UNIVERSITÀ
DEGLI STUDI
FIRENZE

Università degli Studi di Firenze
Dipartimento di Ingegneria dell'Informazione (DINFO)
Corso di Dottorato in Ph.D
Curriculum: Telematics and Information Society

A Comprehensive Cyber Security Enhancing Strategy for Industrial Control Systems in Oil Industry

Candidate
Shaya Alshaya

Supervisors
Prof. Giuli Dino

Dr. Paganelli Federica

PhD Coordinator
Prof. Chisci Luigi

CYCLE XXIX 2013/2016

Acknowledgments

I would like to express my special gratitude to my tutors Professor Dino Giuli, and Dr. Federica Paganelli for encouraging my research and for allowing me to grow professionally and personally I could not have imagined having a better advisor and mentor for my Ph.D study. I would also like to thank Dr. Stefano Turchi for deep and inspiring discussions and his unconditioned, precious friendship. I also want to thank Professor Tommaso Pecorella and Dr. Fazle Hadi for their guidance helped me in all the time of research and writing of this thesis. I would especially like to thank all the my fellow labmates who become friends and shared with me these intense years. I would like to thank the students I supervised, who contributed with their work in opening my mind as a researcher.

Finally, a special thanks to Ahmad , Abdullah, Omar and Dania who supported me with patience and shared the joys and sorrows of this long, long journey.

Abstract

Industrial Control Systems (ICS) play a critical operational role in modern industrial sectors. Businesses depend on this automated control system for various operations to manage processes in the most beneficial manner. Information and Communication Technology (ICT) has enhanced ICS development and implementation. However, such automation advancement may also create many new opportunities for cyber-attacks. Certain industries, such as the oil industry within Gulf Cooperation Council (GCC) countries, have begun renewing industrial control systems and related management to counteract cyber-attacks more effectively. The technological system framework which is herewith mainly taken as reference are the Supervisory Control and Data Acquisition (SCADA) systems.

The analysis and synthesis made through this Ph.D. thesis account for both technical and human factors impinging on cyber-security system performance.

A comprehensive approach has thus adopted to qualify relevant scientific technical contributions available from the literature, as well as to exploit outcomes of actual direct experiences of the involved companies. For such a comprehensive approach some basic analytical contributions have been first provided for: i) qualifying related scientific technical advancements within the cyber-security literature; ii) performing subjective testing within the community of IT operators of ICS, concerned with made experience and human behavior affecting cyber-security.

Such analysis is tuned with the objective of defining and adopting an enhanced comprehensive cyber-security policy within enterprise for ICS operation, which properly

accounts also for relevance of human factors. Therefore, final made contribution is just definition and proposal of appropriate guidelines for such a purpose.

Research activity thus carried out is framed with an interdisciplinary context, as needed to innovate enterprise cyber-security management, including specific support and management of enterprise human resources.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

Cyber security is at the forefront of technology advancement concerns. However, these concerns are even greater for industrial control systems due to the nature of these systems. Technology has advanced at a rapid pace, prompting increased issues in relation to data and cyber security (Kaufman, 2009) [1]. Industrial control systems in various industries including the oil companies of Gulf Cooperation Council(GCC) countries are suffering from these cyber-attacks. It is important to ensure that cyber security is enhanced through proactive measures for various services like cloud computing. According to Kaufman (2009) [1], the technology community is currently pushing to force policymakers to adopt universal standards for all service providers, in the hope that through universal standards, interoperability will be ensured. The technology community is currently pushing to improve security standards for data. Although policymakers are making strides in this regard, technology commonly advances much faster than time allows for effective laws for cyber security to be developed (Kaufman, 2009) [1].

This introductory chapter provides basic information regarding cyber security and industrial control systems, followed by a section developing on the study's focus and importance to the field in general. Next, the theoretical framework is briefly introduced, along with the organization and the methodology. The next two sections focus on research aims and objectives and research questions and hypotheses. Next, the significance of the study is discussed, in order to provide a rationale for the topic selected and justification for this research, including potential benefits within academia and the industry alike. The following section contains definition of key terms within the study. This is followed by the summation of the remainder of the study. The final section allows the chapter to be summarized.

1.1 Background Information

Initially, industrial controls primarily relied on "proprietary networks and hardware" to ensure that they would be less vulnerable to attacks (Byres Lowe, 2004) [2]. However, as technology has advanced, the use of "Ethernet, TCP/IP, and web technologies" has provided more opportunities for cyber-crimes to occur (Byres Lowe, 2004) [1]. As a result, companies must constantly seek a balance between security risks and consequences of risk.

1.2 Statement of the Problem

GCC countries share similar characteristics. For example, all countries within the council are involved because they wish to "strengthen relations in economic, political, defense and cultural" with a wish of achieving complete unity on the model of the European Union" (World Trade Organization, 2016) [3]. Therefore, in some contexts, these countries are more vulnerable than others around the world because this union is much smaller than others, such as the European Union. At the same time, cyber security is much more important for the oil companies in these countries because an attack would be extremely damaging internationally as GCC countries have over 40% of the proven oil reserves within them and produce nearly a third of the global oil supply (Gulf in the News, 2013) [4]. However, many of the oil companies within GCC countries use industrial control networks, making them vulnerable to attack.

Oil companies are attacked for a variety of reasons. Not all of these attacks are conducted through cyber or technological means. In fact, some attacks occur physically, causing extensive damage to equipment, prompting the victimized company to pay significant amounts in repairs and/or replacements for damaged equipment (Obi, 2008) [4]. China, for example, has faced immense problems in establishing oil companies within the Niger Delta. In this case, a youth militia group known as "the Movement for the Emancipation of the Niger Delta (MEND), exploded a car bomb in the city of Warri, warning the Chinese oil companies to stay away from the Niger Delta" (Obi, 2008) [4]. Thus, in some cases, oil companies are seen as threats to the existing society within the region. In the Niger Delta situation, the youth militia threatened the Chinese oil companies, claiming that the Chinese workers were thieves and prompting attacks on them. Even worse, some Chinese oil company workers in the region have been the victims of kidnapping (Obi, 2008) [4]. Given this context, the entry of other companies into fragile economies within GCC countries may prompt attacks on the oil companies, either through physical attacks or through industrial control systems.

1.3 Purpose of the Study

Numerous studies have been conducted considering cyber security and industrial controls (Creery Byres, 2005 [5]; Igure, Laughter, Williams, 2006 [6]; Morris, Vaughn, Dandass, 2011 [7]; Ralston, Graham, Hieb, 2007 [8]; Zhu, Joseph, Sastry, 2011 [9]) . Many of these studies that include industrial controls have focused on supervisory control and data acquisition (SCADA), which is commonly used in oil companies of GCC countries. As these countries hold a significant amount of the world's oil reserves and provides a significant amount of oil annually, an attack to the industrial control systems within GCC country oil companies would be damaging globally. Therefore, this study focuses on analyzing the influence of the human factor in attacks on SCADA systems and provide certain guidelines for the industry regarding this human factor. At the same time, the study seeks to determine how various attacks may affect the GCC oil companies and finally presents several guidelines for these industries.

1.4 Theoretical Framework

Two separate theories are being considered in the construct of this study. The first is systems thinking, which involves understanding how different components of a system influences a larger system (Aronson, 1996 [10]; Salim, 2014 [11]). Through systems thinking, a viewpoint is expanded to "take into account larger and larger numbers of interactions as an issue is being studied" (Aronson, 1996 [10]). It would be possible, of course, to consider the influence of only one attack on the industrial control system of an oil company within a GCC country, considering only in the context of how this single attack would influence all GCC countries and all oil companies. The systems theory approach, however, focuses on finding trends or patterns within data results. The adapted theoretical framework for this study is shown below:

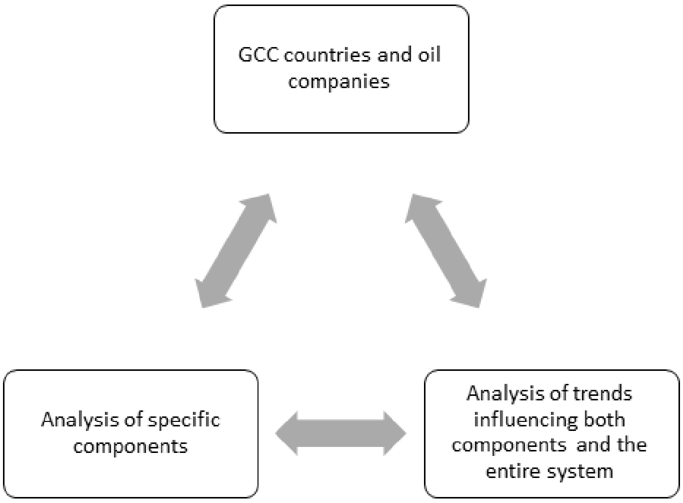

GCC countries and oil companies
Analysis of specific components
Analysis of trends influencing both components and the entire system

Figure 1.1: Theoretical Framework

Figure 1.1 gives an example of how three dimensions overlap to create a whole.

Thus, the systems theory approach and systems thinking approach overlap. The individual components (such as individual case studies) can be analyzed to see what trends exist and how these trends influence both the industrial control system as a whole for that specific company, as well as how the trends might influence all GCC countries.

The number of attacks may be documented for a given year, which would allow the researcher to determine how many attacks occurred in a given year. This information can allow the researcher to potentially determine the probability of future attacks, both physical and technological. These projections would be beneficial not only for the oil companies themselves, but also for the other countries. Using this information, governmental agencies can take strides to provide extra protections to their oil companies, which would be instrumental in maintaining economic stability.

The main contribution of this research, then, is to explore the importance of the human factor involved in cyber security and second one is the documented literature of cyber-attacks, to propose guidelines for the securing the SCADA systems throughout the industry.

1.5 Research Questions

In order to meet the aims and objectives of the study, it is necessary to develop research questions. These research questions include:

1. In what way has cyber security been influenced by the human factor for industrial controls, specifically SCADA, for oil companies in GCC countries?

2. Are cyber-attacks caused by human deficiency, software degradation, or a combination of both?

3. Is there a relationship between the types of platforms used or is there a critical flaw in ICS design that enables ICSs to be infiltrated?

4. Are critical aspects such as human collaboration, platform access, software design, proper implementation and or system monitoring affecting the security of major industrial complexes?

5. Can an implementation of careful human behavior along with evolved software assist in preventing cyber-attacks?

6. To what extent have guidelines been developed to prevent cyber-attacks on industrial controls, specifically SCADA, for oil companies in GCC countries?

7. To what extent have specific trends regarding the human factor emerged in cyber-attacks on industrial controls, specifically SCADA, for oil companies in GCC countries?

8. Is it possible to determine the likelihood of a GCC country being attacked due to having oil companies within it?

1.6 Significance of the Study

As noted within this chapter, prior studies have been conducted regarding cyber security and industrial controls (Creery Byres, 2005 [5]; Igure et al., 2006 [6]; Morris et al., 2011 [7]; Ralston et al., 2007 [8]; Zhu et al., 2011 [9]). These studies have considered the impact of technology weaknesses on industrial controls, yet not necessarily in the context of the systems theory and systems thinking. However, few studies have been conducted regarding cyber security and industrial controls in GCC (Dutta Coury, 2002 [12]; Ulrichsen, 2009 [13]). This study is the most recent of its kind and the first to focus on oil companies within GCC countries. No other studies have been found that combine the use of systems thinking and the systems theory approach to analyze the available information in order to develop a proposal of guidelines for oil companies in these countries to protect themselves. Moreover, this study may be the first of its kind to predict the likelihood of a particular GCC country having its oil companies attacked. This information is expected to be of use to both GCC country governments and oil company owners. For GCC country governments, this information is expected to be beneficial because it will provide a risk assessment of possible attacks. For oil company owners, this information is expected to be beneficial because it will allow these owners to develop new protections for their companies. Finally, this study is significant to academic researchers because it provides a new perspective on an existing problem, as well as outlines potential solutions.

1.7 Definition of Terms

The following terms are found within this study:

Cloud Computing. According to some researchers, cloud computing refers to storing data remotely on servers that are not hosted by the company. In many cases, cloud computing requires paying the host server a monthly, quarterly, semi-annual, or annual fee to use its services. Typically, large amounts of data can be stored on these remote servers, making them ideal for those companies that need to store and easily access large amounts of data (Takabi, Joshi, Ahn, 2010 [14]). Therefore, for the consideration of this study, oil companies that use cloud computing tend to store data on a remote server for easier access at another point in time.

Cyber Attack. A cyber attack is defined as an attempt or success of a cyber criminal in damaging, disrupting, or accessing a computer, network, system, or data without prior authorization (Hathaway et al., 2012 [15]). Therefore, in the consideration of this study, oil companies that have been victimized (even if only an intrusion attempt) by cyber criminals are considered to have been victims of cyber attacks.

Cyber Crime. In general, cyber-crime is defined as any type of crime that is conducted utilizing the Internet or other network (Gordon Ford, 2006 [16]). Therefore, in the consideration of this study, oil companies that have had successful cyber attacks waged against them (meaning that the cyber criminal has accessed the system) are considered to have been a victim of cyber crime.

Cyber Security. Most researchers define cyber security as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets" (von Solms van Niekerk, 2013 [17]). Therefore, in the consideration of this study, cyber security refers to any and all safeguards (such as software, hardware, equipment, and procedures/policies) established by oil companies in order to protect their information and to protect their SCADA systems from being accessed without appropriate authorization.

GCC Country. A GCC country is one of the Arab countries that have similarities, such as language and culture and are focused on similar goals (World Trade Organization, 2016) [3]. In the consideration of this study, the GCC countries being analyzed are Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and/or United Arab Emirates (Byres Lowe, 2004 [2]; United Arab Emirates, 2016 [3]).

Industrial Controls. Most researchers group industrial controls based on different systems that are used in industrial production. A common industry for industrial control systems is the oil industry. These systems are useful in this type of industry because they allow for the use of field devices that can be sent to remote locations for data gathering. The most common types of industrial controls are SCADA systems, distributed control systems (DCS), and programmable logic controllers (PLC) (Faulkner, 1956) [18]. Therefore, in consideration of this study, industrial controls are any controls (particularly SCADA systems) designed to work in the field, resulting in data being obtained for the use of the company.

Supervisory Control and Data Acquisition (SCADA). SCADA is defined as a system that allows for remote monitoring, providing allocations for coded signals to be conveyed across a network or communication channels (McDonald, 1993) [19]. Therefore, in consideration of this study, SCADA systems are any systems used by oil companies that use code to encrypt data from a remote site to a home base or cloud computing server/database

1.8 Organization of the Remainder of the Study

The remaining chapters include the literature review, research methodology, research findings and discussion, and conclusions and recommendations. Because of the remoteness that is associated with SCADA, the first two portions of the literature review discuss both cloud computing and oil companies and cyber security and cloud computing. Next, the chapter discusses cyber security and industrial controls. With this information, the researcher will be able to provide information regarding issues related to cyber security and cyber attacks.

The research methodology provides an overview of the problem and purpose, then restates the research questions. With this information, the research method and design can be developed. Once the research method and design is developed, it is necessary to determine the materials/instruments used in the study. Following this, the population sampling strategy is described, following by the procedures. Next, the chapter provides information regarding data collection, processing, and analysis, followed by methodological assumptions, limitations, and delimitations. Finally, ethical considerations will be discussed. The final two chapters in the study are research results and discussion and conclusions and recommendations.

1.9 Chapter Summary

This chapter introduced the topic of cybersecurity for industrial control systems and how these systems are influenced by human factor. Since technology has advanced quickly, data and cyber security has become a serious concern (Kaufman, 2009) [1]. In response to these concerns, the technology community is currently pushing to force policymakers to adopt universal standards for all service providers. It is believed that through universal standards, interoperability will be ensured. At the same time, the technology community is currently pushing to improve security standards for data. Although policymakers are making strides in this regard, technology commonly advances much faster than time allows for effective laws for cyber security to be developed (Kaufman, 2009) [1]. Industrial controls were previously believed to be less vulnerable to cyber-attacks. However, these systems commonly use web technologies, prompting greater concerns regarding cyber security (Byres Lowe, 2004) [2].

Certain industries, such as the oil industry within GCC countries, utilize industrial control systems, suggesting that there may be greater consequences of cyber-attacks to these industries. Since GCC share similar characteristics, it is commonly thought that these countries are more vulnerable than others within the world because this union is much smaller than others, such as the European Union. At the same time, cyber-attacks on oil companies in GCC countries are even more damaging because of the world's dependence on the oil produced in these countries.

Therefore, this study focuses on analyzing the cyber security risk of oil companies within GCC companies in consideration of attacks occurring through SCADA industrial controls. This is done through considerations of systems thinking (understanding how different components of a system influences a larger system) and the systems theory approach(Aronson, 1996 [10]; Salim, 2014 [11]).

Chapter 2

Literature review

The literature review is divided into several sections. The first two sections discuss oil companies and cloud computing, followed by discussions of cyber security and cloud computing. The third section discusses cyber security and industrial controls, followed by discussions of SCADA system cyber attacks, current resolutions to cyber security issues, and cyber security and GCC countries. The final portion is a brief summary of the chapter.

2.1 Oil Companies and Cloud Computing

Recent research confirms that cloud computing is a viable way for companies to "increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software" (Subashini Kavitha, 2011) [20]. Through cloud computing, companies are commonly able to do more with a lower investment, making cloud computing a popular option for many companies that engage in remote resources, such as oil companies. Still, despite the obvious benefits, there are numerous challenges for oil companies in adopting cloud computing tactics. The most significant difficulty is in relation to data security. In other words, as oil companies deal with extremely sensitive data and operations, they are more vulnerable to potential cyber attacks because of the nature of their tasks. This is because of the potential for significant harm through cyber attacks on oil companies. Moreover, oil companies use large data sets in the course of their tasks, which could increase their vulnerability when using cloud computing (Perrons Hems, 2013) [21]. Additional concerns exist regarding the significant investments that oil companies must make in information technology infrastructures throughout the course of their business operations. At present, much existing infrastructure makes integration to the cloud especially difficult. To combat these difficulties, cloud solutions focusing on private and hybrid cloud applications within the industry have been beneficial, because they allow different benefits to be derived from cloud-based technologies, as well as address cloud computing's constraints (Perrons Hems, 2013). On the other hand, it has been argued the use of these private and hybrid cloud solutions will only be temporary, due to advancements in information technology utilized within the industry. For instance, industries with similar challenges have seen that the use of cloud technologies as they pertain to private and hybrid solutions have been temporary in nature (Perrons Hems, 2013) [21].

A 2010 study shows some of the benefits and risks associated with the migration to the cloud for oil companies. The case study in this 2010 report considers the migration of an information technology system from in-house to Amazon EC2 based on the stakeholder perspective, which provides more information than the typical technical and financial analysis provided by providers (Khajeh-Hosseini, Greenwood, Sommerville, 2010) [22]. Within the case study, the infrastructure would potentially cost 37% less over 5 years on the EC2, as well as eliminate 21% of support calls. Based on these significant results, it was recommended that the system migrate to the cloud network; however, when considering the stakeholder impact analysis, significant risks were associated with this migration. Considering these vulnerabilities, it was argued in the case study that stakeholders consider the organizational implications caused by changes wrought by cloud computing in order to avoid implementations that would negatively impact organization-wide performance (Khajeh-Hosseini et al., 2010) [22]. Based on an article in The American Oil Gas Reporter, cloud technology is expected to significantly impact the way that energy companies, including oil companies, use information technology infrastructures (Seifarth Boush, 2013). The authors argue that although cloud computing is not new, it is being used in new ways due to advancements that have occurred in terms of "mobility, connectivity, and computing hardware" (Seifarth Boush, 2013) [23]. Moreover, the authors argue that the benefits of cloud computing have occurred in a vacuum, mostly because a common constraint of sharing data is connectivity. This constraint led to a modular approach to data sharing. On a small scale, the modular impact was the establishment of hard drives and floppy disks. On an enterprise level, the modular impact was the establishment of isolated data centers utilizing common connections to transmit data. Through this particular model, it became possible for enterprises, or even departments within a single enterprise, to collaborate despite the significant challenges relating to limited bandwidth. This concern has become a reality as, in 2016, there has been significant growth in mobile computing, which has led to increased stressors and expectations on the underlying infrastructure (Seifarth Boush, 2013) [23]. For instance, in the current technological landscape, it is worth noting that many professionals as well as organizations are connected through several devices that commonly include mobile connectivity. In fact, prolific Wi-Fi and data technologies (fiber optics, for example) have created wireless technologies that have nearly unlimited connectivity, which has lessened this particular constraint for oil companies (Seifarth Boush, 2013) [23].

Cloud technology refers to hardware and software that is maintained within a scalable environment and operate concurrently for business purposes, resulting in a unique infrastructure. Although cloud technology is commonly a central focus of the business process, it does not necessarily have all details or functions of different components (Seifarth Boush, 2013) [23]. Importantly, clouds can be public (held outside the firewall of a company) or private (held inside the firewall of a company). The public cloud is used by many customers, allowing for leveraged economy of scale in respect to costs related to hardware and software. The public cloud is used through Internet connectivity allowing for remote viewer serviceability. In contrast, the private cloud allows employees to "access applications and services within the confines of their established networks" (Seifarth Boush, 2013). The likelihood of harm by cyber-attack is reduced in the private cloud because all information is behind the network. However, in order to maintain this reduction, accessibility may be limited for mobile users or contractors without the proper credentials. Regardless of the type of cloud infrastructure, companies utilizing cloud-based services are embracing opportunities to advance technological initiatives from "basic file and Web hosting at a local provider to suites of integrated technologies offered by large firms with international infrastructure" (Seifarth Boush, 2013) [23]. The following figure 2.1 shows the features of cloud technology :

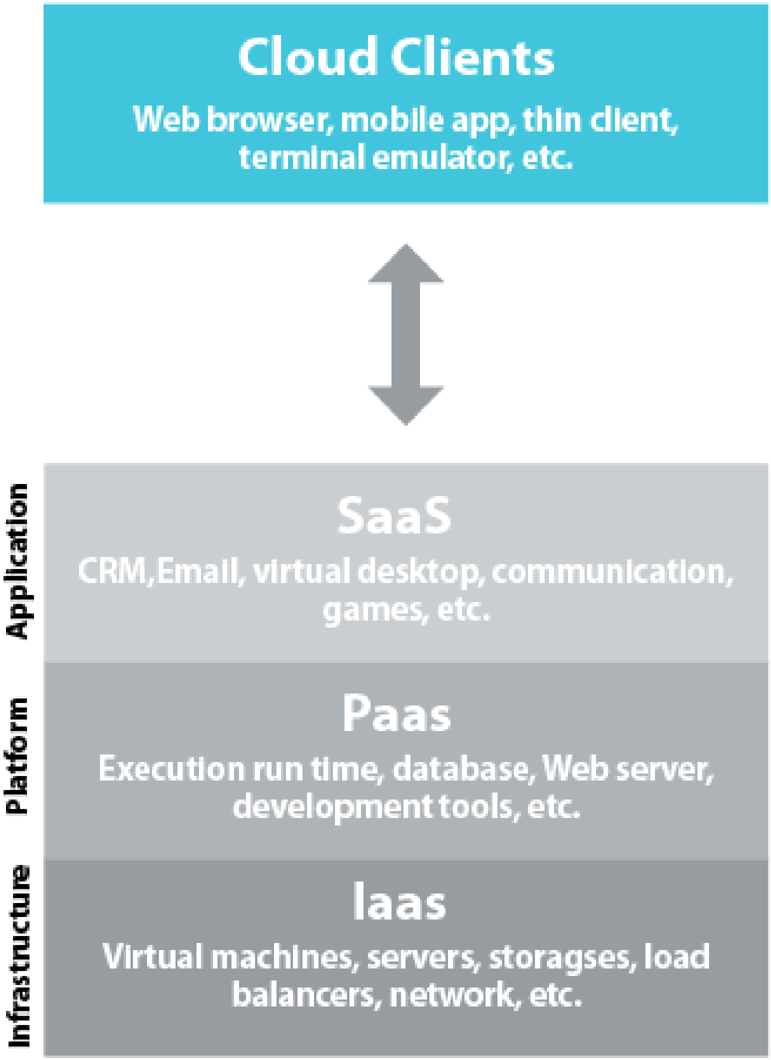

Cloud Clients
Web browser, mobile app, thin client, terminal emulator, etc.
SaaS
CRM,Email, virtual desktop, communication, games, etc.
Paas
Execution run time, database, Web server, development tools, etc.
Iaas
Virtual machines, servers, storagses, load balancers, network, etc.
Application
Platform
Infrastructure

Figure 2.1: Cloud Infrastructure

Cloud services are beneficial because they allow companies to choose the level of services needed based on the complexity of the infrastructure. As shown in Figure 2.1, there are common infrastructure layers within cloud technology, both with interactions and dependencies among different components within each tier. Most people use cloud technology as a service (SaaS) to the point that the absence of this technology would cause major disruptions to daily life, as well as regular communication. This trend has progressed in the business world, especially as agility and reliability increases.

Within the oil and gas industry, service providers have struggled to provide "client-server-based applications for the cloud-based modes. Available offerings include land and right-of-way management, rig tracking, fleet management, water monitoring, and supervisory control and data acquisition management" (Seifarth Boush, 2013) [23]. The benefit of moving these packages is to promote data associated with leasing, treatment, and transmission operations, as well as facility maintenance. At the same time, regulatory compliance and site engineering are increasing the need to directly provide critical information to managers. These developments require the availability of mobile or Wi-Fi data connections (Seifarth Boush, 2013) [23].

Another option of cloud-based services involves platform as a service (PaaS), which is an extension of SaaS. It is desirable because it has an increased speed in deployment for a development environment. Constraints would be further reduced because PaaS allows analysts to collaborate on issues and the platform can be adapted to meet ever-changing demands. The lowest branch is infrastructure as a service (IaaS), yet it is the most fundamental tier of cloud computing. This is because through IaaS, basic hardware services are offered for the establishment of new solutions, which "may include virtual servers, Web and database servers, and mass storage" (Seifarth Boush, 2013) [23]. IaaS is beneficial because services can be deployed easily and quickly, have improved scalability, and can be customized to meet changing needs.

IaaS complexity impacts the cost of services. Moreover, the ability of this complexity varies by the provider. For instance, some providers offer complex infrastructure services, whereas others offer basic services. Regardless of the size of the service provider, critical components are provided, "such as backup and recovery, system redundancy, and virtual and physical security" (Seifarth Boush, 2013) [23]. Complex business may engage services from business processes as a service (BPaaS) in order to develop a solution that utilizes different cloud-based service model tiers. This could involve additional staff, or customized software and/or hardware in order to meet the requirements of an organization, which benefits the organization through quick start-up and reduction in capital investment for a short-term project (Seifarth Boush, 2013) [23].

Although availability of service is a significant problem, there are even more concerns in relation to data security. When using public cloud services, there are increased vulnerable data points. Moreover, different regulations apply for data residing in the cloud. For instance, in the United States, data remaining in the cloud for more than 180 days are considered to be abandoned and can be requested by the government using a subpoena, rather than more complex warrants (39th U.S. Congress, 1986) [24]. Therefore, in order to afford the most protections, data should be encrypted before leaving the company. This is especially true if the company focuses on sensitive data. However, some of this threat can be alleviated if the company only uses non-sensitive or non-proprietary information within the cloud, which would limit exposure to potential breaches. At the same time, in many situations, physical security in the cloud is better than found in a typical company, such as the inclusion of "redundant hardware, distributed locations, shock-resistant buildings, and Internet and power backup" (Seifarth Boush, 2013) [23]. The anticipated benefit of these factors are common reasons for companies to consider utilizing cloud technology in the first place. Since oil companies operate in field-intensive arenas, attainable value can be derived from deploying these types of services because, regardless of the type of data being considered, "reliable and timely data transmission is critical to safe and profitable operations" (Seifarth Boush, 2013) [23].

This type of merger of business functions, according to the Oil Gas Council (2016) [25], is believed to be straightforward. However, oil companies have additional requirements due to the large data sets and high utilization rates of human resources. Currently, some solutions are available within cloud computing to meet these demands; however, these new solutions are in their infancy and do not yet meet the demand of oil companies. For instance, "data processing and graphical modeling requires workstations with very powerful processing capabilities and powerful graphics cards" (Oil Gas Council, 2016) [25]. These requirements are not standard and lie outside the typical cloud-based system scope. As a result, it might be more beneficial to "maintain high power workstations under the operational control of the specialists that need them, whilst seamlessly integrating the software of the workstations with the cloud system for all other functions" (Oil Gas Council, 2016) [25]. This approach results in a development of a hybrid system, rather than two separate systems running independently. This hybrid model is beneficial because it considers the concerns of the oil companies, as well as ensures that all needs are being met.

Among other benefits, cloud computing can result in a decrease in waste and an increase in convenience for oil companies. In fact, oil and gas companies have the potential to reap more benefits from the use of cloud computing than other industries. For instance, the oil industry is reliant upon emerging technologies to meet the demands of the work process. Implementing this new technology can be increasingly expensive, leading companies to balk at further investment, knowing that the technology will soon be obsolete. However, cloud systems are beneficial because they use technology in more efficient ways, "sharing infrastructure amongst multiple users and offices, offering a greater level of scalability and reducing the ongoing cost of implementation and continual development" (Oil Gas Council, 2016) [25]. Since the cost-of-entry is low and commonly on a pay-as-you-go basis, cloud technology is beneficial for smaller oil and gas companies because for an affordable rate, these companies can engage in advanced technology usage through a sophisticated infrastructure with low initial costs, which will increase benefits to the company further (Oil Gas Council, 2016) [25].

Professional cloud systems are hosted and managed by centralized support, which is beneficial because upgrades and hands-on support can be provided, allowing oil and gas companies to respond to operational developments, rather than focusing on technological issues within the infrastructures. Oil companies also need to link with multinational offices, which can be easily completed using cloud computing, due to the centralized system, which provides immediate access for all employees at the time it is needed (Oil Gas Council, 2016) [25]. Traditional solutions involve file versioning, such as checking-in and checking-out files, or adding a version number to the file name. These solutions are viable in the short term and in office; however, they are not beneficial on an inter-office or multinational scale. This is partly because of transmission difficulties, but also because of opportunities of "human error, duplication or data loss" (Oil Gas Council, 2016) [25] This finding indicates that human resources can be more efficiently used through knowledge transfer and collaborative working. Thus, cloud networks are beneficial in that they maximize "productivity, providing a platform for real-time collaboration across the entire workforce and network of consultants" (Oil Gas Council, 2016) [25]. Moreover, oil and gas companies must be able to share sensitive information. Through cloud computing, it is possible to develop shared space on the network to control access to this sensitive information, which provides security in sharing files without using unsafe connections within the Internet.

Most oil companies use remote working-which refers to "working from multiple offices, home or on the road (Oil Gas Council, 2016) [25]. Being able to have the company network accessible during remote working allows employees to meet current demand more easily. Moreover, the use of mobile technology is highly beneficial to transient staff members because connectivity is increased, allowing employees to make contact with their home office, even while working in the field. At the same time, the traditional way of traveling with sensitive information within a laptop is a potential security risk, which could lead to data loss or other company-wide issues. Recovery of lost data files can be more costly than the initial cost of secure storage in private clouds (Oil Gas Council, 2016) [25].

Security through cloud technology is enhanced, particularly in a public cloud. Since all data is stored on the cloud, should disaster occur, not all is lost. In fact, in this scenario, the solution is simply to obtain a new device and connect online in order to access all of the relevant information again. Private cloud technology is also secure due to the increased control of data centers with dedicated firewalls. Access can be customized with authentication processes in order to increase security. Authentication can be for the network, application, or individual PINS and key fobs (Oil Gas Council, 2016) [25]. Thus, software sharing can be done using private cloud technology. When hosting specific software on the cloud, it is possible that all employees can access the information, which can improve operational productivity and increase competitive advantage.

Previously, technology was used to increase efficiency and lower costs. However, efficiency is no longer sufficient to improve productivity. Technology, therefore, is used to drive innovation and to assist companies to exceed the levels of their competitors. In fact, cloud applications are more commonly chosen for company use, rather than traditional applications (Drilling Info, 2012) [26]. Moreover, there have been increases in revenue for these companies as they adopt new technologies leading to improvements in workflows, allowing ideas to flow faster throughout the organization. Thus, the use of SaaS has significantly impacted information technology, due to the benefits of reduced costs and improved efficiency. In fact, "changes in the industry, new regulations, and increased competition have companies looking at technology differently than they did even five years ago" (LandPoint, 2015) [27]. One such revolution has come from cloud computing, especially in relation to surveying and project management. Cloud computing offers the ability to distribute and retrieve information in a short amount of time, improving efficiency and decreasing expenses, making the investment a valuable one to those within the oil industry. For instance, oil companies handle significant amounts of data and manage multiple teams, commonly remotely, which makes the use of cloud computing viable. Therefore, cloud computing can be used to seamlessly integrate information from all parts of the process (such as from different team members) in one location for easy accessibility. Moreover, security is increased because information cannot be accessed without the appropriate credentials (LandPoint, 2015) [27]. Cloud computing enhances "quality control, connectivity, and real-time survey and drilling data" (LandPoint, 2015) [27]. Data can be collected and immediately uploaded for other employees to use, regardless of their location, and existing information can be integrated into other internal systems or used on-site.

Despite its advantages, the oil and gas industry has significant concerns in relation to the use of cloud computing in daily operations. The first concern is security. This is especially true within the GCC countries due to the increased dependence on oil for income. Therefore, expectations of security must be adjusted based on the type of service offered (Bennett, 2013) [28]. For example, if human resources data is being shared, security is enhanced. However, infrastructure services may have all security requirements placed on the customer. Customers need to consider what type of cloud services are being obtained, as well as the sensitivity of the data in order to determine the level of protections needed. The use of big data is another concern for oil companies wishing to engage in cloud computing. Big data can be used "to refer to the Geographic Information Systems used by the industry" (Bennett, 2013) [28]. Those companies that use cloud-based GIS systems need to consider if these systems are fast enough to meet their needs, if data is reliable, and if permissions are accessible for other data sources. Many oil companies have trade secrets due to GIS data stored in the cloud. In fact, "GIS data can represent valuable trade secrets," providing the competitive edge to the company (Bennett, 2013) [28]. As cloud providers typically demand the right to utilize stored data, promises commonly include masking or aggregating data for anonymity. This means that the oil company must determine if this sharing of data is acceptable. Moreover, the method used for aggregation must be considered, as "aggregated data can be reverse engineered and de-anonymized" (Bennett, 2013) [28].

There are solutions to these concerns. For instance, oil companies can get to know the vendor. In fact, "multi-tenancy makes vendors unwilling to vary their contracts" (Bennett, 2013) [28]. However, these customers are beneficial in providing information regarding the vendor, such as the status of the company (such as being a startup or well-established). This information can provide details regarding customer satisfaction. Some companies may decide it is more beneficial to be a major client of a smaller, well-established company than deal with a larger vendor. It is also necessary to consider the insurance carried by the provider, such as cyber liability. Companies need to be meticulous in performance of third-party security audits, which should be performed annually, as well as when significant changes in procedures or environment occur (Bennett, 2013) [28]. Another important consideration is to know the data being stored. For example, it is important to be aware of the nature and sensitivity of the data, due to laws and regulatory oversights that apply to regulated data. As a result, when performing cloud provider evaluations, it is beneficial to ask where the data is stored and who can access it, as well as if the provider has unique data centers. If the data centers are not owned by the provider, it is necessary to determine if the policies and protections of the subcontractors coincide with the vendor's protections and policies. Finally, companies should have an exit strategy in case something happens to the stored data or if something happens to the service provider (Bennett, 2013) [28].

2.2 Cyber Security and Cloud Computing

One of the most recognized cloud computing definitions comes from the National Institute of Standards and Technology (NIST). According to NIST, "cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell Grance, 2011 [29]; Takahashi et al., 2010 [30]). Importantly, cloud computing is scalable, provides for superior user experience, and is characterized by Internet influences. These influences have increased cloud computing development through cloud services. Cloud service market sizes have increased from USD 17 billion in 2009 to over USD 44 billion in 2013 (Gens, 2009) [31]. Thus, IT cloud services will outpace the traditional IT spending over time. However, these services are provided individually, resulting in little interoperability, which can be built through improved international standards in order to "improve application portability enabling resource accommodation between cloud service providers" (Takahashi et al., 2010) [30]. These types of advancements can result in improved reliability when disaster occurs, such as system outages and natural disasters. In fact, "major organizations such as Open Grid Forum (OGF), Distributed Management Task Force (DMTF) and Storage Network Industry Association (SNIA) are currently focusing on the service interoperability issues" (Distributed Management Task Force Inc., 2009 [32]; Metsch, 2009 [33]; Storage Networking Industry Association, 2010 [34]; Takahashi et al., 2010 [30]). Security, however, in relation to cloud computing is still in initial stages of development, despite advocacy about its importance and the provision of some guidelines by the Cloud Security Alliance (CSA) (Cloud Security Alliance, 2011) [35].

Thus, through cloud computing, it has become possible to expand the current capabilities of information technology. Yet as more information is cloud-based, security concerns have been raised. In fact, "security is one of the major issues which reduces the growth of cloud computing and complications with data privacy and data protection continue to plague the market" (Subashini Kavitha, 2011). New cloud computing models need to prepare for and mitigate concerns regarding "the risks of data breaches" (Subashini Kavitha, 2011) [20].

Research shows that the lack of a compliant environment has influenced the growth of cloud computing (Kandukuri, Ramakrishna Paturi, Rakshit, 2009) [36]. It is evident that "organizations using cloud computing as a service infrastructure, critically like to examine the security and confidentiality issues for their business critical insensitive applications. Yet, guaranteeing the security of corporate data in the 'cloud' is difficult, if not impossible, as they provide different services like SaaS, PaaS, and IaaS. Each service has its own security issues" (Kandukuri et al., 2009) [36]. For example, the SaaS model has no visibility regarding data storage and security, which increases concerns regarding this model. It is also noted that "there is a strong apprehension about insider breaches, along with vulnerabilities in the applications and systems' availability that could lead to loss of sensitive data and money. Such challenges can dissuade enterprises from adopting SaaS applications within the cloud" (Subashini Kavitha, 2011) [20].

Through SaaS, the vendor must protect security and ensure that multiple users are not viewing information that is unauthorized (Alliance, 2011; Archer Boehm, 2009 [37]; Brunette Mogull, 2009 [38]; Choudhary, 2007 [39]). SaaS applications have risks involved with "data security, network security, data locality, data integrity, data segregation, data access, and authentication and authorization" (Bamrara, 2015 [40]; Dunn Cavelty, 2014 [41]; Subashini Kavitha, 2011 [20]; von Solms van Niekerk, 2013 [17]).

There are numerous security concerns for cloud computing. For example, there are concerns regarding privileged access - that is, who has access to data and who decides on administrator management (Ramgovind, Eloff, Smith, 2010) [42]. There are also concerns regarding regulatory compliance, such as the cloud vendor undergoing external audits and maintaining security certifications (Brodkin, 2008) [43]. Additional concerns relate to data location, such as control over data location by the vendor (Sumter, 2010) [44]. Further security concerns may involve data segregation, such as encryption availability, including encryption design and testing (Brodkin, 2008) [43]. It is also important to be aware of recovery options, such as what happens to data in times of disaster and how (or if) it can be restored (Serrao, Aguilera Diaz, Cerullo, 2010) [45]. Security concerns also include investigative support, such as the ability to investigate inappropriate or illegal activity (Ramgovind et al., 2010) [42]. Companies also need to be aware of long-term viability, such as if the vendor no longer is in operation (Sabahi, 2011) [46]. Finally, companies must be concerned about data availability (Curran Carlin, 2012 [47]; Shaikh Haider, 2011 [48]).

Different security ontologies have been developed for cloud systems. For example, one ontology has three sub-ontologies-security (Fenz Ekelhart, 2009) [49], enterprise, and location. In this consideration, security encompasses five separate concepts-attribute, threat, rating, control, and vulnerability. A similar ontology was developed for security vulnerabilities, specifically software vulnerabilities (Wang Guo, 2009a, 2009b) [50]. Ontological semantics were used to extend the DMTF Common Information Model to contain security-related information and proposed an arbitrary information system (Tsoumas Gritzalis, 2006 [51]; Tsoumas, Dritsas, Gritzalis, 2005 [52]). A related work allowed for IS ontology to incorporate human behavior and related implications, providing a framework for the investigation of relationships of behavioral implications from IS management decisions prior to the deployment of security controls (Parkin, van Moorsel, Coles, 2009) [53]. Another study resulted in several ontologies using ontology web language (OWL) to establish security annotations aimed at agents and web services, addressing the representation of knowledge, as well as trust and security reasoning issues in relation to Semantic Web (Denker, Kagal, Finin, 2005) [54]. The reusability of these ontologies is limited or at early stages of development (Blanco et al., 2008) [55].

2.3 Cyber Security and Industrial Controls

Industrial control systems (ICS) include DCS and SCADA. At times, programmable logic controllers (PLC) are included as well. Industrial control systems are "typically used in industries such as electric, water and wastewater, oil and natural gas, transportation, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (e.g., automotive, aerospace, and durable goods)" (Stouffer, Falco, Scarfone, 2011) [56]. In most cases, SCADA systems are utilized to control assets that are spread out across a particular area. On the other hand, distributed control systems (DCS) are utilized to control local production systems. Finally, PLCs are used for specific applications and "generally provide regulatory control" (Cardenas, Amin, Sastry, 2008) [57]. Researchers note that "these control systems are vital to the operation of the U.S. critical infrastructures that are often highly interconnected and mutually dependent systems. It is important to note that approximately 90 percent of the nation's critical infrastructures are privately owned and operated" (Ericsson, 2010) [58]. As a result, many ICS are operated by federal agencies. Original ICS had little resemblance to traditional IT systems. However, as IP devices replace proprietary solutions, there are increased possibilities of vulnerabilities and cyber security incidents. Several scholars observe that "as ICS are adopting IT solutions to promote corporate business systems connectivity and remote access capabilities, and are being designed and implemented using industry standard computers, operating systems (OS) and network protocols, they are starting to resemble IT systems. This integration supports new IT capabilities, but it provides significantly less isolation for ICS from the outside world than predecessor systems, creating a greater need to secure these systems" (Cardenas et al., 2009) [57]. Security solutions have been developed for these types of issues in traditional IT systems. However, special precautions are required when introducing these solutions to ICS environments. At times, "new security solutions are needed that are tailored to the ICS environment" (Kim, Brancik, Dickinson, Perrig, Sinopoli, 2012) [59].

ICS has similar characteristics to traditional IT environments. However, there are some major differences. Many of these differences "stem from the fact that logic executing in ICS has a direct effect on the physical world" (Kuipers Fabro, 2006) [60]. For instance, some of the different characteristics can be related to significant risks for human lives (such as health and safety risks), environmental damage, production losses (prompting financial issues), negative economic impacts, and proprietary information compromise (Liu, Xiao, Li, Liang, Chen, 2012) [61]. It is evident that "ICS have unique performance and reliability requirements and often use operating systems and applications that may be considered unconventional to typical IT personnel. Furthermore, the goals of safety and efficiency sometimes conflict with security in the design and operation of control systems" (Dzung, Naedele, Von Hoff, Crevatin, 2005) [62].

Local threats were the primary issue for ICS implementations because of the components being in secured areas, not connected to IT networks or systems. As Peng et al. (2012) [63] notes, however, "the trend toward integrating ICS systems with IT networks provides significantly less isolation for ICS from the outside world than predecessor systems, creating a greater need to secure these systems from remote, external threats" (Peng et al., 2012) [63]. Since wireless networking has increased, ICS has greater risks from those who can access the network, either through authorized access or unauthorized access. Increasingly, "threats to control systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, malicious intruders, complexities, accidents, and natural disasters as well as malicious or accidental actions by insiders" (Patel, Bhatt, Graham, 2009) [64]. Therefore, the security objectives of ICS typically consider availability, integrity, and confidentiality (Felser Sauter, 2004) [65].

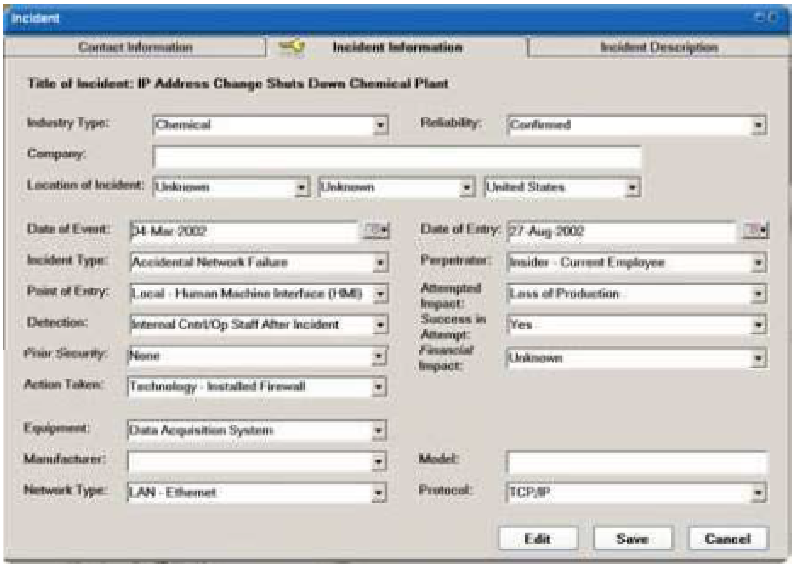
Potential ICS incidents may include disruptions of ICS operations, caused by the blocked or delayed information flow through the network. In other cases, there may be "unauthorized changes to instructions, commands, or alarm thresholds, which could damage, disable, or shut down equipment, create environmental impacts, and/or endanger human life" (Shea, 2004) [66]. There are also incidents where inaccurate information has been sent to operators. Such activity can be done for a number of reasons, such as "to disguise unauthorized changes, or to cause the operators to initiate inappropriate actions, which could have various negative effects"

(Cheminod, Durante, Valenzano, 2013) [67]. Transmission of inaccurate information could lead to the modification of software or configuration settings, or even lead to infecting the software with malware or interfering with safety system operations (Geer, 2006) [68].

Industrial control strategies commonly involve both intranet and Internet technologies, especially in relation to automation and modernization programs. These programs are deemed to be a combination of modernized state-of-the-art and traditional legacy installations. As a result, there are numerous challenges that exist in the establishment of effective security measures. In fact, "control system intrusions can cause environmental damage, safety risks, poor quality and lost production" (Creery Byres, 2005) [5]. There has been an increased "use of interconnected microprocessors in industrial systems" within the past decade (Creery Byres, 2005) [5]. Originally, these microprocessors were deployed in programmable logic controllers (PLC) and distributed control systems (DCS). Since this time, they have progressed to intelligent electronic devices (IED) in different applications, such as substations, heat trace systems, and motor control centers (MCC) (Creery Byres, 2005) [5]. However, concerns have developed regarding the growth of connecting networks. Despite this growth, there is typically little attention paid to security concerns. As has been documented in numerous studies, "intrusions, intentional and unintentional, can cause safety, environmental, production and quality problems" (Creery Byres, 2005 [5]; also discussed in Kuipers Fabro, 2006 [60]; Radmand, Talevski, Petersen, Carlsen, 2010 [69]; Salim, 2014 [11]; Trahan, 2016 [70]; von Solms van Niekerk, 2013 [8]; Yang et al., 2012 [8]; Zhu et al., 2011 [42]). Currently, few standards exist in relation to security, such as Standard 1164 established by the American Petroleum Institute (API) (American Petroleum Institute, 2004) [71]. Most of the standards are not widely known – or simply ignored. In many instances, the security problem can be resolved through the installation of a security criteria for the network as new equipment is deployed (Creery Byres, 2005).

Cyber security problems began gaining wide attention approximately two decades ago. In fact, many organizations have been involved in the resolution of this issue, such as the U.S. National Institute of Standards of Technology beginning in 1995, and the British Standards Institute and the Internet Engineering Task Force (IETF) beginning in 1997 (British Standards Institute, 1995 [72]; Fraser, 1997 [73]; International Organization for Standardization and the International Electrotechnical Commission, 2000; National Institute of Standards and Technology, 1995 [74]). Particularly related to the oil and gas sector are efforts by API in 2004 (American Petroleum Institute, 2004). The ISA-TR99.00.01-2004 focuses on overviews of electronic security technologies (Instrumentation Systems and Automation Society, 2004a), and the ISA-TR99.00.02 [75] focuses on the development of an electronic security program. Industry groups also recommended organization and structure for security plans (Instrumentation Systems and Automation Society, 2004b) [76].

In most cases, process equipment is controlled by devices that are monitored and controlled by Human Machine Interfaces (HMI), which use common operating systems that are networked together to allow for data sharing. In most cases "this data is gathered by maintenance and process groups and then transmitted to management groups" (Creery Byres, 2005) [5]. The ability to gather data has grown recently, resulting in traditional and/or older network being connected to state-of-the-art equipment, yielding a hybrid network. Personal computers can be hacked through tools for identification of vulnerable programs. One such tool is an open port, which uses a listening application on the targeted machine, commonly known as NetBIOS, allowing client software access to LAN resources. One group that tracks industrial cyber security incidents is the British Columbia Institute of Technology (BCIT). BCIT has a database that stores information using web forms, such as the one in the following figure 2.2 :



Title of Incident: IP Address Change Shuts Down Chemical Plant

Industry Type: Chemical
Reliability: Confirmed
Company:
Location of Incident: Unknown | Unknown | United States
Date of Event: 04 Mar 2002
Date of Entry: 27 Aug 2002
Incident Type: Accidental Network Failure
Perpetrator: Insider - Current Employee
Point of Entry: Local - Human Machine Interface (HMI)
Attempted Impact: Loss of Production
Detection: Internal Cntrl/Op Staff After Incident
Success in Attempt: Yes
Prior Security: None
Financial Impact: Unknown
Action Taken: Technology - Installed Firewall
Equipment: Data Acquisition System
Manufacturer:
Model:
Network Type: LAN - Ethernet
Protocol: TCP/IP

Figure 2.2: Typical Security Incident Entry Screen

Based on the information entered in the web forms, such as the one shown in Figure 2.2, companies can protect their networks more effectively. It is important to note that "the majority of industrial incidents prior to 2001 came from internal attacks, while after 2001 outside sources have become the most common attack vector. This swing has been attributed to increased use of common operating systems and applications, larger connected networks and automated 'worm"' attacks" (Creery

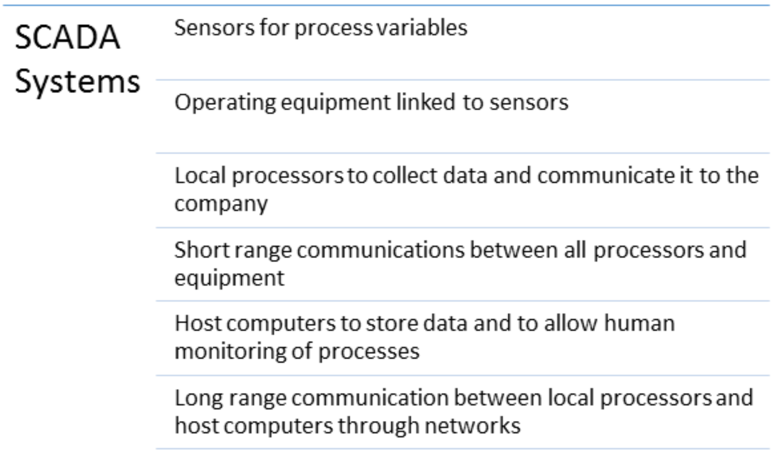
Byres, 2005) [5]. One of the most common attacks comes from virus or worms, which reduces communication between the control computers, resulting in a lack of control over running equipment by operators (Creery Byres, 2005) [5]. When financial impacts of such incidents were estimated, the impact was found to be more than USD 1 million (Byres Lowe, 2004) [2].

2.4 SCADA Systems Cyber Attacks

In 2014, SCADA system cyber attacks doubled (Lennon, 2015) [77]. According to one study, many of these attacks were political in nature. This is because many attackers tend to "target operational capabilities within power plants, factories, and refineries" (Lennon, 2015) [77]. It was also noted that "buffer overflow vulnerabilities were the primary point of attack against SCADA systems, which control remote equipment and collect data on equipment performance, accounting for 25% of the attacks witnessed by Dell" (Lennon, 2015) [77]. Most attacks occurred in Finland, the United Kingdom, and the United States. Attacks were most common in areas that were most consistently connected to the Internet. In 2014, Dell reported 202,322 SCADA attacks in Finland, 69,656 in the U.K., and 51,258 in the U.S. (Lennon, 2015) [77]. According to information provided by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) these attacks appear to be advanced, persistent threats. In fact, "ICS-CERT has issued alerts for multiple campaigns over the last year, including one which focused on the use of the Havex RAT in attacks aimed at ICS, and the second related to BlackEnergy attacks exploiting vulnerabilities in products from GE, Advantech/Broadwin, and Siemens" (Lennon, 2015) [77]. Based on this information, it can be hypothesized that Havex RAT attacks are more common than BlackEnergy attacks. However, due to the wider range of products, the BlackEnergy attacks seem to be more severe.

Yet there is continuous growth of cyber security threats and attacks. Moreover, malware is becoming more sophisticated, which impacts "the security of critical infrastructure, industrial control systems, and Supervisory Control and Data Acquisition (SCADA) control systems" (Hentea, 2008) [78]. Modern infrastructures are reliable because of computerized systems and SCADA systems. Through the development and emergence of online technologies, both systems have been integrated with business systems, increasing cyber threat risks. As a result, concerns have increased regarding the security and safety of SCADA systems, prompting the Presidential Decision Directive 63 to establish critical infrastructure framework protection, as well as the National Strategy to Secure Cyberspace (Hentea, 2008) [78]. According to these documents, critical infrastructure "includes telecommunication, transportation, energy, banking, finance, water supply, emergency services, government services, agriculture, and other fundamental systems and services that are critical to the security, economic prosperity, and social well-being of the public. The critical infrastructure is characterized by interdependencies (physical, cyber, geographic, and logical) and complexity (collections of interacting components)" (Hentea, 2008) [78]. Disruptions in this critical infrastructure can impact other infrastructures, geographic regions, and the economy as a whole. Thus, efforts need to be increased in reducing vulnerabilities of critical infrastructures, as well as improving security operations. One approach is through more effective risk analysis. Risk management is also important and potentially more beneficial to SCADA because it is "based on automated tools and intelligent techniques [that] require minimum or no human intervention in controlling the processes" (Hentea, 2008 [78]). These preventions are crucial to the control system because they are commonly the basis of operations in many industries, such as the oil industry.

In consideration of SCADA systems, increasing concerns have been in relation to security, safety, vulnerabilities, lack of protection, and awareness of threats (Byres Franz, 2005 [79]; Byres, Hoffman, Kube, 2006 [80]). Figure 2.3 shows the components of a SCADA system .



SCADA Systems

- Sensors for process variables
- Operating equipment linked to sensors
- Local processors to collect data and communicate it to the company
- Short range communications between all processors and equipment
- Host computers to store data and to allow human monitoring of processes
- Long range communication between local processors and host computers through networks

Figure 2.3: Components of SCADA System

SCADA systems have wider impacts in many instances because they cover large areas, as compared to distributed control systems, which focus on one specific site in most cases. In many SCADA systems, there are "a variety of both wired and wireless media and protocols involved in getting data back to the central monitoring site. This enables implementation of powerful IP-based SCADA networks over mixed cellular, satellite, and landline systems" (Hentea, 2008) [78]. Concerns are increased for SCADA systems because they can monitor and control thousands of in/out points. The newest SCADA systems will be able to handle nearly 1 million I/O channels. Increasingly advanced SCADA systems have different characteristics: time critical, embedded, fault tolerant, distributed, intelligent, large, open, and heterogeneous (Sanz Arzen, 2003) [81].

The advancement of SCADA systems have led these systems to be ranked high in terms of governmental concerns, especially as terrorists have threatened to attack and have successfully attacked critical infrastructure systems that use SCADA (Dacey, 2003) [82]. The successful attacks have become "more sophisticated and the notion of what kind of vulnerabilities actually matter is constantly changing" (Hentea, 2008) [78]. Commonly, threats are misunderstood or not understood at all, prompting them to be ignored. For example, threats, vulnerabilities, and attacks are at different levels for "software controlling or controlled device, application, storage, data access, LAN, enterprise, Internet, [and] communications" (Hentea, 2008) [78]. Most recently, SCADA systems have adopted web technology in order to meet the need for internal communications. However, web technology is often targeted for automated cyber attacks, especially due to the immaturity of web-based secure software. Moreover, "the reality is that a growing number of worms and viruses spread by exploiting software design, operations, and human interfaces. The software-intensive system design skills for the construction of control systems are often misunderstood. In the control industry, two separate groups of engineers are typically involved in the development of any nontrivial controller: control engineers and programmers"

(Hentea, 2008) [78]. Modern SCADA networks, which are integrated with both corporate networks and the internet, are more vulnerable to unauthorized cyber attacks (Hentea, 2008) [78].

SCADA networks are expected have 99.999% availability, resulting in less than 5.3 minutes of downtime annually. The need for increased security is compelling. Vulnerability reductions and security operation improvements are necessary in order to reduce risks that may impact critical operations. The increased complexity of SCADA systems may impact risks in relation to safety, quality of service, and security for data and systems (Pasik-Duncan, Patton, Schilling, Camacho, 2006) [83]. Researchers note that "SCADA security design and information security management can be improved by applying a wide range of control principles and methods as well productivity control, involving decision-making under uncertainty with increased levels of decision support" (Hentea, 2008) [78]. Several key requirements can be found for establishing increased security. For example, critical path protection can prevent cyber attacks. In fact, one component failure can increase chances for multiple, simultaneous component failures. At the same time, stronger safety policies and procedures can be adopted. These can include "increased awareness of potential vulnerabilities and solutions, as well as implementing stronger safety policies and procedures" (Hentea, 2008) [78]. Next, knowledge management should be supported. For example, "security knowledge is likely to include policy, standards, design and attack patterns, threat models, code samples, reference architecture, and secure development framework" (Hentea, 2008 [78]; Steven, 2006 [84]). It is also important to have system development skills, such as software evaluation, and to have enhanced device security, which involves measuring the cost of security implementation against potential costs if there is discovery of the vulnerabilities of systems (Chao Zhang et al., 2013) [85]. Solutions also need to be developed to increase security and privacy within sensor networks. Moreover, operating systems will need to be based on microkernel architecture in order to limit coding. Thus, software quality can be improved through security features, especially if they are required early in the software development cycle (Menzies Richardson, 2006 [85]; Saydjari, 2002) [86]. Standards need to be complied with for software development, including for the integration of different technologies. Such integration can be initially accomplished through a vulnerability analysis based on different types of solutions-proactive, discovery, and adaptation. As a result of this analysis, there may be innovative risk management approaches, which can include authentication, confidentiality, integrity, availability, and nonrepudiation adherences (Hentea, 2008) [78].

2.5 Current Solutions to Cyber Security Issues

There are several important objectives to solving cyber security issues like these. First, solutions need to be focused on "restricting logical access to the ICS network and network activity" (Cai, Wang, Yu, 2008) [87]. Such restrictions could involve using firewalls and a demilitarized zone (DMZ) architecture, aimed at preventing network traffic from having direct passage between corporate and ICS networks. In these cases, it is important to have "separate authentication mechanisms and credentials for users of the corporate and ICS networks. The ICS should also use a network topology that has multiple layers, with the most critical communications occurring in the most secure and reliable layer" (Hahn Govindarasu, 2011) [88]. Other important steps involve restricting physical access to the network and devices so as to prevent disruption of the functionality of the ICS. It would be beneficial to have access controls, "such as locks, card readers, and/or guards" (Knapp Langill, 2014) [89]. In other instances, it is necessary to protect the individual components from exploitation, which involves using security patches, disabling unused ports and services, restricting privileges to necessary access, monitoring audits, and utilizing security controls (Sommestad, Ericsson, Nordlander, 2010) [90]. It is also important to consider adverse conditions, prompting the design of the ICS so that "each critical component has a redundant counterpart. Additionally, if a component fails, it should fail in a manner that does not generate unnecessary traffic on the ICS or other networks, or does not cause another problem elsewhere, such as a cascading event" (Cai et al., 2008 [78]; C. Wang, Fang, Dai, 2010 [91]).

2.6 Cyber Security and GCC Countries

National power can be derived through cyber attacks because such attacks enhance coercion, influence, and warfare (Lewis, 2014) [92]. However, cyber attacks are not new. As an intelligence tool, cyber technology was originally used in the 1980s. As a warfare tool, cyber attacks were used back in the 1990s (Lewis, 2014) [92]. Within the Persian Gulf States, cyber tools and techniques are significant instruments of national power. Indeed, "the Gulf has become a flashpoint for cyber conflict given the high level of activity and the chance for miscalculation and escalation into conventional conflict. The Gulf is unique in that the use of cyber techniques by governments for covert action is much more prevalent than in any region other than the Korean peninsula" (Lewis, 2014) [92]. Due to the strategic and economic significance of the Persian Gulf, cyber attacks on oil production or physical conflicts could result in global consequences, especially as the use of cyber warfare can result in a shift in the military power balance among the regional states resulting in changes to the Gulf's stability, particularly if GCC states do not increase their defenses against this threat. These defenses have been pre-empted by three incidents. The first was social media impacts and the Internet in Arab uprisings that occurred in 2011, as well as the Green Revolution in Iran in 2009. The second was the 2010 Stuxnet attacks against nuclear facilities in Iran. Finally, the 2012 attacks on Saudi Aramco and Qatari RasGas prompted political leaders to consider cyber security issues (Lewis, 2014) [92].

Chapter 3

Research Methodology

3.1 Introduction

In most situations, data analysis is conducted either quantitatively or qualitatively (Creswell, 2013) [93]. When focusing on quantitative research, deduction, based on positivism and objectivism, is commonly used (Sarantakos, 2012) [94]. Qualitative research, on the other hand, typically uses induction, based on an interpretivism (Reay Jones, 2015) [95]. Through the qualitative method, it is possible to be subjective and develop new knowledge, rather than focus on existing knowledge.

The current study is based on a mixed methods approach in consideration of the theoretical framework established in Chapter 1. The goal for this study was to analyze the overall trends of the cyber security issues for industrial controls, specifically SCADA, for oil companies in GCC countries, as well as probabilities of occurrence based on historical data. The resulting data may be used to provide recommendations for protections for GCC countries and/or oil companies at risk of attack.

3.2 Problem and Purposes Overview

In this study, the problem to be discussed is whether and how the oil companies in GCC countries use industrial control networks that make them vulnerable to attack. The purpose of this mixed methods research project was to examine the trends and patterns that exist in relation to cyber security and industrial controls (specifically SCADA) for oil companies in GCC countries. The independent variable was cyber security. The dependent variable was industrial controls. The variables were measured through a statistical analysis that considers probability statistics, regression analysis, and chi squared test. The data will come from previous cases, which will be used to determine the trends that exist within this field. These trends will be measured based on rate of occurrence and year of occurrence. The goal of the research study was to determine the ways that cyber security has been influenced for industrial controls, determine what guidelines have been developed to prevent cyber-attacks on industrial controls, and determine the probability of cyber-attack trends that have emerged that have allowed oil companies to protect their industrial controls, specifically SCADA, in GCC countries.

3.3 Restatement of the Research Questions

The research questions include:

1. In what way has cyber security been influenced by the human factor for industrial controls, specifically SCADA, for oil companies in GCC countries?

2. To what extent have guidelines been developed to prevent cyber-attacks on industrial controls, specifically SCADA, for oil companies in GCC countries?

3. To what extent have specific trends regarding the human factor emerged in cyber-attacks on industrial controls, specifically SCADA, for oil companies in GCC countries?

4. Is it possible to determine the likelihood of a GCC country in being attacked due to having oil companies within it?

3.4 Research Method and Design

This study is designed as a mixed methods study that uses quantitative and qualitative data. The data were obtained through prior studies in order to determine the trends of cyber-attacks for industrial controls. This data will then be related to oil companies in GCC countries. The specific trends are the qualitative data and will be explained in the Materials/Instruments section. Both types of data were analyzed using Microsoft Excel. However, the two data sets were treated differently. For example, the quantitative data was actually analyzed using Microsoft Excel's data analysis toolpack, while the qualitative data was analyzed using Microsoft Excel for grouping the data into similar categories.

3.5 Materials/Instruments

In order to investigate the impact of human factors in designing the cyber security policy of a company, this thesis has designed a concise questionnaire with eight basic questions.The basis of these questions are the site visits conducted by the author. The author discussed it with the experts/individuals there and come up with the following eight questions:

1. How often do you exchange data via organizational systems (email, etc.)?

2. How often do you use your personal devices (mobile or laptop) inside the organization's network (Wi-Fi)?

3. How often do you use a remote system for your daily work?

4. Do you face difficulties in configuring or using the system or the network?

5. How often do you use a third-party system in your daily work?

6. Do you feel that the network security policy affects workflow?

7. How thorough is your knowledge in cyber security?

8. Have you had an awareness course on cyber security conducted or hosted by your organization?

This research study applies two methods, qualitative and quantitative analysis, to examine the trends and patterns that exist in relation to cyber security and industrial controls (specifically SCADA) for oil companies in GCC countries. The data used for these analyses have been obtained from previously reported cases and will be used to determine the types of attacks launched, their damage, and precautions against such attacks in future. This information will be used to analyze the ways that cyber security has been influenced by the industrial controls. The study is focused on companies' awareness regarding these attacks and their countermeasures. Using this knowledge base, a set of guidelines is proposed in the final chapter of this study.

For the selection and analysis of previously reported cyber-attacks, the following criterion has been adopted:

1. The article must be scholarly or governmental.
2. Preferably it should discuss ICS and cyber security.
3. Preferably the article should be related to oil industry.

Based upon these criteria, a detailed state-of-the-art literature survey was conducted to predict the pattern of the attacks and possible guidelines.

This thesis considered approximately 50 articles based on the preceding criteria. Since computing technology in some form has been used since the 1980s, the span for article searching was 1980 to 2016. This criterion provided a significant time gap of 36 years, which allows this thesis to provide a narrative in relation to changes in technology and how these changes impact the ability of cyber criminals to attack oil companies within GCC countries. Articles were searched primarily on academic databases. However, the author is aware that sometimes articles can be found through a simple Google search and still meet the inclusion criteria. For the second inclusion criteria, it must be noted that it is not necessary for the article to provide specific trends. Rather, there must be enough information for the author to be able to determine trends. Search keywords and key phrases included: "cyber attacks: "cyber attacks GCC countries," "cyber attacks and GCC countries," "attacks oil companies GCC countries," "cyber attacks oil companies GCC countries," "SCADA systems GCC countries," "SCADA systems oil companies GCC countries," "oil companies Bahrain," "oil companies and Bahrain," "oil company attacks Bahrain," "oil company attacks and Bahrain," "oil company attacks in Bahrain," "cyber attacks Bahrain," "cyber attacks and Bahrain," "oil companies Kuwait," "oil companies and Kuwait," "oil company attacks Kuwait," "oil company attacks and Kuwait," "oil company attacks in Kuwait," "cyber attacks Kuwait," "cyber attacks and Kuwait," "oil companies Oman," "oil companies and Oman," "oil company attacks Oman," "oil company attacks and Oman," "oil company attacks in Oman," "cyber attacks Oman," "cyber attacks and Oman," "oil companies Qatar," "oil companies and Qatar," "oil company attacks Qatar," "oil company attacks and Qatar," "oil company attacks in Qatar," "cyber attacks Qatar," "cyber attacks and Qatar," "oil companies Saudi Arabia," "oil companies and Saudi Arabia," "oil company attacks Saudi Arabia," "oil company attacks and Saudi Arabia," "oil company attacks in Saudi Arabia," "cyber attacks Saudi Arabia," "cyber attacks and Saudi Arabia," "oil companies UAE," "oil companies and UAE," "oil company attacks UAE," "oil company attacks and UAE," "oil company attacks in UAE," "cyber attacks UAE," and "cyber attacks and UAE."

3.6 Procedures

The responses from the employees have been collected from the oil industry in the Gulf Cooperation Council (GCC). According to the standard formula proposed by (Krejcie and Morgan, 1970) [96], a total number of about 400 IT people requires a sample size of 196. Consequently, this thesis collected responses from 210 IT employees through personal contacts. All their identities have been kept secret.

The study is justified because it provides answers to research questions through the use of existing data. The data analysis allows the hypothesis to be confirmed or disconfirmed. This research was conducted through the use of a mixed method analysis, focusing on both qualitative and quantitative data. Through consideration of the research results, the existing literature can be furthered by providing another viewpoint of results, such as through GCC country oil companies. Although information was gathered from articles for qualitative data, it was quantified for the collection of quantitative data. The procedure for the qualitative data consisted of a systematic analysis, complete with a quality assessment tool established by Downs and Black (1998) [97], presented in Appendices A and B. Quantitative data was derived from the qualitative data based on themes.

3.7 Data Collection: Processing and Analysis

Quantitative data focuses on numerical values, whereas qualitative data focuses on inferences from the data.Quantitative data was analyzed through statistical analysis

(Creswell, 2013) [93]. Qualitative data, on the other hand, could be used to verify the quantitative data, as well as create links between the current knowledge of cyber-attacks on industrial controls of oil companies in GCC companies and what the data results show.

SPSS software was used to analyze the responses. The remaining part of this section presents the analysis of data and recommendations to the oil industry specifically and to any general industry using ICS.

3.8 Ethical Considerations

There are no ethical considerations to take into account in this study, since all data comes from public sources. However, the author will need to ensure that objectivity remains consistent in conjunction with the research method set forth in preceding sections.

3.9 Chapter Summary

The goal for this study was to analyze the overall trends of the cyber security issues for industrial controls, specifically SCADA, for oil companies in GCC countries, as well as probabilities of occurrence based on historical data. The purpose of this mixed methods research project was to examine the trends and patterns that exist in relation to cyber security and industrial controls (specifically SCADA) for oil companies in GCC countries. The independent variable was cyber security. The dependent variable was industrial controls. The variables were measured through a statistical analysis that considers probability statistics, regression analysis, and chi square test. The goal of the research study was to determine the ways that cyber security has been influenced for industrial controls, determine what guidelines have been developed to prevent cyber-attacks on industrial controls, and determine the probability of cyber-attack trends that have emerged that have allowed oil companies to protect their industrial controls, specifically SCADA, in GCC countries.

Chapter 4

Research Findings and Discussion

This chapter is divided into two major sections, the first related to an analysis of the human factor and second regarding the security of the SCADA system.

4.1 Human Factor

In order to investigate the impact of human factors in designing the cyber security policy of a company, the authors designed a concise, eight-question questionnaire (presented in Chapter 3) examining participants' use of their personal devices, use of remote systems and networks, and cyber security.

Responses from the employees have been collected from the oil industry in the Gulf Cooperation Council (GCC). A total of 210 responses from IT employees were collected. All identities have been kept secret.

SPSS was used to analyze the responses. The remaining part of this section presents the analysis of data and recommendations to the oil industry specifically and to the any general industry using ICS. The results presented in this chapter are based upon the views and responses of the IT people of this important oil industry. These results make the author able to propose the useful guidelines for this industry.

Table 4.1 shows the responses regarding the exchange of data. The response to this question contains the number of days. The response 5.0 shows that the user exchanged the data through private email and third party software five days a week i.e. daily. As the data depicts, the exchange of data is very high with almost 83% of workers taking part. Chi-Square value is within the significant range.

Table 4.1: Exchange of data

Q. How often do you exchange data via organization system (email, etc.)?					
	Responses	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
Valid	**3.0**	**12**	**5.7**	**5.7**	**5.7**
	4.0	24	11.4	11.4	17.1
	5.0	174	82.9	82.9	100.0
	Total	210	100.0	100.0	
Descriptive Statistics					

N	**Mean**	**Std. Deviation**	**Minimum**	**Maximum**
210	4.771	.5404	3.0	5.0

Table 4.2 shows responses regarding the use of personal devices. The analysis of data shows that 51.4% employees used their personal devices in the organization.

Chi-Square	**232.800a**
df	2
Asymp. Sig.	.000

This is a big loophole for cyber-attackers. It is recommended that personal devices should not be allowed in such sensitive organizations. Moreover, open-access Wi-Fi connections must be discouraged in such organizations. Chi-Square value for this item is within the significant range.

Table 4.2: Use of personal devices

Q. How often do you use your personal devices (Mobile Laptop) inside the organization network (Wi-Fi)?					
	Responses	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
Valid	**Daily**	**108**	**51.4**	**51.4**	**51.4**
	Not Allowed	54	25.7	25.7	77.1
	Occasionally	48	22.9	22.9	100.0
	Total	210	100.0	100.0	
Descriptive Statistics					

N	**Mean**	**Std. Deviation**	**Minimum**	**Maximum**
210	1	3	1.74	.842

Table 4.3 shows the responses regarding the remote system access. It is clear from the analysis that almost 80% of employees were accessing the remote systems for

Chi-Square	**31.200a**
df	2
Asymp. Sig.	.000

their daily/routine work. Such access and connections are also vulnerable to cyber-attacks. It is recommended that such connections be protected through standard security protocols. Chi-Square value for this item is within the significant range.

Table 4.3: Remote system access

Q. How often do you use remote system for your daily work?					
Valid	**Responses**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
	Daily	**108**	**51.4**	**51.4**	**51.4**
	Weekly	60	28.6	28.6	80.0
	Never	42	20.0	20.0	100.0
	Total	210	100.0	100.0	
Descriptive Statistics					

N	**Mean**	**Std. Deviation**	**Minimum**	**Maximum**
210	1	3	1.69	.786

Chi-Square	**33.257a**
df	2
Asymp. Sig.	.000

Table 4.4 shows the responses regarding the difficulty in configuring systems and networks. The analysis shows that configuration of system and network is not a difficult task for the employees. Almost 69% of employees stated that it was very easy. It is recommended that network configuration and setup should be confidential, and employees should not be allowed to connect/configure their personal gadgets easily. Some administrative approvals must be implemented to ensure the trustworthiness of the employee and the device.

Table 4.4: Difficulty in configuring systems and networks

Q. Do you face difficulty to configure or use the system or the network?					
	Responses	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
Valid	**No configuration required**	**36**	**17.1**	**17.1**	**17.1**
	Easy	144	68.6	68.6	85.7
	Never	30	14.3	14.3	100.0
	Total	210	100.0	100.0	
Descriptive Statistics					

N	**Mean**	**Std. Deviation**	**Minimum**	**Maximum**
210	1	3	1.97	.561

Chi-Square	**117.600a**
df	2
Asymp. Sig.	.000

Table 4.5 shows the responses regarding the use of third-party systems. As the data depicts, the percentage of participants who always/occasionally used third-party systems was almost 50%. Therefore, it is recommended that such third-party systems must be verified and the software must be checked for security before being able to use the industry's IT infrastructure. Unverified third-party software is vulnerable to cyber-attacks and the companies must protect their operations from these unverified, potentially vulnerable products.

Table 4.5: Use of third-party systems

Q. How often you use a third party system in your daily work?					
Valid	**Responses**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
	Always	**24**	**11.4**	**11.4**	**11.4**
	Occasionally	78	37.1	37.1	48.6
	Never	108	51.4	51.4	100.0
	Total	210	100.0	100.0	
Descriptive Statistics					

N	**Mean**	**Std. Deviation**	**Minimum**	**Maximum**
210	1	3	2.40	.686

Chi-Square	**51.771a**
df	2
Asymp. Sig.	.000

Table 4.6 shows the responses regarding the network security policies effects on

workflow. The responses show that most of the employees thought that network security policies would affect the workflow of the organization. This shows their tendency that they are not willing to accept this change, i.e., they are not willing to enforce or follow various security policies. They think that the workflow will be affected, and thus they do not welcome the new policies. It is recommended that proper counseling of employees is needed to ensure the usefulness and importance of such security policies.

Table 4.6: Network security policy effect on workflow

Q. Do you feel that the network security policy affects workflow?					
Valid	**Responses**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
	Agree	**60**	**28.6**	**28.6**	**28.6**
	Sometimes	120	57.1	57.1	85.7
	Disagree	30	14.3	14.3	100.0
	Total	210	100.0	100.0	
Descriptive Statistics					

N	**Mean**	**Std. Deviation**	**Minimum**	**Maximum**
210	1	3	1.86	.640

Chi-Square	**60.000a**
df	2
Asymp. Sig.	.000

Table 4.7 shows the level of security knowledge of employees. The data show that

many employees do not have complete knowledge regarding cyber security. This is very important, since IT employees of this important industry must have adequate knowledge of cyber security. Therefore, it is recommended that the companies must consider this important aspect while hiring IT personnel for their organization, and/or that regular and mandatory courses are programmed to keep the employees updated on this topic.

Table 4.7: Level of knowledge in cyber security

<table>
<tr><th colspan="6">Q. How much is your knowledge in cyber security?</th></tr>
<tr><th rowspan="7">Valid</th><th>Responses</th><th>Frequency</th><th>Percent</th><th>Valid Percent</th><th>Cumulative Percent</th></tr>
<tr><td>**1.0**</td><td>**24**</td><td>**11.4**</td><td>**11.4**</td><td>**11.4**</td></tr>
<tr><td>1.0</td><td>66</td><td>31.4</td><td>31.4</td><td>42.9</td></tr>
<tr><td>3.0</td><td>66</td><td>31.4</td><td>31.4</td><td>74.3</td></tr>
<tr><td>4.0</td><td>42</td><td>20.0</td><td>20.0</td><td>94.3</td></tr>
<tr><td>5.0</td><td>12</td><td>5.7</td><td>5.7</td><td>100.0</td></tr>
<tr><td>Total</td><td>210</td><td>100.0</td><td>100.0</td><td></td></tr>
<tr><th colspan="6">Descriptive Statistics</th></tr>
</table>

N	Mean	Std. Deviation	Minimum	Maximum
210	1.0	5.0	2.771	1.0739

Chi-Square	56.571a
df	4
Asymp. Sig.	.000

Table 4.8 shows the responses regarding awareness courses on cyber security. This

is a very important aspect, and as the data depicts, almost 80% of employees have never had an awareness course on cyber security, or they have had only one course in a lifetime. It is strongly recommended that the organization arrange such awareness courses on a bi-monthly or quarterly basis to ensure that employees have an up-to-date knowledge of cyber-attacks and their prevention.

Table 4.8: Awareness course on cyber security

Q. Have you had an awareness course on cyber security held by your organization?					
Valid	**Responses**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
	1.0	**24**	**11.4**	**11.4**	**11.4**
	Yearly	48	22.9	22.9	22.9
	Once	84	40.0	40.0	62.9
	Never	78	37.1	37.1	100.0
	Total	210	100.0	100.0	
Descriptive Statistics					

N	Mean	Std. Deviation	Minimum	Maximum
210	1	3	2.14	.763

Chi-Square	**10.629a**
df	2
Asymp. Sig.	.005

4.2 Secure SCADA systems

The areas chosen for this state- of- the- art literature study are cyber security and cloud computing, cyber security and industrial controls, SCADA cyber-attacks and current solutions to cyber security issues.

Research shows that cloud computing is a viable way for companies to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software (Ponemon Institute LLC, 2016) [98]. Through cloud computing, it has become possible to expand the current capabilities of information technology. On the other hand, as more information is cloud based, security concerns have been raised. As a matter fact, "security is one of the major issues which reduces the growth of cloud computing and complications with data privacy and data protection continue to plague the market" (Ponemon Institute LLC, 2016) [98].

New cloud computing models need to prepare for and mitigate concerns regarding the risk of data breaches (Ponemon Institute LLC, 2016) [98]. It is clear that organizations using cloud computing as a service infrastructure need to examine the security and confidentiality issues for their business and sensitive applications. There are numerous security concerns for cloud computing, including privileged access, regulatory compliance, data location, data segregation, and encryption availability, including encryption design and testing (Brodkin, 2008) [43]. It is also important to be aware of recovery options, such as what happens to data in times of disaster and how it can be can be restored (Serrao, Aguilera Diaz, Cerullo, 2010) [45].

Security concerns also include investigative support, such as the ability to investigate inappropriate or illegal activity (Ramgovind et al., 2010).

Original ICS had little resemblance to traditional IT systems. However, as IP devices replace proprietary solutions, there are increased possibilities of vulnerabilities and cyber security incidents. For remote access connectivity and to promote business system connectivity ICSs are implementing the IT solutions. Operating systems, networking protocols and other industry standards start to resemble IT systems. This assimilation provides novel IT capabilities, but with ICSs no longer isolated. Due to this assimilation, ICSs need greater security (Cardenas et al., 2009 [99]; Stouffer et al., 2011) [56].

Security solutions have been developed for these types of issues in traditional IT systems. However, special precautions are required when introducing these solutions to ICS environments. It is evident that reliability and performance requirements are mostly unique for ICSs, which regularly uses unconventional applications and operating systems. IT personnel are not very familiar with these systems. Furthermore, the objectives of security and efficiency sometimes clash with other operations of ICSs (Dzung et al., 2005) [62]. Since wireless networking has increased, ICS has greater risks from those that can access the network, either through authorized access or unauthorized access. Therefore, it is noted that "threats to control systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, malicious intruders, complexities, accidents, and natural disasters as well as malicious or accidental actions by insiders" (Patel et al., 2009) [64].

Therefore, the security objectives of ICS typically consider availability, integrity, and confidentiality. Potential ICS incidents may include disruptions of ICS operations, caused by the blocked or delayed information flow through the network. In other cases, there may be some unauthorized changes like shutting down the systems, changing the priority of instructions, alarm control systems, disabling devices, etc. These could not only affect the normal operation and work flow, but may also be a danger to human lives (Cheminod et al., 2013) [67].

The ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) suggested that these attacks are advanced and persistent. In fact, ICSï£¡CERT has issued alerts for multiple campaigns over the last year (Lennon, 2015) [77].

From the literature review it was determined that most of the current studies present pure technological solutions for securing the industrial control system by considering separate attacks. Hence after conducting a detailed literature review, it was observed that there is room to propose solid recommendations for securing the oil industry in GCC countries.

The quality assessment tool for this study was developed from an instrument created by Downs and Black (1998) [97]for systematic analyses. The purpose of this tool is to ensure that the articles are of acceptable quality in order to be considered for inclusion in the study. The model is based on a 0, 1 scale, where 0 = no or unknown and 1 = yes. Each study will be assessed based on the modified assessment tool established by this researcher. The modification is done to account for study aims, objectives, research questions, and hypotheses. Table Table 4.9 shows the questions used for the data quality assessment:

Table 4.9: Quality Assessment Tool

S.No.	**Quality Assessment**
Q.1	The hypothesis/aim/objective of the study/article is clearly described.
Q.2	In the case of a scholarly article, the main outcomes to be measured are clearly explained in the introduction or methods section. In the case of a governmental database/well-known reliable magazine, the main outcomes (such as the thesis statement) are clearly explained in the introduction or conclusion.
Q.3	In the case of a scholarly article, the characteristics of the participants are described. In the case of a governmental database/well-known reliable magazine, the country or region being analyzed is identified clearly and some characteristics are provided.
Q.4	In the case of a scholarly article, the interventions of interest (such as protections against SCADA attacks) are clearly presented. In the case of a governmental database/well-known reliable magazine, possible solutions or previously attempted solutions are identified.
Q.5	In the case of a scholarly article, the main findings are clearly described. In the case of a governmental database/well-known reliable magazine, statistical information is offered that relates to the topic.
Q.6	The study/article has a logical flow and is clearly presented.
Q.7	In the case of a scholarly article, researcher/study bias was addressed. In the case of a governmental database/well-known reliable magazine, the author took care to consider multiple sides of the situation (such as providing statistical data regarding attacks and then presenting information as to why the attacks may have occurred).
Q.8	The data/results/interviews were reliable and valid (related to the main topic).

The quality assessment is shown in Table 4.10 . A total score of less than 3 is low quality; a total score between 4 and 6 is moderate quality; and a total score between 7 and 8 is high quality (Downs Black, 1998).

Table 4.11 shows the qualitative data analysis from the available sources like the type of attack the resource reported, damages done and precautions etc.

4.3 Proposed Guidelines:

Based upon the data collected from the available published material and its analysis, few guidelines have been proposed to the oil industry specifically or to industry in general to protect their ICS from possible cyber-attacks. These guidelines are based upon the predicted pattern of cyber-attacks available in the literature.

1. Awareness: Industry must initiate awareness programs for their employees, especially IT employees. IT employees are not ready to handle cyber-attacks.

2. Separate the data and network. It is suggested that systems having organizational/important data be isolated from the network.

3. Various licensed and updated software are needed to keep the malwares away.

4. There should be no disruption in critical services and resources like electricity and Internet access etc.

5. Remote access should be minimized.

6. Proactive and scheduled screening of the software and hardware must be ensured.

7. Separate the Information Technology and Operation Technology people and procedures.

8. Hacking prevention programs must be started/enhanced.

9. Mobile and cellular networks must be monitored.

10. Personal gadgets are suggested to be banned in these sensitive organizations in order to protect them from intentional or accidental attack. Personal gadgets are more vulnerable and can also be used by selfish employees to launch internal attacks. However an organization may allow their employees to use their devices as per BYOD(Bring Your Own Device) policies/technologies.

11. Use of external network access and third-party software must be minimized and controlled.

12. Enforcement of standardizations and regulations must be ensured.

13. Isolate the vulnerable systems immediately.

14. Upgrade the systems regularly.

15. Deploy application white-listing, secure configuration, vulnerability management and UB lockdown, etc.

16. Secure hardware platforms including TPM and secure open source and genuine software should be used.

17. Standards-secure communications protocols and encryptions techniques must be used in transactions and data storage.

18. Awareness needs to be improved regarding the potential for social media attacks.

19. Avoid the use of social media for official purposes and in the office for personal use ars well.

20. Obsolete and old systems must be replaced with new and secure systems.

21. Regular training and capacity building programs should be initiated.

22. Knowledge building and trust development programs should be started.

Table 4.10: Completed Quality Assessment

Source	**Q1**	**Q2**	**Q3**	**Q4**	**Q5**	**Q6**	**Q7**	**Q8**	**Total**
(Al-Humaidan, 2013 [71])	1	0	1	1	0	1	0	1	5
(Amin et al., 2013a [100])	1	1	1	1	1	1	1	0	7
(Amin et al., 2010 [101])	0	0	1	0	1	1	1	1	5
(Amin et al., 2013b [102])	0	1	0	1	1	1	0	1	5
(R. Anderson, 2015 [103])	0	0	1	1	1	1	1	0	5
(Ross Anderson&Fuloria,2010 [104])	1	0	1	1	1	1	1	1	7
(Aronson, 1996 [10])	1	0	1	0	1	1	0	1	5
(Ashrafi et al., 2007 [105])	1	0	0	0	1	1	1	1	5
(Birdwell & Mills, 2011 [106])	1	1	0	1	1	0	0	1	5
(Christopher Bronk &Tikk-Ringas,2013 [107])	1	1	0	1	1	1	1	0	6
(Chris Bronk&Tikk-Ringas,2013 [108])	0	0	1	0	1	1	1	1	5
(Byres & Lowe, 2004 [2])	0	0	1	1	1	1	0	1	5
(Cai et al., 2008 [87])	1	1	0	1	1	1	1	1	7
(Alvaro A.CÃąrdenas etal.,2011 [109])	1	0	1	1	1	1	0	0	5
(Cherrayil, 2016 [110])	1	0	0	0	1	1	1	1	5
(Constantin, 2014 [111])	0	1	1	1	0	1	1	1	6
(Creery & Byres, 2005 [5])	0	1	1	1	0	1	1	0	5
(DeSouza, 2016 [112])	0	0	0	1	1	1	1	1	5
(Fernandez & Fernandez,2005 [113])	0	0	0	1	1	1	1	1	5
(Futoransky et al., 2009 [114])	1	1	1	0	0	0	1	1	5
(Gaskell, 2015 [115])	1	0	0	0	1	1	1	1	5
(Genge et al., 2014 [116])	0	0	1	0	1	1	1	1	5
(Goldman, 2016 [117])	1	1	1	1	0	0	1	0	5
(Hahn et al., 2010 [88])	0	0	1	1	1	1	1	0	5
(Hasbini, 2014 [118])	1	1	0	0	0	1	1	1	5
(Hong & Lee, 2010 [119])	1	0	0	0	1	1	1	1	5
(Janicke & Jones, 2013 [120])	1	0	0	1	1	0	1	1	5

Source	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Total
(Jensen, 2009 [121])	1	0	1	0	0	1	1	1	5
(Kang et al., 2009 [122])	1	0	1	0	1	1	1	1	6
(Kaufman, 2009 [1])	0	1	1	1	0	1	1	0	5
(Kovacs, 2014 [123])	1	1	1	1	1	0	0	0	5
(Lim et al., 2010 [124])	1	0	0	1	1	0	1	1	5
(Liu et al., 2012 [61])	1	1	1	1	0	0	1	1	6
(Mahoney, 2006 [125])	0	0	1	1	1	1	1	1	6
(Matthew, 2015 [126])	1	1	0	0	1	0	1	1	5
(McQueen et al., 2006 [127])	1	1	1	0	1	1	1	0	6
(Miller & Rowe, 2012 [128])	1	1	1	1	0	0	1	1	6
(Ministry of Communications and Information Technology, 2016 [129])	1	1	0	1	1	1	0	1	6
(Nagraj, 2014 [130])	0	1	1	0	1	1	1	0	5
(Offshore Energy Today, 2015 [131])	0	0	0	1	1	1	1	1	5
(Okhravi et al., 2011 [132])	0	1	1	0	1	1	1	0	5
(Patel et al., 2009 [64])	1	0	1	1	1	0	1	0	5
(Queiroz et al., 2011 [133])	1	1	1	0	1	0	1	1	6
(Radmand et al., 2010 [69])	1	1	0	1	0	1	0	1	5
(Roy et al., 2010 [134])	1	1	1	1	1	1	0	0	6
(Salim, 2014 [11])	0	1	1	0	1	1	1	0	5
(Sentryo, 2016 [23])	1	1	0	1	1	0	1	1	6
(Sridhar & Manimaran,2010 [135])	1	0	1	0	1	1	1	1	6
(Teixeira, Amin, et al., 2010 [136])	0	0	0	1	1	1	1	1	5
(Teixeira, Sandberg,&Johansson,2010 [137])	1	0	1	1	0	0	1	1	5
(Ten et al., 2007 [138])	1	1	1	0	1	0	1	0	5
(Ten et al., 2008 [139])	1	1	0	0	1	0	1	1	5
(Times News Service, 2015 [140])	1	1	1	1	0	1	1	0	6
(Trahan, 2016 [70])	0	0	1	1	1	1	1	0	5
(Tripwire Inc., 2016 [141])	1	0	1	1	0	0	1	1	5

Source	**Q1**	**Q2**	**Q3**	**Q4**	**Q5**	**Q6**	**Q7**	**Q8**	**Total**
(Vatis, 2001 [142])	1	1	1	1	0	0	1	1	6
(Vijayan, 2016 [143])	1	0	0	1	1	1	1	1	6
(Walker, 2014 [144])	1	0	1	0	1	1	1	1	6
(Waqas, 2013 [145])	1	1	1	0	1	0	1	0	5
(Weaver et al., 2003 [146])	1	1	0	1	0	0	1	1	5
(Wei et al., 2011 [147])	1	1	1	0	0	0	1	1	5
(Yan et al., 2011 [148])	0	1	1	0	0	1	1	1	5
(Yang et al., 2012 [])	0	1	1	1	0	0	1	1	5
(Zhu et al., 2011 [9])	1	1	1	1	0	1	1	0	6

Table 4.11: Qualitative Analysis

Themes from the available sources	**Data**
Influence to cyber security (Cherrayil, 2016 [110]; Nagraj, 2014 [130]) (Ministry of Communications and Information Technology, 2016 [129]) (DeSouza, 2016 [112])(Matthew, 2015 [126]) (Trahan, 2016 [70])(Offshore Energy Today, 2015 [131]) (Miller & Rowe, 2012 [128])(Teixeira, Sandberg, et al., 2010 [136])(Ashrafi et al., 2007 [105])(Ross Anderson & Fuloria, 2010 [104]) (Creery & Byres, 2005 [5])	Threats by terrorist organizations Currency disagreements Large scale threats Civil/economic/political changes/events IT not adequately prepared for attacks Goal is to control oil/energy industry Impacts national strategy/economy 2014 - 41 % attacks Disruption can impact service and cause significant harm Lack of awareness and training Increased remote work Not updating known vulnerable systems Lack of separation between data networks
Guidelines to prevention of attacks (Ministry of Communications and Information Technology, 2016 [129])(Waqas, 2013 [145])(DeSouza, 2016 [112])(Sridhar & Manimaran, 2010 [135])(Okhravi et al., 2011 [132])(Zhu et al., 2011 [9])(Christopher Bronk & Tikk-Ringas, 2013 [107])(Jensen, 2009 [121])	Malware detection activities Proactive screening Increase security for critical infrastructure and sensitive data Separate IT and OT networks Increase funding for hacking preventions Expected to be $ 1.9bn by 2018
Trends of cyber attacks (Cherrayil, 2016 [110])(Ministry of Communications and Information Technology, 2016 [129]) (Hasbini, 2014 [118])(Waqas, 2013 [145])(R. Anderson, 2015 [107])(DeSouza, 2016 [112])(Trahan, 2016 [70])(Offshore Energy Today, 2015 [131])(Yang et al., 2012 [149])(Chris Bronk & Tikk-Ringas, 2013 [107])(Futoransky et al., 2009 [114])(Vatis, 2001 [142])(Radmand et al., 2010 [69])(Fernandez & Fernandez, 2005 [113])	Caused by mobile technology/IT infrastructure Precipitated by malware Impact national security Impact national income Target key sectors 88% increase in UAE attacks in 2013 1,419 in 2013; 792 in 2012; 588 in 2011 Caused by internet 92% of UAE online 65% of attacks in government, energy, finance Typically, only hacking Increase in UAE attacks Hijack corporation networks Trojans commonly used Can cause power/heating outages Leads to equipment damage Most common attacks are spear-phishing tactics More difficult to detect attacks

Themes from the available sources	**Data**
Likelihood of attacks (Cherrayil, 2016 [110])(R. Anderson, 2015 [107])(DeSouza, 2016 [112])(Sentryo, 2016 [23])(Vijayan, 2016 [143])(Tripwire Inc., 2016 [141])(Janicke & Jones, 2013 [120])(Amin et al., 2013a [100])(Birdwell & Mills, 2011 [106])(Mahoney, 2006 [125])(Weaver et al., 2003 [146])(Alvaro A. CÃąrdenas et al., 2011 [109])	Accounts for half of all GCC attacks More attacks as infrastructure increases Target small companies/individuals Popular use of Ransomware More than 82% of oil/gas companies targeted Unknown how many attacks target ICS Increase in successful attacks
Protection of SCADA/industrial controls (Ministry of Communications and Information Technology, 2016 [129])(DeSouza, 2016 [112])(Trahan, 2016 [70])(Lim et al., 2010 [124])(Hahn et al., 2010 [88])(Kang et al., 2009 [122])(McQueen et al., 2006 [127])(Ten et al., 2007 [138])(Ten et al., 2008 [139])(Amin et al., 2010 [101])(Amin et al., 2013b [102])(Liu et al., 2012 [61])(Wei et al., 2011 [147])(Yan et al., 2011 [148])	Increase data security Criminals modify/destroy data Use of separate networks decreases risk Current minimal enforcement of regulations ANS/ISA-62443-3-2 - focuses on network segmentation OT and IT need to work together to prevent attacks Isolate vulnerable systems Upgrade systems Use anti-malware Deploy application whitelisting Deploy secure configuration Deploy vulnerability management USB lockdown
Havex RAT/BlackEnergy attacks (Constantin, 2014 [111])(Walker, 2014 [144])(Kovacs, 2014 [123])(Patel et al., 2009 [64])(Genge et al., 2014 [116])(Creery & Byres, 2005 [5])(Cai et al., 2008 [57])	Originally used against companies Now Havex used against SCADA RAT is Trojan for hacking Uses multiple distribution, such as e-mail Target SCADA and ICS Used for industrial espionage Commonly used by Russian groups Focuses on exploit kits Focuses on existing vulnerabilities

Themes from the available sources	Data
Prediction of future attacks (Cherrayil, 2016 [110]) (Hasbini, 2014 [118])(Waqas, 2013 [145])(R. Anderson, 2015 [107])(Gaskell, 2015 [91])(Goldman, 2016 [117])(Times News Service, 2015 [140])(Al-Humaidan, 2013 [71])(Teixeira, Amin, et al., 2010 [137])(Hong & Lee, 2010 [119])(Roy et al., 2010 [8])(Queiroz et al., 2011 [133])	Currently: 25% UAE, 10% SA/K; 5% O/Q Control/measuring devices lack security and encryption Vulnerable due to information flow protocol and insufficient information flow Exchange of sensitive information can trigger attacks Emphasis on emerging markets Bahrain especially vulnerable due to social media High delay between attack and discovery Increasing mobility increases risk Social media platforms commonly manipulated for attacks/hacking Outdated SCADA systems Confidence in detection is 31GCC face extremely high risk of attacks Over 65% of IT experts think GCC attack is imminent

Chapter 5

Conclusions

The final chapter includes the implications and conclusions to the study.

5.1 Implications

National power can be derived through cyber attacks because it enhances coercion, influence, and warfare (Lewis, 2014) [92]. However, cyber attacks are not new. As an intelligence tool, cyber technology was originally used in the 1980s. As a warfare tool, cyber attacks were used in the 1990s (Lewis, 2014) [92]. Within the Gulf States, a significant instrument of national power is the use of cyber tools and techniques. It is noted that "the Gulf has become a flashpoint for cyber conflict given the high level of activity and the chance for miscalculation and escalation into conventional conflict. The Gulf is unique in that the use of cyber techniques by governments for covert action is much more prevalent than in any region other than the Korean peninsula" (Lewis, 2014) [92]. Due to the strategic and economic significance of the Persian Gulf, cyber attacks on oil production or physical conflicts could result in global consequences, especially as the use of cyber warfare can result in a shift in the military power balance among the regional states resulting in changes to the Gulf's stability, particularly if GCC states do not increase their defenses to this threat. These defenses have been pre-empted by three incidents. The first was social media impacts and the Internet in Arab uprisings that occurred in 2011, as well as the Green Revolution in Iran in 2009. The second was the 2010 Stuxnet attacks against nuclear facilities in Iranian. Finally, the 2012 attacks on Saudi Aramco and Qatari RasGas prompted political leaders to consider cyber security issues (Lewis, 2014) [92].

5.2 Conclusions and Future Directions

This research highlighted the importance for cyber security of the personnel involved in the ICSs. Context is provided by contemporary studies from various ICS failures. Data have been collected from IT employees, and detailed analyses have been presented. Solid recommendations have been proposed for industries to safeguard their ICSs. The researchers believe that exploiting these recommendations will help organizations to protect their ICS from various types of cyberattacks.

Further this dissertation proposed a set of guidelines for the oil industry in GCC countries to make their ICS more secure. After a detailed literature survey, the researcher perceived a set of patterns based on the historical data of security breaches.

Based upon these patterns, a set of guidelines has been proposed for safeguarding the all-important oil industry of GCC countries for continuous, uninterrupted, and risk-free production of oil to the world. By adopting these guidelines, industries can safeguard their ICSs.

The output of the thesis is two research publications and the third paper will present complete research along with a framework for monitoring the cyber security issues in the oil industry of GCC countries. The technological aspects can be coupled with the work proposed in this thesis; this might be a good future direction for the oil industry of GCC countries.

References

[1] L. M. Kaufman, “Data security in the world of cloud computing.” *IEEE Security Privacy Magazine,*, vol. 7(4), p. 61âĂŞ64, 2009. [Online]. Available: http://doi.org/10.1109/MSP.2009.87

[2] . L. J. Byres, E., “The myths and facts behind cyber security risks for industrial control systems.” *In Proceedings of the VDE Kongress*, p. 213âĂŞ218, 2004.

[3] W. T. Organization., “Gulf cooperation council (gcc) countries,” 2016. [Online]. Available: www.wto.aoyama.ac.jp/file/wp-e06-khadija.pdf

[4] G. in the News., “Basic facts about oil and gas in the arab world | arabia, the gulf, and the gcc blog.” 2013. [Online]. Available: http://ncusar.org/blog/2013/03/basic-facts-about-oil-and-gas-in-the-arab-world/

[5] . B. E. J. Creery, A., “Industrial cybersecurity for power system and scada networks,” *In Record of Conference Papers Industry Applications Society 52nd Annual Petroleum and Chemical Industry Conference*, p. 303âĂŞ309, 2005. [Online]. Available: http://doi.org/10.1109/PCICON.2005.1524567

[6] L. S. A. . W. R. D. Igure, V. M., “Security issues in scada networks. computers security„” vol. 25(7), p. 498âĂŞ506, 2006. [Online]. Available: http://doi.org/10.1016/j.cose.2006.03.001

[7] V. R. . D. Y. S. Morris, T., “A testbed for scada control system cybersecurity research and pedagogy,” *In Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research - CSIIRW âĂŹ11*, p. 1, 2011. [Online]. Available: NewYork,NewYork,USA:ACMPress.http://doi.org/10.1145/2179298.2179327

[8] G. J. H. . H. J. L. Ralston, P. A. S., “Cyber security risk assessment for scada and dcs networks.” *ISA Transactions, 46(4)*, p. 583âĂŞ94, 2007. [Online]. Available: http://doi.org/10.1016/j.isatra.2007.04.003

[9] J. A. . S. S. Zhu, B., “A taxonomy of cyber attacks on scada systems.” *In 2011 International Conference on Human Factor and 4th International Conference on Cyber, Physical and Social Computing*, p. 380âĂŞ388, 2011. [Online]. Available: IEEE.http://doi.org/10.1109/iThings/CPSCom.2011.34

[10] D. Aronson, “Overview of systems thinking. retrieved from,” 1996. [Online]. Available: www.thinking.net/Systems_Thinking/OverviewSTarticle.pdf

[11] H. M. Salim, “Cyber safetyâĂŕ: a systems thinking and systems theory approach to managing cyber security risks. massachusetts institute of technology,” 2014. [Online]. Available: Retrievedfromhttp://dspace.mit.edu/handle/1721.1/90804

[12] . C. M. E. Dutta, S., “Ict challenges for the arab world. the global information technology report,” p. 116âĂŞ131, 2002.

[13] K. C. Ulrichsen, "Gulf security: changing internal and external dynamics. london school of economics and political science." 2009. [Online]. Available: http://eprints.lse.ac.uk/25237/1/Ulrichsen_2009.pdf

[14] J. J. B. D. . A. G.-J. Takabi, H., "Security and privacy challenges in cloud computing environments," *IEEE Security Privacy Magazine, 8(6)*, p. 24âĂŞ31, 2010. [Online]. Available: http://doi.org/10.1109/MSP.2010.186

[15] C. R. L. P. N. H.-N. A. P. W. . S. J. Hathaway, O. A., "The law of cyber-attack. california law review,," *The Law of Cyber-Attack. California Law Review*, p. 817âĂŞ885, 2012. [Online]. Available: http://www.jstor.org/stable/23249823?seq=1#page_scan_tab_contents

[16] . F. R. Gordon, S., "On the definition and classification of cybercrime." *Journal in Computer Virology*, vol. 2(1), pp. 13–20, 2006. [Online]. Available: http://doi.org/10.1007/s11416-006-0015-z

[17] . v. N. J. von Solms, R., "From information security to cyber security. computers security, 38,," p. 97âĂŞ102, 2013. [Online]. Available: http://doi.org/10.1016/j.cose.2013.04.004

[18] I. J. Faulkner, "Introduction to session on the application of digital computers in industrial control." *Proceedings of the IEE - Part B: Radio and Electronic Engineering,*, vol. 103(1S), p. 98âĂŞ99, 1956. [Online]. Available: http://doi.org/10.1049/pi-b-1.1956.0019

[19] J. D. McDonald, "Developing and defining basic scada system concepts," *In [Proceedings] 1993 Rural Electric Power Conference. Papers Presented*

at the 37th Annual Conference, pp. 1B3/1–B3/5, 1993. [Online]. Available: http://doi.org/10.1109/REPCON.1993.239563

[20] . K. V. Subashini, S., "A survey on security issues in service delivery models of cloud computing." *Journal of Network and Computer Applications, 34(1)*, p. 1âĂŞ11, 2011.

[21] . H. A. Perrons, R. K., "loud computing in the upstream oil gas industry: A proposed way forward." *Energy Policy, 56(56),*, p. 732âĂŞ737, 2013. [Online]. Available: http://doi.org/10.1016/j.enpol.2013.01.016

[22] G. D. . S. I. Khajeh-Hosseini, A., "Cloud migration: A case study of migrating an enterprise it system to iaas." *In 2010 IEEE 3rd International Conference on Cloud Computing*, p. 450âĂŞ457, 2010. [Online]. Available: http://doi.org/10.1109/CLOUD.2010.37

[23] . B. C. Seifarth, R., "Cloud technology boosts oil and gas operations. sentryo. (2016)." *he Oil and Gas Industry - The Primary Target of Cyberattacks.*, 2013. [Online]. Available: Retrievedfromhttps://www.sentryo.net/oil-and-gas-industry-primary-target-of-cyberattacks/

[24] U. S. C. E. C. P. A. of 1986, 1986. [Online]. Available: UnitedStates.Retrievedfromhttps://it.ojp.gov/privacyliberty/authorities/statutes/1285

[25] O. . G. Council.., "Cloud computing in oil and gas." 2016.

[26] D. Info., "Why cloud computing is the future of oil gas software." 2012. [Online]. Available: http://info.drillinginfo.com/why-cloud-computing-is-the-future-of-oil-gas-software/

[27] LandPoint., "How cloud computing is revolutionizing the oil and gas industry." 2015. [Online]. Available: http://www.landpoint.net/how-cloud-computing-is-revolutionizing-the-oil-and-gas-industry/

[28] M. Bennett, *Cloud Computing for Oil and Gas Companies. Retrieved from*, 2013. [Online]. Available: http://www.oilgasmonitor.com/cloud-computing-oil-gas-companies/

[29] . G. T. Mell, P., "The nist definition of cloud computing." 2011.

[30] K. Y. . F. H. Takahashi, T., "Ontological approach toward cybersecurity in cloud computing," *In Proceedings of the 3rd international conference on Security of information and networks - SIN âĂŹ10*, p. 100, 2010. [Online]. Available: http://doi.org/10.1145/1854099.1854121

[31] F. Gens, "IdcâĂŹs new it cloud services forecast: 2009-2013," *IDC Report, 5*, 2009.

[32] "Distributed management task force inc." *Interoperabile Clouds - A White Paper from the Open Cloud Standards Incubator.*, 2009.

[33] T. Metsch, "Open cloud computing interface-use cases and requirements for a cloud api," *Open Grid Forum.*, 2009.

[34] S. N. I. Association., "Cloud data management interface," 2010.

[35] C. S. Alliance., "Security guidance for critical areas of focus in cloud computing." *Cloud Security Alliance*, vol. 2(1), 2011.

[36] R. P. V. . R. A. Kandukuri, B. R., “Cloud security issues.” *In 2009 IEEE International Conference on Services Computing*, p. 517âĂŞ520, 2009. [Online]. Available: http://doi.org/10.1109/SCC.2009.84

[37] . B. A. Archer, J., “Security guidance for critical areas of focus in cloud computing,” *Cloud Security Alliance*, vol. 2, p. 1âĂŞ76, 2009. [Online]. Available: US.http://doi.org/10.1007/978-1-4419-6967-5_4

[38] . M. R. Brunette, G., “Security guidance for critical areas of focus in cloud computing.” *Cloud Security Alliance,*, vol. 2(1), p. 1âĂŞ76, 2009.

[39] V. Choudhary, “Software as a service: Implications for investment in software development.” *In 2007 40th Annual Hawaii International Conference on System Sciences (HICSSâĂŹ07)*, p. 5209aâĂŞ209a, 2007. [Online]. Available: http://doi.org/10.1109/HICSS.2007.493

[40] A. Bamrara, “Evaluating database security and cyber attacks: A relational approach,” *Journal of Internet Banking Commerce*, vol. 20(2), p. 1âĂŞ8, 2015. [Online]. Available: http://doi.org/10.1016/j.comnet.2010.05.010

[41] M. Dunn Cavelty, “Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. science engineering ethics,” vol. 20(3), p. 701âĂŞ715, 2014. [Online]. Available: http://doi.org/10.1007/s11948-014-9551-y

[42] E. M. M. . S. E. Ramgovind, S., “The management of security in cloud computing,” *In 2010 Information Security for South Africa*, p. 1âĂŞ7, 2010. [Online]. Available: IEEE.http://doi.org/10.1109/ISSA.2010.5588290

[43] J. Brodkin, “Gartner: Seven cloud-computing security risks,” *InfoWorld*, p. 1âĂŞ3, 2008.

[44] L. Sumter, “Cloud computing,” *In Proceedings of the 48th Annual Southeast Regional Conference on - ACM SE âĂŹ10*, p. 1, 2010. [Online]. Available: NewYork,NewYork,USA:ACMPress.http://doi.org/10.1145/1900008.1900152

[45] A. D. V. . C. F. E. SerrÃčo, C., “Web application security (vol. 72),” *Berlin, Heidelberg: Springer Berlin Heidelberg.*, 2010. [Online]. Available: http://doi.org/10.1007/978-3-642-16120-9

[46] F. Sabahi, “Cloud computing security threats and responses.” *In 2011 IEEE 3rd International Conference on Communication Software and Networks*, p. 245âĂŞ249, 2011. [Online]. Available: IEEE.http://doi.org/10.1109/ICCSN.2011.6014715

[47] . C. S. Curran, K., “Pervasive and ubiquitous technology innovations for ambient intelligence environments. igi global.” 2012).

[48] . H. S. Shaikh, F. B., “Security threats in cloud computing.” *In Internet technology and secured transactions (ICITST), 2011 international conference*, p. 214âĂŞ219, 2011. [Online]. Available: IEEE

[49] . E. A. Fenz, S., “Formalizing information security knowledge.” *In Proceedings of the 4th International Symposium on Information, Computer, and Communications Security - ASIACCS âĂŹ09*, p. 183, 2009. [Online]. Available: http://doi.org/10.1145/1533057.1533084

[50] . G. M. Wang, J. A., “Security data mining in an ontology for vulnerability management.” *In 2009 International Joint Conference on Bioinformatics, Systems Biology and Intelligent Computing*, p. 597âĂŞ603, 2009b. [Online]. Available: http://doi.org/10.1109/IJCBS.2009.13

[51] D. S. . G. D. Tsoumas, B., “An ontology-based approach to information systems security management.” 2005. [Online]. Available: http://doi.org/10.1007/11560326_12

[52] . G. D. Tsoumas, B., “Towards an ontology-based security management,” *In 20th International Conference on Advanced Information Networking and Applications - Volume 1 (AINAâĂŹ06)*, p. 985âĂŞ992, 2006. [Online]. Available: http://doi.org/10.1109/AINA.2006.329

[53] v. M. A. . C. R. Parkin, S. E., “An information security ontology incorporating human-behavioural implications.” *In Proceedings of the 2nd international conference on Security of information and networks - SIN âĂŹ09*, p. 46, 2009. [Online]. Available: http://doi.org/10.1145/1626195.1626209

[54] K. L. . F. T. Denker, G., “Security in the semantic web using owl. information security technical report,” vol. 10(1), p. 51âĂŞ58, 2005. [Online]. Available: http://doi.org/10.1016/j.istr.2004.11.002

[55] L. J. V.-G. R. F. E.-T. A. . P. M. Blanco, C., “A systematic review and comparison of security ontologies.” *Third International Conference on Availability, Reliability and Security*, p. 813âĂŞ820, 2008. [Online]. Available: http://doi.org/10.1109/ARES.2008.33

[56] F. J. . S. K. Stouffer, K., “Guide to industrial control systems (ics) security.” *NIST Special Publication, 800(82)*, p. 16âĂŞ16, 2011.

[57] A. S. . S. S. CÃąrdenas, A. A., “Research challenges for the security of control systems.” *HotSeo.*, 2008.

[58] G. N. Ericsson, “Cyber security and power system communicationâĂŤessential parts of a smart grid infrastructure,” *IEEE Transactions on Power Delivery*, vol. 25(3), p. 1501âĂŞ1507, 2010. [Online]. Available: http://doi.org/10.1109/TPWRD.2010.2046654

[59] B. K. D. D. P.-A. . S. B. Kim, T. H.-J., “CyberâĂŞphysical security of a smart grid infrastructure.” *Proceedings of the IEEE,*, vol. 100(1), p. 195âĂŞ209, 2012. [Online]. Available: http://doi.org/10.1109/JPROC.2011.2161428

[60] . F. M. Kuipers, D., “Control systems cyber security: Defense in depth strategies. department of energy.” 2006.

[61] X. Y. L. S. L. W. . C. C. L. P. Liu, J., “Cyber security and privacy issues in smart grids,” *IEEE Communications Surveys Tutorials,*, vol. 14(4), p. 981âĂŞ997., 2012. [Online]. Available: http://doi.org/10.1109/SURV.2011.122111.00145

[62] N. M. V. H. T. P. . C. M. Dzung, D., “Security for industrial communication systems.” *Proceedings of the IEEE*, vol. 93(6), p. 1152âĂŞ1177, 2005. [Online]. Available: http://doi.org/10.1109/JPROC.2005.849714

[63] J. C. X. F. D. Z. X. Q. . G. Y. Peng, Y., “Industrial control system cybersecurity research,” *Journal of Tsinghua University Science and Technology, 52(10)*, p. 1396âĂŞ1408, 2012.

[64] B. G. D. . G. J. H. Patel, S. C., “Improving the cyber security of scada communication networks.” *Communications of the ACM, 52(7)*, p. 139, 2009. [Online]. Available: http://doi.org/10.1145/1538788.1538820

[65] . S. T. Felser, M., “Standardization of industrial ethernet - the next battlefield?” *In IEEE International Workshop on Factory Communication Systems, 2004. Proceedings*, p. 1413âĂŞ420, 2004. [Online]. Available: IEEE.http://doi.org/10.1109/WFCS.2004.1377762

[66] D. A. Shea, “Critical infrastructure: Control systems and the terrorist threat.” 2004.

[67] D. L. . V. A. Cheminod, M., “Review of security issues in industrial networks.” *IEEE Transactions on Industrial Informatics,*, p. 277âĂŞ293, 2013. [Online]. Available: http://doi.org/10.1109/TII.2012.2198666

[68] D. Geer, “Security of critical control systems sparks concern. computer,” vol. 39(1), pp. 20–23, 2006. [Online]. Available: http://doi.org/10.1109/MC.2006.32

[69] T. A. P. S. . C. S. Radmand, P., “Taxonomy of wireless sensor network cyber security attacks in the oil and gas industries,” *In 2010 24th IEEE International Conference on Advanced Information Networking and Applications*, p. 949âĂŞ957, 2010. [Online]. Available: http://doi.org/10.1109/AINA.2010.175

[70] K. Trahan, "Industrial control systems: Next frontier for cyber attacks?" 2016. [Online]. Available: http://www.tripwire.com/state-of-security/featured/ics-next-frontier-for-cyber-attacks/

[71] R. Al-Humaidan, "Gcc prone to cyber attack, say it experts," *American Petroleum Institute. (2004). API Standard 1164 - SCADA Security*, 2013. [Online]. Available: http://www.arabnews.com/news/457183

[72] B. S. Institute, "Bsi 7799 information security," 1995.

[73] B. Fraser, "Rcf 2196 - site security handbook." 1997.

[74] "International organization for standardization and the international electrotechnical commission," *ISO/IEC 17799, Code of Practice for Information Security Management.*, 2000.

[75] "Instrumentation systems and automation society," *ISA-TR99.00.01-2004, Security Technologies for Manufacturing and Control Systems.*, 2004a.

[76] "Instrumentation systems and automation society," *ISA-TR99.00.02-2004, Security Technologies for Manufacturing and Control Systems.*, 2004b.

[77] M. Lennon, "Attacks against scada systems doubled in 2014: Dell." 2015. [Online]. Available: http://www.securityweek.com/attacks-against-scada-systems-doubled-2014-dell

[78] M. Hentea, "Improving security for scada control systems." *Interdisciplinary Journal of Information, Knowledge and Management,*, vol. 3, p. 73, 2008.

[79] . F. M. Byres, E., “Finding the security holes before the hackers do vulnerability discovery in industrial control systems.” *In ISA Technical Conference, Instrumentation Systems and Automation Society.*, 2005.

[80] H. D. . K. N. Byres, E., “On shaky ground âĂŞ a study of security vulnerabilities in control protocols.” *American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human Machine Interface Technology, American Nuclear Society.*, vol. 5, 2006.

[81] . A. K.-E. Sanz, R., “Trends in software and control,” *IEEE Control Systems Magazine, 23(3)*, p. 12âĂŞ15, 2003. [Online]. Available: http://doi.org/10.1109/MCS.2003.1200238

[82] R. Dacey, “Information security: Progress made, but challenges remain to protect federal systems and the nationâĂŹs critical infrastructures.” 2003.

[83] P. R.-S. K. . C. E. F. Pasik-Duncan, B., “Four focused forums.” *IEEE Control Systems Magazine, 26(4)*, p. 93âĂŞ98, 2006. [Online]. Available: http://doi.org/10.1109/MCS.2006.1657882

[84] J. Steven, “Adopting an enterprise software security framework.” *IEEE Security Privacy Magazine, 4(2)*, p. 84âĂŞ87, 2006. [Online]. Available: http://doi.org/10.1109/MSP.2006.33

[85] Z. C. L. D. S. L. M. S. . W. Z. Chao Zhang, Tao Wei, “Practical control flow integrity and randomization for binary executables,” *IEEE Symposium on Security and Privacy*, p. 559âĂŞ573, 2013. [Online]. Available: http://doi.org/10.1109/SP.2013.44

[86] O. Saydjari, “Defending cyberspace,” *Computer, 35(12)*, p. 125âĂŞ127, 2002. [Online]. Available: http://doi.org/10.1109/MC.2002.1106187

[87] W. J. . Y. X. Cai, N., “Scada system security: Complexity, history and new developments.” *6th IEEE International Conference on Industrial Informatics*, p. 569âĂŞ574, 2008. [Online]. Available: IEEE.http://doi.org/10.1109/INDIN.2008.4618165

[88] K. B. G. M. F. J. A. R. S. S. . H. M. Hahn, A., “Development of the powercyber scada security testbed,” *In Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research - CSIIRW âĂŹ10*, p. 1, 2010. [Online]. Available: http://doi.org/10.1145/1852666.1852690

[89] . L. J. T. Knapp, E. D., “Industrial network security: Securing critical infrastructure networks for smart grid, scada, and other industrial control systems. elsevier science.” 2014.

[90] E. G. N. . N. J. Sommestad, T., “Scada system cyber security âĂŤ a comparison of standards.” *In IEEE PES General Meetin*, p. 1âĂŞ8), 2010. [Online]. Available: IEEE.http://doi.org/10.1109/PES.2010.5590215

[91] F. L. . D. Y. Wang, C., “A simulation environment for scada security analysis and assessment.” *In 2010 International Conference on Measuring Technology and Mechatronics Automation Vol. 1*, p. 342âĂŞ347, 2010. [Online]. Available: IEEE.http://doi.org/10.1109/ICMTMA.2010.603

[92] J. Lewis, “Cybersecurity and stability in the gulf,” 2014).

[93] J. W. Creswell, “Research design: Qualitative, quantitative, and mixed methods approaches.” *Los Angeles: Sage Publications, Inc. Critical Values of the Chi-Square Distribution. (n.d.) BOOK*, vol. 2015 SRC), 2013.

[94] S. Sarantakos, “Social research. palgrave macmillan,” 2012. [Online]. Available: Retrievedfromhttps://books.google.com/books?hl=en&lr=&id=IjUdBQAAQBAJ&pgis=1

[95] . J. C. Reay, T., “Qualitatively capturing institutional logics,” *Strategic Organization, 1476127015589981-*, 2015. [Online]. Available: http://doi.org/10.1177/1476127015589981

[96] D. Krejcie, R.V. Morgan, “Determ ining sample size for research activities educational and psychological measurement, 30,” pp. 607–610, 1970.

[97] . B. N. Downs, S. H., “he feasibility of creating a checklist for the assessment of the methodological quality both of randomised and non-randomised studies of health care interventions.” *Journal of Epidemiology Community Health*, p. 377âĂŞ384, 1998. [Online]. Available: http://doi.org/10.1136/jech.52.6.377

[98] P. I. LLC, “Cost of data breach study: Global analysisâĂİ, benchmark research sponsored by ibm, 2015,” 2016. [Online]. Available: August1,2016fromhttps://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF

[99] A. S. S. B. G. A. P. A. . S. S. Cardenas, A., “Challenges for securing cyber physical systems,” *Workshop on Future Directions in Cyber-Physical Systems Security.*, 2009.

[100] L. X. S. S. . B. A. M. Amin, S., "Cyber security of water scada systemsâĂŤpart i: Analysis and experimentation of stealthy deception attacks," *IEEE Transactions on Control Systems Technology*, vol. 21(5), p. 1963âĂŞ1970, 2013a. [Online]. Available: http://doi.org/10.1109/TCST.2012.2211873

[101] L. X. S. S. S. . B. A. M. Amin, S., "Stealthy deception attacks on water scada systems," *In Proceedings of the 13th ACM International Conference on hybrid systems: Computation and control - HSCC*, vol. 10, p. 161, 2010. [Online]. Available: USA.http://doi.org/10.1145/1755952.1755976

[102] ——, "Cyber security of water scada systemsâĂŤpart ii: Attack detection using enhanced hydrodynamic models." *IEEE Transactions on Control Systems Technology*, vol. 21(5), p. 1679âĂŞ1693, 2013b. [Online]. Available: http://doi.org/10.1109/TCST.2012.2211874

[103] R. Anderson, "Cyber attacks targeted at uae increase âĂŞ report. retrieved from," 2015. [Online]. Available: http://gulfbusiness.com/cyber-attacks-targeted-uae-increase-report/

[104] . F. S. Anderson, R., "ecurity economics and critical national infrastructure. in economics of information security and privacy," pp. 55–66, 2010. [Online]. Available: US.http://doi.org/10.1007/978-1-4419-6967-5_4

[105] Y. M. M. C. A. J. . A. H. Y. Ashrafi, R., "E-commerce practices in the arabian gulf gcc business culture: utilisation and outcomes patterns," *International Journal of Business Information Systems*, 2007.

[106] . M. R. Birdwell, M. B., “War fighting in cyberspace: Evolving force presentation and command and control.” 2011.

[107] . T.-R. E. Bronk, C., “Hack or attack? shamoon and the evolution of cyber conflict.” *SSRN Electronic Journal.*, 2013. [Online]. Available: http://doi.org/10.2139/ssrn.2270860

[108] ——, “The cyber attack on saudi aramco. survival, 55(2),” p. 81âĂŞ96, 2013. [Online]. Available: http://doi.org/10.1080/00396338.2013.7844680

[109] A.-S. L. Z.-S. H. Y.-L. H. C.-Y. . S. S. CÃąrdenas, A. A., “Attacks against process control systems,” in *6th ACM Symposium on Information, Computer and Communications Security - ASIACCS*, vol. 11, 2011, p. 355. [Online]. Available: IEEE.http://doi.org/10.1109/INDIN.2008.4618165

[110] N. Cherrayil, “Mideast oil and gas sector faces wider cyberattacks.” 2016. [Online]. Available: http://gulfnews.com/business/sectors/technology/mideast-oil-and-gas-sector-faces-wider-cyberattacks-1.1854885

[111] L. Constantin, “New havex malware variants target industrial control system and scada users.” 2014. [Online]. Available: http://www.pcworld.com/article/2367240/new-havex-malware-variants-target-industrial-control-system-and-scada-users.html

[112] R. DeSouza, “Cyber attacks threatening oil and gas sector severely now than ever before,” 2016. [Online]. Available: https://www.hackread.com/cyber-attacks-threatening-oil-and-gas-sector/

[113] . F. A. E. Fernandez, J. D., “Scada systems: vulnerabilities and remediation.” *Journal of Computing Sciences in Colleges*, vol. 20(4), p. 160âĂŞ168, 2005.

[114] M. F. O. J. . S. C. Futoransky, A., “Simulating cyber-attacks for fun and profit,” *In Proceedings of the Second International ICST Conference on Simulation Tools and Techniques*, p. 4, 2009. [Online]. Available: http://doi.org/10.4108/ICST.SIMUTOOLS2009.5773

[115] H. Gaskell, “Uae is top-two victim of regional cyber attacks.” 2015. [Online]. Available: http://www.arabianbusiness.com/uae-is-top-two-victim-of-regional-cyber-attacks-586181.html

[116] S. C. . H. M. Genge, B., “Impact of network infrastructure parameters to the effectiveness of cyber attacks against industrial control systems.” *International Journal of Computers Communications Control,*, vol. 7(4), p. 674, 2014. [Online]. Available: http://doi.org/10.15837/ijccc.2012.4.1366

[117] J. Goldman, “53 percent of oil and gas companies report surge in cyber attacks.” 2016. [Online]. Available: http://www.esecurityplanet.com/network-security/53-percent-of-oil-and-gas-companies-report-surge-in-cyber-attacks.html

[118] M. Hasbini, “Cybercrime in dubai and uae.” 2014. [Online]. Available: https://securelist.com/blog/research/63682/the-rise-of-cybercrime-in-dubai-and-uae/

[119] . L. M. Hong, S., “Challenges and direction toward secure communication in the scada system,” *In 2010 8th Annual Communication Networks and*

Services Research Conference, p. 381âĂŞ386, 2010. [Online]. Available: http://doi.org/10.1109/CNSR.2010.52

[120] . J. K. Janicke, H., "1st international symposium for ics amp; scada cyber security research 2013:proceedings, leicester, uk, 16-17 september 2013.âĂŕ," *Proceedings of the 1st International Symposium on ICS SCADA Cyber Security Research 2013. BCS.*, 2013.

[121] E. T. Jensen, "Cyber warfare and precautions against the effects of attacks. texas law review, 88." 2009.

[122] L. J.-J. K. S.-J. . P. J.-H. Kang, D.-J., "Analysis on cyber threats to scada systems." *In 2009 Transmission Distribution Conference Exposition: Asia and Pacific*, p. 1âĂŞ4, 2009. [Online]. Available: http://doi.org/10.1109/TD-ASIA.2009.5357008

[123] E. Kovacs, "Attackers using havex rat against industrial control systems." 2014. [Online]. Available: http://www.securityweek.com/attackers-using-havex-rat-against-industrial-control-systems

[124] H. S.-C. M. S.-L. S. J. K.-T. W. L. S. W. . H. B. N. Lim, I. H., "Security protocols against cyber attacks in the distribution automation system." *IEEE Transactions on Power Delivery,*, p. 448âĂŞ455, 2010. [Online]. Available: http://doi.org/10.1109/TPWRD.2009.2021083

[125] W. Mahoney, "Compiler assisted tracking of hacker assaults." *International Conference on I-Warfare and Security, ICIW 2006.*, 2006.

[126] J. Matthew, “Oil industry has become hackersâĂŹ favourite because of potential to create blackouts or spills.” 2015. [Online]. Available: http://www.ibtimes.co.uk/oil-industry-has-become-hackers-favourite-because-potential-create-blackouts/

[127] B. W. F. F. M. A. . B. G. A. McQueen, M. A., “Quantitative cyber risk reduction estimation methodology for a small scada control system.” *In Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSSâĂŹ06)*, p. 226âĂŞ226, 2006. [Online]. Available: http://doi.org/10.1109/HICSS.2006.405

[128] . R. D. Miller, B., “A survey scada of and critical infrastructure incidents,” *In Proceedings of the 1st Annual conference on Research in information technology - RIIT âĂŹ12*, p. 51, 2012. [Online]. Available: http://doi.org/10.1145/2380790.2380805

[129] B. W. F. F. M. A. . B. G. A. McQueen, M. A., “Ministry of communications and information technology.” *Recent study reveals increasing cyber attacks in GCC States.*, 2016. [Online]. Available: http://www.mcit.gov.sa/En/InformationTechnology/Pages/InformationSecurity/Tech-Security19062016_474.aspx

[130] A. Nagraj, “Hackers warn of cyber attacks on oil companies in saudi, uae, qatar.” 2014. [Online]. Available: http://gulfbusiness.com/hackers-warn-cyber-attacks-oil-companies-saudi-uae-qatar

[131] O. E. Today., “Top 10 cyber security threats for oil and gas industry.” 2015. [Online]. Available: http://www.offshoreenergytoday.com/top-10-cyber-security-threats-for-oil-and-gas-industry/

[132] C. A. R. E. Y. S. M. P. . H. J. Okhravi, H., “Creating a cyber moving target for critical infrastructure applications.” *In IFIP Advances in Information and Communication Technology*, p. 107âĂŞ123, 2011. [Online]. Available: SpringerBerlinHeidelberg.http://doi.org/10.1007/978-3-642-24864-1_8

[133] M. A. . T. Z. Queiroz, C., “ScadasimâĂŤa framework for building scada simulations,” *IEEE Transactions on Smart Grid, 2(4)*, p. 589âĂŞ597, 2011. [Online]. Available: http://doi.org/10.1109/TSG.2011.2162432

[134] K. D. S. . T. K. S. Roy, A., “Cyber security analysis using attack countermeasure trees.” *In Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research - CSIIRW âĂŹ10*, p. 1, 2010. [Online]. Available: NewYork,NewYork,USA.http://doi.org/10.1145/1852666.1852698

[135] . M. G. Sridhar, S., “Data integrity attacks and their impacts on scada control system.” *In IEEE PES General Meeting*, p. 1âĂŞ6, 2010. [Online]. Available: IEEE.http://doi.org/10.1109/PES.2010.5590115

[136] A. S. S. H. J. K. H. . S. S. S. Teixeira, A., “Cyber security analysis of state estimators in electric power systems.” *In 49th IEEE Conference on Decision and Control (CDC)*, p. 5991âĂŞ5998, 2010. [Online]. Available: http://doi.org/10.1109/CDC.2010.5717318

[137] S. H. . J. K. H. Teixeira, A., “Networked control systems under cyber attacks with applications to power networks,” *In Proceedings of the 2010 American Control Conference*, p. 3690âĂŞ3696, 2010. [Online]. Available: http://doi.org/10.1109/ACC.2010.5530638

[138] L. C.-C. . G. M. Ten, C.-W., “Vulnerability assessment of cybersecurity for scada systems using attack trees.” *In 2007 IEEE Power Engineering Society General Meeting*, p. 1âĂŞ8, 2007. [Online]. Available: http://doi.org/10.1109/PES.2007.385876

[139] L. C.-C. . M. G. Ten, C.-W., “Vulnerability assessment of cybersecurity for scada systems.” *IEEE Transactions on Power Systems, 23(4)*, p. 1836âĂŞ1846, 2008. [Online]. Available: http://doi.org/10.1109/TPWRS.2008.2002298

[140] T. N. Service., “Protect critical infrastructure against cyberattacks, gcc states urged,” 2015. [Online]. Available: http://timesofoman.com/article/66365/Business/Protect-critical-infrastructure-against-cyberattacks-GCC-states-urged

[141] T. Inc., “Tripwire study: Cyber attackers successfully targeting oil and gas industry.” 2016. [Online]. Available: https://www.tripwire.com/company/news/press-release/tripwire-study-cyber-attackers-successfully-targeting-oil-and-gas-industry/

[142] M. A. Vatis, “Cyber attacks during the war on terrorism: A predictive analysis.” 2001.

[143] J. Vijayan, "Successful attacks on oil and gas companies increasing, survey shows., year = 2016, url = http://www.darkreading.com/vulnerabilities—threats/successful-attacks-on-oil-and-gas-companies-increasing-survey-shows/d/d-id/1323933."

[144] D. Walker, "HavexâĂİ malware strikes industrial sector via watering hole attacks," 2014. [Online]. Available: http://www.scmagazine.com/havex-malware-strikes-industrial-sector-via-watering-hole-attacks/article/357875/

[145] M. Waqas, "Gcc highly vulnerable to cyber attacks âĂŞ survey," 2013. [Online]. Available: Retrievedfromhttp://www.arabiangazette.com/gcc-most-vulnerable-to-cyber-attacks-20130802/

[146] P. V. S.-S. . C. R. Weaver, N., "A taxonomy of computer worms." *In Proceedings of the 2003 ACM workshop on Rapid Malcode - WORMâĂŹ03*, p. 11, 2003. [Online]. Available: NewYork,NewYork,USA.http://doi.org/10.1145/948187.948190

[147] L. Y. J.-M. S. P. M. . R. K. Wei, D., "Protecting smart grid automation systems against cyberattacks." *IEEE Transactions on Smart Grid, 2(4)*, p. 782âĂŞ795, 2011. [Online]. Available: http://doi.org/10.1109/TSG.2011.2159999

[148] L. C.-C.-. G. M. Yan, J., "Cyber intrusion of wind farm scada system and its impact analysis." *In 2011 IEEE/PES Power Systems Conference and Exposition*, p. 1âĂŞ6, 2011. [Online]. Available: http://doi.org/10.1109/PSCE.2011.5772593

[149] P. B.-L.-T. Y. Z. Q. E. G. I. M. K. . S. S. Yang, Y., “Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in smart grid scada systems.” *In International Conference on Sustainable Power Generation and Supply (SUPERGEN 2012)*, p. 138âĂŞ138, 2012. [Online]. Available: InstitutionofEngineeringandTechnology.http://doi.org/10.1049/cp.2012.1831