function they do and to what industry sector they belong to. This was achieved by extracting PLC code from those devices.

This paper [76] deployed honeypots and listed in Shodan to evaluate the impact of banners on devices. A honeypot is a decoy computer system that is connected to the internet for identifying hackers, methods and techniques [195]. They concluded that by manipulating banners, they could lower the exposure of ICS devices, thus lowering the impact of them. A banner usually has information about a computer or a network such as a port number or an operating system version.

Some researchers attempted to gather filters that could be used in a search engine to find online ICS devices. The filters are typically information about a vendor name, software version, file extension names and other configurations that are specific to these devices [77].



	1	2	3	4
0			Portal0000.htm	HTTP
1	SIMATIC S7-300	http://www.automation.siemens.com/mcms/programmable-logic-controll	Siemens, SIMATIC, S7-300	SNMP
2			../CSS/S7Web.css	HTTP
3			/Portal/Portal.mwsl?PriNav=Diag	HTTP
4			DiagTable.mwsl	HTTP
5	Siemens SCALANCE W788-1PRO	http://cache.automation.siemens.com/dnl/Dk/Dk2MTY1AAAA_33318639_H	SCALANCE W788-1PRO Bootloader	FTP
6		OUI: 00-0E-8C-A4-AC-DF	Log on to SCALANCE W Management	HTTP
7			SIMATIC NET - AP Mode.	Telnet
8			SCALANCE Access Point	Telnet
9			SCALANCE W	Telnet
0			/help.html (<title>SCALANCE W Online Help</title>)	HTTP
1			SCALANCE W788-1PRO	SNMP
2	SIMATIC NET SCALANCE X208	http://cache.automation.siemens.com/dnl/zI/zIzNzk4OQAA_25508728_HB/	Siemens, SIMATIC NET, SCALANCE X208	SNMP
3	SIMATIC NET SCALANCE S612	http://www.automation.siemens.com/mcms/industrial-communication/en	Siemens, SIMATIC NET, Scalance S612	SNMP
4	Siemens SCALANCE W746-1PRO		SCALANCE W746-1PRO	SNMP
5	Niagara Framework :: Niagara AX	http://www.niagaraax.com/cs/products/niagara_framework	server: Niagara Web Server	HTTP
6			/login/login.css	HTTP
7				

Figure 3: SCADA Detection Cheat Sheet [194]

Based on the previous works in this section, one can see that ICS devices are present online and there are many tools, techniques and search engines and methods that help in the task of ICS discovery. This is contrary to the common belief that ICS systems are hidden and isolated from the internet. This kind of research helps to determine the direction of ICS security. However, it is only the beginning. There are plenty of other devices that come from other vendors. Many of them are present online, but there is a little or no work to detail how they can be explored. This is an open window for research in this area to cover as many vendors as possible. For example, one could discover those devices' signatures and network details such

as device name, version, network port and many other filters, by using methods that we highlight later.

2.2.1.2 ICS DEVICE SECURITY METRICS AND ASSESSMENTS

There are many metrics systems [78] to evaluate and measure the security of software and hardware in computers. There are metrics that measure vulnerabilities, defences, threats and situations. In this research, the author is interested in vulnerabilities metrics based on threat intelligence such as OSINT. Shodan and ICS-CERT are linked to the Exploit Database [79] and the National Vulnerability Database (NVD) [80] respectively. Both databases depend on the CVSS metric system, as discussed below.

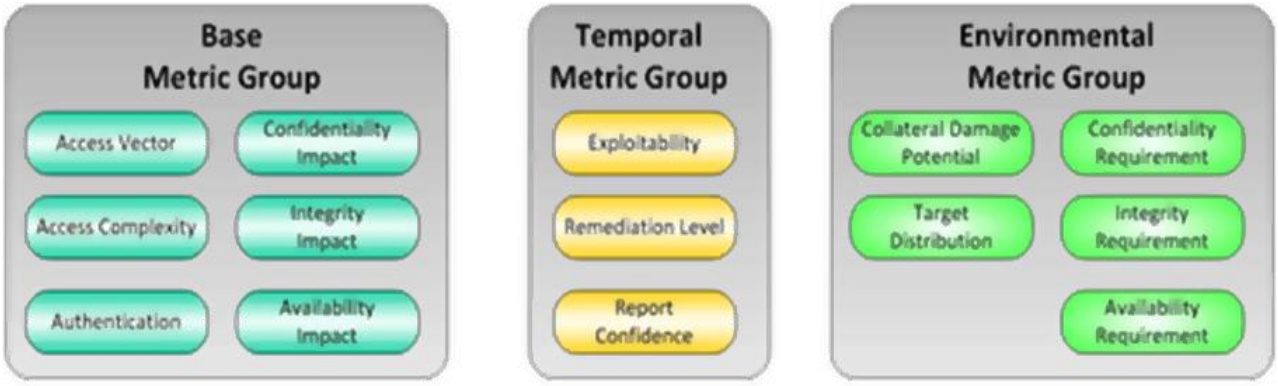


Figure 4: The CVSS metric Groups [197]

The Common Vulnerability Scoring System (CVSS) is a security metric that measures the severity of a vulnerability. It helps organizations manage their vulnerabilities [197]. There are two versions of CVSS: CVSS version 2 and CVSS version 3. CVSS v2 measures the criticality of a vulnerability based on three metrics: Base, temporal and environmental. The base is the constant characteristics of a vulnerability. Temporal is the changing characteristics of vulnerability not including the environment. Environmental are characteristics of a vulnerability that are unique and relevant to a particular user. However, the environmental metric has been removed in CVSS v3. The base and temporal have many sub-metrics. The environmental metric uses the base and temporal metrics by adjusting them to an organization or a situation. The image below shows how CVSS is used to assess vulnerability. We can see only the base metric is used, the temporal and environmental are left to the organization's risk assessment context.

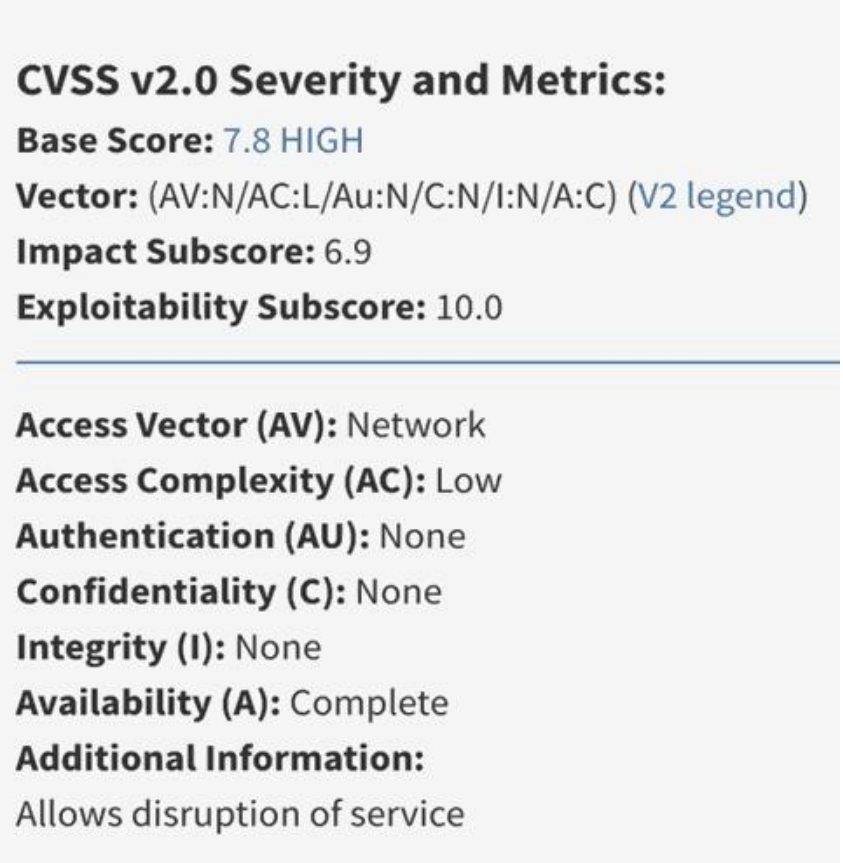


Figure 5: An example of an ICS device CVSS [198]

Most vulnerability databases, such as the NVD and Exploit databases, use a CVSS score assigned with vulnerabilities. Therefore, we use a similar scoring values range as CVSS. We do not intend to compare or replace CVSS. It is purely subjective to choose metrics that work for an organization. To the contrary, our research is an early contribution to developing a metrication system for ICS and iIoT devices.

CVSS versions 2 and 3 suffered criticism and dissatisfaction in the security community. Risk-Based Security [81] criticized CVSS V2 for its inability to distinguish between vulnerabilities with different risks and profiles. It also requires too much knowledge about a vulnerability impact., e.g. how a vulnerability can affect a physical system. Both CVSS v3 & v2 were also criticized for their limitations in assessing ICS and IoT devices (see two reasons below) [82]. The common practice nowadays is to patch a vulnerability based on its CVSS score. This is considered both risky and ineffective for two reasons [78]. One, it is risky because low score vulnerabilities can lead to a high severity threat [83]. Second, it is ineffective because it is a random practice, which means it patches vulnerabilities randomly and not based on what really impacts the organization [83].

In considering existing work for ICS devices' security, it is worth mentioning that there two types of methodologies in security assessment: active and passive. Active assessment is data collection about a target system by actively engaging with it through port scanning while passive assessment is data collection about a system without active engagement [199]. This work [84] proposes a similar work to the Shodan search engine bug feature. The work is useful for device vulnerability assessment and is called the "Shodan-based Vulnerability Assessment Tool" (ShoVAT) [44]. It is a passive vulnerability assessment tool based on the linkage between the Shodan search engine and the National Vulnerability Database (NVD). The tool matches results with their corresponding vulnerability. This paper researched on SCADA components such as PLC and HMI in Shodan, such as Siemens and Rockwell components, and their vulnerabilities using passive and active assessment [85]. Their active technique uses the Nessus vulnerability assessment tool and the passive techniques use the NVD. Both techniques are used to assess the vulnerability of the collected ICS devices. The devices are well-known and trusted brands such as Rockwell, Siemens and Schneider. The vulnerabilities range from default credentials, man-in-the-middle and other exploits This thesis [86], proposes a methodology for finding ICS devices in the Shodan search engine and their corresponding vulnerabilities from databases. The author has collected and analysed data about industrial devices. The data is found in banners that are retrieved by Shodan, such as vendor name, operating system, country, geolocation and other information. A methodology and visualization techniques are proposed to view collected data in webpages using open source technologies.

This research observed that the work of [84], [85] and [86] focus on vulnerability assessment of ICS devices. They depend on the popular vulnerability databases mentioned above. All those databases depend on the widely used CVSS metrics system. However, there are technical issues that depend solely on the CVSS metric system as we explained earlier in this section. For that reason, in our framework, we consider the CVSS as only a factor and as one of many factors that could contribute to the security of ICS devices (See Chapter 4). In addition, the three papers discussed earlier lay the foundations to hunt and analyse ICS devices, one may wonder what to do with all this information and more interestingly, what would be the impact? Finding an answer to this requires an active role from nations, academics and industrial organizations to answer this question before motivated malicious actors do. This challenge is the motivation to explore these two questions in this thesis.

Another approach in the area of ICS security assessment is shown in this paper [87], where the authors proposed a cyber-threat inspection framework for ICS based on OSINT. Their framework collected and analysed OSINT data. The aim of their research is to inspect possible threats related to ICS devices. The concept of OSINT is explained in more depth in Chapters 3 and 4. OSINT is a part of threat intelligence used heavily in cybersecurity practices. The idea of threat intelligence is to gather as much information as possible about a threat or a vulnerability that could have an impact on a target. The benefit of threat intelligence is that it acts as a real-time monitor of what is going on in the cyber world from a security perspective and offers the possibility of updating us with relative knowledge. It is already applied in cybersecurity in general, but it is very helpful to see it in the ICS area as applied to vulnerability and threat assessment. For that reason, this work [87] is applied in our framework as only a part of the equation to study the possible risks that could target online ICS devices (See Chapter 4).

Concerning ICS metrics, our research found an ICS metric called Industry Vulnerability Scoring System "IVSS" [200] [201]. Clint Bodungen developed it [208]. Our framework ICSrank shares the same goal with IVSS, which is to develop an ICS methodology to rank ICS vulnerabilities and security. IVSS is a static or non-transparent metric. A static metric means it is only used by one organization to quantify its risks, or it means it is published to the public via such as CVSS without transparency on how risk was calculated and what are the decision processes were. Public static metrics can cause problems if it lacks important details about a vulnerability or has wrong information, such as an inaccurate risk score. In order to achieve accuracy in ICS device security, comprehensive knowledge about an ICS device is required such as network, system processes, threat event, industry and impact (see chapter 4 & chapter 6). Knowing about this information is beneficial for establishing defensive strategies and in assessing potential risks (32). IVSS is a good start in the direction of ICS security metrics. IVSS has an advantage over traditional CVSS metric systems in being more specific about ICS. However, there are challenging issues for IVSS: it relies on unjustified mathematical equations just like CVSS [202]. The other issue is lack of transparency, i.e. the process of mapping a score or getting a score value should be open to the public to avoid old mistakes in CVSS [202]. Another ICS metric is called "TEMSL" which focuses on five metrics: threat, exposure, mission, safety and loss. It ranks vulnerabilities as none, some and significant [200] [201]. TEMSL does not use any mathematical equations and it uses decision trees to specify the type

of prioritization (e.g. Patching): never, next and now. Both IVSS and TEMSL are not standardised yet and are still work in progress [200] [201].

2.3 SUMMARY

In Section 1, the general concepts of ICS security such as the main vulnerabilities and their causes were examined in depth, common cyber-attacks that target ICS systems were listed with famous incidents and descriptions of threat actors: who they are, why and how they do it and what is their goal. A literature review of general security characteristics of ICS and iIoT devices was also presented. ICS devices suffer from many types of vulnerabilities and the various reasons for these issues were explained. Despite being more modern than ICS devices and designed to be integrated online from the beginning, iIoT devices share many weaknesses with ICS devices as explained above. Many times, these issues arise because manufacturers do not take security and privacy into consideration in the design phase. This research argues that understanding the general characteristics of ICS and iIOT devices is vital to understand why they are insecure and why they are attacked. It is important to take proactive steps to assess the risk and propose necessary countermeasures or solutions.

In Section 2, research areas such as vulnerability assessment techniques and the use of security metrics to assess vulnerabilities in the ICS security domain were explored. Firstly, section 2 showed different techniques for exploring and finding ICS devices online. It explained how existing search signatures, filters and operators need to be researched further to cover as many vendors as possible. Secondly, the current vulnerability assessment methods were discussed. Furthermore, it was argued that vulnerability assessments that depend on CVSS would be improved by incorporating threat intelligence. It also explained why CVSS metrics are not always effective when it comes to the protection stage such as patching.

Related literature to this thesis is classified into 3 types. Type 1 is concerned about bug hunting and ICS indexing by using search engines and vulnerability databases. Type 2 uses existing but limited OSINT resources. Type 3 relies on mathematical equations to rank ICS vulnerabilities. This thesis is a hybrid model of the 3 types. It's the attempt of this research to come up with an approach to solve the limitations of the 3 types. In the next chapter, existing surface attack vulnerabilities of ICS and IoT are discussed.

CHAPTER 3

LITERATURE REVIEW II

3.1 INTRODUCTION

The internet of things refers to the interconnection of electronic and computing devices as well as other devices, whereby they communicate through unique identifier codes. These codes allow communication (transmission of data) over the network without the need for human-computer interaction or human-human intervention [163]. The interconnection of the devices needs to be secure lest malicious actors penetrate the system and pose potentially severe security threats. To understand the security measures that ought to be implemented, security loopholes need to be studied so that effective control measures can be implemented [165]

This chapter discusses existed literature about common issues and attack techniques that target online devices. Chapter 1 and 2 already covered most of those briefly, however this chapter is reviewing current guidelines that categorize vulnerabilities into types. The source that this study is using is OWASP Top 10 guideline [source]. Each category includes detailed information and descriptions about vulnerabilities, attack types and mitigation methods. This type of categorization inspires this research to implement a category and a framework that could be applied to ICS devices. OWASP list consists of essential labels that are applicable to ICS devices. OWASP provides information that can be transformed into a critical knowledge for ICS devices security. ICSrank contributes to knowledge by building novel OSINT categorization framework, that utilizes OSINT with existed cybersecurity frameworks such as OWASP top 10. Below is a list of common ICS and IoT issues and what information are applicable in the research in this thesis.

3.2 TOP 10 IOT/ICS VULNERABILITIES AND RECOMMENDATIONS

As of 2014, the top 10 vulnerabilities were insecure interface of the web, lack of sufficient authorization and authentication, and insecure network service, lack of encryption during transport, privacy issues, insecurity in the cloud interface, insecurity in the mobile interface, lack of sufficient configuration of the security, insecure firmware/software, and poor physical security [162]. Many ICS devices share the above vulnerabilities (see chapter 2). In this chapter, we discuss common IoT/ICS vulnerabilities in more details. The impact of the vulnerability to the business is discussed. Finally, the criteria to determine whether the web interface is secure is checked and the procedure to make the interface secure discussed.

3.2.1 An Insecure Web Interface

Insecure web interfaces present a security risk when working on a particular web page. Hackers and the like in accessing the page may affect the confidentiality, integrity and availability of the information [166]. If the web interface is not well maintained, the website of the company will be quite vulnerable and insecure. A discussion of the various sections is outlined below:

The threat agents: These are agents that have access to the web interface. They may either be external or internal users. The users that interact with the devices or the web may have unauthorized access to the devices interconnected in the IoT. This is feared because accessing the devices means one can manipulate them to show potentially harmful inconsistencies.

The Attack vectors: The web interface is insecure therefore it is easily exploited. The attacker understands that the security measures in the interface can be easily manipulated, hence they use the weak credentials, through enumerating the accounts and plain-text credentials to access the interface. The sources of the weak interface are, for example, the weak account lock-out settings, and lack of session management. In session management secure websites automatically logout individuals after a period of inactivity. This prevents unauthorized access from those that could take advantage of the long period of inactivity especially when a legitimate user forgets to logout. The other issue is SQL-injection and cross-site scripting (CSS). SQL injection means the attacker executes suspicious SQL statements to interfere with

the server and database of the applications. Cross-site scripting means the attacker injects malicious JavaScript code into the browser of the victim. The other source of vulnerability is the exposure of the credentials in the network traffic [166]. This is true when the details in the traffic are not encrypted and can be tapped by attackers. Weak default credentials are the other vulnerabilities. The default credentials should use passwords and usernames that are difficult to crack. In addition, the first-time passwords should be changed upon login.

The security weakness is prevalent because the intention of the attackers is to expose the vulnerabilities of the web interfaces. The threats from external and internal environments are of equal magnitude and should not be underestimated. They are easily detectable when the web interface is manually examined and through the use of automated testing to discover the issues.

The technical impacts of an insecure web interface are quite severe. They result in either the corruption of data or its loss. Other consequences are unaccountability, denial of service and the attacker taking full control of the network's devices. In the case of a business specific IoT, the impacts could mean harm to the customers thereby compromising the entity's devices and the customer devices [172].

However, the determination of the security of the web interface depends on a number of considerations. The web interface should be checked to ensure that the default passwords and usernames are changed during the initial set-ups. Most initial passwords are computer-generated; hence, the customer should be guided to set up strong passwords after the initial set-up before using the web interfaces. This is because the initial credentials can be tapped in the databases. The passwords created should be strong to lockout any probability of being cracked. The other test for a secure web interface is the ability to lock out the user/attacker after three failed attempts. This helps to prevent password guessing and forceful access. The other method of checking a secure interface is through password recovery mechanisms. Currently,the user phone (through call or text of codes), the email addresses and other crucial details are used to recover the passwords. If this fails then customer care has to be contacted. Lack of effective password recovery schemes means that anyone can successfully seek access to accounts. The sites should also be assessed for threats such as SQLi, XSS, and CSRF among others.

The web interface can be made secure by changing the default usernames and passwords after the initial set-up, locking out accounts after a number of failed attempted logins, ensuring that

weak passwords are not allowed. The password recovery should be robust to ensure that information is not available to attackers allowing wrongful validation of the account. Other precautions include encrypting the credentials so that they are not exposed to the network traffic. The web interface should not be susceptible to CSRF, SQLi, or XSS [170].

3.2.2 Insufficient authorization/authentication

Insufficient authorization/authentication means that account access is not fully authorized. User accounts, in most cases, are checked for authenticity and authorization by the user. In organizations, the authorization schemes used include biometric systems such as voice, face and eye recognition, or fingerprints. When checking different interfaces (web, the cloud or the mobile interfaces), there should be authentication measures to prevent unauthorized access. Some authentication schemes are one-time codes and passwords that expire within a few minutes so that the attacker is not allowed to interfere if they do not receive and input the codes immediately [169].

The threat agents are users that access the network through the cloud interface, the mobile interface or the web interface. They could either be the external or the internal users of the system. The attack vectors are averagely exploited. This is by the use of weak passwords and other access information. If the password recovery mechanisms are wanting, they also pose a security threat to the system. Other attack sources/vectors include lack of role-based access control, credentials which are poorly protected and the escalation of the privilege of certain users. Role-based access control means that there will be different sets of information that can be accessed by both external and internal users. For internal users, information accessed by junior management and staff will be quite different from that accessed by the senior employees. Therefore, to access different sets of information, one has to have more passwords and access credentials based on his or her role in the organization or system [8].

The prevalence of security weakness is rather common and easily detected. The discovery is through manual inspection of web interfaces or through automated systems that send reports of the accessed sites to the relevant personnel or authorities. Common sources of security weaknesses are weak passwords and poorly protected hardware or access points. The other mistake is assuming that internal information cannot be accessed by external users on different networks.

The technical implications are denied access, compromise of the devices and network in the IoT, lack of accountability, loss of data and its subsequent corruption. The business impacts are that crucial data for different clients and customers have been compromised, modified or stolen. Other than the business being harmed, customers could be harmed as well.

Some measures should be checked to determine the ease of authorization and authentication of the interfaces. To check for authentication, simple passwords may be used to determine the sufficiency of the password policy. The network traffic also has to be reviewed to check whether credentials are encrypted or transmitted in cleartext. The password control schemes also ought to be checked, for example, checking the complexity of passwords, password expiration, and resets just to mention a few. Finally, the re-authentication schemes should be checked for sensitive features. To check for authorization, access controls can be examined for privilege escalation, and also checking interfaces for separation of roles like the amount of information accessible to administrators and normal users.

The countermeasures to ensure authorization are strong passwords, granular access control, protecting the credentials, using two-factor authentication schemes, secure password recovery schemes, and requiring authentication for sensitive features. Both mobile and computer app authentication should be necessary as well as revoking fake credentials, requiring authentication of the server, and ensuring that the system generates a session key to the client when they need access. The session key should be random and vary [162].

3.2.3 Insecure network Services

Problems arise from vulnerabilities in the network service that is employed in accessing IoT services. Network faults allow intruders to have unauthorized rights to use data and devices. The threat agents may be from internal and external users that manipulate the network to access the flow of data and control of the devices. The network vulnerabilities are exploited in IoT. The attacks on devices can be major causing them to perform unprecedented actions. Although such attacks are uncommon, the detectability is obvious Some of the points of susceptibility arise from buffer overflow and denial of service that render the devices out of reach of the user. Another network issue is network fuzzing. Network fuzzing is a technique that is used to discover security issues by inputting random and massive amounts of data [162]. It usually creates a denial of service, UDP services that are easily exploited, open ports through UPnP and other vulnerable services [165].

The technical impacts of the insecure network are loss of data, denial of service, corruption of data and making other devices on the same network vulnerable. The business impacts are rendering the network useless due to denial of service, or the affected device facilitating attacks on the other devices in the network. Once again, this could harm the customers as well as other extended stakeholders.

To check whether the network is insecure, the open ports of the devices are reviewed using port scanners, identified open ports are checked for any vulnerabilities to DoS, UDP related vulnerabilities, fuzzing and buffer overflow attacks. Other measures are to check whether the open ports are really necessary, or they may be the sources of UPnP attacks.

Four measures should be taken to ensure that the network is shielded from the insecure network services. The first is ensuring only the required ports are open and available when the need arises. This will prevent unnecessarily exposing ports that are not being used. The network should be shielded from fuzzing and buffer overflow attacks and DoS attacks. These often affect the particular device and other devices that are connected to the network. Guarding the ports exposed to the internet through UPnP also serves as an excellent security measure. Finally, any abnormal traffic request should be detected and blocked in the gateway layer of the service [164].

3.2.4 Lack of Transport Encryption

Lack of transport encryption refers to the fact that data being transported across the network is not coded in a manner so that it can only be accessed by authorized users. Therefore, attackers in the network can access it and understand the contents. The threat agents are the people whether insiders or outsiders that can access the network. The attack vectors are normally exploited. The attackers utilize the lack of data encryption over the network. The issue is common and can be easily detected. For wired networks, it can be assumed that the information will only be available to the devices or people on the network. However, for a wireless network, anyone within the range of the wireless network can view the data if there is misconfiguration [164]. To check the network for lack of encryption, readable files and data are checked for the presence of threats. Automation can also be used to check for lack of effective encryption so that adequate measures can be taken.

Exposure of data in transit is dangerous and other than the loss of data, it may become corrupted; hence, the attacker may manipulate user accounts and compromise the system. They may even gain control of it at the expense of the owner. The business is therefore automatically affected especially when customer data is misused for unauthorized reasons. Transport encryption is checked over the network by determining whether the data is in plain text or not. It can also be determined if SSL or TSL is used or ignored and checking the recommended encryption protocols used [163]. Transport encryption is ensured by using protocols like TSL and SSL for data crossing the networks. The industry-standard encryption methods should be used; these methods would protect data from being misused while transiting the network. The received data should be subjected to integrity checking to assess its validity. Other encryption methods are ensuring the secure encryption key, making sure there is message payload encryption, and using only the accepted encryption standards to avoid proprietary encryption protocols.

3.2.5 Privacy Concerns

Privacy concerns are issues related to the exposure of personal data such that there is no confidentiality. In this case, data is not protected and is easily discovered by attackers who gain access to the IoT system. Privacy concerns may arise from access to physical devices, access to data over the network, accessing information in the cloud or personal information in mobile applications. Common sources of privacy concerns are lack of authorization and authentication, lack of data encryption over the network, and insecure network services. When personal data is not adequately protected an attack may come from either inside or outside an organisation.

Privacy concerns are usually caused by a lack of proper protection against the collection of personal data. The discovery of this vulnerability is simple and may be done by checking how the user sets up and activates devices. Automated devices also check for any consistencies in data collection faults and also loss of other sensitive data [171]. The technical impacts of the collection of personal data for misuse may be quite severe because the effects may go beyond the IoT systems. For instance, sometimes personal data such as bank registration and other national bodies expose the data of the users, which can then be manipulated and used maliciously. This is a far-reaching example of the customer being negatively affected when private confidential information is misused.

To check whether there are privacy concerns for the systems connected to the IoT, all of the data types collected by devices, mobile applications and the cloud interfaces are identified. Before transmission over the network, personal identification data should be checked for encryption. This will prevent its exposure over the network. There should also be granulated access to the personal data; access to personal data should be limited to those authorized to handle it.

There are various steps in ensuring that privacy concerns are addressed in an IoT. Data critical to the functionality of the working of the systems should be collected and any other should be left out. This prevents collecting sensitive data. Making the data anonymous is a good step in ensuring privacy and the data should then be encrypted. Another step is ensuring that only authorized personnel have access to the data, more important is the role-based granulated access to the personal information [169]. Finally, retention limits should be set so that clients are aware of such limits.

3.2.6 An Insecure Cloud Interface

Cloud computing has continually offered solutions to the various storage needs of different clients. However, public cloud computing services have been a source of trouble for unsuspecting clients who store their data in them. The source of the threat is from anyone who can access the internet and search for the keywords contained in these cloud databases. The attacker often exploits the lack of sufficient authentication, the lack of data encryption during transport and unauthorized access [167]. Insecurity in the cloud can result from the use of poor account access credentials that are easy to guess. To detect an insecure cloud, the connection is identified, and the SSL checked if it is in use. The password reset mechanism can also be used to check how easy it is for enumeration of the accounts. The technical impacts are severe because the user data may be compromised, and the user may lose control of the interconnected devices. Likewise, the business impacts are severe as data could be stolen and modified so that the attacker gains control of the interconnected devices.

To check for an insecure cloud, login credentials are checked for the ease of change during initial set-up. It could be checked for account locking after a specified number of failed login attempts. It could also be checked for valid password recovery schemes. The API interfaces and the cloud interfaces should also be checked for vulnerability [167].

The suggested methods of securing a cloud interface are changing the default names and passwords after the initial set-up. This will eliminate the use of system-generated passwords. User accounts should be protected from enumeration by simple mechanisms like password reset schemes. There should also be an account log out after a specified number of failed logins. The other security measure is ensuring that data is encrypted online to prevent exposure of credentials; the web interface should be free from XSS, SQLi and CRSF. There should be a two-factor authentication system to prevent any malicious access attempts. Finally, the system should be able to detect and block abnormal requests.

3.2.7 An Insecure Mobile Interface

Most of the applications on mobile phones are connected to the internet. These do not promise absolute security when working online. The applications that control the devices on the IoT are no exception as these may be subjected to malicious attacks if they are not properly guarded or secured. The threat agents are specifically those who can access the mobile application. This is normally exploited where attackers target devices that do not have sufficient authentication features [170]. The other simple method that makes devices susceptible is account enumeration where one attempts to access the IoT with easy-to-guess credentials. Lack of encryption in the transport of the data also poses a security challenge to mobile applications.

The security weakness in mobile applications is generally from credentials that can be easily guessed. It is also possible if the accounts can be retrieved by fake credentials. This discovery can only be made if the connection to the wireless networks is checked for active SSL and the password reset mechanisms are reviewed. Insecurity in mobile networks means that the personal data of the user could be compromised resulting in loss of control of the devices to the attacker [162]. Such stolen, modified or compromised data could result in adverse effects to the customers or clients of the system.

Every interface has to be checked for security, and the methods used in the previous discussions are quite similar. It has to be checked to determine whether default passwords and usernames can be changed after the initial set-up. It should also be primed for the account to lock after a certain number of failed login attempts. The password recovery schemes should also be tested to determine if they assure security and authentication or authorization schemes, for example, through the use of one-time codes that can be verified by the user alone. Two-factor authentication schemes can also be tested to check the exposure of the data over the wireless networks due to the lack of encryption.

To secure mobile interfaces, the default credentials must always be changed after initial set-up to prevent the probability of attackers using the computer-generated default login credentials. Accounts should be protected from enumeration especially by passwords and usernames that can be easily guessed. The third step is ensuring account lock-out after a certain number of failed login attempts. Encryption of the details over the networks prevents their exposure. Two-factor authentication is vital to prevent unauthorized access to applications [165]. In addition,

the mobile application should be coded with an anti-tampering system, and even restrict that app's execution on a tampered operating system.

3.2.8 Insufficient Security Configurability

Insufficient security configurability implies that users are not able to change the security controls in user accounts. It is not possible for the web interface to make use of granulated access or enforcing strong passwords. The major threat agents are from anyone who can access the accounts. Apart from granular permission to access and control the accounts, lack of encryption also poses a major attack vector. Other issues may be the lack of passwords when performing certain operations that compromise the various applications and data. The attack may be accidental or intentional [163].

The major security weakness stems from the inability to alter security controls in the network. This means that the attacker can easily access and alter accounts as the user will not be able to change any controls to lock the attacker out. An example of such situations is where the user is not able to change a password even when it has been cracked by an attacker.

Devices are always compromised in this attack and lead either to the loss of data or its corruption. If the attacker gains control of the devices, they can manipulate accounts and other items for selfish reasons. This may harm the clients and customers adversely. To check whether the systems in place are sufficient, the following should be done: the options for strengthening passwords are checked, checking the separation of administrator and normal user accounts, checking for data encryption, checking security logins, and checking whether the system alerts the administrators to security issues.

These security measures ensure that normal user and administrator accounts are separated. This will prevent the attacker from easily bypassing the administrator controls to affect the confidential information. Data should be encrypted while in transit to ensure that it is not exposed to hackers who could tap it to pose a security threat. The use of strong passwords should be enabled to prevent account enumeration [171]. The system should also keep a log of security events and send notifications to administrators of any security issues detected.

3.2.9 Insecure Firmware/Software

Any software used in systems should have the capability to be updated to ensure that security definitions are updated to block security threats. Failure to update system firmware will always give rise to issues like slowed connection, lack of updated encryption systems and being prone to attacks. The threat agents will be anyone who has access to the network, the devices or the update servers. Some of the common attack vectors are the capture of update files in unencrypted connections. In such cases, attackers are able to update the firmware to fit their malicious intentions. Such attacks may be localized or over the internet [166].

The weakness of the firmware is often seen when the system is not updated, and the vulnerabilities are discovered. Another security weakness is the network through which the updates are made, or an insecure network where the updated files are tapped by the attacker and the security definitions are compromised thereby enabling attacks to be planned. Therefore, network traffic must be checked for encryption and hex editors used to check the update files for any interference.

Insecurity in the firmware is a major issue for users. It means that confidential user data may be compromised and potentially corrupted. Total system failure and loss of control are some of the technical hitches that one may suffer too. Stolen and modified data would mean harm to the clients, attack on the other devices, and loss of total control to the system.

To check for software security, one should check the update file itself for exposure of its crucial information. The production file should also be checked for encryption and proper signing. The transmission mode of the update should be reviewed, checking the update servers, and finally check for validation of the updates. Some of the security measures to be taken include ensuring that the devices are able to perform the desired updates to define the new security measures and reduce susceptibility to the attacks [169]. In the update system, the update files should be encrypted to prevent exposure. The channel of transmission of the update should be protected and encrypted too. The update files should ensure that the confidential data is not exposed. The updates should be signed to verify their source so that any alterations will be detected, and proper security actions are taken. Finally, the update server should be secure with the implementation of a secure boot.

3.2.10 Poor Physical Security

Lack of physical security implies that there is physical access to the devices and storage so that an attacker is able to tamper with the storage system. Access may also be through external ports or USB which s/he uses to access vital ports. Lack of physical security means that sensitive data can be accessed as well as the servers [168].

The major threat agents are those with physical access to the devices. Access may be through USB ports, flash drives, SD cards or other storage methods. It is therefore easy to access data, operating system and other vital information. Physical security in systems is often evident where the attacker can easily access, disassemble, and transfer data to their devices from the main devices. The most common physical access and data transfer mechanism is the use of USB ports/flash drives. This often targets the features intended for maintenance, update and configuration. The technical impact is severe because it leads to compromise, corruption, and loss of data stored in the devices. The stolen data could be modified, and the attacker could take control of the devices and cause further interference with the whole system.

To check for the probability of physical access breaches, administrators should check for the ease of disassembling the devices and how easily storage media can be accessed. The other method is to check access control through USB ports and other external ports. The system should be checked for any administrative interfaces that can be deactivated and any controls that can diminish the administrator's access capability [171].

The security measure taken to control these issues is to ensure that physical access to the devices is restricted only to those authorized. The data storage mediums should also be safeguarded from easy dismantling and removal. This prevents those that access them from readily performing their actions without being noticed. USB ports should be secured and any access through such ports should be authorized and receive authentication. If there is no authorization, the system should send security messages to the owner and lockout the intruder and limit access to the rightful administrators. Additionally, the data in storage media should be encrypted to prevent exposure even after being accessed.

The table below shows the relationship between the OWASP vulnerabilities top ten 2014 and the OSINT information types. The recommendation is also included [162]:

Table 5: OWASP top 10 and OSINT information types and recommendations:

OWASP Vulnerabilities	Recommendations
An Insecure Web Interface	• Change Default credentials after initial set up. • Error messages in case there are failed login attempts. • Check directory listings to track and trace the source of attacks.
Insufficient authorization/ authentication	• Password reset pages to be enabled with authentication. • Default credentials: changed after initial set-up • Server status pages: for active users • Client-side code files for encryption and authentication. • Check the file extension to track what can be installed on the IoT system
Insecure network services	• Password reset pages for authentication of the right users. • Default credentials to be changed after initial set-up. • Protocol ports: to secure the network from attackers who would use freely available ports.
Lack of Transport Encryption	• Server status pages to be encrypted, any interference to be revealed in error messages. • Network and Physical Location; the data in the network should be encrypted, including encryption at the source. • Protocol ports; only engaged protocols should be open to avoid intrusion from free protocols. • Vulnerabilities and data advisories protected
Privacy Concerns	• Password reset pages; should allow for authentication and set strong passwords. • Default credentials should be changed after the initial set-up. • Vulnerabilities and data advisories protected. • Protect the metadata • Keep log files to track the users
An Insecure Cloud Interface	• Password reset pages should allow for authentication, setting of strong passwords and encryption. • Backup files to shield from complete data loss after corruption. • Default credentials should be changed after the initial set-up. • Protect the metadata
An Insecure Mobile Interface	• Default credentials should be changed after the initial set-up. • Password reset pages to allow for secure authentication, username and password changes and allow setting of strong passwords.

OWASP Vulnerabilities	Recommendations
	• Error messages should be sent in case there is any intrusion of failed login attempts. • Client-side code files should be encrypted to prevent the attacker from accessing vital information.
Insufficient Security Configurability	• Configurations file should be encrypted to ensure the attackers do not easily read it. It is not an easy read by the attackers. It should also be signed from the source. • Error messages sent to the administrator in case of any suspicious activity.
Insecure Firmware/ Software	• Design issues should be considered to allow for updates and embedded system security.
Poor Physical Security	• Network and Physical Location should be secured to prevent unauthorized physical access and disassembly of the devices. • Backup files should also be secured from unauthorized personnel. • Keep log files to track the system users. • Database dump files should be secured from unauthorized access

3.3 APPLICATION OF OWASP IN ICSRANK CATEGORIZATION

1. From the above discussion and table 22, one can observe that there is a repeated set of vulnerabilities, attacks and concepts which is applicable to IoT and ICS as discussed in chapter 2 have. This kind information can be classified into the following categories:
2. System or device details: The above information represents ICS/IoT devices They are viewed as the targets of attackers and defenders. Identification of targets is the first step in security. Therefore, it is classified as the main category in ICSrank categories.
3. Default Credentials: There is a repetition of this issue in 6 out of 10 categories. This shows that this issue is very common in many security levels. It is important not to ignore this issue and include it as part of critical OSITN information for ICS devices security. Therefore, it is considered as category in ICSrank.
4. Network details: The theme of the above information reflect information about the device network such as server, client, protocol ports, protocols, encryption and network location This information shows that network details have issues and create vulnerabilities. Therefore, this category is included in ICSrank.

5. Configurations details: This issue is also a major issue as demonstrated above. This issue is reflected in what is seen in Internet from access control issues, sensitive data leakage (explored in depth in chapter 4) and availability of administrative configuration links for everyone. This is seen often in online search engines such as Shodan. This category is added to ICSrank.
6. Vulnerability details: The list above mentions many vulnerabilities in each category, such as design issues, weak authorization mechanisms and every issue above is a vulnerability for an attack. This broad category is also included in ICSrank.
7. Patching details: Many ICS suffer from design issues or other security vulnerabilities. This often is solved by vendors through patching. Patching is essential in cyber security and therefore is included in ICSrank.
8. Defense details: As seen above, every issue has a cause and a remedy. Cyber security is about offering security solutions and protection. This information provides an important role for organizations. Lack of security solutions is problematic and cannot be ignored in ICSrank categories.
9. Attack techniques: Most of the issues listed above have a list of possible cyber-attacks that could happen. The offensive techniques are discussed thoroughly above. Knowledge of these techniques is the foundation of cyber security and is considered in ICSrank as well.

3.4 SUMMARY

The interconnection of devices needs to be secure to prevent attackers from intruding and posing security threats. Establishing security controls is essentials. This cannot be achieved unless, knowledge of critical information is available. OSINT and information are huge in the Internet and it is difficult to find security without direction. The development of ICSrank categories provides an important security checklist of information that are applicable to ICS devices. This categorization paves the way towards an efficient security assessment of information. The following chapter explains more in depth about ICSrank framework and the use of OSINT categorization.

We propose a new mitigation methodology by linking OSINT with current security best practices of security IoT devices. We explained in chapter 2 that ICS and IoT share many security issues for their attack surfaces. OWASP has recommended a list of protections that could be applied to IoT and to ICS as well. The ten OWASP vulnerabilities were explained in detail and linked with OSINT information types. This was to help to understand the security measures that ought to be implemented to maintain a safe IoT/ICS system. Each vulnerability had its threat agents and security weakness discussed. The proposed solution was then made to prevent attacks. Implementing security measures mitigates widespread threats. In the next and last chapter of this thesis, we lay out our final summaries, limitation and future research directions.

CHAPTER 4

ICS RANK FRAMEWORK

4.1 INTRODUCTION

In this chapter, there will be a demonstration on how to use OSINT as a tool to search for information that could give hints regarding the weakness and vulnerabilities of an ICS device. Going forward, we will call this framework the ICSrank framework. The availability of OSINT information and other common vulnerabilities for ICS devices (as discussed in Chapter 2) can make a huge difference to the security of a device. It is important to know where to look to find threats by preparing a list of resources. It is also vital to lay the groundwork on how a search will be conducted, which will be by establishing a search methodology and plan. Finally, it will be as crucial to know what to look for by establishing a knowledge base of ICS security in general. ICSrank will address the previous issues in depth as the chapter proceeds. Chapter Four will include the rules of engagement as well as an in-depth explanation of our framework methodology. A case study will also be introduced to support our data and findings.

4.2 RULES OF ENGAGEMENT

The rules of engagements (ROE) that are used in this research were inspired by [213][214][123]:

1. Interaction with devices only through available web interfaces. Banner information available in the web interface is analysed.

2. No attempt to login into devices' login portals and rejection of any request to enter a password.
3. No active scanning – passive scanning is only undertaken through Shodan or Google dorks.
4. Use OSINT sources such as Exploit database, to find related vulnerabilities and their exploits in order to use them.
5. Organization name, IP and location addresses etc. are not revealed here.

4.3 ICS RANK FRAMEWORK

An exposed online device is likely to be connected to an ICS network. The device has an IP, possibly a web interface and running services etc. (see section 4.8. for a list of possible device information). An attacker can take advantage of OISNT in order to establish an attack campaign for various motives. There are normally two attack stages for ICS (See Chapter 5 for more description). Stage 1 is called the IT (Information technology) stage where the goal is to get access to an IT network part of the ICS organization. Stage 2 is called OT (Operation technology) and is usually the most difficult stage because it requires special knowledge and skills about ICS manipulations and access to its network. Both stages are explained in depth in chapter two and five where we discuss different types of attacks, techniques, motives and impacts. For this reason, this research has divided the framework ICSrank into 3 stages:

1. OSINT Collection and categorization: Collection of related information and categorizing it into 7 categories: System details (S), Network details (N), Configuration (C), Defence (D), Techniques (T), vulnerabilities (O) and credentials. See the next sections for more details.
2. Assessment: This stage is responsible for assessing security of an ICS device – before getting into the system. The assessment is based on available OSINT data about a given ICS device that may or may not leave an impact This stage can be viewed as special ICS knowledge that an attacker can take advantage of. (See below sections).
3. Scoring: This stage is responsible for application of ranking algorithms on an ICS device. The aim is to qualitatively and quantitively assign a risk value for ICS devices based on OSINT assessments. The scoring represents a new way to look at security

level of online (in this chapter) and offline ICS devices (in chapter 6) and their level of attractiveness.

The idea of having 3 stages within ICSrank is to assess each type of OSINT individually and to measure risk for OSINT groups or categories. Each group/category can be assessed by looking at relevant and particular OSINT data as it will be explained later in this chapter and chapter 6. Each stage's OSINT data will be collected and assessed. The logic of separating or categorising the OSINT types is in order to make this OSINT categories, it is essential to know what information to look for. In order to achieve this, one should think like an attacker. A typical attack can be explained by developing a threat event model. A typical threat event model has the following elements [32] [208]:

- Target: An ICS device.
- Vulnerability: A list of potential vulnerabilities
- Attack: method of attack
- Threat vector: The angle/means that the attacker will use to execute the attack.
- Threat source: Type of threat actor: insider, outsider, malware
- Case objective: what is the motive/goal of the attack
- Potential consequences: The resulting impact

The above elements are taken into consideration while developing ICSrank assessment methodology . Those kinds of elements are what most attackers are looking for. Therefore, it is vital to have familiarity with those elements and the associated targeted ICS devices to be able to develop the necessary defense mechanisms and countermeasures.

Based on the discussion above, there 2 stages of ICS attacks, "IT" targets and "ICS" targets, it is assumed that there two types of knowledge that need to be addressed. There is the type of knowledge that is related to IT security and thus can be called OSINT-IT. This type of knowledge is what traditional cyber security research is about and is not covered in this research extensively, because this research aims at assessing ICS devices only. There is the

also the ICS security knowledge and is called OSINT-OT. This type of knowledge is the foundation of this research and is covered in depth in the following sections and chapters. The following is a brief explanation of the differences between OSINT-IT and OSINT-OT:

- OSINT -IT in general has information that benefits an attacker to find ICS targets, discover vulnerabilities, learn about access points and launch an attack to get inside the ICS network (see below sections). This type of information is like a footprint and is essential to be analysed separately.
- OSINT- OT is the type of OSINT data that an attacker needs to proceed with attack stage 2. This information is specific knowledge about ICS system, network and architecture. This type of information requires time and special skills. (See chapter 6).
- Both OSINT data types have different impacts on ICS devices. For example, OSINT-IT can help an attacker get inside a business network or an industrial organization but is unable to cause harm to its ICS operations. On the other hand, OISNT-OT can help an attacker do harm to an ICS device, after he succeeds with stage 1 (see below and chapter 6).
- Separation of data enables more accurate assessment and evaluation. This enables organizations to learn about direct root sources of risks (insider or external) and threats. Knowledge about existing threats (OSINT- IT) that only target IT assets requires a different security preparations plan.
- Knowledge about relative OSINT type can give a better picture of an organization's level of security. This would be beneficial to establish defence strategies that are suitable for IT assets and OT assets individually.
- OSINT data related to IT or OT speciality for each stage requires different skills and expertise. It is easier to separate IT knowledge from the OT domain; this can also provide opportunity for specializing. Many times, analysis is inaccurate when it is done by IT persons or journalists about ICS incidents because they lack expertise about ICS and vice versa.

4.4 EVALUATION OF ICSRANK FRAMEWORK

The approach in this thesis with regard to ICSrank depends heavily on the quality of OSINT information. A list of factors that could affect the quality of the OSINT information that can be obtained has been suggested. These factors can be used to give an overall evaluation of the OSINT methodology previously discussed in Chapter 4 and 6. There are two main factors, namely the nature and relevance of the gathered information and the reliability of the sources to hand.

The nature and relevance of the information is temporal. This means that it is only effective for a period of time before becoming obsolete. For example, if a vulnerability is discovered and then turns out to be outdated due to system patching, then the related information will also be outdated. The same factor applies if a certain vulnerability is not related in nature to a particular device or a system [180].

The second factor will be the reliability of the information sources. It is important to pay attention to the sources where the information is obtained and proceed accordingly. Some sources are formal such as established vulnerability databases. Others are informal and can be found on social media pages or forums. There is always a possibility of error and inaccuracy. In either case, cautious gathering, as well as the sceptical implementation of information, is needed at every stage to guarantee the reliability of the intelligence.

OSINT categories is part of ICSrank. It is based on basic OSINT information that affect ICS devices. As mentioned previously in chapter 3, OSINT categories were inspired from OWASP Top 10 list. In addition to OWASP list, threat modelling techniques is also a source for OSINT categories. The range of ICSrank categories were divided and named according to critical factors that were discussed in chapter 3 and in this chapter. In the following sections, an explanation of how these categories were extracted and developed.

4.5 HOW ICSRANK WORKS

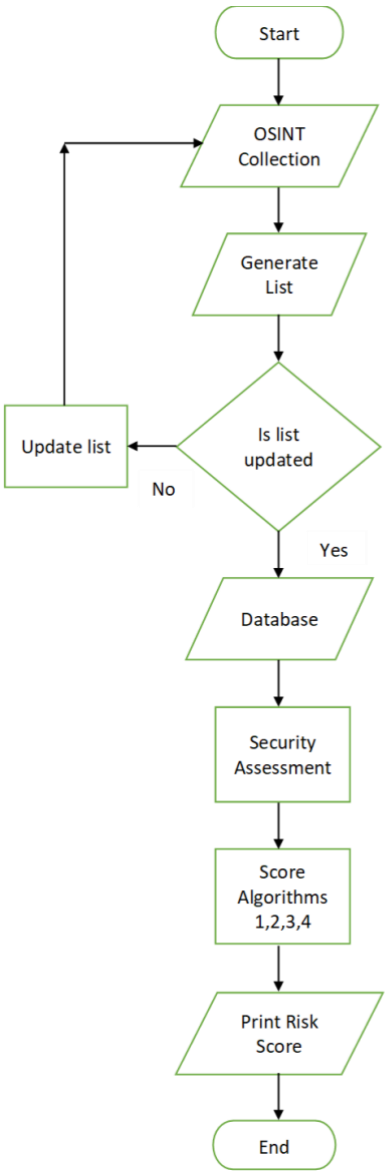


Figure 6

The flowchart (figure 6) explains how ICSrank works in general. The ICSrank is composed of 3 stages: OSINT collection, security assessment and scoring. The first stage: OSINT collection and categorization were explained in previous sections. The data can be collected either manually or automatically using scripts and APIs. The collected data is then classified into its matching categories: system (S), network (N), configuration (C), defense (D), techniques (T), vulnerabilities (O) and credentials (P). The classified data is stored in a list or a database for further analysis.

The second stage is security assessment of the collected and classified data. At this stage the data is analyzed and labeled as either “secure” or “insecure”. The criteria for this labeling is based on the first stage- categorization. As discussed in the previous section, the category exists if main subcategories are matched with existing and related information. So, if a category is satisfied with essential information, its labeled as insecure. However, if not information is available in a category, its labeled as secure. Security mainly depends on the amount of available information in OSINT. More information means less security and privacy. The output of this stage is fed to the next stage for risk analysis.

The third stage is ranking and scoring OSINT data to determine the risk. This process is composed of 4 algorithms. The data is fed first to the first 3 algorithms to determine its risk value. The risk value is determined based on the security level, category type and number of OSINT categories. Algorithm 1 is for ranking critical and high risk. Algorithm 2 is for medium risk. Algorithm 3 is for low or nil risk. The following sections explains these algorithms in depth. The fourth algorithm is used to calculate the number of insecure optional categories for a given OSINT. Finally, the risk value is determined based on the number of main categories and/or optional categories.

4.6 ICSRANK CATEGORIES

This research uses OSINT to evaluate the security of an ICS device in the first stage of attacks that could allow an attacker to discover ICS devices and/or gain access to its network (see chapter 5 for details about first stage attack campaign and chapter 6 about second attack campaign). In this section, the objective is to list and explain the critical information of a device. This information is related to online ICS device that are connected to the internet and the ICS devices that are not. This research classifies critical OSINT into categories that could lead to developing a threat risk. This type of information is called “ICS OSINT” because that information is available in public and is related to external details of an ICS environment such as online exposure, attack surfaces, access points, fingerprints etc.

In this research, ICSrank categories and types that are labeled “main” and “optional”. The main categories are system (S) and network (N). The other 5 categories: configuration (C), defense (D), techniques (T), online surface attack (O) and credentials (P). The main categories are important in terms of usability for an attacker. These types of information are essential. If they

are available in public OSINT, chances that an attacker has strong ground about the targeted ICS device. The optional ones are good bonus to make the target more vulnerable and exposed. Each main category has minimum set of main sub-categories. The reason of labeling subcategories that way is based on concepts of threat modeling discussed later.

The philosophy of labeling main or optional is that main information is critical, which can make the device insecure. Its level of security depends on available OSINT knowledge to the attacker. The amount of knowledge available can help to predict attacker skills level and resources required to perform this attack. The more knowledge available, the easier the attack as this can be demonstrated later in this thesis. Also, each main category S and N or optional category C, D, T, O and P should have its main sub-categories in case of main categories checked and its optional sub-categories in case of optional categories checked. The meaning of "checked" is the availability of information for this sub-category. See below categorizations for an illustration of these concepts.

Furthermore, the main categories are labeled this way in this framework, because of two reasons: Navigation and development. Navigation means ability to choose a target through a number of options. Those options are what is known about a target. If an attacker is attacking a particular organization, he/she has to identify its assets. Those main categories can open a door to other sub-categories and also to other major categories such as network details using further research and OSINT investigation. Development means, when certain information is available about a device, the attacker can use this information to develop further steps and goals.

The ration of OSINT categorizations is based on common threat modelling components [32] and on OSINT sources such as OWASP Top 10 list in chapter 3. Below is a summary of threat components that helped developing ICSrank categories:

- Target: System (S), Network (N).
- Vulnerability: System (S), Network (N), Configuration (C), default credentials (P), Online surface attack (O),
- Attack: Technique (T), Online surface attack,
- Threat vector: System (S), Network (N)

- Threat source: insider, outsider, malware

It is important for an attacker to do his/her due diligence about his/her target – an ICS device in this case. Collecting as much information is vital and important. It's always the first step for an attacker to obtain this knowledge. Once the target is identified, he/she proceeds to look for other vital information as we cover in later categories. The threat modeling components are expressed in ICSrank OSINT 7 categories which are broken into main and optional subcategories.

The information below is a list of ICSrank categorises that is related to the external and internal details of an ICS environment:

1. System details (S):
   - This category is about the system and the ICS device that is targeted or assessed. System information are:
     - Product name (main)
     - Product version (main)
     - Functionality, specification and process (main)
     - Firmware version (main)
     - Product type (optional)
     - Vendor name (optional)
     - Industry domain (optional)
     - Documentation (optional)
     - Processor name (optional)
     - Software name (optional)
     - Serial number (optional)
     - Design issues (optional)
     -
2. Network details(N): This category covers internal network (LAN or WAN) details only not the internet. Information that we are looking for in this category:

- Protocol name (main)
- Protocol port. (main)
- Documentation (Optional)
- IP address (main)
- Network layout (main)

3. Techniques and tools (T): This category cover information about existing tools and technology that could be beneficial to an attacker and harmful to the targeted ICS device. The following is the list:
    - Exploits available online (Optional)
    - Malware available in public (Optional)
    - Proof of concepts (Optional)
    - Security Tools (Optional)
    - Research Tools (Optional)
4. Configuration (C): This property is very powerful if it exists in OSINT. Most of ICS devices suffer from misconfigurations that could affect their security such as access control configuration. This thesis explores more in depth how this can affect the security of a device. Following sections and chapters (list) also show some real-world incidents that resulted in unwanted impacts.
5. Default credentials (P): Many ICS device come with default credentials and some are hardcoded – embedded in the hardware.
6. Online status (O): This category applies mostly to online ICS devices. It is very powerful category to consider when conducting risk assessment. The following information list applies:
    - Internet presence: ICS device is exposed in the internet or not. (Optional)
    - Available vulnerability: See extensive list of common surface attack issues (see section) (Optional)
7. Defense and mitigation (D): This category is normally disclosed by vendors when a vulnerability comes such as patching and mitigation techniques. However, there are

times when they don't. This is critical factor to consider for the device security. The following list is what we look for:

- Patching information: ICS device has a security patch or not. (Optional)
- Mitigation: Some vendors publish mitigation information about a security issue which might be useful for further security hardening. (Optional)

4.7 SENSITIVE OSINT INFORMATION

Sensitive information about an ICS device is a useful resource for attackers [124]. Normally, this information is only unnecessarily exposed because of an error made by administrators or users such as maintaining default settings, credentials, or configurations. It can also be a design fault by vendors such as hardcoded credentials. In this framework, sensitive information is classified into 18 types (see the table below for details). This categorization was chosen to allow us to distinguish between the types of information acquired. Most of the items on the list below were borrowed from Google Dorks [124]. These items are commonly used in passive penetration and reconnaissance [125].

Table 6: OSINT Information types

File extensions (V1)
Directory listings (V2)
Configurations file (V3)
Logs files (V4)
Backup files (V5)
Database dump files (V6)
Client-side code files (V7)
Password reset pages (V8)
Server status pages (V9)
Other meta data (V10)
Technology details (V11)
Images (V12)
Network and Physical Location (V13)
Protocol ports (V14)

Vulnerability data and advisories (v15)
Error messages (V16)
Default credentials (V17)
Design issues (V18)

The above table (Table 6) lists examples of sensitive information sources, types, and usage. For example, log files can be a source of information with a type logging and can be used to find credentials, network, technology, and general device information. This table provides a classification of sources that yield OSINT information about a device. Each source is labelled with a letter "V" and a number that follows. The labelling system classifies that information as a form of potential source of a vulnerability and that's the reason it's labelled as a letter "V".

File extensions are used to indicate the type of file; for example, .txt is a text document, .doc is a word document, .pdf is a pdf document. Directory listing is a web server function that displays all the web-server files when the index file is not present and the default.asp in the particular website. The configurations files are files used in configuring parameters and initial settings for the computer programs. They are used in operating system settings, server process and other user applications. Log files record the events that happen when software is running. It also records communication between communicating users of the message relaying software. A backup file is an archive of the folders and other files in use so that they can be restored if there is loss of data. Similarly, database dump files are used to archive the data in the database so that they could be restored if there is loss of data [161].

Password reset pages are used to reset the usernames and passwords if the client forgets the password or a different password has to be used for security purposes. The password reset pages have to be authenticated through the authorised means like email links and one-time codes to verify the user. The client-side code files are files sent from the web server to the end-user's computer via the browser to run the specific scripts. A server status page informs the client when there is downtime or if the server is not functioning properly. This is especially the case when the server is under maintenance or when there is a security breach that has to be resolved before any access can proceed. Other metadata are used to provide information about the other data stored in the database. Technology details give the information about the systems in use, for example the security features, the operating systems etc. The images in the ICS

system may just be used to identify the devices in the network. An image is a better expression of the device rather than writing the device's name, for example, an image of a bulb is better than the name 'bulb' for the lighting in the IoT.

Network and physical location give the addresses of the network and the geographical address to make it easy to trace the source. Protocol ports in computer networks are the endpoints in communication in either wireless communication devices, or wired devices. They define the logical channels used e.g. TCP, SMTP, UDP among others. Vulnerabilities data and advisories are weaknesses in the system that can be easily exploited by the threat actors. Error messages are the notifications sent to the relevant people on the errors in the system due to things that may not be functioning in the proper manner. They include security warnings about data transfer, failed login attempts and other errors. Default credentials are the computer-generated details given to the first-time user of the system [166]. These default details are often changed by the user to customize it to their specifications, provided they meet the security restrictions. Finally, the design issues are the inherent features or characteristics of the operating systems or the hardware components.

4.8 TAXONOMY OF OSINT THREATS

We have developed a taxonomy of OSINT threats based on OSINT information types in table 8. Possible threats are inspired from our "attack" section 2.6 in Chapter 2 and are associated with that information to demonstrate how an attacker could manipulate this kind of information. The association between OSINT types and the corresponding threats are based on the MITRE ATT&CK for ICS Matrix [5]. That matrix is a collaborative research project that addresses common tactics and techniques used by ICS attackers. It is also based on OWSP Top 10 discussed in chapter 3.

The list of attacks is not exhaustive; not all of the attacks discussed in Chapter 2 are listed and some of them are for demonstration purposes only (See list in Table 7). An extensive list of threats and scenarios will be considered for future academic work.

Table 7: List of Cyber Threats

Data impairment (T1)
Data drop (T2)
Data counterfeit (T3)
Data disclosure (T4)
Frequency jamming (T5)
Data collision (T6)
Router Data Compromise (T7)
Data flooding (T8)
Data eavesdropping and interception (T9)
Denial of Service (DoS) (T10)
Data tempering (T11)
Unauthorised access (T12)
Data spoofing (T13)
Rouge Access point (T14)
Man-in-the-middle (T15)
Data scrambling (T16)
Removable media threat (T17)
Physical security (T18)
Social engineering (T19)
Software attacks (T20)
Faulty hardware (T21)

Table 8: Taxonomy of OSINT Threats

Type of Information	Possible Threats *[5] [54]	Note **
File extensions [V1]	T4, T3, T11, T12	Attacker can target sensitive files knowing their extensions
Directory Listings [V2]	T4, T3, T11, T12	It could lead to an administrator folder and sensitive information
Configuration file [V3]	T4, T3, T11, T12	Extensions: .config, .conf, .cgf, .ini. It is source of sensitive information such as credentials, location of directories, device details, etc.
Logs Files [V4]	T4, T3, T11, T12	It reveals: Passwords, IP address, usernames, etc.
Backup files [V5]	T4, T3, T11, T12	Extension: .bak, .old, .zip
Database dump files [V6]	T4, T3, T11 , t12	It contains:Usernames, passwords, emails, etc.
Client-side code files [V7]	T4, T3, T11, T12	It reveals info about server, hidden credentials or technology
Password reset pages [V8]	T4, T12	See description of T4 & T12
Server status pages [V9]	T4	See T4
Other Meta Data [V10]	T4	See T4
Technology details [V11]	T4, T20	Examples: Hardware, software, vendor, version, etc.
Images [V12]	T4	Example: Images of a plant through a webcam or location map or network diagram
Network and Physical Location [V13]	T1, T4, T17, T18, T20, T16, T5, T10, T2	See Threats description
Protocol ports [V14]	T4, T4, T8, T10, T2	See Threat description
Vulnerability data and advisories [V15]	Based on vulnerability	Depends on vulnerability type
Error messages [V16]	Based on Error Type	It reveals:
		Sensitive information, information about server, technology, software bug, vulnerabilities, directory paths, files
Default credentials [V17]	T12	See T12
Design issues [V18]	T21, T8, T10	See Threat description

* Section 2.1.6 in Chapter 2

** “Reveals” is used in a context of probability not one of certainty.

4.9 ICSRANK ALGORITHMS

4.9.1 Introduction:

ICSrank is composed of 4 algorithms for scoring risk of ICS devices and their OSINT. The goal here is to evaluate OSINT categories that were collected and make a decision to determine their risk level. The higher the number of insecure OSINT information the riskier the device. The higher the severity, the more critical the potential vulnerability is. Below are the ICSrank algorithms that are developed in this research and are used for ranking.

Algorithm 1: Both System (S) and Network (N) details are insecure

```
1 List = S, N, C, D, T, O, P
2 input: List
3 initialize: Status, List
4 loops inside List
5   If S and N = no and C and/or D and/or T and/or O and/or P = no then
          Status = critical
        else Status = high
         endif
  endloop
6 return Status
  output Status
```

Critical risk:

An ICS device is labeled as critical risk when both its system (S) and network (N) details are insecure, known and available in public OSINT. In addition, it has at least one or more optional insecure categories.

High risk:

An ICS device is labeled as high risk is when both its system (S) and network (N) details are insecure, known and available in public OSINT.

Algorithm 1 is applied when both the system (S) and network (N) details of an ICS device are known. In this case its risk label would be “high”. The reason is because if these information about the target is available to an adversary, there is a big chance that he/she can exploit this device.

However, if other optional categories are known to that device, the risk will increase because there is other valuable information available in OSINT that would make the target even more attractive and thus easier to conduct an attack. In that case, the device is labeled as “critical”.

This algorithm works by 6 stages. The First, second and third lines reads the list of categories available about the target. Normally this list is supplied manually or by a database. This list is assessed and updated regularly and fed to ICSrank algorithm. Then it loops insides the list and tests if there are insecure categories. That conditional loop and if-statement will filter the categories to either “critical” if it finds insecure optional features or “high” as default value.

The quantitative scoring method of ICSrank is really simple, flexible and adjustable. If a device is “high” risk, meaning that both system (S) and network (N) details are insecure, the score will be 100%. So, if to choose a score of 10, the risk value will be 10. If a high-risk device is discovered with extra optional insecure features, it would be labeled as” Critical”. Meaning its score will be higher than 100%, thus requires immediate attention. The higher the number of optional categories a device has, the riskier the device.

For example;

Suppose a “high” risk device X is scored 10/10

If ICSrank adds one more optional feature, it would be scored as 11

If device X has 5 insecure optional features, it would be scores as 10*5

If ICSrank removes 1 insecure feature from device X, the score will be 10*4.

Algorithm 2: System (S) details or Network (N) details are insecure

---

1 List = **S**, **N**, C, **D**, **T, O**, **P**

2 input: **List**

3 initialize: **List, Status**

4 loops inside List

5 If S or N = no then

Status = medium

Endif

Endloop

6 return Status

output Status

Medium risk: An ICS device is labeled as medium risk is when either its system (S) or network (N) details are insecure, known and available in OSINT.

The second case to apply algorithm 2, is when either the system (S) or network (N) details of an ICS device is known. It is labeled in this case as “medium”. That’s mainly because there is a 50% chance that the attacker would be able to attack an ICS system. A successful attack must contain knowledge about both the system and its network details such as device name, IP address, port number etc. Knowledge about a system alone means nothing if an attacker can’t reach and allocate the targeted device through the internet. Vice versa is also correct if you know everything about the network details and knows nothing or little about the system, chances the attack would fail and would not be risky or less risky.

Even if optional insecure categories are known, still the attacker has to learn about the system or network, which might take time, resources and effort. Attacking Medium risk devices require medium to advanced attack skills, because of the lack of knowledge of one of the main categories. There might be knowledge about techniques and tools (T) - optional here - about the target, still there must be an effort to collect the other half of main categories.

This algorithm works by 6 stages. The First, second and third lines reads the list of categories available about the target. Normally this list is supplied manually or a database. This list is updated and assessed regularly and fed to ICSrank algorithm. Then it loops insides the list and tests if there are insecure main categories. That conditional loop and if-statement will filter the risk level of a device to “medium” if it finds one of the main features insecure.

This thesis argues as stated above that a main category shapes 50% of risk value of a device. Therefore, if a proposed measurement for risk scoring is given 10, a risk value for a given device here is always “5”. However, like the previous algorithm, if optional categories are added to a device its value would increase up but not reach value 10. Value 10 is reserved for high and critical risk devices only. However, if a medium risk device is ranked 9, it’s still more risky and attractive than a device with score 5. Vice versa is also correct, removing insecure features of a device would lower its score.

For example;

Suppose a medium risk device X is scored 5/10

If ICSrank adds one more insecure optional feature, it would be scored as 6

If ICSrank removes 1 insecure feature from device X, the score will be 5

Algorithm 3: System (S) details and Network (N) details are secure

```
1 List = S, N, C, D, T, O, P
2 input: List
3 initialize: List, Status
4 loops inside List
 5 If S and N = yes and C and/or D and/or T and/or O and/or P = yes then
            Status = none
      else
            Status = low
    endif
6 return Status
   output Status
```

Low or none risk: An ICS device is labeled as low or none risk is when both its system (S) and network (N) details are secure, unknown and unavailable in OSINT.

The third algorithm is applied when both the system (S) and network (N) details of an ICS device are unknown and secure. It is labeled in this case as “low” or “none”. That’s mainly, if a device is unknown nor its network addresses, chances it won’t be targeted by intruders.

If all OSINT categories both main and optional for a particular device are secure, unavailable and unknown in public, the device is labeled as “none” risky. However, if certain optional categories or partial main features are insecure and known, that would make that device a low risk. The difference between low and none risk is the former, there are hints of insecure features that are available in OSINT, that could encourage an attacker to dig for further information. While the later means that there no traces of main or optional information about a device, thus no hints or clues. Low risk devices require advanced skills in order to launch an attack, because an attacker has to apply effort and resources which be costly in terms of time, money and expertise.

This algorithm works by 6 stages. The First, second and third lines reads the list of categories available about the target. Normally this list is supplied manually or by a database. This list is assessed and updated regularly and fed to ICSrank algorithm. Then it loops insides the list and tests if there are insecure categories. That conditional loop and if-statement will filter the risk level of a device to “none” if it finds all the main and optional features secure. Otherwise it would label it as “low” risk if only system (S) and network (N) details are secure.

The risk quantified in this case is estimated below 50%. So “none” risky devices are zero when all device features are secure, and risk is built up as soon there are insecure optional features are discovered. If an insecure main category such as system (S) or network (N) is discovered, the device is not low anymore and it would be promoted to medium risk in case 2.

For example:

Suppose a “none” risk device X is scored 0/10

If ICSrank adds one more optional insecure feature, it would be scored as 1. This is labeled as “low” risk.

If ICSrank removes 1 optional insecure feature from device X, the score will be 0. This is labeled as “none” risk.

If ICSrank adds one main insecure feature, it would be scored as 5. This is labeled as “medium” risk.

Algorithm 4: Update insecure optional categories

```
1 device
2 List_size = number of insecure optional elements
3 input: device, list_size, risk_value
4 initialize: device, list_size, risk_value
5 if status = critical
    print * for each optional element in the list
    print insecure optional elements in list
print risk_score + “*”
  else print number of insecure optional elements in list and print the insecure elements
       print risk_value + number of insecure optional elements

 endif
```

Update algorithms are responsible to update the status of insecure optional features for a given risk label. The extra insecure optional features could be expressed as stars "*". More stars mean more criticality and risk. Vice versa is correct too. In a nutshell, the device can become more/less risky depending on number of insecure optional features. As demonstrated in algorithm 1, high risk label becomes "critical" if it has one or more insecure optional categories. The stars are applied to high risk labels only. In Medium, low and none labels, optional categories are represented as a number.

Algorithm 4 is also applied to other risk labels: medium, low and none. None risk devices can be upgraded to low risk, if it has insecure optional categories. A low risk device with stars is riskier than device with no insecure optional. The same is also applied to medium risk devices, one with optional is riskier than no optional. This goes on to all risk levels. One important point, algorithm 4 don't upgrade risk – except none risky – to another level. The only categories that raise a level are the main categories system (S) and network (N) details. This is explained separately under each algorithm.

4.10 ONLINE SIEMENS S7 PLC

The information detailed below was gathered from the following sources (see Chapter Three for more information):

Device hunting and Exploring: Shodan [129] and Google

Default credentials: SCADAPASS [130]

Filters and Cheat sheets: Google Hacking Database (GHDB) [124] and OWASP SCADA security [131]

Advisories: ICS-CERT [132] + Shodan Exploits [133]

Sample Name: Siemens Simatic S7 PLC

4.10.1 Shodan

Shodan's industrial systems section [134] was used and Siemens was selected. The search operator was port="102". Different PLC brands were returned, but we chose Siemens as a demonstration. Some administrators change the default port for Siemens, and port 102 is sometimes used for many purposes and not just for ICS. Siemens devices are identified by looking at the banner's information.

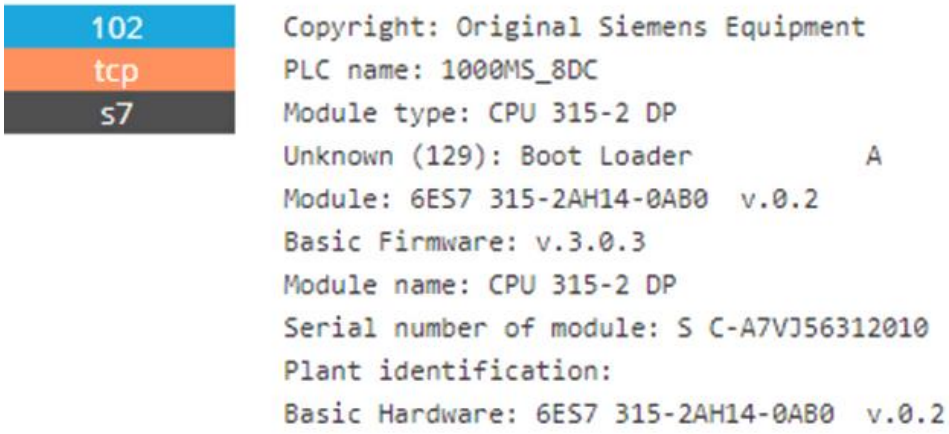


Figure 7:Shodan analysis results of a Siemens equipment device

4.10.1.1 THE GATHERED INFORMATION:

In this section, we list the information (based on Table 10) that we managed to acquire for Siemens PLC. Each item of information is labelled based on the level of risk (see section 4.9), here a risk value for illustration purposes. It is subjectively based on an organization's priorities.

1. Port number (V14): The default port for Siemens PLC is 102. The port number risk level depends on many factors. If a port is open and leads to unauthorized access to an ICS device, then it will be labelled as insecure. However, if the port number is closed and secured then it is assumed to be low risk secure. The port number is part of the network details (N) category and is an essential for this category to classify N as insecure.

2. Device specification (V11): Device type, version, modules, firmware and serial number. [This is a main part of the system category (S). This OSINT can lead to further research in behalf of the attacker because its identified almost comprehensively. S is marked as insecure in this case. This information can be escalated, by (for example) combining it with other Vs and attack tools (T), such as searching for existing vulnerabilities (O), exploits (T) or even reverse engineering (T), which can make the PLC riskier, thus this feature is marked as insecure. Administrators can hide details about the system, so hackers do not take advantage.

3. Location (V13): Physical and IP addresses available (this is not shown for ethical reasons. However, this information was available online and its nor mentioned here for privacy and ethical reasons. This information is categorized under the Network (N) and Online (O) categories. This qualify N to be labelled as insecure.

4. Configuration and server status (V3) (V9): Web access to a configuration wizard via an open http port 80 (see Figure 8). The HTTP status code is 200, which means it allows communication without authentication with the server. That value is a default return value for HTTP servers [135]. This is risky and default configurations must be changed. The green arrow opens a link to the configuration page. This information is part of the configuration (C) category and thus its labelled here as insecure.

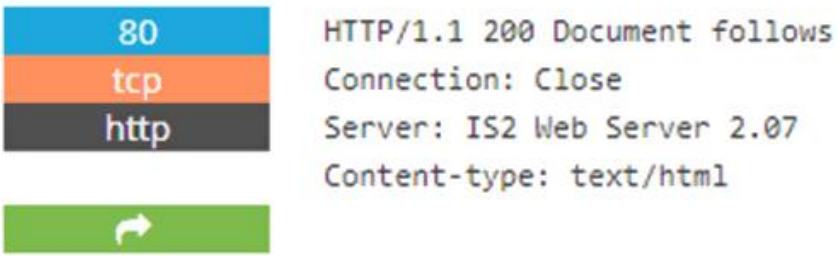


Figure 8:Shodan analysis results of the device's connection and server status

5. Other Meta data (V10): Information such as ISP name, organization name, last update time and other services ports. This information is classified as network system (S), (N) and Online (O). This information increases the risk of a device. Its labelled as insecure.

4.10.2 Google Dorks

Using Google Dorks, many results that contain login portals to Siemens PLC web interface can be obtained that show many configuration and information clues. The login portal, which requires credentials, can either be accessed by knowing default credentials (V17) part of credentials category(P), or through a vulnerability (V15) an online category(O) that could lead to other Vs such as configurations (V3) a configuration category(C), log files (V4) another configuration category(C), server status (V9) a network category(N), technology details (V11) and possibly other sensitive data. The above categories are insecure. The filter used here for Siemens Simatic S7 is inurl:/Portal/Portal.mwsl (See figure 9):

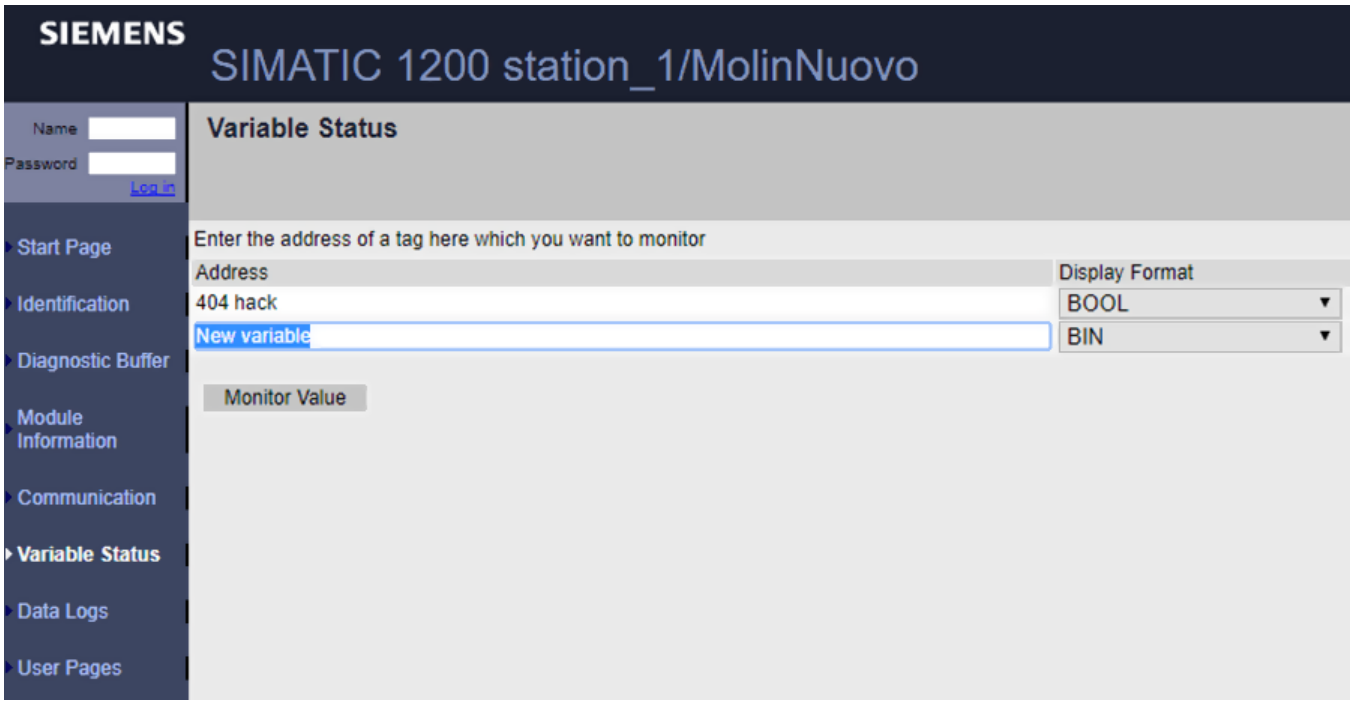


Figure 9: Google Dorks Results

4.10.3 Miscellaneous OSINT

Default credentials: The passwords list was taken from the SCADA Strange Love project [130].

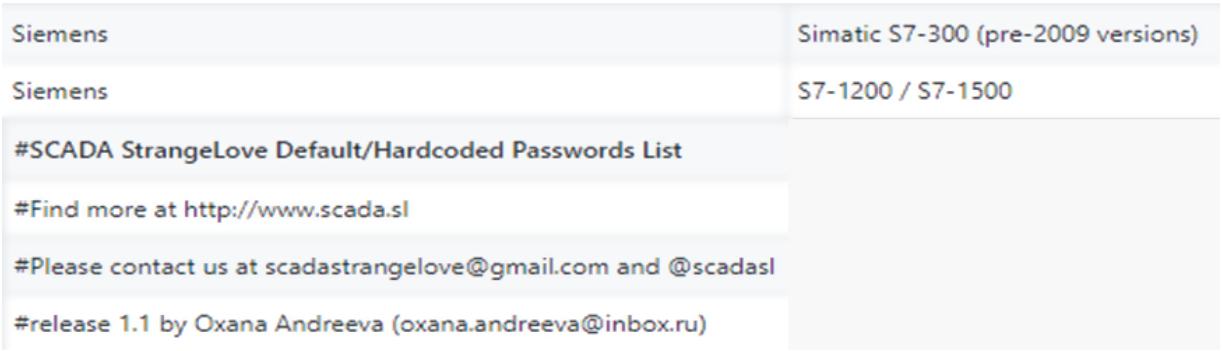


Figure 10: Default ICS devices login credentials

The above diagram shows us a list of default ICS devices logins and passwords [130]. For example, many use the following credentials: “admin. admin” or “admin”/” root” + “password”. [V17]. This is an insecure credentials category.

4.10.4 Databases

We arrived at vulnerabilities (V15) information about our sample from the following vulnerability advisories database:

4.10.5 ICS CERT

Table 9: Siemens device vulnerability information [136]

Siemens	SIMATIC S7-1200
Bug	CROSS-SITE REQUEST FORGERY
CVSS	CVE-2015- 5698 :6.8
Attack/Impact	Attack PLC from its web server, if the victim is active
Port	Remote, Port 80/TCP and Port 443/TCP
Difficulty	Medium Skill
Industry	Chemical, Critical Manufacturing, and Food and Agriculture
Year	2015

As can be observed from the table, the vulnerability of Siemens PLC has a CVSS score of 6.8 considering information such as port numbers (N), model (S), attack methodology (T), sector (S) and bug type (O). This will be ranked as 6.8 if it passes ICSrank risk criteria. This information is considered to be very important and dangerous for an attacker to learn about a device, especially if they find it online. There is a larger problem is if the device is not patched and up to date. This information is really valuable as it provides insecure features such as system (S), network (N), online (o) and techniques (T).

4.10.5.1 SHODAN EXPLOITS

Considering Shodan's Exploit section, more examples of vulnerabilities regarding Siemens PLC can be seen. They are listed in the figure below:

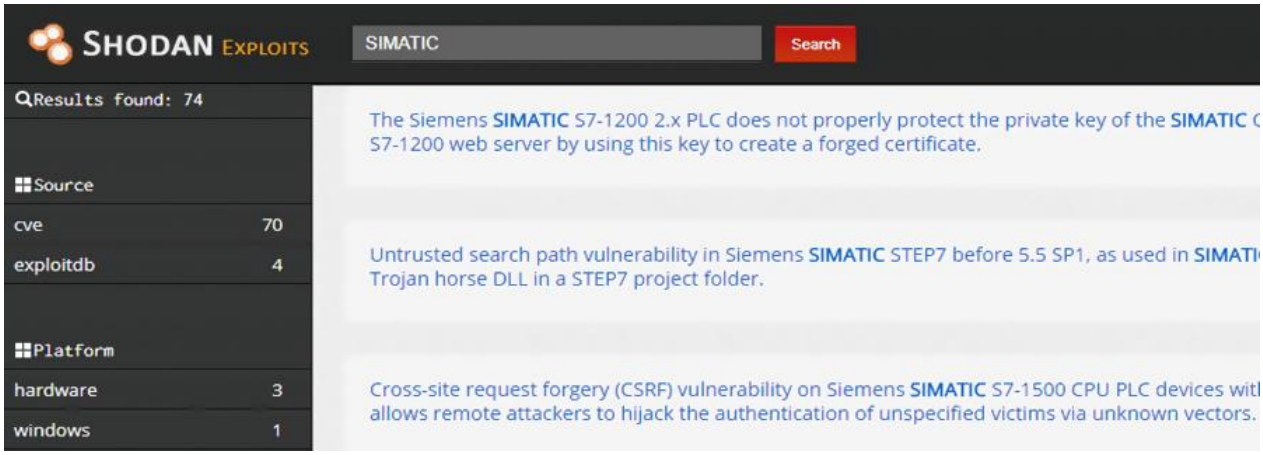


Figure 11: Shodan's Siemens PLC exploit findings

Figure 10 above is a snapshot of Shodan's detected exploit. It allows users to search for devices and their vulnerabilities. If vulnerabilities exist, we will not take its CVSS score for granted unless it passes the framework test. This information is about system details (S), techniques (T) and online (O), which all are insecure.

4.11 RESULT REPORT FOR THE SIEMENS PLC

To conclude the framework, we move on to the final stage by calculating the level of a device risk (see section 4.4.1). This allows an ICS device to be ranked.

4.11.1 PLC OSINT assessment

We arrive at the following vulnerabilities and their security level:

Table 10:: Vulnerabilities and their corresponding security level

OSINT	Bug Symbol	Category	Secure?
Port Number	V14	N	No
Device specification	V11	S	No
Location	V13	N	No
Configuration and server status	V9	C	No
Other Meta data	V10	N	No
CVE	V15	O	No
Default credentials	V17	P	No
Configuration	V3	C	No
Techniques	V15	T	No

This case study shows how to apply ICSrank for online and internet-connected ICS device, which is the Siemens PLC. The device was discovered randomly in Shodan search engine. That lead to further research exploring this source and other OSINT sources as explained above, Based on ICSrank OSINT categories, plenty of categories were found insecure and available in public OSINT.

ICS-CERT database and Shodan could be considered the first sources to be utilized by researchers and attackers. They are rich of many ICS devices with plenty of information and updated regularly. For example, Shodan gave extensive system details (S) about Siemens PLC. Interestingly, it gave critical and insecure network (N) and configuration (C) details. There were hundreds of Siemens PLCs online (O)with so many open ports. Many have a link to a configuration portal (C) which if exploited, it could be a main access to an ICS network. ICS-Cert is really critical for the security of ICS devices. A rich information of vulnerabilities exploits and tools (T) are discussed about many types of ICS devices including our case study. Google is also valuable to find online ICS devices as well default configuration files (C) by using special filters. GitHub has exploits (T), proof of concept (T) and password databases (P) for ICS devices. It seems that the collaboration of security community has exposed so much critical security information about ICS devices. Our research has observed that many exposed

ICS devices are still not secured and using old insecure firmware versions, insecure websites and default credentials.

ICSrank assessment of system details (S) has obtained its data from Shodan, ICS-CERT, Google and GitHub. Most of system details sub-categories are checked as "insecure" thus the assessment of S is insecure. The same sources have aided this research to get network details (N) about this target. Most of its sub-categories are insecure, except the network layer category. the network layer is about the internal network of this ICS device which can be obtained if an initial access was established using the current gathered intelligence. Online ICS devices still be ranked as insecure even if this information is unavailable because of the availability of critical information in this case study such as default credentials (P), online presence (O), existence of vulnerabilities (O) , configuration link (C) and exploits (T). However, non-internet connected ICS is a different matter when it comes to knowledge of network layer, because they are not present online and it's hard to know how to connect to the target. Other optional categories such as credentials (P), techniques (T), configuration (C) are available in OSINT for Siemens PLC discussed here.

It's worth to mention that, online Siemens PLC are riskier than non-online devices, even though they share many of insecure features. The difference is Siemens PLC that are insecure and available in Shodan are already exposed (O). All it takes is to use one of the open source exploits and techniques (T). It does not require advanced skills in that case. However, Siemens PLC that are hidden inside local network (N) and are not exposed online (O) require more advanced skills to acquire deep network details to reach this PLC. It evens require knowledge of other access methods through other threat vectors such as gaining access to an IT network or through other online devices, which again is a lot of work and research.

So far, this chapter has covered comprehensively how to apply ICSrank framework on an online ICS device from identifying, gathering information, to assessment and finally scoring. In chapter 6, this thesis discusses non-online ICS devices and how to apply ICSrank framework on such devices.

4.11.2 OSINT Scoring

Looking at the assessment results in Table 15, The Siemens PLC has the following categories: system (S), network (N), configuration (C), online (O), technique (T) and credentials (P) labelled as insecure. In this case study, Siemens PLC is ranked by using algorithm 1, because both system (S) and network (N) details are insecure. In addition, all the rest optional categories are insecure too. The qualifying score for this device is critical.

This device is scored 10/10 *4. The 10/10 is for the reason that both system (S) and network (N) are insecure. The extra 4 stars means the PLC has 4 extra insecure features. As explained above in the algorithm section that having extra optional insecure features for a high-risk device makes it critically risky.

4.11.3 ICSrank vs CVSS for online ICS devices

At this stage, a comparison between ICSrank metric of Siemens PLC with its current CVSS score is conducted.

CVSS score for SIMATIC S7-1200: 6.8 = 1 available software vulnerability

ICSrank score for SIMATIC S7-1200: 10 *4 = 2 major insecure features plus 4 insecure optional features

It can conclude that CVSS has identified only 1 software vulnerability for this PLC which is cross-site request forgery. This bug can be exploited online through the device's configuration portal by injecting malicious code. CVSS has missed plenty of other insecure features that are available in OSINT, which ICSrank managed to identify and assess. Also, the identified bug by CVSS is ranked 6.8 which is not high risk at all. That would mislead organizations who assess their ICS devices following CVSS, by ignoring it or not classy it as important.

The context of following advisories by CVSS is not complete and comprehensive. It is important to understand the whole threat system which was explained in section 4.8 in order to construct better threat scenarios and be able to decide the required defences. Therefore, ICSrank is built on this threat system to make it more practical in ICS security. CVSS is

developed under the traditional IT security mentality which treats vulnerabilities individually. This is not recommended in ICS security.

Another concept is missing in CVSS system, is ranking the vulnerability individually. This method is flawed, for the above reasons and also for the reason it neglected the differences between online and offline device (non-internet devices). It makes a big difference between the formers. An online device with that CVSS score, according to ICS rank is considered critical. However, a similar device model is hidden in a network and is not connected to the internet might require a different score especially if that configuration portal is only accessed locally.

4.12 SUMMARY

In this chapter, a methodology and framework ICSrank for assessing the risk of an online ICS device have been demonstrated. Chapter 6 utilizes this framework for non-online ICS devices. This research has also provided qualitative and quantitative analysis and explained our rules of engagement with all ICS devices. In addition, it has provided a case study for PLC that is believed to be linked to a control system. This chapter has also proposed a new taxonomy based on OSINT and argues that it is not possible to find them all for one target.

It was also developed a taxonomy of OSINT threats that are associated with attack stages. The taxonomy is based on OSINT information that is available in table 11. Unfortunately, this research has not covered or extracted other OSINT information as proposed in Section 4.8. The list in section 4.8 is a benchmark list that is used to assess an ICS device. This research argues that passive information gathering is a good start to give a roadmap for the organization to assess what security aspects need to be taken as priorities. It was demonstrated that the risk level of a device does not depend exclusively on the number of vulnerabilities but also on the severity of them. However, if two devices have a similar risk level, the quantity based on ICSrank algorithms will be of importance. It shows that there is more than one scenario that could be exploited. This thesis argued that CVSS (See Chapter 2) is not enough to estimate the risk of vulnerabilities. It is out of this research scope to analyse and discuss all factors that affect the security of a device, our study is a step in that direction. OSINT and threat intelligence can greatly influence the security of ICS devices. In the following chapter, it lays out a cyber-physical threat model. It explains the two stages of ICS attacks: stage one IT-attacks

and stage two OT attacks. The next chapter identifies threat actors, vectors, capabilities and consequential impacts.

CHAPTER 5

ICS THREAT ANALYSIS

5.1 INTRODUCTION

In this digital era, cyber presence and the use of digital service tools have practically become necessities for business organizations of all types. With such prominent use of digital technology within the business context, there is also a notable rise in the number of cyber-attacks taking place against businesses and individuals. The precise mechanisms and the impacts of such cyber-attacks can vary significantly depending on the skill and objectives of the attacker [150]. Once successfully implemented, impacts may range from the simple, passive stealing of confidential information to the complete sabotage of the equipment and systems.

In this chapter, this research discusses the security of cyber-physical systems by linking cyber threat operations with this research's physical model "Gas Cylinder filing". This research, therefore, explains vulnerabilities, attack methodologies, goals and objectives, and the possible impacts on physical systems. It also demonstrates ICS specific actions as responses to the penetration of a cyber-domain, as well as an ICS threat model with a corresponding cyber-attack. The case study is built around a safety PLC in a gas system. Consequently, this research illustrates the connection between cyber-attacks and ICS attacks.

5.2 WHO ARE THE ATTACKERS?

Cyber-attackers targeting ICS and online servers can be broadly categorized into the following two groups.

- **Insiders:**

  These are employees, who according to research [148] represent the riskiest threats to security breaches either intentionally or accidentally. They have direct access to the system, or the ability to deploy convenient measures allowing them to physically access the system and attack it. A cyber-attack by such persons is therefore very different from the way an outsider would attack the system due to their having direct access such as login credentials, or physical access to the hardware components of the system [148].

- **Outsiders**

  Outside attackers on ICS systems include people who are not directly affiliated with the business and system owner. They have no direct access to the system, software networking or hardware. There are many types of outside attackers ranging from hobbyists to professional hackers, and government agents [146]. See Chapter 2 for more description of their general motivation. These attacks require knowledge of computers and networking technologies as such information has become essential when hacking and attacking a system. In some cases, amateur cyber-attackers do not actually hack the system; rather they deploy DDoS (distributed denial of services) attacks. These disrupt the service facilities without actually getting into the system through hacking the system.

5.3 TARGETED DEVICES

The targeted ICS devices assumed in our study are:

- **Programmable Logic Controllers (PLC):**

  PLC is a computer system that is specifically designed for use in industrial scenarios; they are also well adapted for the control of manufacturing processes. This can be highlighted by the use of PLCs to control assembly lines in manufacturing and for

robotic instruments. This is possible as they are actually designed for such industries with the following in mind: an automated fault diagnosis, easier programming, and performance reliability [144]. Modern-day PLCs also include the functionalities of networking, distributed control systems, process control, motion control, and relay control.

- **Remote Terminal Units (RTU):**

  RTU refers to a microprocessor device that is used for the purpose of creating an interface to an ICS through telemetry data transmission. This unit receives instructions from the connected devices and transmits it to the master system.

- **Supervisory Control and Data Acquisition (SCADA):**

  SCADA is an architecture of control systems used for the purpose of supervisory management of ICS. SCADA connects with other devices in a system to gather data using PLCs and RTUs while making use of networking and GUI for data collection.

- **Human Machine Interface (HMI):**

  HMI refers to the specific user interface used in industrial machinery and computing systems that allow a human operator to control the controller of the system. A typical HMI includes components of both controlling automation and signalling.

- **Master Terminal Units (MTU's):**

  MTUs are in fairly common use in SCADA systems. MTUs are the devices that provide instructions and commands to the RTU, which can be located remotely in different places. The MTU has control over RTUs, collects data from these units, keeps the information stored, and processes the data to show it to the operator using the HMI user interface [147].

- **Intelligent Electronic Devices (IED'S):**

  IED is a term that is commonly used in the electronics industry for microprocessor controller devices that are used as controllers for various types of energy management equipment like capacitors and circuit breakers.

5.4 ATTACK GOALS AND MOTIVES

Chapter 2 listed common attack methods on ICS assets. In this chapter, research continues what was discussed earlier in chapter 2 that an attack on ICS is normally performed in 2 stages. However, not all attacks have similar motives and goals after they succeed with stage 1, which is to get inside the ICS network. Therefore, it is important to understand the motives of attacks pre-stage one. The end goals of the cyber-attacks and breaking into an ICS network are shown below [32]:

- To change system/device/network configuration and behaviour.
- To make inaccurate changes to system/network information sent to operators.
- To tamper with safety systems.
- To inject malicious software such as malware.
- To steal information and carry out espionage.
- To alter sensitive information.
- To get inside an ICS device/system:

Previous chapters discussed the type of information that an attacker can use to gain access to ICS devices. However, there is a need to learn the methodology that most attackers follow to gain control over a system. The following figure (Figure 12) is an illustration of attack methodology “Kill Chain stage 1” for the cyber stage. The “Kill Chain” is a model developed by Assante and Lee. It is based on the “Cyber Kill Chain” developed by Lockheed Martin analysts [206]. Stage 1 models a campaign that attackers follow against IT or a business network. They also developed “Kill Chain Stage 2” (see Figure 13) [206]. Stage 2 is a model that explains the campaign that attackers follow against ICS.

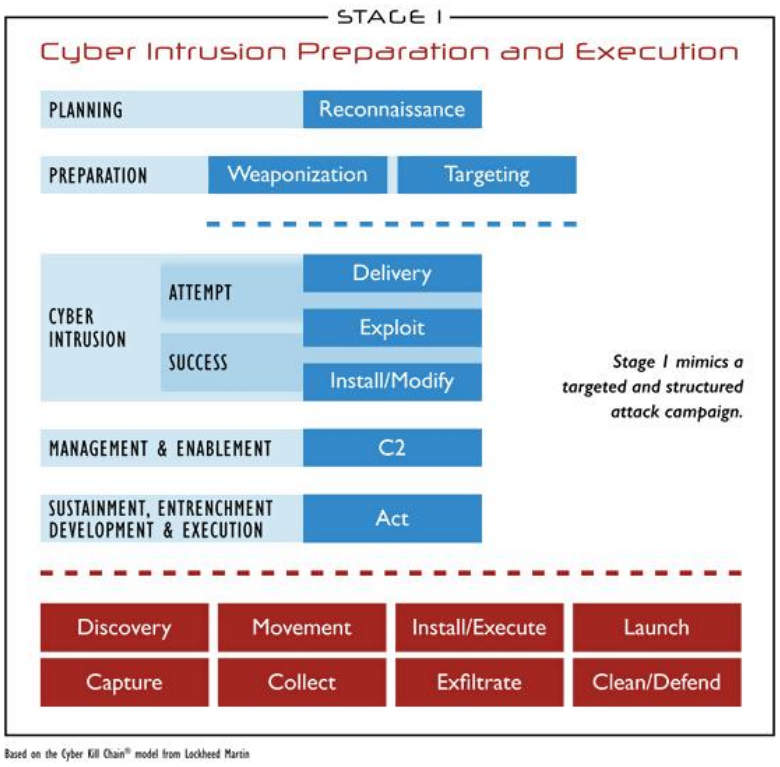


Figure 12: Cyber-attack stage by Assante and Lee [206]

In previous chapters, this research focused specifically on the "Reconnaissance" phase. This is the phase where OSINT gathering takes place. It is a stage where an attacker gathers information about a target system. The following stages: weaponization, delivery, exploitation and gaining command and control are discussed in brief in chapter 2. There are plenty of attack methods to exploit a system. It is out of this research scope to discuss them all in depth. This research illustrates a few of them for the sake of threat modelling of our case study.

5.5 ICS ATTACKS

In previous chapters, this thesis established the OSINT information that an attacker can use to gain access to ICS devices/network. However, gaining entry into an ICS network is not the same as an IT network. IT networks normally share commonalities in assets, design and architecture. There are plenty of guides and resources publicly about IT assets that make it easy for an attacker to gain entry. However, the ICS network is composed of many engineering and mechanical processes that require different skills and expertise and most importantly knowledge about its architecture which are not available in public. Industrial organizations have different ICS architectures that require an attacker to learn each individually if he/she

wants to learn an attack. The attack cannot be copied with other entities. Another difference between IT and OT is depending on the type of compromised device that an attacker has gained control over, that makes the scenario to be different. For example, if a PLC device is connected to the internet, an attacker might or might not be able to cause an impact. It all depends on the administrative security role that he has established when he compromised that device and whether or not that PLC is crucial to the production. The level of ICS network security is not the same for most organizations. Some are weak, while others are secure. Poor ICS networks might expose ICS devices directly to the internet as we saw in Shodan in chapter 4, making it easy for an attacker to make an impact. On the other hand, other ICS networks have a more complex architecture that requires long, deep planning and research.

This research applies some of SANS model concepts [206] to understand how an ICS attack is conducted after a successful cyber-attack. The model shows that an attacker applies some of ICSrank concepts. For example, OSINT collection is similar to stage 1 planning and targeting. As disused in chapter 4, attackers do their homework when choosing a target. They gather related OSINT, and this includes techniques and exploits as mentioned in the SANS model. As for SANS stage 2, development and testing are also based on gathered OSINT information about the internal ICS structure. ICSrank discussed these concepts in detail in chapter 4 & 6. Once inside an ICS network, an attacker normally follows these steps (Figure 13)

- **Develop** a tool or methodology to achieve attack goal, let's assume it's a malware and the target is a PLC.
- **Test** the malware that was developed for validation purpose.
- **Deliver** the malware to the PLC device.
- **Install/Modify** malware files inside the PLC software.
- **Execute** ICS attack by making the PLC act abnormally for instance.

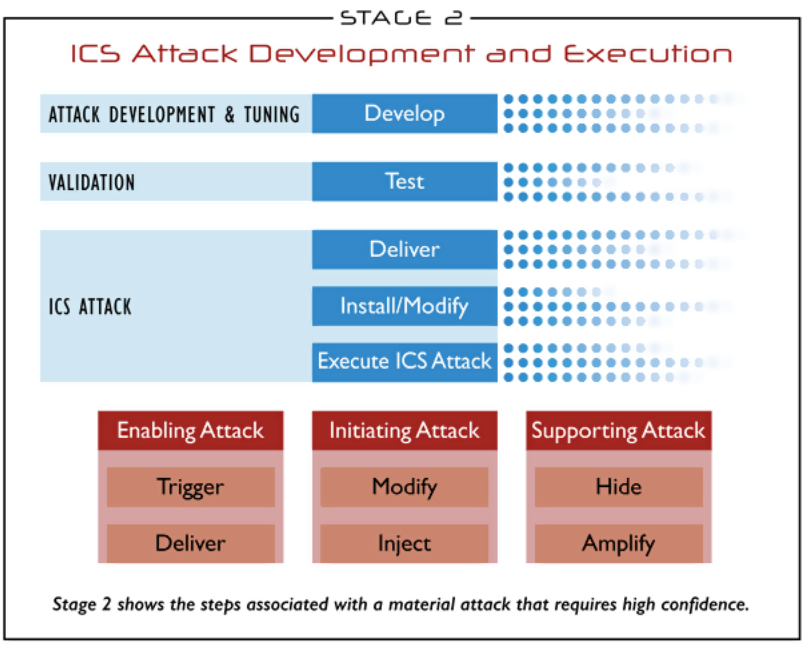


Figure 13:: ICS network Stage by Assante and Lee [206]

ICS attacks are common in industrial systems which would include harmful unauthorized actions that have been committed by insiders either willingly or by mistake [142]. Figure 17 above shows the sequence of actions that commonly are part of ICS attacks on the cyber systems.

5.5.1 ICS attacks on industrial Systems

An attacker who is attempting to perform physical attacks after gaining the capability and access to affect an ICS device has the ability to perform the following actions [137][138]:

- Change Input/output values: This affects ladder logic, valves (closing and opening), connected equipment, motors (turning on and off), product quality, and power disruption. Making such changes in the input/output values can, therefore, lead to financial and environmental issues. This method can also be used in order to spoof administrators about system status by feeding falsified data and information to the administrator [148].
- Infected firmware: This has the capability to do just about anything that is possible using a software firmware upgrade on a system, including disrupting the machine and changing its whole operation procedure [147]. Common impacts of an infected

firmware would include the following: alteration of existing configurations, installing backdoors, installing new features, and functionalities.

- Change read-write access: Making these changes in the system can lead to catastrophic results as the attacker has the option to overhaul the way machines operate in the ICS by changing the read-write access. For instance, an attacker can change the read access of RTUs in a way that data is not readable by the MTU. This makes it impossible for the MTU to collect any data from connected RTU [145]. Similarly, write access can also be changed making it difficult to store the data for backup purposes.
- Stop PLC: This can disable a system or certain components or alter production. Stopping the device is a fully accomplished goal because it stops ladder logic from functioning and entering a safe mode for instance. This affects the availability of the device and causes a denial of action.
- Reprogram control devices' instructions: Changing the instruction set for the control devices can result in reprogramming or altering the way controllers behave in response to the instruction commands sent by the operator and controller [143]. This kind of attack would make it very difficult for the operator to use the ICS in an effective manner with reprogrammed instructions.
- Change control software configuration: Making changes in the control software alters the way the system is controlled by the controller logic in a way that makes it difficult for the operator to control the system, or issue instructions.
- Safety system modified: An ICS would typically include safety measures and systems such as automatic settings backup, firewall, and storage of the information. If the attacker who has gained access to the system can change the safety systems, it can lead to a disaster in terms of both harming the hardware equipment or disrupting the software by corrupting it. An example would be when an attacker can remove or disrupt the cooling system that keeps ICS from getting overheated.

5.5.2 Impact

Computer systems have become ubiquitous in the industrial world to remain competitive and productive. This high degree of dependence of business companies on computer systems and ICS is very prominent and makes the impact of cyber-attacks very significant. Cyber-attacks on ICS devices in an industrial plant can have the following impacts [140] [139]:

- A threat to security: A successful cyber-attack can significantly reduce the safety and security measures deployed by the manufacturing company to keep its confidential data and industrial processes secure, rendering the business operations insecure. The impact can reach to the level of a disaster as any other malicious entity can also attack the system while the security measures are lowered. As a result, the business might need to suspend its operations [146].
- Competitive sabotage: A cyber-attack can also be viewed as an act of sabotage in the corporate world as a successful attack can undermine the reputation, production capacity, and quality of business operations. A competitor in the industry can take advantage of this attack to gain a competitive advantage. In some cases, a competitor can even gather confidential strategic business data of a competitor to gain a competitive edge and steal business secrets.
- Economic disaster: A cyber-attack can lead to reduced production and then to a temporary complete shut-down of production capacity, both of which can completely disrupt sales and money-making opportunities available for the company [143]. For instance, the business may be unable to meet project and supply deadlines resulting in the cancellation of contracts and financial loss.
- Reduction in production capacity: An attacker can use cyber-attacks to render the production capacity of an industrial plant handicapped in a number of ways. Some examples include tampering with the machinery equipment, reprogramming the controller logic, and disabling the firmware security. Such actions would cause the production capacity of the plant to go down to a potentially significant level.
- Equipment damage: In the case of a successful cyber-attack the attacker has the ability to completely alter the system and have a significant degree of control over the software and hardware. Accordingly, many safety attributes and measures of the

system can also be changed in such a way that the equipment is damaged thereby requiring either repair or replacement [142]. Therefore, the business would endure financial loss along with the reduction in production as the equipment is damaged.

- Injury or death of personnel: With the safety measures of the industrial equipment disabled or potentially changed, the equipment can fail or malfunction. Such abnormalities can occur at any random point in time without prior indications or alerts. Serious events can follow including floor personnel being injured due to machine malfunction resulting from the changes made during the attack.
- Release of hazardous materials: Within different types of industrial plants the use of hazardous materials is a common occurrence. These hazardous materials are generally kept safeguarded using cautionary systems. In an attack, the safety measures can be disabled and as a result, hazardous material can be released and cause different kinds of accidents such as fire, poisonous gas leaks and environmental damage.
- Environmental damage: As noted in the previous point, a cyber-attack can potentially result in the release of hazardous materials into the environment. Leakage of such substances can be very harmful to the environment.
- Damage to brand image: Facing a cyber-attack makes it very difficult for a business to keep up with its demand-supply cycle if the production capacity is harmed. In such cases, the business might not be able to fulfil its supply contracts or have the production of faulty products, all of which can cause the reputation of the company to be significantly damaged.

5.6 CASE STUDY: GAS CYLINDER FILLING SYSTEM

5.6.1 Gas Cylinder Safety System security:

Safety systems in gas and other industrial systems are meant to keep physical processes safe. They are the typical ICS devices such as PLCs, sensors, actuators and so on. The difference between regular operation devices and safety devices is safety devices have logical codes built into them [appendix] [32]. Logical codes such as AND, OR, NAND aid a device to make

decisions. While operation devices use these codes: ON, OFF to follow orders from control centres. There are abnormal events and hazards such as fire, explosions and release of poisonous gas that could result from errors and malfunctions in industrial systems. Sometimes safety systems are considered as the last security defence in the face of an attacker [32]. For instance, an attacker might be able to attack a device and bypass all cybersecurity measures, but they cannot cause an impact. The reason is simply most ICS have safety systems. However, this research proposes the following questions:

- What if a safety system doesn't function as intended?
- How could this happen?
- What are the consequences?
- What can we do to prevent the failure of a safety system?

This research focuses on "Safety PLC" as an example of a safety system in ICS. This research is motivated by the TRISIS incident [207] that targeted a PLC controller. Safety PLC takes orders from control centers, and then it directs those orders to other types of components. Normally as mentioned in this research's interview, there are two types of PLCs for every network. There are safety PLCs and operational PLCs. The operational PLC task is to communicate with field devices. However, it cannot send orders to field components without the approval of a safety PLC.

The safety system cannot face cyber-attacks directly [207]. There is an obvious risk in the safety system. For example, if a safety PLC is taken over like in the TRISIS incident [32], it is a game over, because safety PLC is responsible for all main operations [see appendix]. An attacker can make the safety PLC behave in an abnormal way, which can go undetected and, if it succeeds, can cause an impact.

5.6.2 ICS attack taxonomy

Based on the interview with gas company personnel, this research has developed a novel ICS attack/impact taxonomy (Table 11) based on Safety PLC in the gas industry. To this research knowledge, this taxonomy is novel, because its model is based on a real gas cylinder filling system. That model is developed by this research and is validated by engineers in that gas

company. This research argues that this taxonomy is a crucial step towards ICS security. There is a big gap in knowledge between IT and OT. This taxonomy can contribute the following benefits:

- Fill the gap between IT and OT departments. IT people can learn about the ICS process and about ICS assets.
- Develop technologies that use this kind of information. Many IT security technologies do not support or understand internal ICS network packets.
- Ability to perform a risk assessment of the ICS system/network and to analyse potential risk/impact.
- Understanding ICS system/network operations and security could help prioritize patching and other security procedures.
- Development of Threat models of possible scenarios to attack an ICS in the gas industry.
- Sharing of ICS knowledge in public such as an OSINT database. (See details in chapter 8)
- Study attackers' techniques similar to TRSIS incident and prepare for new attacks/techniques

Table 11:A novel Safety PLC attack taxonomy

Action	Action Specific	Physical Property	Action symbol	Impact
Modify Flow	Increase	Flow (Q)	MQ1	Gas cylinder overfill, rapture
	Decrease		MQ2	Gas cylinder half fill
Modify Time	Increase	Time (T)	MT1	Gas cylinder overfill, rapture
	Decrease		MT2	Gas cylinder half fill
Modify Air pressure	Increase	Air Pressure (AP)	MAP1	Destroy air-based devices from high pressure
	Decrease		MAP2	Air-based devices don't operate, due to low pressure
Modify Gas mass	Increase	Gas Mass (GM)	MGM1	Gas cylinder overfill, rapture
	Decrease		MGM2	Gas cylinder half fill
Modify Air supply	Close	Air Pressure (AP)	MAP3	No airflow, operations stop
Modify Sequence Values	Modify	Process Control (PS)	PS1	Affect the entire process. e.g. If the order of operation is affected, the entire filling process fails
Modify Gas tank Level	Increase	Gas Tank Level (GTL)	MGTL1	Overfilled Tanks

5.7 DISCUSSION

This chapter analyzed and outlined the cyber-physical relationship. The general theme of how an attacker can attack an online ICS device was demonstrated. The aim was not to cover all possible attacks, but on building a framework of how to link cyber-attacks with physical attacks. General objectives and physical impacts were briefly introduced. As such, a detailed

discussion of physical attacks is included in the chapters that follow. Our research has introduced a framework (see Chapter 4) that helps to identify threats and vulnerabilities from OSINT. This framework was used in this chapter and extended to incorporate the physical domain. This research further demonstrated this framework's applicability by showing how a piece of public information about a particular device can be turned into an existing vulnerability; thus, possibly launching a threat attack that can impact that device leading to physical and financial repercussions for the business.

This research developed an ICS attacks taxonomy based on safety PLC. The information conveyed in this research established an understanding of the way that physical attacks on online ICS work, and the link between ICS attacks and cyber-attacks. With this information, a reader can understand the extent to which ICS attacks can render an online ICS system useless. Once the attacker intends to disrupt the services and destroy the service provision, they can do so by corrupting the firmware, damaging the hardware components, or by completely overhauling the instruction set. For these reasons, ICS security of the online ICS is arguably just as important as protection against remote attacks. This research takes into consideration that the extent of damage is somewhat similar for both or even higher in some cases of ICS attacks where the actual hardware component is damaged. The impact of damage from ICS attacks ranges from financial aspects of a business, quality of services, and even the brand image of the business. For details of the ICS attacks discussion, refer to (Chapter 6).

5.8 SUMMARY

This research outlined in this chapter, part one of a cyber-physical model, which is the cyber threat section. It demonstrated the possible threats that could target a physical model and outlined the types of attacks, vulnerabilities and consequent impacts. It also briefly linked possible physical attacks with cyber-attacks. It is clear that a system of digital solutions that is vulnerable to any type of cyber-attack whether it is a physical attack or remote digital attack, can easily lead to a complete disruption of services and cause massive damage to the business. From the safety PLC scenarios for a gas system shown in this chapter, it is apparent that the sheer impact that a cyber-attack can have on an organization can be severe enough to sabotage the operational viability of the organization. It can halt production operations of the company, cause equipment to be destroyed, and make the business unable to fulfil its contractual

responsibilities. In designing a security measure to prevent cyber-attacks, a company must consider all possible avenues of attacks including remote digital attacks and physical attacks, including the possibility of company insiders being involved in the process of cyber-attack, either by accident or by intention. With a basic understanding of both ICS attacks and cyber-attacks described in this chapter; the next chapter will outline in depth the ICSrank applications on ICS OSINT.

CHAPTER 6

APPLICATIONS OF ICSRANK

6.1 INTRODUCTION:

The aim of this chapter is to apply ICSrank framework on ICS OSINT. The first case study is to assess Triconex PLC security. The goal is to demonstrate in depth the main 3 stages of this framework: collection, assessment and scoring. This chapter is concerned with ICS devices that are not connected to the Internet. The availability of OSINT information about these devices are examined under ICSrank.

The second case study of this chapter is to apply ICSrank framework on Trisis malware. The framework is concerned about the risks associated with an ICS network and their impact on a physical system. ICSrank is built on the OSINT concept, meaning to analyze risks based on available information in OSINT that are related to Trisis.

The third case study of this chapter is to apply ICSrank on a developed ICS model. This research studies the normal operations of a gas cylinder filling system and then the abnormal operations and their consequences. This research argues that successful cyber or physical attacks on a gas system could result in critical destructive impacts. This research is motivated to comprehend and observe the consequences quantitatively as accurately as possible. However, it is impossible to test this on a real operational system. Therefore, a simulation modelling method has been adopted in this study.

6.2 APPLICATIONS OF ICSRANK FRAMEWORK:

In this section, this research continues using ICSrank framework to assess and rank offline or non-Internet ICS devices based on OSINT. The OSINT information "ICS OSINT" in this chapter and chapter 4 are the same. The context is different. In chapter 4, ICSrank framework was used to assess online ICS devices' security by analyzing and ranking OSINT information relating to that device. The OSINT information is categorized and utilized for attack stage 1 (See also chapter 5). Stage one or (kill chain stage 1) as explained in chapter 5 is the first stage of the attack on ICS devices. What's interesting is any information that is related to an ICS device's security at this stage. Chapter 4 also explained the methodology of OSINT information analysis and assessment.

This chapter uses the same concepts and methodology of OSINT analysis and qualitative/quantitative assessment as in chapter 4. The context is "ICS OSINT" for the 2nd stage; meaning assessing OSINT for non-online ICS devices. This information is all about the internal details of an ICS system or network. This set of information is normally associated with an ICS attack stage 2 (kill chain stage 2). Stage 2 as explained in chapter 5 is the second stage of an ICS attack. It's a very critical stage that requires special knowledge and skills from the attacker. OSINT information for stage 2 is very critical for both defenders and threat actors. The threat actor's possession of "ICS OSINT" information can lead to exploitation of ICS networks and can result in unwanted physical impacts. Defenders on the other hand can use this information for the establishment of proper mitigation and defense techniques.

However, the same qualitative and quantitative algorithms for assessing stage 2 OSINT information is also applied on stage 1 OSINT information in chapter 4. In chapter 4, OSINT information were grouped into 7 categories, assessed using ICSrank algorithms, and ranked to get the final risk score for an ICS device.

6.2.1 Trisis/Triton/HATMAN

This chapter uses the famous incident – as the main theme to conduct 3 case studies. This incident happened in Saudi Arabia [207] when a malware called Triton or TRISIS hit a safety-instrumented system (SIS). The incident happened in 2017 when an employee accepted a

malicious file that carries this malware. The victim was a Saudi oil and gas company. The ICS device that was targeted was Triconex PLC from Schneider Electric. It was a 0-day vulnerability (a new vulnerability that has never been published) that was exploited in the PLC controller. The exploit went undetected because the intrusion detection system or anti-virus software did not carry that exploit signature. The attacker's goal was to replace the logic code in that PLC in order to control it remotely. The exploited firmware allowed the attacker to disable the SIS PLC. Luckily, it failed at some final stage. The attacker lost control after that failure because it already launched an alarm. That failure prevented a crisis for human safety and potential economic losses.

The TRISIS capability could be repeated and replicated on other targets because the tradecraft is out on the internet. The attacker only needs to learn about the new target system and network infrastructure. That learning curve happened in TRISIS where attackers were inside the network undetected for so long before they managed to cause an impact.

6.3 CASE STUDIES:

6.3.1 Case Study 1 : Triconex PLC security

This is an application and collection of "ICS OSINT" from real resources. The methodology and sources of OSINT analysis and synthesis are already explained in chapter 4. The below description is an example of OSINT information which is related to stage 2. The OSINT details information about an ICS system, network, threat information and its impact on this industry (in this case a gas industry). This information is very critical because an attacker can use this information to target new ICS and cause internal damage using similar capabilities such as the "TRISIS" malware and how it was applied. There is a potential that this attack can be replicated. However, not all ICS targets are the same; homework has to be done to gather specific information about the new target. The example below is for illustration purposes only and it gives basic clues about "ICS OSINT" and how it looks. There is missing specific information about the target as it is unethical to mention here, and it is out of this research scope.

In chapter 4, this research applied ICSrank framework to online ICS device- Siemens PLC. This section is a demonstration of how to apply ICSrank on an offline ICS device, in this case Its Triconex PLC. It is worth to mention that in chapter 4, a taxonomy of OSINT was used to label specific forms of information/OSINT with the letter V, the purpose of that was to distinguish/classify each information source individually. Overall all these Vs fall under the 7 main categories which are system (S), network (N) details, configuration details (C), defense (D), Techniques (T), online surface attack (O) and credentials (P). This can be applied here too.

Stage 1: OSINT collection

Source 1: MDudek ICS [5]

Application in ICSrank: System details (S), Network details (N), Configuration details (C), Defense details (D), Techniques and tools (T) and Online surface attack (O).

This source is really useful and dangerous for providing critical information for researchers and attackers too. It's a hub to start from to learn about Triconex PLC and Trisis malware. Below is an explanation of how this source was used in this research.

Trisis Malware files

This source has almost all of Trisis malicious files. The source author admitted its dangerous to post these files, but his reason was other public sources published those. He added those files for research purpose. The following files are the core Trisis files to understand: trilogy.exe and library.zip

Trilog.exe is a python compiled file. It is the main malware file and executable. When it is executed by a victim it extracts and drops 4 files: script_test.py, library.zip, inject.bin and imain.bin. in the targeted Trisiation workstation.

After execution, script_test.py uses two payloads: inject.bin as a backdoor injector and imain.bin as a backdoor. The script communicates with the device and its protocol using crafted libraries available in library.zip. See an illustration image below.

Figure 14: How Trisis works [218]

This library.zip file contains Tristation protocol implementation which were implemented by reverse engineering Triconex hardware its software. The attackers were able to obtain those resources. Its worth to mention that the device was undocumented (Nozomi), that left the attackers to discover everything by their own once they had the device and its software.

On reflection about Triconex and OSINT. The attackers developed researched system details (S) using the available resources. They later also managed to find a target and its network details (N) . Then they developed the necessary tools and techniques (T). All knowledge was built from scratch and self-effort. This could happen to any ICS device that is not documented or available in OSINT. This technique is called zero-day vulnerability, which means no prior vulnerabilities are available. And That's why it is a good reason to keep a radar on OSINT, because attackers are always looking for OSINT knowledge for attractive targets. They also learn from OSINT similar and applicable techniques.

The malware files are an indication of availability of critical OSINT that could be classified based on ICSrank as techniques (T) which is the malware itself, system (S) and network (N) details which can be extracted as from the files and code inside the malware. This extracted information is discussed in the following sections.

Malware Detection rules:

There is a folder in this source that hosts Yara detection rules. These rules were developed by ICS-CERT and FireEye Mandiant [219][221]. Those rules can be used for defense purposes to detect Trisis/HATMAN files. ICSrank classifies this OSINT in the collection process as defense (D) information.

Source 2: Nozomi Github Tritools [223]

Application in ICSrank: System details (S), Network details (N), Defense (D), Techniques and tools (T) and Online surface attack (O).

This source is used mainly in this research to obtain the Trisis network packets and to apply ICSrank framework on this type of OSINT as explained later in this chapter. This github contains two types of tools (T): the packet file and a honeypot. The network packets will be examined later in depth in this chapter. That file is important to learn system (S) and network (N) details about Triconex and Tristation protocol. Its also critical to study the behavior of Trisis malware, thus learn new techniques (T) and expose device and protocol vulnerabilities (O). The packet file comes also with a dissector script written in Lua language. This dissector is used to show direction of communication, translate function codes, extraction of programs and functions and most importantly detection of Triton malware (source). The dissector provides useful information for ICSrank; The above usage can help extract knowledge about the system (S) and network (N) details, vulnerabilities (O) and defense information (D). The script file is used in this research as a companion to learn about the device system, protocol and its function codes.

The other project in this source is the Triconex honeypot. The honeypot is used mainly to emulate the behavior the real Triconex PLC for research purposes. It gives insight about system (S) and network (N) details. Although it’s very useful to experiment with, however it is out of this research scope to cover its details. This could be a done in future studies.

Source 3: ICS-Cert , Dragos and FireEye [219][211][221]

Application in ICSrank: System details (S), Network details (N), Configuration details (C), Defense details (D), Techniques and tools (T) and Online surface attack (O).

These sources are used through all this chapter to extract OSINT related to Triconex and Trisis. These sources are full of technical details and descriptions of Triconex and Trisis. They are used as a reference tool to build ICSrank philosophies and concepts, apply this framework on Triconex PLC and specially to evaluate this research findings for the following case studies. Especially those resources are established organizations in the field of ICS security.

The following assessment is based on what is available in OSINT. So, this information ranks Triconex PLC based on OSINT based on multiple sources by applying ICSrank. However, in this research, another case study is illustrated to assess Triconex based on a single source which is a pcap file. The research goes in depth analysis of network packets in order to extract OSINT information and therefore analyzed using ICSrank. Based on this research, this kind of assessment is never done before; using ICSrank techniques on OSINT in general and applying ICSrank on ICS device network traffics in particular.

Stage 2: OSINT assessment

In this section, the same technique of chapter 4 is applied here. It starts of gathering related OSINT, assessment and analysis and finally scoring the gathered OSINT. This approach is the nutshell of ICSrank framework. As mentioned in chapter 4, ICSrank has 7 OSINT categories that represent the knowledge. These are System (S) and network details (N), configuration (C), (defense (D), Techniques (T), Online (O) and credentials (P). This knowledge is extracted from public OSINT. Below is the explanation.

System details (S):

Device name: Schneider Electric Triconex Tricon

Processor: MP860 PowerPC

Device Model: Triconex 3008 processor modules

Firmware Version: 10.0-10.4

Software name: Tristan Suite 1131 v4.9.0 (build 117)

Documentation: Available [V11]

Device Vendor: Schneider Electric

Score: Insecure

The system details (S) in the table (number) shows that almost everything is known about the Triconex PLC system details. This information is available in public OSINT to everybody. Asset owners who have this kind of device should be careful of this. At attacker can study this information and learn how to develop his/her own to exploit this device vulnerabilities. Documentation section is available in many sources especially the ones that are used in this research above. Therefore, to apply ICSrank assessment, all the main categories are available in OSINT, therefore this device is labeled insecure in this category. Assessment should be carried to other categories as well.

Network details (N):

Protocol Name: Tristation

Protocol Port: 1502 UDP [V14]

IP address: N/A

Network Layout: N/A

Documentation: Available [V11]

Score: Secure

The main categories for a network category are protocol name and port, ip address and network layout. Only two main categories are known in OSINT, in the assumption that the device is offline and is not available online. The known categories are protocol name and port number [V14]. There are also plenty of information about this protocol functionality mentioned in this research resources above. However, this kind of information is optional, because an attack

could be conducted even if this information is not available. An attacker can learn about this detail by experimenting with the device if he has it, or by installing sniffers that listen to an ICS traffic like many existed attacks and techniques (mention some of them here). The device is not online as assumed; therefore, its IP address is not known. Therefore, no information about its network layout is available. A caution for this asset owners, this device is only one thread away from being ranked as "insecure" because once its IP address is known, the network layout can be discovered in a matter of time. Thus, this device is assessed as medium risk, because only one main category is known.

The knowledge of communications between workstation and Tricon PLC, documentations (above) and manufactories' documentations enables Nozomi team and Trisis attackers to extract network and system details by using reverse engineering methods. [220] [V11]

Online surface attack (O):

Internet presence: N/A

Vulnerability: ICSA-18-107-02 [V15]

Score: Insecure

There is a critical vulnerability advised by ICS-CERT (ICSA-18-107-02) [V15] with a CVSS score 9. The vulnerability is Improper Restriction of Operations inside a Memory Buffer. That means that an attacker can read and write to memory buffer without restrictions. This vulnerability is available ion public OSINT and is therefore this category is classified as "insecure". This category also checks if a device is online. But in this case, it is not.

Configuration (C):

Configuration: Run/remote – program [V3]

Score: insecure

The device has two modes: "program" mode and "run/remote" mode which should be the default mode. In the "run/remote" mode the device cannot be programmed or exploited. However, in "Program" mode the device is programable and thus is vulnerable. The recent

Trisis attack occurred because the device was in program mode [V3]. It could be learned that this category is very critical and what made the attack happens. Without it the attack wouldn't exist. That's why configurations are very critical in ICS security and that's one of the key philosophies of ICSrank which is to find critical OSINT. The device is therefore classified as "Insecure".

Figure 15: Triconex modes [221]

Techniques, exploits and tools (T):

Exploits: Trisis mawlare [V15]

Malware: Trisis malware

Proof of concepts: Honeypot

Tools: Nozmomi tools

Score: Insecure

Based on this research, there were plenty of techniques, exploits and tools that are related to this device. This research explores extensively one of the important tools and techniques which is the network packets of Trisis malware developed by Nozomi lab. The packets were captured and stored in an application programming interface file (API) which is abbreviated as libcap or pcap. This file is available in one of the main OSINT resources Github [223]. See above for more information about these sources and their application in ICSrank framework. These tools are not only important but also critical because they teach the attacker many aspects of the device and its protocol as this research explores later. This category is considered in the cybersecurity domain very important. Researchers and attackers are always looking for existing tools and exploits. They also share this knowledge in OSINT often. The availability of this vast knowledge for Triconex PLC makes this category "insecure".

Defense and mitigations (D):

Patching information: N/A

Mitigations: Available

Score: Secure

Based on OSINT assessment, the defense category is classified as "secure", because there are existing mitigations techniques, advisories and tools offered by vendors and organizations – see below. That would benefit the asset owners to be aware of existing vulnerabilities and be able to implement security.

For example ICS-Cert , FireEye offered some guidelines [220] [221]:

- Always keep the device on run mode and not program mode. Also, addition of alarm for program mode when it goes on.
- Avoid Tristation workstations to connect to a large network
- Remove Triconex sis to connect to a persistent network
- Enable Triconex communication modules to enhance protocol security.
- Isolate safety PLCs in a different network/zone from operational components.
- Secure safety PLCs physically by locking them in cabinets in secure rooms.

- Data media exchange such as CDs or USBs should be scanned before use in computers connected to safety networks.
- Laptops should be scanned and sanitized if they are used to connect to safety networks.
- Some safety PLC devices have physical key switches to lock a device and thus prevent it from being tampered with, it is recommended to activate this feature by default.
- Allow authentication features for connecting to safety devices and disable unnecessary backdoor accounts that are used for maintenance.

Detection tools that enable asset owners to detect malicious packets in their network were also given to public freely. An example is the development of Yara rules [220][219][221] The rules are able to detect suspicious files and critical Triconext PLC. Despite patching information – an optional category - is not available from Schneider, the device is still secure in this category. The reason is because Schneider and others provided guidelines and the main advice was is to secure the configurations which would have prevented the attack altogether.

Stage 3: Triconex PLC score

Category	**Secure?**
System (S)	**NO**
Network (N)	**Yes**
Configuration (C)	**No**
Defense (D)	**Yes**
Techniques (T)	**No**
Vulnerability (O)	**No**
Credentials (P)	**N/A**
Number of insecure main categories	**1**
Number of insecure optional categories	**3**

Risk Label	**Medium**
Risk score	**8 / 10**

Looking at the above assessment, System details (S) are known in public OSINT while network details (N) are not known about any target like and IP address which represent an ICS device or its organization. The other unknown fields such as network structure of a target is not there. In short, no target is defined that would make the network category secure. The system details of that device are insecure especially for those organizations that use this device. Based on ICSrank algorithms in chapter 4, if one main target such as network (N) is secure, the device would be classified as "medium risk". There are obviously insecure optional categories such as technique (T), online(O) and configuration. The Triconex PLC discussed in this research should be put under monitor by asset owners and researchers, because if any major network details are leaked or exposed in search engines such as Shodan, it would be classified as "critical" risk. In the next section, this research explores in depth the behavior of Trisis malware by using OSINT information and related sources.

The risk score for this device is 8/10. As discussed in chapter 4, a medium risk device is scored 5/10 if it has no insecure optional categories. There are 3 insecure optional categories here, therefore for each category, ICSrank increments the risk score by 1.

6.3.2 Case Study 2: Trisis OSINT

In this section, a lengthy discussion and analysis of network behavior of Trisis is conducted. The network details of the "Malware_exec. pcap"- a real Trisis behavior developed by Nozomi is to be put under ICSrank microscope. It is an attempt of this thesis to apply a security assessment of the existing malware OSINT which is related to ICS devices.

Techniques (T)

There are the techniques (T) that are used in this case study to discover this OSINT knowledge – system (S), network (N) and attacker behavior that can be shared. These techniques (T) are a set of filters and keywords that could be viewed as a set of skills that were developed, learned and harvested during this research process. The techniques and skills that were employed are 4 tools (T):

1. Wireshark: is the main platform for this experiment to run the Trisis pcap file. It filters specific packets and exports the results to a text file.
2. A text editor: Used for analysis and text mining the exported text file.
3. "Malware_exec. pcap": the Trisis packets file developed by Nozomi.
4. "Tristation.lua": The Wireshark dissector developed by Nozomi.

The benefit from this OSINT source (pcap file) can be summarized in one word, and it would be techniques (T). The file is extensively full of techniques that were performed by Nozomi that mimic an attacker. Those techniques (T) can be learned and applied to a similar environment – including this PLC and the TS protocol.

There are the techniques that were used in this case study to discover this OSINT knowledge – system, network and attacker behavior and thus can be shared here. These techniques are a set of filters and keywords that could be viewed as a set of skills that were developed, learned and harvested during this research process. The skills were employed using a variety of tools and platforms: Wireshark is the main platform for this experiment. The second tool is a text editor. These skills are beneficial to defenders and attackers like if exposed in public.

The capture file is quite large. It contains 895 packets. It was difficult to know where to start at the beginning to make sense of the traffic. Luckily Nozomi Networks has a blog article [222] that describes their analysis tool – aka the dissector that is used in this research [223]. The article briefly mentions the "Allocate program" command and how it was used to detect the malware. In this research, that command was used to develop the following analysis.

The communication of packets between the attacker (Nozomi team) and the PLC device were analyzed. A common behavior was observed here. A set of commands were issued in particular order and time to achieve a particular output and response from the controller. This behavior can be observed by identifying the two communication members: the attacker and the controller. This could be achieved by identifying their IP addresses and familiarity with source and destination fields.

System and network details (S) (N) can be extracted from this file. This where the attacker is trying to gather information about the controller (S) by issuing command 19. The command is found in Wireshark by using this filter:

```
ts.ts_cmd == 19
```

The response command from the controller is 108 [Get CP status response]. This command reveals this information for the attacker (see figure 16) , the Wireshark packet is translated by the Dissector script which is written in the figure (17).

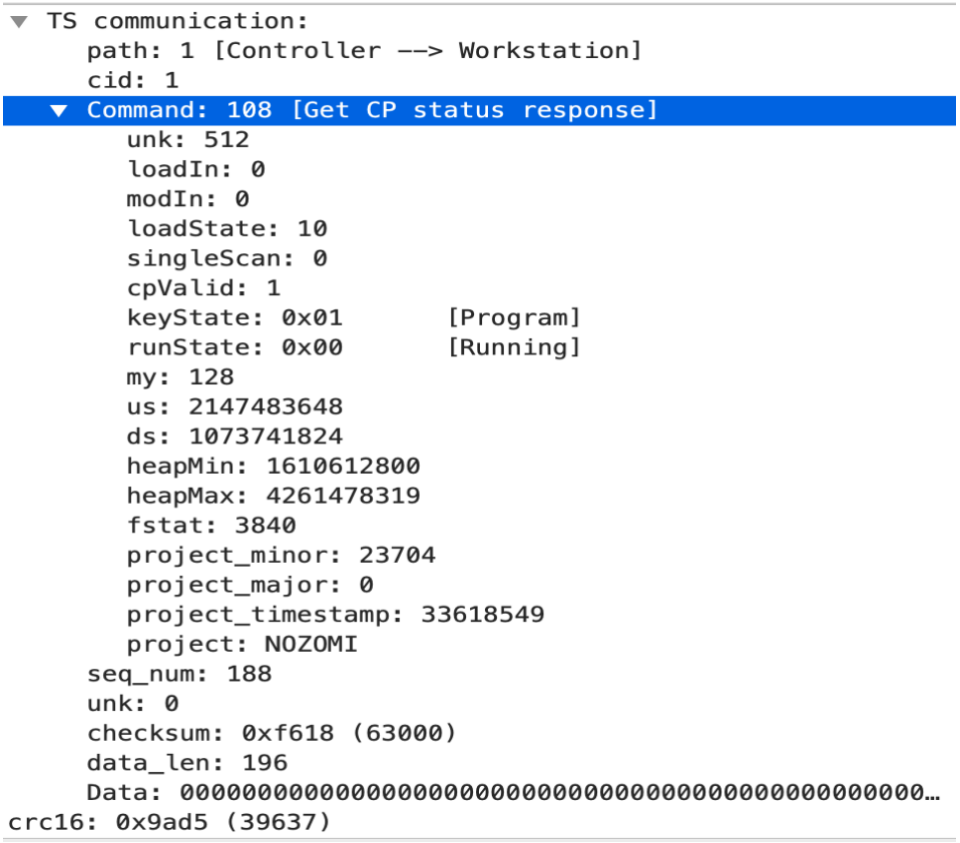


Figure 16:CP status results

```
ts_proto.fields = {
                    message_type,
          crc16,
          crc32,
                    message_length,
                    cid,
                    ts_cmd,
                    ts_sequence,
                    ts_unknown,
                    ts_checksum,
                    ts_length,
                    ts_cp_keyState,
                    ts_cp_runState,
                    ts_cp_fstat,
                    ts_function,
          ts_program,
          ts_signature,
                    ts_project,
                    ts_path,
          ts_module,
          ts_full_program
}
```

Figure 17:Dissector Script

This is one of the most used – 338 times - function performed by the attacker, to the obtain CP status or control value. The malicious injector discussed above uses this function to track PresetStatus that stores the control value in the controller memory. The controller gives this information back to the attacker by issuing this Command 108 labeled as [Get CP status response]. This function is used to accomplish 3 tasks [220]:

- Decide the number of cycles to idle before payload injection takes place.
- Control the counter to control/track execution progress
- Debug the controller in case of failure, to get information about the injector

The above information demonstrates a technique used by the attacker (T) to get information from the Triconex. This information shows how this PLC works (S) and how to communicate with this device (T) (N). This information is available and valuable in OSINT for researchers and attackers. The information also can be exploitable and repeatable for similar devices.

Based on this research, the following commands were observed to occur frequently by the attacker and the controller. Command 65 which is labeled and translated as [Upload program] in the Lua script and Wireshark respectively. It was used by the attacker 26 times. Its functionality is similar to its label. Command 162 is labeled [Upload program response] and it was the response of the controller 20 times. The other command is 100 and labeled as [Command rejected], it was the response by the controller.

The rejection happened 16 times. After digging Wireshark and the exported text file, this filter was used in Wireshark, to find the rejected packets:

ts.ts_cmd == 100

The explanation of this rejection according to an ICS-CERT report is that, Triconext allows (S) downloading the malicious programs only 3 times. It was a response to upload program issued 3 times by an attacker. So, it's like a repeated cycle until the whole programs are downloaded. After each cycle, the attacker uses the command 19 [Get CP Status] after issuing the upload function. That command is issued for the explained reasons above. This is another technique (T) that shows how an attacker uses these commands (S) to communicate (N) with the controller.

A brief statistic for other commands that were found inside the packets is shown in ((Table 12). A text mining technique was used to find the following functions. The results of Wireshark were customized and exported to a text file for further analysis and OSINT discovery. Those functions summarize the main functions that were communicated between the attacker and the controller. In addition, the system and network commands that were discussed previously.

Table 12:name functions statistics

Upload function	ID	Counts
Upload	66	72
Upload function	163	63
Start download	1	3
Download change permitted	102	3
Allocate program	55	3
Allocate program response	153	3
End download change	11	3
Modification accepted	103	3
Run program	20	1

It can be concluded that command 55,153,11 and 103 were used 3 times. That's no coincidence, because three were 3 cycles/stages performed by the attacker to append the malicious files inside the controller [220]. The appending can be traced by issuing the command 55 [Allocate

program] (see figure 18). The malware was executed 1 time and, it can be seen above in the table about the command 20.

These statistics is useful OSINT in many aspects;It provides information about important commands built-in Triconex (S) and how many times they were communicated (N). And most importantly the potential that they pose if they were misused. This could be of enormous value for considering defense (D) strategies to prevent misuse of such commands by means of access control and detection methods. In the next section, further analysis to identify attacker techniques (T) and how these commands were used. Also, a demonstration of how to extract OSINT from these malicious packets.

Based on the analysis of the traffic file using the "Allocate Program" filter as a starting point, it was observed two repeated behaviors and scenarios that happened between the attacker and the Triconex PLC controller. The 3 packets that contain the "Allocate Program" were packet: 73,76 and 887. That command was proceeded and followed by specific commands in the following order :(see table 13)

ts.ts_cmd == 55

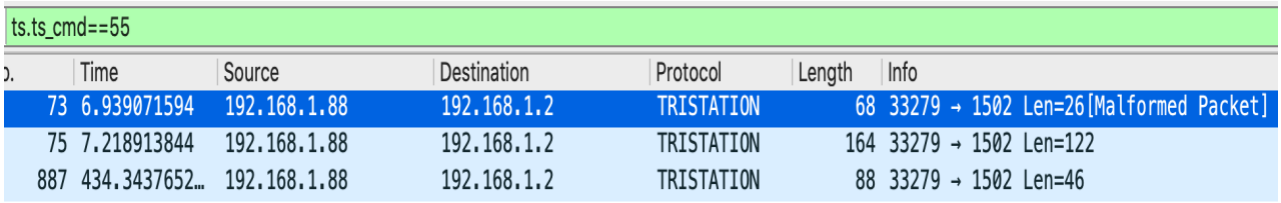


Figure 18:Allocate program command

The malware injection process was a result of communication between the attacker and the controller, using specific functions back and forth. These commands are built-in the Tristation protocol. Their names and corresponding values are described in the dissector file developed by Nozomi [223]. The below scenario was communicated using the following functions:

Table 13:Common functions

Command	Value
Start download	1
Download change permitted	102
Allocate program	55
Allocate program response	153
End download change	11
Modification accepted	103
Run program	20

This command "Allocate program" is used 3 times by the attacker to append the malicious files. The attacker sent this command to the controller for execution [218]. The files were allocated 3 times successfully by the controller and downloaded. The malicious files modified the controller original firmware and finally the final malware file was executed. This behavior based on this research statistics summarizes the whole malware operation (T) and objectives.

It is worth mentioning that Wireshark has a feature called "Expert Info"[225]. This feature keeps tracks of anomalies in the capture file [219]. With the help of dissectors this feature can provide extra information about uncommon network behavior. This piece of OSINT can be used for defense (D) strategies such as packet detection by recognizing the packet signature or structure. In this research, expert info identified the malware packets (see figure 19). Expert info can be found using the "Allocate Program" command filter mentioned above or the following filter:

ts.ts_cmd == 55 && _ws.expert

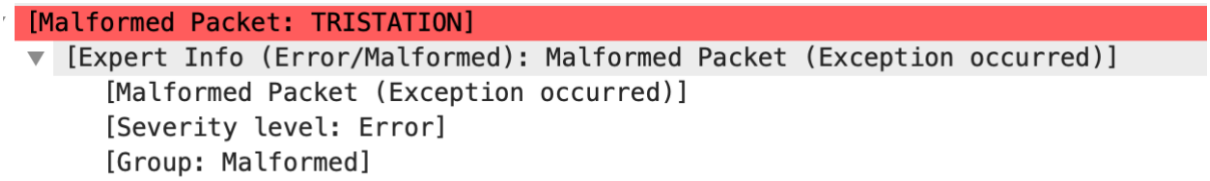


Figure 19:Expert info in WireShark

The malicious file is detected by the dissector in the below figure (20). The is composed of the signature of the malicious file: ffff6038020000442000804e. This part is defined in the dissector as “ts.ts_full_program” in the “TriStation.lua” script (see below) Then its broken into 3 smaller programs, which are defined in the dissector file as “ts.ts_program”. The number of 3 files explains why each cycle is composed of three downloads as explained previously.

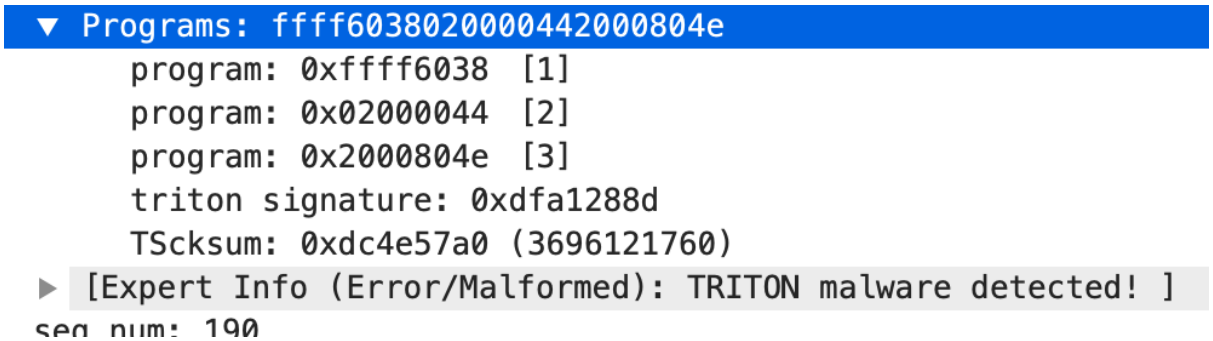


Figure 20:A List of malicious files

ts_progra = ProtoField.uint32("ts.ts_program", "program", base.HEX)

ts_full_program = ProtoField.new ("Programs","ts.ts_full_program”, ftypes.BYTES)

```
private rule hatman_nullsub : hatman {
    strings:
        $nullsub = { ff ff 60 38 02 00 00 44 20 00 80 4e }
    condition:
        hatman_filesize and $nullsub
}
```

Figure 21:Yara rule

Summary report:

This research started by collecting related OSINT data to Triconex PLC and Trisis maklware. However, case study 2 is different than case study 1. Case study 2 is concerned only with assessing the Trisis network data "Malware_exec. pcap", and not with the overall OSINT data that were analyzed in case study 1. The resources were analyzed and classified based on ICSrank OSINT categories: system (S) and network (N) details, configurations (C), defense details (D), techniques (T), online vulnerabilities (O) and credentials. The objective of case study 2 is to demonstrate how ICSrank works on individual OSINT resources and how to extract, categorize, assess and rank them. Collection and categorization is done in the above section. The next step is to assess these categories into secure or insecure. Here is the assessment discussion a summary table of the assessment:

Trisis security assessment

Category	**Secure**
System details (S)	**Yes**
Network details (N)	**Yes**
Configuration (C)	**Yes**
Defense details (D)	**YES**
Techniques (T)	**NO**
Vulnerability (O)	**NO**
Credentials (P)	**Yes**
Number of insecure main categories	**N/A**
Number of insecure optional categories	**2**
Risk Label	**Low**
Risk score	**2**

System details (S) and Network details (N)

The above information is a result of reverse engineering the Triconex PLC and its protocol Tristation. Indeed, they provide critical information about those, both system (S) and network details. However, this source “malware_exec. pcap” by itself is secure, here is why.

To make a system (S) category, based on ICSrank, certain categories such as product name, version, firmware version and functionality must be known. In the mentioned source, only 2 categories are known: product name and functionality. This information if stripped from existing related OSINT is not sufficient. The affected product and firmware version must be known, to raise a security flag. The OSINT is really rich of functionality information which is critical if combined with a known system. Individual sources according to this research are not normally enough to label advice. ICSrank is combination of OSINT source to help obtain a broader perspective. Sometimes OSINT sources such this one is incomplete by its own and looks secure, but if combined with other OSINT it could turn into a lethal weapon, which is the case with this data. It’s very similar to the Lego game, it only makes sense if all parts are assembled together. Incomplete system details (S) are labeled therefore as secure.

The network (N) details are more abundant than system (S) details, because this source is about network packets. So, it’s obviously there are plenty of information about main and optional information about the protocol. Protocol name and port were available as main categories. The IP address and network layout are not available. Optional details such as protocol functionality- an optional category is available too. Therefore, this category is classified as secure. Network details are similar to the system details in terms of their security. They are critical when other sources are combined with them like case 1.

Configuration (C)

Although, there was no indication of taking advantage of insecure configuration within the data, one can be certain that the whole protocol is insecure by design which is even worse than relying on configurations, which Schneider did by implementing operation features such as run and program mode. That’s because once the attacker is within the network, he/she has full control and freedom. So, this feature (C) is secure based on this OSINT alone, because this case study doesn’t contain configuration information.

Defense (D)

The network data in the exported network information is a valuable OSINT information to help detect abnormal traffic. That and familiarity of critical functions that an attacker might use is a bonus. This OSINT can make Triconex device and Tristation protocol more secure due to those OSINT. Thus, the defense and mitigation category (D) is labeled secure.

Techniques (T)

This is the most abundant information that were extracted from this data. As discussed above, an attack behavior (T) was learned, ranging from common usage of functions to specific ranges of filters that were utilized in this research to find this behavior. This OSINT (T) if shared and stored in a public database -as this research proposes earlier in this thesis, the research skills (T) and insights could be learned by researchers. These skills could also be acquired by attackers too. Availability of this knowledge and skills is twofold. It makes this OSINT insecure as it teaches malicious actors' new information and on the other hand its useful for researchers and defenders. This category (T) is labeled as insecure.

Vulnerability (O)

Going through the network traffic data, it was observed that are is a critical vulnerability. The list of commands above that allowed the attacker to communicate with the controller, interact, upload and download files is a serious security issue, because an attacker was given full supervisory privileges without out any verification [220]. Therefore, the online surface attack category (O)is labeled as insecure.

Credentials (P)

There was no finding of any credentials or authentication happening in the network data. This category (P) is secure. Although on reflection, this is not a good thing because it demonstrates that the device and its protocol is in secure by allowing access and modification for the unauthorized.

Trisis score*:*

The final step in ICSrank is to rank this OSINT individually. The purpose of this stage is to see the level of this OSINT- the network data security. It could be used to rank the device by itself or this source alone. As explained this information above this OSINT does not show information about specific version, only it targets the device name. From the above analysis , and based on ICSrank algorithms in chapter 4 of this thesis, both major categories system (S) and network (N) details are secure, this would classify this OSINT or device in the low security level because it has other categories such as techniques (T) and vulnerability (O) as insecure. The risk score of this case study is 2/10. Number 2 reflects the number of insecure optional categories. Low risks always have positive numerical values as opposed to "none" risky which have zero value.

6.3.3 Case Study 3: Gas model

This is the last case study,its a follow up to the previous 2 case studies in this chapter. This research attempts to propose a scenario of what could have been happen if the Trisis Malware succeeded. It demonstrates two possible scenarios of attacks on the Triconex PLC. The simulation is a proof-of-concept and by no means it represents a real gas plant. However, as mentioned earlier and in the appendix the model has been verified with a local gas producing company in Kuwait.

This simulation and its data can be shared to the ICS security community and be available in public OSINT. There are many open source models of ICS systems in OSINT that are being used by researchers and organizations. These models offer useful knowledge to understand and learn about ICS systems.

In this section, this research applies ICSrank framework on this model and its findings. The goal is to explore how models can contribute to OSINT and ICS security. This is achieved by exploring what type of information models provide, how related and beneficial they are and what's their impact on security. The gas cylinder filling model is used as a case study to answer those questions.

Based on the attack taxonomy model in chapter 5 (Table 16), this research chooses 2 types - out of 6 - ICS attacks to simulate in the gas cylinder filling model. In that model, the focus is on studying two physical properties. This case study simulates gas filling system normal and abnormal behavior. The abnormal behavior is interpreted as malicious actions performed by an attacker. This research assumes the attacker has established access inside an ICS network using the threat model and the scenario that we explained in the previous section (section 6.4.1). The attacker has many options for attacks to perform inside the network (Chapter 5). This research narrows ICS targets and chooses a safety PLC device that belongs to a gas filling system. Below sections are the case study and data generated by this model.

6.3.3.1 GAS CYLINDER FILLING MODEL [151-160]

This section describes the use of methodologies in the form of numerical computations, which can explain a real physical system for 'filling a gas cylinder'. The modelling tools will be used to analyse the system and simulate various conditions to detect abnormalities possibly caused by cyber-attack.

The mathematical model presents the basic mass balance equations connecting various measurements from the online sensors and instruments that are installed in the plant for filling a gas cylinder.

The mass balance equations, which are in the form of ordinary differential equations (ODE's) in the time domain were solved numerically. The ODE's are solved using the inbuilt solver algorithms in MATLAB. The differential equations are written in a standard format to which the solver algorithms can be applied. Details of the basic structure of the code and the system will be discussed further in the sections below. Two different scenarios are discussed here to study the response system and to build correlations between various measured variables in the process.

The simulation results are presented in the form of charts, tables and graphs. These will demonstrate the output of the system to given inputs and random conditions along a time period. Details will be provided on creating a block diagram, simplifying it, and creating a final structure that includes the mathematical function that would replicate the input-output relations in a gas cylinder filling process.

In the "Methodology section", the procedure followed, and the tools used will be demonstrated and then the factors affecting the modelling of the system will be explained. The procedure followed requires building analytical equations and using Matlab and Simulink to code and solve the system equations. The resulting correlations will identify abnormal measurements associated with the system and allow comparison with normal operating conditions. This can help present the case where the operator can detect the possibility of cyber-attack.

6.3.3.2 GAS CYLINDER FILLING MODEL DESIGN

An interview (see appendix B) is conducted with a senior engineer whose employer is a gas producer organization that implements ICS technologies. The interview dealt with questions such as the real-world risks and impacts of a serious malfunction occurring either intentionally (from malicious third parties), or unintentionally from internal errors and malfunctions.

This Simulink model is based on physical properties given to us in the interview. The physical properties of a gas cylinder are mass of a cylinder (empty and full) and cylinder volume. Other properties are filling time and gas flow rate. The goal of our model is to simulate real physical aspects of a gas cylinder process. The model and its properties are discussed in the following sections.

6.3.3.3 PROCESS DESCRIPTION & MATHEMATICAL MODEL [151-160]

In the following system, the process of filling a cylinder with gas from a certain industry with constant pressure and throughput is described. The following diagram gives a brief schematic of the gas filling process (appendix A).

The upstream pressure of the gas filling station is maintained at 17 bar and the filling completes when the pressure of the cylinder reaches the required weight. The weight of the cylinder, the pressure inside the cylinder as well as the Gas throughput (flowrate) is measured dynamically during the filling process. The dimensions of the cylinder, the total mass of the cylinder, operating conditions for the filling process has been presented below.

6.3.3.4 CYLINDER PROPERTIES

Mass of empty cylinder (m1) = 16 kg

Mass of gas (m2) = 12 kg

Total mass (m = m1 + m2) = 28 kg

The volume of the cylinder = 21 m3

Filling time for cylinder = 75 seconds

Flowrate (Qin) = 45 m3/hr

Data on the properties of the gas is also vital for calculating the pressure – mass - flowrate relationship. Therefore, this information has also been taken into consideration during the construction of the model.

6.3.3.5 GAS PROPERTIES

Density of the gas (ρ) = 0.564 kmol/m3

Molecular weight (M.W) = 22.695 kg/kmol

Filling temperature (T) = 273 K

DERIVATION OF THE EQUATION 1

$$\frac{dm}{dt} = mass\ flow\ rate\ (\frac{kg}{s})$$

Formula:

Mass flow rate = Volume flow rate * Density

Parameter Unit

Mass flow rate: kg/s

Volume flow rate: m^3/s

Density: kg/m^3

Q_{in} = Volume Flow rate (m^3/s)

$\rho 1$ = Density (kg/m^3)

$$\frac{dm}{dt} = \rho 1 * Q_{in} \qquad \textit{Equation 1}$$

Change the unit of the density

Density in kg/m^3 = (Density in $kmol/m^3$) * (Molecular Weight of the gas

$$\rho 1 = \rho * MW \qquad \textit{Equation 2}$$

Put *Equation 2* in *Equation 1*

$$\frac{dm}{dt} = \rho * Q_{in} * MW \qquad \textit{Equation 3}$$

DERIVATION OF THE EQUATION 2

Non Ideal Gas Equation

$$PV = ZnRT \qquad \textbf{Equation 3}$$

P = Pressure of the gas (bar)

V = Volume of the Cylinder (m^3)

Z = Compressibility Factor

n = Number of moles

R = Universal Gas Constant = $8.314*10^{-2}$ bar.m^3 mol^{-1} K^{-1}

T = Temperature of the Gas (K)

$$P = \frac{Z\ n\ RT}{V}$$

n = mass of the gas/Molecular mass of the gas = m/M

$$P = \frac{Z\ mRT}{V*MW}$$ ***Equation 4***

Density(kg/m^3) = mass of gas(kg)/Volume of the cylinder(V)

ρ1 = m/V (Put it in Equation 5)

$$P = \frac{Z\ \rho 1 RT}{MW}$$ ***Equation 6***

DERIVATION OF EQUATION 3

Van der walls equation of a state for real gas

$(P + a/V_m^2) *(V_m – b) = RT$ ***Equation 7***

P = Pressure of the gas, bar

a = measure of attraction b/w the gas molecule, bar $(m^3)^2/(kmole)^2$

V_m = Molar Volume, m^3/kmole

b = It is a accounts for the volume occupied by the gas molecules, which decreases the available open volume

R = Universal Gas Constant, bar.m^3 $kmol^{-1}$ K^{-1}

T = Temperature of the Gas, K

Assumption

Molar volume V_m is large, b becomes negligible in comparison with V_m

$V_m - b \sim V_m$

$$(P + a/V_{2m}) *(V_m) = RT \qquad \textit{Equation 8}$$

$$(PV_m/RT) + (a/V_mRT) = 1 \qquad \textit{Equation 9}$$

$$Z = PV_m/RT \qquad \textit{Equation 10}$$

Z = Compressibility Factor

Put Equation 10 in Equation 9

$Z + (a/V_mRT) = 1$

$$Z = 1 - (a/V_mRT) \qquad \textit{Equation 11}$$

Rearranging Equation 8

$V_m = RT/ (P + a/V_{2m})$ ***Equation 12***

Put Equation 12 in Equation 11

$Z = 1 – a*(P + a/V_{2m})/(RT)_2$

$Z = 1 – P*a/(RT)_2 – a_2/(V_mRT)_2$

Molar Volume = $1/ \rho$

$Z = 1 – P*a/(RT)_2 – (\rho_2\ a_2)/(V_mRT)_2$ ***Equation 13***

$a = 9.385$ bar $(m_3)_2/(kmol)_2$ (reference)

$R = 8.314$ bar.m_3. $kmol_{-1}$. K_{-1}

T = 273 K

$Z = 1 – P/54.89 – 0.0544$

$Z = 0.9456 - P/54.89$ ***Equation 14***

DERIVATION OF EQUATION 4

From Equation 6

$$P = \frac{Z\ \rho 1 RT}{MW}$$

Put Equation 14 in Equation 6

$P = (0.9456 - P/54.89) * \rho 1 *R*T/MW$

After putting all the values

$\rho 1 = 54.88*(P)/ (51.9 – P)$ ***Equation 15***

DERIVATION OF EQUATION 5

$$P = \frac{Z * \text{m} * R * T}{V * MW}$$

Put Equation 14 in above equation

$$P = \frac{(0.9456 - \text{P}/54.89) * \text{m} * R * T}{V * MW}$$

$$\text{P} = \frac{0.9456 * \text{m} * R * T}{V * MW} - \frac{\text{P} * \text{m} * R * T}{54.89 * V * MW}$$

$$\frac{\text{P} * V * MW}{\text{m} * R * T} + \frac{\text{P}}{54.89} = 0.9456$$

$$\text{P}\left[\frac{1}{54.89} + \frac{V\ M.W}{R\ T\ m}\right] = 0.9456$$

$$P = 0.9456 * \left[\frac{1}{54.89} + \frac{V\ M.W}{R\ T\ m}\right]^{-1} \qquad \textit{Equation 16}$$

The filling time for a single cylinder is fixed at 75 seconds (See cylinder properties above). Therefore, the simulation time for one filling cycle is chosen to be the same.

The equations presented in this section take the inputs for cylinder dimensions and the gas properties from the user and can predict the total mass of the cylinder at the end of a single filling cycle and the pressure of the cylinder. The combination of differential and algebraic equations presented in this section is numerically solved using the Runge-Kutta method. The solver algorithm is implemented in MATLAB to give the predicted values of the above-mentioned output.

6.3.3.6 MODEL CODE REVIEW

In this section, the MATLAB script used to code the equations explained in the above section and the conditional loops used to find the relations between different variables, are discussed. The section also contains the code used to plot the relations between the cylinder pressure, the mass of the cylinder and the flow rate of the gas in the cylinder. The complete code is presented in the Appendix. (Appendix A)

The model code contains 3 sections.

MAIN.m

This section begins with the data on the cylinder dimensions, gas properties and other operational parameters such as filling cycle. It is followed by two loops of 20 steps each where the gas flowrate and the filling time are changed from -10% to 10% of the range of correct operational values. For each value in this range, the correct function file (cylinder_cal_time.m and cylinder_cal_flow.m) is called, which contains the algorithm to calculate the total mass and the final pressure for a resulting filling cycle.

This file also presents the code to plot the graphs based on the results obtained from the simulation.

cylinder_cal_flow.m

This function file accepts the gas flow rate as input and directs it towards the ODE 45 solver. The filling time, in this case, is fixed at 75 seconds since the only variable in this part of the code is flowrate. The solver generates the dynamic values of the mass in the cylinder with time. The values of the mass inside the cylinder at the end of a single filling time is selected and is assigned to the final mass of the cylinder. In the next step, the resulting pressure in the cylinder is calculated by writing the pressure – mass relation presented in Equation 5.

cylinder_cal_time.m

This function file accepts the filling cycle time as an input and activates the ODE 45 solver. The gas flow rate, in this case, is fixed at 45 (m3/hr) since the only variable in this part of the

code is the filling time. The solver generates the dynamic values of the mass in the cylinder with time. This code acts in a somewhat similar sequence as the previous code by selecting the value of the mass inside the cylinder at the end of single filling time. In the next step, the resulting pressure in the cylinder is calculated by writing the pressure – mass relation presented in Equation 5.

mass_cal.m

In this section the differential eq. 1 is coded. This file gives the rate of change of mass at every time step. The 'ODE45 solver' to generate time-varying dynamic values of the mass inside the cylinder uses this value.

6.3.3.7 GAS MODEL EVALUATION

In the course of this thesis, a gas cylinder filling model has been developed and analysed: the gas cylinder model. Below, a brief explanation of our evaluation methodology is provided.

An interview was conducted with a Kuwaiti national gas company: Kuwait Oil Tanker Company (KOTC). In the interview, the model was demonstrated, and they gave approximate values for important variables such as gas flow, pressure, temperature and density, cylinder weights and other values. Their advice on possible critical and physical impacts, whenever there is an alteration of the gas attributes was followed. This interview aided this study for the purpose of evaluation and making the gas cylinder model closely resemble a real gas plant in Kuwait. The full interview is available in Appendix B.

6.3.3.8 GAS MODEL ATTACK TYPES:

The mathematical model has been proven as a precise replication of the real process of the 'gas cylinder filling system'. This model can provide an exact correlation between the pressure, gas flow rate and the filling time. The physical scenario of an external attack on the measuring/ monitoring system can be simulated by changing one of the parameters described above and

how these variations can be detected by comparing the values to the model's predicted values. Two types of attacks are simulated as follows:

- Random variations: This is random changes in a system state. If an attacker happens to make sudden changes in the filling time for instance, to increase the filling time at 1 instance and then suddenly decrease at every filling cycle. A random variable is an easier form of attack and chances of detecting them are easier.
- Systematic increase: A systematic increase is when the filling cycle time is changed in a single direction over a larger period of time. This sort of attack is difficult to detect. Since the gradual increase would often go undetected until the physical effect can be noticed.

6.3.3.9 CHANGING INFLOW

In this section, two conditions are simulated where the attacker could provide

- Random variations
- Systematic increase

These variations were provided in the gas flow rate filling the cylinder. This case is simulated in the code by providing a dummy inflow variable. The results from the simulation with the dummy inflow variables are compared with the pressure vs flow rate correlations obtained from the model described above. From the results presented in Figure 25 it can be inferred that in the case of an external influence where the gas inflow rate is being changed or tampered with, the output pressure in the cylinder can help to detect the event.

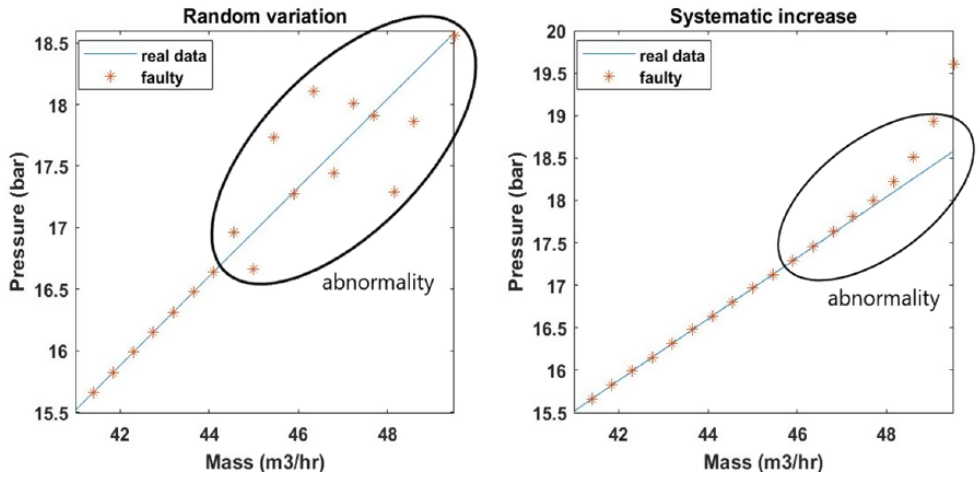


Figure 22:Detecting abnormality in flowrate (left) random variation (right) gradual increase

6.3.3.10 CHANGING FILLING TIME

A similar exercise was repeated, but in this case the variations were provided for the 'filling time' in the cylinder. The following two conditions were simulated where the attacker could provide:

- Random variation.
- Systematic increase

in the filling time. When the filling time is reduced the underfilling of the cylinder would result in a lower final pressure. Increasing the final pressure could result in a higher end pressure, which if allowed unchecked would result in a rupture. These two cases were simulated in MATLAB and the output pressure was compared with the values generated from the pressure vs time correlation graphs presented in the model above. From the plots presented in Figure 26, it would be possible to observe the presence of an abnormality in the measurements.

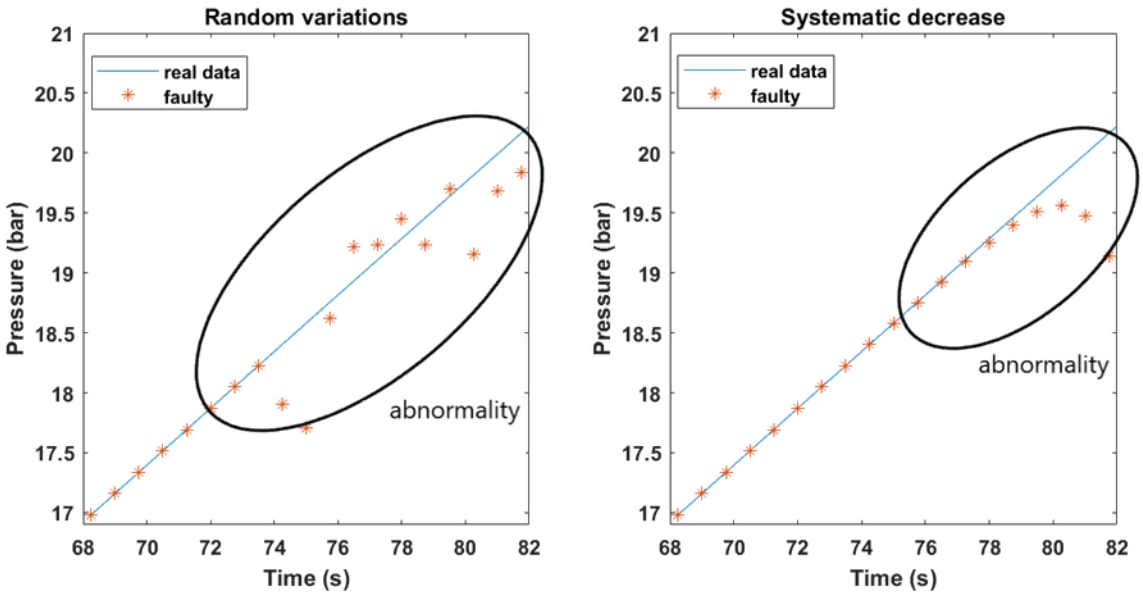


Figure 23:: Detecting abnormality in filling time (left) random variation (right) gradual decrease

6.3.3.11 APPLICATION OF ICSRANK ON RESEARCH CONCEPTS [GAS MODEL] (R)

As mentioned in chapter 4, the sub-categories inside each main category are flexible. Meaning they are customizable according to researchers and organization's needs. The reason is because sometimes new categories come out, some categories are removed or disappear and also security is subjective, meaning not all organization view security in the same lens. There are thousands of research concepts, tools and ideas. They include lots of information to be classified and assessed. Many of this information don't or can't fit into the proposed subcategories within the categories. Therefore, it's not practical to ignore this information or squeeze them into improper categorization.

Due to that, this research proposes a customizable system (S) and network (N) details to fit ICS devices, systems and ideas that are not commercial or industrial- being used in real industries. This type of categorizations includes research ideas, proof of concept, simulations tools and techniques. This would improve the OSINT value for the ICS security community and would indeed affect the security score of real ICS devices in the market. The aim of this thesis is to appreciate all kinds of knowledge in this field and to prove that this knowledge is of value to ICS security. This research adopts this concept and demonstrates below how this could be achieved. This kind of OSINT is labelled with a letter "R" to indicate that it's a research OSINT.

Stage 1: OSINT collection

The OSINT here is theoretical and conceptual. Therefore, the subcategories are filled based on the model specifications and assumptions. At this stage, listing of available OSINTs is mentioned. The later section discusses what to do with OSINT and its implication on security.

System details (S):

System name: Gas cylinder filling model

System details: Liquified Petroleum Gas (LPG) , see section (6.2.2) for more details about properties, pressure, flow rate, temperature and mass .

System functionality: The model is produced using mathematical equations. These equations are translated to a Simulink code

System data: The data is generated in graphs.

Industry domain: gas

Network details (N):

Network is modelled in Simulink

Network medium is assumed to be achieved via internet and then to a local network. The simulation is based on the threat model of Trisis malware in chapter 5 and early chapter 6.

Configuration (C)

Based on the Trisis threat model, the device was on a program mode.

Defence (D)

It is easier to detect random variation attacks than Systematic attacks. Therefore, this defensive (D) technique could be added to OSINT categories.

Technique (T)

Method of attacks on Triconex PLC:

- Change inflow
- Change filling time

Impact: Both attacks were done either systematically or by a random variation method. The systematic method causes more damage.

Vulnerability (O):

Based on the Trisis malware scenarios, in chapter 6 case study 1 and 2. There is a vulnerability: ICSA-18-107-02. This vulnerability allows an attacker to exploit and modify the memory buffer without restrictions.

Credential (P)

No available information. It doesn't exist for the Trisis incident.

Stage 2: OSINT assessment

Category / Secure

System (S): No

Network (N): Yes

Configuration (C): Yes

Defence (D): Yes

Technique (T): No

Vulnerability (O):NO

Credentials: N/A

System details (S):

There is a wealth of system (S) details that were collected from the gas cylinder model. This information could be added to OSINT for research purposes. This OSINT can enable asset owners of gas plants or researchers to understand gas filling operation by going through models and simulations. This is beneficial for those who have not yet own real gas facilities and are curious to learn or even build their own simulations. On the attacker perspective, this knowledge can help him/her get this knowledge too, because most cyber attackers don't know about physical systems such as gas plants. In addition, this information could be added to any

ICS device that belongs to this industrial domain for assessment purposes, which can be taken into account especially this model has been validated by a real gas company during this research. This information as labelled as insecure.

Network details (N):

There isn't much explained in this model alone about the network. However, it only demonstrates the variables mechanism. For example, what happens if a given variable such as a pressure change. This behaviour can implement by a researcher or an attacker based on the targeted ICS device and protocol. Therefore, this information can be of a value if the device and protocol are learned, like the Trisis incident. The attacker knew the system and the protocol, and it would be a bonus if he/she understood the basics of a gas properties that are explained in this model. Therefore, this category alone is labelled as secure.

Configuration details (C):

The model here hasn't got any information about this category. However, it was mentioned in the collection process that is based on real incident. So, if this perspective is taken into consideration. An attacker or a researcher may be able to look for default configurations that enable him/her to manipulate similar gas types. This category is labelled as secure.

Defence details (D):

The model demonstrates that systematic changes in gas properties is difficult to detect while the random variation are detectable. That give insights to prepare for these attacks and implement suitable mitigations strategies. This category is labelled as secure because of the availability of detection mechanisms that were observed in the model

Techniques (T):

A demonstration in depth of two types of attacks in the gas model and their impact on physical gas properties. These techniques can be applied to similar gas types and properties. Asset owners can benefit from these techniques and can guard against misbehaviour. Attackers on the other hand can harness this knowledge and build more sophisticated attacks. This category is labelled as insecure

Vulnerability (O):

This model demonstrates how to manipulate gas physical properties; therefore, it shows possible weaknesses (O) if applied on a real ICS device related to a gas industry. Like the above techniques, this makes this category insecure

Credentials (P):

No information was available in this category. This category is secure.

Stage 3: ICSrank scoring and conclusion:

This gas model based on the assessment earlier, has 1 main insecure category and 2 optional insecure optional categories. Based on ICSrank algorithms, this OSINT is labelled as a medium risk. The risk score is 7/10. Medium risks are scored 5/10. (see chapter 4). The extra insecure optional categories raise that figure up. This OSINT informs real physical properties of Liquified Petroleum Gas (LPG). The information as stated above can be included with any ICS devices assessment within a gas industry. There is an applicable OSINT information in ICS security. To understand ICS security, an understanding of industrial systems is required. The gas industry is widely established in the world and according to this research, these mechanical aspects are real. Therefore, it is important to understand these physical aspects together with the cyber aspects. This section is a contribution in this area. This study proves that research and theoretical concept should be included in the security assessment of ICS systems and shared online among ICS communities, to build a solid OSINT knowledge.

6.4 DISCUSSION AND CONCLUSION

ICSrank framework fills many of the gaps that many metrics systems lack in ICS (See CHAPTER 2). The one major concept or a drawback discussed in chapter 2, that this research aims to develop in this thesis is the accuracy of a device security level. What is meant by accuracy: the 7 ICS OSINT categories that have information about an ICS device security listed in section 6.3.1. They provide all together – when accurately combined - a good probability of risk occurrence (likelihood), thus making risk scoring more accurate. Unlike traditional IT risk assessment methods, where they depend mostly on time probability, which is risky [32]. In ICS security assessment, one cannot depend on probability. It can cause serious issues for an organization. For example, suppose a PLC has a critical vulnerability (maybe linked to a gas pipe), but because it is not a common vulnerability to be exploited, it was ranked as low based on occurrence probability. This can lead to flagging this vulnerability as non-critical and not important to patch. The priority level here is problematic [32] because if this PLC is critical for production and other processes, a disaster could happen if an attacker finds out about it and manages to exploit it.

The theoretical and practical usage of ICSrank methodology above can give significant knowledge about the security of a device. It can give a prediction of the level of security risk. When making a decision, the above information/framework can help estimate the risk value by considering ICS OSINT information and the calculation of risk score. Apparently, nobody knows or can obtain all the information listed in ICS OSINT. It all depends on who is doing the assessment and what is available on the public web. If an asset owner is doing it, there will be a more accurate estimation than if it is done by an external entity. Therefore, we suggest a methodology such as a public database of ICS OSINT information (See chapter 8). The idea of this suggestion is that this database collects information about existing ICS vulnerabilities and could be shared and edited in public, which could improve the accuracy of scoring risks and ICS security (see chapter 8).

The 1st and 2nd case studies; Triconex PLC and Trisis OSINT respectively, were presented to examine related OSINT. It was shown, that threat risk level could be estimated based on ICSrank algorithms. The results proved that ICS devices are affected by OSINT when it comes to OSINT security. It was observed in case study 2, OSINT risk level was low, because that

information was evaluated without a context. However, when it was combined with another OSINT for a given device such as Case 1, it raised the overall OSINT risk level to medium with a value close to high risk. This shows that risk scores that focus on one source of information without considering other factors- OSINT, are limited and non-informative about the actual risk. This argument was proven too in Chapter 4 findings for the Siemens PLC.

The 3rd case study demonstrated the value of considering research projects as a source of OSINT information. The risk value for that case was medium which indicates that this information can benefit the security of ICS devices and their OSINT. On the contrary, that argument was raised to not undervalue of research tools and information. Above is a gas cylinder filling system was developed for modelling the operation to replicate the process that occurs during the filling of a gas cylinder. The preliminary test of the model has shown that the basic relationships between various input and output variables have been met that validate the functioning of the model.

The research in this chapter, has provided a novel methodology to analyse and view OSINT information. There are 3 types of OSINT information: comprehensive, partial and conceptual. The comprehensive information is covered in case study 1, partial information in case study 2 and conceptual or research information in case study 3. The outcome of this contributes to ICS security assessment by improving risk accuracy of existed vulnerabilities. It also enables to extract more informative data about an ICS device and its risk. It also takes a whole approach that uses multi OSINT sources. ICSrank also assess and ranks individual. Even individual sources are treated differently than most of traditional metrics (already explained in chapter 4 and chapter 6). The ICSrank scoring methodology is not just built on mathematical equations or individual risk/vulnerability factors, on the contrary ICSrank adopts a more comprehensive framework that considers a multi-dimensional approach. It considers relative and critical information that are categorized, assessed and ranked based on algorithms that were based and built on established security frameworks and best practices. This chapter ends this research. The following is the last chapter and includes the thesis conclusion and future directions.

CHAPTER 7

GENERAL CONCLUSION

7.1 INTRODUCTION:

Critical infrastructures are being pushed towards automation and smart technology. Special search engines find ICS devices. ICS devices are exposed online more than ever. Even hidden devices deep within networks are found and targeted. That's mainly because the wealth of information in OSINT created new and sophisticated threats. The need to make sense of scattered information is necessary. Furthermore, the need to know what to do with it and how to view it. This chapter summarizes this research by presenting a general conclusion of research findings and future directions.

7.2 FUTURE DIRECTIONS:

- Development of an ICS Database: This database can fill a significant gap in the ICS security industry. Asset owners, policymakers, researchers and governments can use and contribute to this database. The database will have the following features:
    1. Improved collection process: This research is limited to few sources and is not automated. The proposed database will apply ICSrank framework throughout the 3 stages. It has a wider range of resources. It uses crawlers and API to collect data from the Internet. Categorization should have improved mining techniques and classification algorithms – preferably AI algorithms. There will be implemented

automation techniques to filter out raw data from search sources and store it as ICSrank categories.

2. Improved assessment process: The assessment process is done manually here and should be automated in the future database. The process should be intelligent enough to make decision and classify data as secure or not.
3. Improved ranking process: ICSrank scoring should be automated. Its algorithms will be implemented using a web programming langue that is capable to identify labels and categories and to make decisions.
4. Implementation of an update mechanism that updates the database regularly, its categories, and risk label for stored devices and information.

- Increase the research scope of ICSrank, applications and case studies. The finding can be included in the proposed ICS database above:

1. Include new types of OSINT information such as analysing google images and its security impact on ICS security. It could be achieved by implementing proven machine learning methods such as image recognition.
2. More research should be done on a wider variety of ICS devices and sectors as the scope of ICS devices for this research was limited. Another limitation of this research is that the methodology that was used throughout was not designed to address exploration in the gas sector in a thorough yet intensive manner.
3. Application of ICSrank on existing ICS malwares. The aim is to build and extract new knowledge and insights.
4. Analysis of more examples of CVSS-ranked vulnerabilities and devices and compare it with ICSrank framework. The research should include the usage of qualitative and quantitative approaches.

7.3 GENERAL CONCLUSION:

As the world becomes more interconnected, companies and governments will become more reliant than ever on the internet. However, this increased interconnectivity has brought an increased need for infrastructure cybersecurity. Both criminals and hostile governments are more than capable of launching crippling attacks on critical infrastructure such as power grids, telecommunications networks, and even electoral ballot counting systems. Both corporations and policymakers alike are calling for additional cyber-security infrastructure.

The motivation behind this research was to continue where previous researchers left off. We wanted to map out a taxonomy of cyber-attacks, cybersecurity vulnerabilities etc. and create a quantified scoring system to better gauge how vulnerable physical devices are against cyber-attacks. This would allow us to better identify weaknesses and prescribe solutions to future cyber-attack scenarios. This study was designed to acquire a better understanding of common cyber-security vulnerabilities and attacks using OSINT sources and pre-existing research from past infrastructure cybersecurity research. We wanted to demonstrate how certain cyber-attack vulnerabilities and impacts on physical devices are linked by using a gas pipeline and gas cylinder as a model.

After simulating "what-if" cyber-attack scenarios on our gas cylinder-filling model, we concluded that more interconnected systems are vulnerable to attacks. Furthermore, we analysed that the criticality of vulnerability in physical devices is also an important factor to consider. If a government or company does not follow certain cyber-security best practices, then the vulnerability of physical devices becomes more pronounced and the impact of cyber-attacks intensifies.

Industrial Control Systems are a ubiquitous part of managing physical sites in energy infrastructure. Therefore, discussing and addressing the inherent vulnerability of ICS is important to reduce infrastructure vulnerability. In this research, human ignorance is a critical factor when assessing cybersecurity vulnerability. This is because most cyber-attacks happen when the victim is caught unawares because they do not know the common vulnerabilities in cybersecurity infrastructure or the best practices in minimizing the risk of a cyber-attack. Therefore, any solution for increasing the security of energy infrastructure will require raising awareness of common security vulnerabilities.

The increased proliferation of OSINT sources such as Google, Shodan or social media has exacerbated the vulnerability of ICS against cyber-attacks. Attackers have access to a wealth of knowledge on a company or government's energy infrastructure, allowing them to exploit easily any vulnerability present in ICS devices. OSINT has also led to the rise of other methods of cyber-attacks such as phishing that allows malicious actors to access sensitive data on individuals and firms.

There is a call to use OSINT constructively to improve the security of critical infrastructure. This thesis contributes to knowledge by the introduction of a novel framework to view OSINT information that is related to ICS devices. The broader view of multi factors that affect a device security instead of a single factor is favourable, informative and accurate. A dynamic update of information approach is better than static approach. ICSrank is built on the above philosophy. Instead of relying on mathematical equations alone which are not built on rational ground like most metrics today, ICSrank builds its ground from open sources and relies on context. That doesn't mean single sources are not useful, it means they should be handled as a complement to other information. In ICSrank, dynamic means no information are obsolete. It also means adding of new information or even removing it. This can affect the risk level and keep up to date with new information. This approach is more favourable than relying on inaccurate and irrelevant information. The categorization in ICSrank is also flexible to adjust with certain sources as demonstrated in ch6 and also to suit the organization needs.

The abundance of information in the Internet makes it difficult to keep up with it, make sense of or use in cybersecurity. There must be an established direction by figuring out what information to look for and preferably where. Categorization of information helps in this direction. Established databases and source provide wealth of critical information to choose from. Familiarity of cyber security basics for IT in general and OT in specific is a key factor. ICSrank categories is built upon knowledge of essential security information for ics devices. ICSrank is composed of 7 categories that make sense of this wealth of information. Those categories are applicable to ICS devices both online and offline. Every category has subcategories as they a treated like an assessment check list.

The ability to assess and analyse information is a must in security practices. For example, how to make sense of it and what to do with it. In order to make precautions and implement defences, information must be put in context. Information in the Internet can be of value or no value at

all. It Can affect security, or it can't. ICSrank classifies information into major and optional information. An information is of value if it has certain and compulsory data in it. ICSrank evaluates information as valid, if certain criteria are met. Then it classifies this information as secure or insecure. Some information is missing and is labelled as non-available accordingly

In order to make decisions on available information in the Internet easier, it has to be processed. ICSrank processes this information into well informing data. The goal is to evaluate the data risk level. Numerical values are not important like in most existed metrics. In ICSrank, the value is in the meaning of output and its practicality. The concept here in ICSrank is common sense, the more sensitive information is available, the more issues and possibly higher chances of threats could happen. ICSrank is built on this concept. There is core information that are essential to know about and protect with regard to an ICS device. Other types of information are a bonus and can increase the likelihood of risk occurrence and threat attractiveness. ICSrank score indicates what is critically known about a device and what's its position in being an attractive to a threat. Knowing this position is vital to establish security controls, because ICSrank guides what to focus on. It gives also an indication of future risks.

This research offers a security solution in critical infrastructure. It opens doors to many aspects of security practices. Taking action should be based on real and good data. Many solutions lack efficiency, because they were not built on accurate information. Wrong or inaccurate information leads to wrong assessment and therefore leads to wrong output. This research is a step in the direction towards obtaining, viewing and evaluating the right information with ICSrank lenses.

REFERENCES

[1] K. Stouffer, J. Falco, and K. Scarfone, “Guide to Industrial Control Systems (ICS) Security,” 2011. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf. [Accessed: 26-June-2018].

[2] “DNP - Overview of the DNP3 Protocol.” [Online]. Available: http://www.dnp.org/Pages/AboutDefault.aspx. [Accessed: 26-June-2018].

[3] “IEC - International Electrotechnical Commission.” [Online]. Available: http://www.iec.ch/. [Accessed: 07-June-2018].

[4] “Modbus Technical Resources.” [Online]. Available: http://www.modbus.org/tech.php. [Accessed: 26-June-2018].

[5] “PI - PROFIBUS & PROFINET International: Home.” [Online]. Available: http://www.profibus.com/. [Accessed: 14-June-2018].

[6] “American Gas Association - Natural Gas.” [Online]. Available: http://www.aga.org/Pages/default.aspx. [Accessed: 26-June-2018].

[7] “Modbus Interactions.” [Online]. Available: http://gridconnect.com/blog/wp-content/uploads/2013/03/MODBUS-Request-Response.bmp. [Accessed: 26-May-2018].

[8] “Hacker jailed for revenge sewage attacks • The Register.” [Online]. Available: http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/. [Accessed: 22-May-2018].

[9] “Slammer worm crashed Ohio nuke plant network.” [Online]. Available: http://www.securityfocus.com/news/6767. [Accessed: 22-May-2018].

[10] B. Miller and D. Rowe, “A survey SCADA of and critical infrastructure incidents,” in Proceedings of the 1st Annual conference on Research in information technology - RIIT ’12, 2012, p. 51.

[11] “Summing up Stuxnet in 4 Easy Sections - (plus Handy Presentation) | Tofino Industrial Security Solution”, Tofinosecurity.com, 2011. [Online]. Available: http://www.tofinosecurity.com/blog/summing-stuxnet-4-easy-sections-plus-handy-presentation. [Accessed: 27-June-2018].

[12] Idaho National Laboratory, “Vulnerability Analysis of Energy Delivery Control Systems,” 2011. [Online]. Available: http://energy.gov/sites/prod/files/Vulnerability Analysis of Energy Delivery Control Systems.pdf. [Accessed: 26-June-2018].

[13] V. M. Igure, S. A. Laughter, and R. D. Williams, “Security issues in SCADA networks,” Comput. Secur., vol. 25, no. 7, pp. 498–506, May. 2006.

[14] “Modbus packet.” [Online]. Available: http://www.digitalbond.com/wp-content/uploads/2011/02/Modbus2.png. [Accessed: 26-May-2018].

[15] R. C.-W. Phan, “Authenticated Modbus Protocol for Critical Infrastructure Protection,” IEEE Transactions on Power Delivery, vol. 27, no. 3, pp. 1687–1689, Jul. 2012.

[16] G.-Y. Liao, Y.-J. Chen, W.-C. Lu, and T.-C. Cheng, “Toward Authenticating the Master in the Modbus Protocol,” IEEE Transactions on Power Delivery, vol. 23, no. 4, pp. 2628–2629, Oct. 2008.

[17] T. H. Morris, B. A. Jones, R. B. Vaughn, and Y. S. Dandass, “Deterministic Intrusion Detection Rules for MODBUS Protocols,” in 2013 46th Hawaii International Conference on System Sciences, 2013, pp. 1773–1781.

[18] T. Morris, R. Vaughn, and Y. Dandass, “A Retrofit Network Intrusion Detection System for MODBUS RTU and ASCII Industrial Control Systems,” in System Science (HICSS), 2012 45th Hawaii International Conference on, 2012, pp. 2338–2345.

[19] I. Nai Fovino, A. Coletta, A. Carcano, and M. Masera, “Critical State-Based Filtering System for Securing SCADA Network Protocols,” IEEE Trans. Ind. Electron., vol. 59, no. 10, pp. 3943–3950, Oct. 2012.

[20] S. Parthasarathy and D. Kundur, “Bloom filter-based intrusion detection for smart grid SCADA,” in Electrical & Computer Engineering (CCECE), 2012 25th IEEE Canadian Conference on, 2012, pp. 1–6--.

[21] W. Tang and A. Sui, “Secure protocol lifecycle and its application in power industry,” in 2008 Third International Conference on Electric Utility Deregulation and Restructuring and Power Technologies, 2008, pp. 592–597.

[22] N. Cai, J. Wang, and X. Yu, “SCADA system security: Complexity, history and new developments,” in 2008 6th IEEE International Conference on Industrial Informatics, 2008, pp. 569–574.

[23] W. H. Han, G. W. Zhang, Z. P. Wang, and H. X. Ren, “Teaching Reform on the Course of Measurement & Control Instrument Network Technology,” Natl. Teach. Semin. Cryptogr. Inf. Secur., pp. 77–79, 2010.

[24] P. Huitsing, R. Chandia, M. Papa, and S. Shenoi, “Attack taxonomies for the Modbus protocols,” Int. J. Crit. Infrastruct. Prot., vol. 1, pp. 37–44, 2008.

[25] “Modbus TCP Rules.” [Online]. Available: http://www.digitalbond.com/tools/quickdraw/modbus-tcp-rules/. [Accessed: 18-May-2018].

[26] I. N. Fovino, M. Masera, L. Guidi, and G. Carpi, “An experimental platform for assessing SCADA vulnerabilities and countermeasures in power plants,” in 3rd International Conference on Human System Interaction, 2010, pp. 679–686.

[27] I. Nai Fovino, A. Carcano, M. Masera, and A. Trombetta, “An experimental investigation of malware attacks on SCADA systems,” Int. J. Crit. Infrastruct. Prot., vol. 2, no. 4, pp. 139–145, Dec. 2009.

[28] I. Fovino, M. Masera, and A. Colleta, “Taxonomy of security solutions for the SCADA Sector,” 2010. [Online]. Available: http://www.cen.eu/cen/Sectors/Sectors/ISSS/Focus/Documents/D22.pdf.

[29] I. N. Fovino, A. Carcano, T. D. L. Murel, A. Trombetta, M. Masera, and I. C. Soc, “Modbus/DNP3 State-based Intrusion Detection System,” Int. Conf. Adv. Inf. Netw. Appl., pp. 729–736, 2011.

[30] C. Queiroz, A. Mahmood, J. Hu, Z. Tari, and X. Yu, “Building a SCADA Security Testbed,” in 2009 Third International Conference on Network and System Security, 2009, pp. 357–364.

[31] I. Fovino, A. Carcano, M. Masera, and A. Trombetta, “Design and implementation of a secure modbus protocol,” Crit. Infrastruct. Prot. III, pp. 83–96, 2009.

[32] E. Knapp, “Chapter 4 - Industrial Network Protocols,” in Industrial Network Security, Boston: Syngress, 2011, pp. 55–87.

[33] S. East, J. Butts, M. Papa, and S. Shenoi, “A taxonomy of attacks on the DNP3 protocol,” in IFIP Advances in Information and Communication Technology, vol. 311, C. Palmer and S. Shenoi, Eds. Berlin: Springer-Verlag Berlin, 2009, pp. 67–81.

[34] T. Mander, R. Cheung, and F. Nabhani, “Power system DNP3 data object security using data sets,” Comput. Secur., vol. 29, pp. 487–500, 2010.

[35] J. Akerberg and M. Bjorkman, “Exploring Security in PROFINET IO,” in Computer Software and Applications Conference, 2009. COMPSAC ’09. 33rd Annual IEEE International, 2009, vol. 1, pp. 406–412.

[36] M. Baud and M. Felser, “Profinet IO-Device Emulator based on the Man-in-the-middle Attack,” in Emerging Technologies and Factory Automation, 2006. ETFA ’06. IEEE Conference on, 2006, pp. 437–440.

[37] R. L. Rutledge, A. K. Massey, A. I. Antón, and P. Swire, “Defining the Internet of Devices: Privacy and Security Implications,” 2014.

[38] T. text provides general information S. assumes no liability for the information given being complete or correct D. to varying update cycles and S. C. D. M. up-to-D. D. T. R. in the Text, “Internet of Things: Statistics and Facts,” www.statista.com. [Online].

Available: https://www.statista.com/topics/2637/internet-of-things/. [Accessed: 20-June-2018].

[39] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” Comput. Netw., vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[40] E. Vasilomanolakis, J. Daubert, M. Luthra, V. Gazis, A. Wiesmaier, and P. Kikiras, “On the Security and Privacy of Internet of Things Architectures and Systems.”

[41] “Internet of Things Top Ten 2014-OWASP.pdf,” Google Docs. [Online]. Available: https://drive.google.com/file/d/0B52IUvO0LP6ON2VzZVFkNGF6aVE/view?usp=sharing&usp=embed_facebook. [Accessed: 29-June-2018].

[42] “Open-Source Intelligence ATP 2-22.9 - atp2-22-9.pdf.” [Online]. Available: https://fas.org/irp/doddir/army/atp2-22-9.pdf. [Accessed: 31-May-2018].

[43] “Project SHINE Findings Report (1-Oct-2014),” 09:39:46 UTC.

[44] “Project SHINE: 1,000,000 Internet-Connected SCADA and ICS Systems and Counting | Tofino Industrial Security Solution.” [Online]. Available: https://www.tofinosecurity.com/blog/project-shine-1000000-internet-connected-scada-and-ics-systems-and-counting. [Accessed: 23-May-2018].

[45] “What is industrial internet of things (IIoT)? - Definition from WhatIs.com,” IoT Agenda. [Online]. Available: https://internetofthingsagenda.techtarget.com/definition/Industrial-Internet-of-Things-IIoT. [Accessed: 06-Jul-2018].

[46] “BlackEnergy APT Attacks | What is BlackEnergy? | Threat Definition | Kaspersky Lab.” [Online]. Available: https://www.kaspersky.com/resource-center/threats/blackenergy. [Accessed: 29-Aug-2018].

[47] Z. Flom, "Shedding Light on BlackEnergy With Open Source Intelligence", Recorded Future, 2016. [Online]. Available: https://www.recordedfuture.com/blackenergy-malware-analysis/. [Accessed: 18- Sep- 2018].

[48] E. P. Leverett, “Quantitatively assessing and visualising industrial system attack surfaces,” Univ. Camb. Darwin Coll., vol. 7, 2011.

[49] M. Pendleton, R. Garcia-Lebron, and S. Xu, “A Survey on Security Metrics,” ArXiv Prepr. ArXiv160105792, 2016.

[50] “CVSS and the Internet of Things.” [Online]. Available: https://insights.sei.cmu.edu/cert/2015/09/cvss-and-the-internet-of-things.html. [Accessed: 26-June-2018].

[51] “DNV GL reveals top ten cyber security vulnerabilities for the oil and gas industry,” DNV GL. [Online]. Available: https://www.dnvgl.com/news/dnv-gl-reveals-top-ten-

cyber-security-vulnerabilities-for-the-oil-and-gas-industry-48532. [Accessed: 19-Apr-2018].

[52] A. Humayed, J. Lin, F. Li, and B. Luo, “Cyber-Physical Systems Security–A Survey,” ArXiv Prepr. ArXiv170104525, 2017.

[53] U. P. D. Ani, H. He, and A. Tiwari, “Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective,” J. Cyber Secur. Technol., pp. 1–43, 2016.

[54] “Internet of Things Top Ten 2014-OWASP.pdf,” Google Docs. [Online]. Available: https://drive.google.com/file/d/0B52IUvO0LP6ON2VzZVFkNGF6aVE/view?usp=sharing&usp=embed_facebook. [Accessed: 29-Jul-2018].

[55] L. D. Xu, W. He, and S. Li, “Internet of Things in Industries: A Survey,” IEEE Trans. Ind. Inform., vol. 10, no. 4, pp. 2233–2243, Nov. 2014.

[56] T. Abera et al., “Invited-Things, trouble, trust: on building trust in IoT systems,” in Proceedings of the 53rd Annual Design Automation Conference, 2016, p. 121.

[57] J. Romero-Mariona, R. Hallman, M. Kline, J. San Miguel, M. Major, and L. Kerr, “Security in the Industrial Internet of Things,” 2016.

[58] Y.-S. Ko, I.-K. Ra, and C.-S. Kim, “A Study on IP Exposure Notification System for IoT Devices Using IP Search Engine Shodan,” Int. J. Multimed. Ubiquitous Eng., vol. 10, no. 12, pp. 61–66, 2015.

[59] “Oil-and-Gas-Cyber-security-from-SAP-to-ICS.pdf.” [Online]. Available: https://erpscan.com/wp-content/uploads/publications/Oil-and-Gas-Cyber-security-from-SAP-to-ICS.pdf. [Accessed: 16-May-2018].

[60] K. Habib and W. Leister, “Threats identification for the smart Internet of Things in eHealth and adaptive security countermeasures,” in 2015 7th International Conference on New Technologies, Mobility and Security (NTMS), 2015, pp. 1–5.

[61] T. Frantti, H. Hietalahti, and R. Savola, “A risk-driven security analysis and metrics development for WSN-MCN router,” in 2013 International Conference on ICT Convergence (ICTC), 2013, pp. 342–347.

[62] J. Anu, R. Agrawal, C. Seay, and S. Bhattacharya, “Smart Grid Security Risks,” in 2015 12th International Conference on Information Technology - New Generations (ITNG), 2015, pp. 485–489.

[63] A. W. Atamli and A. Martin, “Threat-Based Security Analysis for the Internet of Things,” in 2014 International Workshop on Secure Internet of Things (SIoT), 2014, pp. 35–43.

[64] P. W. Parfomak, “Pipeline Cybersecurity: Federal Policy,” 2012.

[65] D. Beresford, “Exploiting Siemens Simatic S7 PLCs,” Black Hat USA, 2011.

[66] K. Wilhoit, “Who’s Really Attacking Your ICS Equipment?” Trend Micro, 2013.

[67] “Cyber Threat Source Descriptions | ICS-CERT.” [Online]. Available: https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions. [Accessed: 03-Aug-2018].

[68] B. Miller and D. Rowe, “A survey SCADA of and critical infrastructure incidents,” in Proceedings of the 1st Annual conference on Research in information technology, 2012, pp. 51–56.

[69] “Censys,” Censys. [Online]. Available: https://censys.io/. [Accessed: 13-Aug-2018].

[70] R. D. Graham, “MASSCAN: Mass IP port scanner,” URL Httpsgithub Comrobertdavidgrahammasscan, 2014.

[71] “Shodan.” [Online]. Available: https://www.shodan.io/. [Accessed: 25-July-2018].

[72] “ZMap · The Internet Scanner.” [Online]. Available: https://zmap.io/. [Accessed: 04-Aug-2018].

[73] J. François, A. Lahmadi, V. Giannini, D. Cupif, F. Beck, and B. Wallrich, “Optimizing internet scanning for assessing industrial systems exposure,” in 2016 International Wireless Communications and Mobile Computing Conference (IWCMC), 2016, pp. 516–522.

[74] R. Bodenheim, J. Butts, S. Dunlap, and B. Mullins, “Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices,” Int. J. Crit. Infrastruct. Prot., vol. 7, no. 2, pp. 114–123, Jun. 2014.

[75] P. M. Williams, “Distinguishing Internet-facing ICS Devices Using PLC Programming Information,” DTIC Document, 2014.

[76] R. C. Bodenheim, “Impact of the Shodan Computer Search Engine on Internet-facing Industrial Control System Devices,” DTIC Document, 2014.

[77] “SCADA detection cheat sheet - v.1.0.xlsx - OWASP.” [Online]. Available: https://www.owasp.org/index.php/File:SCADA_detection_cheat_sheet_-_v.1.0.xlsx. [Accessed: 29-July-2018].

[78] M. Pendleton, R. Garcia-Lebron, and S. Xu, “A Survey on Security Metrics,” ArXiv Prepr. ArXiv160105792, 2016.

[79] “Offensive Security’s Exploit Database Archive.” [Online]. Available: https://www.exploit-db.com/. [Accessed: 16-May-2018].

[80] “NVD - Home.” [Online]. Available: https://nvd.nist.gov/. [Accessed: 16-Aug-2018].

[81] "CVSSv2 Shortcomings, Faults, and Failures Formulation", Riskbasedsecurity.com, 2013. [Online]. Available: https://www.riskbasedsecurity.com/2013/02/cvssv2-shortcomings-faults-and-failures-formulation/. [Accessed: 01- Sep- 2018].

[82] "CVSS and the Internet of Things." [Online]. Available: https://insights.sei.cmu.edu/cert/2015/09/cvss-and-the-internet-of-things.html. [Accessed: 26-July-2018].

[83] W. E. Burr et al., "Electronic Authentication Guideline," Spec. Publ. NIST SP - 800-63-1, Dec. 2011.

[84] B. Genge and C. Enăchescu, "Article title: ShoVAT: Shodan-based vulnerability assessment tool for Internet-facing services," 2014.

[85] S. Samtani, S. Yu, H. Zhu, M. Patton, and H. Chen, "Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques," in 2016 IEEE Conference on Intelligence and Security Informatics (ISI), 2016, pp. 25–30.

[86] E. P. Leverett, "Quantitatively assessing and visualising industrial system attack surfaces," Univ. Camb. Darwin Coll., vol. 7, 2011.

[87] S. Lee and T. Shon, "Open source intelligence base cyber threat inspection framework for critical infrastructures," in 2016 Future Technologies Conference (FTC), 2016, pp. 1030–1033.

[88] "OSINT Training by Michael Bazzell | Open Source Intelligence Techniques." [Online]. Available: https://inteltechniques.com/links.html. [Accessed: 13-Aug-2018].

[89] "Intelligence Gathering - The Penetration Testing Execution Standard." [Online]. Available: http://www.pentest-standard.org/index.php/Intelligence_Gathering. [Accessed: 16-Aug-2018].

[90] "Censys," Censys. [Online]. Available: https://censys.io/. [Accessed: 13-Aug-2018].

[91] R. D. Graham, "MASSCAN: Mass IP port scanner," Available: https://github.com/robertdavidgraham/masscan, [Accessed:13-Aug-2018].

[92] "Shodan." [Online]. Available: https://www.shodan.io/. [Accessed: 25-July-2018].

[93] "ZMap · The Internet Scanner." [Online]. Available: https://zmap.io/. [Accessed: 04-Sep-2018].

[94] "Project SHINE Findings Report (1-Oct-2014)," 09:39:46 UTC.

[95] "Shodan Search Engine: Amphion Forum San Francisco," 18:14:21 UTC.

[96] “SANS Penetration Testing | Getting the Most Out of Shodan Searches | SANS Institute.” [Online]. Available: https://pen-testing.sans.org/blog/2015/12/08/effective-shodan-searches/. [Accessed: 16-July-2018].

[97] “Industrial Control Systems.” [Online]. Available: https://www.shodan.io/explore/category/industrial-control-systems. [Accessed: 24-Aug-2018].

[98] “SHODAN for Penetration Testers - DEFCON-18-Schearer-SHODAN.pdf.” [Online]. Available: https://www.defcon.org/images/defcon-18/dc-18-presentations/Schearer/DEFCON-18-Schearer-SHODAN.pdf. [Accessed: 27-Aug-2018].

[99] “Google Hacking Database (GHDB).” [Online]. Available: https://www.exploit-db.com/google-hacking-database/. [Accessed: 27-Aug-2018].

[100] “Bing.” [Online]. Available: https://www.bing.com/. [Accessed: 13-Aug-2018].

[101] “SCADA detection cheat sheet - v.1.0.xlsx - OWASP.” [Online]. Available: https://www.owasp.org/index.php/File:SCADA_detection_cheat_sheet_-_v.1.0.xlsx. [Accessed: 29-June-2018].

[102] “Google hacking,” Wikipedia. 22-Jul-2018.

[103] “ICS-CERT |.” [Online]. Available: https://ics-cert.us-cert.gov/. [Accessed: 13-Aug-2018].

[104] “Pastebin.com - #1 paste tool since 2002!” Pastebin.com. [Online]. Available: https://pastebin.com/.

[105] “Cyber Security for Critical Infrastructure Protection - SCADAhacker.” [Online]. Available: https://scadahacker.com/. [Accessed: 13-Aug-2018].

[106] “Digital Bond – For Secure & Robust ICS.” [Online]. Available: https://www.digitalbond.com/. [Accessed: 13-Aug-2018].

[107] Redpoint: Digital Bond’s ICS Enumeration Tools. Digital Bond, 2017.

[108] “OWASP.” [Online]. Available: https://www.owasp.org/index.php/Main_Page. [Accessed: 13-Aug-2018].

[109] S. StrangeLove, SCADAPASS: SCADA StrangeLove Default/Hardcoded Passwords List. 2017.

[110] K. Poojary, Nine OSINT tools every security researcher must have, [Online] https://www.computerweekly.com/photostory/2240160102/Nine-must-have-OSINT-tools/1/Nine-OSINT-tools-every-security-researcher-must-have

[111] "Recon-ng", Tools.kali.org, 2014. [Online]. Available: https://tools.kali.org/information-gathering/recon-ng. [Accessed: 18- Sep- 2018].

[112] Maltego, [Online available]: https://www.paterva.com/

[113] FOCA, [Online available]: https://www.elevenpaths.com/labstools/foca/index.html

[114] Metagoofil, [Online available]: https://tools.kali.org/information-gathering/metagoofil

[115] Amap, [Online available]: https://www.thc.org/thc-amap/

[116] Automator, [Online available]: http://www.tekdefense.com/automater/

[117] Braa, [Online available]: https://tools.kali.org/information-gathering/braa

[118] Dnmap, [Online available]: http://mateslab.weebly.com/dnmap-the-distributed-nmap.html

[119] Ghost Phisher, [Online available]: https://code.google.com/p/ghost-phisher/

[120] "mirandaupnptool", Code.google.com. [Online]. Available: https://code.google.com/archive/p/mirandaupnptool/. [Accessed: 18- Sep- 2018].

[121] Nmap, [Online available]: http://nmap.org/

[122] SMBMap, [Online available]: https://github.com/ShawnDEvans/smbmap

[123] E. P. Leverett, "Quantitatively assessing and visualising industrial system attack surfaces," Univ. Camb. Darwin Coll., vol. 7, 2011.

[124] "Google Hacking Database (GHDB)." [Online]. Available: https://www.exploit-db.com/google-hacking-database/. [Accessed: 27-Jul-2018].

[125] "Passive Reconnaissance," Security Sift, 05-Feb-2014. [Online]. Available: https://www.securitysift.com/passive-reconnaissance/. [Accessed: 08-Aug-2018].

[126] "SpiderControl SCADA Web Server | ICS-CERT." [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-17-234-03. [Accessed: 27-Aug-2018].

[127] S. Mittal, P. K. Das, V. Mulwad, A. Joshi, and T. Finin, "CyberTwitter: Using Twitter to generate alerts for cybersecurity threats and vulnerabilities," in 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), 2016, pp. 860–867.

[128] "NVD - CVSS." [Online]. Available: https://nvd.nist.gov/vuln-metrics/cvss. [Accessed: 26-Jul-2017].

[129] “Shodan.” [Online]. Available: https://www.shodan.io/. [Accessed: 25-June-2018].

[130] S. StrangeLove, SCADAPASS: SCADA StrangeLove Default/Hardcoded Passwords List. 2017.

[131] “Projects/OWASP Scada Security Project - OWASP.” [Online]. Available: https://www.owasp.org/index.php/Projects/OWASP_Scada_Security_Project. [Accessed: 19-July-2018].

[132] “Siemens SIMATIC S7-1200 CSRF Vulnerability | ICS-CERT.” [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-15-239-02. [Accessed: 03-Aug-2018].

[133] “Shodan Exploits.” [Online]. Available: https://exploits.shodan.io/welcome. [Accessed: 27-Aug-2018].

[134] “Industrial Control Systems.” [Online]. Available: https://www.shodan.io/explore/category/industrial-control-systems. [Accessed: 24-Aug-2018].

[135] M. Hall, “A Fast Introduction to Basic Servlet Programming,” 2002.

[136] “ICS-CERT |.” [Online]. Available: https://ics-cert.us-cert.gov/. [Accessed: 13-Aug-2018].

[137] M. Gjendemsjø, “Creating a Weapon of Mass Disruption: Attacking Programmable Logic Controllers,” 2013.

[138] K. A. Stouffer, J. A. Falco, and K. A. Scarfone, “Sp 800-82. guide to industrial control systems (ics) security: Supervisory control and data acquisition (scada) systems, distributed control systems (dcs), and other control system configurations such as programmable logic controllers (plc),” 2011.

[139] K. Stouffer, J. Falco, and K. Scarfone, “Guide to industrial control systems (ICS) security,” NIST Spec. Publ., vol. 800, no. 82, pp. 16–16, 2011.

[140] “Oil-and-Gas-Cyber-security-from-SAP-to-ICS.pdf.” [Online]. Available: https://erpscan.com/wp-content/uploads/publications/Oil-and-Gas-Cyber-security-from-SAP-to-ICS.pdf. [Accessed: 16-May-2018].

[141] “Internet of Things Top Ten 2014-OWASP.pdf,” Google Docs, 29-Jul-2015. [Online]. Available: https://drive.google.com/file/d/0B52IUvO0LP6ON2VzZVFkNGF6aVE/view?usp=sharing&usp=embed_facebook. [Accessed: 29-July-2018].

[142] Bryant, WD 2015, International Conflict and Cyberspace Superiority: Theory and Practice, Routledge.

[143] Cardenas, AA, Amin, S, Sinopoli, B, Giani, A, Perrig, A & Sastry, S 2009, 'Challenges for Securing Cyber Physical Systems', In Workshop on future directions in cyber-physical systems security, vol 5, pp. 11-23.

[144] Colbert, EJM & Kott, A 2016, Cyber-security of SCADA and Other Industrial Control Systems, Springer.

[145] Li, Z, Shahidehpour, M, Alabdulwahab, A & Abusorrah, A 2016, 'Bilevel Model for Analyzing Coordinated Cyber-Physical Attacks on Power Systems', IEEE Transactions on Smart Grid, vol 7, no. 5, pp. 2260-2272.

[146] Loukas, G 2015, Cyber-Physical Attacks: A Growing Invisible Threat, Butterworth-Heinemann.

[147] Macaulay, T & Singer, BL 2016, Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS, CRC Press.

[148] Pasqualetti, F, Dörfler, F & Bullo, F 2011, 'Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design', 2011 50th IEEE Conference on Decision and Control and European Control Conference, vol 1, no. 1, pp. 67-76.

[149] Pasqualetti, F, Dörfler, F & Bullo, F 2013, 'Attack Detection and Identification in Cyber-Physical Systems', IEEE Transactions on Automatic Control, vol 11, p. 58.

[150] Xia, Y, Liu, Y & Chen, H 2013, 'Architecture support for guest-transparent VM protection from untrusted hypervisor and physical attacks', 2013 IEEE 19th International Symposium on High Performance Computer Architecture (HPCA), vol 1, no. 1, pp. 28-43.

[151] Herrán-González, A., De La Cruz, J.M., De Andrés-Toro, B. and Risco-Martín, J.L., 2009. Modelling and simulation of a gas distribution pipeline network. Applied Mathematical Modelling, 33(3), pp.1584-1600.

[152] A. D. Woldeyohannes, M. Amin, and A. Majid, “Simulation of Natural Gas Transmission Pipeline Network System Performance,” J. Energy Power Eng., vol. 3, no. 12, pp. 1934–8975, 2009.

[153] D. Matko, G. Geiger, and W. Gregoritza, “Pipeline simulation techniques,” Math. Comput. Simul., vol. 52, no. 3–4, pp. 211–230, 2000.

[154] Herrán-González, A., De La Cruz, J.M., De Andrés-Toro, B. and Risco-Martín, J.L., 2009. Modelling and simulation of a gas distribution pipeline network. Applied Mathematical Modelling, 33(3), pp.1584-1600.

[155] S. L. Ke and H. C. Ti, “Transient analysis of isothermal gas flow in pipeline network,” Chem. Eng. J., vol. 76, no. 2, pp. 169–177, 2000.

[156] S. Wu, R. Z. Ríos-Mercado, E. A. Boyd, and L. R. Scott, “Model relaxations for the fuel cost minimization of steady-state gas pipeline networks,” Math. Comput. Model., vol. 31, no. 2–3, pp. 197–220, 2000.

[157] R. Ortiz Cebolla, B. Acosta, N. De Miguel, and P. Moretto, “Effect of precooled inlet gas temperature and mass flow rate on final state of charge during hydrogen vehicle refueling,” Int. J. Hydrogen Energy, vol. 40, no. 13, pp. 4698–4706, 2015.

[158] J. O. Andrzej, “Hierarchical Control of Transient Flow in Natural Gas Pipeline Systems,” vol. 5, no. 4, 1998.

[159] D. Matko, G. Geiger, W. Gregoritza, Pipeline simulation techniques, Math. Comput. Simul. 52 (2000) 211–230.

[160] J.Pamponet, P. Neto, Modelado dina´mico en redes de transporte de flujocompresible para aplicar en la deteccio´n de pe´rdidas entiempo real, Bol. Te´c. PETROBRAS, Rio de Janeiro, 45(2):abr./jun., 2002.

[161] J.Nivethan and M. Papa, "On the use of open-source firewalls in ICS/SCADA systems", Information Security Journal: A Global Perspective, vol. 25, no. 1-3, pp. 83-93, 2016.

[162] OWASP, "Top 10 2014-I10 Poor Physical Security - OWASP", Owasp.org, 2014. [Online]. Available: https://www.owasp.org/index.php/Top_10_2014-I10_Poor_Physical_Security. [Accessed: 16- Aug- 2018].

[163] S.Pechetti, A. Jindal and R. Bose, "Exploiting Mapping Diversity for Enhancing Security at Physical Layer in the Internet of Things", IEEE Internet of Things Journal, pp. 1-1, 2018.

[164] A. Bashir and A. Hussain Mir, "Securing Communication in MQTT enabled Internet of Things with Lightweight security protocol", EAI Endorsed Transactions on Internet of Things, vol. 3, no. 12, p. 154390, 2018.

[165] B.Padmanabhuni and H. Tan, "Techniques for Defending from Buffer Overflow Vulnerability Security Exploits", IEEE Internet Computing, 2011.

[166] A. Pal, "The Internet of Things (IoT) – Threats and Countermeasures", Cso.com.au, 2018. [Online]. Available: https://www.cso.com.au/article/575407/internet-things-iot-threats-countermeasures/. [Accessed: 16- Aug- 2018].

[167] R.Piggin, “Using open source intelligence to improve ICS amp; SCADA Security,” in IET Seminar on Cyber Security for Industrial Control Systems, 2014, pp. 1–30.

[168] K.Wilhoit, “Who’s Really Attacking Your ICS Equipment?” Trend Micro, 2013.

[169] “Project SHINE Findings Report (1-Oct-2014),” 09:39:46 UTC.

[170] “Oil-and-Gas-Cyber-security-from-SAP-to-ICS.pdf.” [Online]. Available: https://erpscan.com/wp-content/uploads/publications/Oil-and-Gas-Cyber-security-from-SAP-to-ICS.pdf. [Accessed: 16-Aug-2018].

[171] R. C. Bodenheim, “Impact of the Shodan Computer Search Engine on Internet-facing Industrial Control System Devices,” DTIC Document, 2014.

[172] M. Pendleton, R. Garcia-Lebron, and S. Xu, “A Survey on Security Metrics,” ArXivPrepr. ArXiv160105792, 2016.

[173] B. Genge and C. Enăchescu, "ShoVAT: Shodan-based vulnerability assessment tool for Internet-facing services", Security and Communication Networks, vol. 9, no. 15, pp. 2696-2714, 2015.

[174] E. P. Leverett, “Quantitatively assessing and visualising industrial system attack surfaces,” Univ. Camb. Darwin Coll., vol. 7, 2011.

[175] “Honeypot Or Not.” [Online]. Available: https://honeyscore.shodan.io/. [Accessed: 07-Aug-2018].

[176] “Industrial Control System.” [Online]. Available: cite

[177] M. Rouse, "What is internet of things (IoT)? - Definition from WhatIs.com", IoT Agenda. [Online]. Available: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT. [Accessed: 18- Sep- 2018].

[178] “What is Open-Source Intelligence (OSINT)?” [Online]. Available: https://software.microfocus.com/en-us/what-is/open-source-intelligence-osint. [Accessed: 01- Sep- 2018]

[179] “SCADA.” [Online]. Available: http://www.subnet.com/resources/dictionary/SCADA.aspx. [Accessed: 01- Sep- 2018]

[180] S. Mittal, P. K. Das, V. Mulwad, A. Joshi, and T. Finin, “CyberTwitter: Using Twitter to generate alerts for cybersecurity threats and vulnerabilities,” in IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), 2016, pp. 860–867.

[181] Techopedia, "What is the Secure Sockets Layer (SSL)? - Definition from Techopedia", Techopedia.com, 2019. [Online]. Available: https://www.techopedia.com/definition/24025/secure-sockets-layer-ssl. [Accessed: 26-Jul- 2019].

[182] Techopedia, "What is Transport Layer Security (TLS)? - Definition from Techopedia", Techopedia.com, 2019. [Online]. Available: https://www.techopedia.com/definition/4143/transport-layer-security-tls. [Accessed: 26- Jul- 2019].

[183] Techopedia, "What is an SQL Injection? - Definition from Techopedia", Techopedia.com, 2019. [Online]. Available: https://www.techopedia.com/definition/4126/sql-injection. [Accessed: 28- Jul- 2019].

[184] Techopedia, "What is Cross Site Scripting (XSS)? - Definition from Techopedia", Techopedia.com, 2019. [Online]. Available: https://www.techopedia.com/definition/24435/cross-site-scripting-xss. [Accessed: 28- Jul- 2019].

[185] Techopedia, "What is User Datagram Protocol (UDP)? - Definition from Techopedia", Techopedia.com, 2019. [Online]. Available: https://www.techopedia.com/definition/13460/user-datagram-protocol-udp. [Accessed: 28- Jul- 2019].

[186] Techopedia, "What is Simple Mail Transfer Protocol (SMTP)? - Definition from Techopedia", Techopedia.com, 2019. [Online]. Available: https://www.techopedia.com/definition/1710/simple-mail-transfer-protocol-smtp. [Accessed: 28- Jul- 2019].

[187] Techopedia, "What is Transmission Control Protocol (TCP)? - Definition from Techopedia", Techopedia.com, 2019. [Online]. Available: https://www.techopedia.com/definition/5773/transmission-control-protocol-tcp. [Accessed: 28- Jul- 2019].

[188] Techopedia, "What is Cross-Site Request Forgery (CSRF)? - Definition from Techopedia", Techopedia.com, 2019. [Online]. Available: https://www.techopedia.com/definition/172/cross-site-request-forgery-csrf. [Accessed: 28- Jul- 2019].

[189] E. Kyriakides and M. Polycarpou, Intelligent Monitoring, Control, and Security of Critical Infrastructure Systems. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015.

[190] Techopedia, "What is a Man-in-the-Middle Attack (MITM)? - Definition from Techopedia", Techopedia.com, 2019. [Online]. Available: https://www.techopedia.com/definition/4018/man-in-the-middle-attack-mitm. [Accessed: 28- Jul- 2019].

[191] GitHub, "What is Attack Surface Analysis and Why is it Important?", GitHub, 2019. [Online]. Available: https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Attack_Surface_Analysis_Cheat_Sheet.md. [Accessed: 29- Jul- 2019].

[192] Techopedia, "What is Spear Phishing? - Definition from Techopedia", Techopedia.com, 2019. [Online]. Available: https://www.techopedia.com/definition/4121/spear-phishing. [Accessed: 29- Jul- 2019].

[193] K. Popović and Ž. Hocenski, "Cloud computing security issues and challenges," The 33rd International Convention MIPRO, Opatija, 2010, pp. 344-349.

[194] OWASP, "File: SCADA detection cheat sheet - v.1.0.xlsx - OWASP", Owasp.org, 2019. [Online]. Available: https://www.owasp.org/index.php/File:SCADA_detection_cheat_sheet_-_v.1.0.xlsx. [Accessed: 30- Jul- 2019].

[195] Techopedia, "What is Honeypot? - Definition from Techopedia", Techopedia.com, 2019. [Online]. Available: https://www.techopedia.com/definition/10278/honeypot. [Accessed: 30- Jul- 2019].

[196] GE Digital, "Everything you need to know about IIoT | GE Digital", Ge.com, 2019. [Online]. Available: https://www.ge.com/digital/blog/everything-you-need-know-about-industrial-internet-things. [Accessed: 30- Jul- 2019].

[197] FIRST, "Common Vulnerability Scoring System SIG", FIRST — Forum of Incident Response and Security Teams, 2019. [Online]. Available: https://www.first.org/cvss/. [Accessed: 30- Jul- 2019].

[198] NIST, "NVD - CVE-2017-12741", Nvd.nist.gov, 2019. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2017-12741. [Accessed: 30- Jul- 2019].

[199] WhatIs, "What is passive reconnaissance? - Definition from WhatIs.com", WhatIs.com, 2019. [Online]. Available: https://whatis.techtarget.com/definition/passive-reconnaissance. [Accessed: 30- Jul- 2019].

[200] IVSS, "INDUSTRIAL VULNERABILITY SCORING SYSTEM (IVSS)", Securingics.com, 2019. [Online]. Available: http://www.securingics.com/IVSS/IVSS.html. [Accessed: 30- Jul- 2019].

[201] S4 Events, "A New CVSS For ICS Vulnerabilities", YouTube, 2019. [Online]. Available: https://www.youtube.com/watch?v=-6cThOCm9co&t=753s. [Accessed: 30- Jul- 2019].

[202] J. Spring, E. Hatleback, A. Householder, A. Manion and D. Shick, "TOWARDS IMPROVING CVSS", SOFTWARE ENGINEERING INSTITUTE | CARNEGIE MELLON UNIVERSITY, 2019.

[203] Shodan, "Industrial Control Systems", Shodan.io, 2019. [Online]. Available: https://www.shodan.io/explore/category/industrial-control-systems. [Accessed: 30- Jul- 2019].

[204] SANS, "SANS Penetration Testing | Getting the Most Out of Shodan Searches | SANS Institute", Pen-testing.sans.org, 2019. [Online]. Available: https://pen-testing.sans.org/blog/pen-testing/2015/12/08/effective-shodan-searches. [Accessed: 30- Jul- 2019].

[205] Techopedia, "What is a Backdoor? - Definition from Techopedia", Techopedia.com, 2019. [Online]. Available: https://www.techopedia.com/definition/3743/backdoor. [Accessed: 30- Jul- 2019].

[206] M. Assante and R. Lee, "SANS Institute: Reading Room - Industrial Control Systems / SCADA", Sans.org, 2019. [Online]. Available: https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297. [Accessed: 01- Aug- 2019].

[207] K. Jackson, "Triton/Trisis Attack Was More Widespread Than Publicly Known", Dark Reading, 2019. [Online]. Available: https://www.darkreading.com/attacks-breaches/triton-trisis-attack-was-more-widespread-than-publicly-known/d/d-id/1333661. [Accessed: 01- Aug- 2019].

[208] C. Bodungen, B. Singer, A. Shbeeb, S. Hilt and K. Wilhoit, Hacking Exposed Industrial Control Systems. London: McGraw Hill, 2017, pp. 90-92.

[209] J. Darlaston and J. Wintle, "Safety factors in the design and use of pressure equipment", Engineering Failure Analysis, vol. 14, no. 3, pp. 471-480, 2007. Available: 10.1016/j.engfailanal.2005.08.004 [Accessed 2 August 2019].

[210] CONPOT, "CONPOT ICS/SCADA Honeypot", Conpot.org, 2019. [Online]. Available: http://conpot.org/. [Accessed: 05- Aug- 2019].

[211] Dragos, "TRISIS Malware: Analysis of Safety System Targeted Malware", Dragos.com, 2019. [Online]. Available: https://dragos.com/wp-content/uploads/TRISIS-01.pdf. [Accessed: 05- Aug- 2019].

[212] V. M. Igure, S. A. Laughter, and R. D. Williams, “Security issues in SCADA networks,” Comput. Secur., vol. 25, no. 7, pp. 498–506, Oct. 2006, doi: 10.1016/j.cose.2006.03.001.

[213] “Significant Cyber Incidents | Center for Strategic and International Studies.” https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents (accessed Jun. 18, 2020).

[214] “10 Tips for Doing OSINT Legally,” Media Sonar Technologies. https://mediasonar.com/2020/03/11/10-tips-for-doing-osint-legally/ (accessed May 25, 2020).

[215] “Microsoft Cloud Penetration Testing Rules of Engagement.” https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement (accessed May 25, 2020).

[216] “attackics.” https://collaborate.mitre.org/attackics/index.php/Main_Page (accessed May 26, 2020).

[217] MDudek-ICS, MDudek-ICS/TRISIS-TRITON-HATMAN. 2020.

[218] A. D. Pinto, Y. Dragoni, and A. Carcano, “TRITON: The First ICS Cyber Attack on Safety Instrument Systems,” p. 28.

[219] “Schneider Electric Triconex Tricon (Update B) | CISA.” https://www.us-cert.gov/ics/advisories/ICSA-18-107-02 (accessed Jun. 05, 2020).

[220] “HatMan - Safety System Targeted Malware (Update B) | CISA.” https://www.us-cert.gov/ics/MAR-17-352-01-HatMan-Safety-System-Targeted-Malware-Update-B (accessed Jun. 22, 2020).

[221] “A Totally Tubular Treatise on TRITON and TriStation,” FireEye. https://www.fireeye.com/blog/threat-research/2018/06/totally-tubular-treatise-on-triton-and-tristation.html (accessed Mar. 20, 2020).

[222] “Attackers Deploy New ICS Attack Framework ‘TRITON’ and Cause Operational Disruption to Critical Infrastructure,” FireEye. https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html (accessed Apr. 16, 2020).

[223] NozomiNetworks/tricotools. Nozomi Networks, 2020.

[224] Y. Dragoni, “New TRITON Analysis Tool: Wireshark Dissector for TriStation Protocol,” Nozomi Networks, Jul. 18, 2018. https://www.nozominetworks.com/blog/new-triton-analysis-tool-wireshark-dissector-for-tristation-protocol/ (accessed Mar. 13, 2020).

[225] “7.4. Expert Information.” https://www.wireshark.org/docs/wsug_html_chunked/ChAdvExpert.html (accessed Apr. 12, 2020).

APPENDIX

APPENDIX A: MATLAB CODE

a. MAIN.m

```
clear all
clc

global V Qin0 rho MW R T time0

%% VARIABLES USED IN THE SYSTEM
V = 0.937; %volume of the cylinder (m3)
rho=0.564; %density of the gas (kmol/m3)
R=8.3151*10^-2; %Gas constant (bar. m3/kmol. K)
T=378; %temperature (Kelvin)
MW=22.695; %molecular weight of the Gas (kg/kmol)
Qin0=45/3600; %flowrate of the gas (m3/sec)
time0=75; %filling time


%% CHANGES IN GAS FLOWRATE
for i=1:20
    Q_in(i)=Qin0*(0.9+i/100);
y_flow(: i)=cylinder_cal_flow(Q_in(i));
end


%% CHANGES IN FILLING TIME
%change in filling time
fori=1:20
    time(i)=time0*(0.9+i/100);
y_time(:,i)=cylinder_cal_time(time(i));
end


%% Plotting Graphs Case I
%Mass vs Flow
plot (Q_in*3600, y_flow(1,:),'-');
xlabel ('Gas Flowrate (m3/hr)') % x-axis label
ylabel ('Mass (kg)') % y-axis label
xlim ([41 49.5])
ylim ([26.9 29.5])

%Presure vs Flow
plot (Q_in*3600, y_flow(2,:),'-');
xlabel ('Mass (m3/hr)') % x-axis label
ylabel ('Pressure (bar)') % y-axis label
xlim ([41 49.5])
ylim ([15.49 18.6])
```

```
%Mass vs Pressure
plot (y_flow(1, :),y_flow(2,:),'-');
xlabel ('Mass (m3/hr)') % x-axis label
ylabel ('Pressure (bar)') % y-axis label
xlim ([26.9 29.5])
ylim ([15.49 18.6])


%% Plotting Graphs Case II
%Mass vs Flow
plot (Q_in*3600, y_time(1,:),'-');
xlabel ('Gas Flowrate (m3/hr)') % x-axis label
ylabel ('Mass (kg)') % y-axis label
xlim ([41 49.5])
ylim ([26.9 29.5])

%Presure vs Flow
plot (Q_in*3600, y_time(2,:),'-');
xlabel ('Mass (m3/hr)') % x-axis label
ylabel ('Pressure (bar)') % y-axis label
xlim ([41 49.5])
ylim ([15.49 18.6])

%Mass vs Pressure
plot (y_flow(1, :),y_time(2,:),'-');
xlabel ('Mass (m3/hr)') % x-axis label
ylabel ('Pressure (bar)') % y-axis label
xlim ([26.9 29.5])
ylim ([15.49 18.6])
```

b. cylinder_cal_flow.m

```
function y0 = cylinder_cal_flow(x)
global V MW R T Qin time0

Qin=x;
X0=16; %initial weight of the cylinder
[t, x] =ode45('mass_cal', [0 time0], X0);

W=x(end,1); %weight of the cylinder after 75 seconds

%CALCULATE THE PRESSURE
P=0.9716*((V*MW)/(R*T*(W-16)) +(105.26^-1)) ^-1;

y0=[W;P];
```

c. cylinder_cal_time.m

```
function y0 = cylinder_cal_time(x)
global V MW R T

X0=16; %initial weight of the cylinder
time=x; %filling time
[t,x]=ode45('mass_cal',[0 time], X0);

W=x(end,1); %weight of the cylinder after 75 seconds
```

```
%CALCULATE THE PRESSURE
P=0.9716*((V*MW)/(R*T*(W-16)) +(105.26^-1)) ^-1;

y0=[W;P];
```

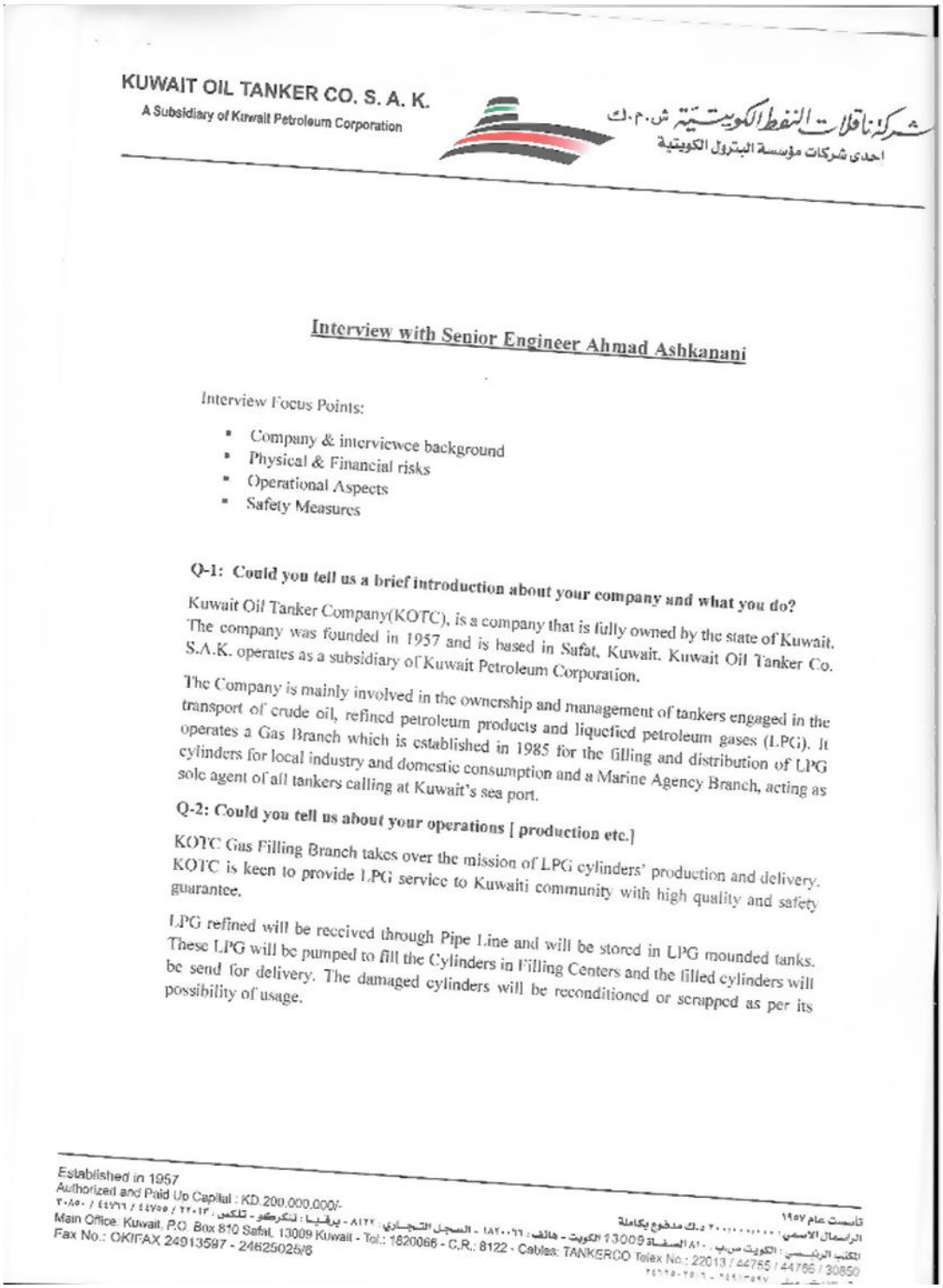
d. mass_cal.m

```
functiondydt = mass_cal(t, x)

global Qin rho MW

dydt=Qin*rho*MW;
```

APPENDIX B: INTERVIEW WITH A SENIOR ENGINEER (GAS COMPANY)



KUWAIT OIL TANKER CO. S. A. K.
A Subsidiary of Kuwait Petroleum Corporation

شركة ناقلات النفط الكويتية ش.م.ك
احدى شركات مؤسسة البترول الكويتية

Interview with Senior Engineer Ahmad Ashkanani

Interview Focus Points:

- Company & interviewee background
- Physical & Financial risks
- Operational Aspects
- Safety Measures

Q-1: Could you tell us a brief introduction about your company and what you do?

Kuwait Oil Tanker Company(KOTC), is a company that is fully owned by the state of Kuwait. The company was founded in 1957 and is based in Safat, Kuwait. Kuwait Oil Tanker Co. S.A.K. operates as a subsidiary of Kuwait Petroleum Corporation.

The Company is mainly involved in the ownership and management of tankers engaged in the transport of crude oil, refined petroleum products and liquefied petroleum gases (LPG). It operates a Gas Branch which is established in 1985 for the filling and distribution of LPG cylinders for local industry and domestic consumption and a Marine Agency Branch, acting as sole agent of all tankers calling at Kuwait's sea port.

Q-2: Could you tell us about your operations [production etc.]

KOTC Gas Filling Branch takes over the mission of LPG cylinders' production and delivery. KOTC is keen to provide LPG service to Kuwaiti community with high quality and safety guarantee.

LPG refined will be received through Pipe Line and will be stored in LPG mounded tanks. These LPG will be pumped to fill the Cylinders in Filling Centers and the filled cylinders will be send for delivery. The damaged cylinders will be reconditioned or scrapped as per its possibility of usage.

Established in 1957
Authorized and Paid Up Capital : KD.200,000,000/-
Main Office: Kuwait, P.O. Box 810 Safat, 13009 Kuwait - Tel.: 1820066 - C.R.: 8122 - Cables: TANKERCO Telex No.: 22013 / 44755 / 44766 / 30850
Fax No.: OKIFAX 24913597 - 24825025/6

تأسست عام ١٩٥٧
رأسمال الاسمي: ٢٠٠,٠٠٠,٠٠٠ د.ك مدفوع بكاملة
المكتب الرئيسي: الكويت ص.ب: ٨١٠ الصفاة 13009 الكويت - هاتف: ١٨٢٠٠٦٦ - السجل التجاري: ٨١٢٢ - برقيا: لنكركو - تلكس: ٢٢٠١٣ / ٤٤٧٥٥ / ٤٤٧٦٦ / ٣٠٨٥٠

Facts about LPG Cylinders:

- Time to fill: 75 seconds
- Pressure used to fill: 17 Bar
- Q(flow) used to fill: 45 m^3 / h
- Cylinder weight (empty): 16 kg
- Gas quantity inside a cylinder: 12 kg
- Filled cylinder: 28 kg

An average of 30,000 cylinders are produced in our filling centers per day.

Q-3: Could you tell us about physical and financial risks and impact if something goes wrong?

The physical and financial risks can be explained through some examples:

Example 1: Changing the inflow of the LPG at constant time
The increase in flow rate will increase the mass and pressure of pipelines. This would lead to the pipeline rupture and damages in filling centers which will result in production cost loss.
Example 2: Changing the filling time of LPG at constant flow rate
The increase in filling time will increase the mass and pressure of pipelines. This would lead to the pipeline rupture and damages in filling centers which will result in production cost loss. The company will face a loss of amount 3000/- KD per hour, in case of any operational failure.

Q-4: What are the financial costs impacted by operational malfunctions?

A loss of 750 Fills would be suffered per each LPG cylinders in case of any operational malfunctions.

Therefore, the financial loss per hour is:

4000 Cylinders' x 0.750 KD = 3000/- KD

Q-5: What are the safety measures that your company undertake to protect its gas operations?

- Gas leakage detection
- DCS protection.
- Safety relief valve
- Level protection tank (Level Switch)

Ahmed Ashkanani

Senior Operation Engineer

KOTC Gas Filling Branch-Shuaiba

Interview with senior engineer Ahmad Ashkanani # 2

Interview Focus points:

- Model design and data evaluation
- Safety PLC functionality and security
- Safety PLC attack taxonomy

Thanks for accepting to meet us for the second time. The aim of this second meeting is to discuss the above points. First: we have sent you the "Gas Cylinder Filling" model and model generated data. We also included our findings. We would be thankful if you take a look at our work and give us your feedback. Second: We are interested to know more about "Safety PLC" its operation, importance and security. Our motive is based on our research, we found that attackers target "safety systems" recently. This scenario is a real incident that happened in 2017 for a gas company in the Middle East. Third: We are thinking to develop an attack taxonomy on Safety PLC and study its impact. We appreciate if you could share with us your experience on those topics.

Topic 1: Model design and data evaluation

Q-1: Could you share with us your thoughts on the model design?

Answer: ***After reviewing the model design, everything seems perfect as well as the calculations is awesome***

Q-2: We used Simulink to simulate our model, we were able to generate data and graphs that represent: normal operation and two abnormal operations. How do you find our data/graphs?

Answer: ***they represented the real situation, which is ok***

Q-3: Please give us your feedback on our findings.

Answer: All are okey, just you need to mention dimensions of the LPG cylinder

KUWAIT OIL TANKER CO. S. A. K.
A Subsidiary of Kuwait Petroleum Corporation

شركة ناقلات النفط الكويتية ش.م.ك
إحدى شركات مؤسسة البترول الكويتية

Topic 2: Safety PLC functionality and security

Q-1: How many safety PLC do you have? Where?

Answer: filling centers: 5 PLCS , Tanks : 4 PLCS

Q-2: What's the role of safety PLC? How significant is it?

Answer: Safety PLC works as a guard for Operations PLC in order to check each action before anything happens

Q-3: What are the challenges that could affect a safety PLC?

Answer: any error has an impact on whole operation.

Topic 3: Safety PLC attack taxonomy

Q-1: What we learned today at the meeting, that safety PLC is responsible for many critical operations. This is a list of possibilities of operational misuse and their impact summed up in a table. Please share your opinion.

Action	Action Specific	Physical Property	Action symbol	Impact
Modify Flow	Increase	Flow (Q)	MQ1	Gas cylinder overfill, rapture
	Decrease		MQ2	Gas cylinder half fill
Modify time	Increase	Time (T)	MT1	Gas cylinder overfill, rapture
	Decrease		MT2	Gas cylinder half fill
Modify Air Pressure	Increase	Air Pressure (AP)	MAP1	Destroy air-based devices from high pressure
	Decrease		MAP2	Air-based devices don't operate, due to low pressure
Modify Gas Mass	Increase	Gas Mass (GM)	MGM1	Gas cylinder overfill, rapture
	Decrease		MGM2	Gas cylinder half fill
Modify Air supply	Close	Air Pressure (AP)	MAP3	No air flow, operations stop
Modify Sequence Values	Modify	Process Control (PS)	PS1	Affect entire process. e.g. If order of operation is affected, entire filling process fails
Modify Gas tank Level	Increase	Gas Tank Level (GTL)	MGTL1	Overfilled Tanks

KUWAIT OIL TANKER CO. S. A. K.
A Subsidiary of Kuwait Petroleum Corporation

شركة ناقلات النفط الكويتية ش.م.ك
إحدى شركات مؤسسة البترول الكويتية

Answer Topic 3

After reviewing the study, it has been figured out that the model almost reflects the real situation at the plant.
Moreover, the cases that are suggested from your side seems right as well as the predictions of actions invert the reality.

Ahmed Ashkanani
Senior Operation Engineer

Established in 1957
Authorized and Paid Up Capital : KD 200 000 000/-
Main Office: Kuwait, P.O. Box 810 Safat, 13009 Kuwait - Tel.: 1820000 - C.R.: 8122 - Cables: TANKERCO Telex No.: 22013 / 44755 / 44766 / 30650
Fax No.: OKOFAX 24913597 - 24825025/6

تأسست عام ١٩٥٧
الرأسمال الاسمي: ٢٠٠٠٠٠٠٠٠ د.ك مدفوع بكامله
المكتب الرئيسي: الكويت ص.ب ٨١٠ الصفاة 13009 الكويت - هاتف: ١٨٢٠٠٠٠ - السجل التجاري: ٨١٢٢ - برقيا: تنكركم - تلكس: ٢٢٠١٣ / ٤٤٧٥٥ / ٣٠٦٥٠ / ٤٤٧٦٦
رقم الفاكسميلي: ٢٤٨١٣٥٩٧ - ٢٤٨٢٥٠٢٥/٦