

https://dspace.org/

The challenges experienced in power substation cyber-security in South Africa

Mutize, Cephas

2016
http://hdl.handle.net/10539/22504

Downloaded from a DSpace repository. https://dspace.org/

The challenges experienced in power substation

Cyber-security in South Africa.

Cephas Mutize

A research report submitted to the Faculty of Commerce, Law and Management, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Business Administration

Johannesburg, 2016

Supervisor: Antony Soicher

ABSTRACT

There has been an increase in the number of attacks on the industrial control systems (ICS) world-wide in recent years due to a number of reasons, one of which includes the standardisation of the communication system in the industry. This research focuses on the challenges that the industry is facing in making ICS cyber-secure. The intention is to use the information in assessing the initiatives that stakeholders have instituted to curb the attacks and to improve stakeholder understanding for the problem at hand and to inform government to fast track the legislation on cyber-crime and cyber-security. The qualitative data was collected through four unstructured interviews with the specialists in the industry, academics and consultants and 64 responses were received for 13 question questionnaire to the Control Systems Users and Practitioners. The main challenge was the lack of legislation to govern the guide the industry on cyber-security and the other problems will fall away with the introduction the sound legislation. It was found that a good number of organizations that are compliant to good practices are not experiencing many challenges. Considering that South Africa does not have cyber-security legislation, no cyber-security response teams and knowledge sharing in the industry, it is surprising that the responses from ICS operators shows that there is some protection from cyber-attacks and the lack of news on major incidents confirms this also. It is therefore important to have the cyber-security legislation and to comply to implement best practice to avoid losses due to cyber-attacks.

DECLARATION

I, Cephas Mutize, declare that this research report is my own work except as indicated in the references and acknowledgements. It is submitted in partial fulfilment of the requirements for the degree of Master of Business Administration at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in this or any other university.



Cephas Mutize

Signed at WITS UNIVERSITY

On the 30th day of MAY 2016

DEDICATION

I would like to dedicate this thesis to my grandmother Ravaki Rinomhota and my mother Winnet Rinomhota, without whose unwavering support this research would not have been possible.

ACKNOWLEDGEMENTS

I wish to thank:

- Antony Soicher for his professional guidance, his time and dedication in making this research a success.
- Fedile Akinsete, Jay Punwasi (MD) and Dr. Roswita Hamunyela for editorial advice.
- Interviewees for their insight: Dr. Jabu Mtsweni, Cobus Pool, Prince Manana, Gustav Engelbrecht and many others who responded to the surveys.
- Dr. Roswita Hamunyela for all the motivational talks.

The financial assistance from the Wits Business School through a bursary to pursue the MBA studies is also acknowledged.

Opinions expressed and the conclusions arrived at in this dissertation are those of the author, and are not necessarily to be attributed to the Wits Business School.

TABLE OF CONTENTS

ABSTRACT i

DECLARATION ii

DEDICATION iii

ACKNOWLEDGEMENTS iv

LIST OF TABLES viii

LIST OF FIGURES ix

CHAPTER 1. INTRODUCTION 1

1.1 PURPOSE OF THE STUDY 1
1.2 CONTEXT OF THE STUDY 1
1.3 PROBLEM STATEMENT 4
1.3.1 MAIN PROBLEM 4
1.3.2 SUB-PROBLEMS 4
1.4 SIGNIFICANCE OF THE STUDY 4
1.5 DELIMITATIONS OF THE STUDY 6
1.6 DEFINITIONS AND ABBREVIATIONS 6
1.7 ASSUMPTIONS 7

CHAPTER 2. LITERATURE REVIEW 9

2.1 INTRODUCTION 9
2.2 DEFINITION OF TERMS 9
2.3 CYBER SECURITY 10
2.3.1 INFORMATION TECHNOLOGY 10
2.3.2 OPERATIONAL TECHNOLOGY 10
2.3.3 TYPES OF CYBER-ATTACKS 10
2.3.4 ICS NETWORKING 101 11
2.3.5 CYBER-ATTACKS ON ICS 12
2.3.6 RISK IN CYBER SECURITY 16
2.3.7 THE TYPICAL ICS EQUIPMENT 17
2.3.8 STANDARDS AND SPECIFICATIONS 19
2.4 SOUTH AFRICAN CONTEXT 20
2.4.1 THE DRAFT CYBER-CRIMES AND CYBER-SECURITY BILL 20
2.4.2 AUTOMATION LEVEL 21
2.5 CHALLENGES IN ICS CYBER-SECURITY 21
2.5.1 RESEARCH QUESTION 1 25
2.6 IMPACT OF CHALLENGES 25

2.6.1 EMPLOYEE ICS CYBER-SECURITY SKILL 25
2.6.2 ORGANIZATIONAL ICS CYBER-SECURITY BEHAVIOUR 26
2.6.3 COMPLIANCE 26
2.6.4 RESEARCH QUESTION 2 26
2.7 CONCLUSION OF LITERATURE REVIEW 26
2.7.1 RESEARCH QUESTION 1: 27
2.7.1 RESEARCH QUESTION 2 27

CHAPTER 3. RESEARCH METHODOLOGY 28

3.1 INTRODUCTION 28
3.2 RESEARCH METHODOLOGY 28
3.3 RESEARCH DESIGN 29
3.4 POPULATION AND SAMPLE 29
3.4.1 POPULATION 29
3.4.2 SAMPLE AND SAMPLING METHOD 30
3.5 THE RESEARCH INSTRUMENT 31
3.6 PROCEDURE FOR DATA COLLECTION 31
3.7 DATA ANALYSIS AND INTERPRETATION 33
3.8 LIMITATIONS OF THE STUDY 35
3.9 VALIDITY AND RELIABILITY 36
3.9.1 EXTERNAL VALIDITY 36
3.9.2 INTERNAL VALIDITY 36
3.9.3 RELIABILITY 36
3.10 DEMOGRAPHIC PROFILE OF RESPONDENTS 37

CHAPTER 4. PRESENTATION OF RESULTS 38

4.1 INTRODUCTION 38
4.2 CHALLENGES EXPERIENCED IN SUBSTATION CYBER SECURITY IN SOUTH AFRICA. 38
4.3 TO WHAT EXTEND DOES THE CHALLENGES REALLY AFFECT THE INDUSTRY'S ICS SECURITY IN SOUTH AFRICA. 42
4.3.1 EMPLOYEE ICS CYBER-SECURITY KNOWLEDGE 45
4.3.2 ORGANIZATIONAL ICS CYBER-SECURITY BEHAVIOUR 46
4.3.3 COMPLIANCE 48
4.4 SUMMARY OF THE RESULTS 51

CHAPTER 5. DISCUSSION OF THE RESULTS 52

5.1 INTRODUCTION 52
5.2 CHALLENGES EXPERIENCED IN SUBSTATION CYBER SECURITY IN SOUTH AFRICA. 52
5.3 TO WHAT EXTEND DOES THE CHALLENGES REALLY AFFECT THE INDUSTRY'S ICS SECURITY IN SOUTH AFRICA. 54
5.3.1 EMPLOYEE ICS CYBER-SECURITY KNOWLEDGE 54
5.3.2 ORGANIZATIONAL ICS CYBER SECURITY BEHAVIOUR 54
5.3.3 COMPLIANCE 55

5.4 CONCLUSION 55

CHAPTER 6. CONCLUSIONS & RECOMMENDATIONS 57

6.1 INTRODUCTION 57
6.2 CONCLUSIONS OF THE STUDY 57
6.3 RECOMMENDATIONS 57
6.4 SUGGESTIONS FOR FURTHER RESEARCH 58

REFERENCES.....i

APPENDIX A 5

APPENDIX B 10

LIST OF TABLES

Table 1: Definition of terms. 6

Table 2: Meaning of abbreviations. 7

Table 3: Comparing IT and OT equipment (Chipley, 2014; H. Luiijf & te Paske, 2015). 15

Table 4: Organizations active in the cyber-security space. 15

Table 5: Specifications relevant to substation cyber security. 19

Table 6: Interview Respondents profile for first research question. 29

Table 7: Profile of respondents. 30

Table 8: Employee ICS cyber-security knowledge. 45

Table 9: Organizational ICS behaviour results. 46

Table 10: Compliance level response data. 49

Table 11: The icebreaker questions for interview. 10

Table 12: survey questions with variable 11

LIST OF FIGURES

Figure 1: The effects of cyber-attacks. 2

Figure 2: The significance of the study. 5

Figure 3: Research process layout. 9

Figure 4: SCADA system layout courtesy of "The Viking Project" 2015). 11

Figure 5: Vulnerability ICS report (CERT, 2015). 13

Figure 6: The timelines of cyber incidences in ICS history (GICSP, Assante, & Conway, 2014; RISI, 2015). 14

Figure 7: ICS lifecycle (Group, 2015). 14

Figure 8: The process of law making in South Africa (Parliament, 2016). 21

Figure 9: Summary of procedure for data collection for interview. 32

Figure 10: Summary of procedure for data collection for survey. 33

Figure 11: Data analysis in Qualitative Research [adapted from Creswell (2014, p. 436)]. 34

Figure 12: Compliance and no-compliance criterion. 35

Figure 13: Responses classified per industry. 43

Figure 14: The responses across South African provinces. 43

Figure 15: Automation level. 44

Figure 16: Network internet connectedness. 44

Figure 17: Employee skill profile (against skill). 45

Figure 18: Employee skill profile (against skill level). 46

Figure 19: Organizational ICS behaviour (against 5-point Likert scale). 47

Figure 20: Organizational ICS behaviour (against behaviour)..... 48

Figure 21: Organizational ICS cyber-security compliance level. 49

Figure 22: Organizational ICS cyber-security non-compliance level. 50

Figure 23: Compliance level (spider diagram)..... 50

CHAPTER 1. INTRODUCTION

1.1 Purpose of the study

The purpose of this research is to identify the industrial control systems cyber-security challenges and determine its prevalence in South Africa.

1.2 Context of the study

The advent of the internet has seen a significant shift in economic activity to the cyberspace, provides a platform for global communication and is a source of revenue for many (Bohme & Moore, 2012). This has also translated into an increase in online criminal activity (cybercrime).

Security in Information Technology (IT) has been in the core of the design and operation of systems, software and hardware for decades because it has been around for few decades now (H. Luiijf & te Paske, 2015). However security concerns have only been around for only a decade in the operational technology (OT) because its only now that it has drawn attention to the cyber-criminals (H. Luiijf & te Paske, 2015; Macaulay & Singer, 2011). This development in OT is attributed to the standardization of the communication in the Industrial Control System (ICS) devices, the modular design of ICS devices and the rise in cyber-warfare; this has led to rise in the attacks on ICS (Cárdenas, Radosavac, Grossklags, Chuang, & Hoofnagle, 2009).

The world has experienced many ICS cyber-security incidences in the past few decades (Podbregar & Podbregar, 2012; RISI, 2015). The consequence of a successful cyber-attack incidents are loss of human lives through explosions in volatile industries, the revocation of license to operate due to an environmental incident (environmental damage), financial loss due to damage and loss of intellectual property, reputational damage (summarised in Figure 1) (Cárdenas et al., 2009). All of which results in some loss to the organization and society. Such incidences highlight the need for constant evaluation and improvement of cyber-security systems.

Many organizations are active in the ICS space and deal with the recording of incidents, while others respond to incidences. In the United States of America (US), Industrial Control System - Certification Authority (ICS-CERT) provides the recording, response and also certification services for organizations who fall victims to cyber-crime (CERT, 2015). The European Union has a CERT but they encourage individual member countries to have their own CERTs (CERT, 2015). The countries in Africa that have CERTS are Kenya, Tanzania and South Africa (CERT, 2015). The South African CERT is in its infancy and does not respond to incidents yet.

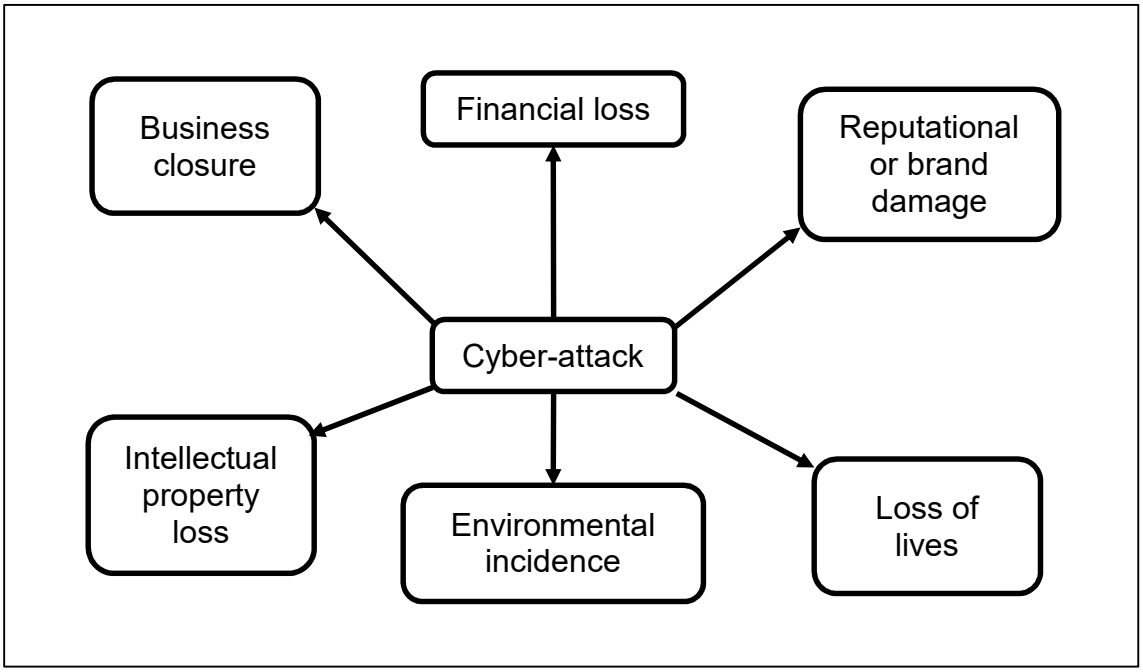

Figure 1: The effects of cyber-attacks.

There is insufficient recorded information for South African ICS incidences. There are only two confirmed recordings of South African incidences on the RISI (2015) database. The first was the infection of the Open Platforms Communication (OPC) server in 2009, which resulted in the plant running blind for 8 hours, fortunately, no major loss were incurred. The second incident was in 2007 when the South African National Defence Force's automated anti-aircraft cannon malfunctioned and led to the killing of 9 and the injury of 14 (RISI, 2015).The fact that there are only two reported incidents could mean that there either not much cyber-criminal activity or that incidents are not being reported in South Africa.

The South African control industry has seen a steady increase in automation over the years but there are still industries that still do manual operations. While automated industries incur the need for cyber security, the non-automated industry tend not to require it due to the low probability of exposure to external attacks. The South African industry has not adapted to the practice of reporting incidents as the rest of the developed world has. This directly translates to the industry unable to share the cyber-attacks information with each other and collectively unable to fight the crime.

The global ICS cyber-crime reporting and response are well defined and well-coordinated compared to the South African one (M. Dlamini, Eloff, & Eloff, 2009; Pack, 2012). The fight against cybercrime in ICS requires a coordinated effort from industry and government (Pack, 2012). Furthermore, the industries can learn from incidents in other sectors and countries (RISI, 2015). However, the learning and improvements depend on the reporting of the incidences as well as the response to attacks in the country. This ensures the capturing of the incident and that the records are kept at the same place for ease of analysis and decision-making. There appears to be little or no records of South African ICS cybercrime incidences and there is currently no coordinated response team for the South African ICS-CERT.

The cybercrime and cyber security legislation in South Africa is still in the draft stage. The similar document world over defines the types of crime in the cyber-space and their penalties, gives the roles and responsibilities of the stakeholders and defines the code of conduct in the fight against cyber-crime. It can therefore be stated that the beginning of an effective fight against cyber-crime depends on this legislation if the South African legislation is to be similar to the developed world's ones.

The motives for cyber-crime are potential gains from cyber-attacks, exacerbated by the internet and the lower chances of getting caught and this translates to be more convenient, profitable and less expensive to commit and less risky also (Cárdenas et al., 2009). This together with ineffective legislation and law enforcement creates mistrust of our ICS networks (Cárdenas et al., 2009). The

resulting financial losses due to internet crime in the United States for 2014 were $800 million (FBI, 2014).

The reasons that companies may not report cyber-incidents are that financial impacts, brand reputational damage, sharing information may inform attackers of vulnerability, job security fears, perceived lack of flaw enforcement and ignorance (Cárdenas et al., 2009).

It is therefore important to determine the ICS cyber-security challenges in South Africa and find out whether the challenges experienced globally are also experienced in South Africa, furthermore determine the impact of the challenges in industry's ICS cyber-security in South Africa. This will give insight into whether South African industries are at risk or the relevance of global ICS security risks to the South African context. The elimination of these challenges will ensure that the loss mitigation.

1.3 Problem statement

1.3.1 *Main problem*

The aim of this research is to identify the industrial control systems cyber-security challenges and determine its prevalence in South Africa.

1.3.2 *Sub-problems*

The first sub-problem is to identify the challenges experienced in ICS cyber-security in South Africa.

The second sub-problem is to determine the impact of the challenges in industry's ICS cyber-security in South Africa.

1.4 Significance of the study

Cyber-crime is not good for the business because it leads to loss of production, property and personnel (Cashell, Jackson, Jickling, & Webel, 2004). When a virus

infects equipment, for instance, production time is lost while trying to get the equipment to normal operation. If for instance an explosion or equipment damage is sustained during a cyber-attack, it could lead to loss of equipment, which directly translates to loss of income for an organization (Wen & Qianchuan, 2014). The explosion in a petrochemical industry for instance could result in the loss of personnel and is devastating not only to the organization but to the society also. For the organization, it is the loss of talent and reputational damage and the society losses bread winners are the main reasons cyber-crime on ICS should be prevented (Axelrod, 2013).

To emphasize the significance of the study, Figure 2 illustrates the process of securing the ICS. The identified challenges are then mitigated to make the ICS cyber-secure. The study will also assist the government and organizational managers to gauge the success of their cyber-security initiatives, which include awareness campaigns. This document could be used by anyone who wants to have a general understanding of the ICS cyber-security and cyber-crime.

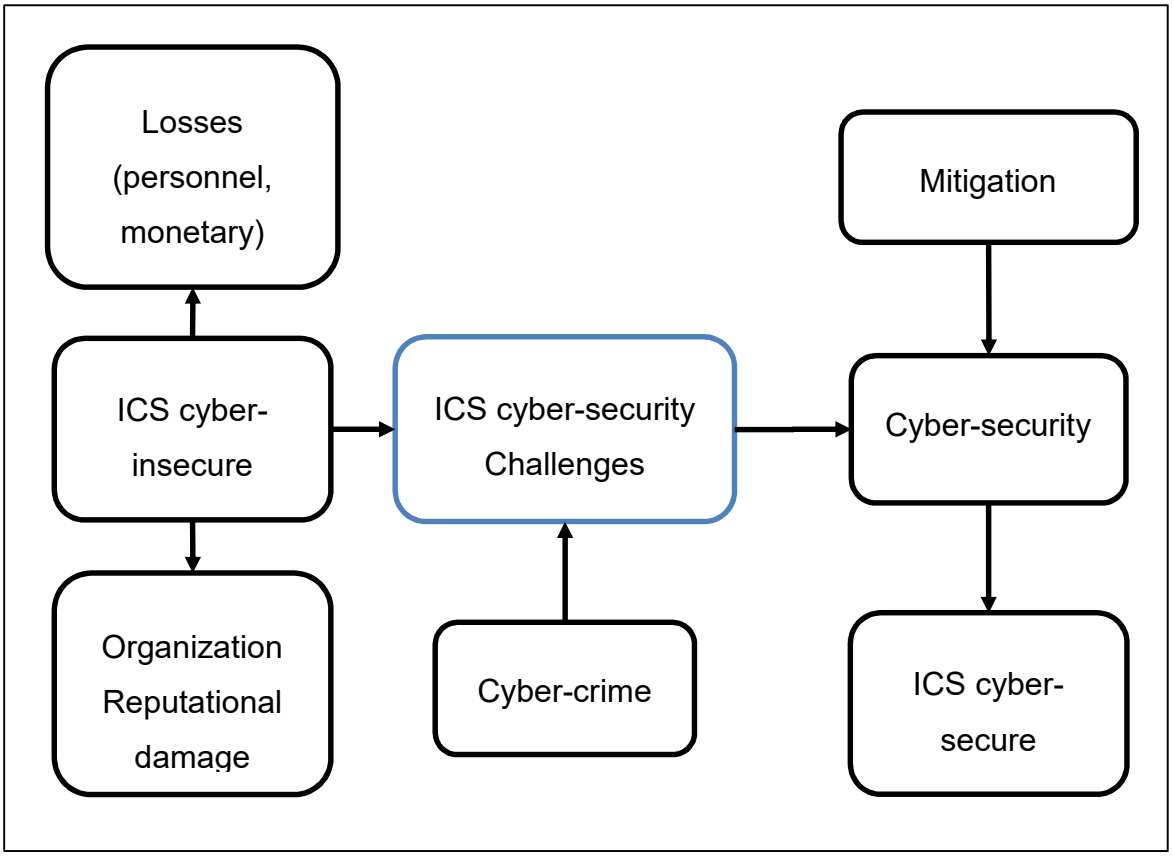

Figure 2: The significance of the study.

Decision makers, managers and business owners to understand the need to improve ICS cyber-security will use the information obtained from the study and knowing the challenges is the first step in addressing them effectively. Business analysts to motivate the business case for increased cyber-security could also use this study. This could also assist the managers to comply with the relevant legislation that relates to information security. The challenges could be used by managers to improve the cyber-security in the organization and benchmark their organization with the rest.

This research will also provide motivation to the ministry of Justice and Correctional services of South Africa to fast track the process of making the cyber-crime and cyber-security bill into law.

1.5 Delimitations of the study

The study include all kinds of ICSs typically found in an industry for example SCADA, DCS, PLC and HMI. All these are collectively termed ICSs for the purposes of this research (McDonald, 2012). The IT cyber-security challenges are not included in this research, when presented it is only to aid understanding. The study is limited to the South African context. The detailed definitions and classification of cyber-crime is not included.

1.6 Definitions and abbreviations

Table 1: Definition of terms.

TERM	DEFINITION
Cyber activity	Any activity done online
Cyber-crime	Illegal acts committed using information or communication technologies (SSA, 2011).
Cyber-criminal	A person who commits a cybercrime.
Cyber-espionage	The use of the internet to spy (Uma & Padmavathi, 2013).
Cyber-security	Z. Dlamini and Modise (2013)defines cyber-security as a “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, organization and user assets.”
Cyber-space	The internet

Cyber-terrorism	Casing mass disruption and destruction of property and life (Uma & Padmavathi, 2013).
Cyberwar	The act of a nation disrupting other nation's network to gain advantages of tactics and military nature (Uma & Padmavathi, 2013).
PLC	The PLC is a robust automation device which is widely used to control process equipment, according to sensor information and/or human input (Wen & Qianchuan, 2014).

Table 2: Meaning of abbreviations.

ABBREVIATION	MEANING
ICS	Industrial Control Systems (McDonald, 2012)
SCADA	Supervisory control and data acquisition
DCS	Distributed control system(IEEE, 2008)
PLC	Programmable logic controller (Creery & Byres, 2005)
HMI	Human machine interface
IED	Intelligent electronic device (Creery & Byres, 2005; IEEE, 2008)
OPC	Object Linking and Embedding for Process Control
OT	Operational Technology
IT	Information technology
LAN	Local Area Network (Creery & Byres, 2005)
WAN	Wide Area Network (Creery & Byres, 2005)
WAN	Wide Area Network (Creery & Byres, 2005)
WLAN	Wireless Local Area Network (Creery & Byres, 2005)
VPN	Virtual Private Networks (Creery & Byres, 2005)
TCP/IP	Transmission Control Protocol/Internet Protocol (Creery & Byres, 2005)
ISMS	Information security management system (Stouffer, Falco, & Scarfone, 2011)
ICS-CERT	Industrial Control System Cyber Emergency Response Team (Bada, Creese, Goldsmith, Mitchell, & Phillips, 2014)
CERT	Cyber Emergency Response Team (Bada et al., 2014)

1.7 Assumptions

- Respondents provide accurate perspectives and experiences.
- Respondents are assumed to have experience in ICS at substation level
- It is assumed that the more secure the system is, the less probable it is to being attacked.
- In the absence of cyber-crime and cyber- data on South Africa, we can assume that the events world over are also affecting South Africa.

- Since there is not much research done in South Africa on the subject, we assume that the challenges experienced world over are also experienced in South Africa.
- The snowball sampling tends to be limited to certain geography or type of respondents who know each other.

CHAPTER 2. LITERATURE REVIEW

2.1 Introduction

This chapter looks at literature review and it is divided into three sub-sections. The first the section defines the ICS cyber-security. The second section will introduce the challenges faced in ICS cyber-security and the third section will look at the prevalence of the challenges in industries in South Africa.

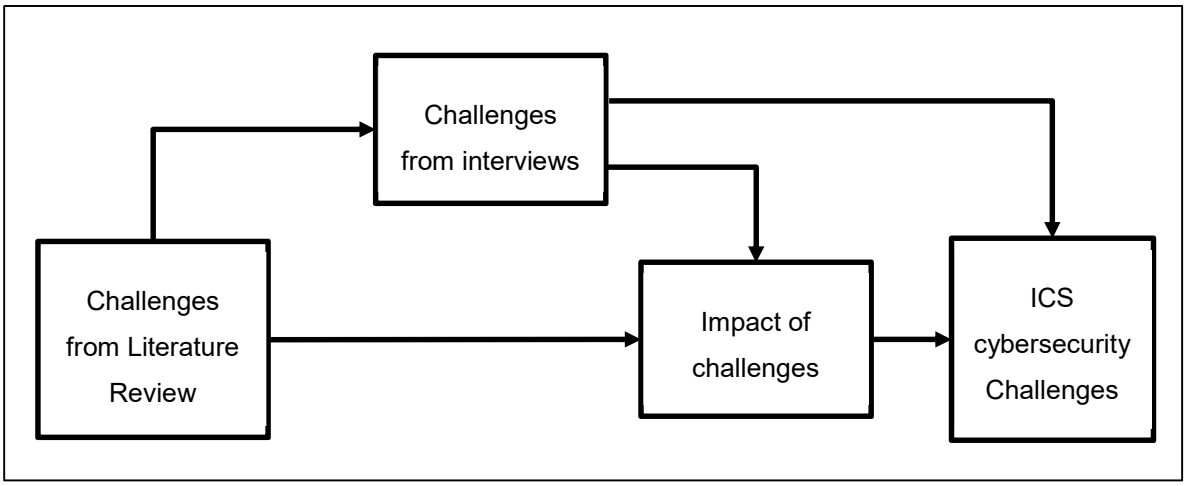

Figure 3: Research process layout.

The global challenges in the ICS cyber-security are initially presented from literature review and interviews confirm the South African challenges as shown in Figure 3. The impact of the challenges to some of the ICS professionals was then investigated.

2.2 Definition of terms

Cyber-crime is defined by Uma and Padmavathi (2013) as “the use of computers and the internet to exploit users for material gain”.

The working definition of cybercrime is illegal acts committed using information or communication technologies (SSA, 2011).

The prefix cyber stands for computer and electromagnetic related activities (Nye Jr, 2011).

The challenges are the hindrances preventing the implementation of the best practice in the cyber-security (McDonald, 2012).

2.3 Cyber security

2.3.1 *Information Technology*

To understand ICS cyber-security, it is important to differentiate between information technology (IT) and operational technology (OT). The increase cyber-activity has also translated to an increase in online criminal activity (cybercrime). Cybercrime has been given many definitions in literature, the Draft National Cybersecurity Policy Framework for South Africa defines it as illegal acts committed using information or communication technologies (SSA, 2011).

2.3.2 *Operational Technology*

The Industrial Control Systems (ICS) is a broad term used to describe the systems that are used to control, monitor and manage production systems (Macaulay & Singer, 2011). These include the supervisory control and data acquisition (SCADA), programmable logic controller (PLC), distributed control system (DCS), human machine interface (HMI) and Energy Management Control System (EMCS). An example of an ICS in the home is the controls of an air conditioner controller, where a temperature sensor data is used to determine the amount of coolant required to cool or heat up a room. The Industrial Control Systems (ICS) are classified as Operation Technology (OT) while the ordinary PC is regarded as Information Technology (IT) (Wen & Qianchuan, 2014). In recent years the OT has become more similar to the IT as technology is rapidly advancing and the effect is increased risk of cyber-attacks on ICS (Kozik & Choras, 2013), just as PC.

2.3.3 *Types of cyber-attacks*

The cyber-attacks can be classified based on purpose, legality, severity of involvement, scope and network types (Uma & Padmavathi, 2013).

2.3.4 *ICS networking 101*

The substation is a place where ICSs are housed and the ICS forms the heart of the control of the industry (Wen & Qianchuan, 2014). If the ICSs are not cyber secure, they can have devastating consequences to the industry, which in extreme cases can cause injury to personnel or cause environmental incidences (Adar & Wuchner, 2005; Byres & Lowe, 2004).

A pictorial view of a SCADA system and its peripheral devices for a substation is shown in Figure 4. The diagram shows the typical interface amongst the office, SCADA, substations and the internet networks. The substation network is typically connected to outside equipment via Intelligent Electronic Devices (IEDs) (IEEE, 2008).

The storage of data on cyber-attacks can help us understand the behaviour of the criminals and the cost of cyber-crime (Cárdenas et al., 2009).

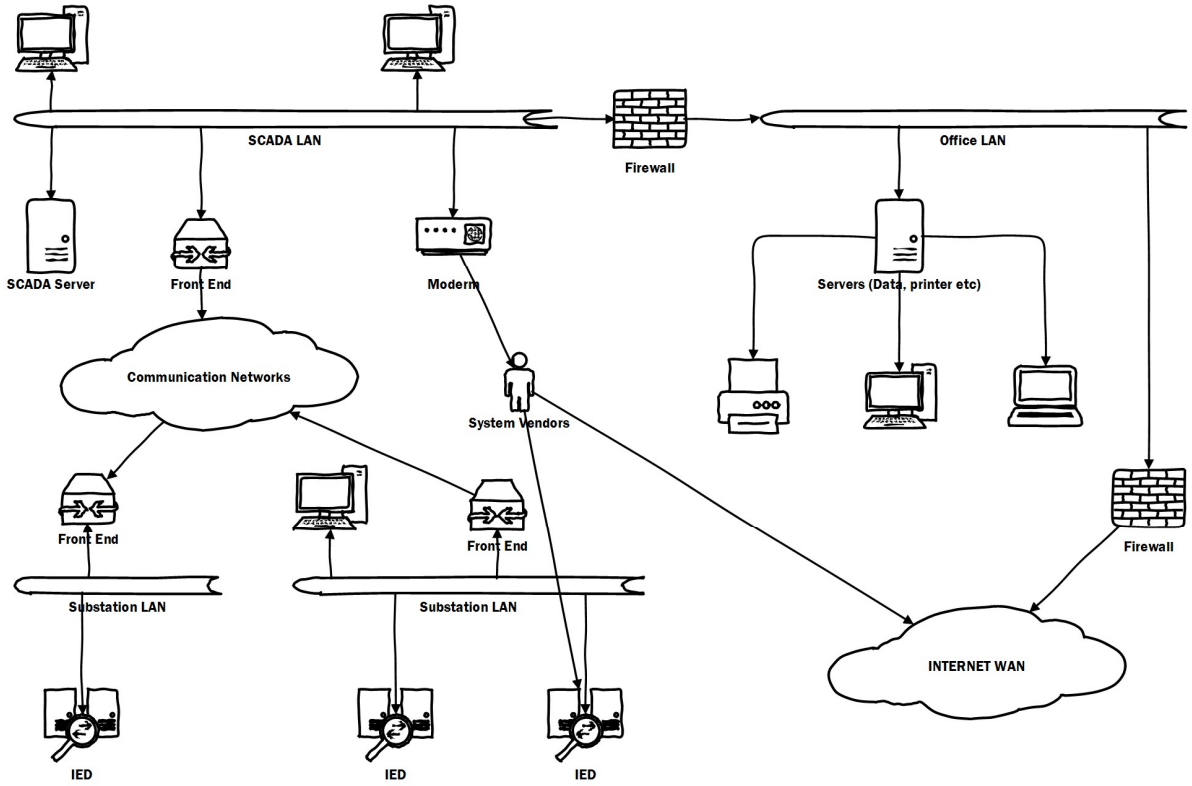

Figure 4: SCADA system layout.

The substation needs to communicate with devices in the field so that they are able to deduce their running load and the equipment status (IEEE, 2008). The

IEDs allow the control of the equipment. The control of the equipment is not normally done in the substation but usually in a control room. The information to start or stop for instance needs to be given to the equipment through the same IEDs via the substation (McDonald, 2012).

The substations need to communicate to the same network to consolidate the information transmitted to and from the substation (IEEE, 2000). Different parts of the equipment may be supplied with power through different substations (McDonald, 2012). In the substation will be the SCADA system which records all the set information that is available on the network like the motor current, the status of the equipment and when it changed, the disturbance recordings when the undesired effect happens in the system that needs looking at (McDonald, 2012).

In some instances, the vendors will have access to the equipment via the local network or via the internet (Zurich, 2015). If any local connection has to go through the internet there is a requirement for a firewall as it is regarded as an unsafe zone (also known as demilitarized zones DMZ) (IEEE, 2000). The connection between workstation or control rooms is usually through the DCS, which allows the issued control commands to be transmitted as information instead of the physical cables that leave the IEDs in substation to the field (Zurich, 2015). The technical people usually prefer to view the status of equipment or control their equipment while sitting in their offices and to do that there is usually a firewall in between for extra security (IEEE, 2008). This ensures that unauthorised employees do not access the control systems. There is also a firewall from the office network to the internet as expected to protect the company network from outsiders (Zurich, 2015).

2.3.5 *Cyber-attacks on ICS*

There have been confirmed reports about ICS cyber-attacks in recent years. In the United Kingdom in 2006, an organization called ABB performed a remote upgrade to the Power Control Centre (which was unplanned and unannounced) which resulted in the loss of control and view of the network for 22 minutes (RISI, 2015). Another incident was in the United States in 2008, when an engineer from

a power utility disabled two levels of protection in the Florida Power and Light Flagami substation which resulted in a short circuit fault (RISI, 2015). This affected up to four million customers and Turkey Point nuclear power plant (RISI, 2015). This shows that even though ICS attacks are rare, when they do happen, their effects cannot be foreseen until they are resolved.

Besides RISI, ICS-CERT also record incidences. The data in Figure 5 shows that there is a steady increase in vulnerability from 2011 to 2014. The timelines of selected ICS cybersecurity events are depicted in Figure 6.

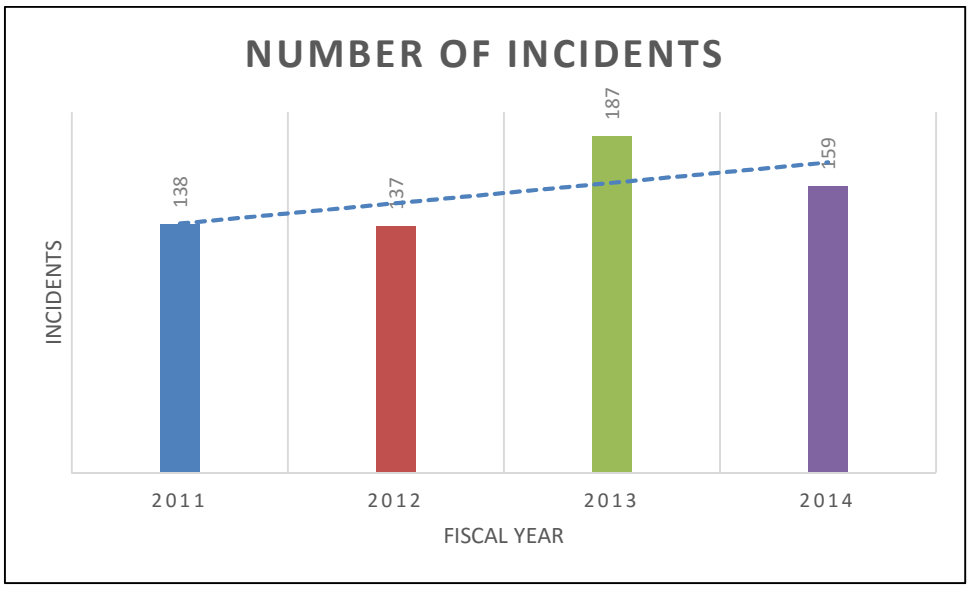

Figure 5: Vulnerability ICS report (CERT, 2015).

The impact of a cyber-attack on ICSs depends on the importance and criticality of the equipment supplied by it, environmental damage, the amount of money required to restore (or replace) service, the loss in revenue lost and the brand reputational damage caused by it (Byres & Lowe, 2004). This means that if the attack is successful, in its extreme it can cause loss of life and/or loss of revenue depending on the criticality of the equipment affected and its fail safe.

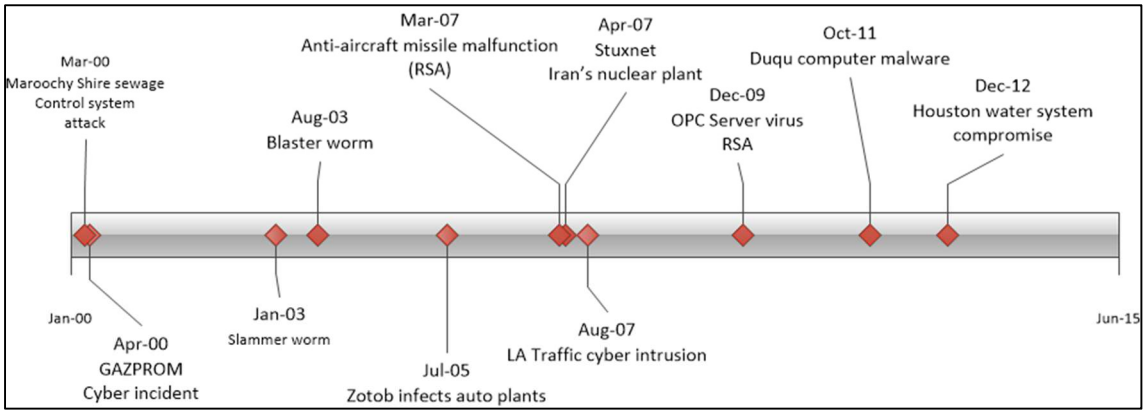

Figure 6: The timelines of cyber incidences in ICS history (GICSP, Assante, & Conway, 2014; RISI, 2015).

Figure 6 shows timeline of some important cyber-incidents in history, where in March 2000, the Maroochy Shire sewage plant attacks, in March 2007 the anti-aircraft missile malfunctioned and December 2012 there was a Houston water system compromise (RISI, 2015).

The perpetrators of cyber-crimes in the ICS space are cybercriminals, disgruntled employees, terrorists, activists and organized criminals (Cardenas et al., 2009). Their names also say something about their motives.

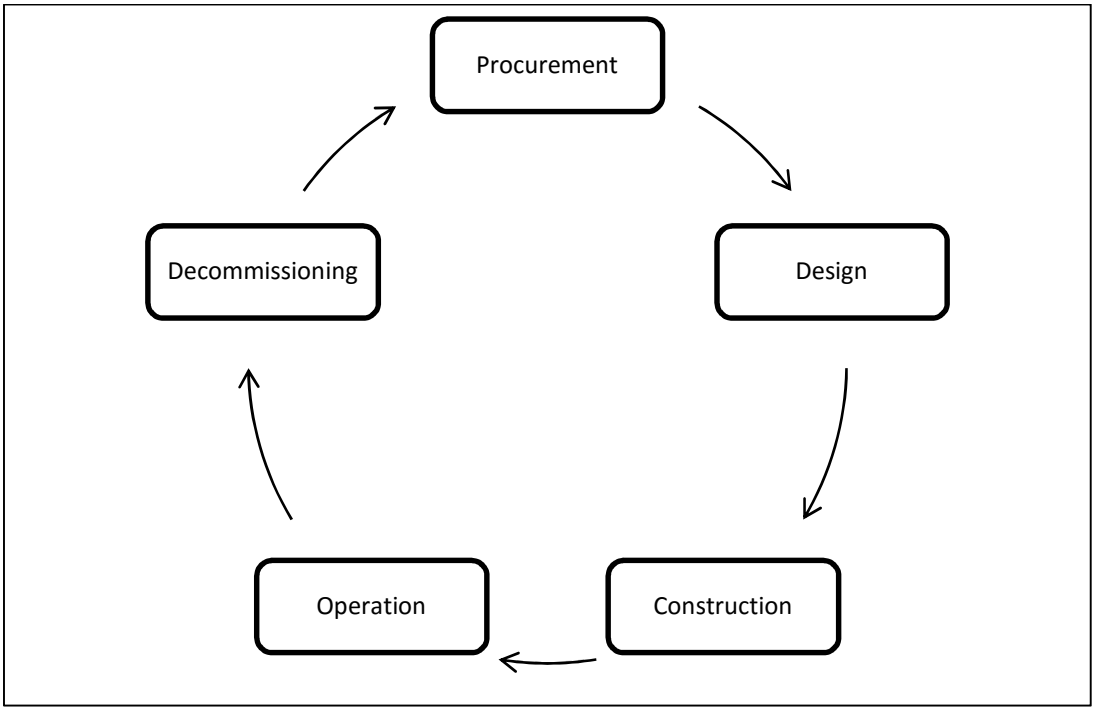

Figure 7: ICS lifecycle (Group, 2015).

The lifecycle of ICS shown in Figure 7 and is similar to the lifecycle of an asset. The lifecycle follows the sequence: procurement, design, construction, operation and decommissioning (Group, 2015). To ensure protection at all times, the good practices of cyber security should be observed at all stages of the ICS lifecycle (Group, 2015).

Table 3: Comparing IT and OT equipment (Chipley, 2014; H. Luiijf & te Paske, 2015).

	IT	**OT**
Security Priority	confidentiality, integrity, availability	Availability, visibility, operability, integrity
Purpose	transactions, information	control and monitor processes and equipment
Role	Supports people	controls machines
Availability	when needed	all the time
Anti-malware	required by default	Uncommon
Interfaces	web browser, terminal key board	sensors, actuators, hand held devices
life span	3 to 5 years	10 to 25 years
password	8 digit Lockout protects the network	3 digit Lockout after 3 attempts undesirable

Table 4: Organizations active in the cyber-security space.

ORGANIZATION	RESPONSIBILITIES	SITE
Industrial Control System Cyber Emergency Response Team (ICS-CERT)	Reduces risks on all critical infrastructures by collaborating with stakeholders and collaborates with international and private sector CERTs to share control systems-related incidences and mitigation measures.	https://ics-cert.us-cert.gov/
Repository of Industrial Security Incidents (RISI)	Provides a platform to report incidents and provides the information to the public.	http://www.risidata.com/
Department of Justice & Constitutional Development - Cyber Safety (DOJ&CD)	Provide information on cyber-crime, cyber safety and online security.	http://www.justice.gov.za/cybersafety/cybersafety.html

ORGANIZATION	RESPONSIBILITIES	SITE
Department of Telecommunications and Postal Services - Child Online Protection (DTPS)	Collaborates with international organizations to promote the online protection of children by educating them on safe online behaviour.	http://www.dtps.gov.za/key-programmes/child-online-protection.html
Electronic Communications Security - Computer Security Incident Response Team (ECS-CSIRT)	Handles computer security incidents to prevent future incidents with high priority given to the Government assets and critical infrastructure.	http://www.first.org/members/teams/ecs-csirt
Film and Publications Board - Pro Child (FBP)	A public service for reporting child pornography or sexual abuse images found on the internet.	http://www.fpbprochild.org.za/
Internet Service Providers Association - Code of Conduct (ISPA)	This is the representative body of ISP's governing their conduct. They provide information on cyber-crime.	http://ispa.org.za/
South African Banking Risk Information Centre - Safety Tips (SABRIC)	Representative body for the banks to fight organized crime. Provides information on cybercrime issues.	https://www.sabric.co.za/
South African Police Service - Youth Desk (SAPS)	Publishes tips on internet safety, cyber bullying. No reporting facility.	http://www.saps.gov.za/youth_desk/teens/internet_safety.php
South African Revenue Services - Scams and phishing attacks (SARS)	Provides information on reporting suspicious or fraudulent activities.	http://www.sars.gov.za/TargTaxCrime/ReportCrime/Pages/default.aspx
University of Johannesburg Centre of Excellence in Cyber Security (UJ-CECS)	University of Johannesburg and the academy of computer science and software engineering initiative to address cybercrime in South Africa. Allow for reporting and viewing statistics on cybercrime.	http://adam.uj.ac.za/csi/
Wolfpack Africa	Educating user on cyber threats. Allows reporting.	http://alertafrica.com/

2.3.6 *Risk in cyber security*

Wen and Qianchuan (2014) states that the money spent on cyber-security cannot be recovered. The benefit only comes in the savings made from a potential event which are financial savings, undamaged reputation, health and safety incidence avoidance and environmental incident avoidance (Byres & Lowe, 2004). In risk

management, it is not always possible to eliminate all the risks, as resources are always limited. Some risks are eliminated but some are managed and some transferred to risk managers such as insurance. The conformation to current specifications and standards ensures the implementation of lifelong lessons.

Cyber-security is a risk in business and its business case should be approached from the loss prevention and safety side rather than using the traditional methods like net present value (NPV) to derive viability (Shim & Siegel, 2010). This means that NPV will always be negative, not understanding the type of risk could lead to no implementation of cyber security in ICS protection as it will not make business sense.

2.3.7 *The typical ICS equipment*

Electricity is essential to the running of the industry, it is virtually impossible to run without it (McDonald, 2012). There is a need to have control of when to switch on or shut it down the equipment and to do so without the damage to equipment of any other personnel (McDonald, 2012). Electricity can be dangerous if not delivered safely (McDonald, 2012). The function of the ICS contained in the substation to ensure that the electricity is delivered safely and these are for protection relays and circuit breakers. (McDonald, 2012).

The PLC and the DCS systems function to control the equipment outside of the substation (Wen & Qianchuan, 2014). These can be housed outside of the substation but have traditionally been located inside the substation. The ICSs in the field (plant) that are not part of research are controllers, transmitters and level controllers. The SCADA system enables the collection of all network parameter data and the control of ICSs connected on the network (Wen & Qianchuan, 2014).

The substation aims to ensure the safe provision of electricity to the connected load which is mainly the equipment in the industry (McDonald, 2012). This equipment needs to constantly communicate amongst themselves to get each other’s information in order to successfully and safely complete the mission (IEEE, 2008). The network layout of the substation is presented in Figure 4.

The communication and interconnection in the substation has not always been through network devices. Originally it was done through physical wire connections (McDonald, 2012; Wen & Qianchuan, 2014), which was costly as a large quantity of copper wires was required to construct the network and the network never left the substation (McDonald, 2012). This configuration meant that for anyone to intentionally disrupt the operation would have to be in the substation but nowadays cyber-crime can be committed without being physically present at the scene on an attack (Wen & Qianchuan, 2014).

From the hardwired situation the network evolved to smarter electronics that had communication ability but the networking devices were proprietary so it was difficult connect to them (Wen & Qianchuan, 2014). This created an added protection layer to cyber attack (Creery & Byres, 2005). Once connected, the network was difficult to breach, so it provided a certain layer of protection to the network (Wen & Qianchuan, 2014).

The use of the ethernet today makes it easier to connect to the ICS network and the cost of the devices has decreased (Creery & Byres, 2005). This means that the movement from proprietary technology to internet based technology has lowered the price of ICS but has created a natural weakness in the network.

The ICSs also evolved to using the internet-based protocols (modular). This resulted in the security of the substation network being compromised as the applications became similar to the ordinary PC application (Kozik & Choras, 2013). The attacker and cybercriminals have already been working to attack the PC for a decade now, so the transition to ICS similar to the PC is easier (GICSP et al., 2014). That is how we arrived to the cyber security state that we are now as far as the substation ICSs are concerned.

The attention to ICS cyber security from the world government, community and academia has increased ever since Stuxnet in 2007 (Wen & Qianchuan, 2014). While the attacks are not common, there have been some recorded and confirmed incidences of industrial cyber incidences world over.

2.3.8 *Standards and Specifications*

In engineering, design work is governed by standards and specifications, which stipulates the best practice minimum required performance (Boyes, 2015). In South Africa, the issue and review of standards is governed by the South African Bureau of Standards (SABS). SABS is in turn governed by the Standards Act, 2008 (Act No. 5 of 2008). The best practices are incorporated into the standards when the standard is reviewed. The design and operation of some of the ICSs found in a substation are governed by the standards shown in Table 5.

It is interesting to note that most of the incidences are caused by the lack of the most basic of protection besides all the education and standards available (Boyes, 2015).

Table 5: Specifications relevant to substation cyber security.

SPECIFICATION/STANDARD	TITLE
BS 17799-2005 ISO/IEC 27001-2005 SANS 27001-2006	Information security management systems
BS 17799-2005 ISO/IEC 27002-2013 SANS 27002-2014	Code of practice for information security controls
IEEE 1402-2000	IEEE Guide for Electric Power Substation Physical and Electronic Security
API 1164	Pipeline SCADA Security, Second Edition
ISA-TR99.00.02-2004	Integrating Electronic Security into the Manufacturing and Control Systems Environment
IEEE PC37.1™ IEC 62443-2-1	IEEE Standard for SCADA and Automation Systems
IEEE Standard 1686™-2007	IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities

The standard IEC 27001-2005, for instance was designed for all industries and describes the role of all stakeholders in the company with regards to information security in a well-established information security management system (ISMS) (ISO & IEC, 2005).

2.4 South African Context

2.4.1 *The draft cyber-crimes and cyber-security Bill*

The “Bill” in this section refers to the Cyber-crimes and Cyber-security Bill draft for public comment. The Bill presents the type of offenses in the cyber-space and the penalties to the offences. These offenses include unlawful data access, interception, interference with devices, malware acts, data acquisition and possession, computer fraud cyber terrorism ("Cyercrime and Cybersecurity Bill - Draft for public comment," 2015).

Because cyber-crime can be committed in one jurisdiction while the offender may reside in another, this offers a broader definition of jurisdiction than we know. The Bill further regulates the investigative powers, search, and gaining access, seizure of devices, international cooperation and aspects of evidence ("Cyercrime and Cybersecurity Bill - Draft for public comment," 2015).

There is the provision in the bill to have a 24/7 point of contact and the establishment of the structures to deal with cyber-security. The Bill also provides a framework to identify and declaration of National Critical Information Infrastructure ("Cyercrime and Cybersecurity Bill - Draft for public comment," 2015).

The Bill also imposes obligations on electronic communication service providers on issues that influence cyber-security. The Bill provides for the president of the Republic of South Africa to enter into agreements with other states to promote cyber-security ("Cyercrime and Cybersecurity Bill - Draft for public comment," 2015).

The introduction of this Bill will cause certain laws to change and the bill gives the provision to modify the other laws.

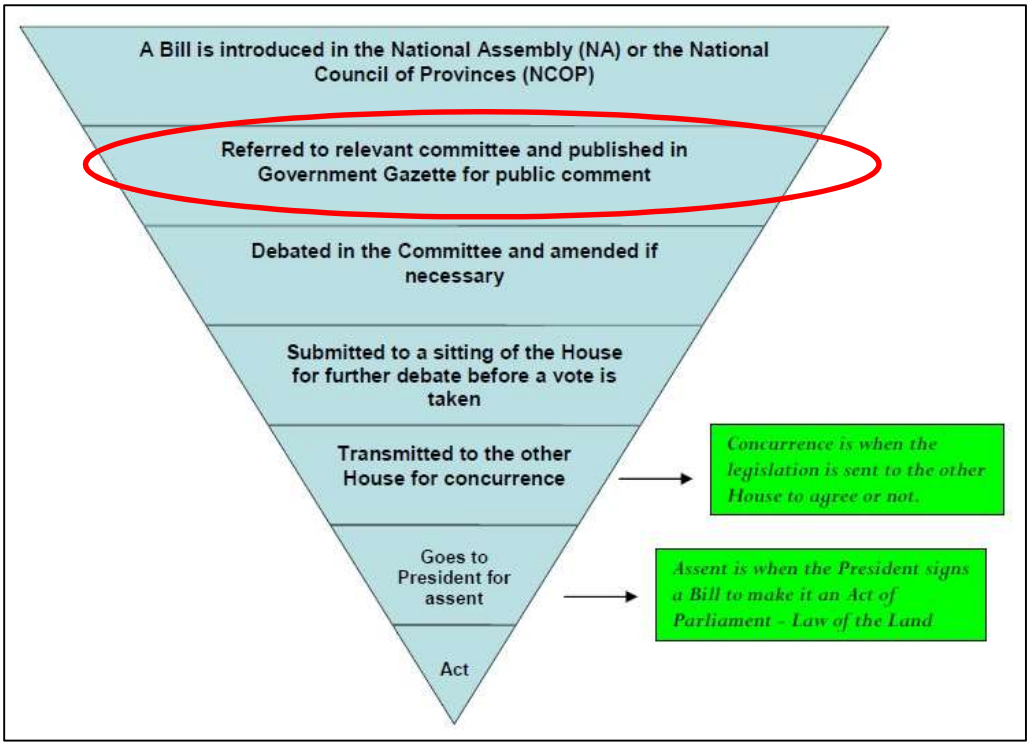

Figure 8: The process of law making in South Africa (Parliament, 2016).

The Bill is out for public comment, this means that it has gone through only one process in the making of a Law and there are four more steps before it can become Law (see Figure 8) ("Cyercrime and Cybersecurity Bill - Draft for public comment," 2015).

2.4.2 *Automation Level*

The south African companies are lowly automated at 31% which is lower than the global 56% (Jonker, 2015). The level of ICS automation translates to the probability of data availability online, where ICS that is not automated might have a low risk of cyber-attack and the automated one has a higher risk.

2.5 Challenges in ICS cyber-security

The ISC cyber security initiatives have come a long way but there are still some challenges. The report on South African cyber threat sited the lack of a “functional national Computer Security Incident Response Team (CSIRT)” as a challenge to

cyber security Pack (2012). In Europe, the CIR-SERT team are responsible for the response of ICS incidences and keep the records of all incidents.

There is a need to determine the difference between benign threats from real threats to protect the organization from internal threats (Kozik & Choras, 2013). The ICS has no way of detecting the intentions of the user. The industries also grow the network by adding other devices without looking into the network architecture; this weakens the network security and efficiency by creating backdoors that the attackers for intrusion (Creery & Byres, 2005). At some point, there is a need to re-design the network architecture before anything else is added (Lee, 2008).

Another hindrance to the creation of a cyber-secure ICS network is the lack of communication between the (OT) engineers with their IT counterparts (Wen & Qianchuan, 2014). It is believed that the IT professionals shutdown when they hear about the OT and vice versa (Creery & Byres, 2005). The control engineers could learn from the IT and IT should be willing to lend a hand; the security of the ICS depends on the cooperation of the two. The cyber-security issues have been dealt with by the IT for the past 2 decades but the control engineers only know about it recently (Wen & Qianchuan, 2014).

The non-intrusive devices used to determine the correct configuration of devices usually causes the control devices to fail (Creery & Byres, 2005). This means that installing these devices to check consistency is not an option as reliability is still a priority in ICS operation (Adar & Wuchner, 2005).

Due to the long lifespan of ICS equipment, the old (legacy) and the new equipment are being mixed on the same network as organizations replace some old equipment (Creery & Byres, 2005). This creates a problem where the latest equipment has higher specification of security while the other old equipment doesn’t (Kozik & Choras, 2013). The legacy equipment then becomes the weakest link in security.

In the industry there is a lack of direction from management on the direction of the company in terms of ICS security (Creery & Byres, 2005). The equipment in the industry is run for 24 hours a day and the software patches presents a security

management issue where software needs to be tested for security and functionality before installation (Creery & Byres, 2005; Kozik & Choras, 2013). The result is usually software that has not been updated for years and its security is compromised (Lee, 2008).

The modular computers used in SCADA (Windows OS) are prone to attacks as they have the same architecture with the ordinary PC (Kargl, van der Heijden, Konig, Valdes, & Dacier, 2014) and the ordinary OC has been attacked by viruses for the past two decades (Wen & Qianchuan, 2014).

The ICSs were not designed to withstand dedicated attacks, so when an attack is dedicated, it disables it completely (Kargl et al., 2014). A demostration of this was done at the ISA Expo in October 2004 when a PLC program was compromises and this eventually lead to the PLC shutting down (Kargl et al., 2014). The attacker usually creates the malicious software from reverse engineering the PLC firmware (Stouffer, Falco, & Scarfone, 2008).

The control of access to physical infrastructure helps limit the number of cyber-security breaches, this limits the would be attackers to the employees of the firm who are responsible for the particular equipment, so obviously this does not eliminate the sabotage component (Flynn, Huth, Trzeciak, & Buttles, 2012). The ICS also require password protection in order to keep out local and remote intruders (Wen & Qianchuan, 2014).

When procuring new equipment, it is important to follow the cyber-security procurement procedure if the organization has one, this ensures that the equipment procured will follow the minimum requirements for cyber-security (Goff, Glantz, & Massello, 2014). The equipment also need to be designed for cyber-security as an equipment on its own that is secure is not good for a system that is not secure (Lee, 2008).

During commissioning of the equipment, thorough testing is required to ensure that the protection does what it intended, this also applies to vendor patch installation during the lifetime of the ICS equipment, where the software should be tested thoroughly (ISO & IEC, 2005; Lee, 2008). When disposing of old ICS,

memory should be cleaned so that after disposal, no one can use the program in the device to craft virus for the ICS (Wen & Qianchuan, 2014).

When a vendor comes to upgrade, repair or install any equipment on your site, it is very important to accompany them and know what they are doing, to prevent them from installing viruses and wrong programs on your system (ISO & IEC, 2005; Wen & Qianchuan, 2014).

An organization needs a cyber-security policy, which determines the conduct to ensure systems are cyber secure and the policy needs to be established if it is not drafted and followed all the time it if exists and reviewed regularly since the industry is always changing (Flynn et al., 2012).

The education of employees and stakeholders on cyber-security promotes the culture of cyber-security within the organization and this culture of cyber-security will lessen the number of cyber-incidents (E. Luiijf, 2008). The remote connections need to be secure and continuously monitored since they pose the most risk (Wen & Qianchuan, 2014).

The monitoring of users and user behaviour on the ICS network ensures the identification of disruptive behaviour and allows the organizations to act to prevent disruptive behaviour (Flynn et al., 2012). A cyber-security centred termination procedure eliminates sabotage as sabotage is perpetrated by disgruntled and notice serving employees, this only helps the laid off employees from committing sabotage against the organization (Wen & Qianchuan, 2014).

The cyber-incident manifests itself as an equipment malfunction so it is important to understand the healthy behaviour of equipment so when the malfunction happen, it will be easy to identify (Wang & Lu, 2013; Wen & Qianchuan, 2014).

Cyber-crime has led to more equipment computer resources being used for monitoring instead of data provision (Wang & Lu, 2013). This means that extra budgets not directly required for the mission forms constituent of the total cost of ICS (Pearson, 2011).

There are many reasons cited in the literature for perpetrators committing cyber-crime. Some reasons are that cybercrime is easy to commit, requires few resources, can be committed in a jurisdiction without being there and that cybercrime still has a lot of grey areas (Ayofe & Oluwaseyifunmitan, 2009). In South Africa the cybercrime has been on the increase with phishing and identity theft as the most prevalent activities (I. Z. Dlamini, 2012).

To prove that there are attacks happening in the RSA, the respondent set up a water plant mimic PLC control system called a “honeypot” (Pool, 2014). A honeypot is a virtual system that represents a running plant, its left with some weaker security to allow for hackers to attack, the PLC was attacked to a point of shutdown (Pool, 2014). The results were about 5% malware, 26% recon, 4% denial of service and 35% hacks (Pool, 2014). This brings in the issue of not recording incidents, does not necessarily mean that there are no incidents happening and there is a possibility of the incidents going unnoticed because organizations do not have the resources or the knowhow to identify them.

2.5.1 *Research question 1*

What are the ICS cyber security challenges faced in South Africa?

2.6 Impact of challenges

A research on the impact of the challenges has not been investigated in South Africa, evidenced by the lack of literature. The ICS cyber-security knowledge of employees and the behaviour of organizations can make a difference in the fight against cyber-crime. Knowledgeable employees and organizations are better position to identify and react to attacks.

2.6.1 *Employee ICS cyber-security skill*

There is a current shortage of ICS cyber-security skills in the country (Daniels, 2007). The ICS skills are readily available while the ICS cyber-security skills are scarce since the profession is relatively new.

2.6.2 *Organizational ICS cyber-security behaviour*

The separation of duties prevents sabotage and error by making many people complete a task instead of one (Wen & Qianchuan, 2014). Where one person could have taken the whole system down without separation of duties, ensures that a few people have to collaborate to take the system down due to access restrictions.

2.6.3 *Compliance*

Compliance was measured from the best practices contained in engineering standards. Standards are a compilation of the prolonged industrial best practices. South Africa is purchasing and using the worldwide standards through the equipment it uses; which are imported most form Europe and America. The compliance goes beyond getting equipment compliant with certain standards.

2.6.4 *Research Question 2*

To determine the impact of the challenges in industry's ICS cyber-security in South Africa.

2.7 Conclusion of Literature Review

The literature review first introduced the subject of cyber-security; the South African context is presented, followed by the challenges in the ICS cyber-security and lastly the impact of the challenges.

Some of the challenges presented are:

- insider threats
- conflict between IT and OT
- the mixing of legacy and new equipment is a challenge
- management buy in is a challenge
- the ICS are not designed for a dedicated attacks,
- access control is an issue

- protection needs to be by design
- compliance issues during disposure
- the need for testing software during commissioning
- vendors needing accompaniment
- cyber security is required for organization
- employee education necessary
- insider attacks
- The importance of knowing the operation of the healthy equipment.

The most difficult challenge is to prevent a cyber-attack perpetrated from the inside of the organization.

The impact of the challenges is divided into employee ICS cyber-security skills, organizational ICS cyber-security behaviour and compliance to ICS cyber-security best practice. The is a shortage of skills in the engineering sector in South Africa. There is no previous research on organizational behaviour and compliance rate in literature.

2.7.1 *Research Question 1:*

What are the cyber security ICS challenges faced by industries in South Africa?

2.7.1 *Research Question 2*

To determine the impact of the challenges in industry's ICS cyber-security in South Africa.

CHAPTER 3. RESEARCH METHODOLOGY

3.1 Introduction

This chapter describes the methodology used to conduct the research. The chapter first discusses the choice of qualitative research and then followed by the review of the research design and the instrument used. The chapter then ends with how validity and reliability in the research is addressed.

3.2 Research methodology

There are three main research methodologies which are Qualitative, Quantitative and mixed (Bryman, 2012). Creswell (2003, p. 18) defines quantitative research as:

"one in which the investigator primarily uses post positivist claims for developing knowledge, employs strategies of inquiry such as experiments and surveys, and collects data on predetermined instruments that yield statistical data"

And defines qualitative research as

"one in which the inquirer often makes knowledge claims based primarily on constructivist perspectives or advocacy/participatory perspectives or both".

The research sought to establish if the ICS cyber-security challenges experienced by the world are the same in the South African context and the impact these challenges are having to the industry. The qualitative research method is employed in this research. Question 1 was addressed through interviews and questionnaire and question two was answered through a questionnaire. It is the most suitable because the questions are open ended for research question 1 and the data from questionnaire yields ordinal and categorical data, which is qualitative because the data is text, not continuous and non-parametric (Creswell, 2014).

3.3 Research Design

There are five generic designs which are Experimental, Cross-sectional, Longitudinal, Case study and comparative (Bryman, 2012). This research design is a descriptive cross-sectional study of the challenges that South Africa is facing in the ICS cyber-security.

3.4 Population and sample

3.4.1 *Population*

The population defines all possible respondents (Bryman, 2012). The population for this research are all people with ICS and those with ICS cyber-security knowledge. Even though the data was collected from people, the data collected was about devices and processes that form the ICS network.

Table 6: Interview Respondents profile for first research question.

Respondent	Credentials
Senior Researcher, Senior specialist from renowned research organization	BSc and PHD computer science, cyber-security project execution experience, commented on draft legislation
Manager: Systems and Automation – consulting firm	Master of Engineering, 10 years' systems engineer, 10 years' principal engineer
Senior Automation Consultant Engineer-renowned Utilities Company	BSc and MEng Electrical Engineering
ICS custodian	BSc computer science, MSc Engineering Management

The profile of the respondents for the survey (research question two), were professionals working with ICS on a daily basis which was composed of engineers, technicians, supervisors and service providers.

There are estimated 120 000 all discipline engineers, technologists and technicians in the country according to ECSA (2014). This is divided for all 8

recognised disciplines, so electrical engineers are about 15 000. this number is further divided into electrical and electronic professionals, so the population is about 7500 for electrical engineers, technologists and technicians.

The ICS cyber-security experts in ICS are very few in South Africa, an estimate of around 200 is made for this research, since the actual number is not known, which is 2.6% of the control engineering professionals.

3.4.2 *Sample and sampling method*

Good practice requires that the samples be chosen randomly or using probabilities (Bryman, 2012). This is however not always possible due to constraints (Bryman, 2012), in this research the geographical location and willingness of organizations to give permissions were those constraints. A representative sample of organizations was chosen using the snowball method, with the initial respondents chosen from the researcher's contacts from industry. The respondents will be chosen using a non-probability (of type convenience) sample method.

The sample size is balancing act between time and cost (Bryman, 2012). As the sample size increases, the sampling error is reduced but is not a guarantee of precision (Bryman, 2012). The population of technical experts is relatively homogeneous so a small population is acceptable (Bryman, 2012). The list of experts acquainted to the researcher formed the initial sample for the snowball method used to obtain the quota of respondents required.

The profiles of respondents are listed in Table 7.

Table 7: Profile of respondents.

Description of respondent	**Expected Sample**	**Population**
ICS cyber-security expert	6	200
ICS knowledgeable personnel (maintenance official, engineer, technician)	80	7500

3.5 The research instrument

The research instrument is a semi-structured interview schedule for research question one and a full-structured questionnaire for question two. The instrument for research question two is new formulated for this research but informed by Flynn et al. (2012).

The questionnaire is less costly and less time consuming but however requires some level of literacy (Guyette, 1983). To attract respondents the questions asked are beneficial to the respondents as the organization can know their security compliance status (Creswell, 2014). Respondents benefit from the research in that they can also receive a copy of the research report when completed.

The first instrument asks ICS cyber security experts what the challenges they are facing are and guideline questions from literature review was used to guide the conversation. The challenges found were compared with the literature and then used to formulate the questionnaire to answer the second research question.

Research question two is formulated from literature review challenges together with the interview found challenges. It measures the impact of these challenges to the industry.

To answer question one, an unstructured interview was conducted from four respondents.

To answer the second question, considering the constraints of time, heterogeneity, the analysis to be conducted and cost, the sample size was chosen as 80 from a diverse industry. Only 64 responses were received from ICS practitioners.

3.6 Procedure for data collection

The research data was collected for research question one by semi-structured interview and for the quantitative research question two using a questionnaire and the web (Qualtrics®). For the research question one, four respondents were

interviewed and for research question two, 64 respondents responded to 13 questions. For research question two, the information was collected through research questions administered through Qualtrics ®, with most of them five point Likert scale type. The respondents completed the questions asked to the best of their knowledge.

The interview was semi-structured and results were scripted and the script files were stored on one computer with a backup stored on one memory device. The file was password protected to ensure that no one else sees the contents to protect the privacy and confidentiality of the respondents. The industry and biographical information was then scripted to protect the interviewee. The Qualtrics ® data's biographical information is stored on Qualtrics® and all the information extracted did not contain biographical information and this is also to protect the respondents'.

The process of data collection for the interview is shown in Figure 9, which is interview, audio recording, transcription and then data analysis.

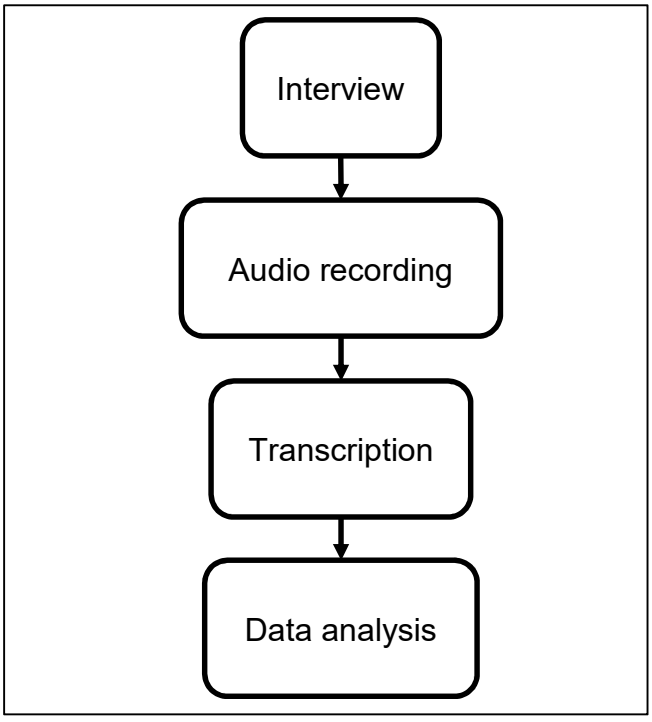

Figure 9: Summary of procedure for data collection for interview.

The process for data analysis for the survey is shown in Figure 10, where it starts with preparing the respondents list and the survey. The questions are then

translated to Qualtrics ® and then a mock survey is sent out to pick out any errors. The feedback from the mock survey was then incorporated in the survey. The survey was then sent out to the respondents and about a week later those who had not completed the survey were sent kind reminders to complete the survey, some were even called to be reminded. When there was no more responses coming through, a decision was taken to kill the survey, after which the data was then analysed.

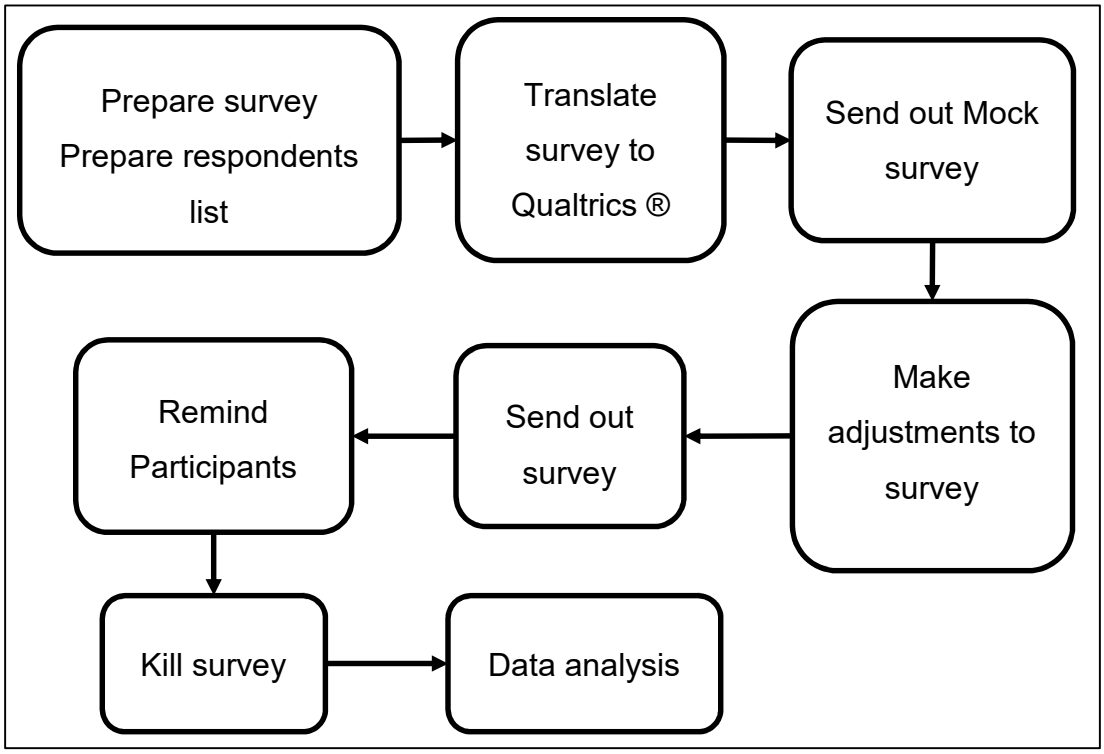

Figure 10: Summary of procedure for data collection for survey.

3.7 Data analysis and interpretation

The interview scripts were edited repeatedly to ensure that there are no errors before analysis. The data analysis process began by organising and preparing data by questions and responses and then read all the scripts to gain some understanding. The responses were expounded on and the meaning of the descriptions sought. The process of data analysis for the interviews is summarised by flowchart in Figure 11.

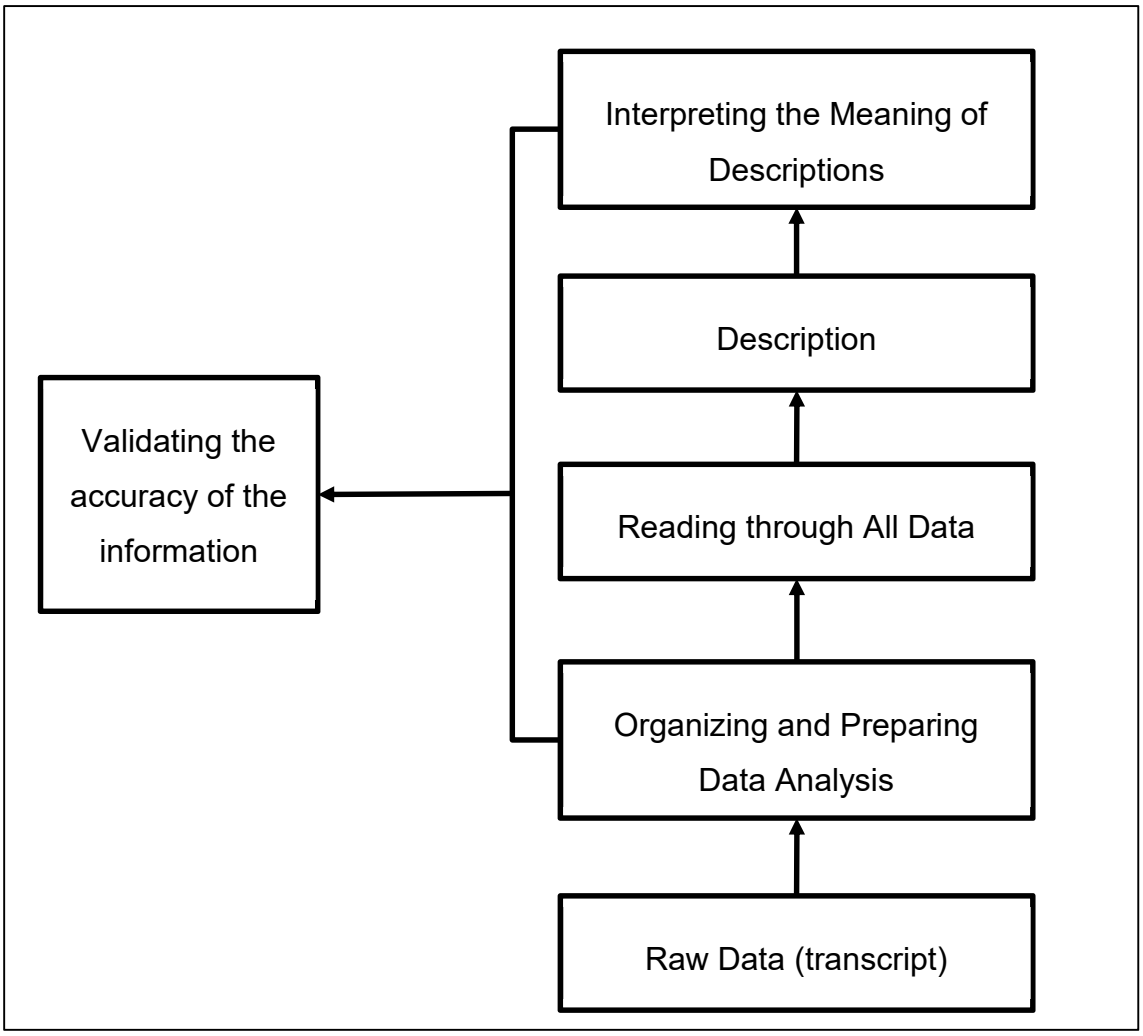

Figure 11: Data analysis in Qualitative Research [adapted from Creswell (2014, p. 436)].

The data for the survey was first analysed by the eye to determine if there are anomalies like missing data. The data was then cleaned out where missing data of more than 80% was completely deleted from the records. The data was then coded as shown in APPENDIX A for ease of analysis. The variables are dichotomous and ordinal so the descriptive statistics cannot be used to analyse the data (Bryman, 2012).

The Figure 12 shows the criterion used to obtain compliance from the data where the never, rarely and sometimes are used to signal non-compliance, while quite and very often are used to signal compliance of the 5 point Likert scale.

Never	Rarely	Sometimes	Quite often	Very often
Non-compliance			Compliance	

Figure 12: Compliance and no-compliance criterion.

The results for the questionnaire were analysed through simple comparisons and presented using the graphs and tables.

3.8 Limitations of the study

The limitation to the study are:

- The data contain, as much information as the respondent know.
- There are not many ICS cyber-security professional in South Africa as the profession is new; this limits the quality of the responses.
- Some respondents decided not to participate and so a larger number of respondents was initially sourced.
- The researcher could been seen as a nuisance. This was curbed by being as friendly as possible.
- Researcher did not have good listening skills, which is why all the interviews were recorded for future reference and notes were taken.
- To avoid disturbances to the interviews or surveys by the busy workplace, the meetings were scheduled as “busy” in the interviewee’s calendar and friendly reminders sent to respondents in surveys, at convenient times like end of day, lunchtime and after hours.
- Not all people could articulate their views, this is curbed by repeating the responses to confirm understanding.
- Snowball sampling could affect validity since the sampling will not be random.

3.9 Validity and reliability

3.9.1 *External validity*

External validity means the ability to generalise the findings (Bryman, 2012). The qualitative research is not intended to be generalizable by nature (Creswell, 2014). The studies will not be generalizable since the sample does not follow a random distribution with the use of snowball sampling.

3.9.2 *Internal validity*

Internal validity is the ability to measure the intended parameter (Bryman, 2012). For this research it is whether the questions are able to capture what cyber security methods the company is using. The selection of the respondents was such that they were knowledgeable to ensure that the questions were answered correctly. The questions are structured such that one construct is questioned by more than one question.

The validity of the information supplied was checked by sending the final report of findings to the interviewees for verification. Their comments were incorporated into the final report. The checking of transcripts for mistakes were also employed to improve validity. The results from similar responses were compared for triangulation purposes but could not be said for all responses as the research was semi-structured and responses were not the same.

3.9.3 *Reliability*

The definition of reliability is given by Bryman (2012, p. 169) as the “consistency of a measure of a concept”, this means that the results will not fluctuate over time or depending on who is observing. In this research, it means that if another person were to do the same research they would yield similar results. The selection of professional individuals for research question one will increase the reliability of the responses. Only interviewees with sound knowledge of the subject were chosen for research both research questions.

3.10 Demographic profile of respondents

The respondents for question one were four professionals. These were a senior ICS cyber-security researcher (PhD), an ICS cyber-security consultant, and two ICS cyber-security custodians (MSc Electrical Engineering). The gender, age and other demographic information was not necessary for this research. The respondents for question two were ICS knowledgeable personnel, which includes technicians, engineers, supervisors and artisans, these people interact with ICS on a day-to-day basis. The research side-lined people without internet or computer access for question two as it was administered through a web platform called Qualtrics ®.

CHAPTER 4. PRESENTATION OF RESULTS

4.1 Introduction

The results are presented using different methods, which are graphs, tables and text from respondents. This chapter presents responses from interviews first and then results from the survey.

4.2 Challenges experienced in substation cyber security in South Africa.

One interviewee alluded that government is currently the process of drafting the cyber-security legislation but not so many people are involved and are aware of the process. The draft legislation will require a lot of resources to implement and this means it will be difficult to implement since capacity building takes time. The legislation process did not receive the expected publicity.

When cyber-incidents are investigated, the victims are found to not have changed the default security credentials for their equipment, which should happen during commissioning.

There is no tradition of data custody in RSA, people do not collect and share data except in the banking industry. There are many problems involved with the ICS that are overlooked because of lack of understanding of ICS security.

The business case for cyber-security is difficult to make because in organizations, like in insurance the loss that comes with an event is not quantifiable until the event has transpired. This makes it difficult to justify in business terms where benefit and risk are in monetary terms. If a similar event has not happened in the past, it is almost impossible to quantify.

Intellectual property theft is on the increase where syndicates are looking to steal certain organization’s laptops to get the intellectual property, for sale or to commit other crimes. The user credentials to login to the organization networks are on

the laptops and these are important to steal information or launch an attack on an organization.

When designing systems for organizations, the highest (most cost effective) security level is specified. The segregation of systems with demilitarised zones (DMZ) is standard practice to ensure protection that in the event of a breach; the intruder will not have access to the rest of the network, but only the breached section.

There is a lack of ICS cyber-security experts in the country; one respondent suggested only two in the country. The systems and solutions that people sell are usually not what they are and if you are not an expert; you will never know. The solution providers take advantage of the people's lack of knowledge in the area to make money with solutions that are not sound.

The evolution of hardware for ICS has made them susceptible to PC viruses and these are introduced to the ICS mainly via USB flash drives and CD-ROMs. Viruses are generally crafted to attack specific systems, but there are some that just use up the computer resources and in turn slowdown or disable the intended device functions. A PC virus can affect an ICS if their architecture is similar and if the virus is meant to exhaust the computer resources.

Most organizations are not even thinking of making the system cyber-secure yet, they want to make it functional to start with and then look at cyber security in the future. The problem is if your design is not secure in the beginning, it might be difficult when you want to add additional functionality that requires it in the future. The architecture is very important.

The desired solution in ICS cyber-security is not always possible because businesses exist to make money and at some point, it does not make financial sense. The more robust solutions are costly and some companies even offer breach free solutions but at a price.

Since one interviewee's organization does not have their ICS information online, he thought that the issue of ICS cyber-security does not affect him.

The problem of people unaware of cybersecurity, the interviewee suggested that it was better if some people did not know what they were doing, and then the damage inflicted unknowingly is smaller than that inflicted by someone who knows. Argues though that he experienced that some older members on the electrical fraternity do not want to learn new things but the younger members are interested in learning the cyber-security issues. The cyber-security is a dynamic industry and requires continuous and fast learning to keep up.

One interviewee does not trust the information shared by the US-CERT, saying that because of the cyber-warfare that is at play, some crucial information might be omitted and only outdated and irrelevant information shared for the world to see. In light of this, the respondent recommends that RSA does its own research and not rely on the US-CERT for information.

There is a cost attached investigating and recording an incident, it is usually easier to just replace the equipment. Usually an original equipment manufacturer is invited to investigate the failure of the equipment and this creates a conflict of interest. There also might be some conflict of interest in calling the manufacturer to determine the cause of failure of his equipment. The culture of not documenting and reporting incidences was then attributed to this

One interviewee thought that the top leadership intervention was required to change the interest to learn about cyber-security in his organization. Most of the organizations do not have cybersecurity termination procedure.

The pace of legislating the cyber-security is slow, this was attributed to the lack of political will. The policy requires many skills in the cyber-space for it to be implemented. After the legislation of the policy, there is more work with putting the infrastructure and capacity building. The policy is a one address all issues in all the sectors involved in the cyberspace, for instance the policy that addresses espionage should not be the same with one that addresses cyber-warfare.

The lack of recording of ICS cyber-incidents is hampering people from sharing and knowing what is happening in the cyber-security arena. The Republic of South Africa does not mandate companies to report an incident to anybody, because there is no custodian and it is not mandatory to report. Organizations do

not report the incidences due to mainly fear of reputational damage, which is directly linked to brand equity.

The misnomer that IT concentrates on bandwidth and OT concentrates on availability is a common deign problem where every system should be designed to provide confidentiality, integrity and availability. Organizations that cannot afford the full functional automation with full security should not automate in the first place as its riskier that way.

The ICS cyber-security is still in its infant stage in South Africa, so there is a lot of “noise” in the industry, people sell products and solutions that does not necessarily serve their client’s purpose.

People generally do not implement the basic protection to their ICS; some just even leave the basic passwords that comes with the devices from the original equipment manufacturers.

Engineer built systems are generally not built for security or all other extras but built for functionality. The Engineers should consult the IT specialists when designing to get assistance on the security side of things, a good example is the Modbus system that was designed by engineers and lacks in security.

The organizations that have IT and OT networks coupled together don’t have control of their OT network as it is usually controlled by IT. The priorities for IT and OT are different, for in instance if the network is down IT can wait for Monday but OT requires that it gets fixed immediately otherwise there is no remote control of the plant.

The introduction of improved OT technology in ICS means that there is a need for the employee skills to be upgraded. This makes the older employees resist the new upgrade while younger employees are flexible with the learning.

The plants that are scattered around the country present a unique challenge to have the data collected available and controlled in one place. Internet is the only option with GSM networks transferring the data between control room and the plant. The encryption of the data is very important to ensure that no one else can

see the data that is being sent and that the data is not changed when it travels through the internet.

There are many challenges facing the ICS cyber-space in South Africa. The major challenge is the lack of legislation to guide role payers, most of the other challenge will be addressed if this is addressed. The other challenges are lack of data recording, there are attacks happening in organizations unknowingly, lack of awareness, lack of trust in information supplied on CERT sites, antagonism between IT and OT professionals and change management issues with the new technology. The challenges that South Africa is experiencing is unique, as they have long been solved in first world countries. Most of the challenges that South Africa is experiencing could be solved by a sound legislation as a basis.

While the rest of the world is solving current problems as reported on CERTs, South Africa is still stuck in the old trying to create the infrastructure. There is no telling the scale of the attacks and the amount of information that could have been leaked to the outside world and the financial loss caused by loss of competitive advantage or equipment and reputational damage.

4.3 The impact of the challenges in industry's ICS cyber-security in South Africa.

The number of 80 surveys were sent out and only 64 responded, but of those only 44 were used, and about 20 responses were not usable because the responses data were missing more that 20% data.

The age, sex, qualifications and other demographic information of respondents were not necessary for this research. The only demographic data of note was the industry type (Figure 13) and province (Figure 14) in which the organization is situated. The challenges presented here were obtained for literature review and some from the research question one.

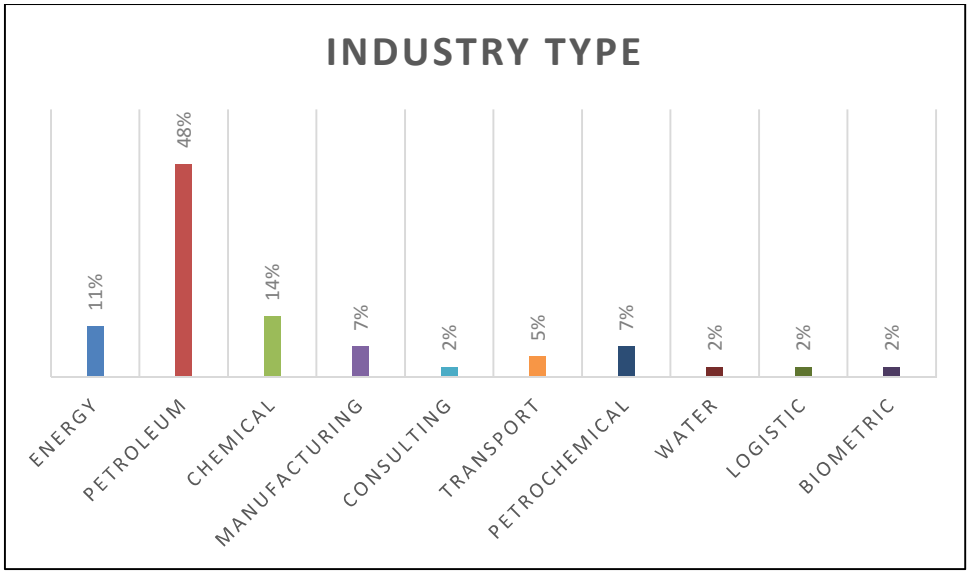

Figure 13: Responses classified per industry.

The Figure 13 shows the classified per industry where the petroleum industry has the most responses (at 48%), consulting, water and biometric industries recorded the least of 2%.

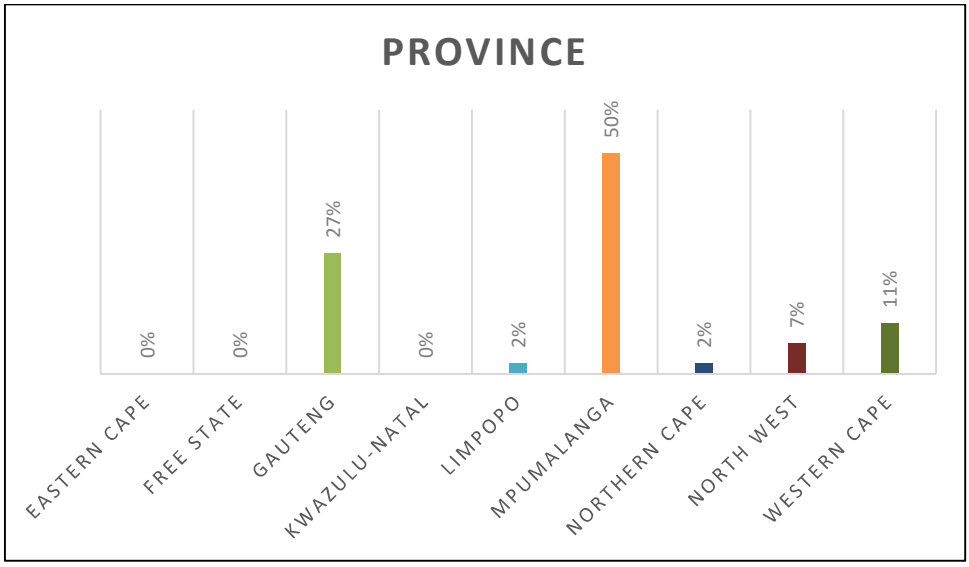

Figure 14: The responses across South African provinces.

The Figure 14 shows the respondents classified according to provinces in South Africa, most of the respondents were from Mpumalanga (with 50%) and there were no respondents from Eastern Cape, Free State and KwaZulu-Natal.

Most of the organizations in the sample size are fully automated (61%) with quite a few that are not automated at all (20%) as shown in Figure 15.

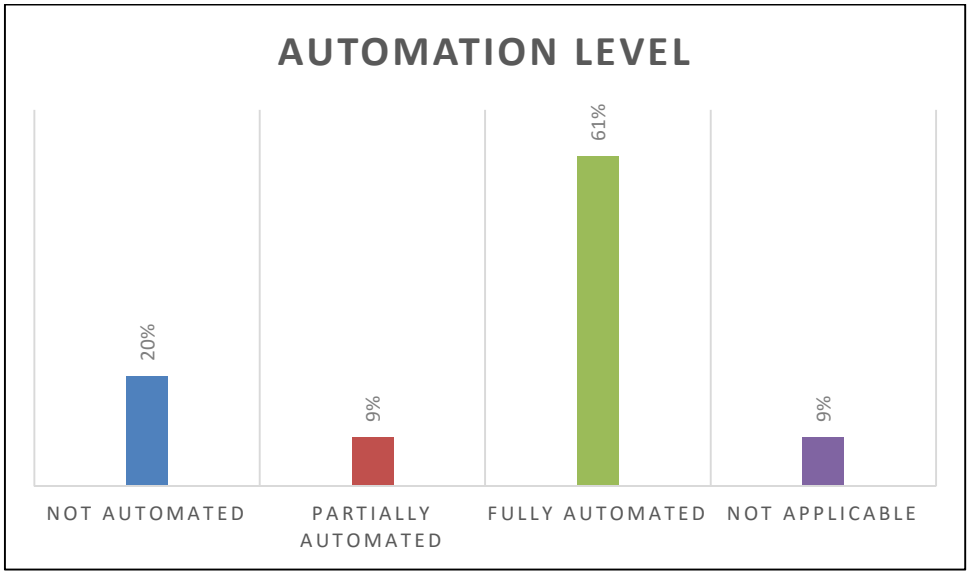

Figure 15: Automation level.

About 48% of the organizations have their ICS networks connected to the internet as shown in Figure 16.

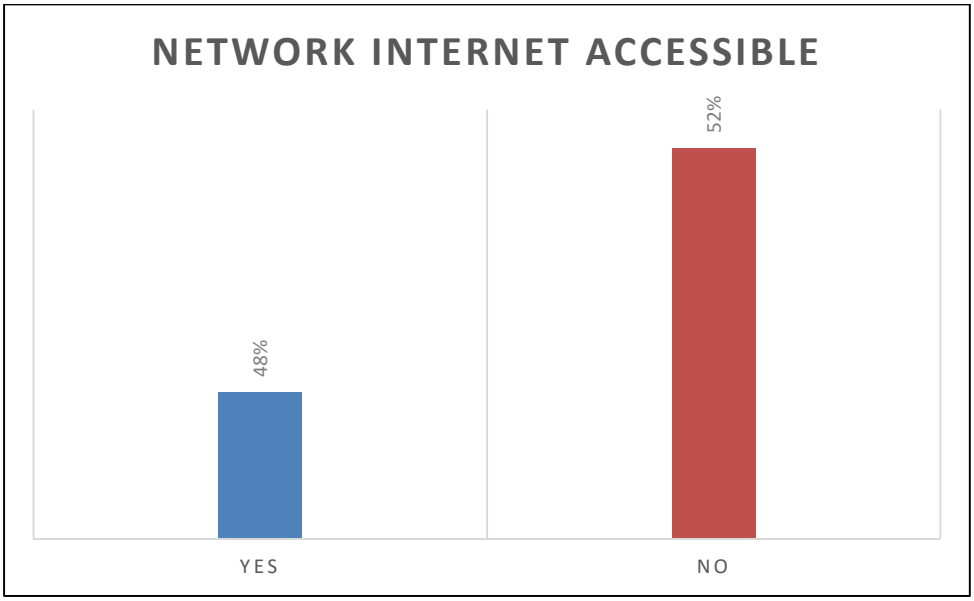

Figure 16: Network internet connectedness.

4.3.1 *Employee ICS cyber-security knowledge*

The results of the employee ICS cyber-security knowledge level are presented in Table 8.

Table 8: Employee ICS cyber-security knowledge.

	ICS	ICS Cyber-security	ICS Operation
Amateur	3	30	18
Developer	5	1	8
Professional	36	13	18

The results show that a large number of respondents (82%) have professional knowledge of ICS operation and 7% are amateurs as shown in Figure 17 and Figure 18. The majority of respondents are amateurs in ICS cyber-security (68%), only 2% are still learning the subject and about 30% claim to be professionals.

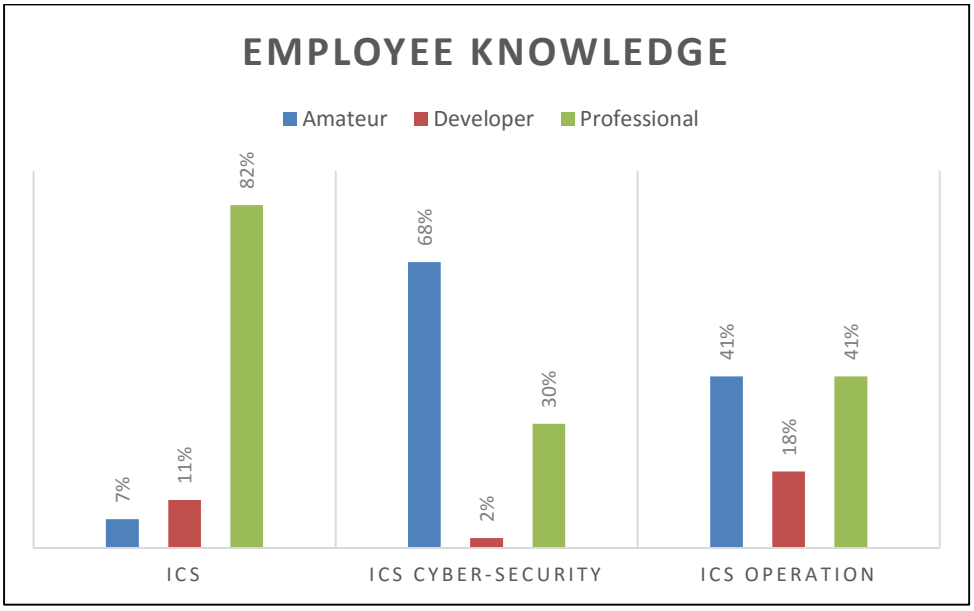

Figure 17: Employee skill profile (against skill).

There were 41% respondents who claimed to be professionals and 41% amateurs in the ICS normal operation and only 18% were still learning (as shown in Figure 17 and Figure 18).

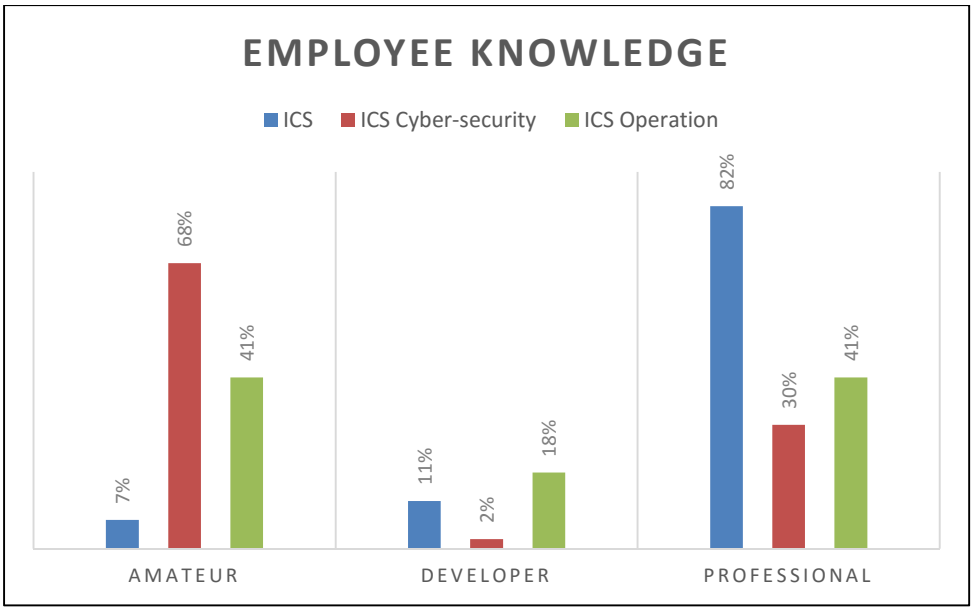

Figure 18: Employee skill profile (against skill level).

4.3.2 *Organizational ICS cyber-security behaviour*

The results for the organizational ICS behaviour are presented in Table 9.

Table 9: Organizational ICS behaviour results.

	Incident Recording	Software Tests	Memory Cleaning	Access Control	Security Review	Backup & Recovery	Service provider accompaniment	Policy Enforcement	Education	Employee awareness	Incident Reporting	Service Provider Awareness
Never	10	2	5	2	3	2	2	3	5	3	6	2
Rarely	18	9	14	5	7	7	7	2	6	8	4	2
Sometimes	12	8	17	7	15	4	10	11	9	8	11	12
Quite often	3	20	6	18	11	15	10	15	15	13	16	12
Very often	1	5	2	12	8	16	14	12	8	11	6	15

Most organizations confirm that they rarely experience cyber-security incidents and only one respondent said that they experienced them quite often. Most organizations claim that they test software quite often and only 2 organizations never test their software at all (5%) as shown in Figure 19 and Figure 20. There

is quite a number of organizations who rarely and sometimes erase the memory of devices before disposal (32%).

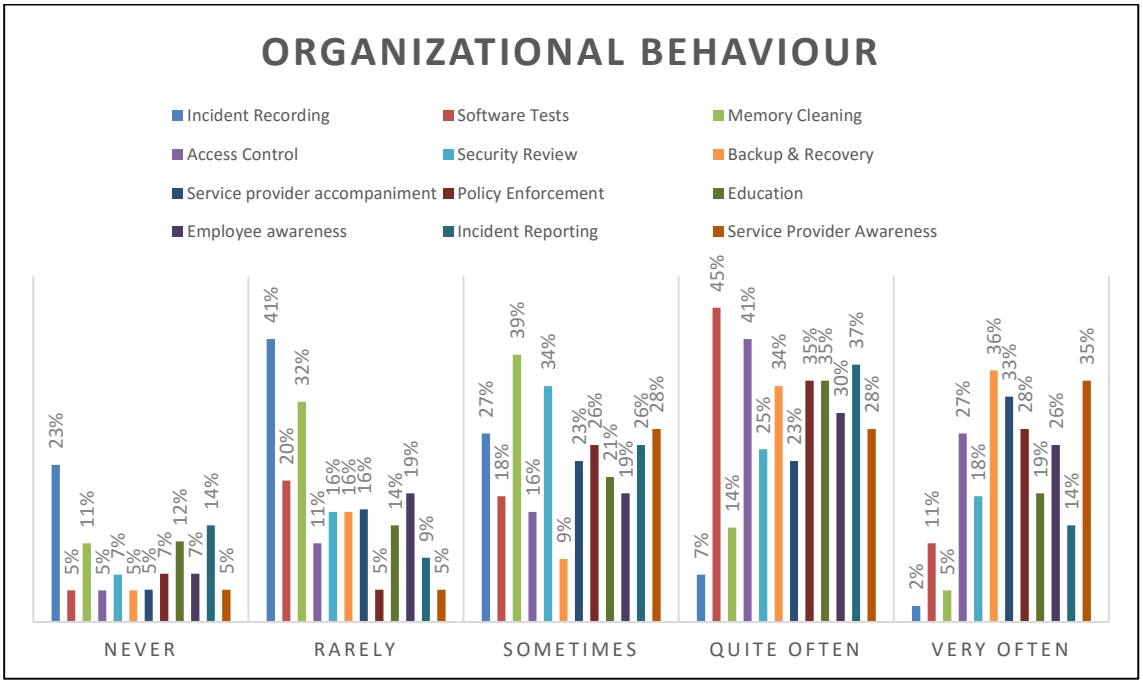

Figure 19: Organizational ICS behaviour (against 5-point Likert scale).

Most organizations very often accompany their service providers while performing a service for them, quite often enforce the ICS policies, quite often educate their staff on ICS security, quite often report cyber incidents and very often provide service provider awareness to cyber-security as shown in Figure 19 and Figure 20.

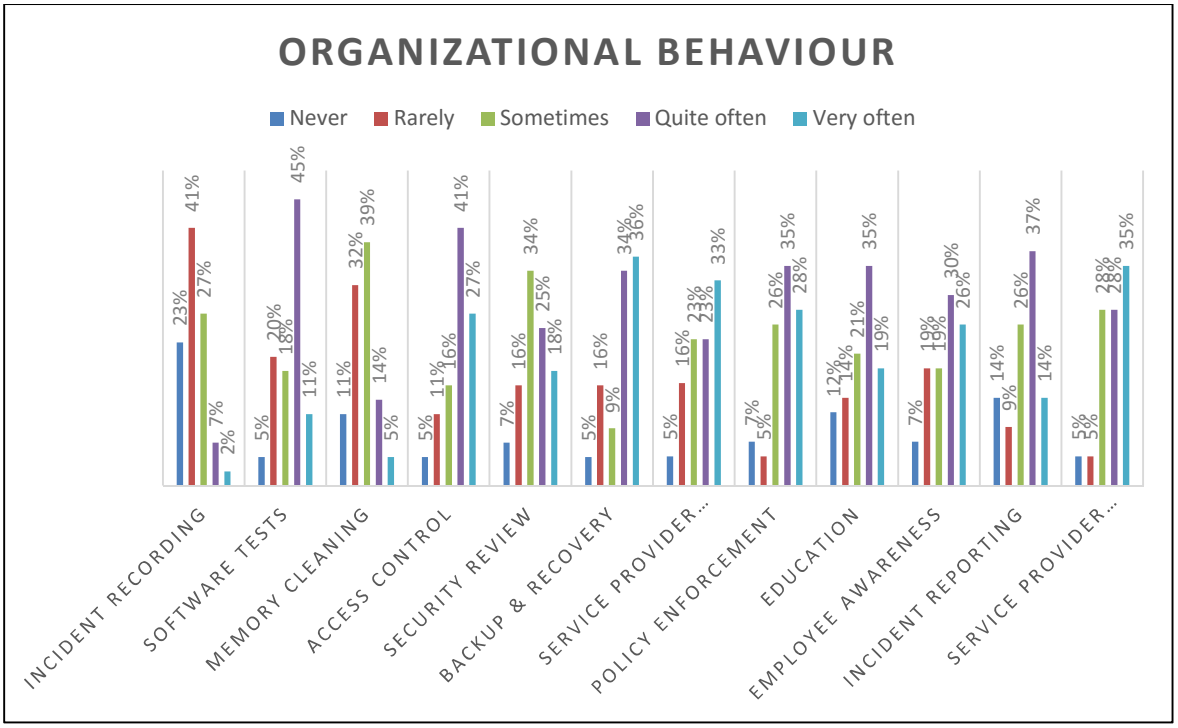

Figure 20: Organizational ICS behaviour (against behaviour).

Most organizations enforce separation of duties to employees, control access to ICS, log user events, log equipment operations, secure and monitor ICS connections.

4.3.3 *Compliance*

The responses to the organizational behavioural questions shown in Figure 19 were then classified as compliance and non-compliance where the often answers were classified as compliance and anything else as non-compliance (shown in Figure 12). The compliance data is given in Table 10 and visually presented in Figure 21 and Figure 22.

Table 10: Compliance level response data.

	Incident Recording	Software Tests	Memory Cleaning	Access Control	Security Review	Backup & Recovery	Service provider accompaniment	Policy Enforcement	Education	Employee awareness	Incident Reporting	Service Provider Awareness
Compliance	4	25	8	30	19	31	24	27	23	24	22	27
Non-compliance	40	19	36	14	25	13	19	16	20	19	21	16

The implementation of backup and recovery is their most compliant activity at 70%. The rest of the compliance levels range between 43%-68% accept for incident recording (9%) and memory cleaning for ICS that is replaced (18%). The overall compliance rate is 51% on average.

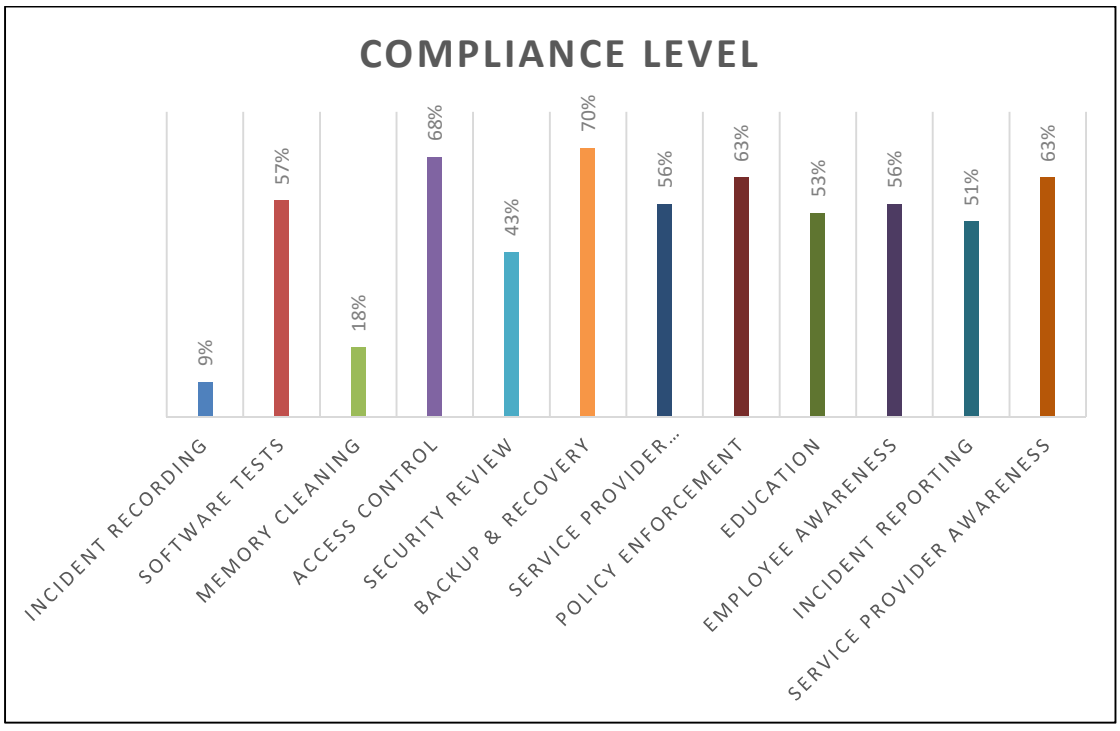

Figure 21: Organizational ICS cyber-security compliance level.

The non-compliance is the opposite of compliance, shown in Figure 22. The overall non-compliance is 49%.

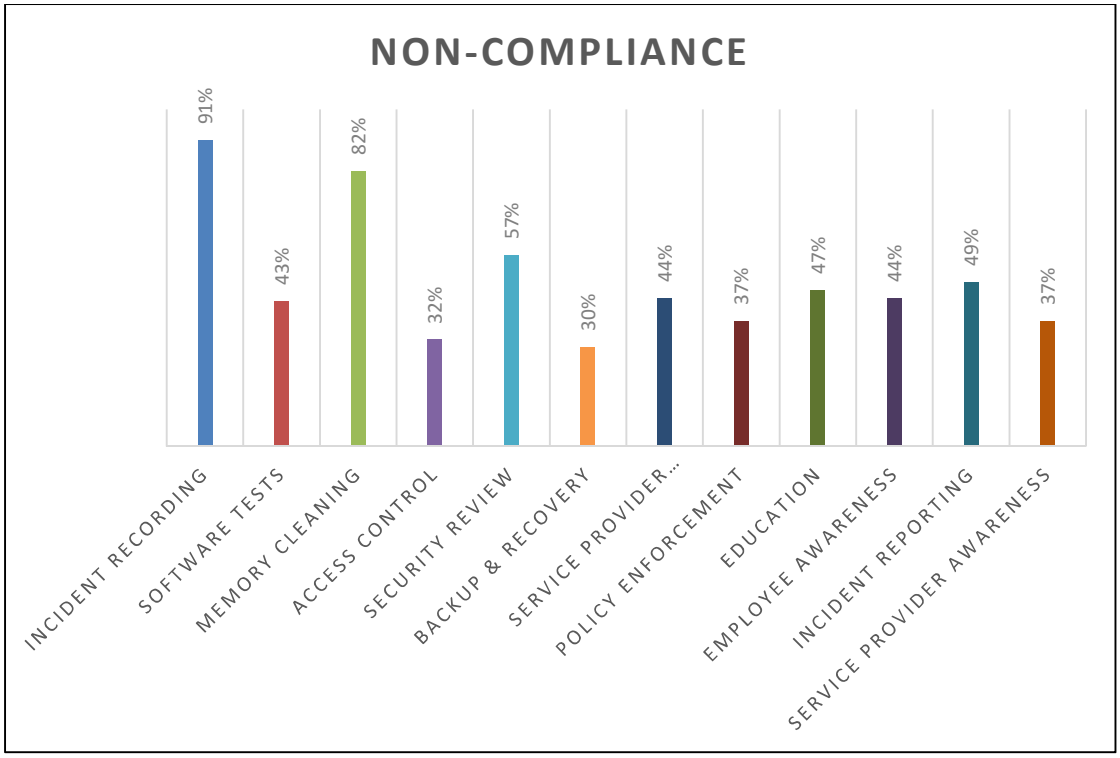

Figure 22: Organizational ICS cyber-security non-compliance level.

The non-compliance exceed compliance in the cyber-security incident recording (91%), memory cleaning (82%) and holding security reviews (57%) as shown in Figure 23.

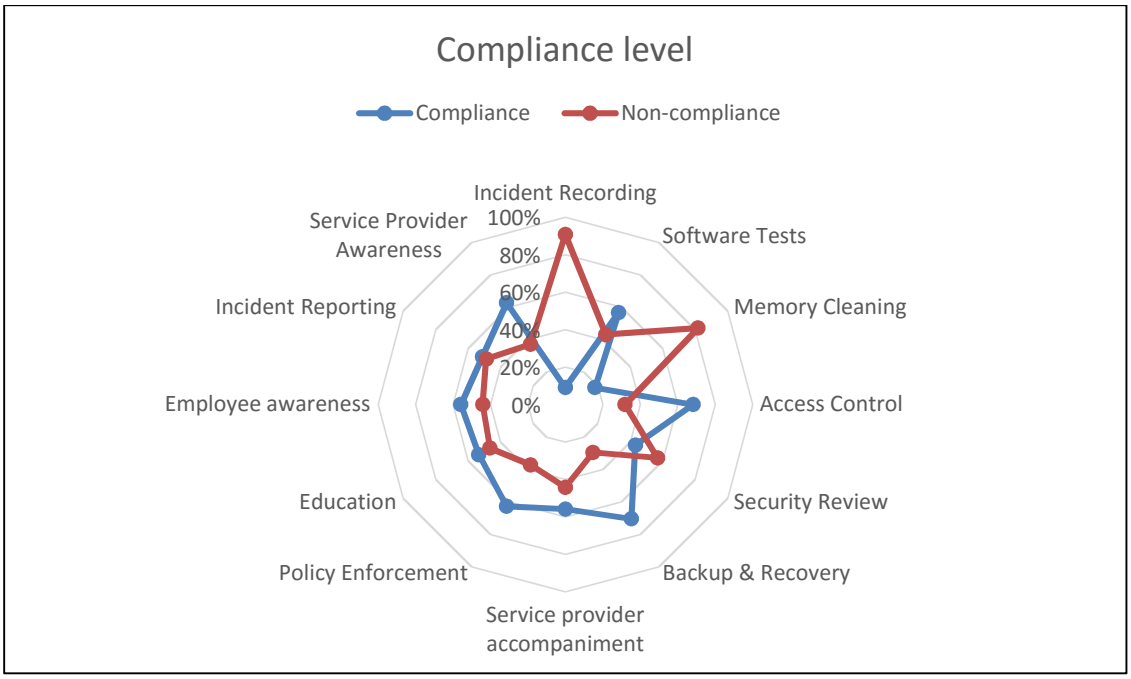

Figure 23: Compliance level (spider diagram).

South African industry is more skilled in the ICS normal operation but lacking in the ICS cyber-security The industry is about 51% compliant to the best practices.

4.4 Summary of the results

Most respondents echoed the lack of legislation together with the reporting of incidents as the hindrance to improved ICS cyber security. The organizations also ignore cyber-related incidents due to lack of knowledge on the subject and due to the fact that finding the root cause is more expensive. The business case for ICS cyber-security is very difficult to justify due to lack of data on previous incident and because the impact is usually unknown until incident occurs.

Most organizations in South Africa are not at the level of worrying about cyber-security yet, they are preoccupied with trying to make the system work in the first place. The people have the tendency of not implementing the basic security in their ICS.

The knowledge of the respondents is strong in the ICS, followed by the operation of ICS and least in ICs cyber-security. The organizational ICS behaviour is strong in backing up and recovery followed by the provision of ICS awareness to service providers and the least is the recording of incidents. The 51% of organizations are compliant with the best practices in ICS cyber-security.

CHAPTER 5. DISCUSSION OF THE RESULTS

5.1 Introduction

This chapter discuss the results and contrasts them with the literature review. The chapter first discusses the challenges that are experienced in South Africa and then the perceptions that the industry has on the specified challenges then follows. The chapter is the concluded by the conclusion of the results.

5.2 Challenges experienced in substation cyber security in South Africa.

While the world is reacting to attacks, South Africa is still trying to have a policy that defines the ground rules in the cyber-space. The world is also trying to improve the security in research and designs while in South Africa we are trying to have a solution that just functions in the first place.

The cyber-security legislation is regarded as the point of departure in cyber-security in South Africa as it defines the types crimes and their prosecution, the response and the role players. The ongoing process of drafting the legislation process was not publicised extensively, even though some stakeholders were requested to comment, certain role players might not have given their input and that could lead to a biased or incomplete legislation. The other view was that the legislation was too general and needed to be subdivided to the different components where for example the cyber-warfare legislation should not be the same with the phishing legislation.

The legislation does not make mention of OT, it is only structured for IT. The legislation in its draft format requires a variation of skills and South Africa faces a challenge to build the skills capacity required. There is currently no tradition of data custody, this will be addressed with the current draft legislation, where ICS-CERT will collect the data and respond to incidents.

Cyber-security's existence is difficult to prove to decision makers in organizations, to prove this, one of the respondents set up a virtual plant with decent security.

The general the lack of cyber-security professionals and the lack of understanding in organizations in South Africa exposes the organizations to solutions that might not work, where people are taking advantage.

The development of common communication protocols means that the OT is similar to IT equipment and that means that the OT equipment is susceptible to IT dedicated attacks. This means that the owners of OT equipment will have to keep their ears on the ground for vulnerabilities and patches concerning their equipment.

The South African situation where most of the organizations are not looking at cyber-security yet but still looking at the functionality of equipment, presents a unique challenge in this global world. The fact that cyber-crime has no jurisdiction, makes it most susceptible to attacks and the reason that there have been no major incidents reported is amazing. The reason South Africa is surviving could be that the suppliers of ICS equipment have an idea of what is going on with cyber-security since they are global, thus supply secure systems to organizations unknowingly.

The justification of cyber-security is difficult but the organizations are upgrading by default when they replace equipment and not including it in the justification, which leads to misclassification of the capital part of the renewal and thus have misrepresentation of tax in the organization’s books. The reputation cost that can result from cyber-event can be regarded as priceless as in some industries it could mean the break of a company where competitors can take over. The standard security should be a minimum to prevent this.

The fact that the organizational data is not accessible online does not exonerate the organization from implementing sound cyber security measures, as they are still susceptible to internal attacks and might want to make the data available in the future.

The reasons that many organizations do not report and investigate incidents are justified as cost and the fear of organizational reputational damage.

Most organizations do not have cyber-security linked termination procedure, this leaves them vulnerable to sabotage attacks. This is usually perpetrated by disgruntled employees or serving resignation notice employees.

5.3 The impact of the challenges to the industry's ICS cyber-security

The sample size yielded a 61% automation level with the respondents and 9% did not know if they were automated or not and gave the response of not applicable. This means that most of the organizations have a reason to be concerned about cyber-security s they are more susceptible to external attacks.

The reason there has not been devastating incidents reported could be partly because when organizations contract the service providers to design their systems, they usually employ the most secure systems by default. This explains why there has not been reports of incidents in the newly installed systems and less because people know what they are doing in ICS cyber-security.

The level of automation means that most of the organizations are susceptible to cyber-security incidents since they are automated.

5.3.1 *Employee ICS cyber-security knowledge*

The employee knowledge on ICS and cyber-security is important if the ICs is to be kept secure from cyber-crime incidents. The responses show that the employees are professionals in ICS (at 82%), but as expected only 30% are experts in ICS cyber-security.

5.3.2 *Organizational ICS cyber security behaviour*

Most organizations claim that they rarely experience cyber-incidents; this is in agreement with the fact that South Africa does not report incidents and the lack of awareness on the subject of cyber-security.

5.3.3 *Compliance*

Most companies implement backup and recovery processes for their ICS software at 70%. The access control also tops on activities that organizations are more compliant on.

The overall compliance of 51% means that the organizations in South Africa are compliant as much as they are not compliant with the best practices in ICS cyber security. The organizations are oblivious to the existence of attacks in their organizations.

5.4 Conclusion

There are many challenges facing the ICS cyber-space in South Africa. The major challenge is the lack of legislation to guide role payers, the other challenge will be addressed if this is addressed. The other challenges are lack of data recording, there are attacks happening to organizations unknowingly, lack of awareness, lack of trust in information supplied on CERT sites, antagonism between IT and OT professionals and change management issues with the new technology. The challenges that South Africa is experiencing is unique, as they have long been solved in first world countries. Most of the challenges that South Africa is experiencing can be solved by a sound legislation.

While the rest of the world is solving current problems as reported on CERTs, South Africa is still stuck in the old trying to create the infrastructure. There is no telling the scale of the attacks and the amount of information that could have been leaked to the outside world and the financial loss caused by loss of competitive advantage or equipment and reputational damage.

South African industry is more skilled in the ICS normal operation but lacking in the ICS cyber-security. The organizations are oblivious to the existence of attacks in their organizations, most of the organizations claim that they mostly have not experienced any cyber-activity, this could be attributed to the lack of knowledge on what constitutes cyber-activity because they manifest as normal equipment malfunction. This is deduced from the trap systems that have been setup and the

other more secure nations are experiencing. The industry is about 51% compliant to the best practices, this shows that for a country without a cyber-security legislation and does not record incidences, it is doing reasonably well.

Most organizations have their processes automated so have a cause for concern in ICS cyber security. The low level of ICS knowledge amongst ICS professionals is concerning because for them to protect the ICS network, they need to know what they are protecting it from. Generally, organizations are compliant with the good ICS cyber-security practice.

CHAPTER 6. CONCLUSIONS & RECOMMENDATIONS

6.1 Introduction

This chapter present the conclusions of the research to find the challenges affecting ICS cyber-security in South Africa. The chapter first presents the conclusion, then recommendations and then lastly presents the suggestions for future research.

6.2 Conclusions of the study

There are many challenges facing the ICS cyber-security in South Africa, the main of which is the lack of legislation. The other challenges are addressable with the introduction of the cyber-crime and cyber-security legislation. This therefore means that the draft legislation is a point of departure in securing the ICS cyber-space.

South African industry is more skilled in the ICS normal operation but lacking in the ICS cyber-security. The organizations are oblivious to the existence of attacks in their organizations, most of the organizations claim that they mostly have not experienced any cyber-attack, this could be attributed to the lack of knowledge on what constitutes cyber-activity because they usually manifest as normal equipment malfunction. The industry is about 51% compliant to the best practices, this shows that for a country without a cyber-security legislation and does not record incidences, it is doing reasonably well.

The challenges that South Africa is experiencing are the ones experienced by the rest of the world and more because while the rest of the world is looking at the latest cyber-attacks, South Africa is still susceptible to the old ones.

6.3 Recommendations

The business decision makers, managers and owners could use the information on the prevalence of attacks and the level of compliance to approve the

applications for increased cyber-security. The success of the government and organizational awareness campaigns is very low as not many professionals are aware of the ICS cyber security, what more the non-professionals.

The general understanding of what constitutes a cyber-incident is contained in this document and anyone can now be educated on the subject. The ignorance of the existence of the cyber-crime in the ICS could be outdated with this research.

This should be motivation enough for the drivers of the cyber-security and cyber-crime Bill to increase the momentum of making the Bill to Law.

6.4 Suggestions for further research

The generalizability of the results could be improved by increased reach on the surveys to cover the rest of the provinces even though the economic activities are not distributed evenly.

The reason why there are not many high impact cyber-incidents is not understood when all the data says that the cyber-security in South Africa, this is an area for studying.

REFERENCES

Adar, E., & Wuchner, A. (2005, 3-4 Nov. 2005). *Risk management for critical infrastructure protection (CIP) challenges, best practices & tools.* Paper presented at the Critical Infrastructure Protection, First IEEE International Workshop on.

Axelrod, C. W. (2013, 3-3 May 2013). *Managing the risks of cyber-physical systems.* Paper presented at the Systems, Applications and Technology Conference (LISAT), 2013 IEEE Long Island.

Ayofe, A. N., & Oluwaseyifunmitan, O. (2009). Towards Ameliorating Cybercrime and Cybersecurity. *International Journal of Computer Science and Information Security (IJCSIS), 3*(1), 1-11.

Bada, M., Creese, S., Goldsmith, M., Mitchell, C., & Phillips, E. (2014). Computer Security Incident Response Teams (CSIRTs) An Overview.

Bohme, R., & Moore, T. (2012, 23-24 Oct. 2012). *How do consumers react to cybercrime?* Paper presented at the eCrime Researchers Summit (eCrime), 2012.

Boyes, H. (2015, 2-3 Feb. 2015). *Best practices in an ICS environment.* Paper presented at the Cyber Security for Industrial Control Systems.

Bryman, A. (2012). *Social research methods*: Oxford university press.

Byres, E., & Lowe, J. (2004). *The myths and facts behind cyber security risks for industrial control systems.* Paper presented at the Proceedings of the VDE Kongress.

Cardenas, A., Amin, S., Sinopoli, B., Giani, A., Perrig, A., & Sastry, S. (2009). *Challenges for securing cyber physical systems.* Paper presented at the Workshop on future directions in cyber-physical systems security.

Cárdenas, A. A., Radosavac, S., Grossklags, J., Chuang, J., & Hoofnagle, C. J. (2009). *An economic map of cybercrime*.

Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004). *The economic impact of cyber-attacks*.

CERT. (2015). *INCIDENT RESPONSE/VULNERABILITY COORDINATION IN 2014*. Retrieved from https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf: https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf

Chipley, M. (2014, 23 October 2014). Cybersecurity. Retrieved from http://www.wbdg.org/resources/cybersecurity.php

Creery, A., & Byres, E. (2005). *Industrial cybersecurity for power system and SCADA networks.* Paper presented at the Petroleum and Chemical Industry Conference, 2005. Industry Applications Society 52nd Annual.

Creswell, J. W. (2003). *Research design: Qualitative, quantitative, and mixed methods approaches*: Sage publications.

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (S. Publications Ed. 4 ed.): Sage publications.

Cyercrime and Cybersecurity Bill - Draft for public comment, xx, DEPARTMENT OF JUSTICE AND CORRECTIONAL SERVICES 128 (2015).

Daniels, R. (2007). Skills shortages in South Africa: A literature review.

Dlamini, I. Z. (2012). *Cyber Security Awareness Initiatives in South Africa: A Synergy Approach*. Retrieved from http://researchspace.csir.co.za/dspace/bitstream/10204/5941/1/Dlamini_2012.pdf: http://researchspace.csir.co.za/dspace/bitstream/10204/5941/1/Dlamini_2012.pdf

Dlamini, M., Eloff, J. H., & Eloff, M. M. (2009). Information security: The moving target. *Computers & Security, 28*(3), 189-198.

Dlamini, Z., & Modise, M. (2013). Cyber security awareness initiatives in South Africa: A synergy approach. *Case Stud. Inf. Warf. Secur. Res. Teach. Stud*, 1.

ECSA. (2014). *National Engineering Skills Survey*. Retrieved from Website: https://www.ecsa.co.za/news/Surveys%20PDFs/200215_ECSA_National_Engineering_Skills_Survey_Report_April_2014.pdf

FBI. (2014). *2014 Internet Crime Report*. Retrieved from https://www.fbi.gov/news/news_blog/2014-ic3-annual-report: https://www.fbi.gov/news/news_blog/2014-ic3-annual-report

Flynn, L., Huth, C., Trzeciak, R., & Buttles, P. (2012). *Best practices against insider threats for all nations.* Paper presented at the Cybersecurity Summit (WCS), 2012 Third Worldwide.

GICSP, E. H., Assante, M., & Conway, T. (2014). An Abbreviated History of Automation & Industrial Controls Systems and Cybersecurity.

Goff, E., Glantz, C., & Massello, R. (2014). *Cybersecurity procurement language for energy delivery systems.* Paper presented at the Proceedings of the 9th Annual Cyber and Information Security Research Conference.

Group, P. C. (2015). *Manage industrial control system lifecycle*. Retrieved from http://www.cpni.gov.uk/Documents/Publications/2015/12-May-2015-3.%20Manage%20ICS%20Lifecycle%20Final%20v1.0.pdf

Guyette, S. (1983). *Community-based research: A handbook for Native Americans*: Amer Indian Studies Center.

IEEE. (2000). IEEE Guide for Electric Power Substation Physical and Electronic Security. *IEEE Std 1402-2000*, i. doi:10.1109/IEEESTD.2000.91305

IEEE. (2008). IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities. *IEEE Std 1686-2007*, 1-22. doi:10.1109/IEEESTD.2008.4453853

ISO, & IEC. (2005). IEC 27001: Information technology–Security techniques–Information security management systems–Requirements: ISO/IEC.

Jonker, M. (2015, 22 July 2015). South African business slow to embrace automation. Retrieved from http://www.grantthornton.co.za/de/insights/articles/south-african-business-slow-to-embrace-automation/

Kargl, F., van der Heijden, R. W., Konig, H., Valdes, A., & Dacier, M. C. (2014). Insights on the Security and Dependability of Industrial Control Systems. *Security & Privacy, IEEE, 12*(6), 75-78. doi:10.1109/MSP.2014.120

Kozik, R., & Choras, M. (2013, 23-25 Sept. 2013). *Current cyber security threats and challenges in critical infrastructures protection.* Paper presented at the Informatics and Applications (ICIA),2013 Second International Conference on.

Lee, E. (2008). *Cyber physical systems: Design challenges.* Paper presented at the Object Oriented Real-Time Distributed Computing (ISORC), 2008 11th IEEE International Symposium on.

Luiijf, E. (2008). SCADA Security Good Practices for the Drinking Water Sector. *TNO, The Hague, TNO-DV*, C096.

Luiijf, H., & te Paske, B. (2015). Cyber Security of Industrial Control Systems.

Macaulay, T., & Singer, B. L. (2011). *Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS*: CRC Press.

McDonald, J. D. (2012). *Electric power substations engineering*: CRC press.

Nye Jr, J. S. (2011). *Nuclear lessons for cyber security*. Retrieved from

Pack, W. (2012). *2012/3: The South African Cyber Threat Barometer*. Retrieved from https://www.wolfpackrisk.com/SA%202012%20Cyber%20Threat%20Barometer_Medium_res.pdf: https://www.wolfpackrisk.com/SA%202012%20Cyber%20Threat%20Barometer_Medium_res.pdf

Parliament. (2016). How Law is Made. Retrieved from http://www.parliament.gov.za/live/content.php?Item_ID=1843

Pearson, I. L. (2011). Smart grid cyber security for Europe. *Energy Policy, 39*(9), 5211-5218.

Podbregar, I., & Podbregar, M. F. (2012, 26-29 Aug. 2012). *Critical Infrastructure and Internal Controls.* Paper presented at the Advances in Social Networks Analysis and Mining (ASONAM), 2012 IEEE/ACM International Conference on.

Pool, C. (2014, 15 July 2014). Cyber security protection industrial control systems. *EngineerIT*.

RISI. (2015). Repository of Industrial Security Incidents. Retrieved 23 June 2015 http://www.risidata.com/Database

Shim, J. K., & Siegel, J. G. (2010). *Dictionary of accounting terms*: Barron's Hauppauge, NY.

SSA. (2011). *Draft National Cybersecurity Policy Framework For South Africa*. Retrieved from https://www.google.co.za/search?newwindow=1&site=&source=hp&q=Draft+National+Cybersecurity+Policy+Framework+For+South+Africa&oq=Draft+National+Cybersecurity+Policy+Framework+For+South+Africa&gs_l=hp.3..0i22i30.1378.1378.0.2345.2.2.0.0.0.0.809.1114.3-1j6-1.2.0.msedr...0...1c.1.62.hp..1.1.302.0.dFw0i0S0lPI: https://www.google.co.za/search?newwindow=1&site=&source=hp&q=Draft+National+Cybersecurity+Policy+Framework+For+South+Africa&oq=Draft+National+Cybersecurity+Policy+Framework+For+South+Africa&gs_l=hp.3..0i22i30.1378.1378.0.2345.2.2.0.0.0.0.809.1114.3-1j6-1.2.0.msedr...0...1c.1.62.hp..1.1.302.0.dFw0i0S0lPI

Stouffer, K., Falco, J., & Scarfone, K. (2008). Guide to industrial control systems (ICS) security. *NIST Special Publication, 800*(82), 16-16.

Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to industrial control systems (ICS) security. *NIST Special Publication*, 800-882.

Uma, M., & Padmavathi, G. (2013). A Survey on Various Cyber Attacks and their Classification. *IJ Network Security, 15*(5), 390-396.

Wang, W., & Lu, Z. (2013). Cyber security in the Smart Grid: Survey and challenges. *Computer Networks, 57*(5), 1344-1371.

Wen, Y., & Qianchuan, Z. (2014, 8-10 Aug. 2014). *Cyber security issues of critical components for industrial control system.* Paper presented at the Guidance, Navigation and Control Conference (CGNCC), 2014 IEEE Chinese.

Zurich, E. T. H. (2015, 15 April 2010). The Viking Project. Retrieved from http://control.ee.ethz.ch/~viking/

APPENDIX A

Actual research instrument

Q1 Informed Consent Form

Introduction

This study is conducted as a Research Project for Wits Business School Masters in Business Administration studies. Its intention is to find the compliance to best practice in Industrial Control Systems (ICS) cyber-security.

Procedures

You will be asked questions about organizational and your behaviour and systems that are in place to cyber-secure the ICS in your organization. The questionnaire consists of 13 questions and will take approximately 15 minutes or less. This questionnaire will be conducted with an online Qualtrics ®-created survey.

Risks/Discomforts

Risks are minimal for involvement in this study. Although we do not expect any harm to come upon any participants due to electronic malfunction of the computer, it is possible though extremely rare and uncommon.

Benefits

There are no direct benefits for participants, except by a copy of the report when completed. However, it is hoped that through your participation, researchers will learn more about the level of compliance to best practices in South Africa.

Confidentiality

All data obtained from participants will be kept confidential and will only be reported in an aggregate format (by reporting only combined results and never reporting individual ones). All questionnaires will be concealed, and no one other than then primary investigator and assistant researches listed below will have access to them. The data collected will be stored in the HIPPA-compliant, Qualtrics ®-secure database until it has been deleted by the primary investigator.

Compensation

There is no direct compensation, however, participants may earn extra academic credit, at the discretion of their professors.

Participation

Participation in this research study is completely voluntary. You have the right to withdraw at any time or refuse to participate entirely. If you desire to withdraw, please close your internet browser and notify the principal investigator at this email: mutizec@gmail.com.

Questions about the Research

If you have questions regarding this study, you may contact (principal investigator), at +27 72 581 3961.

Questions about your Rights as Research Participants

If you have questions, you do not feel comfortable asking the researcher, you may contact the supervisor Antony Soicher from Wits Business School at antony@wbs.soicher.net.

Definitions

ICS - Industrial Control System, components of which include DCS, PLC, SCADA, Protection Relays and other IEDs.

Q2 I have read, understood, and printed a copy of, the above consent form and desire of my own free will to participate in this study.

- ❍ Yes (1)
- ❍ No (2)

If No Is Selected, Then Skip to End of Survey

Q3 Which of the following best describes the industry your organization is in?

- ❍ Energy (1)

- ❍ Petroleum (2)
- ❍ Chemical (3)
- ❍ Manufacturing (4)
- ❍ Consulting (5)
- ❍ Transport (6)
- ❍ Petrochemical (7)
- ❍ Water (8)
- ❍ Logistic (9)
- ❍ Biometric (10)

Q4 Which province is your organization situated?

- ❍ Eastern Cape (1)
- ❍ Free State (2)
- ❍ Gauteng (3)
- ❍ KwaZulu-Natal (4)
- ❍ Limpopo (5)
- ❍ Mpumalanga (6)
- ❍ Northern Cape (7)
- ❍ North West (8)
- ❍ Western Cape (9)

Q5 What is your level of knowledge of

		Amateur (1)	Developer (2)	Professional (3)
5_1	Industrial Control Systems (PLC, SCADA, RELAYS, DCS)? (1)	❍	❍	❍
5_2	Cyber-security in ICS? (2)	❍	❍	❍
5_3	Normal ICS operation? (3)	❍	❍	❍

Q6 What is the level of automation of your ICSs?

		Not automated (1)	Partially automated (2)	Fully automated (3)	Not applicable (4)
6	Automation (1)	❍	❍	❍	❍

Q7 Do you have an externally accessible network for organization's ICS?

❍ Yes (1)
❍ No (2)

Q9 How often does your organization?

		Never (1)	Rarely (2)	Sometimes (3)	Quite Often (4)	Very Often (5)
9_1	Experience cyber-security incidents? (1)	❍	❍	❍	❍	❍
9_2	Test software on ICS? (2)	❍	❍	❍	❍	❍
9_3	Erase memory on redundant ICSs? (3)	❍	❍	❍	❍	❍
9_4	Implement controlled access to ICS? (4)	❍	❍	❍	❍	❍
9_5	Hold security reviews on ICS? (5)	❍	❍	❍	❍	❍
9_6	Implement secure backup and recovery process? (6)	❍	❍	❍	❍	❍

Q10 Does your organization implement access control on ICS?

❍ Yes (1)
❍ No (2)

Q11 Does your organization have a cyber-security centred employee termination procedure?

- ❍ Yes (1)
- ❍ No (2)

Q12 How often does your organization?

		Never (1)	Rarely (2)	Sometimes (3)	Quite Often (4)	Very Often (5)
12_1	Accompany service providers working on your equipment? (1)	❍	❍	❍	❍	❍
12_2	Enforce ICS policies? (2)	❍	❍	❍	❍	❍
12_3	Educate staff on ICS security? (3)	❍	❍	❍	❍	❍
12_4	Create cyber-security awareness to employees? (4)	❍	❍	❍	❍	❍
12_5	Report ICS incidences? (5)	❍	❍	❍	❍	❍
12_6	Know what service providers do on your equipment? (6)	❍	❍	❍	❍	❍

Q13 Does your organization?

		Yes (1)	No (2)
13_1	Enforce the separation of duties? (1)	❍	❍
13_2	Control and monitor access to ICS? (2)	❍	❍
13_3	Log users' events on ICS? (3)	❍	❍
13_4	Log equipment operations? (4)	❍	❍
13_5	Secure and monitor ICS connections? (5)	❍	❍

APPENDIX B

Table 11: The icebreaker questions for interview.

1	Q	How much do you know about cybersecurity in the ICS?
	A	
2	Q	Have you experienced any cyber-security incidents in your career in South Africa?
	A	
3	Q	Do you think Cyber-Security on ICS is an issue in South Africa and Why?
	A	
4	Q	The draft legislation on ICS cybersecurity is out on comments. Do you think that the delay in the Legislation is an issue in South Africa and why?
	A	
5	Q	Literature says that it is difficult to motivate the business case because it is usually based on losses incurred and not potential loss. Is motivating the business case for cyber-security an issue and why?
	A	
6	Q	There is a lack of reporting of ICS cyber-security incidents evidenced by a non-functional response team and the world data. What do you attribute the lack of reporting on incidents in South Africa, compared to the rest of the world?
	A	
7	Q	What is perception on the level of awareness of ICS cybersecurity in South Africa and why?
	A	
8	Q	Have you encountered the conflict between IT and OT on what they think ICS cybersecurity is?
	A	
9	Q	What are your views on the ICS cyber-security skills availability in South Africa?

	A	
10	Q	Are they any design issues you have encountered while designing for cyber-security?
	A	
11	Q	Are there any construction and commissioning issues you have encountered?
	A	
12	Q	What are the other issues on ICS cyber-security have you encountered.
	A	

Table 12: survey questions with variable

Question #	Variable Name	Variable Group	Type	Research Question
Q1			Categorical	
Q2			Categorical	
Q3	Industry Type	Industry	Categorical	
Q4	Province	Location	Categorical	
Q5_1	ICS	User knowledge	Ordinal	2a
Q5_2	ICS Cyber-security		Ordinal	2a
Q5_3	ICS Operation		Ordinal	2a
Q6_1	Automation Level	Automation level	Ordinal	
Q7	Network Internet Accessible	network type	Categorical (binary)	
Q9_1	Incident Recording	Organizational behaviour	Ordinal	2b,2c
Q9_2	Software Tests		Ordinal	2b,2c
Q9_3	Memory Cleaning		Ordinal	2b,2c
Q9_4	Access Control		Ordinal	2b,2c
Q9_5	Security Review		Ordinal	2b,2c
Q9_6	Backup & Recovery		Ordinal	2b,2c

Question #	Variable Name	Variable Group	Type	Research Question
Q11	Termination Procedure		Categorical	2b,2c
Q12_1	Service provider accompaniment		Ordinal	2b,2c
Q12_2	Policy Enforcement		Ordinal	2b,2c
Q12_3	Education		Ordinal	2b,2c
Q12_4	Employee awareness		Ordinal	2b,2c
Q12_5	Incident Reporting		Ordinal	2b,2c
Q12_6	Service Provider Awareness		Ordinal	2b,2c
Q13_1	Separation of Duties		Categorical	2b,2c
Q13_2	Access Control		Categorical	2b,2c
Q13_3	User activity log		Categorical	2b,2c
Q13_4	Operations log		Categorical	2b,2c
Q13_5	Connection monitoring		Categorical	2b,2c