1-1-2015

A Threat Intelligence Framework for Access Control Security In The Oil Industry

Faisal Talal Alaskandrani
Purdue University

Graduate School Form 30
Updated 1/15/2015

PURDUE UNIVERSITY
GRADUATE SCHOOL
Thesis/Dissertation Acceptance

This is to certify that the thesis/dissertation prepared

By Faisal T. Alaskandrani

Entitled
A Threat Intelligence Framework for Access Control Security in the Oil Industry

For the degree of Master of Science

Is approved by the final examining committee:

Marcus Rogers
Chair

Eric Dietz

Baijian Yang

To the best of my knowledge and as understood by the student in the Thesis/Dissertation Agreement, Publication Delay, and Certification Disclaimer (Graduate School Form 32), this thesis/dissertation adheres to the provisions of Purdue University's "Policy of Integrity in Research" and the use of copyright material.

Approved by Major Professor(s): Marcus Rogers

Approved by: Marcus Rogers 12/09/2015
Head of the Departmental Graduate Program Date

A THREAT INTELLIGENCE FRAMEWORK FOR ACCESS CONTROL SECURITY IN THE OIL INDUSTRY

A Thesis

Submitted to the Faculty

of

Purdue University

by

Faisal T. Alaskandrani

In Partial Fulfillment of the

Requirements for the Degree

of

Master of Science

December 2015

Purdue University

West Lafayette, Indiana

For my Family, Father & Mother, Grandfather, & Grandmother, my six Sisters, my beloved Wife, and my two lovely kids, Layla & Hamza. You are the force of nature that made this happen. You where my backbone & Support, for that I thank you all and hope you are as happy as I am to have finished one more chapter in my life

TABLE OF CONTENTS

Page

Page

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

API	Application Programming Interface
APT	Advanced Persistent Threats
ARAMCO	Arabian American Company
CIF	Collective Intelligence Framework
ICS	Industrial Control Systems
IT	Information Technology
NIST	National Institute of Standards and Technology
OS	Operating Systems
OSTI	Open Source Threat Intelligence Framework
RTU.	Remote Terminal Unit
SABIC	Saudi Arabia Basic Industries Corporation
SAV	Server Aided Verification
SCADA	Supervisory Control and Data Acquisition Systems

GLOSSARY

Advanced Persistent Threats (APT s), are by far the biggest threat an organization could deal with since it is continuous and persistent until it achieves its goal. An example of that could be espionage from a different organization (Ponemon Institute LLC, 2014).

Community Sources, are members with trusted relationship with the energy company. Examples would be providers, suppliers or subsidiaries that has an economical mutual benefit from co-existing with the enterprise. For Example, Saudi Aramco, has close ties with Saudi Arabia Basic Industries Corporation (SABIC) another petrochemical company that could share information related to Cyber Threat Intelligence. Nonetheless, due to the nature of the company government security reports could also be available due to the national security implications of the company's operational requirement.

Deterrence, is the ability to retaliate and render the attacker means of attacking unavailable.

External Sources, are broken into two categories one which is publicly available information, and other paid reports from Security Agencies.

Hacktivists, are a group of individuals that are motivated by political agenda trying to influence decision making by inflecting damage or sabotaging the image of the targeted organization.

ICS, Industrial Control System (ICS) are systems that provide the ability to control industrial systems from a centralized location or a single device.

Insider Threats, is considered one of the top Attackers Category since its human in nature which is unpredictable. Employees who are disgruntled or others with ability to go over their clearance could prove to be a huge threat to any organization (Ponemon Institute LLC, 2014).

Internal Sources, such as Incident reports or data logs gathered from devices such as firewalls and routers or monitoring systems that secures networks and end nodes.

Nation State Actors, Another Attacker Category in the Threat Intelligence framework with organizations and global economy under political agenda it shows that sometimes nations gain from actions against organization being it a cyber war or retaliation of some sort (Ponemon Institute LLC, 2014).

Prevention and protection, All actions and process in place that fortifies the organization and minimizes the damage that can be taken by adversaries and this goes along with the minimum required from any organization regardless of the adversary in place.

Resilience, This strategy capitalizes on the fact the failure is inevitable and therefore minimizing the damage and effect after the fact should be minimal in assets and down time.

SCADA System, is a Supervisory Control System & Data Acquisition. That manages the gathering of data collected from a set of devices and displays it in a user friendly manner appropriate to the industry it is implanted in.

Script Kiddie, Another Attacker Category in the Threat Intelligence, who are usually individuals with no real agenda other than self-gratification from the ability to bypass security measures or inflicting damage to an easy target (Mateski, et al., 2012).

ABSTRACT

Alaskandrani, Faisal T. M.S., Purdue University, December 2015. A Threat Intelligence Framework for Access Control Security In The Oil Industry. Major Professor: Marcus Rogers.

The research investigates the problem raised by the rapid development in the technology industry giving security concerns in facilities built by the energy industry containing diverse platforms. The difficulty of continuous updates to network security architecture and assessment gave rise to the need to use threat intelligence frameworks to better asses and address networks security issues. Focusing on access control security to the ICS and SCADA systems that is being utilized to carry out mission critical and life threatening operations. The research evaluates different threat intelligence frameworks that can be implemented in the industry seeking the most suitable and applicable one that address the issue and provide more security measures. The validity of the result is limited to the same environment that was researched as well as the technologies being utilized. The research concludes that it is possible to utilize a Threat Intelligence framework to prioritize security in Access Control Measures in the Oil Industry.

CHAPTER 1. INTRODUCTION

1.1 Statement of the Problem

Due to the long lasting life cycle of energy industry facilities, control systems installed exceed their warranty or support period from different parties involved such as the operating system developer. Without the appropriate support, Industrial Control System (ICS) and Supervisory Control System & Data Acquisition SCADA systems become more prone to vulnerabilities and open to threats with no appropriate measures to overcome or contain the situation (Choo, 2011). Therefore, continuously finding appropriate measures and best practices that can be implemented across different platforms and segregated systems is a challenge and a security concern for companies and stakeholders in the energy section industry. A Threat Intelligence Framework in place would help streamline the process needed to fortify the facility and systems in place.

1.2 Significance of the Problem

The changing nature of the ICS systems developed for the energy industry has shifted from closed networks to open and connected ones (Igure, Laughter, & Williams, 2006). Although this provides greater, faster and easier access to involved parties and beneficiaries of those systems, it also poses a huge security threat. Systems developed in the past relied on isolation as a mechanism of protection and, therefore, security measures

had not been addressed. While the environment has changed from isolation to inclusion, the premise is still affecting the development cycle of the ICS and SCADA systems being used (Sommestad, Ekstedt, Holm, & Afzal, 2010). Moreover, the energy industry facilities in general are built and designed to last for several decades with minimum changes and continued maintenance. Therefore, hardware being used and systems installed eventually become obsolete, yet necessary for continues operation (Gold, 2009). Nonetheless, continuing to addressing those security concerns is important to companies working in the energy industry; hence, a threat intelligence framework is required.

Furthermore, the huge shadow bestowed by the energy industry; and specifically, the oil industry above all industries, begs the question of how important it is to the world economics and countries exporting or importing energy resources. Therefore, securing the production in different operations in those industries will help countries maintain their economic status, income, or revenue.

1.3 Scope of the Study

This study was limited to facilities hosting the Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition systems (SCADA). Furthermore, the study focuses on the energy section and primarily the oil industry within it. Moreover, the study involves Saudi Aramco Oil Company as an example that is used in this research. The company was selected due to the researcher's knowledge about the company during its recent cyber-attack in 2013.

Security challenges has been restricted to the lifecycle of the ICS and SCADA system development with regards to the operating system platforms and in conjunction

with current technologies associated with network security and threats. The research discusses several intelligence frameworks in order to find the suitable one that addresses continues reinforcement of network security.

1.4 Purpose of the Study

Today, ICS systems are rapidly evolving from proprietary to open standard protocols, from special purpose hardware and software to common Information Technology (IT) products, and from isolation to interconnection with corporate networks. Moreover, ICS systems were never designed with security in mind and many contain numerous security related vulnerabilities. On the other hand, technologies and devices used in the network industry out rapidly evolving providing a wider area of attack for any adversary. Therefore, continues revision and evaluation of network security procedures, practices, and devices is crucial to maintaining a safe and operational facility (Hieb, Chreiver, & Graham, 2013).

This thesis discussed threat intelligence frameworks that can be applied to Industrial Control Systems (ICS) security challenges such as ICS cyber security requirements, interactions with outside networks to gain access to security patches, and antivirus. The thesis explored several frameworks that could support the continuity of securing facilities and operation across the corporate network of Saudi Aramco.

1.5 Research Question

Can a threat intelligence framework prioritize security access control upgrades for industrial control systems in the oil industry?

1.6 Assumptions, Limitations & Delimitations

In this section the author is going to describe the assumptions and limitations and delimitations of the research question.

1.6.1 Assumptions

The current list is of assumptions for this master's thesis:

1- Information provided in the report is accurate and precise
2- Access control systems are appropriately maintained
3- SCADA system operators are experts and knowledgeable
4- No intentional error or malicious intention with employees working in security or handling ICS systems
5- Systems are updated appropriately
6- Security records are properly maintained and documented
7- Study assumes open budget and available funding for required security measures
8- Reasonable adherence to well-known Security and best practices
9- Compatibility measures are in place between different vendors and devices
10- Control systems installed are properly tested and verified before deployment and startup of the facility
11- Implementation of any framework is done in concurrence with any shutdown.
12- A single facility is used for framework comparison.

1.6.2 Limitations

The current list is the limitations for this master's thesis:

1- Sample and study was limited to the energy section industry
2- Information related to access control security was used.
3- Information is limited to public available resources only
4- Comparison is done based on a single facility
5- Financial expenses is limited to design and hardware required
6- Facilities being compared is limited to single stage facilities and not multiple stages.
7- Comparison values assigned to the framework is based on researcher personal knowledge in the industry.

1.6.3 Delimitations

The current list is of delimitations for this master's thesis:

1- Security controls that are not associated with access control as not included
2- Reports that are not cleared by Saudi Aramco was not used
3- Incomplete reports was not included in the study as source of information
4- Manpower required is not factored in this study.

1.7 Summary

The research at hand is addressing the means of continuously securing access control systems deployed in the energy section industry in order to protect its multiple layer network and different platforms. Security measures have been known to be an issue in facilities in the industry due to the nature of the business being static over long periods of time while technological advances in the network architecture changes rapidly (Gold, 2009).

Having different operating systems and control systems as well as hardware installed in facilities built for decades stands create a challenge for security experts to maintain security in general. Nonetheless, access control security is one aspect that eludes more than any since human evolvement is a major aspect. Restricting access has been one of the prime security measures that is known to humanity. Yet, in this century it has transcended physical world and introduced digital and virtual environments as well.

After examining and identifying the research merits, scope and significance the next chapter discusses current threat intelligence frameworks that can be utilized in the energy industry. Researcher provided an insight on literature available that is related to the research topic in the industry.

CHAPTER 2. REVIEW OF THE LITERATURE

The energy industry has always been crucial to world economics. Governments pay close attention and interest to the sector, and private companies are always catering and investing in supplying their demands and needs. The Industrial Control Systems (ICS) and Supervisory Control and Acquisition systems (SCADA) are both examples of systems that are used by energy companies and customized to their desire or to how much is being paid. Nevertheless, such systems have their own product life cycle (PLC) that affects the security and business continuity of companies working in the energy industry including oil and gas.

The nature of the operation environment, being its economic importance to the stake holders or the safety of the employees running the equipment adds to the importance of security including access control measures (Leith & Piper, 2013). Moreover, ICS systems deal with life threatening variables such high pressure, power, temperature, and flow. Each of these, if not controlled and properly monitored, could lead to casualties and irreversible consequences to the involved assets or environment.

2.1 Variables in ICS

Facilities in the energy industry are built to last for several decades with minimum changes given regular maintenance. Therefore, hardware and software selection and

installation is meticulous to insure compatibility and minimum intervention (Ralstona, Grahamb, & Hiebb, 2007). In fact, ICS and SCADA systems and their operating systems (OS) are selected based on compatibilities and, in some cases, the system is designed to run on a specific version of an operating system exclusively. Consequently, that decision has a huge effect on the security aspect of the system and the level of support available including the access control measures used.

ICS systems are very unique and there are many companies that develops it all around the world. For example, Emerson Process Management, Honeywell Process Solutions, Invensys, Siemens Energy & Automation, Yokogawa Electric(McMahon & Montague, 2005). Unlike the ICS systems that can be very unique and distinct even from the same company, operating systems running those programs are mostly one of three; Windows, UNIX and Linux. In addition, one major difference between them is in the proprietary and licensing. UNIX is one of the oldest Operating systems and was initially developed around 1970. The system was proprietary and licenses were needed to procure the OS. Linux was developed to be a look a-like system similar to UNIX but it was an open source system available to anyone. Several versions have been released since the early 1990s. However, some UNIX based systems are considered open source and could be acquired without licenses or purchasing. Windows was also developed after UNIX. However, due to its graphical user interface and ease of use it has become a dominant operating system in the industry despite the fact that it is proprietary and requires purchased licenses to operate.

Furthermore, these differences are important and come into place when product support is sought. ICS system vendors could support their systems long after deploying

them at any given time but Operating systems do not share that flexibility if offered. Linux is supported by groups and enthusiasts with no professional entity or authority backing the operating system because of their open source nature. UNIX based systems, are licensed and support in any customized system is mostly limited or very expensive. Windows, on the other hand, provides support for 10-15 years, including the extended support period. That time frame is considered very short for industries working in the energy section (Windows, 2014).

With short or limited operating system support, running delicate and sensitive ICS systems that has long passed its own product life cycle support provided by its vendor presents a danger. The safety and security of those systems are jeopardized, including the access control measures implemented (Gold, 2009).

2.1.1 Operating Systems

Operating systems are software responsible to manage hardware and software resources available to be used by applications installed while interpreting inputs and reflecting outputs (Stallings, 2012). As mentioned earlier, the three major operating systems are UNIX, Linux, and Windows. Discussing those will provide a better understanding about long-term support of those platforms.

UNIX, is multitasking, multiuser system utility developed by AT&T, however some companies had customized it and therefore licenses can be needed. In the case of custom designed systems support is limited and cannot be depended upon by industries in the energy section due to the high threat, demand and safety concerns associated with it. Nevertheless, ICS developers utilizing Unix-based software solution will provide the support needed to troubleshoot issues. That being said, their knowledge in both the OS

and software is a great asset since all the interactions and interfaces are known and available for troubleshooting code line by line (Ritchie & Thompson, 1978).

Linux**,** is an open source system and is therefore similar to the UNIX system. ICS developers utilizing the Linux-based systems will take ownership and responsibility in troubleshooting any issue including ones related to the operating system (Linux, 2009).

Windows, is a completely different and is more like a "black box" to ICS developers. The development is done based on an application programming interface (API) that is published by Microsoft. Thus, support provided by the ICS vendor is limited to the software itself and is closely related to OS functions, rather than the complete OS. Therefore, OS support is basically what is offered and regulated by Microsoft licenses (Strom, 2015). This two layer interaction can cause issues in pinpointing problems and therefore delay solutions of mitigations.

In summary, an Oil Facility that has Industrial systems such as ICS and SCADA might be able to get support to those programs if something was to go wrong. However, that could not be said about the Operating Systems that are running it. As time goes by support to these OS becomes very limited and sometimes not available and thus affects the complete platform in which ICS and SCADA software is running on.

2.1.2 Industrial Control Systems

Due to security reasons ICS developers in the past have requested in some cases full isolation of their system from all other networks and devices not associated with their system to guarantee its operation and reliability. Systems developed and installed have been carefully installed as "islands" with no outside communication or correspondence. That isolation has provided a false sense of security. The fact that systems are not

connected to the outside world or external variables give the illusion that it is protected because it is autonomic and enclosed. Consequently, security practices in developing their software was neglected or non-existent (Nicholson, Webber, Dyer, Patel, & Janicke, 2012). However, due to isolation, those problems did not surface to the point where it became the center of attention in order to have it addressed.

In reality, conversions of networks have been the norm in this decade. Systems are no longer isolated in "islands of networks". Communication between different systems is becoming more and more essential for continuance and optimized operation (Ralstona, Grahamb, & Hiebb, 2007). While the network structure changed, the security practices in developing the ICS systems has yet to catch up or own up to the challenge. Developers have been adding security as an additive feature following the completion of the ICS software instead of employing it in every step of the process. This huge difference in attitude leads to vulnerabilities in the system, including access control issues.

Furthermore, on average the development cycle of an ICS or SCADA system ranges from 3-5 years, based on the range and complexity of the system. Nonetheless, developers in some cases are willing to provide support to their software for up to 15 years after discontinuation (Bradbury, 2012). Yet, that support is usually operational in nature and very rarely includes security or access control updates or fixes to their system.

2.1.3 Access Control

Access Control is measures, workflows and procedures put in place to limit, manage access to physical locations or logical systems. Access is either granted or not. If Access is permitted then the level of access could be put in place to limit and manage it

by giving access to everything or some things. Details and examples are shown in this section..

Are security measures in place to limit the availability of information, systems or functionality to privileged or assigned personal, that includes hardware and software mechanisms ranging from key cards to passwords to monitor and audit establishing accountability and attribution? History has shown that gates and barriers are the means needed to limit access or protect physical assets. However, with the technology age and virtual world, user names and passwords have been the main way of implementing logical access control. In reality, critical facilities implement both for added security. Nonetheless, a single means of authentication is no longer valuable or rendered secure (Warfield, 2012).

With advancements in technology, authentication using biological features has been utilized and implemented. For example, finger prints, eye scanners, voice recognition and facial recognition devices have been used as secondary access control measures. Moreover, tokens generating systematic numbers and other system generating massages with pass codes to systems are also being used as a secondary measure for identification (Vaidya, Makrakis, & Mouftah, 2013).

Generally, a mix and match approach among the previous concepts is implemented in facilities based on level of security, budget and importance. Therefore, in industrial facilities physical gates and walls are in place and secure identification cards are being used to physically limit access to the facility. On the other hand, access to a system is controlled using passwords and a secondary access control such as finger print

or tokens. In some cases different locations within facilities require other layers of access control (Wiles, et al., 2007).

Consequently, access control information needs to be managed, monitored and maintained to insure up to date information. Therefore, a centralized system or server is put in place to manage those credentials. Nevertheless, the task is difficult to maintain in a multi-layer network configuration or a mixed system environment in which different people have different access levels in different or multiple systems. For example, Several Employees might be given different levels of access to individual systems, Employee A is allowed Admin privilege on System B but only user privilege on system C, and Employee B is allowed Admin privilege on system C but only view access to system B.

2.1.4 Threats

Now days, technology threats in the Oil Industry have been mostly external. Therefore, protections and counter measures were tailored to secure the systems from outside access. However, since ICS systems and SCADA systems have been always in isolation that was not an issue and therefore external attacks were not considered threatening. Thus, the focus was on internal employees' privileges and level of clearance. But with the expansion and development in the network structure of those devices and systems, external threats have been introduced to the equation once again. In fact, such threats are in some cases carried out by large entities including government agencies (Warfield, 2012). For example, the Stuxnet virus that was deployed to a specific Honeywell system in only a certain country and in limited numbers of nuclear facilities (Genge, Siaterlis, Fovino, & Masera, 2012). Another example would be, the Shamoon

incident that hit Saudi Aramco, the biggest oil producing company in the world located in Saudi Arabia (Helman, 2012).

Since threat levels have increased and the surface of attack has widened with the shear range of networks interconnected together, it stands to be reasoned that old security methods of managing access control to sensitive systems such as ICS and SCADA should be questioned (Willems & Software, 2011).

On the other hand, connectivity between networks introduces corporate users that are interested in analyzing and observing the data outputted from their end node points in their facilities. Introducing different business needs onto the operational requirements for optimization and reporting purposes increases the internal threat level to SCADA and ICS systems exposed. Storey (2009) stated that understanding the process control network in which SCADA and ICS rides on is very important however, people and politics should not be neglected and thus should be considered if a truly secure solution is to be built.

2.1.5 Current Studies

Researchers have been studying the issue in detail, especially with the wide range of systems in place including legacy systems. A study suggesting using add-on measures to legacy systems utilizing microkernel-based architecture isolates network-interacting where bloom filters are in place to authenticate commands and access levels have been published recently (Hieb, Chreiver, & Graham, 2013). Such studies provide different meanings to accomplish access control measures, especially in an environment where systems could have been put in place more than a decade ago. Nevertheless, other solutions have also been introduced that utilize public-key certificates in conjunction with

zero-knowledge protocol in server aided verification (SAV), attribute certificates and multiple factor and level authentications (Vaidya, Makrakis, & Mouftah, 2013).

Other studies showed the lack of effective security measures and total reliance on a single mechanism for access control, and that is usually demonstrated by the developers of the ICS and SCADA system (Cetinceviz & Bayindir, 2012). For Example, Systems that only used single user name and password without biometric authentication or the other way around. Nevertheless, some also discuss the threats and vulnerabilities added to those systems due to improper implementations stemming from lack of knowledge, complexity of the system, insufficient funds and missing required documentation (Sommestad, Ekstedt, Holm, & Afzal, 2010).

"In 2010, Singapore's Senior Minister of State for Law & Home Affairs explained that 'with the ever-changing cyber landscape, we can expect to see adversaries evolve and come up with new threats to circumvent our security defenses. [And flagged that it] is therefore necessary for the IT security industry as a whole to step up to the plate to meet this challenge with innovative and strategic solutions against these emerging threats" (Choo, 2011, p. 728). Moreover, focus and attention should be added into the development life cycle of ICS and SCADA systems.

2.2 Typical Oil Field Infrastructure Design

Now that the author have covered different aspects of the Control Systems used in an oil field facilities, it is important to draw a complete picture of how the facilities are typical designs while covering the difference access control measures implemented.

2.2.1 Access Control

At first Physical Access Control is discussed; any facility that deals with energy and due to safety reasons is always protected. Typically, Facilities will have a wall surrounding it or a means to limit access and control incoming and outgoing personal. At the entrance, people are provided access after being searched and their work Identification Card is checked. Depending on the criticality of the facility, a secondary biometric measure might be in place. It is important to note that within those facilities there are command centers and other locations that implements further security measures that is not available to all employees and requires a certain level of clearance.

After gaining access to the locations that include the systems monitoring and controlling the facilities and the production of the oil logical access control measures will be in place, an engineer will typically be given a station that includes a password protected system that requires login using previously assigned accounts. Some of those systems are specialized to provide different access levels based on employee's job classification or clearance level. For example, an operator will be able to see different reading of pressure and oil flow rate from a specific well, but only an engineer can modify settings to increase or decrease the flow rate by adjusting the well head opening or turbine rotation speed.

Unfortunately, even with this detailed access control measures some ICS vendors and SCADA vendors will also dictate shared user accounts that are used by multiple personals. For example, a single user name and password for all operators, or a generic password that is used to share data across multiple systems via a centralized database that cannot be changed. In the following section, the author discussed the network design and

different devices that are attached to it and the access control security measures that it carries.

2.2.2 Network Design

So before getting into the security details of the network design, the author will discuss the flow of information, what is the point of origin? Destination? As well, as the users?

At the start, an oil facility objective is to be able to produce oil by extracting it from the geographical topology in the area, refine it from any contamination and stabilize it for transportation in order to sell it. Those three functions can be done in a single facility or several facilities that each carries a single functionality before transferring the oil to the next one (ABB, 2013).

Once an oil reservoir is found a study is made to decide the best locations to drill wells to maximize production and limit pockets of oil that cannot be extracted. Once the order is in place an oil well is drilled and several sensors are installed in the well head to monitor several oil attributes such as temperature, pressure, and flow rate. When refining the oil other devices are installed that monitors other attributes such as the density, composition (Cetinceviz & Bayindir, 2012). These sensors produce the raw data that is usually stored locally at a Remote Terminal Unit (RTU). The RTU stores data for a defined time while formatting it and preparing it for transportation over a network to the local command center. Communication could be done via radio, GSM, WI-FI, or fiber optic cables. Similar to a tree structure where the oil fields represents the tree leaves data is usually aggregated over several networking nodes before it reaches the trunk or in our example the main command center database.

After that data is being created from the sensors in the field and information is being transported via the network from the RTUs to the local database, SCADA systems and ICS applications utilizes that data to graphically represent the information for operators and engineers on site. Operators monitor those values to ensure operational wells are producing the required amount of oil, set forth by engineers, decided by management, and dictated by market demand. Operators also monitor well activities for any anomaly or safety concern due to the high pressure high temperature values of the oil being extracted (Cetinceviz & Bayindir, 2012).

Typically, information gathered in the database from the oil field sensors is also accessed by research and development for further refinement and future studies or expansion to the reservoir. If the company has operations in different reservoirs or different facilities on the same one, data might be aggregated to a higher and bigger centralized data base from the local facilities. Data is owned and used by the facilities it's produced from. Nevertheless, other employees that might not be within that facility itself also use it.

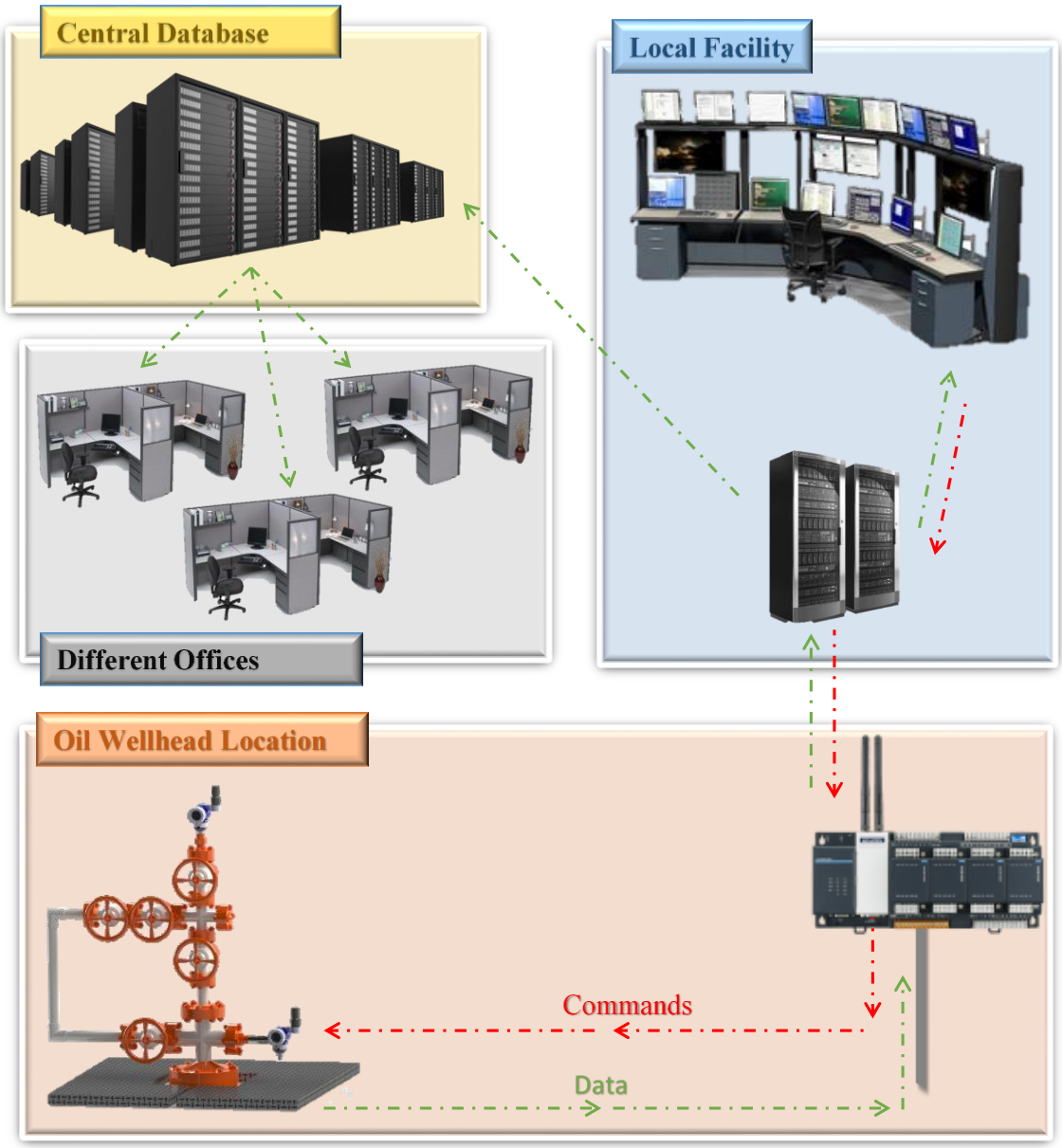

Figure 2-1 Typical Smart Wellhead Design

The above diagram is developed based on many oil facilities that was visited and is considered a typical design for a smart oil wellhead implementation. As shown in the

graph above, Security Access Control measures are usually implemented in the RTU around every oil well head to protect the data source. However, since those locations are usually scattered across a large areas and sometimes in very remote locations, physical security is sometime a huge challenge. RTUs are usually installed in cabinets that require special keys to open and the RTU consul itself is password protected.

Every device on the network such as routers that are used to aggregate several RTU traffic into a single network is also password protected within a cabinet. This is in case it was being transported via fiber optic or different radio relay stations. If it was via GSM network then communication is directed directly to the local database via the telecommunication network of the GSM Company.

The next step is the local database that is also password protected and physically secure in a limited access room hosting several critical servers and devices. In some cases this could be the last and final location where data is being stored and in others it could be simply another aggregation point before its being sent to a bigger centralized Database.

2.3 Threat Intelligence Frameworks

For an enterprise, threat intelligence is "an ecosystem of contextually relevant and evidence-based knowledge – integrated into platforms and tools – to quickly and accurately address dangers to individuals, organizations, or assets in a standardized, consumable format." (Los, Robinson, Clark, Brooks, & Brown, 2014, p. 2)

Figure 2-2 Five Stages of Threat Intelligence

In general, the lifecycle of a given threat Intelligence framework goes over the above five stages shown in Figure 2-2. The planning stage is where goals are set and decisions are made as of what is should be protected. In the resource stage, resources are allocated to support the goal set in the first stage. Processing is the stage in which data is being acquired and information is gathered to achieve the goal set in the planning stage and within the limitation of the resources allocated. The Analyzing stage is where everything gathered is studied and analyzed to get results that help achieve our planned target. Finally Dissemination stage is where the results of all the previous stages have been achieve and is being implemented or distributed to induce action and change towards the goal set in the very beginning (Rocha, 2015).

To compare the frameworks selected out of these five stages the following three is discussed: Processing, Analyzing, and Dissemination. Each of which can be broken into more sub categories and specialized segments. Yet they are always streamlined after each

other. Information provided from intelligence sources is analyzed to identify threats and means of protection that is then implemented as a response in order to mitigate and address those issues. The following sections will discuss those categories.

2.3.1 Planning

In an energy sector or an enterprise that is striving to supply power to its customers the main driver for threat intelligence process is to secure and maintain assets and operational continuity (Farnham, 2013). However, in Saudi Aramco the company accounts for 80% of the national income GDP therefore the security of the enterprise is also driven by national security and the country's economic stability or existence (CIA, 2014).

2.3.2 Intelligence Sources

In general, enterprises in the energy sector are relatively similar in their sources of information. That includes internal sources, community, and external sources that are identified in the definitions section (Farnham, 2013). However, those sources are also broken into two more general categories, open source and private. Open source information is what is available and accessible free while private sources are ones that are not, which may include but not limited to, internally developed sources or feeds purchased from other third party security companies.

2.3.3 Requirements of Threat Intelligence

In order to automate and collaborate efforts with such systems a standardized format needs to be available to share indications of compromise and other related security aspects across devices and system to be able to analyze and respond to those reports.

Tools have to be selected to cover all related aspects of security that is of concern to the enterprise.

2.3.4 Analyzing Cyber Threat Intelligence Input

In every system, input gathered will greatly affect the quality of the system results. KPGM International has defined it as "Is the ability to analyze cyber intelligence gathered and to make links between discrete pieces of information to create actionable intelligence" (KPMG International, 2013, p. 4). This can be achieved using automated tools and trained operatives and personal.

2.3.5 Response to Cyber Threat Intelligence

From data that has been analyze actions are driven to mitigate security issues. This phase is continually being evaluated in order to keep up with the development or changes in the field. Nonetheless, respond is also affected by the kind of adversary or attacker. Attackers can be classified into the categories found in the definition section, Insider Threat, APT, Nation State Actors, Script Kiddie, and Hacktivist. (Ponemon Institute LLC, 2014). With all those types of adversaries in mind tactics of defending and the paths selected to respond is usually one of the following three mentioned below (Miller & Lachow, 2008).

First is prevention and protection, it differs from organization to another based on the level of sophistication and spending based on the expected area of effect and damage influenced. Second is, Resilience, this could be a choice of action when the adversary is Nation State or highly sophisticated APT. Third is Deterrence, which could be used when dealing with APT and all types of adversaries other than nation state. Companies might opt out of getting into this path due to lack of resource available to carry out such actions

or due to issues of legalities. For Saudi Aramco, this option is one that is available to be used.

2.4 Frameworks Selected

Upon reviewing ten threat intelligence framework the following, three covered the complete process of threat intelligence in a given organization without being too specific that it cannot be tailored to any given need or requirement by that specific organization. The frameworks are;

- National Institute of Standards and Technology (NIST), Cybersecurity Framework
- Open Source Threat Intelligence Framework (OSTI)
- Collective Intelligence Framework (CIF)

2.4.1 NIST Cybersecurity Framework

The framework developed by NIST under the Executive Order 13636 given by Barack Obama the current president to address the continues rising security threats to the nations critical infrastructure. (Sedgewick, 2014). This framework is a voluntary framework that helps reduce cyber risk to critical infrastructures. Since the Oil industry is part of the energy infrastructure it is applicable and suitable to be used for the purpose of this study. It's also good to note that this framework is being continuously evaluated and updated as need by NIST.

2.5 OSTI Framework

The framework is being taught by SANS institute. It utilizes open source intelligence that can be analyzed for actionable intelligence. This framework is also

developed in 2013 and is continually being updated by the institution (Maxwell, 2013). A great example of how open source can assist and support in securing ICS and SCADA system is a study made that tried to bridge the gap. In which he tries to shorten the gap between the security professionals and the SCADA and ICS ones. A detailed simulation and examples where provided that shows how open sources could be a viable and affordable solution. (Nguyen, 2014)

2.6 Collective Intelligence Framework

The framework is based on an open source software on Google Code Hosting services developed by the community of users. Currently it is being run and administrated by a non-profit organization called CSIRT Gadgets Foundation. The code is also available in GitHub for all developers and community users (CSIRTGadgets, 2015).

2.7 Summary

In general, ICS and SCADA systems have been tasked to handle real-time life-threatening systems in order to manage critical infrastructures by governments and private sectors. Security measures such as access control is lagging behind in the development of those infrastructures. Threats introduced by the convergence of network and internet connectivity have already caused damage and casualties in several incidents in the past decade. Researchers have identified those gaps. However these gaps are still affected by the continuous development of technologies, in relation to the product life cycle of the ICS and SCADA system (Igure, Laughter, & Williams, 2006). With those advancements, adversaries have a wider range of effect and damage.

In this thesis an effort was made to focus on threat intelligence frameworks that can be implemented to continually secure access control means in different OS environments in the energy section. Scholars and researchers have been identifying different measures that help protect infrastructures using access control methods such as passwords, tokens and biometric features. However, such actions with intelligence information gathered would help capitalize on budgets being spent in the right manner to achieve security. In fact, examples in the following case studies have been published to discuss the added security in enhancing such measures.

The importance of security is well acknowledged by entities related to the energy industry. Therefore, this study will provide some information and insight that will help prevent and secure assets and lives by its implementation. The mislead idea that cyber attacks, malware and viruses cannot cause causalities is wrong. Affecting ICS and SCADA systems remotely could cause undesirable reaction that could lead to explosions or exposure to harmful gasses and material. Maintaining security and access control measures by assessing and evaluating assets and procedures to eliminate unlawful action or negligent decisions is a goal in farther securing facilities in the Energy industry (Wiles, et al., 2007).

CHAPTER 3. PROCEDURES AND DATA COLLECTION

3.1 Methodology

Information used in this research was initially suppose to be acquired from reports and studies related to security and the oil and energy industry. However, due to the security nature of such information it was unobtainable. Therefore, a point system was developed that help rank different frameworks, based on the researcher experience in the field as shown in this Chapter.

3.2 Data Collection

As a result to the sensitivity of the data being studied, data was to be collected from public available reports related to the SCADA and ICS systems published or released by companies or associates in the energy industry dealing with access control security measure. Such companies are, Saudi ARAMCO, SABIC, Qatar Gas, Yokogawa.

3.3 Data Analysis

Data collected initially was supposed to be from open sources available and subsequent to fully acquiring enough data, in order to find, similar patterns in the results after analyzing the information. However, due to the nature of this data, being classified as secure information and thus not available for public it was unfortunate that no

company accepted to share security realted data that helps the research. Therefore, a point system was created.

3.4 Criteria

After cross-analyzing ten of currently acceptable and used framework in the industry, several criteria's have been identified to be relevant to companies in the oil industry or energy section in general. The following were the points used in this study to evaluate different threat intelligence frameworks being applied to an oil company. Followed by a simple table to score each of those criteria:

- Applicable: Can be implemented in Oil Company covering all assets ranging from remote areas to business headquarters.

Expandable Horizontally: The ability to expand and include more assets/lactation as needed.

- Expandable Vertically: The ability to add more hierarchical layers to the Framework based on security requirements
- Ease of implementation: Implementation is understandable and easy to use by all stake holders
- Expenses: Ranges from Free to very expensive in comparison to each other, covering all implementation needed such as software/hardware/ procedures/ training.
- Flexible: Accepts variation of implementation based on several criteria such as location, asset type, and security level
- Covers all sources of Data: does it cover all sources of data available? Or some degree of it?

- Provide measurable Results: Provide a meaningful number as an evaluation for an asset or a security risk
- Provide Comparative Ranking: Ability to prioritize risks and vulnerabilities
- Recurring costs: how frequently does the framework require additional spending to operate? Note this does not cover any security implementation or decisions derived from the framework.

In the following table, criteria are either; binary, or points from 0-4. In some of the criteria mentioned, the answer is either a yes or a no therefore maximum or minimum point score was assigned to reflect that. As for the other criteria, the scale from 0-4 was based on how much of the framework could be implanted, or how long it takes to be implemented. Those values help rank the framework based on all the criteria selected.

Table 3-1 Criteria Table

Criteria	0	1	2	3	4
Applicable	No	25%	50%	75%	100%
Expandable Horizontally	No	-	-	-	Yes
Expandable Vertically	No	-	-	-	Yes
Ease of implementation	5 Year	3 Years	2 Years	1 Years	> 1 Year
Expenses	1M	500K	250K	100K	Free
Flexible	No				Yes
Covers all sources of data	No	25%	50%	75%	Yes
Provide Measurable Results	No	-	-		Yes
Provide Comparative Ranking	No	-	-	-	Yes
Recurring costs	1 Year	2 Years	3 Years	5 Years	0

3.5 Reliability

This research provides a unique conclusion that can be generalized in similar settings and environments. However, with time passing by some of the findings might be irrelevant due to fast nature of advancement in technology and hence security related issues. Furthermore, the result achieved can be provided to several companies to assess and confirm the findings. Research is reliable and results could be carried out in companies working in the oil industry to test and ensure the efficiency of security upgrade utilizing the threat intelligence framework

CHAPTER 4. FINDINGS

As described in previous chapters, the objective of this study was to determine the availability and ability of currently established and well-known threat intelligence framework to rank security measures upgrades in the oil field industry.

4.1 NIST Cybersecurity Framework

The following table on the next page shows the scores given to each criteria previously discussed in the mythology chapter for the NIST Cybersecurity Framework.

Table 4-1 NIST Cybersecurity Framework

Criteria	Score
Applicable	Yes (4)
Expandable Horizontally	Yes (4)
Expandable Vertically	Yes (4)
Ease of implementation	Somewhat Difficult (1)
Expenses	Very Expensive (0)
Flexible	Yes (4)
Covers all sources of data	Yes (4)
Provide Measurable Results	Yes (4)
Provide Comparative Ranking	Yes (4)
Recurring costs	Every 6 Months (0)
Total Points	29

NIST, a framework developed by the US Federal Government scored the highest in the comparison as proven by the upcoming results. The NIST Framework has been generalized to the point that it can accommodate anything. However, that comes with a price. In order to accommodate a company specific needs a lot of customization and in house work will need to be done which makes it the most expensive framework with difficulty in implementation and a huge toll on continue maintenance. Yet, the fruits of this effort will be evident in providing the most related trusted actionable intelligence that can be produced by any framework (NIST, 2014).

4.2 OSTI Framework

The following table shows the scores given to each criteria previously discussed in the mythology chapter for OSTI.

Table 4-2 OSIT Framework

Criteria	Score
Applicable	Yes (4)
Expandable Horizontally	Yes (4)
Expandable Vertically	Yes (4)
Ease of implementation	Normal (2)
Expenses	Free (4)
Flexible	Yes (4)
Covers all sources of data	No (0)
Provide Measurable Results	No (0)
Provide Comparative Ranking	No (0)
Recurring costs	No (4)
Total Points	26

The Open Source Threat Intelligence Framework is free, with no recurring cost. However, since data, sources are untrusted or vetted external sources it cannot be actionable and trusted as NIST Framework. It is also important to note that it does not cover all sources of data and only the ones that are available to public (Maxwell, 2013).

4.3 Collective Intelligence Framework

The following table shows the scores given to each criteria previously discussed in the mythology chapter for CIF.

Table 4-3 CIF

Criteria	Score
Applicable	Yes (4)
Expandable Horizontally	No (0)
Expandable Vertically	Yes (4)
Ease of implementation	Somewhat Difficult (1)
Expenses	Free (4)
Flexible	Yes (4)
Covers all sources of data	No (0)
Provide Measurable Results	Yes (4)
Provide Comparative Ranking	No (0)
Recurring costs	No (4)
Total Points	25

Collective Intelligence Framework (CIF) is an open source software based framework that aggregates data sources, unify information display and provide actionable measures and results. Unfortunately, since its open source it is community driven and sources that available for utilization are limited to extensions that provides appropriate API to the main program. Thus, not all sources or types of data are vetted or can be used

which makes comparative ranking of outputs difficult to nonexistent (CSIRTGadgets, 2015).

4.4 Comparison

Table 4-4 Frameworks Comparison

Criteria	NIST	OSTIF	CIT
Applicable	Yes (4)	Yes (4)	Yes (4)
Expandable Horizontally	Yes (4)	Yes (4)	No (0)
Expandable Vertically	Yes (4)	Yes (4)	Yes (4)
Ease of implementation	Somewhat Difficult (1)	Normal (2)	Somewhat Difficult (1)
Expenses	Very Expensive (0)	Free (4)	Free (4)
Flexible	Yes (4)	Yes (4)	Yes (4)
Covers all sources of data	Yes (4)	No (0)	No (0)
Provide Measurable Results	Yes (4)	No (0)	Yes (4)
Provide Comparative Ranking	Yes (4)	No (0)	No (0)
Recurring costs	Every 6 Months (0)	No (4)	No (4)
Total Points	29	26	25

From the Table above it is evident that NIST scored better than the other frameworks due to its general nature. However, OSTI is also a viable solution since it is free with no continues upgrades required or maintenance cost, which also could be said

about CIF. Nonetheless, since both OSTI and CIF use mainly publicly available sources of intelligence it could hypothetically provide inaccurate risk information that might drive a different priority ranking for potential security upgrades. Having said that, vetting and vigorously analyzing all that public information is time consuming but could provide some information that can be translated into actionable intelligence.

On the other hand, NIST covers all public and private information, which is customizable to the specific organization threat factors and actors. Which in the end provides the most accurate and reliable intelligence.

CHAPTER 5. DISCUSSION

In the previous chapters, the possibility of utilizing any threat intelligence framework in prioritizing security upgrades in Access Control Systems in the oil industry was discussed. The author covered different aspects and systems involved, what criteria is important in defining what type of framework would be applicable, Finally, the author used the mythology and scored the three different frameworks as shown in the results chapter. In this chapter, a more detailed approach will explain our results while striving to answer the research question.

In this chapter, results from the criteria developed were discussed while tying it with the research question. This will help explain the relevant, as well as the score value representation to our thesis problem.

Flexibility, Intel gathering is difficult and unique to any organization due to their setup, type of equipment used, and network layout. It could also be different within facilities in the same organization. In Fact, it could be argued that it is also different within the diverse systems in the same facility. Which brings up the importance of having a general framework that is flexible to accommodate change and diversity of the organizational structure or operational design. In our results, it is apparent that all frameworks selected have been identified as flexible frameworks.

Expandability, is another criteria that is important since those facilities are continually changing in order to keep up with the increase in demand or reduction in production. The ability to expand horizontally by adding new nodes to the current layer is very important since the drilling of oil wills is a frequent operation that is carried out to increase production or replace maintain current flow rate. Expanding vertically, is more hierarchical in nature and is needed to generalize information to different levels of stockholders such as local supervisors, general supervisors, managers, etc. This is a great feature to have but not a necessity like the ability to expand horizontally.

Furthermore, the rest of the criteria are variables that simply helps differentiate between the frameworks. For example, how expensive is it to implement and if it has any reoccurring costs is something that might be important to some users more than others might. Ease of implementation might be another factor to be taken into consideration based on the organizational size. The last three criteria that might be of most concern are, verity of sources being used, ability to provide measurable results or comparative ranking. Those three criteria are what the author discussed in the following sections of this chapter in more details.

5.1.1 Frameworks Data Inputs

Information gathered as mentioned previously is very important in defining the quality and reliability of your out coming output. Being able to cover all sources of data is very important. However, not all frameworks selected in this study was able to incorporate all data sources. NIST cybersecurity framework is flexible and generalized in such a way that it can accommodate any source of input wither its publicly available, in-house developed or third party provided. On the other hand, OSTI framework deals with

the open source data, which is available freely by other organizations. CIF, is also limited and its limitation has nothing to do with cost. CIF limitation is based on add-ons and plugins that are developed by the community to accept and normalize feeds to be used by the system. Therefore, a source can only be used if it has an appropriate extension that is added to the main program to interpret and utilize its feed. Therefore, NIST seems to be the only Framework that can accommodate any type of source.

5.1.2 Frameworks Ability to Measure results

The ability to quantify the values of inputs and threats provided is very helpful in providing a general understanding of ranking among data. Thus, again our three frameworks are very different in these criteria. NIST once more since it is flexible and designed by the user specification is able to provide such information that is set forth by the user. CIF, is also able to provide that as part of the software package. However, the OSTI framework does not provide such information. Being able to assign numbers to threat actors or vulnerabilities discovered is helpful in future analysis leading to potential ranking among those inputs.

5.1.3 Frameworks Ability to Rank Results

NIST, yet again seems to be able to accommodate this criteria since it is customized and designed by the user. That could not be said to the other two frameworks since information provided and sources of data are not comprehensive in nature or do not provide measurable data. This makes NIST cybersecurity framework the most suitable one to potentially answers the research question in hand.

5.2 Conclusion

Out of all Frameworks selected, NIST has shown the ability to be adoptable, flexible and reliable. However, that comes with a huge price tag and an ongoing cost on the organization. The reason NIST framework is able to accommodate any criteria being set is the inherited nature of it being generalized to accommodate any industry or organization that strives to implement it. The continues in-house customization of the framework will yield the best results imaginable for any organization as long as its carried out appropriately.

Nonetheless, Open Source Threat Intelligence or Collective Intelligence Framework, should not be completely excluded because for a small organization with limited resources either of them could be a solution that increases security measures in a better way than simply going in blind. In Fact, even with available financial resources, the size of the company or the manpower available might not justify the huge cost encored from implementing a NIST framework (Holland, 2013).

Finally, the answer is not believed to be either or. A hybrid solution could be best as well as less expensive than simply using a NIST cyber security framework. NIST framework provides all the guidelines necessary to be implemented for a threat intelligence framework to be used in an organization. Data and information is being developed and analyzed in-house driving decisions and upgrades needed (Shackleford, 2015). However, it does not exclusively throw out the possibility of utilizing Open source intelligence feeds. In fact, it is possible to use the open source threat intelligence framework to help focus the data being analyzed and developed within the organization without neglecting the other complete picture. Furthermore, the Collective Intelligence

Framework could be used as a platform to help streamline all sources that include open one and the ones that are developed in house or even ones that are acquired by third parties. The financial cost of developing a complete threat intelligence framework platform for NIST drops down to a set of extensions that are uniquely used by the organization facilitating the use of the CIF.

Finally, going back to the research question, is it possible to prioritize Access control Security upgrades within an organization in the oil industry utilizing a threat intelligence framework ? The answer is yes, it can be done using the NIST framework separately or in conjunction with other frameworks.

Nevertheless, this research was also able to identify a ranking system that can be utilized to score and evaluate any security framework and its applicability to a specific company within the energy section industry. Those criteria can be given a different scale based on the company's unique needs. Results will be reliable and a definite answer will emerge upon successfully applying it similar to the research in hand.

5.3 Future Research

Now that the answer was found using the frameworks available, a question arises if those frameworks are optimum specifically for the oil and gas industry. Is it possible to develop a new framework that is more efficient and suitable for the industry? Can a framework be developed that is less expensive? Or with minimum ongoing cost ? How difference is this to an electrical or energy specific Organization? Could this be implemented to get actual results that verify our findings?

REFERENCES

REFERENCES

ABB. (2013, August 22). *Oil and gas production handbook*. Retrieved from http://www04.abb.com/global/seitp/seitp202.nsf/0/f8414ee6c6813f5548257c14001f11f2/$file/Oil+and+gas+production+handbook.pdf

Cetinceviz, Y., & Bayindir, R. (2012). Design and implementation of an internet based effective controlling and monitoring system with wireless fieldbus communications technologies for process automation—An experimental study. *ISA Transactions, 51*, 461–470. doi:10.1016/j.isatra.2012.01.001

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security, 30*, 719-731. doi:10.1016/j.cose.2011.08.004

CIA. (2014, June 20). *The World Factbook Saudi Arabia*. Retrieved from Central Intelligence Agency: https://www.cia.gov/library/publications/the-world-factbook/geos/sa.html

CSIRTGadgets. (2015, July 10). *The CIF Book*. Retrieved from https://github.com/csirtgadgets/massive-octo-spice/wiki/The-CIF-Book

Farnham, G. (2013, Oct). *Tools and Standards for Cyber Threat Intelligence Projects.* Bethesda: SANS Institute. Retrieved from http://www.sans.org/reading-room/whitepapers/warfare/tools-standards-cyber-threat-intelligence-projects-34375

Genge, B., Siaterlis, C., Fovino, I. N., & Masera, M. (2012). A cyber-physical experimentation environment for the security analysis. *Computers and Electrical Engineering, 38*, 1146-1161.

Gold, S. (2009, August). The SCADA challenge: Securing critical infrastructure.

Network Security, Volume 2009(8), pp. 18-20.

Helman, C. (2012, July 16). *The world's biggest oil companies*. Retrieved from http://www.forbes.com/sites/christopherhelman/2012/07/16/the-worlds-25-biggest-oil-companies/

Hieb, J. L., Chreiver, J. S., & Graham, J. H. (2013, March). A security-hardened appliance for implementing authentication and access control in SCADA infrastructures with legacy field devices. *International Journal of Critical Infrastructure Protection, 6*(3), 12-24.

Holland, R. (2013, January 15). *Five steps to build an effective threat*. Retrieved from http://www.coresecurity.com/system/files/attachments/2013/04/RickHollandFiveStepstoBuild.pdf

Igure, V. M., Laughter, S. A., & Williams, R. D. (2006). Security issues in SCADA networks. *Computers & Security, 25*, 498 –506. doi:10.1016/j.cose.2006.03.001

KPMG International. (2013, May). *Cyber threat intelligence and the lessons from law enforcement.* Sydney: KPMG International Cooperative.

Leith, H., & Piper, J. W. (2013). Identification and application of security measures for petrochemical industrial control systems. *Journal of Loss Prevention in the Process Industries, 26*, 982-993. doi:10.1016/j.jlp.2013.10.009

Linux. (2009, April 03). *What is Linux: An overview of the linux operating system*. Retrieved from https://www.linux.com/learn/new-user-guides/376-linux-is-everywhere-an-overview-of-the-linux-operating-system

Los, R., Robinson, J., Clark, J., Brooks, R., & Brown, W. (2014, Dec). *Threat Intelligence.* Denver: Accuvant. Retrieved from http://files.accuvant.com/web/file/d96f8c4996ee4571999bcf513126399c/Threat%20Intelligence_Solution%20Primer.pdf

Mateski, M., Trevino, C. M., Veitch, C. K., Michalski, J., Harris, J. M., Maruoka, S., & Frye, J. (2012, March). *Cyber Threat Metrics.* Albuquerque: Sandia National Laboratories.

Maxwell, K. R. (2013). *Open Source Threat Intelligence.* Dallas: Verizon.

McMahon, T., & Montague, J. (2005, December 5). *Top 50 Automation Companies of 2004*. Retrieved from http://www.controlglobal.com/articles/2005/543/

Miller, R. A., & Lachow, I. (2008, Jan). Strategic fragility: Infrastructure protection and national security in the information age. *Defense Horizons*(59).

Nguyen, C.-K. Q. (2014). *Industrial control systems (ICS) & supervisory control & data aquisition (SCADA) cybersecurity of power grid systems: Simulation/ Modeling/ Cyber defense using open source and virtualization.* West Lafayette: Purdue University.

Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of cyber-warfare. *Computers & Security, 31*, 418-436. doi:10.1016/j.cose.2012.02.009

NIST. (2014). *Framework for Improving Critical Infrastructure Cybersecurity.* Gaithersburg: NIST.

Ponemon Institute LLC. (2014, Jan). *Cyber Security Incident Response: Are we as prepared as we think?* Traverse City: Ponemon Institute. Retrieved from https://www.lancope.com/sites/default/files/Lancope-Ponemon-Report-Cyber-Security-Incident-Response.pdf

Ralstona, P., Grahamb, J., & Hiebb, J. (2007). Cyber security risk assessment for SCADA and DCS networks. *ISA Transactions, 46*, 583–594.

Ritchie, D. M., & Thompson, K. (1978). The UNIX tme-sharing system. *Bell System Tech. J, 57*, 1905–1929.

Rocha, L. (2015, August 15). *The 5 steps of the intelligence cycle*. Retrieved from http://countuponsecurity.com/2015/08/15/the-5-steps-of-the-intelligence-cycle/

Sedgewick, A. (2014, November 24). *Cybersecurity framework: Current status and next steps*. Retrieved from https://resilience.enisa.europa.eu/nis-platform/shared-documents/eu-us-preliminary-workshop-comparing-approaches/11_24_14-NIST_Slides.pdf

Shackleford, D. (2015). *Who's Using Cyberthreat Intelligence and How?* Bethesda: SANS Institute. Retrieved from http://www.sans.org/reading-room/whitepapers/analyst/cyberthreat-intelligence-how-35767

Sommestad, T., Ekstedt, M., Holm, H., & Afzal, M. (2010, February). Security mistakes in information system deployment projects. *Industrial Information & Control System, 19*(2), 80-94. doi:10.1108/09685221111143033

Strom, D. (2015, September 15). *The Impact of the End of Windows XP on Your Enterprise*. Retrieved from https://securityintelligence.com/the-impact-of-the-end-of-windows-xp-on-your-enterprise/

Vaidya, B., Makrakis, D., & Mouftah, a. H. (2013, January). Authentication and authorization mechanisms for substation automation in smart grid network. *IEEE Network, 27*(1), pp. 5-11.

Warfield, D. (2012). Critical infrastructures: IT security and threats from private sector ownership. *Information Security Journal: A Global Perspective, 21*, 127–136. doi:10.1080/19393555.2011.652289

Wiles, J., Claypoole, T., Drake, P., Henry, P., Johnson, L., Lowther, S., . . . Windle, J. (. (2007). *Techno Security's Guide to Securing SCADA.* Burlington: Syngress Publishing.

Willems, E., & Software, G. D. (2011, March). Cyber-terrorism in the process industry. *Computer Fraud & Security Bulletin, Volume 2011*, 16-19. doi:10.1016/S1361-3723(11)70032-X

Windows. (2014, February 1). *Windows lifecycle fact sheet*. Retrieved from http://windows.microsoft.com/en-us/windows/lifecycle