UNIVERSITY OF KWAZULU-NATAL

Cyber-Security and Governance for Industrial Control Systems (ICS) in South Africa

By

Barend Hendrik Pretorius

Student Number: 200276341

A dissertation submitted in fulfilment of the requirements for the degree of

Masters of Commence in Information Systems

School of Management, Information Technology and Governance

College of Law and Management Studies

Supervisor: Dr. Brett van Niekerk

Co-supervisor: Karna Naidoo

2016

Declaration

I, Barend Pretorius, declare that: -

i. The research reported in this dissertation, except where otherwise indicated, is my original research;

ii. This dissertation has not been submitted for any degree or examination at any other university;

iii. This dissertation does not contain other persons' writing, unless specifically acknowledged as being sourced from other persons;

iv. This dissertation does not contain text, graphics or tables copied and pasted from the internet, unless specifically acknowledged and the source being detailed in the dissertation and in the reference section.

Barend Pretorius

(Student Number: 200276341)

Acknowledgements

Eerbewys en glorie aan die belangrikste, God. Vir my vrou, Elserie en my ouers, Dr Buks en Charlotte Pretorius, wat my bygestaan het gedurende hierdie tyd, die skripsie is opgedra aan julle. Vir die res van my familie en vriende, baie dankie vir al julle ondersteuning.

To my supervisors Dr Brett van Niekerk and Mr Karna Naidoo, your direction, proficiency and nurturing during this Master’s journey is greatly appreciated. You are a continuous source of energy and inspiration for my academic career. You both have gone beyond the call of duty. Dr van Niekerk, you have consistently guided and supported me without which I wouldn’t have complete this research. My colleagues and friends who participated or supported me with my research, thank you, it is much appreciated. To my language editor, Ms. Trishana Ramluckan, your assistance was much appreciated.

Abstract

Industrial control systems (ICS) and supervisory, control, and data acquisition (SCADA) systems have evolved from operating in a relatively trusting environment to the current prevalence of public networks. Cyber-threats are evolving to become more sophisticated. The Stuxnet malware brought home how vulnerable ICS/SCADA systems potentially are. There is no or limited information available as to the current state of ICS/SCADA in South Africa including the factors influencing ICS/SCADA and how they are secured and governed. Due to the nature of the systems, ICS/SCADA cyber-security and governance faces additional challenges compared to the corporate networks, and critical systems may be left exposed. There exists control frameworks internationally, however there are new South African legislation that needs to be taken into account. South Africa is also falling behind in cyber-security, therefore there is a concern in securing ICS controlling key infrastructure critical to the South African economy as there are little known facts about this.

This aim of the study is to assess the current state of ICS/SCADA in South Africa, determine the main governance frameworks employed, and to develop a control framework addressing the shortfalls. Elements of the Technology Acceptance Model (TAM) and the Protection Motivation Theory (PMT) are used to guide the study. Quantitative methods are used to determine the perceived susceptibility, security confidence, and governance for ICS/SCADA environment. Qualitative methods were used to review the current control frameworks, standards and legislation relevant to this environment.

The study found that the top threat/risk for ICS/SCADA are malware and the top vulnerability is unpatched systems. Furthermore, the framework used most in South Africa to secure and govern ICS/SCADA environments are Control Objectives for Information and Related Technology (COBIT) and from the document analysis the best suited framework overall is Centre for the Protection of National Infrastructure (CPNI). Taking these frameworks into account as well as relevant risks, threats and vulnerabilities, a consolidated framework aligned to South Africa were developed suggesting leading practices for securing and governing ICS/SCADA systems in South Africa.

Contents

List of Figures

List of Tables

List of Acronyms

BCP	Business Continuity Plan
CCTA	Central Computer and Telecommunications Agency
CIA	Confidentiality (C), Integrity (I) and Availability (A)
CD	Compact Disk
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CIP	Critical Infrastructure Protection
CMDB	Configuration Management Database
CMM	Capability Maturity Model
COBIT	Control Objectives for Information and Related Technology
CPI	Common Industrial Protocol
CPNI	Centre for the Protection of National Infrastructure
DCS	Distributed Control Systems
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Control Protocol
DNP3	Distributed Network Protocol
DoS	Denial of service
DRP	Disaster Recovery Plan
DVD	Digital Video Disc
ECT	Electronic Communications and Transactions
ENISA	European Union Agency for Network and Information Security

FBI	Federal Bureau of Investigation
HMI	Human Machine Interface
HR	Human Resources
ICCP	Inter Control Center Protocol
ICCWS	International Conference on Cyber Warfare and Security
ICS	Industrial Control Systems
ICS-CERT	Industrial Control Systems Computer Emergency Response Team
IEC	International Electrotechnical Commission
IED	Intelligent electronic device
IJCWT	International Journal of Cyber Warfare and Terrorism
ISACA	Information Systems Audit and Control Association
ISO	International Organisation for Standardisation
IT	Information Technology
ITIL	Information Technology Infrastructure Library
LAN	Local area network
MISS	Minimum Information Security Standard
MTU	Master Terminal Unit
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NGO	Non-Governmental Organisation
NPO	Non-profit Organisation
OPM	Office of Personnel Management
OT	Operational Technology
PLC	Programmable Logic Controllers

PMT	Protection Motivation Theory
POPI	Protection of Personal Information
RICA	Regulation of Interception of Communications and Provision of Communication-Related Information
RTU	Remote Terminal Unit
SABC	South African Broadcasting Corporation
SANS	System Administration, Audit, Network and Security
SAPS	South African Police Service
SCADA	Supervisory Control and Data Acquisition
SIC	Security Intelligence Centre
SIEM	Security Information and Event Management
SIS	Safety Instrumented Systems
SOC	State Owned Company
TAM	Technology Acceptance Model
TCP	Transport Communication Protocol
USB	Universal Serial Bus

Chapter 1 Introduction

1.1 Introduction

Cyber-espionage and cyber-attack tools have been evolving to become more sophisticated, resulting in the increased speculation over nation-sponsored malware and campaigns. An increase in cyber-criminal gangs and other groups increases the complexity of the threat landscape. Industrial control systems (ICS) and supervisory, control, and data acquisition (SCADA) systems have evolved from operating in a relatively trusting environment to the current prevalence of public networks. In 2010 Stuxnet brought home how vulnerable control systems potentially are. There have been subsequent cases where advanced cyber-attack and cyber-espionage tools have targeted ICS/SCADA, and there are numerous examples of compromises of such systems. Due to the nature of the systems, ICS/SCADA security and governance faces additional challenges compared to the corporate networks, and critical systems may be left exposed. This research explored the increasingly complex cyber-war and cyber-espionage threat landscape, and illustrate cases where South Africa has been affected. Vulnerabilities and threats related to the ICS/SCADA environment in South Africa are discussed, compared to international vulnerabilities and threats. Suggested controls for addressing risks, vulnerabilities and threats relevant to ICS/SCADA in South Africa are discussed. Figure 1.1 is a graphical representation of the outline of this chapter and overall structure.

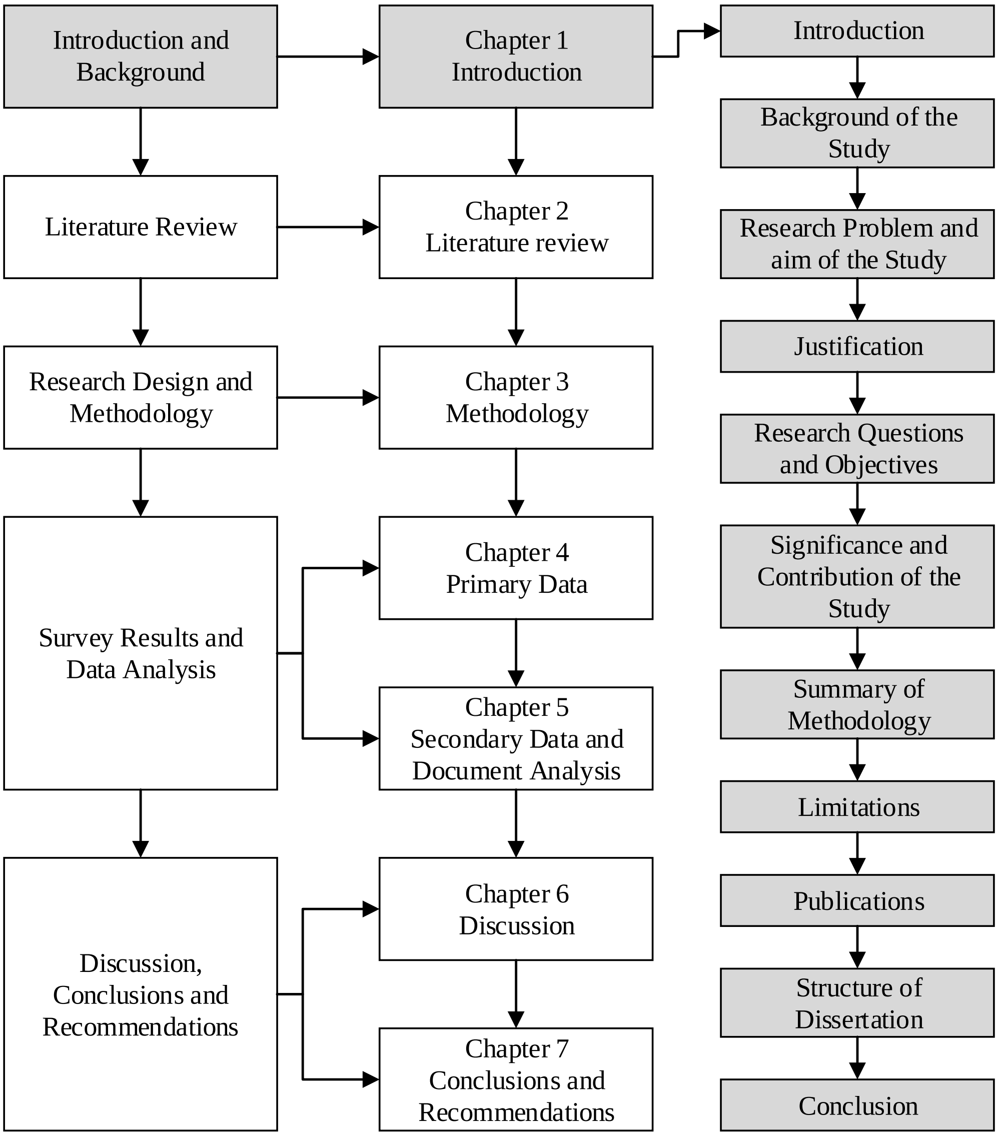

Introduction and Background
Chapter 1 Introduction
Introduction
Background of the Study
Literature Review
Chapter 2 Literature review
Research Problem and aim of the Study
Justification
Research Design and Methodology
Chapter 3 Methodology
Research Questions and Objectives
Chapter 4 Primary Data
Significance and Contribution of the Study
Survey Results and Data Analysis
Summary of Methodology
Chapter 5 Secondary Data and Document Analysis
Limitations
Chapter 6 Discussion
Publications
Discussion, Conclusions and Recommendations
Structure of Dissertation
Chapter 7 Conclusions and Recommendations
Conclusion

Figure 1.1: Graphical representation of Chapter 1 outline

1.2 Background of the Study

According to Stouffer, Falco and Kent (2006), Industrial control system (ICS) is a common name for various types of control systems which include Supervisory Control and Data Acquisition (SCADA) systems. ICS/SCADA systems are computers that control transportation systems, water and sewage systems and other critical infrastructure and industrial plants.

A number of security incidents relate to ICS/SCADA world-wide. These incidents increased and became more sophisticated by the introduction of Stuxnet in 2010. Stuxnet exposed how vulnerable control systems are when it bypassed a number of security controls to cause physical damage to an Iranian nuclear facility. Recently more variants of Stuxnet, namely Flame, Gauss, Duqu (Nakashima & Warrick 2012; Nakashima, Miller & Tate 2012; Rodionov 2012) have been found as well as new malware including Havex/Dragon fly (Walker 2014) which are more advanced.

South Africa is lacking in cyber-security, and it is a growing risk to business in South Africa. Neither the government nor business are adding adequate resources to combat it (Jones 2014). State Security Minister David Mhlobo announced in 2015 that cyber-security and the government's ability to combat cyber-crime would be a top priority in 2015 (Davis 2015).

Internationally there are control frameworks in place, however in South Africa new legislation is being released e.g. POPI as well as existing legislation and frameworks such as the King III Report and requirements for Public Sectors such as the Minimum Information Security Standard (MISS) that needs to be taken into consideration. South Africa is falling behind in cyber-security, therefore there is a concern in securing ICS controlling key infrastructure critical to the South African economy.

1.3 Research problem and aim of study

There is no or limited information available as to the current state of ICS in South Africa including the factors influencing ICS and how they are governed. This research assessed the current practices and environment of ICS in South Africa, to develop a consolidated framework aligned to South Africa with consideration to new and existing legislation. There are limited academic studies done for South Africa by Chileshe and van Heerden (2012) and Wolfpack (2016) therefore this study will fill this gap.

1.4 Justification

ICS/SCADA Security is still a growing field in South Africa and has not as yet been fully established. As mentioned in Section 1.3, this study is intended to fill a gap of limited academic studies done in the South African context. This study assessed what the current state of ICS/SCADA Security in South Africa is and develop an ICS/SCADA control framework to address common concerns by taking into account new and existing legislation. This ICS/SCADA control framework will enable organisations to improve security and governance of their ICS/SCADA systems which will lead to greater availability and reliability of computer systems running their operations.

1.5 Research Questions and Objectives

The aim of the research is broken down into the following research questions and objectives.

1.5.1 Research Questions

The research questions underpinning this study are:

- What are the factors (vulnerabilities and threats) influencing ICS/SCADA security in South Africa?
- What are the best measures to govern these factors that influence ICS/SCADA security in South Africa?
- What is the impact of non-governed ICS/SCADA?

- How are ICS/SCADA secured and governed?
- What are the perception of the suitability of the implemented controls/measures to mitigate the treats and risks?
- What would an ideal framework be given the results of the previous question?

1.5.2 Research Objectives

The objectives of this study are:

- To determine the factors (vulnerabilities and threats) influencing ICS security in South Africa.
- To determine what the best mitigating controls to govern and secure ICS/SCADA systems in South Africa are.
- To determine the impact of non-governed ICS.
- To determine how ICS in South Africa are secured and governed.
- To establish if the confidence levels of implemented controls/measures mitigating the threats and risks are sufficient.
- To develop a control framework addressing the shortfalls for ICS security in South Africa.

1.6 Significance and Contribution of the Study

This study provides a unique South African view point. ICS/SCADA security is still a growing field in South Africa and have not yet been fully established. As mentioned in Section 1.3, there are limited academic studies done in South Africa and this contributes by providing this knowledge. A governance and security control framework taking into consideration the threats, vulnerabilities and risks related to ICS/SCADA in South Africa was proposed.

1.7 Summary of Methodology

Exploratory research and design research was used for the process of designing a control framework. A mixed methods approach was used underpinned by the research tools: quantitative instruments include questionnaire, system data, and secondary data from document analysis; and qualitative tools include document analysis and Shodan, an open source tool used as a search engine for internet connected devices.

A cross-sectional study was done to determine the state of ICS/SCADA in South Africa at a single point in time. The sample size for the questionnaire was at minimum 30 people across various professional organisations and companies running ICS/SCADA systems, these include Information Systems Audit and Control Association (ISACA) and a large State Owned Company (SOC). Data collected from questionnaires was analysed using descriptive statistics, and documents was analysed using thematic analysis. Shodan was used to collect data on ICS/SCADA systems. Tools such as Excel was used for the coding and summarising process.

The study used elements of the Technology Acceptance Model (TAM) and the Protection Motivation Theory (PMT) to develop a conceptual framework. The results of the questionnaires, questions, data analysis and decisions formed part of the input in the methodology to develop a control framework to address the gaps.

1.8 Limitations

It was difficult to determine the exact population as there are limited studies on governance and security of ICS/SCADA in South Africa conducted and difficult in determining the individuals with ICS/SCADA knowledge. The questionnaire was sent out to the broader community (refer to Section 1.7) and a question was included upfront to determine the relevance of the respondents. From the document analysis, inconsistency of reports from Security vendors were discovered. This includes differences between current and previous year's categories as well as different categorisation used between the various vendors. This complicated the overall analysis and could lead to some bias towards certain vulnerabilities and threats. Although this might have a small implication on the study, this might impact someone in the industry trying to use various reports to determine the top vulnerabilities and might wrongly place emphasis on non-prevalent vulnerabilities.

1.9 Publications

This is a Masters by dissertation, however the following publications emanated from the research:

- Academic journal: Pretorius, B., & Van Niekerk, B., 2016, 'Cyber-Security for ICS/SCADA: A South African Perspective', *International Journal of Cyber Warfare and Terrorism (IJCWT)* 6(3), pp 1 – 16. Available from http://www.igi-global.com/article/cyber-security-for-icsscada/159880;
- Academic conference: Pretorius, B., & Van Niekerk, B., 2015, 'Cyber-Security and Governance for ICS/SCADA in South Africa', in *The Proceedings of the 10th International Conference on Cyber Warfare and Security,* Academic Conferences and Publishing International Limited, UK, pp 241-251;
- Practitioner conference: Pretorius, B., & Van Niekerk, B., 2015, 'Cyber-Security and Governance for ICS/SCADA in South Africa', *ISACA South Africa Annual Conference 2015*; and
- Invited presentation: Pretorius, B., & Van Niekerk, B., 2016, 'Cyber-Security and Governance for ICS/SCADA in South Africa', *KPMG CIO Agenda June 2016*.

1.10 Structure of dissertation

This dissertation consisted of seven chapters (including this chapter). This chapter introduced the study and described the research approach. Chapter 2 presented a literature review on ICS/SCADA. Chapter

3 discussed the research methodology and the research design that guided this study, while Chapter 4 presented the quantitative and qualitative data analysis. Chapter 5 looked at various documents from local and international as well as network security device data and analysed and compared these. Chapter 6 presented a discussion based on the quantitative and qualitative data analysed and in relation to the secondary data analysis. Chapter 7 concludes the study by presenting the conclusions, the limitations, proposes areas for future research and a final conclusion.

1.11 Summary

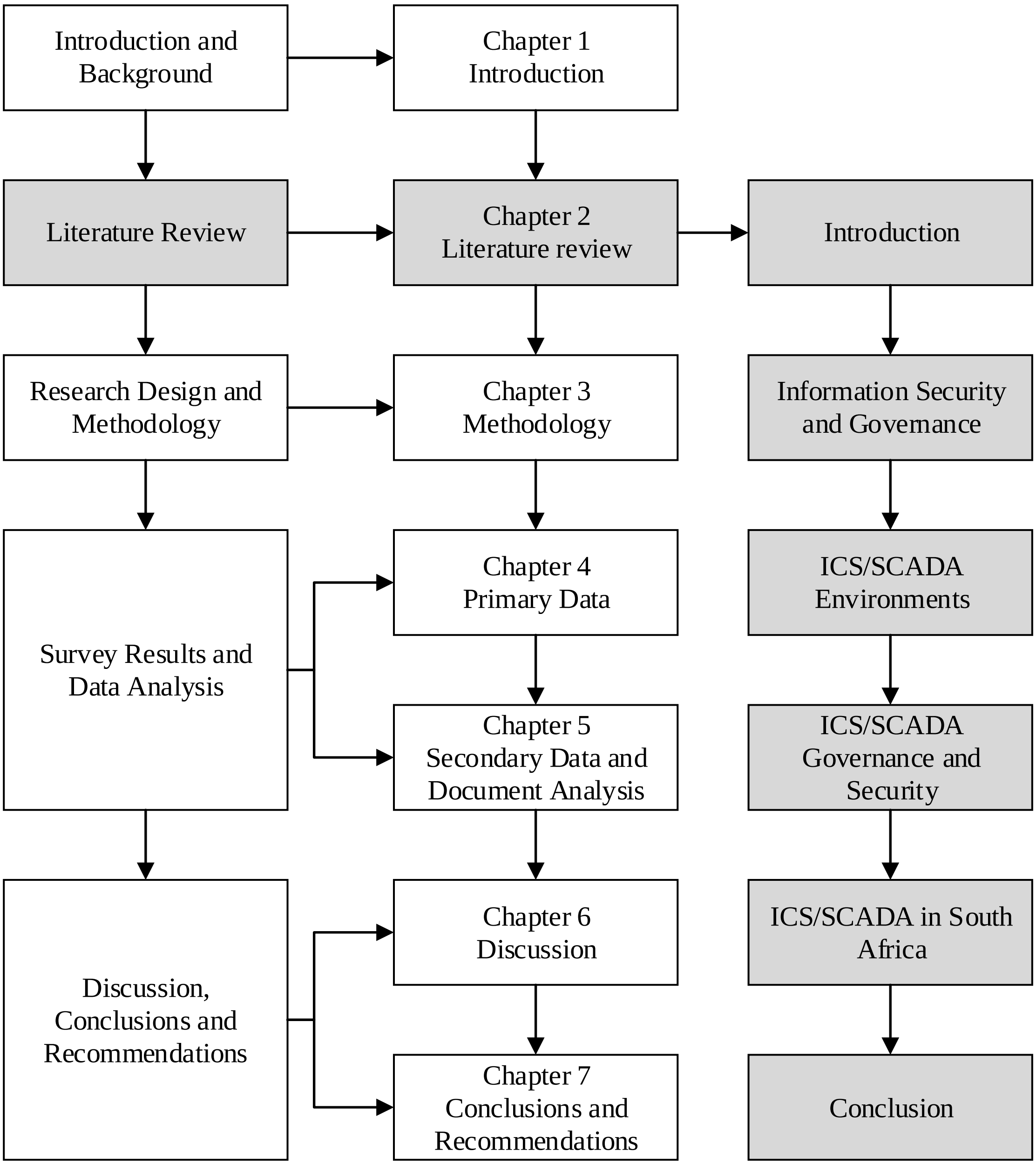
Industrial control systems (ICS) and Supervisory, Control, and Data Acquisition (SCADA) systems have evolved from operating in a relatively trusting environment to the current prevalence of public networks and evolving cyber-threat environment. ICS/SCADA is still a growing field in South Africa and no or limited information is available on the current state of these systems in South Africa. This research aims at determining the factors influencing ICS/SCADA in South Africa, their impact, how they are currently secured and governed and determine the best measures to mitigate the risks.

Chapter 2 Literature Review

2.1 Introduction

Industrial control systems (ICS) and supervisory, control and data acquisition (SCADA) are terms that are often used to describe all forms of control systems and automation in industrial and process controls. However, this is not entirely accurate. It has been become practice that ICS is used as the general term, and SCADA is a subset of this and generally refers to systems that span a large geographic area (Byres 2012). These types of systems are often used in critical national infrastructure (Miller & Rowe 2012) such as pipelines and electric power generation and distribution (Chileshe & van Heerden 2012). These types of systems were being implemented using mechanical pneumatics prior to the advent of microelectronics, and the introduction of microcontrollers and microprocessors revolutionised the field (Byres). ICS/SCADA systems were originally separate from the corporate network and operated specialist communication protocols, however they slowly started implementing standardised protocols and were connected to the corporate networks and the Internet (Brodsky & Radvanovsky 2013; Miller & Rowe). Control systems were originally limited to a specific plant or site, however with the evolution of computing and networks there was a drive towards real-time monitoring and control of geographically separate sites. As the ICS/SCADA developed to interconnected systems with standard protocols, they became more vulnerable to attack (Brodsky & Radvanovsky; Krutz 2006).

This chapter discusses information security and governance principles and incidents, then goes on to introduce ICS/SCADA environment and its components. International ICS/SCADA incidents are discussed as well as vulnerabilities and threats. The background of the research objectives, namely ICS/SCADA in South Africa is discussed as well as legislation and challenges. The chapter concludes by introducing a methodology on developing a control framework for ICS/SCADA in South Africa. The next chapter explores this methodology and the studies research methodology in more detail. Figure 2.1 is a graphical representation of the outline of this chapter and overall structure.



Introduction and Background
Chapter 1 Introduction
Literature Review
Chapter 2 Literature review
Introduction
Research Design and Methodology
Chapter 3 Methodology
Information Security and Governance
Survey Results and Data Analysis
Chapter 4 Primary Data
ICS/SCADA Environments
Chapter 5 Secondary Data and Document Analysis
ICS/SCADA Governance and Security
Discussion, Conclusions and Recommendations
Chapter 6 Discussion
ICS/SCADA in South Africa
Chapter 7 Conclusions and Recommendations
Conclusion

Figure 2.1: Graphical representation of Chapter 2 outline

2.2 Information Security and Governance

Security is when something is secured and free from risk or danger (Whitman & Mattord 2012:8). Security should similarly be applied to a company's information assets which must be protected from all possible threats at all times in any form and in any condition. Protecting information from unauthorised use or access, interruption or destruction, alteration, leak, examination, or recording, regardless if it is electronic or physical, is also information security.

Information Security refers to securing a company's information assets. Securing information assets is not only about implementing usernames and passwords; it plays a significant part in the securing of a company's intangible assets which also improves its business processes and increases stakeholder confidence (Susanto, Almunawar & Tuan 2012: 67). Information security refers to the safeguarding of information, including critical elements such as systems, hardware, and storage of information, transport of information, people and processes involved. The safeguarding of information is achieved through the implementation of policies, procedures, awareness programs and training of users, as well as information security tools or technology (Whitman & Mattord 2012:10).

Information security requires a complete approach that includes every part of the company, (RSA 2014). This can be achieved by performing active monitoring, detection of abnormal events and appropriate response to threats (Esri 2014:2). The following categories needs to work together to jointly secure a company's information assets (Carroll, 2014: 12):

1) Physical security and environmental controls: procedures to protect an organisation's assets, and people from threats which include unauthorised physical access or natural disasters;

2) Operations security: procedures to ensure the organisation can perform its operations with limited interruptions or compromises. This includes its ability to prevent, detect and recover from an incident or compromise such that normal operations can continue;

3) Communications security: this include the protection of the organisation's transport of data and media with supporting tools to enable its objectives;

4) Network security: protection and monitoring of an organisation's networks and devices to ensure it is used according to its purpose without compromise or downtime;

5) Database security: protection of an organisation's data stored in a database; and

6) Storage security: this includes expert techniques to protect an organisation's information in its storage area networks (Whitman & Mattord 2012: 8).

Information Security Governance according to (Whitman & Mattord 2012:29-33), is agreed upon roles and responsibilities implemented by the board and executive management in order to provide and achieve strategic alignment of information security and business strategy, ensuring objectives are achieved and to mitigate and manage risks and threats to information resources.

2.2.1 Information Security Triad

Information Security is supported by the "CIA Model" or "CIA triangle" (Whitman & Mattord 2012:11-13) that explains three aspects of information security that needs to be preserved. The following three aspects form the CIA Model: Confidentiality (C), Integrity (I) and Availability (A).

Confidentiality refers to the access of information or data (physical or electronic) and that only people that should have access to sensitive information or data and need to access it, have access. Anyone else having access that should not have access is refer to as an unauthorised person. Confidentiality is breached when unauthorised persons either intentionally or unintentionally gain access to sensitive information that they should not have access to (Whitman & Mattord 2012:11-13).

Integrity refers to the reliability of information or data (physical or electronic) which include complete, uncorrupted and uncompromised. The integrity of information or data is compromised when it is not complete or damaged, corrupted, compromised, or destroyed (Whitman & Mattord 2012:11-13).

Availability refers to information or data being available to authorised users when required. This includes not only data but infrastructure as well. Availability is compromised when data, information or infrastructure is not available to authorised users when it should be (Whitman & Mattord 2012:11-13).

The CIA concepts needs to be taken into consideration when designing and building a secure system as well as improving existing systems. Depending on the type of information system, certain elements of CIA plays a more important role than others. For example, for operational systems availability is more crucial than confidentiality, where as a financial system, confidentiality and integrity is more crucial than availability.

Mechanisms to ensure that user's actions cannot be denied, is referred to as non-repudiation, of which examples include sending an email, or signing a document.

2.2.2 Vulnerability and Threats

An organisation needs to identify risks, threats and vulnerabilities and adequately mitigate them to reduce the risk so that the organisation can have a successful information security strategy (Rhodes-Ousley 2013).

2.2.2.1 Vulnerability

A vulnerability is a fault in a software program or program code that allows unauthorised modification or destruction of data, or single point of failure or misconfiguration which could result in the confidentiality, integrity and availability of information being compromised (Shahriar & Zulkcernine 2012).

2.2.2.2 Threat

Exploiting a weakness in a current vulnerability is known as a threat (Dahbur, Mohammad & Tarakji 2011:3). This could cause damage to the data and systems. A vulnerability could be used to gain unauthorised access to a company's network, systems and ultimately sensitive data (Dahbur et al.).

A company's information assets are at all times under threat (Whitman & Mattord, 2012:11). An organisation needs to identify the threats and possible mitigating controls in order to reduce the risks these threats represent to ensure correct balance of Information Security controls. Threats may differ from company to company and environment to environment. Threats should be classified, categorised and prioritised in order to adequately mitigate them. Someone who is acting out the threat is referred to as a threat actor.

2.2.2.3 Incident

An incident is defined by Jones (2013:8-9) as an event that could include:

- Unauthorised access to an organisation’s network and systems;
- Unauthorised access to confidential information;
- Virus/malware outbreak on an organisation’s systems or network;
- Unauthorised interruption or denial of access to an organisation’s data or systems; and
- Unauthorised or accidental destruction or altering of an organisation’s data.

2.2.2.4 Risk

According to the System Administration, Audit, Network and Security (SANS) SANS Institute (2006) risk is the possible damage that may arise from a current or future process. From an ICT perspective risk is the damage to a process or related information resulting from an intentional or unintentional event that negatively impacts the process or the related information. The process of understanding and responding to the factors that may lead to a failure in the Information Security triad or CIA of a system is called risk management.

SANS Institute (2016) also defines Risk as a function of the likelihood of a given threat source’s exploiting a potential vulnerability, and the impact of that it has on an organisation.

The general definition used to calculate risk is that risk is the product of the probability and impact (Boehm 1991):

Risk = Probability x Impact

The threats and vulnerabilities also need to be consider when calculating the risk. SANS Institute (2012) mentions that risk, threat and vulnerability needs to be used together and defines risk as follows:

Risk = (probability x impact x threat x vulnerabilities)/countermeasures or controls

2.2.3 Information Security Controls

The following categories defined in Section 2.2, needs to work together to jointly secure the company’s information assets (Carroll, 2014: 12):

- Physical security;
- Operations security;

- Communications security;
- Network security;
- Database security; and
- Storage security

2.2.3.1 Types of Information security controls

Information Security controls can be grouped into the following categories (Rhodes-Ousley 2013):

- Preventative – This control will prevent threats before they exploit a vulnerability;
- Detective – This control will discover or detect a threat that are busy occurring or have occurred;
- Deterrent – These controls will discourage both insider and outsider attacks;
- Corrective – Will restore the Integrity of information;
- Recovery – Will restore the Availability of information; and
- Compensative – Where another control fails, this control will protect.

Multiple implementations of each of the information security control in the above categories needs to be considered in order to protect against different threats, (Rhodes-Ousley 2013):

- Administrative Controls – Policies, procedures and standards defined and enforced by senior management;
- Physical Controls – Controls that are physically present;
- Logical/technical – Controls performed by software/technology;
- Operational Controls – Control performed by people as part of operations; and
- Virtual Controls – logical/technical controls that are triggered when certain situations occur.

Table 2.1 provides examples of Information Security controls that fall within a particular category and method of implementation.

Table 2.1 Information Security Control for different Threats

	Administrative	Physical	Logical/Technical	Operational	Virtual
Preventative	Standards, Procedures	Access control (Biometric or locks)	Firewalls, IPS	Guards on station	Access control list
Detective		Cameras, log book, alarm	IDS, audit logs, SIEM	Guards patrolling	
Deterrent	Policies	Signs, barbed wire	Warning messages	Visible guards and cameras	Dynamic pop-up warnings
Corrective	HR penalties		Redundancy		
Recovery			Backups, data replication	Disaster recovery plans	
Compensative			Manual processes		

Adapted from: Rhodes-Ousley (2013)

2.2.3.2 Defence in Depth

The basic principle of information security architectures is to implement layered security, this is referred to as defence in depth (Whitman & Mattord 2012). Defence in depth originated from a military term in which multiple layer of defence is used to protect something valuable from the enemy. This makes it more difficult for the enemy to attack. An example is a castle back in the medieval times. There are multiple layers used for defence. These include a moat, a draw bridge with water, high castle wall, a heavy steel gate and watchmen.

This similar concept can be applied in securing sensitive information and protection a company's information assets. It is an information security best practice to use Defence in depth. Defence in depth is achieved through implementing multiple layers of controls. Example data sitting in a database is encrypted with restricted access control via the application, the database and application is installed on a server running appropriate anti-virus software, the server sitting on a secure network behind a firewall and in a secure physical location. Figure 2.2 illustrates the Defence in depth concept. Rhodes-Ousley (2013) also refers to this as the onion model.

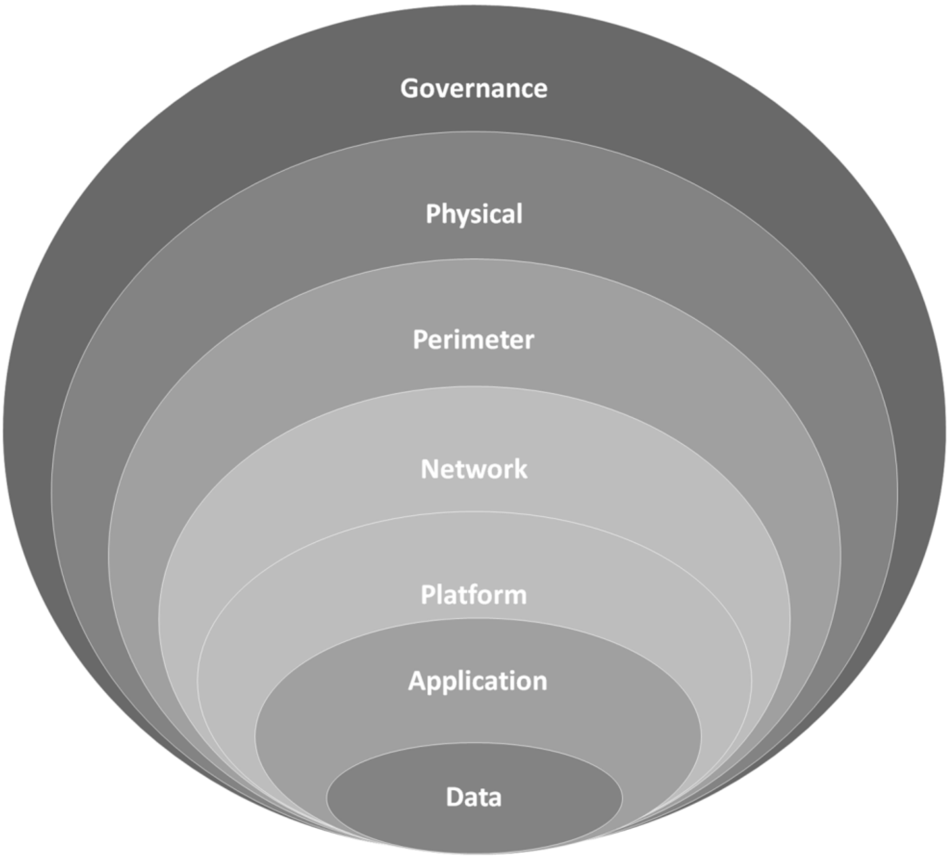


Figure 2.2: Defence in Depth

Adapted from: Sentrillion (2012)

2.2.3.3 Monitoring

Threat management is a modern technique that is used every day to perform network security correlation. Data gathered from different sources needs to be correlated to identify relationships, patterns, and trends. A Security Information and Event Management (SIEM) systems of Security Intelligence Centre (SIC) can assist with this, can collect and aggregate the relevant data from the following sources: Firewall logs, Intrusion detection and prevention systems, Network device data and Operating system or application logs (Amoroso 2013).

2.2.3.4 Capability Maturity Model

Acohido (2015) states that a Capability Maturity Model (CMM) is generally used by a company to determine the maturity of their information security position and to improve their position. The CMM will determine the maturity of the processes and identify steps that are required to increase the maturity of these processes. There are normally five stages of the CMM (Acohido):

- *Level 1: Initial or Basic* - Information security activities are ad hoc and in most cases, no formal information security program is in place. A very minimal or basic level of information security controls are in place;
- *Level 2: Developing or Evolving* - Informal responsibilities are assigned to an individual who is developing an information security program, policies and procedures. Informal communication around information security issues are taking place. Information Security Controls are inconsistently applied;
- *Level 3: Defined or Established* - Policies and procedures are defined, roles and responsibilities are defined but minimum accountability or enforcement;
- *Level 4: Managed or Advanced* – Clear defined Information security roles and responsibilities with formal information security committee consisting of business and operations managers. Information Security Controls are consistently applied; and
- *Level 5: Optimising or Leading* - Business have accepted the residual risk associated with their use of information and technology. Full accountability from business for information security failures or policy and procedure violations. There are continuous self-improvement processes in place that are regularly reviewed and updated. The company has an information security aware culture.

CMM increases the efficiency and effectiveness of information security programs by focusing on comprehensive processes that can advance, develop to be more automated and become integrated into the overall operational infrastructure (Acohido 2015). An example of a CMM is displayed in Figure 2.3.

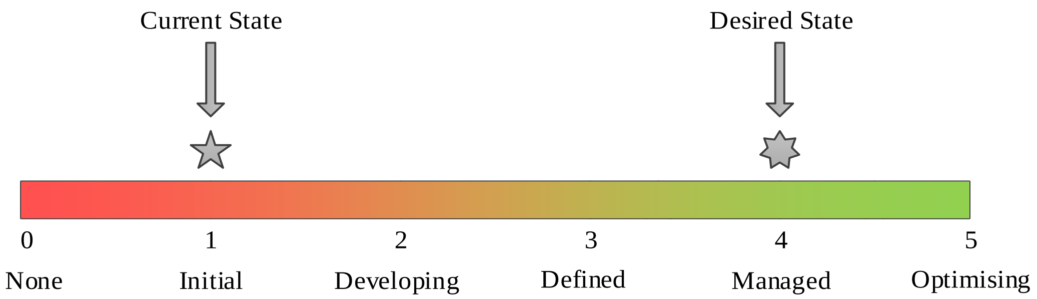


Figure 2.3: CMM example

Adapted from: Acohido (2015)

2.2.4 IT Security and Governance Frameworks

Internationally there exist a couple of control frameworks to govern and secure IT in an organisation. The most common ones are:

2.2.4.1 COBIT

The *Control Objectives for Information and Related Technology (COBIT)* was first released by ISACA (2012) in 1996 to assist financial audit community to control and govern their IT environments. The latest version of COBIT, version 5 was released in 2012. This included a section on Information Security and how to oversee and manage it.

2.2.4.2 ISO/IEC 27002

The International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC) published the ISO/IEC 27002 as an information security standard to be used for corporate security (ISO/IEC 2013). According to Knapp (2011) that although the ISO/IEC 27002 mentions protection of ICS/SCADA networks less specifically, it is useful as it maps directly to additional national standards of certain countries, including South Africa.

2.2.4.3 ITIL

The *Information Technology Infrastructure Library (ITIL)* was developed by the Central Computer and Telecommunications Agency (CCTA) as a set of best practices for IT service management.

2.2.4.4 SANS 20 critical controls

The SANS institute developed the Center for Internet Security (CIS) Critical Security Controls which are a list of recommended activities, which were developed from the most common attack patterns and provide exact and actionable ways to end the most persistent and dangerous attacks. The effectiveness of the controls has been tested across a comprehensive community of government and industry experts. (SANS 2016b)

2.2.5 Global incidents

There have been a huge number of security incidents worldwide. The most notable ones in the last five years are:

2.2.5.1 Sony

Although Sony is more famous for the hack in 2014, the company was also compromised back in April and October 2011. Around 77 million users had their names, addresses and other personal, data stolen from the PlayStation Network and Sony Online Entertainment accounts (Quinn & Arthur, 2011)

In November 2014, a devastating cyber-attack was launched on Sony Pictures. Malware written by hackers spread across Sony's global network, destroying almost half of the network. The attackers even had an extraordinary deleting algorithm that overwrote the data seven different ways and the code destroyed each computer's start-up software leaving the computer unusable (Elkind 2015). Valuable company data were stolen and leaked online. This included sensitive emails from executives, personal data from employees and copies of upcoming films. Sony's co-chairman had to resign because of the hack (Groden 2015).

2.2.5.2 Adobe

In 2013 Adobe's networks were breached by hackers. User information was stolen as well as the source code for certain Adobe programs. The user information includes email addresses and passwords for 150 million users, and credit card data for 2.9 million users (Howley 2015).

2.2.5.3 Target

In 2013, a Heating, ventilation and air conditioning (HVAC) contractor working within Target, had his credentials compromised (Riley, Elgin, Lawrence & Matlack 2014). The credentials were used by hackers to gain access to Target's network resulting in over 40 million credit and debit card numbers, and 70 million consumer email addresses being stolen. The CEO Gregg Steinhafel resigned and Target had to settle a class-action lawsuit for $10 million. (Howley 2015)

2.2.5.4 eBay

In May 2014, hackers gained access to eBay's network via compromised employee login information resulting in more than 145 million user data being stolen (Howley 2015). Although information such as login credentials, encrypted passwords, email addresses and physical addresses was stolen, no payment information was compromised (Groden 2015).

2.2.5.5 Anthem

In March 2015, a healthcare insurer, Anthem was hacked by suspected Chinese government-sponsored hackers (Howley 2015). Around 80 million customer's Social Security numbers, employment details, and other personal information was stolen. Luckily no medical data was compromised. (Groden 2015).

2.2.5.6 Ashley Madison

In August 2015, hackers stole and revealed online the information of 32 million users of a dating website for married people wanting affairs (Groden 2015). The site has a policy of not deleting users' personal information (names, addresses, credit cards and search history), which left many users fearing that they might be blackmailed or publically shame. Speculations are still out on how the site was breach. Day (2015) speculate that it was either an inside or external threat or most likely a cross-site scripting vulnerability.

2.2.5.7 U.S. Office of Personnel Management (OPM)

In 2015 login credentials from the employee of a third-party government contractor were stolen by hackers, suspected to be Chinese government-sponsored, and used to gain access to the U.S. Office of Personnel Management systems (Howley 2015). This resulted in U.S. government employees having their Social Security numbers and other personal information being compromised.

2.2.6 South African Information Security

Norton Rose Fulbright (2012) indicated there is an increase in Phishing attacks in South Africa. South Africa is the second most targeted country for such attacks. The Federal Bureau of Investigation (FBI) ranked South Africa 11th out of 50 countries that reported Internet based complaints in 2014 (Federal Bureau of Investigation 2014). Cyber-crime in South Africa is regarded as a priority crime by the Directorate of Priority Crime, also known as the Hawks (Hubeschle 2011).

According to IT News Africa (2016), 8.8 million South Africans have fallen victim to cyber-crime and Vicente (2016) indicated South Africa is the top cyber-crime target in Africa. Cyber-crime has cost the South African economy around R35 billion in 2015 (Chiloane 2016) as South African organisations are unprepared and ill-equipped to handle emerging cyber-threats. They also rely on outdated protection strategies (Alfreds 2016).

2.2.7 South African Incidents

There have been numerous cyber-attacks or incidents in South Africa. Below some of the more notable ones in the last five years are discussed in this section:

2.2.7.1 The National Department of Water Affairs

In June 2011 the National Department of Water Affairs systems got hacked via password fraud causing the Department to lose R2.84 million (Patrick 2016).

2.2.7.2 South African Postbank

The South African Postbank's financial systems was hacked in January 2012. R42 million was stolen via mule accounts (Rasool 2012).

2.2.7.3 South African Police Service

The South African Police Service (SAPS) had their website hacked to reveal the personal details of almost 16 thousand whistle-blowers. This was in retaliation for the Marikana shootings. In addition, hundreds of SAPS personnel had their names, ranks and contact details leaked by the hacker (Roane 2013).

2.2.7.4 Gautrain Management Agency bank account

In November 2014, the Gautrain Management Agency bank account was hacked and came close to being robbed of R800 million (Patrick 2016).

2.2.7.5 Eskom's payroll system

Eskom's payroll system was almost hacked in November 2014, by two of its employees but was foiled by the Hawks. (Patrick 2016).

2.2.7.6 Road Traffic Management Corporation bank account

In October 2015, the Road Traffic Management Corporation's bank account was hacked and R8.5 million was stolen by hackers (Mkhwanazi 2015). Five people believed to be part of a syndicate were arrested for fraud and corruption.

2.2.7.7 Anonymous Africa DDoS

A hacker called Anonymous Africa, performed a distributed denial of service DDoS attack on the African National Congress (ANC) and Independent Online (IOL) websites in June 2013 and the South African Broadcasting Corporation (SABC) website in June 2016 by taking them offline (Vermeulen 2016b). This was in retaliation over a decision by SABC not to broadcast violent protests and the ANC for being one of Mugabe's "biggest enablers".

Also in June 2016, Anonymous performed DDoS attack on Gupta owned websites including *The New Age* (newspaper), ANN7 (news channel), and Sahara and Oakbay Investments (Solomon 2016). This was a statement by the hacktivist group against corrupt parties and corporations.

2.2.7.8 Anonymous Operation Africa (#OpAfrica)

The hacker group Anonymous hacked the Government Communications and Information Services (GCIS) database in early 2016. They hacker group released personal details of 1500 employees including their names, email addresses, phone numbers and password hashes as part of "Operation Africa" or #OpAfrica. The Operation Africa is said to focus on internet censorship and child labour (Vermeulen 2016a). In July 2016, Armscor, which is the acquisition organisation for the South African Department of Defence, was hacked. The hacker group Anonymous hacked their website to breach the settlement and invoicing system. Details of access to 19 938 supplier IDs, names and their passwords has been leaked (Fripp 2016; Van Zyl 2016). The hacktivists used a simple SQL injection to hack and breach the data. This was part of the hacktivists plan to target corrupt African governments as Armscor was in the news related to a contentious tender for a VIP Aircraft for the South African government.

2.3 ICS/SCADA environments

This section provides an overview of ICS/SCADA systems and discuss the differences between ICS/SCADA environments and traditional IT networks. Previous versions of this section was published as an academic journal in the *International Journal of Cyber Warfare and Terrorism* (IJCWT) in July 2016 (Pretorius & Van Niekerk 2016) and the *10th International Conference on Cyber Warfare and Security* (ICCWS) on 24 and 25 March 2015 (Pretorius & Van Niekerk 2015). In addition, aspects of this literature was also presented at the ISACA South Africa conference in August 2015, and KPMG Chief Information Officer (CIO) Agenda in June 2016.

2.3.1 Overview

Industrial control system (ICS) is a common name for various types of control systems (Stouffer, Falco & Kent 2006), these include Supervisory Control and Data Acquisition or known as SCADA systems, Distributed Control Systems (DCS), and other smaller components such as Programmable Logic Controllers (PLC). These systems are mostly found in the critical infrastructure and industrial sectors. ICS/SCADA are normally used in industries such as oil and gas, automotive, chemical, food, transportation, water, electrical, pharmaceutical, paper, and certain manufacturing. These systems are key and critical to the operations of these industries.

According to Stouffer *et al.* (2006), SCADA systems are dispersed systems used to control geographically distributed equipment, sometimes scattered over couple of square kilometers, where data acquisition and control are centralised and critical to the operations. They are used to control systems such as transportation systems, electrical power grids, water and sewage systems, and pipelines transporting chemicals.

2.3.1.1 ICS/SCADA components

There are various devices within an ICS/SCADA environment that make up the system. These range from sensors in the field that collect data or information, the systems that distribute them and store them to systems that allow human or user interaction to monitor, change and control operations. Below are some of the more common components:

- **RTUs** – Remote Terminal Unit (RTU) is often housed in a substation or remote part of the plant. RTUs aim is to monitor field devices and transmit the data to next level device and finally to a central station that is monitored (Knapp 2011).

- **MTU** – Master Terminal Unit is a central located unit that collects data normally from RTU and feed it through to a central station (Knapp 2011).
- **PLCs** – Programmable Logic Controllers (PLCs) is a specialised machine, similar to a computer, which are used to automate functions within an ICS/SCADA network. They are specially configured for specific inputs and outputs, generally from field devices (Knapp 2011).
- **HMI -** The Human Machine Interface (HMI) is a physical control panel that allows users to monitor, change or configure settings of the underlying process. (Stouffer, Phillitteri, Lightman, Abrams, Hahn 2015).
- **Supervisory workstations –** These workstations run generally on Windows operating systems and give the user a graphical overview of the ICS/SCADA environment. These can sometimes be the central station from where operations are monitored and controlled (Knapp 2011).
- **Data Historians –** Data Historians are specialised software that stores the collected values and information in a database build for this purpose. Data points that are stored in the Historian are sometime referred to as tags. These can contain anything from frequencies of motors, temperatures to weights or cargo (Knapp 2011).
- **Other components –** Field devices are sensor, devices in the field that provide input or output to either PLCs or RTUs. These devices can be anything from a sensor that measures weight or temperature to a motor that control the frequency of motors. These are also referred to as an intelligent electronic device (IED) (Knapp 2011). There are also other components such as industrial network switch which are used to convert industrial protocols to IT protocols. Physical access scanners, printers, routers, and wireless routers are also found in ICS/SCADA environments.

2.3.1.2 ICS/SCADA Communication

ICS/SCADA components are connected to each other through a local area network (LAN) and information or communication takes place via certain protocols. Certain protocols use designated ports. A port is an end point of network communication and has a close relationship with an IP address and communication protocol. Different services use different ports. In most cases the ICS/SCADA network protocols are not standardised and are considered to be manufacturer-proprietary (Project SHINE, 2014).

ICS/SCADA protocols are real-time communication protocols, designed to interface and connection between ICS/SCADA systems and components via the designated ports. There are dozens of protocols, however the following protocols and ports are the most common:

- **Modbus (Port 502)** – Modbus is the oldest and most common used ICS/SCADA protocol. Modbus is commonly used for communication between PLCs and HMIs, however can be used between any I/O device, sensors and other communication devices. Modbus typically lacks authentication, encryption and checksum (Knapp 2011). Modbus uses the Transport Communication Protocol (TCP) and the port that is most often used is Port 502 (Project SHINE 2014).
- **Siemens/ICCP (Port 102)** – The Inter Control Center Protocol (ICCP) is a protocol used for communication between control centers within the energy industry (Knapp 2011). ICCP also lacks authentication and encryption. Siemens use Port 102 for remote programming and PLC connections via the Ethernet (Project SHINE, 2014).
- **DNP3 (Port 20000)** – The Distributed Network Protocol (DNP3) us mainly used for communication between master control stations and remote or slave devices. It is more common in the electricity and water industries (Project SHINE 2014). The authentication and encryption is not inherent within DNP3. There are a number of vulnerabilities due to the complexity of the protocol. The Port 20000 is dedicated to DNP3 (Knapp 2011).
- **Ethernet/IP (Port 44818) –** Ethernet/IP uses the standard Ethernet frames and combines it with the Common Industrial Protocol (CIP) to communicate (Knapp 2011). Ethernet/IP is used in most industries including automotive, manufacturing, and hybrid (Project SHINE 2014). Ethernet/IP is a real time Ethernet protocol and contains vulnerabilities. Ethernet and IP security, similar to that of an IT network, is required at the perimeter (Knapp).
- **BACNet (Port 47808) –** BACNet is a protocol used for communication in building automation. This includes air conditioners and heating, light controls, access controls, and fire detection systems. It uses Port 47808 for communication between building automation devices.

2.3.2 Differences between ICS/SCADA and Traditional IT Networks

There are a number of differences between ICS/SCADA networks and traditional IT networks (those used in enterprises or corporations), which often result in challenges for managing the information security of the ICS/SCADA networks. The summary of differences described by Neitzel and Huba (2014) are in the sections 2.3.2.1 to 2.3.2.10:

2.3.2.1 Different security objectives

Ensuring confidentiality is often the primary focus on many IT networks whereas availability is the primary focus of information security in ICS/SCADA networks.

2.3.2.2 Network topology and segmentation

ICS/SCADA systems are usually much smaller than IT networks with static configurations instead of dynamic. Therefore, the use of Dynamic Host Control Protocol (DHCP) and Wi-Fi is not encouraged.

ICS/SCADA networks should not have access to internet or email, and should be segregated from corporate IT networks, either standalone or via a firewall. Traditionally IT networks are segmented into subnets.

2.3.2.3 Functional partitioning

The bulk of corporate IT networks will be segregated by administration function (e.g. finance, HR). ICS/SCADA is partitioned into three levels:

- The physical process;
- The intelligent devices and sensors; and
- The control systems which are described by the ANSI/ISA95 Purdue reference model (Control Global 2008).

ICS/SCADA devices need to be in separate network zones according to their security and access requirements.

2.3.2.4 Physical components and impact

Although ICS/SCADA systems use standard operating systems and computer hardware to run software applications, they often fall outside the domain of IT. The ICS/SCADA applications are either custom built or vendor specific and could possible cause a conflict with the information security controls defined by IT security policies. This often requires the information security controls to be vendor specific.

2.3.2.5 Default passwords

Often it is found that default passwords are hard coded into applications or hardware, allowing easy access, but also opens a big security hole (Paganini 2013). A list of hardcoded and default passwords is freely available making it easier for threat actors or hackers to exploit the ICS/SCADA systems should passwords still remain default or appropriate controls not be in place. The list of hardcoded and default passwords was compiled by SCADA Strangelove (2015). This is discussed and analysed in Section 5.5.

2.3.2.6 User account management

Users of IT systems are often controlled by administrators through Active Directory or similar mechanisms which contain a specific list of users for the operating system and application. ICS/SCADA use more of a role-based type of access control to grant users access to ICS/SCADA systems, devices and data. Possible roles include maintenance engineers, process engineers and operators. Often user accounts are shared and there might be no accountability if something goes wrong.

2.3.2.7 Safety Instrumented Systems (SIS)

Safety is an essential aspect of any plant operation, and these systems are responsible for ensuring safety by placing any process into a safe state if it is detected that the conditions of the process could threaten safety. SISs are distinct from ICS/SCADA systems but they can be integrated. The SIS network and components are proprietary and should be securely isolated or segmented from the ICS network. There is no equivalent system under traditional IT networks.

2.3.2.8 Patch management and untested software

ICS/SCADA systems are typically implemented to a specific operating system version and hardware configuration; changing either of these might result in the ICS/SCADA system not functioning properly. This requires all updates to be thoroughly tested with the ICS/SCADA system prior to approval for implementation. Similarly, patching and antivirus updates for ICS needs to be tested and approved. Due to the disruption to operations, scheduling and validation is also required to ensure safe and repeatable control. Updates and patching are therefore not done on operational ICS/SCADA systems at the same time as the IT patching schedule. There is also the problem that many ICS/SCADA systems are based on outdated operating systems such as Windows XP, where patches are no longer available as the operating system is no longer supported. The obsolescence stems from the fact that ICS/SCADA systems have a lifecycle of 15-30 years, which exceeds that of many commercially available computer operating systems (Pella 2013).

2.3.2.9 Security inconveniences

Information Security is more often found to be an inconveniences in the ICS/SCADA environment especially if it may result in a decrease in performance. Long passwords may hinder access in an emergency and Information Security should not affect alerts or alarms. The focus is more on Availability than on Confidentiality.

2.3.2.10 Other differences

Other differences between ICS/SCADA and IT networks include:

- No clear ownership. ICS/SCADA is often not controlled by Information Technology (IT) department but by an engineering or maintenance department, often referred to as Operational Technology (OT). Often these parties do not communicate or collaborate information or leverage of each other’s skills. These two departments, IT and OT, work in silos, do not share knowledge with each other and do not trust each other. Both parties like to take credit for SCADA, but not ownership (Pretorius & Van Niekerk 2016);
- Removable media (USB drives, DVDs/CDs, external drives) is part of daily operations in an IT department but pose a big risk when introduced to an ICS/SCADA environment. Amoroso (2013) indicates that removable media devices such as removable storage should be restricted in areas that have critical components of telecommunications infrastructure; similarly,

ICS/SCADA components of critical infrastructure should have limited exposure to removable media and mobile computing devices, as these could accidentally bypass security mechanisms and introduce malware or viruses. Most often ICS/SCADA systems does not have antivirus or have outdated antivirus and malware or viruses are not detected (Pretorius & Van Niekerk 2016);

- Inventory of ICS/SCADA components and network diagrams are generally outdated or not as comprehensive as IT network diagrams. In some cases, the networks, components, and safety systems are not even documented (Pretorius & Van Niekerk 2016);
- Physical security and environmental for ICS/SCADA differ from traditional IT networks. ICS/SCADA equipment most often resides in operational areas such as substations, cranes, conveyors, and haulers, which do not conform to best practices for IT server rooms. There are also additional environmental elements that needs to be considered, such as dust and protection thereof (Pretorius & Van Niekerk 2016); and
- Wireless communications are a point of debate: it is best to not use Wi-Fi for ICS/SCADA as these extents the range of attack, e.g. an attacker can sit outside the plant and hack the ICS/SCADA systems. However, in some ICS/SCADA environments there exist other wireless networks or wireless links, such as radio links and point to point wireless connections. Unfortunately, most of these wireless networks/link either use weak encryption mechanisms or old technology (Pretorius & Van Niekerk 2016).

2.4 ICS/SCADA Governance and Security

This section discusses the various ICS/SCADA governance and security controls and frameworks that exist, cyber-security incidents involving industrial control and related systems, the vulnerabilities and threats related to ICS/SCADA environments. Similarly to Section 2.3, aspects of this section were previously published or presented as outlined.

2.4.1 ICS/SCADA Control Frameworks

There are various international governance and security frameworks related to ICS/SCADA systems. This section provides a brief introduction to each security framework and are analysed in more detail in Section 5.4. The frameworks described in this section are:

2.4.1.1 NIST SP800-82

The National Institute of Standards and Technology’s (NIST) special publication 800-82, published a Guide to Industrial Control Systems (ICS) Security in 2006 (Stouffer *et al.* 2006). This provides guidance for establishing secure ICS/SCADA environments. The latest revision was released in 2015 (Stouffer *et al.* 2015).

2.4.1.2 ENISA

The European Union Agency for Network and Information Security (ENISA) published a standard called, *Protecting Industrial Control Systems: Recommendations for Europe and Member States.* (ENISA 2011). ENISA conducted a research and survey-based study to obtain the current perspective of ICS/SCADA protection for Europe, but including international environments. This includes threats, risks and challenges related to ICS/SCADA security. From the study they proposed seven recommendations for Europe and Member states in securing ICS.

2.4.1.3 CPNI framework.

The *Centre for the Protection of National Infrastructure (CPNI)* is the United Kingdom government authority which provides advice on securing national infrastructure to organisations (CPNI 2008). The CPNI published a framework, *Good Practice Guide: Process Control and SCADA Security*, to provide best practice principles for process control and SCADA system security.

2.4.1.4 Others

- *21 Steps to Improve Cyber Security of SCADA Networks* - The U.S. Department of Energy (2007) and President's Critical Infrastructure Protection Board developed this guide containing 21 steps to assist any organisation to improve their security for ICS/SCADA networks;
- *NERC CIP* – The North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) contains standards and security measures for protecting the North American bulk electric systems and it carry heavy fines for non-compliance (Knapp 2011); and
- *Safeguarding Australia from Cyberterrorism: A Proposed Cyber-terrorism SCADA Risk Framework for Australia* - Beggs and Warren (2008) propose a risk framework to assess Australian SCADA systems threats from cyber-terrorism. The framework integrated a cyber-terrorism capability assessment model with Australasian standards for SCADA risk assessments.

Figure 2.4 shows a high level comparison between the NIST, CPNI, and the frameworks from Section 2.2.4, namely COBIT 5 and ISO/IEC 27002. This shows at a high level how they align and which sections overlap. An in depth analysis between frameworks are discussion in Section 5.4.

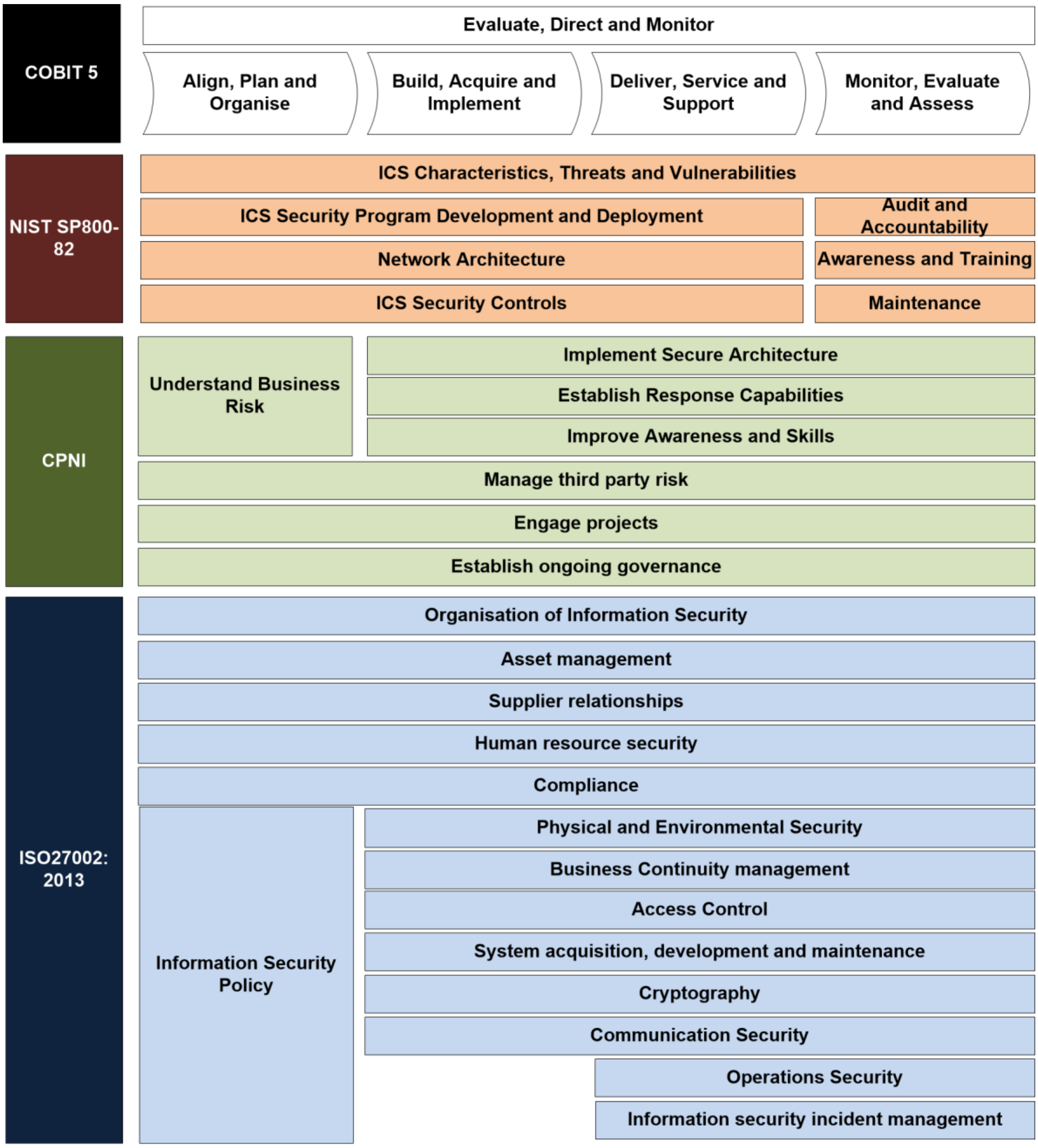

COBIT 5
Evaluate, Direct and Monitor
Align, Plan and Organise
Build, Acquire and Implement
Deliver, Service and Support
Monitor, Evaluate and Assess
NIST SP800-82
ICS Characteristics, Threats and Vulnerabilities
ICS Security Program Development and Deployment
Audit and Accountability
Network Architecture
Awareness and Training
ICS Security Controls
Maintenance
CPNI
Understand Business Risk
Implement Secure Architecture
Establish Response Capabilities
Improve Awareness and Skills
Manage third party risk
Engage projects
Establish ongoing governance
ISO27002: 2013
Organisation of Information Security
Asset management
Supplier relationships
Human resource security
Compliance
Information Security Policy
Physical and Environmental Security
Business Continuity management
Access Control
System acquisition, development and maintenance
Cryptography
Communication Security
Operations Security
Information security incident management

Figure 2.4: Alignment of Information Governance and Security Frameworks for SCADA

Source: Author compilation

2.4.2 Threats, vulnerabilities and attack methods against ICS/SCADA

In order to develop a comprehensive control framework that addressed the relevant risks, one has to look at the threats, vulnerabilities and risks related to the ICS/SCADA environment. The Centre for the Protection of National Infrastructure (CPNI 2008) list the following threat sources that should be considered at minimum:

- Hackers;
- Criminals;
- Internal attackers;

- Staff undertaking unauthorised actions;
- Disgruntled staff;
- Illegal information brokers;
- Corporate intelligence;
- Terrorists;
- Organised crime;
- Foreign intelligence services; and
- Protesters and activists (environmental, political, animal rights).

The CPNI (2008) also list the following threat types that should be considered: Malware (including viruses, Trojans, worms, backdoors, bots and spyware); loss of confidentiality, integrity or availability (denial of service); hackers (internal, external, external with insider knowledge); and unauthorised control.

The SANS Institute (2013) performed a survey and list the top 5 threat vectors as:

- Malware;
- Internal threats;
- External threats;
- Phishing; and
- Industrial espionage.

To determine if any vulnerabilities exist and to fully understand vulnerabilities, a detailed assessment of all the system components, (e.g. servers, workstations, network infrastructure) need to be performed (CPNI 2008). Table 2.2 provides a list of common vulnerabilities as listed by CPNI (2008), National Cybersecurity and Communications Integration Center (2014) and Stamp, Dillinger, Young and DePoy (2003). These vulnerabilities relate to administration, network architecture, devices and platforms. If problems exist with the SCADA security policy, this could lead to poor administrative procedures and vulnerabilities in the SCADA system. Each vulnerability has a significant impact on the SCADA operations (Stamp *et al.* 2003).

According to the 2014 and 2015 *Internet Security Threat Reports*, (Symantec 2014a, 2015), the number of newly discovered public SCADA vulnerabilities have decreased from 129 in 2011 to 85 in 2012 and a significant decrease to 39 in 2013 and 35 in 2014. This decrease could be due to attention that has been placed on SCADA security following the discovery of the Stuxnet worm in 2010. Denial of service (DoS), buffer overflow and information disclosure vulnerabilities account for over 60% of the detected vulnerabilities in 2014 and 2015. Detailed analysis is discussed further in Section 5.2.1.

Table 2.2: Common Vulnerabilities

Category	Vulnerability
User and Device Access Management	There are no password controls (password length, complexity, passwords don't expire etc.)
	Passwords are often stored in plain sight near critical systems.
	Passwords are not encrypted in transit.
	Passwords are shared.
	Power-on and screen saver passwords are not used.
	Minimal administrative access controls are applied. Users have administrator privileges.
Patch Management	Operating System, Database and Application security patches are not updated.
Configuration Management	No backup or documentation of configurations for network device, equipment and platforms.
	No resilience and continuity of systems.
	Default Operating Systems, Databases and Application configurations are used, which enables insecure and unnecessary services.
Network perimeter/Connections to other systems	SCADA networks are directly connected to IT or corporate networks. Firewalls are non-existent or poorly configured at interfaces to IT or corporate networks.
	SCADA networks are used for non-SCADA traffic, e.g. CCTV.
	Dial-up access exists on individual workstations within the SCADA network.
Monitoring & Logging	System logs are neither collected nor reviewed.
	There is no security monitoring on the SCADA network.
	Firewall and router logs are neither collected nor reviewed.
Remote Access	Authentication for remote access is insufficient or non-existent.
	Remote access into the SCADA network uses shared passwords and shared accounts.
Physical Security	There is not proper physical protection of equipment (network, platforms and devices).
	Physical access to equipment is not restricted to critical personnel only.
	Environmental controls are not considered.
Wireless Connections	Wireless LAN technology used in the SCADA network do not have strong authentication.
	Wireless connections use default configuration/passwords and/or no data protection between clients and access points.
Anti-virus/Malware Protection	Antivirus software does either not exist or is outdated.
	Removable media is used and not scanned with antivirus or scan with outdated antivirus software.

Adapted from: CPNI (2008), National Cybersecurity and Communications Integration Center (2014), (Stamp *et al*, 2003)

This shows the importance that the availability characteristic of information plays in the SCADA environment. SCADA systems can be classified as high availability systems. Availability enables SCADA systems to be provide information, when needed, without interference or obstruction to authorised users in the right format (Whitman & Mattord 2012). In order to ensure availability of SCADA systems, denial of service attacks must be stopped.

2.4.3 ICS/SCADA incidents

A number of ICS/SCADA security incidents have been recorded. The most notable of these are:

2.4.3.1 Malware

In 2003 the Davis-Besse Nuclear Power Plant's Safety Parameter Display System and Plant Process Computers were disabled for a few hours due to a SQL Slammer infection as a result of an unpatched machine (Chileshe & van Heerden 2012; Miller & Rowe 2012). The CSX Corporation had a number of their systems shot down in 2003 due to the Sobig virus. This caused train delays and impact on the business (Miller & Rowe 2012).

From 2010 to 2012 a series of malware variants, including the infamous Stuxnet and Flame malware, infected machines. These variants are reportedly related to Duqu and Gauss. Stuxnet affected programmable logic controllers, and resulted in physical damage to an Iranian nuclear facility (Nakashima & Warrick 2012; Nakashima, Miller & Tate 2012; Rodionov 2012). In June 2014 the Havex malware was reported to be collecting data from ICS and SCADA systems in the energy sector (Walker 2014).

The BlackEnergy malware was used to target the Ukrainian power grid and contained modifications to disrupt industrial control systems (Kovacs 2016). This was the first known instance where a cyber-attack caused a blackout. The hackers gained access to the control systems via a SSH backdoor.

2.4.3.2 Suspected foreign intelligence services

In 1982 a trans-Siberian pipeline exploded, alleged due to a logic bomb inserted into the control system design by the CIA. The explosion was reported to be 3kT TNT equivalent (Miller & Rowe 2012; Weiss 2008; Andress & Winterfield 2011).

Reports indicate that the Baku-Tbilisi-Ceyhan pipeline control systems were compromised in 2008, and this resulted in an explosion (Robertson & Riley 2014). Speciously hackers super-pressurised the crude oil in the pipeline and shut down alarms and communication to warn about this. They gained access to the alarm management system via a vulnerability in the camera communication software. A professor of the national security affairs at the US Naval War College stated this "rewrites the history of cyberwar."

2.4.3.3 Insider threat

In 1992 an ex-employee who was fired, hacked into Chevron and disabled the emergency alert network. It was not detected until an actual emergency arose and the system failed (Miller & Rowe 2012). In 1999 hackers with the aid of a disgruntled insider used a Trojan to access the controls for the Gazprom pipelines (Miller & Rowe 2012).

A disgruntled employee of the company supplying controllers to an Australian sewerage company, Maroochy Water System, gained remote access in 2000 to the sewerage system and released sewerage into the waterways in an attempt to get a job with the municipality (Abrams & Weiss 2008; Wyld 2004).

The Target breach was traced back to stolen third party credentials, where the vendor was a heating, ventilation and air-conditioning (HVAC) sub-contractor (Krebs 2014). This hack was discussed in more detail in Section 2.2.5.

2.4.3.4 Hackers

For over a month in 1994 a hacker used a dialup modem to gain access and install backdoors to access billing information of Salt River, however could also gain access to the monitoring and delivery systems for power and water. The attacker had a five-hour session connected to the canal control systems (Miller & Rowe 2012).

In 2001 foreign hackers gained access to the California System Operator computer networks for two weeks, but were not able to access the PCS networks (Miller & Rowe 2012). Polish trams were derailed in 2008 due to a switching system being compromised and change using basic remote control electronics (Leyden 2008). Late in 2014 a blast furnace at a German steel mill was damaged after hackers obtained access to the mill’s control systems (BBC 2014).

2.4.3.5 Vulnerabilities

In September 2014 a vulnerability in the Bash shell of Linux was announced. This vulnerability allowed for remote code execution, and some SCADA systems were vulnerable. The full extent of device affected by the ShellShock bash bug is still not known. Siemens released an update for the SIMATIC PCS 7 to patch several vulnerabilities. The SIMATIC PCS 7 is affected by the vulnerabilities because of the software WinCC being incorporated into the product (Kovacs 2014). It was revealed in 2015 by researchers of the existence of vulnerabilities in SCADA components used in modern railways (Paganini 2016).

2.4.3.6 Nuclear power plant

The head of an international nuclear energy group indicated that a disruption at one of their nuclear power plants was caused by a cyber-attack (Brook 2016).

2.4.3.7 Other incidents

Whilst not necessarily compromising ICS/SCADA, have affected systems key to the operation of critical infrastructure and related organisations. These incidents include:

- Carmel Tunnels Toll Road – on 8 September 2013 a Trojan infected the Israeli toll plaza, specifically targeting the security camera system, hindering essential operations over two days and caused financial damage (Ashford 2013);
- Saudi Aramco – on 15 August 2012 Saudi Aramco was forced to shut down its network due to a serious malware infection affecting approximately 30 000 machines, however the main operations systems were not affected (Leyden 2012; Mills 2012);
- Conficker – in 2009 the Conficker worm affected a French military airfield, preventing aircraft from taking off, and British warships (Kirk 2009; Willsher 2009);
- Antwerp port – in 2013 hackers used remote access devices to aid smuggling operations at the port; it is possible that the hackers could control the logistics system (Dunn 2013);
- Oil rigs – in 2014 it was reported that an oil rig was disabled after hackers tilted it, and another was inoperable for 19 days due to malware infection (Wagstaff 2014);
- Warsaw airport – in 2015 aircraft were grounded after a denial of service attack disrupted the network (Brook 2015); and
- Researchers have demonstrated that many vehicles can be hacked if physical access can be gained, and once hacked some vehicles can be controlled (Higgins 2015). Another researcher reportedly compromised an aircraft's controls by hacking the in-flight entertainment (Zetter 2015).

These incidents indicate that the threats against ICS/SCADA systems are real and not unnecessary panic. The following section outlines the vulnerabilities and the attacks methods that threats use to target them.

2.5 ICS/SCADA in South Africa

This section covers the ICS/SCADA implementations and relevant South African legislation and governance frameworks. Challenges in the South African environment are described. Similarly, to Section 2.3, aspects of this section were previously published or presented as outlined.

2.5.1 SCADA Implementations in South Africa

Chileshe and van Heerden (2012) listed where ICS/SCADA systems are implemented in South Africa and include Eskom, the mining and mineral processing industry, the sugar industry, and the Durban water recycling plant. Other ICS/SCADA environments include eThekwini/Durban Electricity (Online Tenders 2014), petro-chemical industry, the automotive industry, breweries, and transport industries (Gautrain, ports, railways and pipelines). The physical transport infrastructure also includes the airports operated by the Airports Company of South Africa, and the various toll roads, including e-Tolls. Krutz (2006) indicates that ports have SCADA systems in cranes, terminal equipment, and locks; railways contain signalling and control elements for waysides.

As many of these implementations are related to critical infrastructure upon which the South African economy is based, a major cyber-attack disrupting any of these process-driven industries could have drastic economic and secondary social consequences.

In December 2009 a South Africa petro-chemical company's SCADA systems were affected by the 'PE_Sality' virus, resulting in the operators have to run the plant with limited of no visibility for eight hours before the infected servers were recovered (Cusimano 2010).

The Wolfpack Information Risk team, recently conducted a survey in South Africa on Critical Infrastructure (Wolfpack 2016). This research was conducted independently and at the same time as this study was being conducted and the report, *Critical Information Infrastructure Protection Report*, was released in June 2016. A small section of the survey and report was dedicated ICS/SCADA systems while the rest of the survey and report was on Critical Information Infrastructure such as Information Security Governance and Risk Management, Legal Regulation and Compliance, Critical Access Management, Human Resource Management and Supplier Security, Physical (Environmental) Security, Security Architecture and Design, Telecommunications and Network Security, Access Control, Operational Security, Cryptography, Software Development and Application Security, and the National CII landscape. The Wolfpack survey was distributed to a different audience as this study and the number of participant related to the ICS/SCADA part could not be determined. The Wolfpack survey found that the top four threat vectors for ICS/SCADA systems are: Insider exploits, and combined secondly, External threats, Attacks originating within the internal network and Information security policy violations. Detailed analysis is discussed further in Section 5.2.5.

2.5.2 South African Legislation and Governance Related to ICS/SCADA

There are a number of legislation and governance frameworks specific to South Africa that relate to ICS/SCADA. The National Key Point Act deals with security of critical infrastructure or resources; there is a proposal to repeal this act and replace it with the Crucial Infrastructure Act. The Electronic Communications and Transactions (ECT) Act (Government of Republic of South Africa 2002a) sets out regulations for electronic communications, and provides outlines of basic security and prohibited actions. Prohibited actions include the intentional interference of electronic communications, which will apply to communications amongst SCADA systems and the various subcomponents.

The Regulation of Interception of Communications and Provision of Communication-Related Information (RICA) Act (Government of Republic of South Africa 2002b) is also relevant to ICS/SCADA. Whilst the public focus of RICA has been on cellular phones, this act is applicable for ICS/SCADA environments where there are remote units that connect to the SCADA server via an Access Point Name (APN) or Virtual Private Network (VPN). As these units contain subscriber identity module (SIM) cards, they are required to comply with the RICA act.

The Protection of Personal Information (POPI) Act (Government of Republic of South Africa 2013) requires the protection and safeguarding of personal as well as corporate data by ensuring safeguarding of the information. Certain ICS/SCADA systems host critical information on their databases and vendors may have access to this information or sensitive configuration information. In such cases it will be necessary for controls to be implemented to ensure compliance with the act.

The National Cybersecurity Policy Framework provides for national and sector response teams, a National Cybersecurity Advisory Council, and other initiatives. Furthermore, a draft Cybercrimes and Cybersecurity Bill (Government of Republic of South Africa 2015) has been released and could also have a potential impact on the ICS/SCADA environments in South Africa if enacted. King III is a corporate governance framework, which apportions accountability to the board and executives of the organisation. ICS/SCADA systems will need to be adequately governed in order to comply with the requirements.

The acts discussed in this section may not be obliviously applicable to ICS/SCADA environments, however as is evident, under certain conditions they are applicable. Therefore, IT governance and security functions may in future be required to have more oversight into ICS/SCADA systems.

2.5.3 Challenges

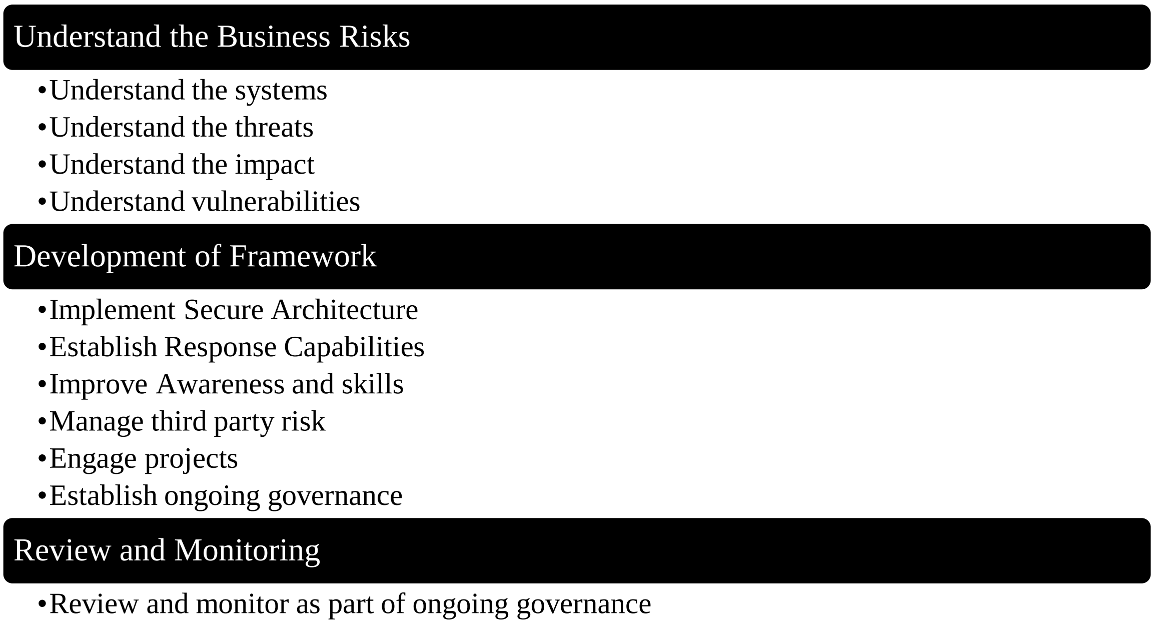
The differences between SCADA and traditional IT discussed in Section 2.3.2 result in a number of challenges, which need to be taken into account when developing a control framework for South Africa. The outdated systems, particularly Windows XP which is no longer supported, makes implementing patching impossible, resulting in vulnerabilities that are difficult to mitigate. In addition, patching and security mechanisms often cannot be done on a live production environment, which limits the time period in which to do this. In some environments, there are only one or two days in the year in which the company’s operations or plant are not operational.

ICS/SCADA often falls under the responsibility of engineering and not IT, therefore IT security has less influence over the systems. Therefore, there are extra challenges in achieving buy-off from all stakeholders, particularly given the other challenges and business impact described above.

2.5.4 Framework development

The framework development process consisted of a number of steps. The overall background needs to be understood, including the business environment, the systems, threats, and vulnerabilities (CPNI 2008). The CPNI (2008) list the following steps in developing a framework: Understand the business risks → implement secure architecture → establish response capabilities → improve awareness and skills → manage third party risk → engage projects → establish ongoing governance. To fully understand the business risk, one has to understand the risks, threats, impact, and vulnerabilities.

The process can also be group together as displayed in Figure 2.5.



Understand the Business Risks

- Understand the systems
- Understand the threats
- Understand the impact
- Understand vulnerabilities

Development of Framework

- Implement Secure Architecture
- Establish Response Capabilities
- Improve Awareness and skills
- Manage third party risk
- Engage projects
- Establish ongoing governance

Review and Monitoring

- Review and monitor as part of ongoing governance

Figure 2.5: Framework development steps

Adapted from: CPNI (2008)

Before a control framework is developed, it is important for a company to understand the risk they face from likely compromises to ICS/SCADA systems. To fully understand the business risk, an organisation needs to start by understanding of the system or environment, then the threats, impact and vulnerabilities that could have an impact to the environment. Each of the steps from ‘Understanding the business risks’ needs to be conducted as a step on their own. The following steps all from part of the framework development and is grouped thereunder: Implement secure architecture, establish response capabilities, improve awareness and skills, manage third party risk, engage projects and establish ongoing governance. This can be displayed in a process or methodology on developing a control framework, taking into account the above. The steps in the methodology is illustrated in Figure 2.6.

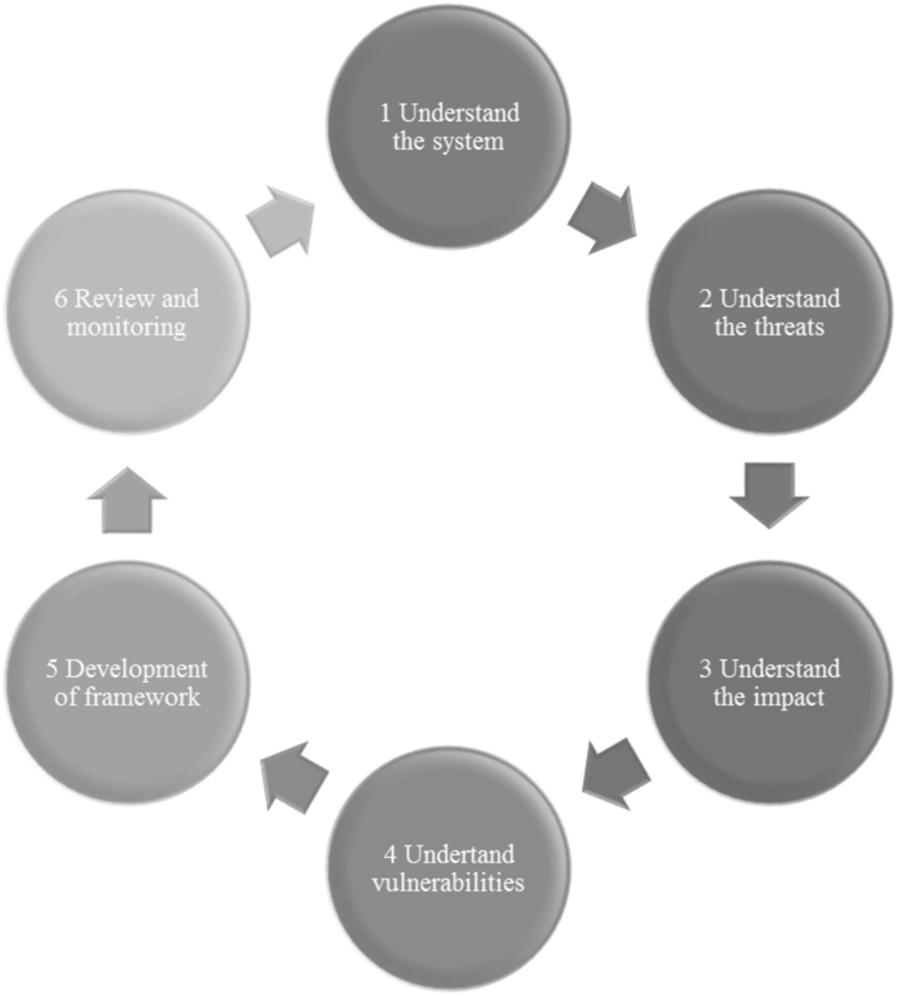


Figure 2.6: Framework Development Methodology

Adapted from: CPNI (2008)

2.5.4.1 Understand the system

An organisation or company needs to conduct a formal inventory and analysis of the ICS/SCADA systems and components in the environment. This include the role of each system is, location, owner, management and support thereof, and business criticality CPNI (2008).

2.5.4.2 Understand the threats

The threats to ICS/SCADA environment needs to be fully evaluated. Examples include: hackers, viruses or malware, unauthorised control. Refer to Section 2.4.3 for list of threats to ICS/SCADA environment CPNI (2008).

2.5.4.3 Understand the impact

The impact and consequences that a threat could have to the ICS/SCADA environment should be understood and documented. This could include financial loss, loss of life, operations downtime, and reputational loss CPNI (2008).

2.5.4.4 Understand vulnerabilities

Vulnerability assessments should be conducted for the ICS/SCADA environment to determine possible vulnerabilities. Section 2.4.3 contains a list of possible vulnerabilities to ICS/SCADA systems CPNI (2008).

2.5.4.5 Development of frameworks

A control framework is developed based on the business risk assessment, which include the threats, impact and vulnerabilities to the ICS/SCADA environment. The framework should include technical, procedural and management controls to adequately protect the ICS/SCADA systems. The framework should also include: Implementation of secure architecture, establishment of response capabilities, improvement of awareness and skills, management of third party risk, project management and establishment of ongoing governance CPNI (2008).

2.5.4.6 Review and monitoring

It is important to regular review the above steps as any changes to systems, threats, impact or vulnerabilities will change the business risk and either render certain controls in the framework outdated or inadequate. Example an implementation of new technology such as LTE brings new risks, threats and vulnerabilities to the organisation and adequate mitigating controls needs to be implemented to cater for them. Ongoing monitoring of the environment needs to take place to identify any new systems changes, threats, vulnerabilities and corresponding update of the control framework should take place at minimum annually CPNI (2008).

2.6 Summary

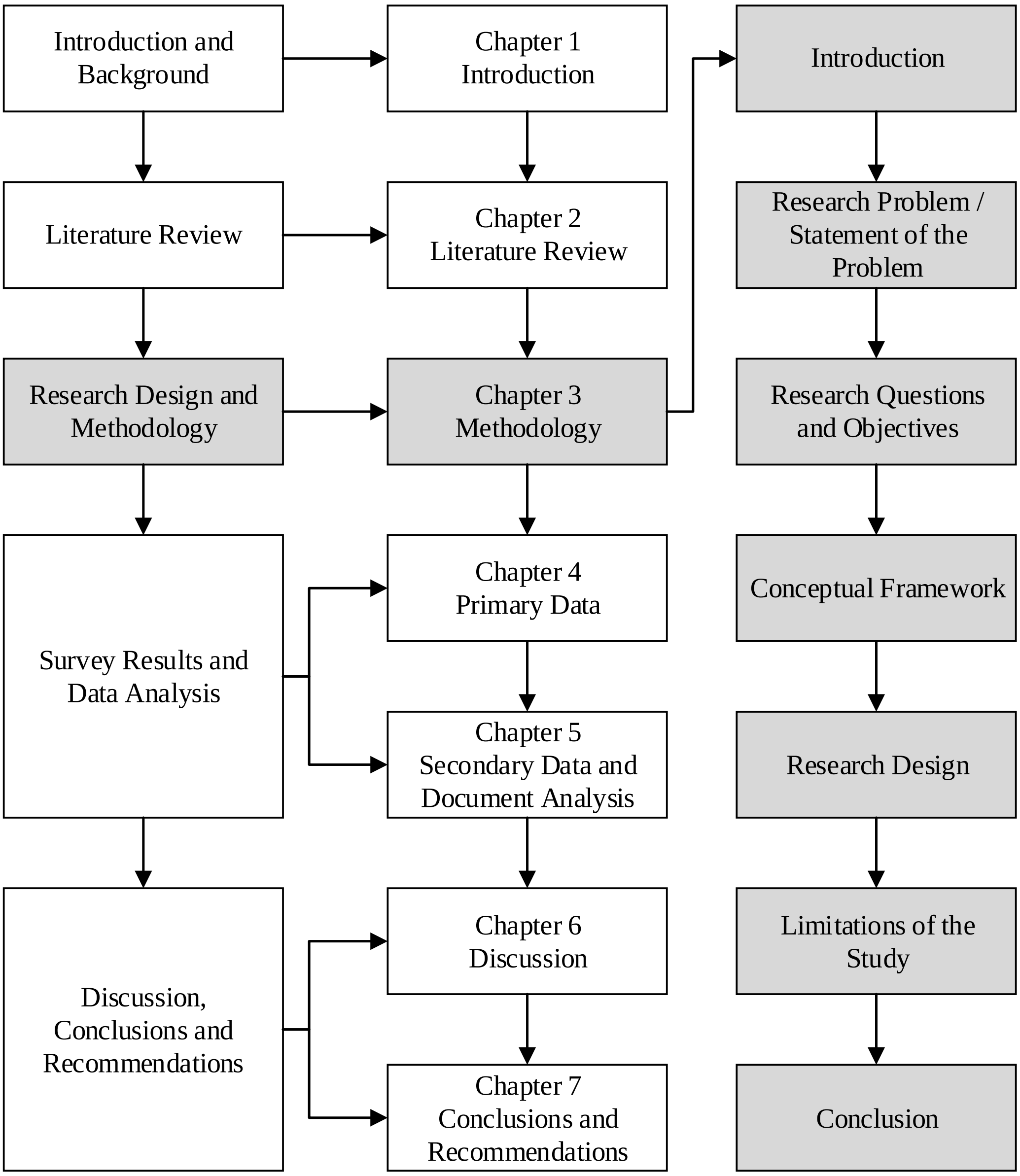
Information Security, its risks and controls in general were discussed. Internationally cyber-crime has increased and in South Africa, millions have fallen victim to cyber-crime. Cyber-crime has cost the South African economy billions in 2015. The vulnerabilities and threats related specifically to ICS/SCADA were discussed. As is evident from the incidents that have already occurred, the ICS/SCADA environment can be targeted and can cause significant disruption.

South Africa has a number of ICS/SCADA implementations in infrastructure that is crucial to the economy; it is therefore important that these are protected. Security in the SCADA environment face a number of challenges. There exist international control frameworks, which if organised with a defence-in-depth approach, may overcome these challenges and provide a sufficient level of protection to these ICS/SCAD systems. The methodology to develop control framework for ICS/SCADA was also discussed. The next chapter discusses the research methodology.

Chapter 3 Methodology

3.1 Introduction

This chapter highlights the research problem and the significance and contribution of the study. The research questions and research objectives are discussed. Methods of the research design are examined in relation to the research onion. The sampling strategies including the population, size, and data collection methods are explored. The data analysis and conceptual framework together with questionnaire design are mentioned. Figure 3.1 is a graphical representation of the outline of this chapter and overall structure.



Introduction and Background
Chapter 1 Introduction
Introduction
Literature Review
Chapter 2 Literature Review
Research Problem / Statement of the Problem
Research Design and Methodology
Chapter 3 Methodology
Research Questions and Objectives
Survey Results and Data Analysis
Chapter 4 Primary Data
Conceptual Framework
Chapter 5 Secondary Data and Document Analysis
Research Design
Discussion, Conclusions and Recommendations
Chapter 6 Discussion
Limitations of the Study
Chapter 7 Conclusions and Recommendations
Conclusion

Figure 3.1: Graphical representation of Chapter 3 outline

3.1.1 Significance and Contribution of the study

This study provides a unique South African view point. ICS/SCADA security is still a growing field in South Africa and has not as yet been fully established. There are limited academic studies done for South Africa (Chileshe & van Heerden 2012) therefore this study aimed to fill this gap.

This study assessed the current state of ICS/SCADA security in South Africa and from the analysis an ICS/SCADA control framework was to address common concerns by taking into account new and existing legislation. This ICS/SCADA control framework will enable organisations to improve security and governance of their ICS/SCADA systems which will lead to greater availability and reliability of computer systems running their operations.

3.2 Research Problem/Statement of the Problem

There is no or limited information available as to the current state of ICS/SCADA in South Africa including the factors influencing ICS/SCADA and how they are governed. This research assesses the current practices of ICS/SCADA in SA, to develop a consolidated framework aligned to South Africa taken into account new and existing legislation.

3.3 Research Questions and objectives

3.3.1 Research Questions

The research questions underpinning this study were:

- What are the factors (vulnerabilities and threats) influencing ICS/SCADA security in South Africa?
- What are the best measures to govern these factors that influence ICS/SCADA security in South Africa?
- What is the impact of non-governed ICS/SCADA?
- How are ICS/SCADA secured and governed?
- What are the perception of the suitability of the implemented controls/measures to mitigate the treats and risks?

3.3.2 Research Objectives

The objectives of this study were:

- To determine the factors (vulnerabilities and threats) influencing ICS/SCADA security in South Africa.
- To determine what the best mitigating controls to govern and secure ICS/SCADA systems in South Africa are.
- To determine the impact of non-governed ICS/SCADA.

- To determine how ICS/SCADA in South Africa are secured and governed.
- To establish if the confidence levels of implemented controls/measures mitigating the threats and risks are sufficient.
- To develop a control framework addressing the shortfalls for ICS/SCADA security in South Africa.

3.4 Conceptual Framework

Elements of Technology Acceptance Model (TAM) and the Protection Motivation Theory (PMT) were used. TAM explains that technology cannot improve an organisations performance if they are not being used (Davis, Bagozzi, & Warshaw 1989). This similar model relates to a governance framework, which cannot improve an organisations risk profile if it is not being used. In order to understand and predict user acceptance, one needs to better understand why technology/control frameworks are either accepted or rejected by people. TAM was previously used for cyber-security in a study by Cheng and Shi-bo (2014).

The protection motivation theory was initially developed by Rogers (1975) to better understand the impact of fear appeals and how to cope with them. He later expand on the theory (Rogers 1983) where he expanded the theory to a general impact of persuasive communication. The PMT suggests protections based on the following factors:

- The perceived severity of a threatening event (impact);
- The perceived likelihood of the occurrence (probability) or threats and vulnerabilities;
- The efficacy of the recommended preventive behaviour; and
- The perceived self-efficacy.

The protection motivation theory was used in a cyber-security study by Sommestad, Karlzen and Hallberg (2015) and recently in an information security study by Kinnunen (2016).

The first two variables of PMT, (perceived severity of a threatening event and perceived likelihood) forming the Threat Appraisal and the latter (the efficacy of the recommended preventive behaviour and perceived self-efficacy) the Coping Appraisal. When combining this with the elements of TAM, the perceived usefulness (usability of security) and perceived ease-of-use (ease of use of security), the model as shown in Figure 3.2 is formed. In summary, the probability and impact (red blocks) and coping response (blue block) are from the PMT model. The usability of security (green block) from TAM and the perceived ease-of-use (green block) from both TAM and PMT.

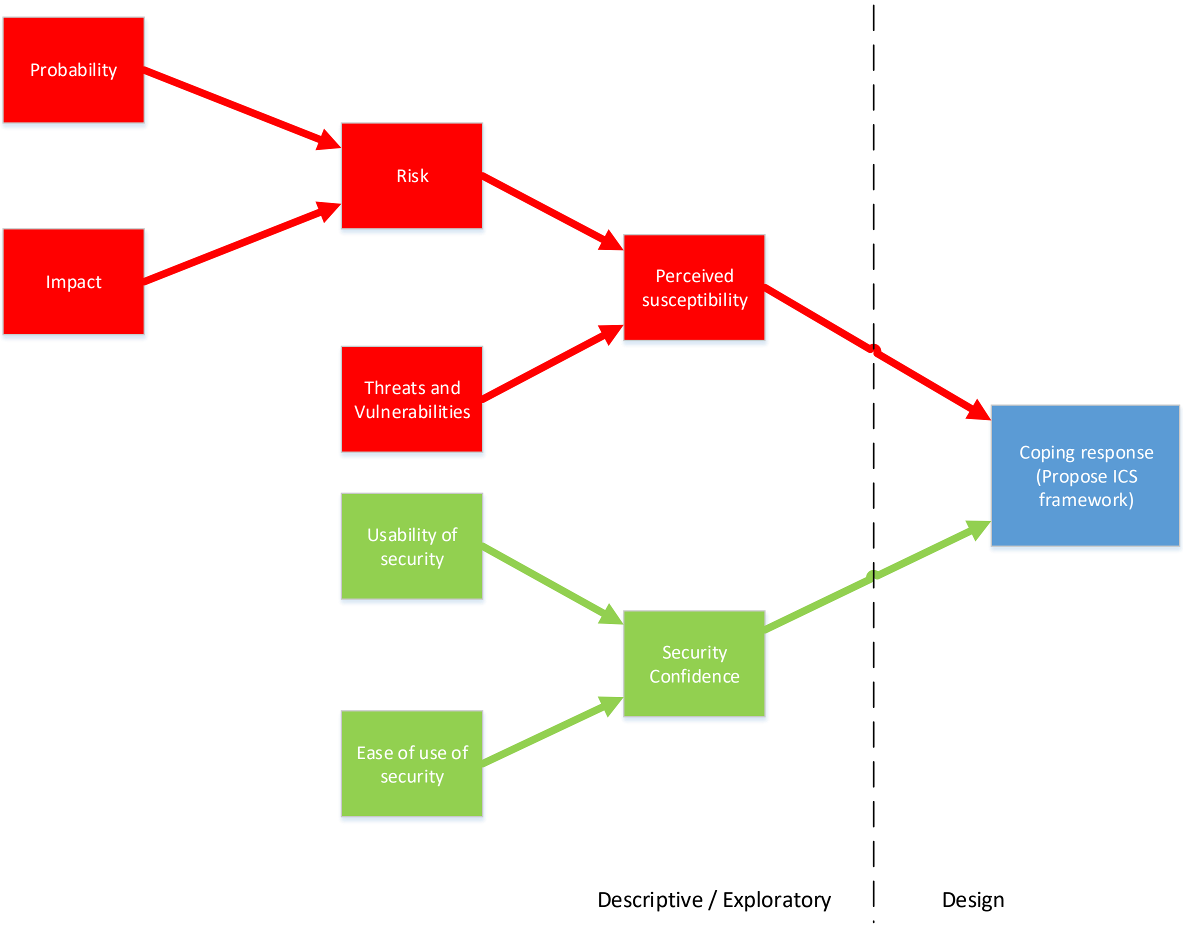


Figure 3.2: Research Framework

Source: Author compilation

The general definition used to calculate risk is that risk is the product of the probability and impact. I.e. Risk = Probability x Impact. (Boehm 1991). The risk together with the threats and vulnerabilities (Red Blocks) creates the perceived susceptibility (Red Block). Combining the usability and the ease of use of security (Green Blocks) provides the security confidence (Green Block). The security confidence and perceived susceptibility is used to create the proposed coping response or ICS/SCADA control framework (Blue Block).

3.5 Research Design

3.5.1 Research Onion

Researchers normally propose a piece of research to answer a question or address a problem. The researcher begins by determining what data are needed and then decide how they will obtain the data. Various techniques like questionnaires, observation and analysis can be used to obtain the data. The final decision about the overall research will only be represented by techniques used to obtain data, and the methods to analyse these data (Saunders & Tosey 2013). They used the representation of the 'Research Onion' to illustrate how the final design (the inner layer of the research onion) needed to be considered in relation to other design elements (the outer layers of the research onion). Figure 3.3 is a representation of the proposed 'Research Onion' and the different design elements that were used to conduct this research. Each layer is discussed in Section 3.5.2.

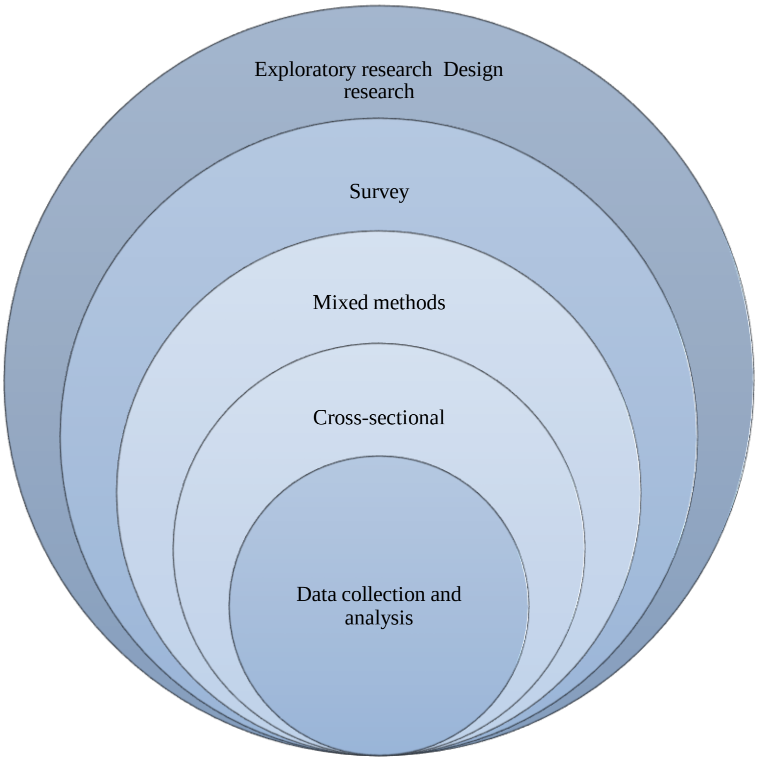

Exploratory research Design research
Survey
Mixed methods
Cross-sectional
Data collection and analysis

Figure 3.3: Research Onion for the Study

Adapted from: Saunders and Tosey, 2013

3.5.2 Research design

The outer layers of the research onion consists of the exploratory research and design research. The design research, mainly focus on research around the process of design and developing from the work in the design methods. The concept is expanded to include research embedded within the process of designing a control framework.

A survey strategy is used. It offers a highly economical way of collecting large amounts of data to address who, what, where, when and how of the factors influencing the frameworks in South Africa. This strategy generated both rich and statistical data.

A mixed methods approach was used for data collection and analysis, refer to research Approaches/Paradigms in Section 3.5.3.

The next layer in the research onion is a cross-sectional study, which analyses data or responses from a survey at a specific point in time. This type of study is used as one of the research objectives is to determine the state of ICS/SCADA in South Africa and the cross-sectional study, which uses qualitative and quantitative research surveying both people and documents measured the state of SCADA/ICS in South Africa at a single point in time.

The inner layer of the research onion includes decisions on the sample groups, and content of the questionnaires. The results of the questionnaires, questions, data analysis and decisions forms part of the input in the methodology to develop a control framework to address the gaps.

3.5.3 Research Approaches/Paradigms

There are two general categories of research methodologies; quantitative and qualitative. The first method, quantitative provides numerical predictions, percentages, frequency, occurrence, trends, and others (Patton 2005) whereas the latter, qualitative method describes data at an in-depth level, without data analysis or statistics and helps to understand how a person is thinking or why an event occurs.

A mixed methods approach is used. Both quantitative and qualitative research methods are used in the process of the study, data collection and analysis. This includes questionnaires, systems data, results from Shodan and analysis of documents from security alerts and advisories. Using mixed methods assists to offset limitations and fill/predict gaps in data should these exist in the individual methods. A combination of exploratory and design research is used to develop the research or conceptual framework, refer to Section 3.4.

3.5.4 Study Site

South Africa is the area of study with specific focus on various professional organisations and companies running ICS/SCADA systems with a focus on South Africa.

3.5.5 Data collection methods

In the study, different documentary evidence was collected. Questionnaires was sent out using email to the target population, refer to Section 3.5.6. Documents such as existing frameworks, security alerts reports and trends was obtained. Data from Shodan (a tool to search for internet connected devices) and data from security systems was obtained and sanitised. The different collection methods are set out in Table 3.1.

Table 3.1: Data collection methods

Source:	Risk (Impact & Probability)	Threat	Vulnerability	Security confidence (Ease of Use & Usability)
Questionnaire	Yes	Yes	Yes	Yes
Security system data		Yes	Yes	
Shodan (open source tool)		Yes	Yes	
Reports and security alerts and advisories		Yes	Yes	

3.5.6 Target Population

The target population included information security, governance and SCADA/ICS professionals. The intent was to specifically focus on people with relevant SCADA/ICS experience in order to obtain valuable/useful information. The ISACA South Africa chapter, which is the largest IT security and governance professional body in the country, as well as a large SOC, both contain members with the relevant professional experience to participate in the questionnaires. The questionnaire was distributed to members of the ISACA community and the large SOC.

3.5.7 Sampling Strategies

A sample is a subset of the full population from which data is obtained by the researcher (Yin 2009). The sample of this study was selected from information security, governance and SCADA/ICS professionals who have experience with SCADA security. The questionnaire had a covering question to establish the experience of the respondent.

As the number of organisations and professionals that have knowledge of ICS/SCADA systems was unknown, a sample size could not be determined upfront. A sample size for the questionnaires was anticipated to be at minimum 30 people across various professional organisations and companies running ICS/SCADA systems. These include ISACA and a large SOC, as mentioned in Section 3.5.6. These organisations were selected based on convenience of access. ISACA is the largest body of professionals with cyber-security and IT governance knowledge in South Africa and therefore there was a higher change of receiving valid responses.

The sample for the document analysis was chosen by selecting common and freely available framework and standards related to Governance, Information security and ICS/SCADA. International best practices (e.g. standards from CPNI, COBIT) were used.

3.5.8 Data Quality Control

There are multiple methods that were used. The data triangulation brings together the data from multiple methods which complements each other and improves data quality. The data collected from the questionnaires and the document analysis was compared to ensure reliability and validity.

3.5.9 Measurements

A combination of sematic differential and Likert scales were used. The first to determine the population's attitude toward ICS/SCADA security and the latter, Likert, to scaling responses from the questionnaires. Secondary data was measured as explained in Section 3.5.10.

3.5.10 Data analysis

The art of analysing raw data with the objectives of drawing assumptions about the information, is data analysis according to Rubin (2008). The systematic procedure for evaluating or reviewing documents is defined according to Bowen (2009) as document analysis. Data was collected through questionnaires, and documents was analysed using thematic analysis method which identified themes within the data and reporting them. This is method is suitable as the analysis of the data using this technique consolidates or groups the data collected and then describes the data sets in detail.

The data from questionnaires was analysed using descriptive statistics. Data collected from Shodan, reports and advisories, was also analysed using descriptive statistics which summarised and described the data to determine the perceived susceptibility.

Data from multiple network security devices were obtained for a two-year period and anonymised. The data from the network devices was categorised into the vulnerability categories for further analysis.

COBIT was initially selected as it is a well-documented control framework aligned with other frameworks. The relevant categories were divided into pre-determined categories based on Information Security controls as described in Section 2.2.3. As the other documents were analysed additional categories were included if they were not already considered. Microsoft Excel was used for the coding and summarising process. The coding was as follows: red if nothing is mentioned about the control, orange if the control is briefly mentioned, yellow if the control mentioned cannot be implemented immediately and require modification to align to an ICS/SCADA environment and green is the control is relevant to an ICS/SCADA environment

Reports from security vendors was used as secondary data. Data from reports were categorised into various threat categories and compared to each other to determine the top threats and vulnerabilities.

Descriptive statistics was used to analyse the data to show patterns and summarise the data to determine the perceive threats, risks and vulnerabilities to be in order to develop a control framework for ICS/SCADA in South Africa. Due to the author’s Honours Degree in Statistics, the statistical analysis was performed by the author.

Correlation is used to determine the relationship between two variables. Where the correlation coefficient, *r*, is between example -0.3 to -0.1, the correlation is weak. A strong correlation is when the correlation coefficient, *r*, is between -1 to -0.5 or 0.5 to 1 (MathBits 2016).

Using a combination of the various analysis enables data to be treated in a way that will make it possible to interpret the requirements to develop a control framework to address the short falls in ICS/SCADA security and governance.

3.6 Questionnaire design

The questionnaire was one of the main research instruments. Closed-ended Likert scale questions were used in line with the study's objectives. A covering question was asked to determine the experience of the respondent with ICS/SCADA systems. Those with no knowledge of ICS/SCADA systems was then further excluded from the study.

Table 3.2 lists an outline of the questionnaire. The complete questionnaire can be found in Appendix A. Table 3.3 links the research objectives to the relevant questions.

Table 3.2: Outline of questionnaire

Section	Details
Section A	Demographics
Section B	ICS/SCADA experience
Section C	Factors influencing ICS/SCADA
Section D	Best measures to govern and protect

Table 3.3: Research Objective linked to Questions

Research Objective	Question reference
RO1: To determine the factors (vulnerabilities and threats) influencing ICS security in South Africa	Section C (C2, C4, C5)
RO2: To determine what the best mitigating controls to govern and secure ICS/SCADA systems in South Africa are.	Section C (C6)
RO3: To determine the impact of non-governed ICS	Section C (C3, C7, C8, C9)
RO4: To determine how ICS in South Africa are secured and governed	Section D (D1, D2, D3 (maturity))
RO5: To establish if the confidence levels of implemented controls/measures mitigating the threats and risks are sufficient	Section D (D4, D5, D7)
RO6: To develop a control framework addressing the shortfalls for ICS security in South Africa	N/A

3.6.1 Ethical and administrative consideration

A research proposal was presented to the Higher Degrees Committee of the School of Management, Information Technology and Governance at University of KwaZulu-Natal. Comments and suggestions from the members were noted and incorporated. Refer to Appendix F for the approval letter. This dissertation was also send for language and technical editing, refer to Appendix E.

Ethical approval for this research was obtained from the University of KwaZulu-Natal Ethics Committee, a gate keeper memorandum from large State Owned Company (SOC), who wished to not be named, and a gate keeper's letter from ISACA South Africa. There is no impact on human dignity. Informed consent from respondents was obtained prior to them participating in order to allow them to make the decision to participate based on adequate knowledge of the study. All the respondents to the questionnaire were anonymous. Any corporate data used in the study was anonymised and names were de-identified to ensure confidentiality and integrity.

3.7 Limitations of the study

This is unique to the South African situation, but can be generalised beyond South Africa. It was difficult to determine statistical reliability as there is uncertain population size, limited studies on governance and security of ICS/SCADA conducted in South Africa and difficult in determining the individuals with ICS/SCADA knowledge. The questionnaire was sent out to the broader community, refer to Section 3.5.7, and a question was included upfront to determine the relevance of the respondents.

Inconsistency of reports from security vendors were discovered during the document analysis. This includes differences between current and previous year's categories as well as different categorisation used between the various vendors. This could lead to some bias towards certain vulnerabilities and threats complicated the overall analysis. From the study's perspective, this might only have a small implication, however this might impact someone in the industry trying to use various reports to determine the top vulnerabilities and might wrongly place emphasis on non-prevalent vulnerabilities.

3.8 Summary

This chapter discussed the research problem and objectives and the research methodology that was used in the study as well as limitations. This study employed mixed methods that were discussed. The target population, sampling strategies, data collection and data analysis was described. A conceptual framework was also discussed. The next chapter analyses the primary data which is the survey or questionnaire.

Chapter 4 Primary Data

4.1 Introduction

This chapter presents analysis of the online questionnaire as described in Section 3.6. The sample of this study was selected from information security, governance and SCADA/ICS professionals who have experience with SCADA security. The online questionnaire was distributed via mail to members of two communities (ISACA South Africa Chapter and a large SOC). A covering question was asked in the questionnaire to establish the experience of the respondent and attempts to address the research objectives as mentioned in Section 1.5. The reliability tests in Section 4.8, show high internal consistency. Figure 4.1 is a graphical representation of the outline of this chapter and overall structure.

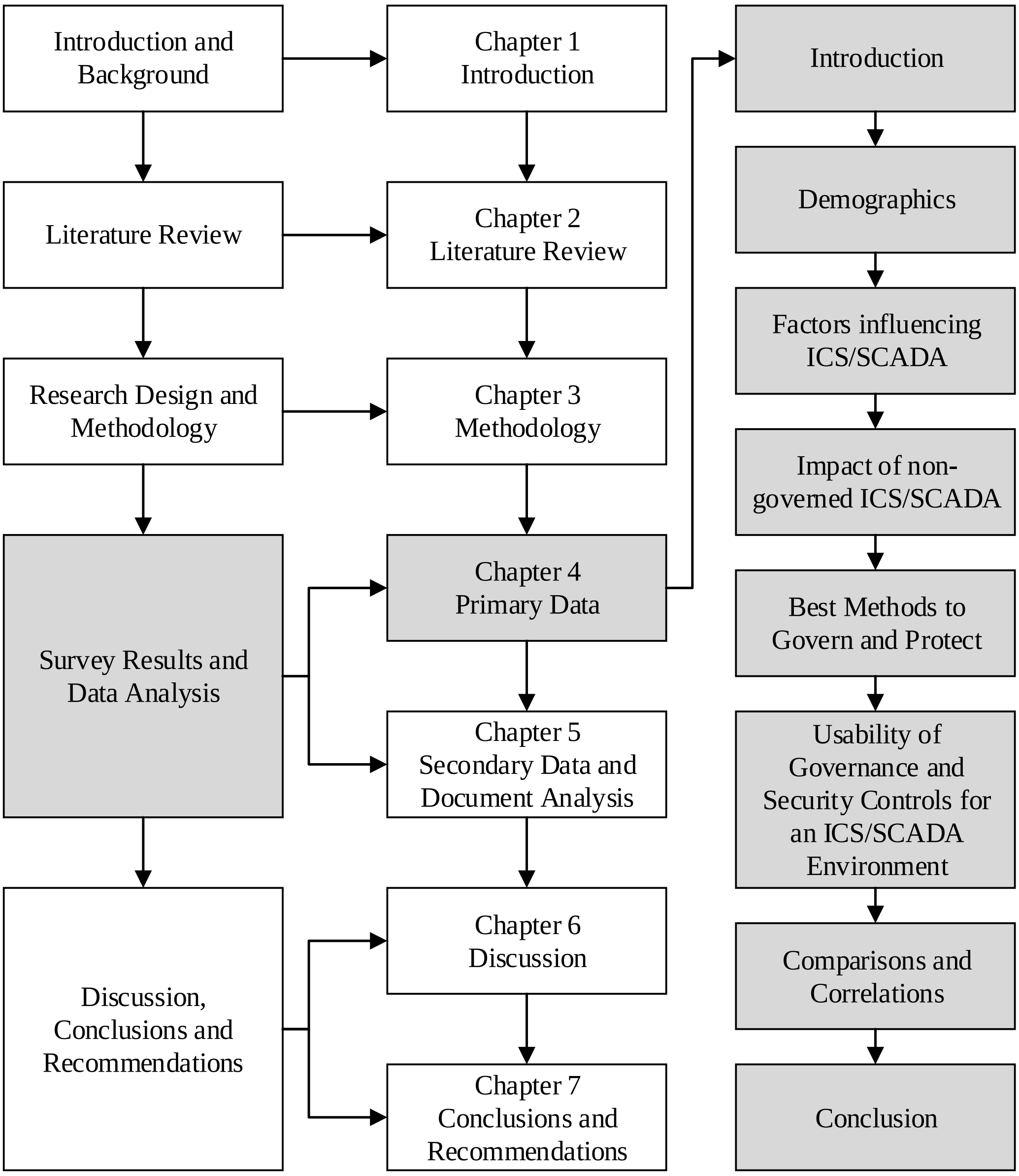

Introduction and Background
Chapter 1 Introduction
Introduction
Literature Review
Chapter 2 Literature Review
Demographics
Research Design and Methodology
Chapter 3 Methodology
Factors influencing ICS/SCADA
Impact of non-governed ICS/SCADA
Survey Results and Data Analysis
Chapter 4 Primary Data
Best Methods to Govern and Protect
Chapter 5 Secondary Data and Document Analysis
Usability of Governance and Security Controls for an ICS/SCADA Environment
Discussion, Conclusions and Recommendations
Chapter 6 Discussion
Comparisons and Correlations
Chapter 7 Conclusions and Recommendations
Conclusion

Figure 4.1: Graphical representation of Chapter 4 outline

4.2 Demographics

The Demographics relates to the following questions in the questionnaire:

- Question A1 Type of Organisation;
- Question A2 Sector;
- Question A3 Job Function;
- Question A4 Number of Employees;
- Question B1 What is your primary interaction with ICS/SCADA; and
- Question B2 How many years of experience with ICS/SCADA systems do you have.

4.2.1 Type of organisation

Figure 4.2 illustrates the type of organisation to whom the respondents belongs to. The majority of the respondents (36 or 52%) were from a *Public Organisation*, 23 (33%) from a *Private Organisation*, 4 (6%) from *Non-Governmental Organisation (NGO)/Non-profit organisation (NPO)* and 6 (9%) from *Other* types of organisations. The large percentage of *Public Organisations* that responded are useful and strengthen the research as majority of critical infrastructure are managed by *Public Organisations*.

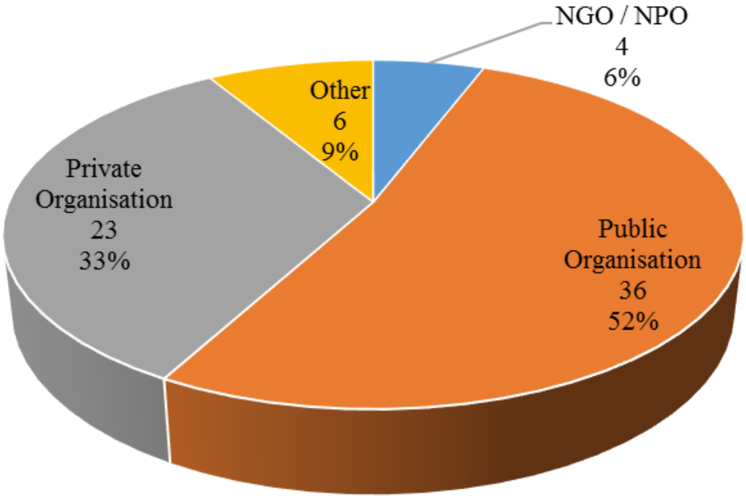


Figure 4.2: Type of organisations

4.2.2 Sector

Figure 4.3 shows that 24 (35%) of respondents were from a *Transport/Logistics* sector; 10 (14%) from *Government*, 8 (12%) from *Consulting*, *Finance* and *IT/Telecoms* respectively; 2 (3%) each from *Energy*, *Human Resources*, *Manufacturing* and *Other*; while *Education*, *Mining* and *Public services (Fire, Police, Health care)* each was 1 (1%). The respondents from *Human Resources* are abnormal as there is not necessary ICS/SCADA systems used in *Human Resources*. However, when looking at the rest of the questions answered by those from the *Human Resources* sector, they indicated they had no knowledge of ICS/SCADA systems.

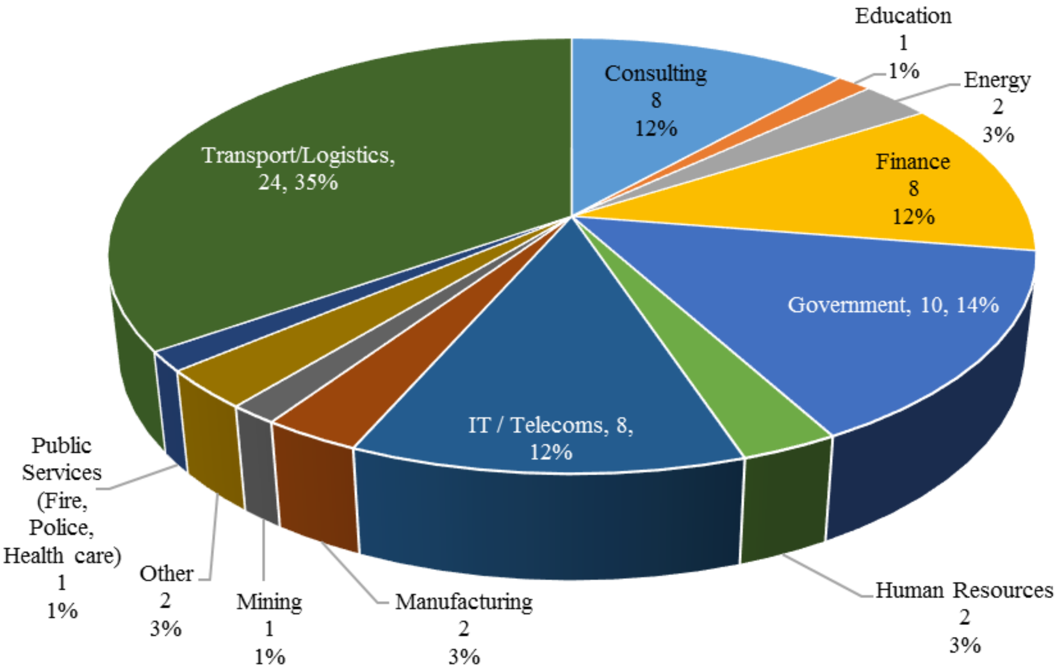


Figure 4.3: Sector

4.2.3 Job function

Figure 4.4 illustrates the job function the respondents have. The majority 34 (50%) of respondents shared between *Management* (17 or 25%) and *Analyst/technical* (17 or 25%), 12 (17%) from *Risk/Governance/Compliance*, 6 (9%) *Senior Management*, 4 (6%) *IT administrator (System/Network/Database)*, 4 (6%) *Engineering*, 3 (4%) *Consultant*, 3 (4%) from *C-level (CIO, Chief Information Security Officer (CISO), Chief Executive Officer (CEO), Chief Financial Officer(CFO))*, and *Operations*, *Maintenance* and *Other* all 1 (1.33%) each. The split amongst the various job functions are suitable as the participants have different interactions with ICS/SCADA based on their job function and will give a more accurate result.

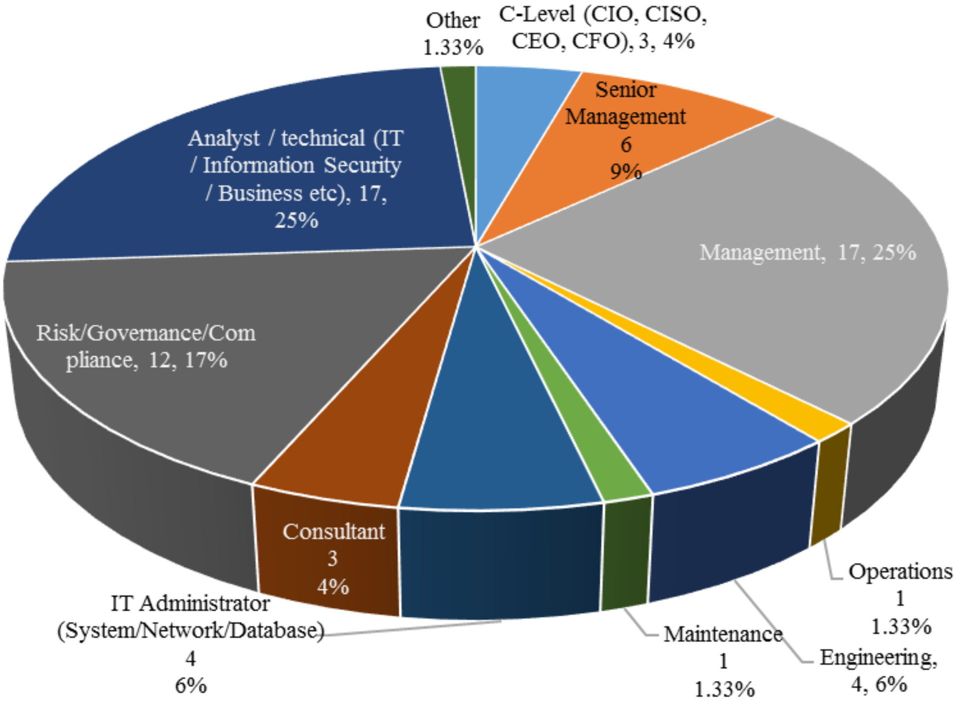


Figure 4.4: Job function

4.2.4 Number of employees

Figure 4.5 indicates that 32 (46%) of respondents work at a company with *5,000 or more* employees, 18 (26%) at a company with between *1,001 to 5,000* employees, 7 (10%) at a company with *100 – 1,000* and 12 (17%) at a company *less than 100*. The results make sense as one of the communities that the questionnaire was sent to is a large SOC.

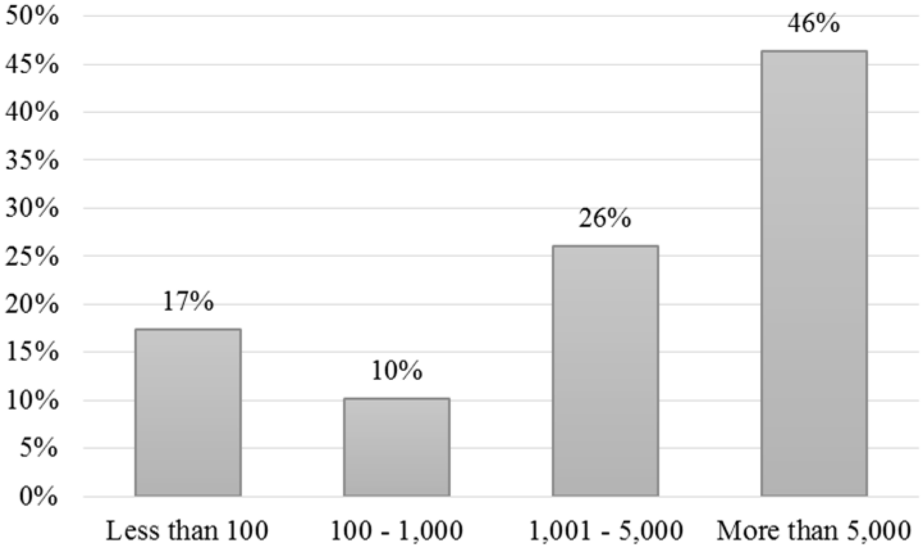


Figure 4.5: Number of employees

4.2.5 Primary interaction with ICS/SCADA

Figure 4.6 indicates that 21 (30%) of respondents had *No knowledge of ICS/SCADA*, 15 (22%) interacted with ICS/SCADA via *Audit/Consulting*, 11 (16%) through *IT*, 7 (10%) through *Governance/Risk/Compliance*, and 12% split between *Security* 4 (6%) and *Management of ICS/SCADA* 4 (6%). From the respondents, 3 (4%) showed *Some awareness of the risks/issues* of ICS/SCADA, 2 (3%) interacted with ICS/SCADA through *Engineering*, 1 (1.5%) through *Operations* and through *Academic research* each.

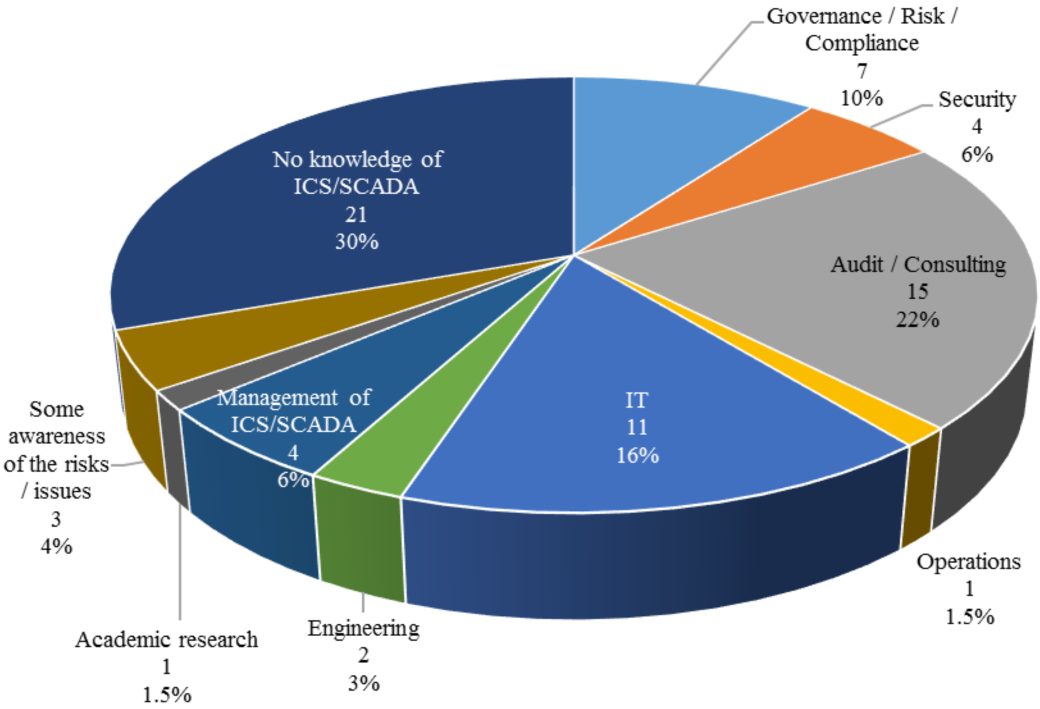


Figure 4.6: Primary interaction with ICS/SCADA

After this question, the 21 (30%) participants that had *No knowledge of ICS/SCADA* were excluded from answering further questions. A summary of the respondents is listed in Table 4.1.

4.2.6 Experience with ICS/SCADA

Figure 4.7 depicts the number of years of ICS/SCADA experience the respondents have. 22 (32%) have *None*, which relates to the 21 (30%) of respondents that had *No knowledge of ICS/SCADA*. 15 (22%) of respondents have *2 to 5 years* of ICS/SCADA experience, 13 (19%) *1 to 2 years*, 9 (13%) *5 to 10 years*, 6 (9%) *10 to 20 years* and only 1 (1%) *more than 20 years*.

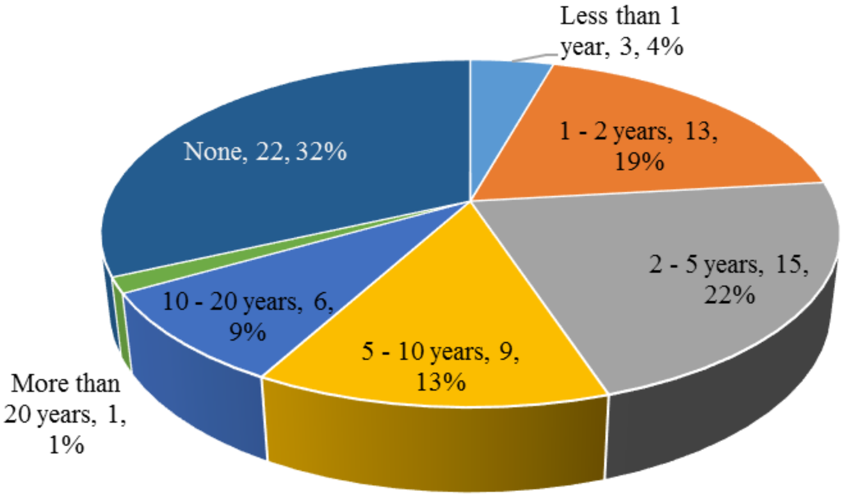


Figure 4.7: Experience with ICS/SCADA

4.3 Factors influencing ICS/SCADA

This section relates to the research objective to determine the factors (vulnerabilities and threats) influencing ICS security in South Africa.

The responses received from the respondents for demographics in Section 4.2 included respondents with no knowledge of ICS/SCADA systems. The respondents with no knowledge of ICS/SCADA was excluded from this point. A summary of the respondent's knowledge of ICS/SCADA are listed in Table 4.1.

Respondent	Number of respondents	Result
No knowledge of ICS/SCADA	21	Excluded from study
Knowledge of ICS/SCADA	48	Included as relevant to study
Total	**69**	

Table 4.1: Summary of respondent's knowledge of ICS/SCADA

4.3.1 Level of visibility of threats

The respondents were asked how they would rate the level of visibility of threats in their ICS/SCADA environment or an ICS/SCADA environment that you have encountered. This relates to Question C1 of the questionnaire. The results are displayed in Figure 4.8. A majority, 25 (52%) of the respondents had an *Average/OK* visibility of the threats in their ICS/SCADA environment and 12 (25%) *Poor* visibility. Only 6 (13%) and 1 (2%) had a *Good* or *Very good/Excellent* visibility of the threats to ICS/SCADA respectively. This indicates that there is still a third (or 33%) of respondents that had a *Poor* (25%) or *Very poor* (8%) visibility of threats on their ICS/SCADA environment which could indicate that these ICS/SCADA environments are not governed. This contributes to the research problem that there is no or limited information available as to the current state of ICS/SCADA systems and the factors (vulnerabilities and threats) are unknown.

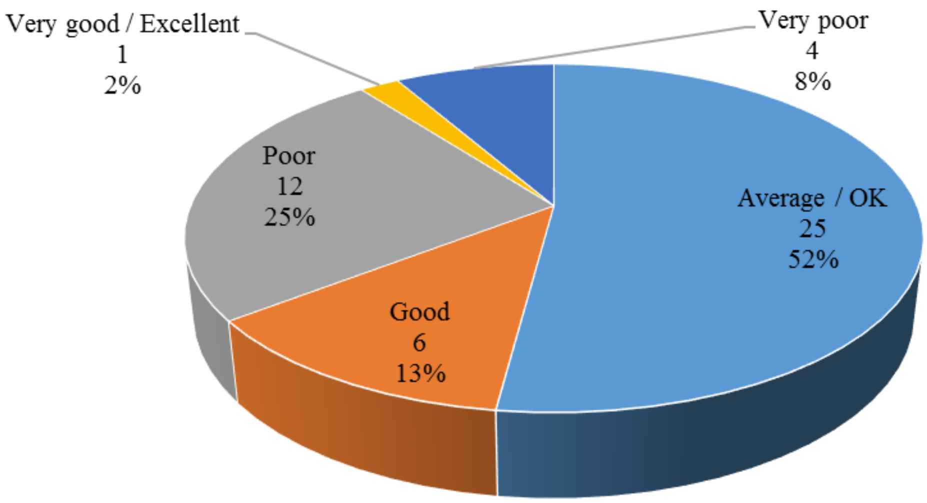


Figure 4.8: Level of visibility of threats for ICS/SCADA

4.3.2 Likelihood/Probability of Threats

This relates to Question C2 of the questionnaire. Figure 4.9 shows the likelihood (probability) of threats occurring in ICS/SCADA environments. In order to generate the descriptive statistics, the responses were rated from ‘1’, *Very low* to ‘5’ *Very High*. Table 4.2 shows the frequency and full descriptive statistics of the threat rating from *Very low* (may only occur in exceptional circumstances) to *Very high* (Expected to occur frequently and in most circumstances).

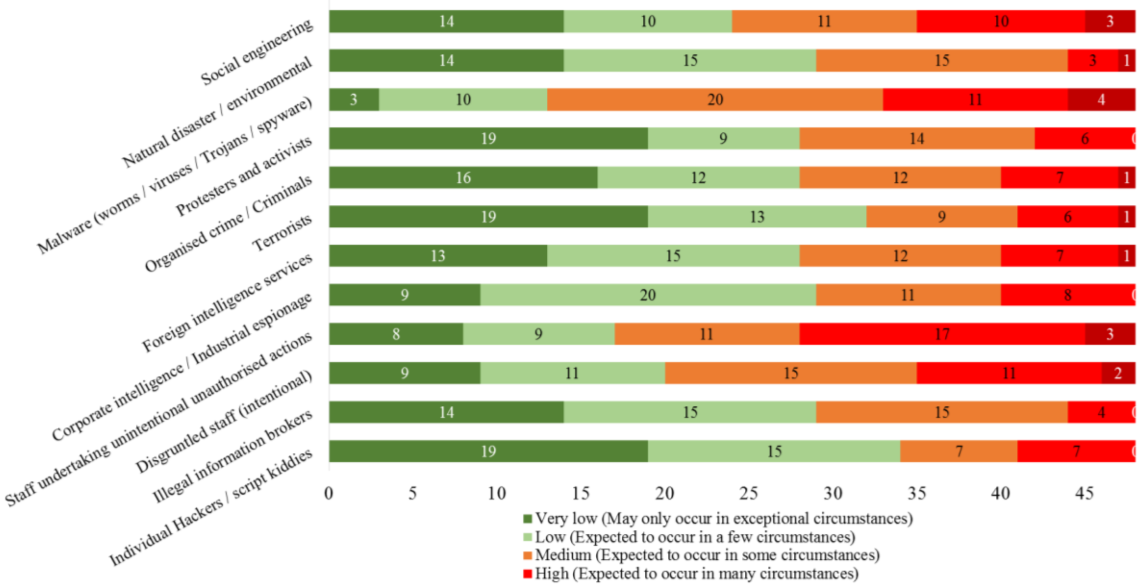


Figure 4.9: Threats related to ICS/SCADA environment

From the responses, it was noted that the top three threats likely to occur are *Malware* with a mean of 3.06 (*Medium* - expected to occur in some circumstances), *Staff undertaking unintentional unauthorised actions* with a mean of 2.96 (leaning towards *Medium* - expected to occur in some circumstances) and *disgruntled staff (intentional)* with a mean of 2.71 (also leaning towards *Medium* - expected to occur in some circumstances).

Table 4.2: Frequency and descriptive statistics table of threats

	Individual Hackers/script kiddies	Illegal information brokers	Disgruntled staff (intentional)	Staff undertaking unintentional unauthorised actions	Corporate intelligence/Industrial espionage	Foreign intelligence services	Terrorists	Organised crime/Criminals	Protesters and activists	Malware	Natural disaster/environmental	Social engineering
Very low	19	14	9	8	9	13	19	16	19	3	14	14
Low	15	15	11	9	20	15	13	12	9	10	15	10
Medium	7	15	15	11	11	12	9	12	14	20	15	11
High	7	4	11	17	8	7	6	7	6	11	3	10
Very high	0	0	2	3	0	1	1	1	0	4	1	3
Mean	2.04	2.19	2.71	2.96	2.38	2.33	2.10	2.27	2.15	3.06	2.21	2.54
Std Deviation	1.07	0.96	1.15	1.22	0.98	1.10	1.13	1.14	1.09	1.02	1.01	1.29
Variance	1.15	0.92	1.32	1.49	0.96	1.21	1.29	1.31	1.19	1.04	1.02	1.66
Kurtosis	-0.79	-0.99	-0.90	-1.04	-0.85	-0.74	-0.55	-0.89	-1.31	-0.25	-0.24	-1.13
Skewness	0.67	0.21	-0.01	-0.28	0.30	0.40	0.70	0.42	0.31	0.00	0.47	0.25
Confidence Level (95.0%)	0.31	0.28	0.33	0.35	0.28	0.32	0.33	0.33	0.32	0.30	0.29	0.37
Rank			3	2						1		

The 95% confidence intervals for the top three threats are 0.30 for *Malware*, 0.35 for *Staff undertaking unintentional unauthorised action* and 0.33 for *disgruntled staff (intentional)*. This indicates that with a 95% confidence, the population mean for each of the above are *Malware* with a population mean of between 2.77 (mean – confidence = 3.06 – 0.30) to 3.36 (mean + confidence = 3.06 + 0.30), *Staff undertaking unintentional unauthorised actions* with a population mean of between 2.60 to 3.31 and *disgruntled staff (intentional)* with a population mean of 2.38 to 3.04.

The bottom three threats likely to occur are: *Individual Hackers/script kiddies* with a mean of 2.04, *Terrorist* with a mean of 2.10 and *Protesters and activists (environmental/political/animal rights)* with a mean of 2.15 all leaning strongly towards *Low* (Expected to occur in a few circumstances).

4.3.3 Top threats

This relates to Question C4 of the questionnaire. The respondents were asked to indicate the top three threats by selecting only three of the threats on the list of the question. The top three threats are: *Staff undertaking unintentional unauthorised actions* (e.g. making changes without following change control process) which 32 (67%) of the respondents selected, *Malware (worms/viruses/Trojans/spyware)* 30 (63%) and *disgruntled staff (intentional)* 23 (48%). The results are displayed in Figure 4.10.

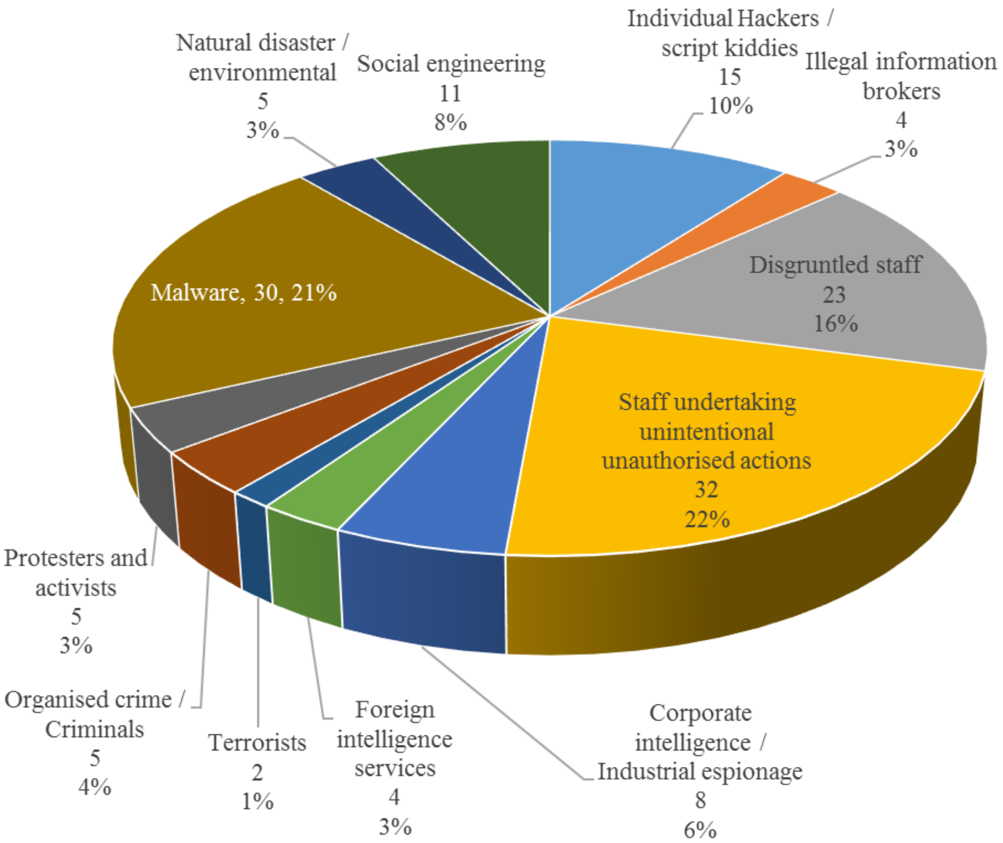


Figure 4.10: Top threats related to ICS/SCADA environment

Comparing the top three threats with the top three threats in Section 4.3.2, it is observed that the top three correspond with the previous question, however the order is slightly different. *Staff undertaking unintentional unauthorised actions* (e.g. making changes without following change control process) was second in the previous question and *Malware (worms/viruses/Trojans/spyware)* 63% came out first. The threat, *disgruntled staff (intentional)* remained third in both questions showing consistency.

4.3.4 Impact of threats

This relates to Question C3 of the questionnaire. Figure 4.11 shows the impact of threats related to ICS/SCADA environments. Table 4.3 shows the frequency of the impact of the threat rating from *Very low or no impact (e.g. no impact of service)* to *Very high* impact (e.g. service disruption for significant time). In order to generate the descriptive statistics, the responses were rated from ‘1’, *Very low impact* to ‘5’ *Very High impact*.

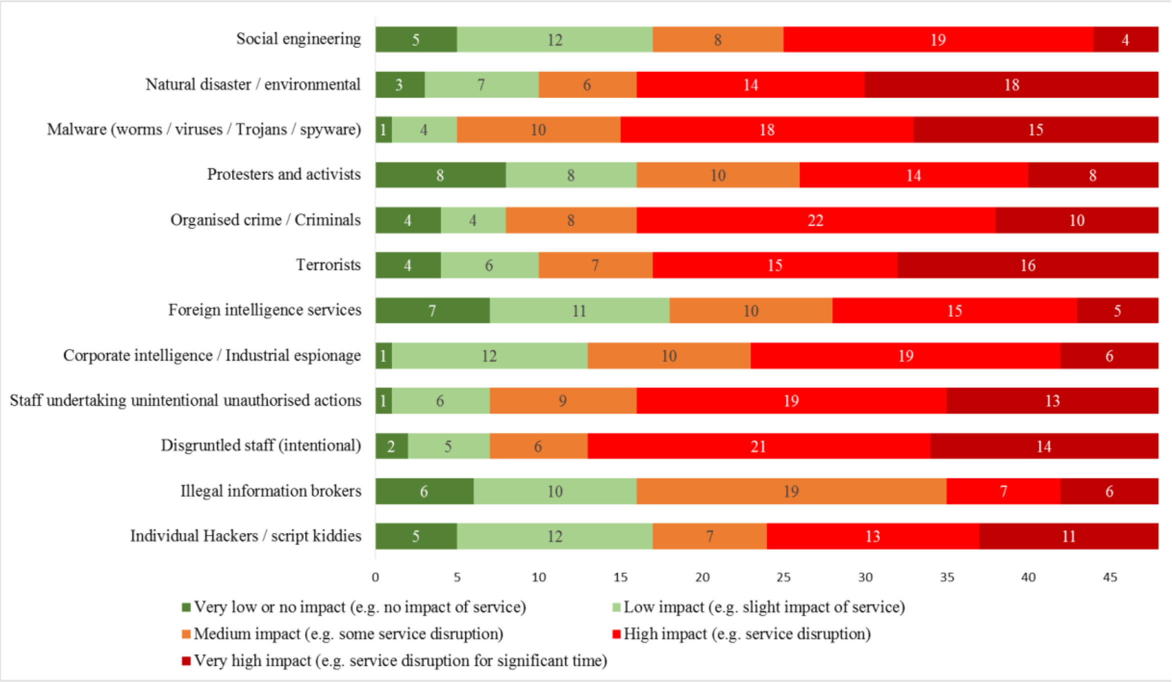


Figure 4.11: Impact of threats related to ICS/SCADA environment

From the responses, the top three threats likely to impact ICS/SCADA systems are *Malware* with a mean of 3.88 (*Medium impact* – e.g. some service disruption, but also leaning towards *High impact* – e.g. service disruption), *disgruntled staff (intentional)* with a mean of 3.83 (also *Medium impact* - expected to occur in some circumstances, but also leaning towards *High impact* – e.g. service disruption), and *Staff undertaking unintentional unauthorised actions* with a mean of 3.77 (*Medium* - expected to occur in some circumstances but also leaning towards *High impact* – e.g. service disruption).

The 95% confidence intervals for the top three threats are 0.30 for *Malware*, 0.32 for *disgruntled staff (intentional)*, and 0.31 for *Staff undertaking unintentional unauthorised action*. This indicates that with 95% confidence, the population mean for each of the above are *Malware* with a population mean of between 3.58 (mean – confidence = 3.88 – 0.30) to 4.17 (mean + confidence = 3.88 + 0.30), *disgruntled staff (intentional)* with a population mean of 3.51 to 4.15 and *Staff undertaking unintentional unauthorised actions* with a population mean of between 3.46 to 4.08.

Table 4.3: Frequency and descriptive statistics of the impact of threat

	Individual Hackers/script kiddies	Illegal information brokers	Disgruntled staff	Staff undertaking unintentional unauthorised actions	Corporate intelligence/Industrial espionage	Foreign intelligence services	Terrorists	Organised crime/Criminals	Protesters and activists	Malware	Natural disaster/environmental	Social engineering
Very low	5	6	2	1	1	7	4	4	8	1	3	5
Low	12	10	5	6	12	11	6	4	8	4	7	12
Medium	7	19	6	9	10	10	7	8	10	10	6	8
High	13	7	21	19	19	15	15	22	14	18	14	19
Very high	11	6	14	13	6	5	16	10	8	15	18	4
Mean	3.27	2.94	3.83	3.77	3.35	3.00	3.69	3.63	3.13	3.88	3.77	3.10
Std Deviation	1.35	1.17	1.10	1.06	1.06	1.25	1.29	1.16	1.35	1.02	1.28	1.19
Variance	1.82	1.38	1.21	1.12	1.13	1.57	1.67	1.35	1.81	1.05	1.63	1.41
Kurtosis	-1.26	-0.53	0.36	-0.28	-0.95	-1.08	-0.53	0.21	-1.12	0.05	-0.56	-1.03
Skewness	-0.19	0.13	-0.96	-0.65	-0.21	-0.13	-0.74	-0.91	-0.24	-0.73	-0.77	-0.29
Confidence Level (95.0%)	0.39	0.34	0.32	0.31	0.31	0.36	0.37	0.34	0.39	0.30	0.37	0.35
Rank			2	3						1	3	

The bottom three threats likely to have less impact on ICS/SCADA systems should they occur are: *Illegal information brokers* with a mean of 2.94, *Foreign intelligence services* with a mean of 3.00 and *Social engineering (phishing emails etc.)* with a mean of 3.10 all leaning strongly towards *Low* (Expected to occur in a few circumstances).

The top 3 threats are consistent with the answers received from the respondents in Section 4.3.3, although the order of the top three is slightly different.

4.3.5 Vulnerabilities related to ICS/SCADA

This relates to Question C5 of the questionnaire. Figure 4.12 shows the vulnerabilities related to ICS/SCADA environments. Table 4.4 shows the frequency and full descriptive statistics of the vulnerability rating from *very low* to *very high*. In order to generate the descriptive statistics, the responses were rated from '1', *Very low* to '5' *Very High*.

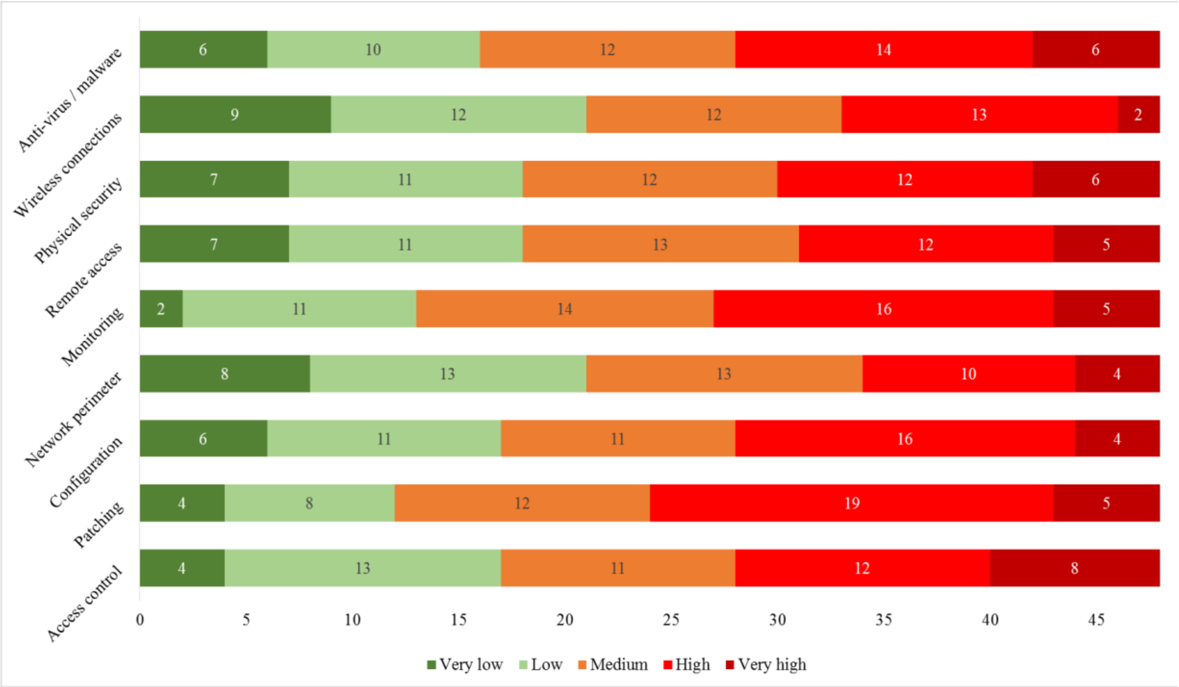


Figure 4.12: Vulnerabilities related to ICS/SCADA environment

From the responses, the top three vulnerabilities related to ICS/SCADA systems are *Patching (outdated or unpatched systems)* with a mean of 3.27 (*Medium*), *No or limited Monitoring* with a mean of 3.23 (also *Medium*), and *Access control (No or weak passwords)* with a mean of 3.15 (*Medium*).

The 95% confidence intervals for the top three vulnerabilities related to ICS/SCADA systems are 0.33 for *Patching*, 0.31 for *No or limited Monitoring* and 0.36 for *Access control (No or weak passwords)*. This indicates that with 95% confidence the population mean for each of the above are *Patching* with a population mean of between 2.94 (mean – confidence = 3.27 – 0.33) to 3.60 (mean + confidence = 3.27 + 0.33), *Monitoring* with a population mean of 2.92 to 3.54 and *Access control* with a population mean of between 2.79 to 3.51 and.

The bottom three vulnerabilities on ICS/SCADA systems are: *Wireless connections – overlooked and poorly configured* with a mean of 2.73, *Network perimeter – Unsecure, firewall don't exist/misconfigured, direct connections to internet* with a mean of 2.77 and *Remote access – authentication not secure/shared passwords for vendors* with a mean of 2.94 all leaning strongly towards *Medium* vulnerability.

Table 4.4: Frequency and descriptive statistics of vulnerabilities

	Access control	Patching	Configuration	Network perimeter	Monitoring	Remote access	Physical security	Wireless connections	Anti-virus/ malware
Very low	4	4	6	8	2	7	7	9	6
Low	13	8	11	13	11	11	11	12	10
Medium	11	12	11	13	14	13	12	12	12
High	12	19	16	10	16	12	12	13	14
Very high	8	5	4	4	5	5	6	2	6
Mean	3.15	3.27	3.02	2.77	3.23	2.94	2.98	2.73	3.08
Std Deviation	1.24	1.12	1.19	1.21	1.06	1.23	1.26	1.18	1.23
Variance	1.53	1.27	1.43	1.46	1.12	1.51	1.60	1.39	1.52
Kurtosis	-1.06	-0.52	-0.96	-0.87	-0.69	-0.93	-1.01	-1.07	-0.94
Skewness	-0.01	-0.47	-0.20	0.16	-0.14	-0.02	-0.03	-0.01	-0.16
Confidence Level (95.0%)	0.36	0.33	0.35	0.35	0.31	0.36	0.37	0.34	0.36
Rank	3	1			2				

4.3.6 Do you have controls in place to mitigate the vulnerabilities related to ICS/SCADA?

This relates to Question C6 of the questionnaire. Figure 4.13 shows the controls in place to mitigate the vulnerabilities related to ICS/SCADA environments. Table 4.4 shows the frequency and full descriptive statistics of the controls mitigating vulnerability. In order to generate the descriptive statistics, the responses were rated from ‘1’, *Have not implemented anything* to ‘5’ *Implemented and operating effectively*. The mean, etc. have been calculated by removing the *N/A* and *Not sure* responses.

From the responses, it is noted that the top three controls mitigating vulnerabilities in the ICS/SCADA environments are *Configuration (Default configuration, no backup of configuration)* with a mean of 3.91 (*Partially Implemented/in progress,* but leaning strongly towards *Implemented control requires improvement*), *Physical security* with a mean of 3.89 (*Partially Implemented/in progress*, but leaning strongly towards *Implemented control requires improvement*), and *Network perimeter (Unsecure, firewall don’t exist/misconfigured, direct connections to internet*) with a mean of 3.85 (*Partially Implemented/in progress*, but leaning towards *Implemented control requires improvement*).

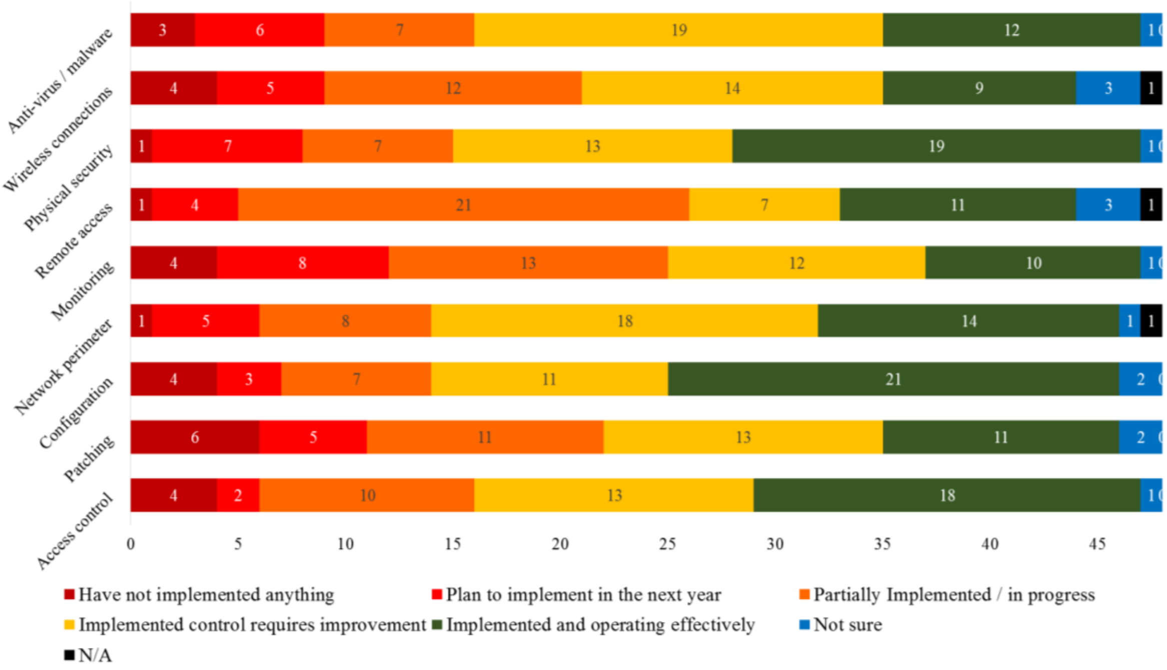


Figure 4.13: Controls mitigating vulnerabilities related to ICS/SCADA environment

The 95% confidence intervals for the top three controls mitigating vulnerabilities in the ICS/SCADA environments are 0.39 for *Configuration*, 0.34 for *Physical security*, and 0.31 for *Network perimeter*. This indicates that with 95% confidence the population mean for each of the above, taking into account those who responded are *Configuration* with a population mean of between 3.53 (mean – confidence = 3.91 – 0.39) to 4.30 (mean + confidence = 3.91 + 0.39), *Physical security* with a population mean of 3.55 to 4.24 and *Network perimeter* with a population mean of between 3.54 to 4.16. This further indicates that the top three controls mitigating vulnerabilities in the ICS/SCADA environments are between *Partially Implemented/in progress*, and *Implemented control requires improvement.*

The bottom three controls mitigating vulnerabilities in the ICS/SCADA environments are: *Monitoring* with a mean of 3.34, *Patching* with a mean of 3.39 and *Wireless connections* with a mean of 3.43 all *Partially Implemented/in progress*. The top three controls do not address the Top threats as mentioned in Section 4.3.3 as well as the top three vulnerabilities. The control for addressing one of the top three vulnerabilities, lack of Patching/inadequate patching, is one of the three bottom controls as indicated by the respondents. There is a clear misalignment in prioritising controls to address top threats and vulnerabilities.

Table 4.5: Frequency and descriptive statistics of controls mitigating vulnerabilities

	Access control	Patching	Configuration	Network perimeter	Monitoring	Remote access	Physical security	Wireless connections	Anti-virus/ malware
Have not implemented anything	4	6	4	1	4	1	1	4	3
Plan to implement in the next year	2	5	3	5	8	4	7	5	6
Partially Implemented/in progress	10	11	7	8	13	21	7	12	7
Implemented control requires improvement	13	13	11	18	12	7	13	14	19
Implemented and operating effectively	18	11	21	14	10	11	19	9	12
Not sure	1	2	2	1	1	3	1	3	1
N/A	0	0	0	1	0	1	0	1	0
Count (n-N/A - Unsure/Unknown)	47	46	46	46	47	44	47	44	47
Mean*	3.83	3.39	3.91	3.85	3.34	3.52	3.89	3.43	3.66
Std Deviation*	1.24	1.32	1.30	1.05	1.24	1.05	1.17	1.21	1.18
Variance*	1.54	1.75	1.68	1.11	1.53	1.09	1.36	1.46	1.40
Kurtosis*	0.13	-0.81	0.05	-0.06	-0.85	-0.62	-0.61	-0.50	-0.24
Skewness*	-0.95	-0.47	-1.05	-0.76	-0.26	0.06	-0.73	-0.50	-0.77
Confidence Level (95.0%)*	0.36	0.39	0.39	0.31	0.36	0.32	0.34	0.37	0.35
Rank			1	3			2		

* The mean, Standard Deviation, Variance, Kurtosis, Skewness and Confidence Level have been calculated by removing the *N/A* and *Not sure* responses.

4.4 Impact of non-governed ICS/SCADA

This section attempts to address the research objective to determine the impact of non-governed ICS/SCADA should the factor materialise.

4.4.1 Impact of non-governed ICS/SCADA systems

This relates to Question C7 of the questionnaire. Figures 4.14 shows the impact of non-governed ICS/SCADA should these factors materialise. The Table 4.5 shows the frequency and full descriptive statistics of the impact of non-governed ICS/SCADA should these factors materialise rating from *Insignificant (no impact on service/regulation)*, *Minor (Slight impact on service/regulation), Moderate (Some service disruption/potential for adverse publicity), Major (Service disruption/adverse publicity not avoidable)* and *Extreme/Catastrophic (Service interrupted for significant time/major adverse publicity not avoidable).*

In order to generate the descriptive statistics, the responses were rated from ‘1’, Insignificant (no impact on service/regulation) to ‘5’ Extreme/Catastrophic (Service interrupted for significant time/major adverse publicity not avoidable).

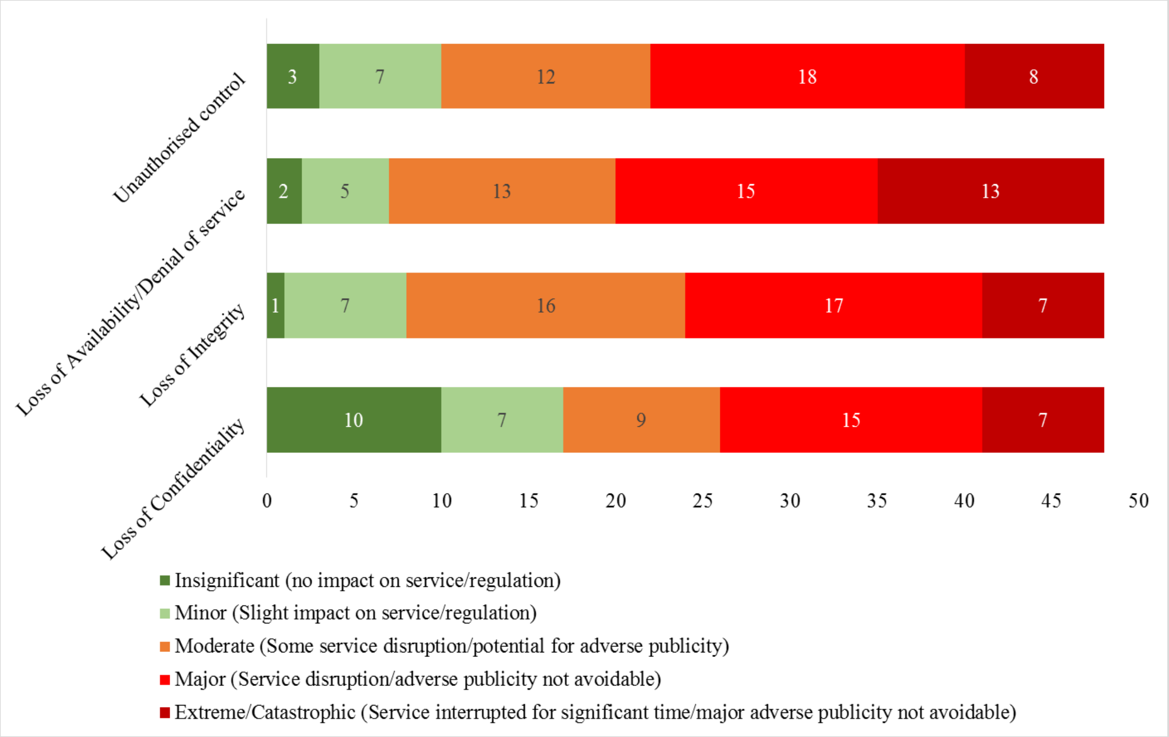


Figure 4.14: Impact of non-governed ICS/SCADA environment

From the responses, the top three impacts of non-governed ICS/SCADA environments should threats and vulnerabilities materialise, are *Loss of Availability/Denial of service* with a mean of 3.67 which is *Moderate (Some service disruption/potential for adverse publicity)*, secondly *Loss of Integrity* with a mean of 3.46 also *Moderate (Some service disruption/potential for adverse publicity)*, and *Unauthorised control* with a mean of 3.44 also *Moderate (Some service disruption/potential for adverse publicity)*.

The 95% confidence intervals for the top three impacts of non-governed ICS/SCADA environments should threats and vulnerabilities materialise are 0.32 for *Loss of Availability/Denial*, 0.29 for secondly *Loss of Integrity*, and 0.33 for *Unauthorised control*. This indicates that the population mean for each of the above, with 95% confidence, are *Loss of Availability/Denial* with a population mean of between 3.34 (mean – confidence = 3.67 – 0.32) to 3.99 (mean + confidence = 3.67 + 0.32), *Loss of Integrity* with a population mean of 3.17 to 3.75 and *Unauthorised control* with a population mean of between 3.11 to 3.77.

Table 4.6: Frequency and descriptive statistics of impact of non-governed ICS/SCADA

	Loss of Confidentiality	**Loss of Integrity**	**Loss of Availability/Denial of service**	**Unauthorised control**
Insignificant (no impact on service/regulation)	10	1	2	3
Minor (Slight impact on service/regulation)	7	7	5	7
Moderate (Some service disruption/potential for adverse publicity)	9	16	13	12
Major (Service disruption/adverse publicity not avoidable)	15	17	15	18
Extreme/Catastrophic (Service interrupted for significant time/major adverse publicity not avoidable)	7	7	13	8
Mean	3.04	3.46	3.67	3.44
Std Deviation	1.38	0.99	1.12	1.13
Variance	1.91	0.98	1.25	1.27
Kurtosis	-1.24	-0.42	-0.35	-0.43
Skewness	-0.23	-0.22	-0.53	-0.49
Confidence Level (95.0%)	0.40	0.29	0.32	0.33
Rank	4	2	1	3

4.4.2 Materialisation of the threats

4.4.2.1 Have any of the threats occurred in your organisation or an ICS/SCADA environment that you have encountered?

This relates to Question C8 of the questionnaire. Figure 4.15 indicates that 37% of respondents did not have a threat occurred in their ICS/SCADA environment. 25% of respondents indicated that a threat did occur, 15% *Can't disclose*, 13% are *Not sure* while 10% indicated *Maybe*. From this it could be concluded that only 37% did not have a threat occurred in their ICS/SCADA environment, while the remaining 63% might possibly have had a threat that occurred in their ICS/SCADA environment. This strengthens the need to secure ICS/SCADA systems as 63% of respondents might had a threat occurred in their ICS/SCADA systems.

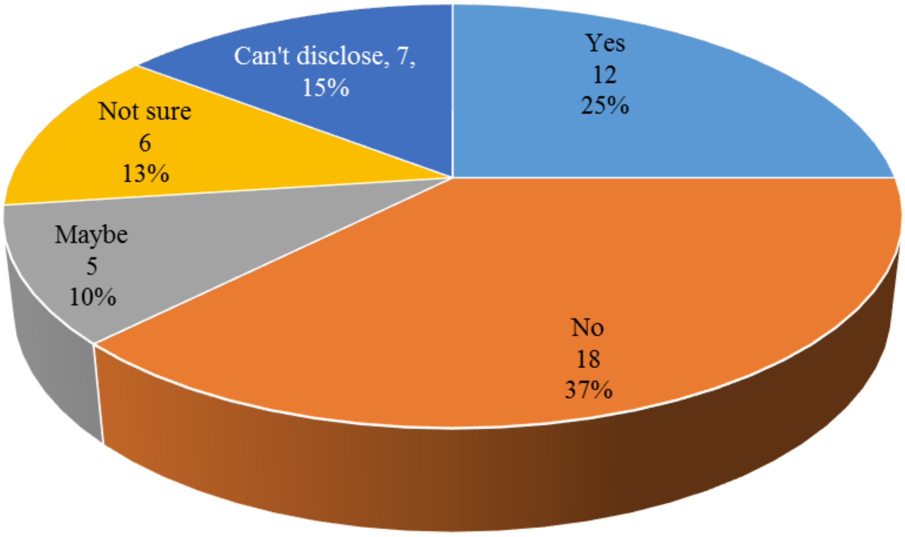


Figure 4.15: Threats occurred in ICS/SCADA environment

4.4.2.2 How many times did such events occur in the past 12 months?

This relates to Question C9 of the questionnaire. The respondents that answered *Yes*, indicating a threat occurred in Question C8 in Section 4.4.2.1 were further asked regarding the threat. Those who answered *No*, *Maybe*, *Not sure* or *Can't disclose* were excluded from Questions C9 and C10. Figure 4.16 indicates that 42% of respondents indicated that the threat/event occurred *2 – 4* times in the past 12 months, 41% of respondents had a threat/event occurred *Once* and 17% of respondents had a threat/event occurred *5 – 10* times in the past month. This further strengthens the need of a control framework as 59% of respondents indicated that a threat occurred more than twice in the last 12 months.

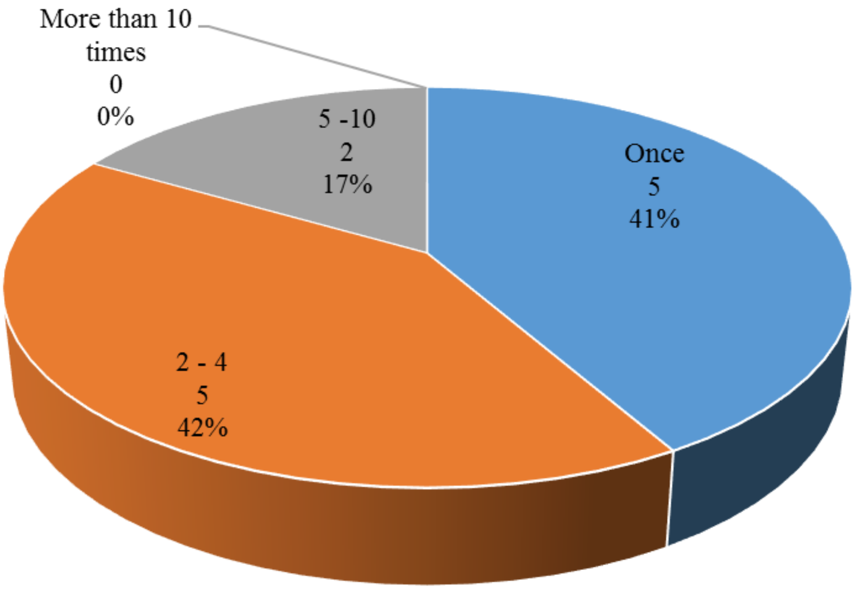


Figure 4.16: No of time a threats occurred in ICS/SCADA environment

4.4.2.3 How long did it take to discover the threat?

This relates to Question C10 of the questionnaire. Figure 4.17 indicates that 42% of those respondents that had a confirmed threat materialising took between one week to one month *(7 – 30 days)* to discover it. A quarter or 25% discovered the threat within one day, 17% took between *2 to 7 days*, 8% between *1 to 3 months*, and 8% were *unable to answer*.

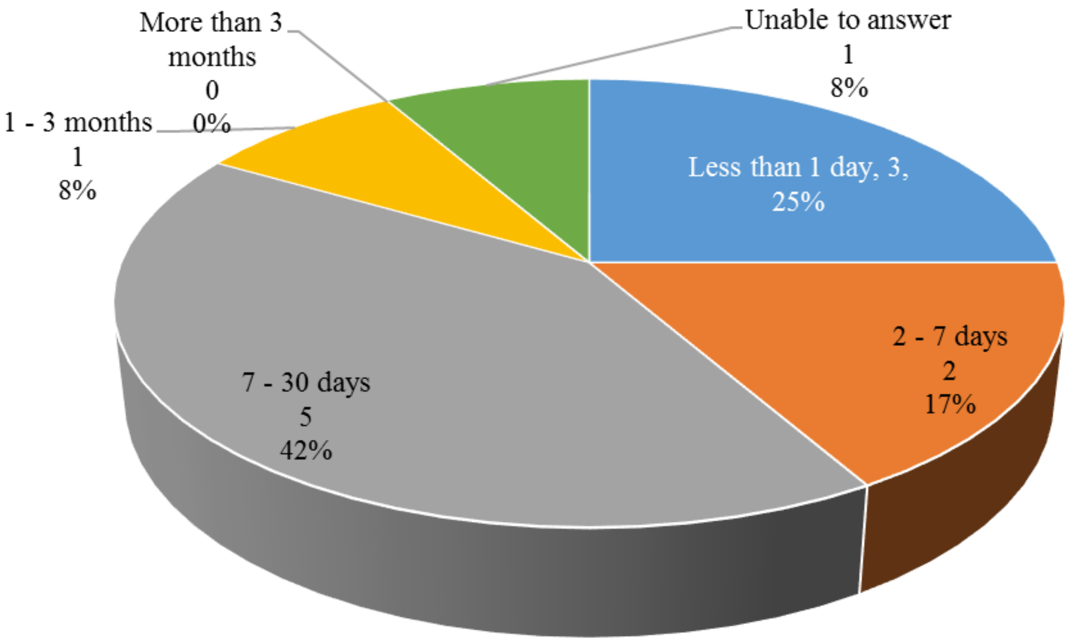


Figure 4.17: Time it took to discover a threats that occurred in ICS/SCADA environment

4.5 Best methods to govern and protect

This section of the questionnaires relates to the research objective to determine what the best measures to govern these factors that influence ICS security in South Africa are.

4.5.1 How are ICS/SCADA systems secured and governed?

This relates to Question D1 of the questionnaire. Figure 4.18 illustrates that the majority of the respondents (69%) indicated *We have control frameworks in place*. 17% of respondents indicated that *ICS/SCADA is regulatory monitored*, 8% were *Not sure* how ICS/SCADA systems are secured and governed, 4% indicated that ICS/SCADA systems are *Not governed* while 2% indicated *Other*.

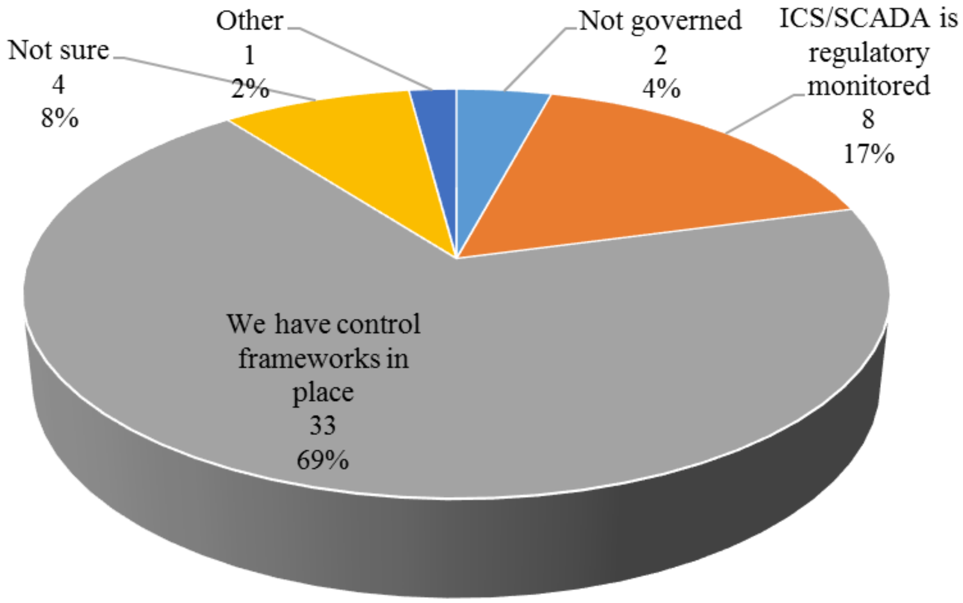


Figure 4.18: How ICS/SCADA is governed

4.5.2 Which of the following control frameworks do you make use of?

This relates to Question D2 of the questionnaire. Figure 4.19 indicates the control frameworks used by the participants to secure and govern ICS/SCADA systems.

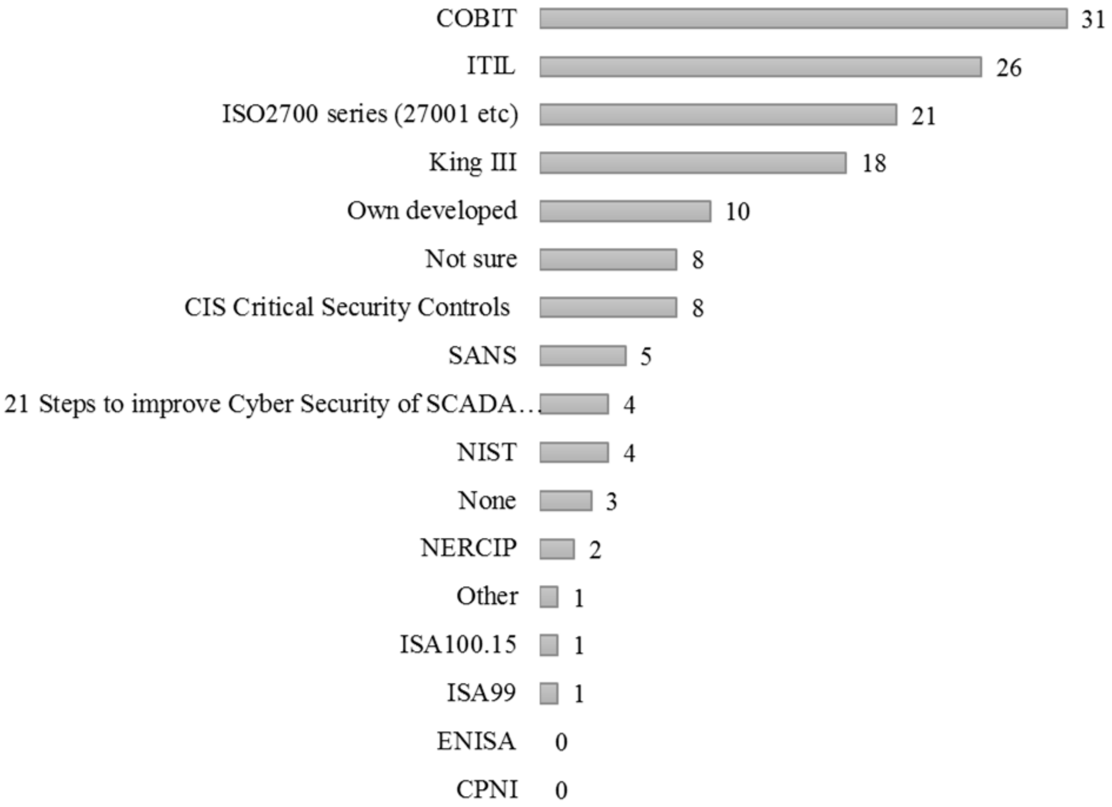


Figure 4.19: Control frameworks used

From the responses it is noted that the top three frameworks used by the respondents to govern and secure their ICS/SCADA environments are COBIT, secondly ITIL and the ISO 27001 series. The three frameworks that used the least by the respondents to govern and secure their ICS/SCADA environments are ISA99, ENISA and CPNI. COBIT is suitable from a governance and security perspective, however ITIL is more suitable in standard IT environment as it focuses more on IT service management. The own develop framework might fit if it is adequately aligned to address threats, vulnerabilities and risks in the respondents' environment. The CPNI is a framework used by UK and although suitable for ICS/SCADA systems, it might not be popular in South Africa, refer to Section 5.4 for framework comparisons.

4.6 Usability of governance and security controls for an ICS/SCADA environment

This section of the questionnaire relates to the research objective to establish if the confidence levels of implemented controls/measures mitigating the threats and risks are sufficient.

4.6.1 Maturity of governance and security

This relates to Question D3 of the questionnaire. Figures 4.20 indicates how respondents see the maturity of governance and security for their ICS/SCADA environment. 38% of respondents indicated that the maturity of their ICS/SCADA environment is *Established*, 25% indicated the maturity of their environment is *Evolving* and 25% also indicated their environment is *Basic*. 10% of ICS/SCADA environments are *Advanced* and only 2% *Leading.* In order to generate the descriptive statistics, the responses were rated from '1', *Basic* to '5' *Leading*.

Table 4.7: Frequency for Maturity of governance and security of ICS/SCADA environment

	Frequency
1 - Basic (Very minimal or basic level of controls)	12
2 - Evolving (Inconsistently applied controls)	12
3 - Established (Controls in place, but there is a need for enhancement)	18
4 - Advanced (Control are consistently applied)	5
5 - Leading (Controls are established, consistently applied, regularly reviewed and coordinated)	1
Mean	2.40
Std Deviation	1.05
Variance	1.10
Kurtosis	-0.64
Skewness	0.17
Confidence Level (95.0%)	0.30

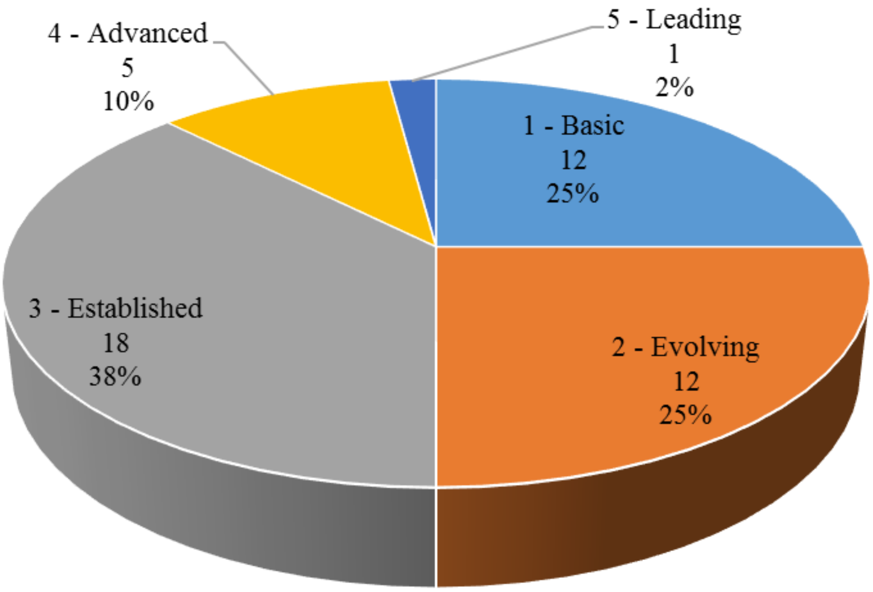


Figure 4.20: Maturity of governance and security of ICS/SCADA environment

From the responses, the mean for responses of the maturity of governance and security for ICS/SCADA environment is 2.40.

The 95% confidence intervals for this is 0.30. This indicates that with 95% confidence, the population mean for the maturity of governance and security for the ICS/SCADA environment is between 2.10 (mean – confidence = 2.40 – 0.30) to 2. 70 (mean + confidence = 2.40 + 0.30). This indicates that the population mean for the maturity of governance and security for ICS/SCADA environments, as per the CMM discussed in Section 2.2.3.4, is between *Evolving (Inconsistently applied controls)* leaning slightly towards *Established (Controls in place, but there is a need for enhancement)*. The CMM is displayed in Figure 4.21.

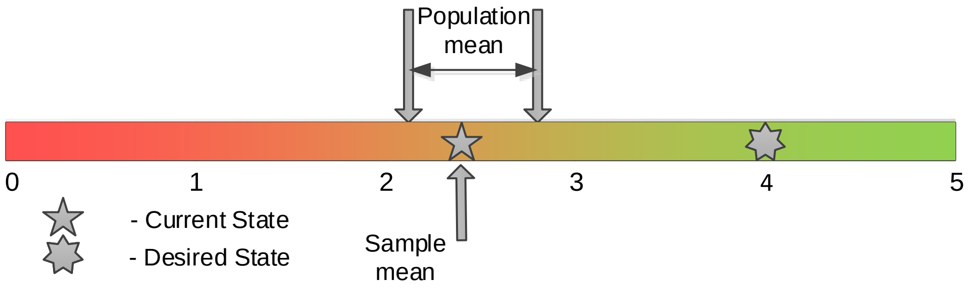


Figure 4.21: ICS/SCADA maturity

4.6.2 How effective are the following controls implemented in your ICS/SCADA environment?

This relates to Question D4 of the questionnaire. In order to generate the descriptive statistics, the responses were rated from '1', *Have not implemented* to '5' *Implemented and operating effectively*. The mean, etc. have been calculated by removing the *N/A* and *Unsure/Unknown* responses. Table 4.8 shows the frequency and descriptive statistics for effectiveness of controls implemented in ICS/SCADA environment for the Top three and bottom three, the full list is displayed in Appendix B.

Table 4.8: Frequency and descriptive statistics for effectiveness of controls implemented in ICS/SCADA environment

	Data encryption	**Physical access control**	**Environmental standards**	**SIEM or security intelligence centre**	**Strategy of ICS/SCADA**	**Firewalls in place**
Have not implemented	12	2	4	11	9	2
Plan to implement in the next year	2	2	2	3	6	2
Partially Implemented/in progress	10	9	7	11	9	11
Implemented but requires improvement	15	14	14	15	15	11
Implemented and operating effectively	9	21	19	7	6	21
Unsure/Unknown	0	0	2	1	2	0
N/A	0	0	0	0	1	1
Count (n-N/A - Unsure/Unknown)	48	48	46	47	45	47
Mean*	3.15	4.04	3.91	3.09	3.07	4.00
Std Deviation*	1.46	1.09	1.24	1.40	1.36	1.12
Variance*	2.13	1.19	1.55	1.95	1.84	1.26
Kurtosis*	-1.21	0.80	0.46	-1.14	-1.15	0.32
Skewness*	-0.39	-1.11	-1.13	-0.36	-0.30	-0.96
Rank	3rd last	1	3	2nd last	last	2

* The table of frequencies listed. The mean, Standard Deviation, Variance, Kurtosis, Skewness and Confidence Level have been calculated by removing the *N/A* and *Unsure/Unknown* responses.

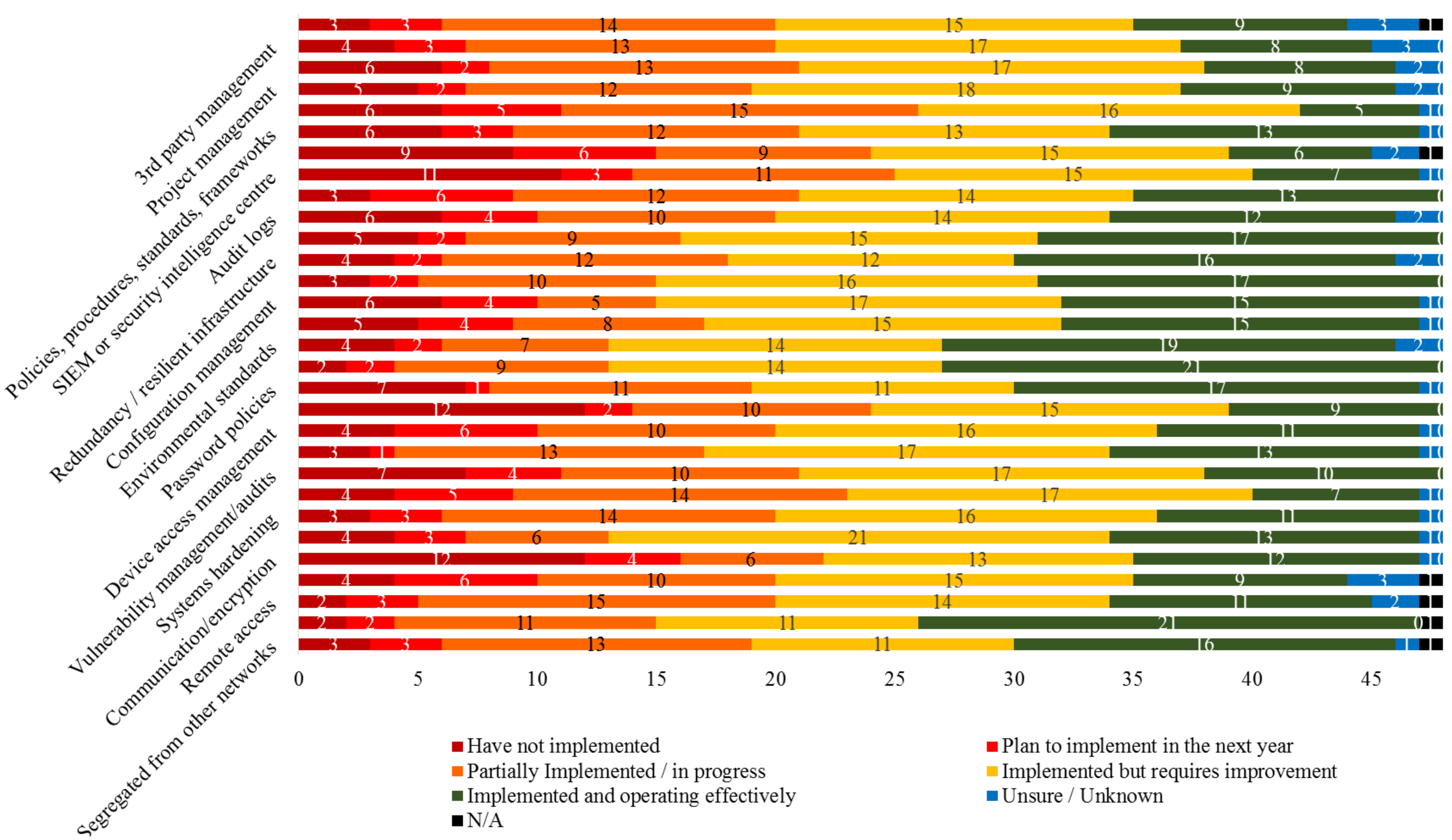


Figure 4.22: Effectiveness of controls implemented

From the responses, as shown in Figure 4.22, the top three effective controls implemented in the ICS/SCADA environments are *Physical access control* with a mean of 4.04 (*Implemented but requires improvement*), secondly *Firewalls in place* with a mean of 4.00 (*Implemented but requires improvement*), and *Environmental standards* with a mean of 3.91 (*Partially Implemented/in progress* but leaning strongly towards *Implemented but requires improvement*).

The 95% confidence intervals for the top three effective controls implemented in the ICS/SCADA environments are 0.32 for *Physical access*, 0.33 for *Firewalls in place*, and 0.37 for *Environmental standards*. This indicates that with 95% confidence, the population mean for each of the above are, *Physical access* with a population mean of between 3.72 (mean – confidence = 4.04 – 0.32) to 4.36 (mean + confidence = 4.04 + 0.32), *Firewalls in place* with a population mean of 3.67 to 4.33 and *Environmental standards* with a population mean of between 3.54 to 4.28.

The bottom three effective controls implemented in the ICS/SCADA environments are: *Strategy of ICS/SCADA* with a mean of 3.07, *SIEM or security intelligence centre* with a mean of 3.09 and *Data encryption* with a mean of 3.15, which all relates to *Partially Implemented/in progress*.

4.6.3 How easy is it /was it to implement the following controls implemented in your ICS/SCADA environment?

This relates to Question D5 of the questionnaire. In order to generate the descriptive statistics, the responses were rated from '1', *Very difficult to implement* to '5' *Very easy to implement*. The mean, etc. have been calculated by removing the *N/A* responses. Table 4.9 shows the frequency and descriptive statistics for effectiveness of controls implemented in ICS/SCADA environment for the Top three and bottom three, the full list is displayed in Appendix C.

From the responses as see in Figure 4.23, it was noted that the top three easiest controls to implement for the ICS/SCADA environment are *Physical access control* with a mean of 3.59 (*Implement with some challenges*), *Environmental standards* with a mean of 3.48 (*Implement with some challenges*), and *Virus/malware protection* with a mean of 3.47 (*Implement with some challenges*).

The 95% confidence intervals for the top three threats are 0.28 for *Physical access control*, 0.29 for *Environmental standards*, and 0.30 for *Virus/malware protection*. This indicates that with 95% confidence, the population mean for each of the above are *Physical access control* with a population mean of between 3.31 (mean – confidence = 3.59 – 0.28) to 3.86 (mean + confidence = 3.59 + 0.28), *Environmental standards* with a population mean of 3.19 to 3.76 and *Virus/malware protection* with a population mean of between 3.16 to 3.77.

Table 4.9: Frequency and descriptive statistics for how easy it is/was to implement controls in ICS/SCADA environment

	Physical access control	Environmental standards	Remote access	3rd party remote access	Virus/malware protection	Systems hardening
Very difficult to implement	1	1	2	1	1	1
Difficult to implement	4	4	7	6	6	12
Implement with some challenges	15	16	20	23	14	19
Easy to implement	19	16	10	10	16	9
Very easy to implement	7	5	2	1	6	2
N/A	2	6	7	7	5	5
Count (n-N/A)	46	42	41	41	43	43
Mean*	3.59	3.48	3.07	3.10	3.47	2.98
Std Deviation*	0.93	0.92	0.91	0.77	0.98	0.89
Variance*	0.87	0.84	0.82	0.59	0.97	0.79
Kurtosis*	0.16	0.18	0.27	0.75	-0.31	-0.13
Skewness*	-0.44	-0.33	-0.15	-0.17	-0.29	0.26
Rank	1	2			3	

* The table of frequencies listed. The mean, Standard Deviation, Variance, Kurtosis, Skewness and Confidence Level have been calculated by removing the *N/A* responses.

The bottom three most difficult controls to implement for the ICS/SCADA environment are: *Systems hardening* with a mean of 2.98 (*Difficult to implement leaning highly towards Implement with some challenges*), *Remote access* with a mean of 3.07 (*Implement with some challenges*) and *3rd party remote access* with a mean of 3.10 (*Implement with some challenges*).

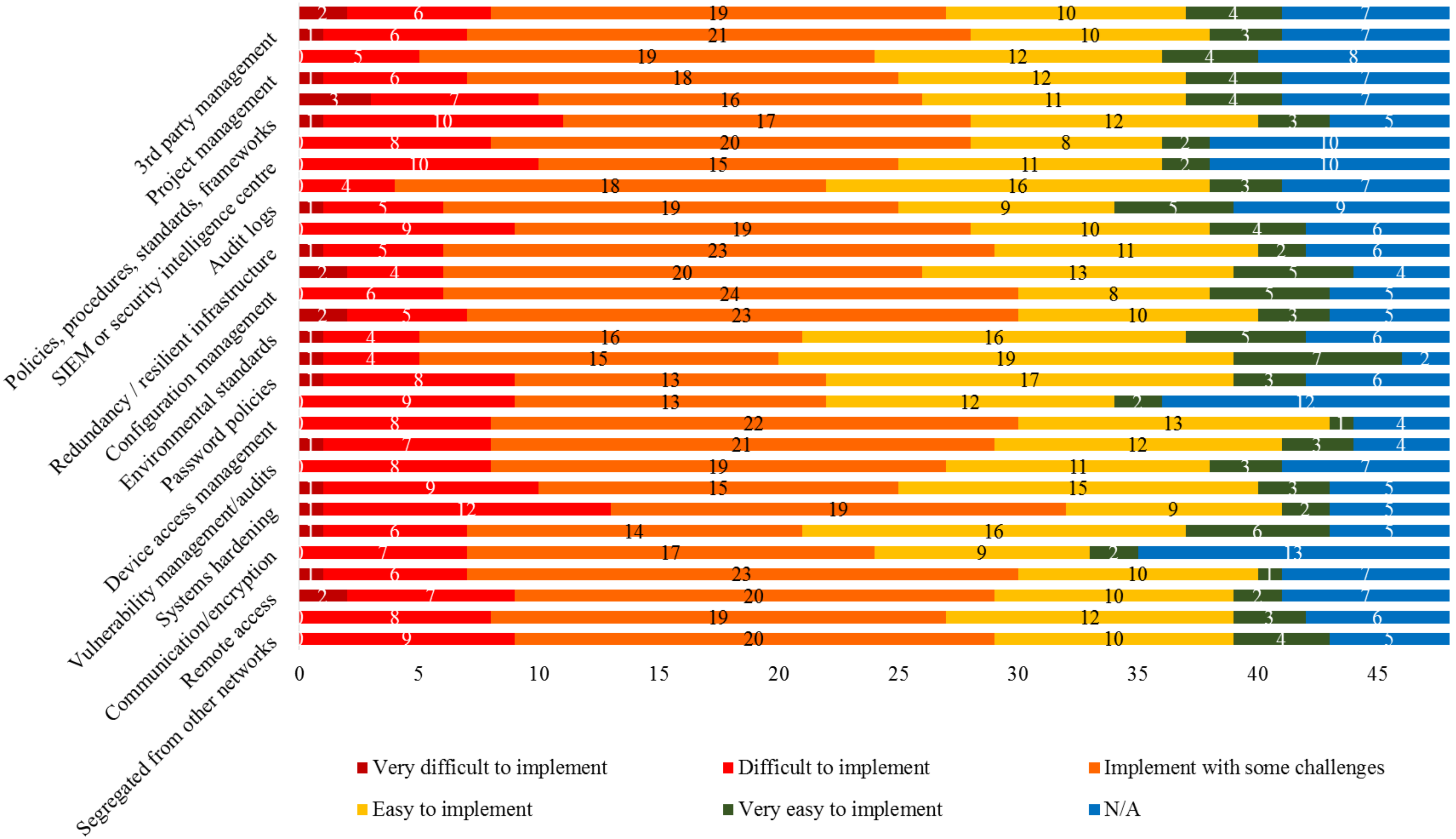


Figure 4.23: Ease of implementation of controls in ICS/SCADA environment

4.6.4 What type of intelligence do you rely on to detect threats aimed at your ICS/SCADA systems?

This relates to Question D6 of the questionnaire. Figure 4.24 shows what type of intelligence the respondents rely on to detect threats aimed at their ICS/SCADA environment. 32 respondents *Rely on staff to know when to search out events*, 25 *Use anomaly detection tools like SIEM/SIC to identify trends*, 20 *Review audit logs* and 3 had *No* (none) intelligence to detect threats in their ICS/SCADA environment. 1 had *another method.*

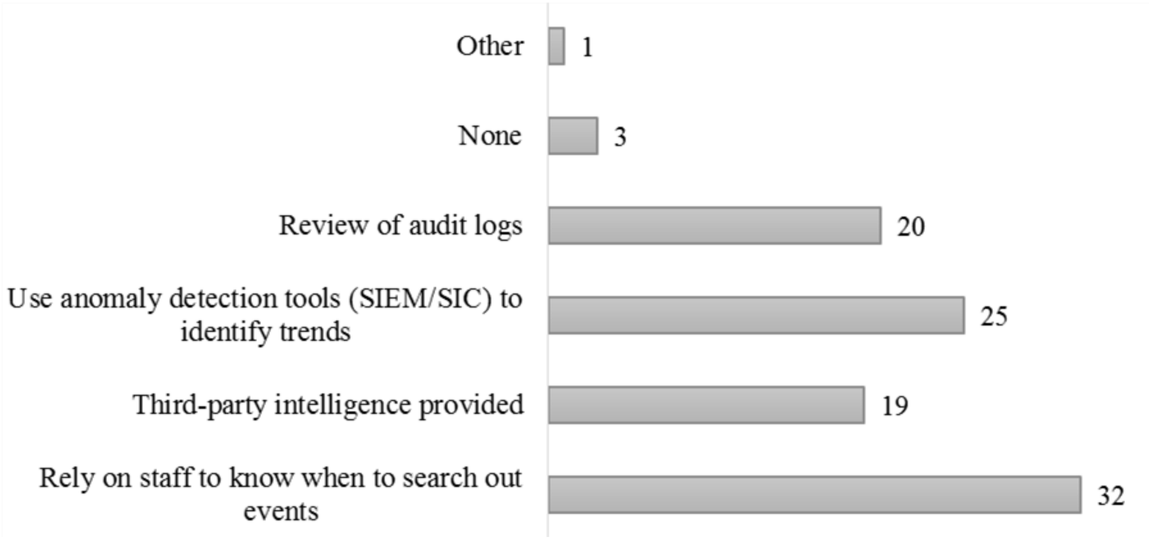


Figure 4.24: Methods/intelligence use to detect threats in ICS/SCADA environment

4.6.5 How confident/certain are you that the implemented controls mitigating the threats and risks are sufficient?

This relates to Question D7 of the questionnaire. Figure 4.25 indicates how confident/certain the respondents are that the implemented controls mitigating the threats and risks sufficiently. 35% of respondents indicated that they are *Moderately confident* that the implemented controls mitigate the threats and risks sufficiently, 29% indicated that they are *Somewhat confident* and 23% indicated that they are *Confident* that the implemented controls mitigate the threats and risks sufficiently, whereas 13% respondents indicated that they are *Not confident* at all that the implemented controls mitigate the threats and risks sufficiently. No one indicated that they are *Very confident* that the implemented controls mitigate the threats and risks sufficiently. In order to generate the descriptive statistics, the responses were rated from ‘1’, *Not confident at all* to ‘5’ *Very confident*.

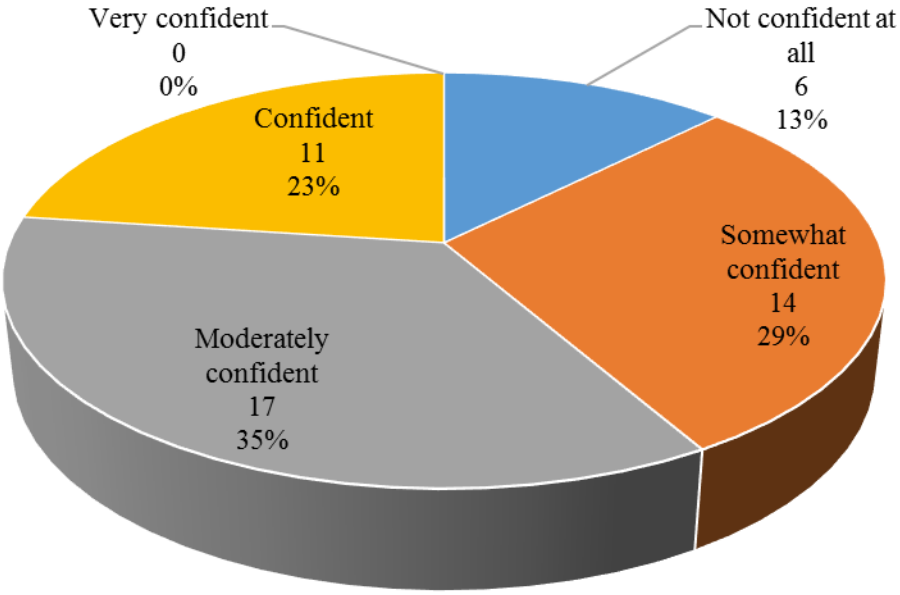


Figure 4.25: Confidence of implemented controls

Table 4.10: Frequency how confident/certain the respondents are that the implemented controls mitigating the threats and risks sufficiently

	Frequency	Percentage
Not confident at all	6	13%
Somewhat confident	14	29%
Moderately confident	17	35%
Confident	11	23%
Very confident	0	0%
Mean	2.69	
Std Deviation	0.97	
Variance	0.94	
Kurtosis	-0.90	
Skewness	-0.19	
Confidence Level (95.0%)	0.28	

From the responses, in Table 4.10, it is noted that the mean for responses of how confident/certain the respondents are that the implemented controls mitigating the threats and risks sufficiently for ICS/SCADA environment is 2.69, which is *Somewhat confident* leaning towards *Moderately confident*.

The 95% confidence intervals for this is 0.28. This indicates that with 95% confidence, the population mean for how confident/certain the respondents are that the implemented controls mitigating the threats and risks sufficiently for ICS/SCADA environment is between 2.41 (mean – confidence = 2.69 – 0.28) to 2.97 (mean + confidence = 2.69 + 0.28). This indicates that the population mean for how confident/certain the respondents are that the implemented controls mitigating the threats and risks sufficiently for ICS/SCADA environment is between *Somewhat confident* leaning heavily towards *Moderately confident*.

4.6.6 What are your top three priorities when it comes to implementing effective controls for the security of your control systems or ICS/SCADA systems that you have encountered?

This relates to Question D8 of the questionnaire. The top 3 priorities when it comes to implementing effective controls for the security of ICS/SCADA systems are: 1. *Preventing control system service interruption* which majority 24 (50%) of the respondents selected, 2. *Preventing financial loss/Protecting shareholder value* 20 (42%) and 2. *Protecting health and safety of employees* 17 (35%) as depicted in Figure 4.26.

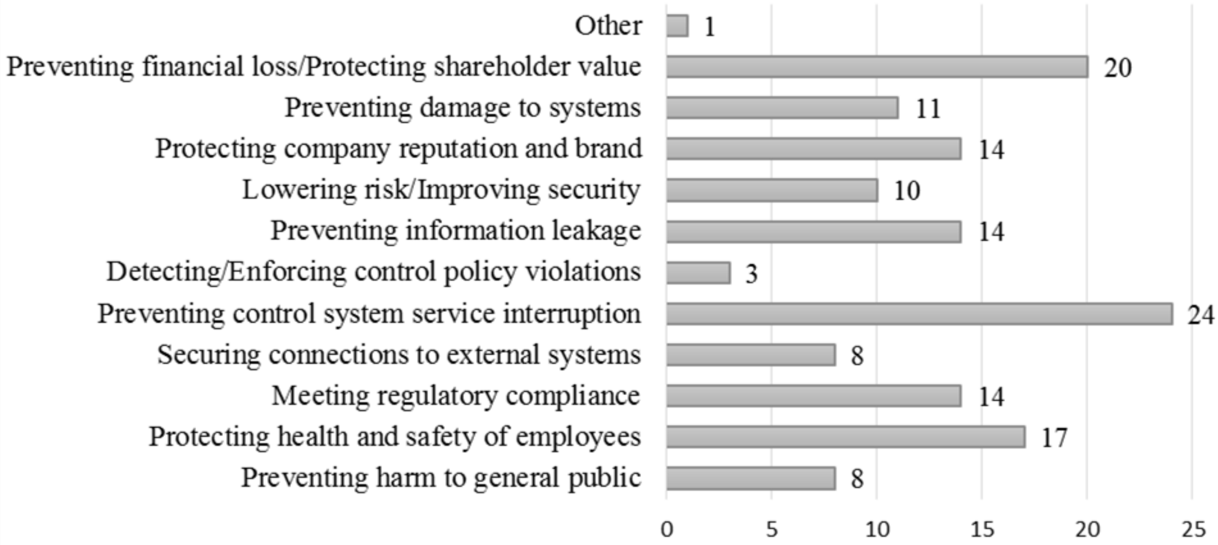


Figure 4.26: Top priorities for implementing effective controls

We can conclude from Figure 4.26 that 24 (50%) of respondents indicated that their top priority is Preventing control system service interruption, which aligns to Section 2.2.1 which indicated that for ICS/SCADA systems availability is more important than confidentiality and integrity.

4.7 Comparisons and correlations

This section looks at comparisons and correlations between various questions in order to determine groupings or clusters as well as validating the responses from earlier questions.

4.7.1 Risk of threats

As discussed in Section 3.4, risk is defined as *Impact* times *Probability/Likelihood*. The mean from the *Probability/Likelihood* of each threat from Section 4.3.2 was taken as well the mean from the *impact* of the threat from Section 4.3.4. The means of each threat's *Probability/Likelihood* vs the mean of each threat's *Impact* was plotted in Figure 4.34.

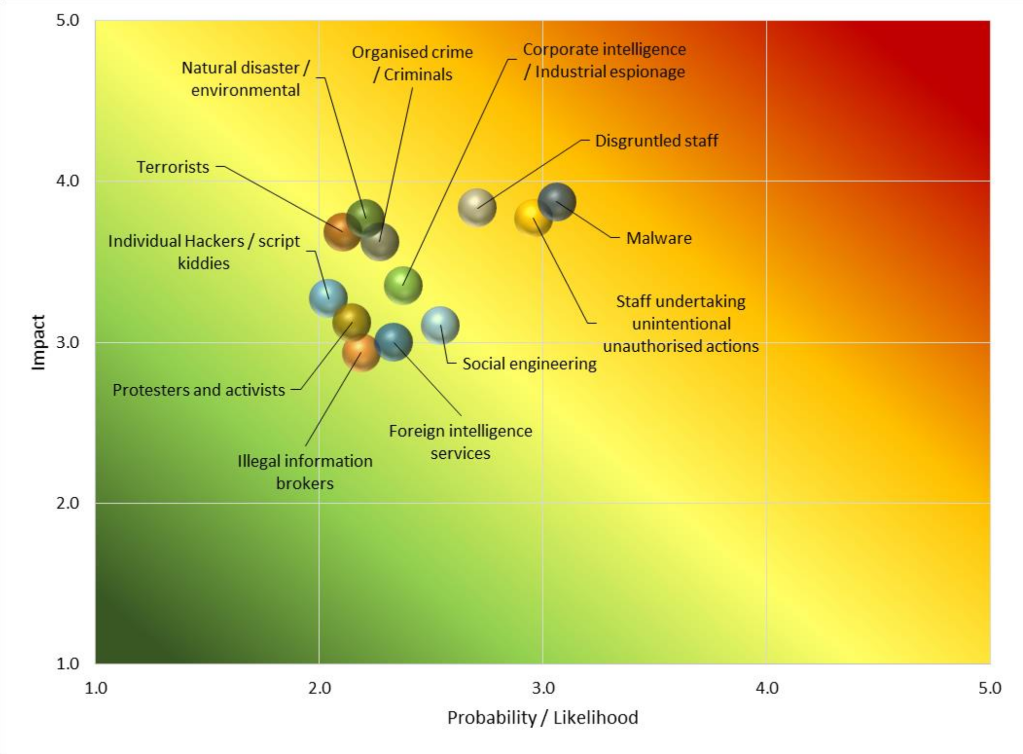


Figure 4.27: Risk (Impact vs Probability/Likelihood)

From Figure 4.27 it was observed that the top three risks to ICS/SCADA environment are *Malware*, *Staff undertaking unintentional unauthorised actions* and *disgruntled staff*. Comparing this to the top three threats likely to occur, it is noted that this is exactly the same with *Malware* being the top threat, *Staff undertaking unintentional unauthorised actions* and *disgruntled staff (intentional)*. Also comparing this to the top three threats likely to impact ICS/SCADA systems, the top three is similar but in a slightly different order. Malware is still the top threat to impact ICS/SCADA systems, secondly is *disgruntled staff (intentional)* and *Staff undertaking unintentional unauthorised actions*.

We can also see from Figure 4.27 that there are almost three distinct clusters. The first being the top three risks*; Malware, Staff undertaking unintentional unauthorised actions* and *disgruntled staff*. The second cluster or grouping consists of *Organised crime/Criminals, Natural disaster/environmental, Terrorists* and *Corporate intelligence/Industrial espionage*, all having Probability/Likelihood above two (*Low* - Expected to occur in a few circumstances) but higher impact, above 3.6 (leaning towards *High impact* – e.g. service disruption). The third cluster consist of threats also have a Probability/Likelihood above two (*Low* - Expected to occur in a few circumstances) but lower impact just above three (*Medium impact* – e.g. some service disruption). The threats that make up this cluster or grouping are: *Foreign intelligence services, Illegal information brokers, Protesters and activists, Individual Hackers/script kiddies* and *Social engineering*.

4.7.2 Correlation between Probability/Likelihood and Impact of threats

The correlation between the Probability/Likelihood of a threat occurring and the Impact of threats on ICS/SCADA environments were calculated. Only the components were the two variables are correlated are shown and the self-correlation has been removed for convenience, hence there is no symmetry.

Table 4.11: Partial correlation Matrix between Probability/Likelihood and Impact of threats

		Probability/Likelihood											
		Individual Hackers/script kiddies	Illegal information brokers	Disgruntled staff (intentional)	Staff undertaking unintentional unauthorised actions	Corporate intelligence/Industrial	Foreign intelligence services	Terrorists	Organised crime/Criminals	[Protesters and activists	Malware	Natural disaster/environmental	Social engineering
Impact	Individual Hackers/script kiddies	0.26	0.26	0.07	0.10	-0.09	-0.13	-0.03	-0.09	0.10	-0.06	-0.10	-0.31
	Illegal information brokers	0.29	0.26	0.21	0.00	0.08	0.15	0.10	0.09	0.26	0.04	-0.17	0.22
	Disgruntled staff (intentional)	0.06	0.01	0.47	0.50	0.16	-0.01	-0.12	-0.12	0.22	-0.03	0.07	-0.09
	Staff undertaking unintentional unauthorised actions	0.08	0.17	0.40	0.49	0.21	0.05	-0.09	0.09	0.12	0.23	0.05	0.14
	Corporate intelligence/Industrial espionage	-0.05	-0.09	0.12	-0.02	0.38	0.13	-0.05	0.11	0.12	0.00	-0.07	0.45
	Foreign intelligence services	0.11	0.09	0.24	-0.10	0.33	0.40	0.36	0.46	0.45	0.03	0.05	0.41
	Terrorists	0.07	0.12	0.32	-0.04	0.21	0.23	0.28	0.38	0.44	0.02	0.12	0.17
	Organised crime/Criminals	-0.04	0.20	0.16	0.00	0.20	0.08	0.24	0.40	0.36	0.18	0.12	0.20
	Protesters and activists	0.13	0.18	0.24	0.17	0.16	0.22	0.31	0.27	0.54	0.09	0.17	0.05
	Malware	0.00	0.09	0.04	0.13	0.22	0.15	0.14	0.14	0.09	0.25	0.07	0.02
	Natural disaster/environmental	-0.26	-0.09	-0.06	0.10	0.29	0.07	0.12	0.13	0.10	0.03	0.38	0.10
	Social engineering (phishing emails etc.)	-0.12	-0.04	0.02	-0.23	0.28	0.20	0.02	0.24	0.20	-0.04	0.09	0.50

From the partial correlation Matrix in Table 4.11, it was observed that there is a strong correlation (where the correlation coefficient, *r*, is greater than 0.5) between the Probability/Likelihood of the threat (*Staff undertaking unintentional unauthorised actions (e.g. making changes without following change control process)*) and the impact that the threat (*disgruntled staff (intentional)*) have. This could indicate that the respondents see Probability/Likelihood of *Staff undertaking unintentional unauthorised actions* similar to the impact that *disgruntled staff (intentional)* would have.

There are also strong correlations between the Probability/Likelihood of the threat (*Protesters and activists*) with the impact of the same threat. This is similar for the Probability/Likelihood and the impact of the threat (*Protesters and activists*).

4.7.3 Security confidence

As previously discussed in Section 3.4, the security confidence is made up from *Usability of security* (How effective are the following controls implemented in your ICS/SCADA environment) and *Ease of use of security* (How easy is it /was it to implement the following controls implemented in your ICS/SCADA environment). The mean from the effectiveness of each control from Section 4.6.1 was taken as well the mean from the ease of implementation of each control from Section 4.6.2. The mean of the effectiveness versus the mean of ease of implementation for each control was plotted in Figure 4.35.

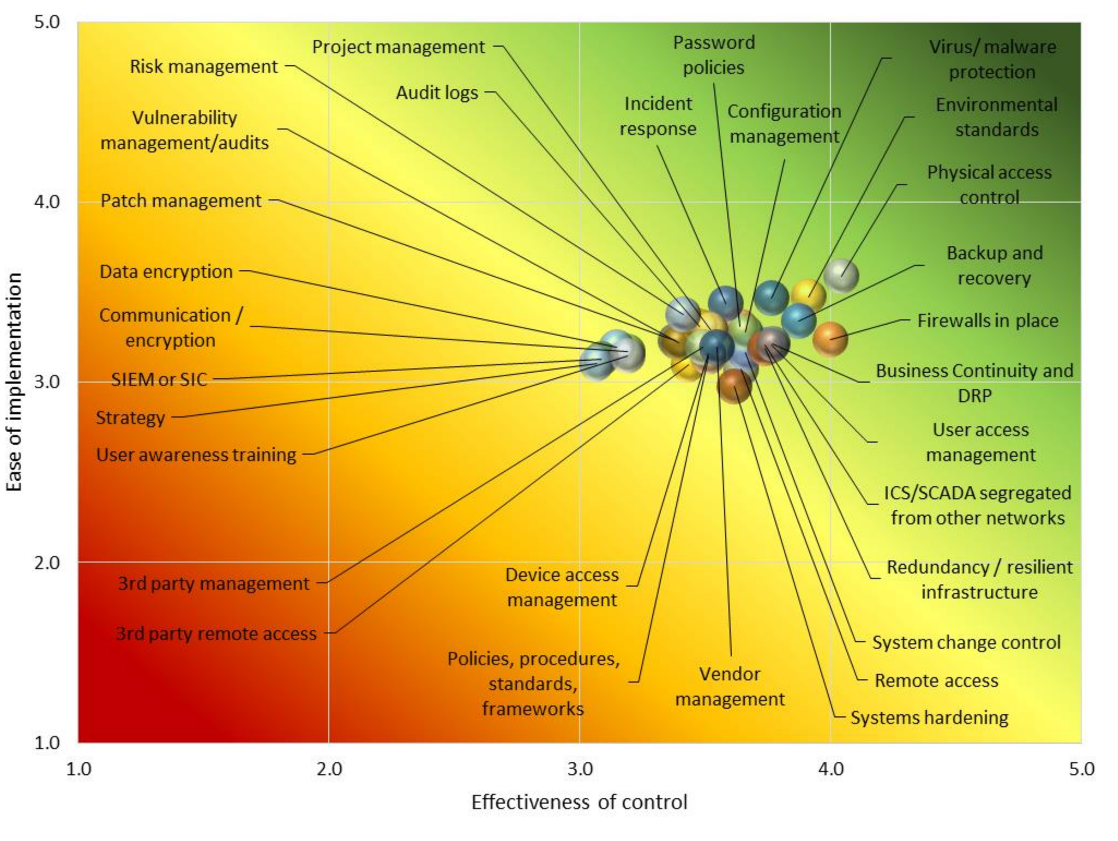


Figure 4.28: Effectiveness of control vs Ease of implementation

From Figure 4.28 the top five security confidence controls are *Physical access control*, *Environmental standards*, *Backup and recovery*, *Firewalls in place*, and *Virus/malware protection*. Comparing this to the top three effective control implemented in the ICS/SCADA environments, it is noted *Physical access control* is also first followed by *Firewalls* and *Environmental controls*. (*Partially Implemented/in progress* but leaning strongly towards *Implemented but requires improvement*).

Also comparing the security confidence controls with the top three easiest controls to implement for the ICS/SCADA environment, *Physical access control* is again first followed by *Environmental standards* which the same as the security confidence shown. *Virus/ malware protection* is third under easiest controls to implement for the ICS/SCADA environment, but is fifth of the security confidence controls.

We can also see from Figure 4.28 that there is a distinct group of controls which have less security confidence. These are *User awareness training, ICS/SCADA strategy, SIEM or SIC, Communication/encryption* and *Data encryption*. From the effectiveness of the controls implemented it is noted that these controls are *Partially Implemented/in progress* and from ease of implementation the controls are *Implemented with some challenges*.

4.7.4 Correlation between Probability/likelihood of threats and Vulnerabilities

The correlation between the Probability/Likelihood of a threat occurring and the Vulnerabilities of ICS/SCADA environments were calculated. As before, only the components were the two variables are correlated are shown and the self-correlation has been removed for convenience.

From the partial correlation matrix in Table 4.12, it is noted there is a strong correlation (where the correlation coefficient, *r*, is greater than 0.5) between the Probability/Likelihood of the threat *(Staff undertaking unintentional unauthorised actions* (e.g. making changes without following change control process)) and the vulnerability *Patching* - outdated/unpatched. This could indicate that the respondent sees Probability/Likelihood of *Staff undertaking unintentional unauthorised* actions occurring where there are *no patching or patches is outdated*.

Similar the Probability/Likelihood of the threat *Corporate intelligence/Industrial espionage* have a strong correlation to the following three vulnerability: *Patching - outdated/unpatched, Remote access – authentication not secure/shared passwords for vendors* and *Wireless connections – overlooked and poorly configured*. This could indicate that the respondents see Probability/Likelihood of *Corporate intelligence/Industrial espionage* occurring where there are *no patching or patches is outdated,* or where there is a vulnerability in *remote access* or *poorly configured/unsecure wireless connections*.

Table 4.12: Partial correlation Matrix between Probability/Likelihood of threats and Vulnerabilities

		Probability/Likelihood of threat											
		Individual Hackers/script kiddies	Illegal information brokers	Disgruntled staff	Staff undertaking unintentional unauthorised actions	Corporate intelligence/Industrial espionage	Foreign intelligence services	Terrorists	Organised crime/Criminals	Protesters and activists	Malware	Natural disaster/environmental	Social engineering
Vulnerabilities	Access control - No or weak password	0.25	0.28	0.27	0.43	0.34	0.25	0.25	0.20	0.31	0.20	0.33	0.02
	Patching - outdated/unpatched	0.29	0.44	0.23	0.50	0.56	0.34	0.36	0.40	0.33	0.41	0.44	0.25
	Configuration – Default configuration, no backup of configuration	0.23	0.37	0.19	0.45	0.21	0.11	0.12	0.14	0.23	0.33	0.16	-0.02
	Network perimeter – Unsecure, firewall don’t exist/misconfigured, direct connections to internet	0.25	0.33	0.12	0.37	0.36	0.24	0.22	0.31	0.27	0.50	0.42	0.19
	Monitoring – No or limited	0.33	0.31	0.23	0.39	0.35	0.23	0.28	0.26	0.36	0.26	0.29	-0.12
	Remote access – authentication not secure/shared passwords for vendors	0.29	0.39	0.32	0.38	0.51	0.41	0.33	0.39	0.36	0.26	0.29	0.37
	Physical security – inadequate protection and/or no environmental controls	-0.08	0.02	0.19	0.32	0.16	0.04	0.08	0.17	0.22	0.25	0.34	0.18
	Wireless connections – overlooked and poorly configured	0.14	0.33	0.27	0.33	0.55	0.19	0.10	0.32	0.26	0.35	0.30	0.49
	Anti-virus/malware – No software installed/unused/outdated	0.13	0.17	0.02	0.24	0.41	0.26	0.12	0.12	0.18	0.25	0.33	0.28

4.8 Reliability

The questions listed in Table 4.13 contained questions for which the Cronbach Alpha coefficient could be calculated. Questions A1 – A4, B1 – B2, C4, C8, D1 – D3 and D6 –D8 contained one variable and the Cronbach Alpha’s coefficient could not be calculated. Where the Cronbach Alpha coefficient is between 0.8 and 0.9, the internal consistency is good and where the Cronbach Alpha coefficient is greater than 0.9, the internal consistency is excellent. Overall the internal consistency ranges from acceptable to excellent. This shows great reliability of the data.

Table 4.13: Cronbach Alpha for each question

Question	Cronbach Alpha	Description
C2 Threats related to ICS/SCADA	0.872918615	Internal consistency is *good*
C3 Impact should threats related to ICS/SCADA occur	0.864274112	Internal consistency is *good*
C5 Vulnerabilities related to ICS/SCADA	0.904610256	Internal consistency is *excellent*
C6 Controls to mitigate the vulnerabilities related to ICS/SCADA	0.966448585	Internal consistency is *excellent*
C7 Impact of non-governed ICS should these factors materialise	0.799746473	Internal consistency is *acceptable* bordering *good*
D4 Effectiveness of controls in ICS/SCADA environment	0.968958699*	Internal consistency is *excellent*
D5 Easy is it /was to implement controls in ICS/SCADA environment	0.974722628*	Internal consistency is *excellent*

* There values were calculated by imputing the values. Imputed values are when the actual values are not available for the calculation and they are blank. For the questions, D4 and D5, there were either *Not applicable* answers or *Not sure* answers and hence the actual values were not available.

4.9 Summary

The chapter presented the results from the questionnaire survey. A third of respondents that had a poor or very poor visibility of threats on their ICS/SCADA environment which could indicate that these ICS/SCADA environments are not governed. The top three threats likely to occur as well as have an impact are *malware*, *staff undertaking unintentional unauthorised actions* and *disgruntled staff*. This was triangulated to another question where the respondents indicate the same top threats.

The study found that the top three vulnerabilities related to ICS/SCADA systems are *patching (outdated or unpatched systems)*, *no or limited monitoring* and *access control (no or weak passwords)*.

The top three controls mitigating vulnerabilities in the ICS/SCADA environments are *configuration (default configuration, no backup of configuration)*, *physical security* and *network perimeter* (unsecure, firewall don't exist/misconfigured, direct connections to internet) all *partially implemented/in progress*, but leaning towards *implemented control requires improvement*.

It was noted the top three impacts of non-governed ICS/SCADA environments should threats and vulnerabilities materialise, are *loss of availability/denial of service*, *loss of integrity* and *unauthorised control*.

Almost two thirds of respondents might possibly have had a threat that occurred in their ICS/SCADA environment. The study found that the top three frameworks used by the respondents to govern and secure their ICS/SCADA environments are COBIT, ITIL and the ISO 27001 series.

The maturity of governance and security for ICS/SCADA environments is between *evolving* (Inconsistently applied controls) leaning slightly towards *established* (controls in place, but there is a need for enhancement).

The top three effective controls implemented in the ICS/SCADA environments are *physical access control*, *firewalls in place*, and *environmental standards* and the top three easiest controls to implement are *physical access control*, *environmental standards* and *virus/malware protection*. Only the *virus/malware protection* addresses one of the top threats. This shows a misalignment of focusing and implementing controls that does not mitigate the top threats and vulnerabilities.

Chapter 5 Secondary Data and Document Analysis

5.1 Introduction

This chapter presents the analysis of secondary data and documents. The documentary methods to collect the data from open source, security system data, reports and advisories, was analysed using descriptive statistics which was then summarised in order to address the Research Objectives as mentioned in Section 1.5.

Data from Shodan and from security systems was obtained, sanitised and analysed. The document analysis was performed by selecting existing frameworks, security alerts reports and trends. The data from the documents was then divided into pre-determined categories, coded and summarised. Figure 5.1 is a graphical representation of the outline of this chapter and overall structure.

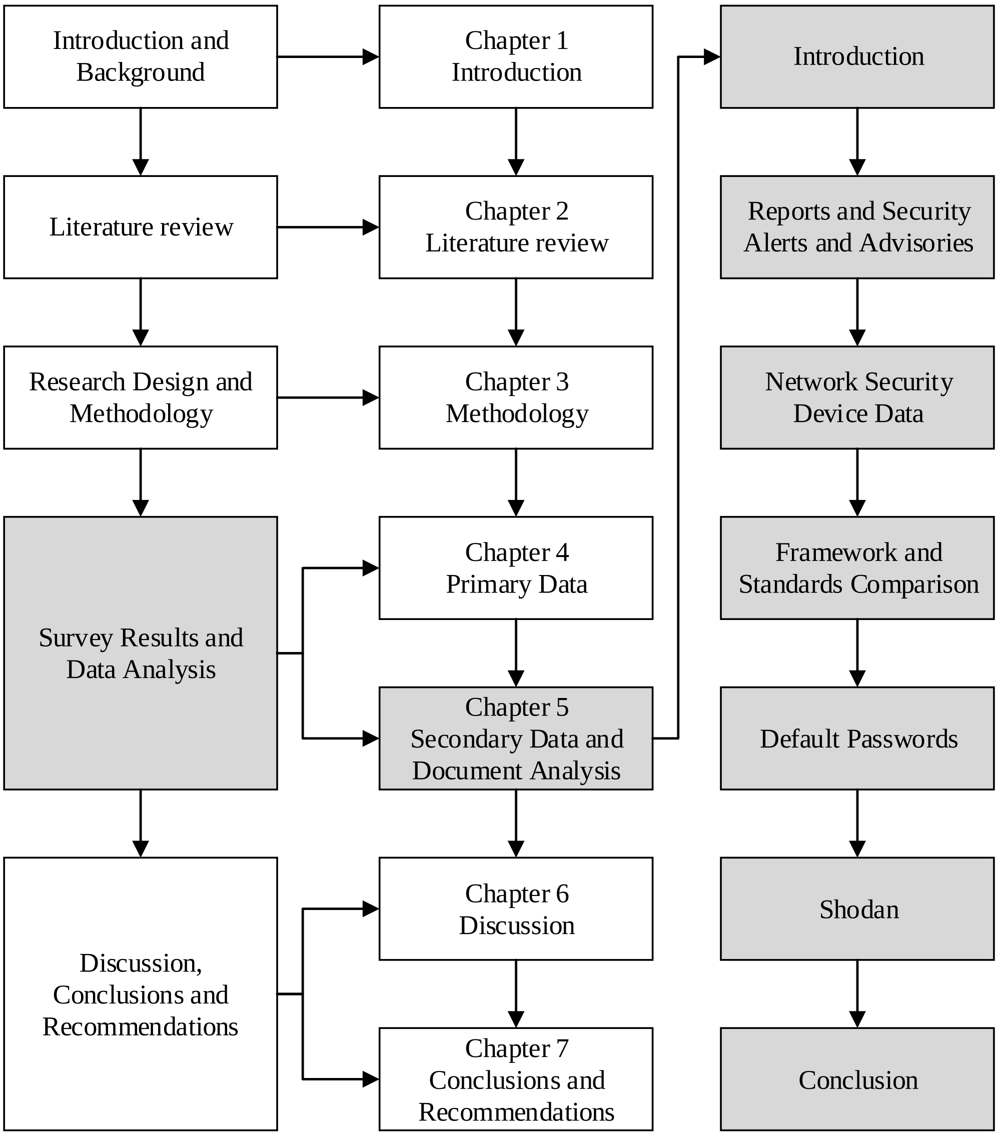

Introduction and Background
Chapter 1 Introduction
Introduction
Literature review
Chapter 2 Literature review
Reports and Security Alerts and Advisories
Research Design and Methodology
Chapter 3 Methodology
Network Security Device Data
Survey Results and Data Analysis
Chapter 4 Primary Data
Framework and Standards Comparison
Chapter 5 Secondary Data and Document Analysis
Default Passwords
Discussion, Conclusions and Recommendations
Chapter 6 Discussion
Shodan
Chapter 7 Conclusions and Recommendations
Conclusion

Figure 5.1: Graphical representation of Chapter 5 outline

5.2 Reports and Security Alerts and Advisories

The sample for the document analysis was chosen by selecting common and freely available security alert reports and trends related to Governance, Information security and ICS/SCADA. International reports, trends as well as one study from South Africa was used.

5.2.1 Symantec reports

Symantec has one of the world's most complete vulnerability databases and has been established as one of the most comprehensive sources of internet threat data making it ideal for information security threat and vulnerability information (Symantec 2016a, 2016b). Annually Symantec releases their Internet Security Threat Report that contain information around vulnerabilities in order to give consumers to enterprises necessary information to secure their systems effectively. Of particular note is the section on ICS/SCADA vulnerabilities which were reported on since 2010. For the analysis, the vulnerabilities related to ICS/SCADA were analysed.

The Symantec reports were obtained for a three year period, 2013 (Symantec 2014a, 2014b), 2014 (Symantec 2015) and 2015 (Symantec 2016a, 2016b). The vulnerabilities for ICS/SCADA were then categorised based on their description into the broader vulnerability type categories as displayed in Table 5.1. From Table 5.1, denial of service was the top vulnerability in 2013 with 37.5%, Memory corruption/buffer overflow second with 18.8% and information disclosure third at 15.6%. In 2014 denial of service declining and dropped from first in 2013 to seventh place in 2014. Memory corruption/buffer overflow increased to 28.6% as the top vulnerability in 2014. Info disclosure second with 22.9% and remote code execution and privilege escalation combined third with 11.4%. In 2015 security bypass was the top vulnerability at 22.8% followed closely by remote code execution at 21.9%. Third place was denial of service at 14.9%.

Combining the totals for the three years it is noted that the top combined vulnerability is security bypass at 17.7%, denial of service and memory corruption/buffer overflow both second with 17.1% each. Thirdly was remote code execution at 16.6%. The graphical representation is presented in Figure 5.1.

From Table 5.1, Figure 5.2 and Figure 5.3 it is observed that the total number of vulnerabilities from 2013 to 2014 have increased at a minimum margin, however the increase between 2014 to 2015 have increased significantly from 35 in 2014 to 114 in 2015. The number of Security Bypass vulnerabilities have significantly increase from 3 in 2014 to 26 in 2015, a 767% increase. Denial of Service vulnerabilities have also significantly increase by 750% from 2 in 2014 to 17 in 2015. Remote code execution vulnerabilities have increased by 525%, 4 in 2104 to 25 in 2015. An increase of 400% was seen for Code injection, moving from 1 in 2014 to 5 in 2015. There was also a 50% increase in the Memory corruption/buffer overflow vulnerability, 10 in 2014 to 15 in 2015. Other vulnerabilities increase by 100% from 3 in 2014 to 6 in 2015. This indicates that more and more vulnerabilities are being discovered and the rate of new vulnerabilities almost double year on year leave ICS/SCADA systems more exposed.

Table 5.1: Symantec reports years 2013 to 2015 combined

Vulnerability	Year						TOTAL	
	2013		2014		2015			
	No	**%**	**No**	**%**	**No**	**%**	**No**	**%**
Cross site scripting	1	3.1%	0	0.0%	6	5.3%	7	**3.9%**
Denial of service	12	37.5%	2	5.7%	17	14.9%	31	**17.1%**
Info disclosure	5	15.6%	8	22.9%	9	7.9%	22	**12.2%**
Memory corruption/buffer overflow	6	18.8%	10	28.6%	15	13.2%	31	**17.1%**
Other	2	6.3%	3	8.6%	6	5.3%	11	**6.1%**
Remote code execution	1	3.1%	4	11.4%	25	21.9%	30	**16.6%**
Security bypass	3	9.4%	3	8.6%	26	22.8%	32	**17.7%**
Code injection	2	6.3%	1	2.9%	5	4.4%	8	**4.4%**
Privilege escalation	0	0.0%	4	11.4%	5	4.4%	9	**5.0%**
Grand Total	**32**	**100%**	**35**	**100%**	**114**	**100%**	**181**	**100%**

Adapted from: Symantec (2014a, 2014b, 2015, 2016a, 2016b)

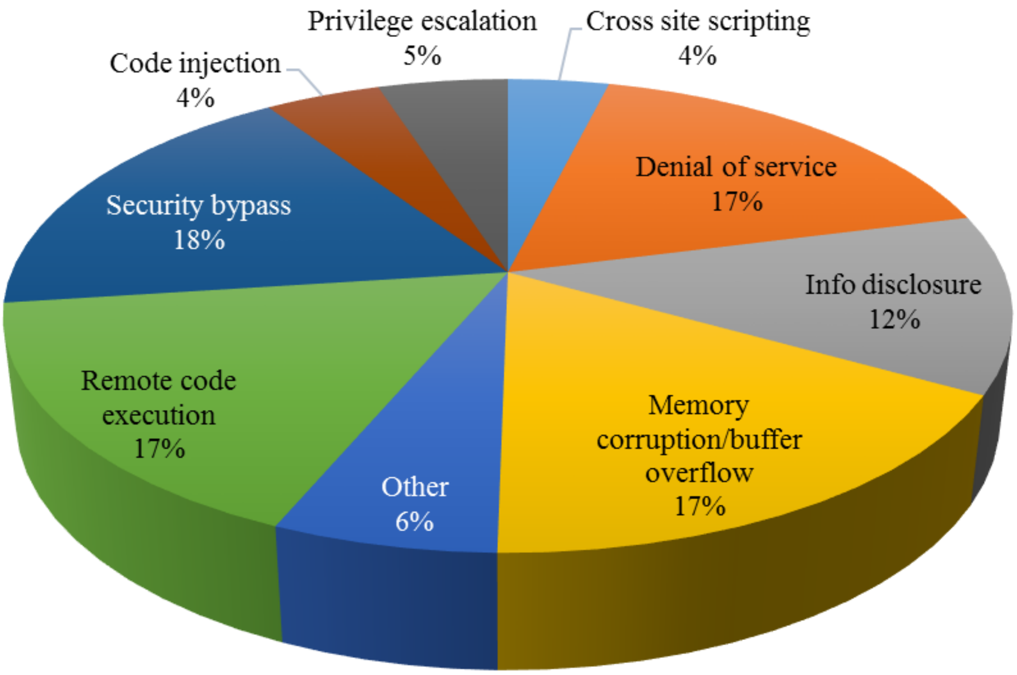


Figure 5.2: Symantec Report years 2013 to 2015 combined

Adapted from: Symantec (2014a, 2014b, 2015, 2016a, 2016b)

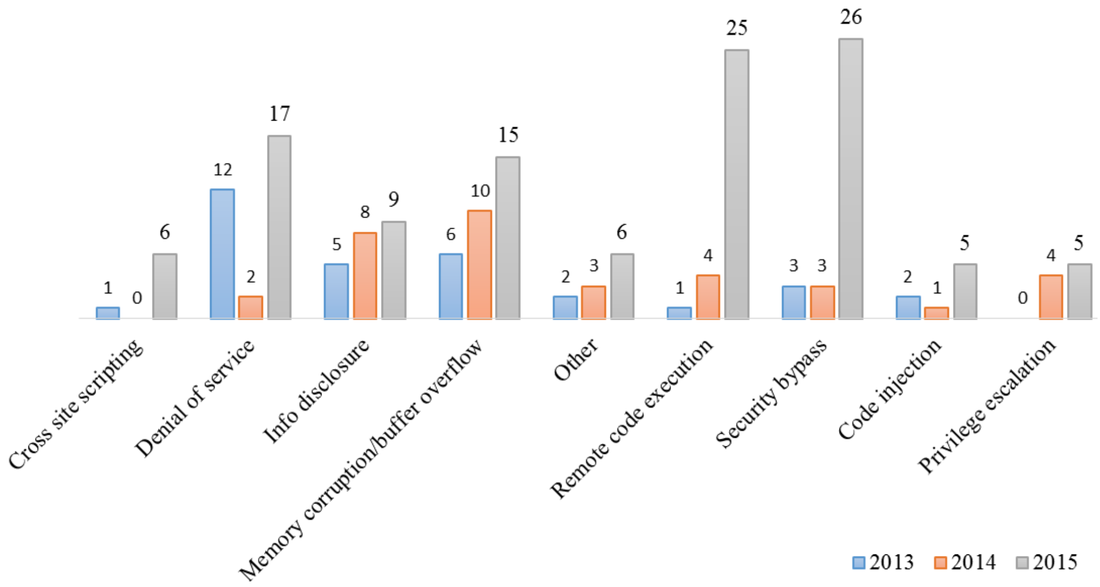


Figure 5.3: Symantec Report 2013 to 2015 comparison

Adapted from: Symantec (2014a, 2014b, 2015, 2016a, 2016b)

5.2.2 ICS-CERT

As part of the Industrial Control Systems Computer Emergency Response Team (ICS-CERT) mandate to reduce risk on critical infrastructure across the US, they compile an annual report to share security incidents and mitigating measures. The reports for 2014 (National Cybersecurity and Communications Integration Center 2014) and 2015 (National Cybersecurity and Communications Integration Center 2015) were obtained. The ICS-CERT responded to 245 incidents and to 295 incidents in 2014 and 2015 respectively. The ICS-CERT reports for 2014 and 2015 are listed per sector in Table 5.2.

From Table 5.2, and Figures 5.4 and 5.5, it was noted that the top sector in 2014 where incidents occurred were the Energy Sector with 32.2% and secondly Critical Manufacturing Sector where 26.5% of the incidents occurred. In 2015 there was an increase in the overall number of incidents as well as in the sectors, Critical Manufacturing Sector contributing 32.9% of the incidents and the Energy Sector experiencing 15.6% of the incidents. Combining the incidents for the two years, the top sectors experiencing incidents are Critical Manufacturing Sector with 30% and the Energy Sector with 23.1%. The other sectors all contribute less than 10% each. This shows that since the number of vulnerabilities increased year on year, see Section 5.2.1, so does the incidents increase. The increase in incidents in the Critical Manufacturing Sector, Transportation system and Water and Wastewater system sectors indicate that ICS/SCADA systems in critical operations are more and more becoming a target.

Table 5.2: ICS-CERT report 2014 and 2015

	2014		2015		Total	
Sector	No	%	No	%	No	%
Chemical Sector	4	1.6%	4	1.4%	**8**	**1.5%**
Commercial Facilities Sector	7	2.9%	3	1.0%	**10**	**1.9%**
Communications Sector	14	5.7%	13	4.4%	**27**	**5.0%**
Critical Manufacturing Sector	65	26.5%	97	32.9%	**162**	**30.0%**
Dams Sector	0	0.0%	6	2.0%	**6**	**1.1%**
Defence Industrial Base Sector	0	0.0%	2	0.7%	**2**	**0.4%**
Energy Sector	79	32.2%	46	15.6%	**125**	**23.1%**
Financial Services Sector	3	1.2%	2	0.7%	**5**	**0.9%**
Food and Agricultural Sector	2	0.8%	2	0.7%	**4**	**0.7%**
Government Facilities Sector	13	5.3%	18	6.1%	**31**	**5.7%**
Healthcare and Public Health Sector	15	6.1%	14	4.7%	**29**	**5.4%**
Information Technology Sector	5	2.0%	6	2.0%	**11**	**2.0%**
Nuclear Reactors, Materials, and Waste Sector	6	2.4%	7	2.4%	**13**	**2.4%**
Transportation Systems Sector	12	4.9%	23	7.8%	**35**	**6.5%**
Water and Wastewater Systems Sector	14	5.7%	25	8.5%	**39**	**7.2%**
Unknown	6	2.4%	27	9.2%	**33**	**6.1%**
Totals	**245**	**100%**	**295**	**100%**	**540**	**100%**

Adapted from: National Cybersecurity and Communications Integration Center (2014, 2015)

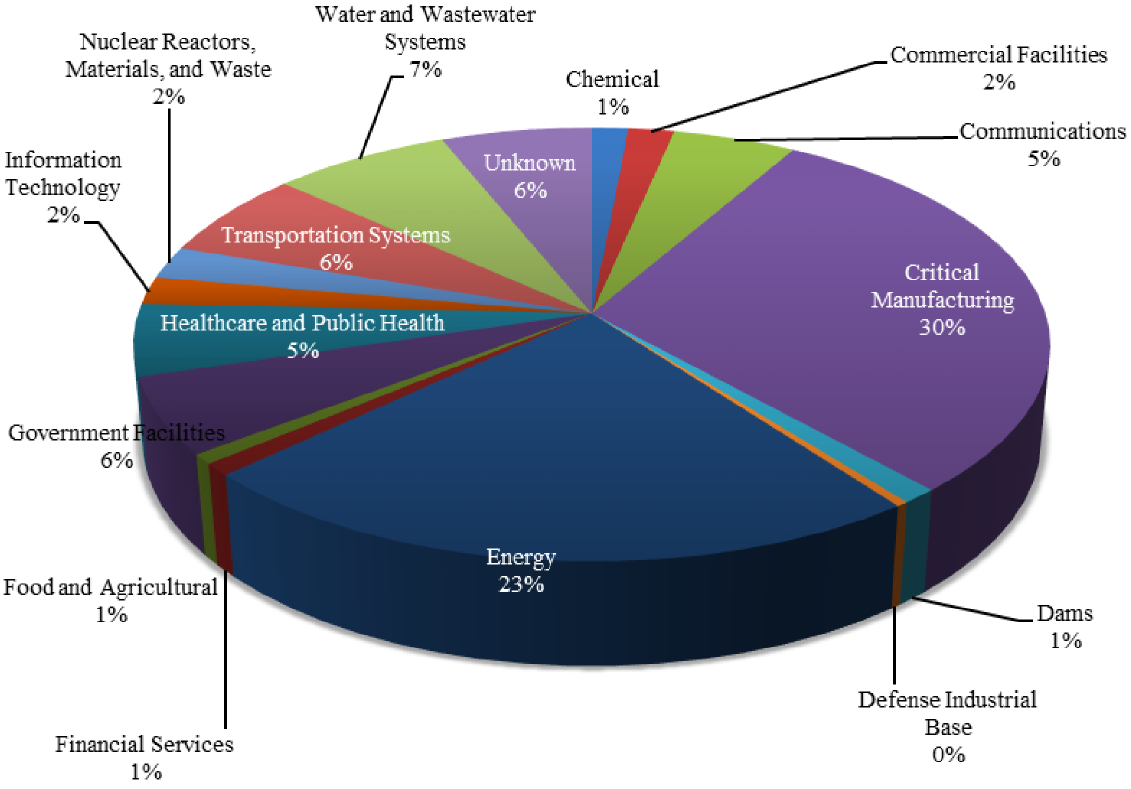


Figure 5.4: ICS-CERT 2014 and 2015 combined

Adapted from: National Cybersecurity and Communications Integration Center (2014, 2015)

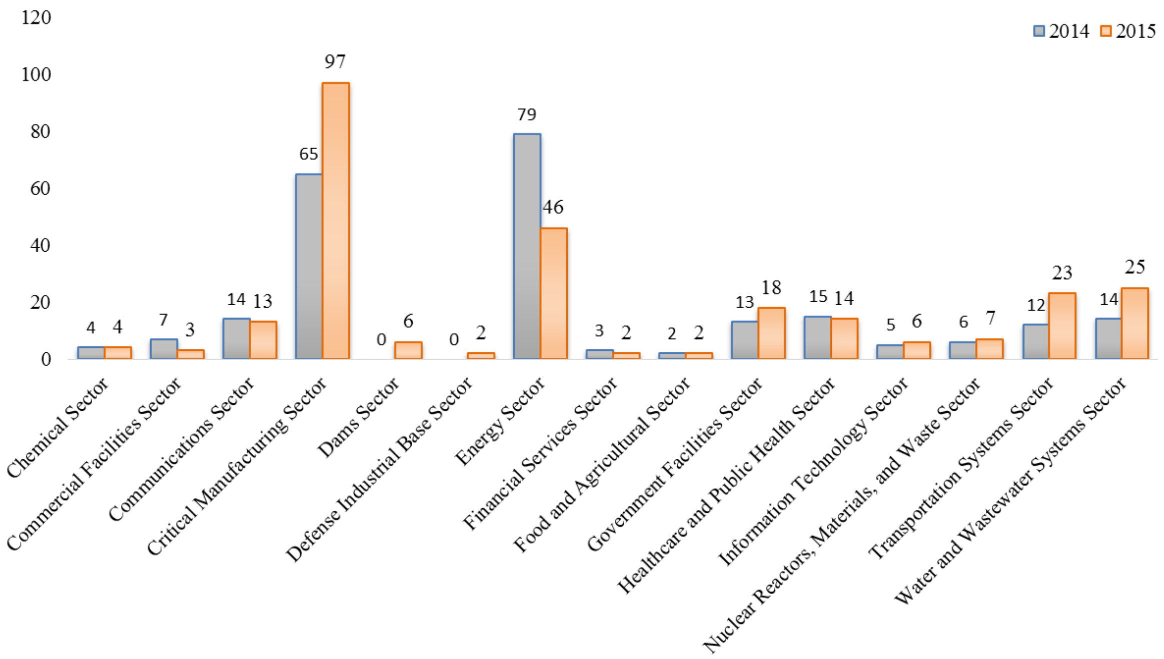


Figure 5.5: ICS-CERT 2014 and 2015 comparison

Adapted from: National Cybersecurity and Communications Integration Center (2014, 2015)

5.2.3 SANS survey

The SANS institute report annually on the state of ICS security in the hope that the report would contribute towards improving the condition of ICS/SCADA security. The SANS institute conducted surveys from 2013. The SANS surveys from 2013, 2014, 2015, and 2016 (SANS 2013, 2014, 2015, 2016a) was obtained.

5.2.3.1 Threat Vectors

As part of the SANS survey, the participants were asked to list the Top 3 threat vectors. The results are displayed in Table.

Table 5.3: SANS Threat Vectors 2013 to 2016

Threat Vector	2013	2014	2015	2016
External threat	65%	60%	73%	61%
Internal threat	71%	71%	49%	70%
Integration of IT into control system networks	-	-	46%	29%
Malware	72%	53%	41%	41%
Phishing scams	52%	35%	30%	34%
Industrial espionage	32%	25%	29%	25%
Extortion	20%	9%	19%	18%
Cyber-security policy violations	-	33%	-	-
External threat from supply chain or partners	-	-	-	24%
Other	8%	6%	8%	5%

Adapted from: SANS (2013, 2014, 2015, 2016a)

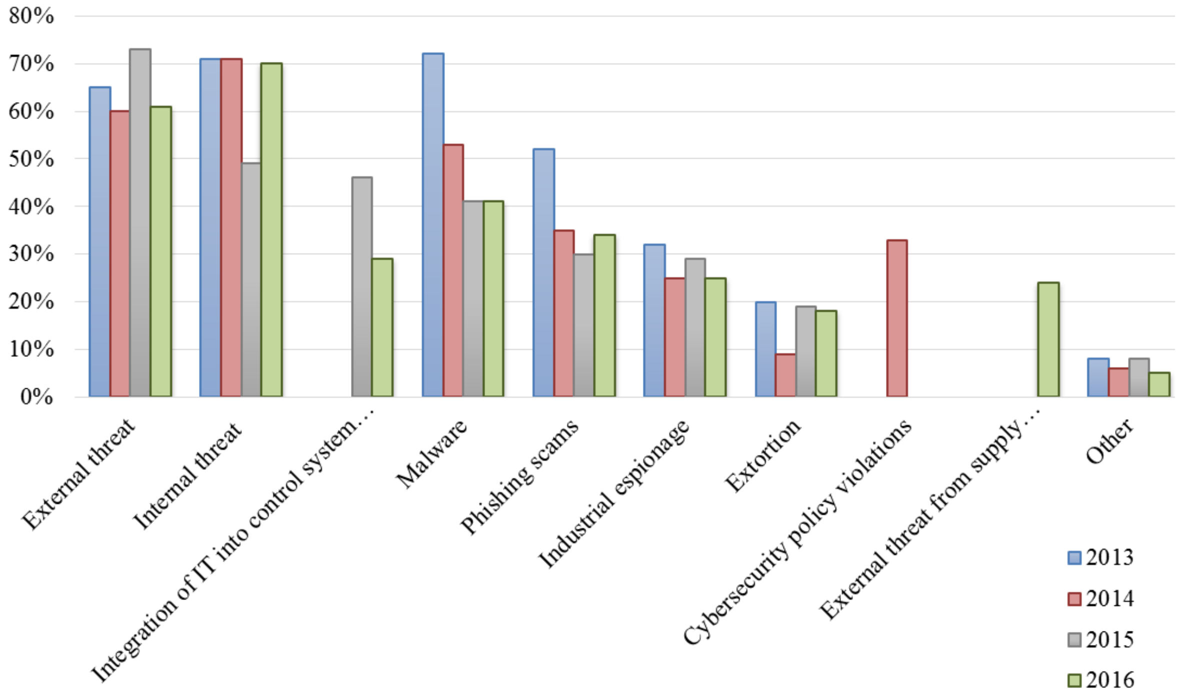


Figure 5.6: SANS Threat Vectors 2013 to 2016

Adapted from: SANS (2013, 2014, 2015, 2016a)

From Table 5.3 and Figure 5.6 it is noted that the top threat vectors in 2013 were Malware, Internal Threat and External Threat. 2014 saw Internal Threat moved to first place, External Threat second and Malware dropped to third. In 2015, External Threat increase to first place while Internal Threat dropped to second. The third place in 2015 was attributed to a new Threat, Integration of IT into Control System Networks. 2016 repeated the exact same pattern as 2014 with Internal Threat in first place, External Threat second and Malware third.

External Threat has slightly decreased from 2013 to 2014 and then increased in 2015 just to decrease again in 2016 to a similar level as 2014. Internal threat remained the same for 2013/2014, decreased in 2015 and returned to approximately the same level in 2016 as it was in 2013/2014. Malware trend indicated that the threat has decreased from 2013 to 2014 and decreased again in 2015, but remained the same in 2016.

Phishing Scams generally decreased as well as Industrial Espionage and Other Threats. Integration of IT into Control System Networks Threat was introduced in 2015 and decreased in 2016. Cyber-security Policy Violations was a new Threat that only appeared in 2014. This implies an increase in internal threat as internal staff are violating policies.

The top three threat vectors for each year are summarised in Table 5.4:

Table 5.4: SANS Top Threat Vectors 2013 to 2016

Year	Top threat		
	First	Second	Third
2013	Malware (72%)	Internal Threat (71%)	External Threat (65%)
2014	Internal Threat (71%)	External Threat (60%)	Malware (53%)
2015	External Threat (73%)	Internal Threat (49%)	Integration of IT into Control System Networks (46%)
2016	Internal Threat (70%)	External Threat (61%)	Malware (41%)

Adapted from: SANS (2013, 2014, 2015, 2016a)

The top threats overall are: Internal Threat, External Threat and Malware. All these threats could have an impact on the operation of ICS/SCADA systems and could lead to disruption to the operations or organisation. This is further discussed in Section 6.2.2.

5.2.3.2 Security Standard/Frameworks used

As part of the SANS survey, 2013 to 2015, the participants were asked to list the security standard or control frameworks used. The results are displayed in Table 5.5.

Table 5.5: SANS Security Standard used 2013 to 2015

Security Standard	2013	2014	2015
NIST Guide to SCADA and Industrial Control Systems Security (SP 800-82)	40%	32%	49%
NERC CIP	30%	20%	37%
Critical Security Controls	34%	26%	34%
ISA99 (Industrial Automation and Control Systems Security)/IEC 62443	18%	18%	29%
ISO 27000 series including 27001 and others		20%	28%
Other	26%	6%	9%
ENISA Guide to Protecting ICS - Recommendations for Europe and Member States		6%	8%
ISA100.15 Backhaul Network Architecture		5%	7%
Qatar ICS Security Standard		4%	6%
Chemical Facility Antiterrorism Standards (CFATS)	6%	7%	5%
Unsure		27%	

Adapted from: SANS (2013, 2014, 2015, 2016a)

From Table 5.5 and Figure 5.7 it was noted that the most frequent standard used in 2013 is the NIST Guide to SCADA and Industrial Control Systems Security (40%), followed by the 20 Critical Security Controls (34%) and NERC CIP (30%). The ‘Other’ category was at 26%. Like 2013, the control framework used the most in 2014 were the NIST Guide (32%) again followed by the Critical Security Controls (26%). The NERC CIP and ISO 27000 tied in third position at 20%. The Other category decreased from 26% in 2013 to 6% in 2014 as new frameworks/standards being selected by the participants. These include: ENISA Guide to Protecting ICS—Recommendations for Europe and Member States (6%), ISA100.15 Backhaul Network Architecture (5%), and Qatar ICS Security Standard (4%). There was also however 27% of participants that were unsure of what control framework/standard is being used.

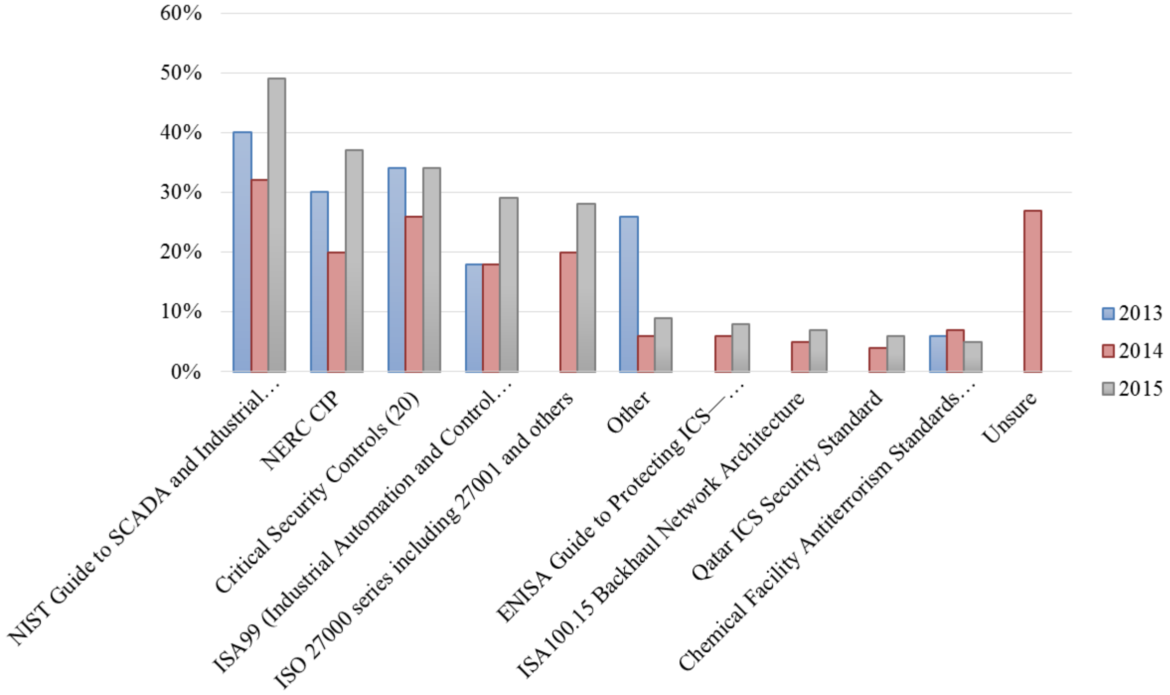


Figure 5.7: SANS Security Standards used 2013 to 2015

Adapted from: SANS (2013, 2014, 2015, 2016a)

In 2015 similar results show NIST being the most popular at 49%, but NERC CIP moving to second spot from 20% in 2014 to 37% in 2015. The Critical Security Controls also made the top 3 again at 34%. There was an increase in the use of the ISA99 standard as it moved from 18% in both 2013 and 2014 to 29% in 2015.

Combining the results from all three years the top three frameworks/standards consistently used are: NIST, Critical Security Controls and NERC CIP. There has been a general increase in the use of NIST and NERC, while the use of the Critical Security Controls remained similar.

5.2.4 Kaspersky Report

Kaspersky conducted research about vulnerabilities by gathering information from various sources such as ICS-CERT, Siemens Product CERT and compiled a report, Industrial Control System Vulnerabilities Statistics (Kaspersky 2016). The Kaspersky report provides a summary of the present global condition for ICS security, to determine the vulnerabilities of ICS/SCADA systems as well as looking at the vulnerable ICS components exposed to the Internet.

The Kaspersky report for 2015 was obtained and analysed. From Figure 5.8 it is noted that the top three vulnerabilities are: Buffer overflow, use of hard-coded credentials and cross-site scripting.

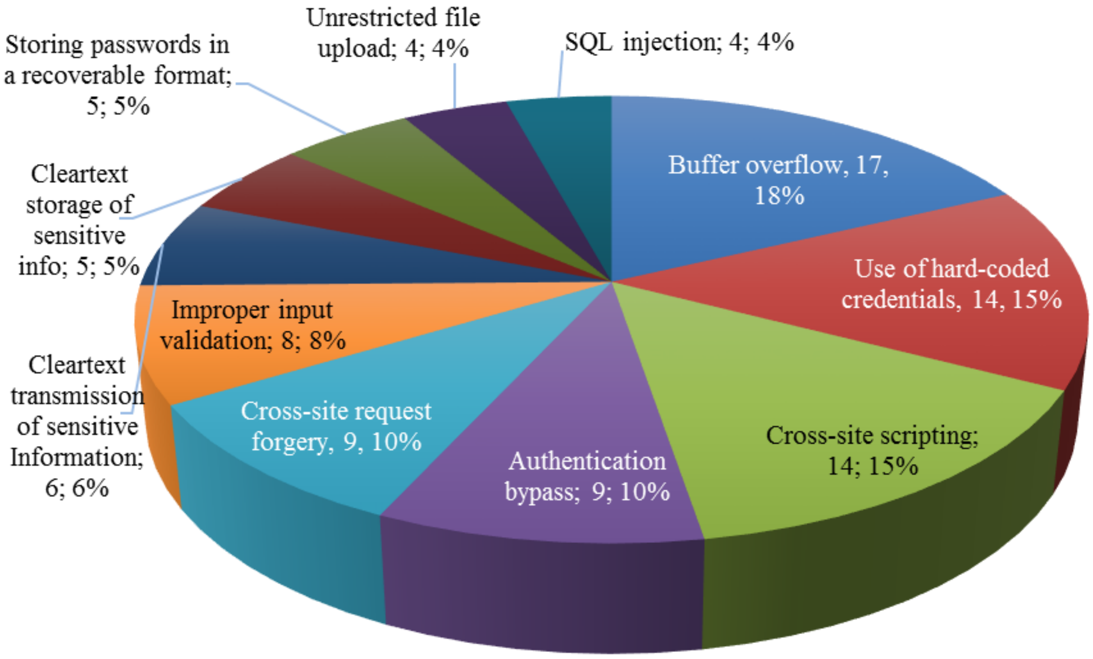


Figure 5.8: Kaspersky ICS Vulnerabilities

Adapted from: Kaspersky (2016)

5.2.5 Wolfpack

Wolfpack Information Risk conducted a survey on Critical Information Infrastructure in South Africa (Wolfpack 2016). This research was conducted independently and at the same time as this study was being conducted and the report, Critical Information Infrastructure Protection Report, was released in June 2016. Although this report focused on Critical Information Infrastructure Protection in South Africa, only a small section was dedicated ICS/SCADA systems. Similar questions were asked compared to the SANS report, as discussed in Section 5.2.3. The Wolfpack survey was distributed to a different audience as this study and the number of participant related to the ICS/SCADA part could not be determined.

From the survey conducted by Wolfpack Information Risk, as displayed in Figure 5.9 the top three threat vectors for ICS/SCADA systems were: Insider exploits (selected by 63%), and combined secondly, each selected by 56% of the participants, are External threats, Attacks originating within the internal network and Information security policy violations. Malware was selected by 31% of the participants.

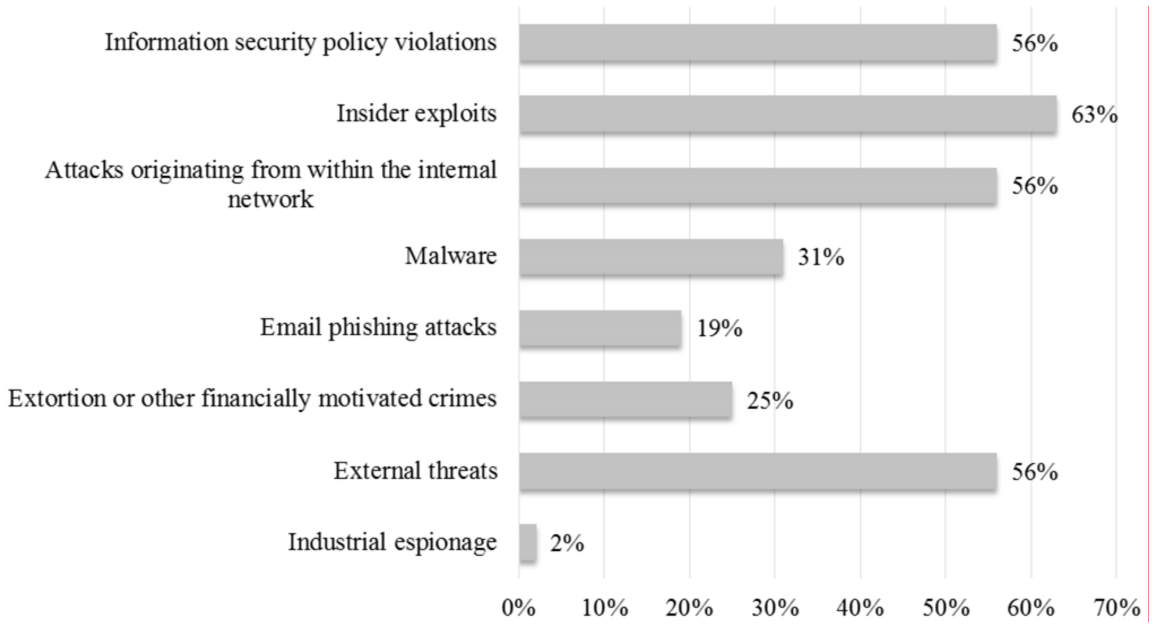


Figure 5.9: Wolfpack Top Vulnerabilities

Adapted from: Wolfpack (2016)

5.2.6 Comparing reports

This section compares vulnerabilities and threats from the Symantec, Kaspersky, SANS, Wolfpack and ICS-CERT reports as discussed in Section 5.2.1 to Section 5.2.5. The objective of this comparison is to determine the most prevalent vulnerabilities and threats in order to see if there are any similarities between these reports.

5.2.6.1 Vulnerabilities:

Table 5.6 compared the vulnerabilities reported from Symantec to Kaspersky for the year 2015. Security Bypass was reported as the Top vulnerability from the Symantec report, while Kaspersky reported the Top vulnerability as Buffer overflow, second use of hard-coded credentials compared to remote code execution reported by Symantec and cross-site scripting whereas denial of service was reported as the third biggest vulnerability by Symantec.

Table 5.6: Comparing vulnerabilities

Year	Report	Top vulnerability		
		First	Second	Third
2015	**Symantec**	Security bypass (26/ 24%)	Remote code (25/23%)	Denial of service (17/15.7%)
	Kaspersky	Buffer overflow (17/17.9%)	Use of hard-coded credentials (14)14%	Cross-site scripting (14/14%)

Author Compiled, Source: Symantec (2015), Kaspersky (2015)

The most prevalent vulnerabilities for 2015 are security bypass, remote code execution and buffer overflow. Others include denial of service, use of hard-coded credentials and cross-site scripting.

5.2.6.2 Threats

Table 5.7 compare the vulnerabilities reported from SANS to Wolfpack for the year 2016. SANS reported internal threat as the top threat which is similar to the top threat, insider exploits reported by Wolfpack. Similar external threat was reported by both SANS and Wolfpack as the second biggest threat, although attacks originating within the internal network and Information security policy violations were combined the second biggest threats as reported by Wolfpack. Malware was reported as third biggest threat by SANS whereas Wolfpack reported it as the fifth biggest.

Table 5.7: Comparing threats,

Year	Report	Top threat		
		First	Second	Third
2016	**SANS**	Internal threat (70%)	External threat (61%)	Malware (41%)
	Wolfpack	Insider exploits (63%)	External threats; Attacks originating within the internal network; and Information security policy violations. (56% each)	

Author Compiled, Source: SANS (2016); Wolfpack (2016)

Top three perceived threats from SANS report are Internal Threat, External Threat and Malware. The reports from 2013 to 2015 have similar threats appearing in various orders each year.

The most prevalent Threats are: Internal/Insider threat, External Threat and Malware.

5.3 Network Security Device Data

Logs pertaining to multiple network security devices were obtained for a two-year period, 1 May 2014 until 30 April 2016 from a large South African state owned company, wishing to remain anonymous. The vulnerabilities were then categorised as displayed in Table 5.8. From Table 5.8 and Figure 5.10, it was noted that cross site scripting is the top vulnerability for both years with 43.5% for Year 1 and 52.7% for Year 2 and a combined Total of 46.8%. The second highest vulnerability is Information Disclosure also for both years with 30.7% for Year 1 and 13.7% for Year 2 with a combined total of 24.7% for both years. The other vulnerabilities are all below 10% each for both years.

From Table 5.1 and Figure 5.11 the total number of vulnerabilities from Year 1 to Year 2 has decreased. This could be due to patching and vulnerability management that were more effective. The percentage Cross site scripting has increased from 43.5% in Year 1 to 52.7% in Year 2, an increase of 9.2%. Information disclosure has decreased from 30.7% in Year 1 to 13.7% in Year 2, a decrease of 17%. Other vulnerabilities that have increased include Remote code execution which has increased from 3.8% in Year 1 to 7.7% in Year 2 and Privilege escalation from 6.3% in Year 1 to 8.4% in Year 2.

Table 5.8: Vulnerability categorised

Vulnerability	Year 1		Year 2		TOTAL	
	No	%	No	%	No	%
Code Injection	779	2.7%	611	3.9%	**1,390**	**3.1%**
Cross site scripting	12,425	43.5%	8,248	52.7%	**20,673**	**46.8%**
Denial of Service	127	0.4%	61	0.4%	**188**	**0.4%**
Info Disclosure	8,772	30.7%	2,148	13.7%	**10,920**	**24.7%**
Memory corruption/buffer overflow	34	0.1%	29	0.2%	**63**	**0.1%**
Other	1,584	5.5%	682	4.4%	**2,266**	**5.1%**
Privilege escalation	1,801	6.3%	1,307	8.4%	**3,108**	**7.0%**
Remote code execution	1,081	3.8%	1,211	7.7%	**2,292**	**5.2%**
Security Bypass	1,940	6.8%	1,355	8.7%	**3,295**	**7.5%**
Grand Total	**28,543**	**100%**	**15,652**	**100%**	**44,195**	**100%**

Author Compiled, Source: Network Security Device Data

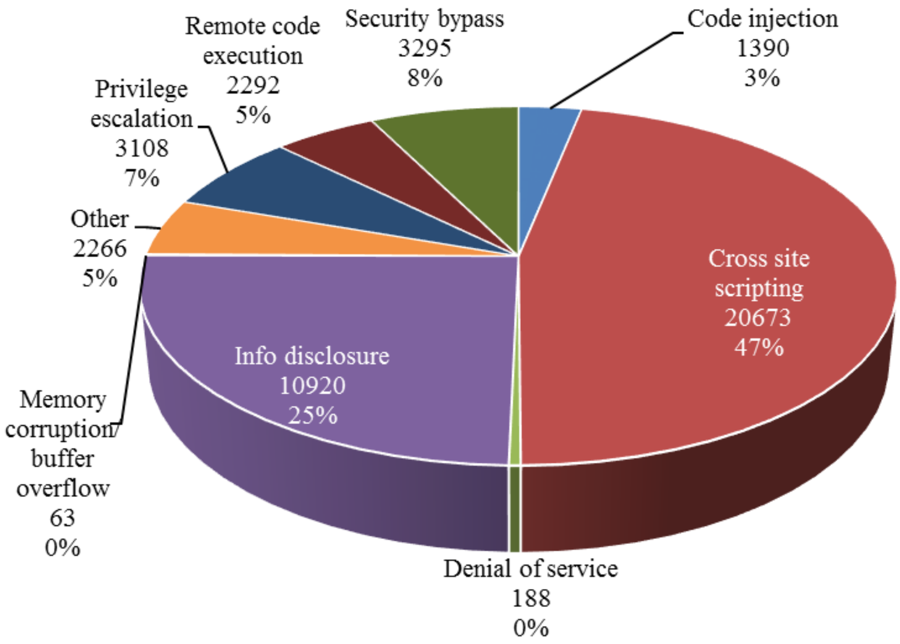


Figure 5.10: Vulnerabilities

Author Compiled, Source: Network Security Device Data

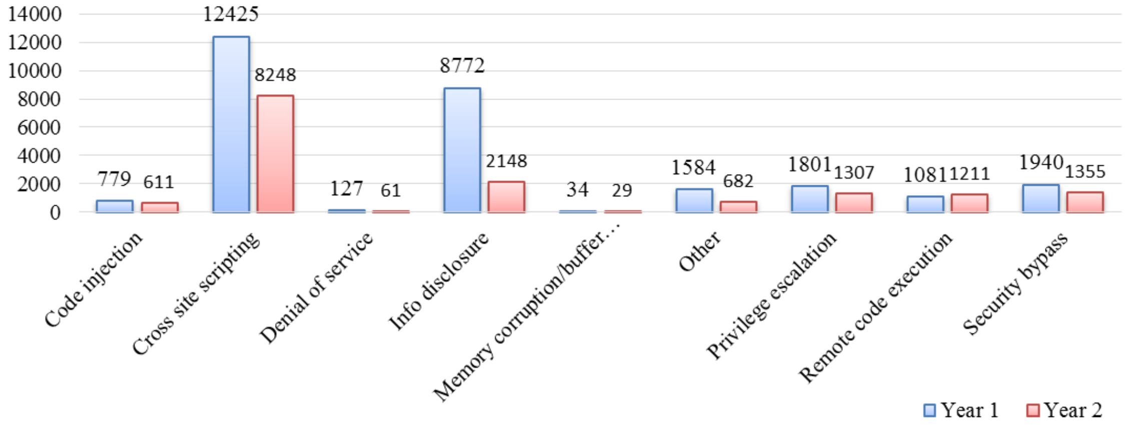


Figure 5.11: Comparison Year 1 vs Year 2

Author Compiled, Source: Network Security Device Data

5.3.1 Comparing to other reports

Table 5.9 compare the vulnerabilities from Symantec and Kaspersky to the network security device vulnerabilities. For 2014 it was noted information disclosure was the second biggest vulnerability for both Symantec and the network security device with memory corruption/buffer overflow being the top vulnerability for Symantec and cross site scripting for the network security device. Remote code execution and security bypass taking third largest vulnerability for Symantec and the network security device respectively. In 2015 it was observed security bypass being the top vulnerability from the Symantec report, while cross site scripting remained the top vulnerability for the network security device. Kaspersky reported the top vulnerability as buffer overflow, second use of hard-coded credentials and cross-site scripting. This is further discussed in Section 6.3.2.

Table 5.9: Comparing vulnerabilities

Year	Report	Top vulnerability		
		First	Second	Third
2014	**Symantec**	Memory corruption/buffer overflow	Info disclosure	Remote code
	Network security device	Cross site scripting	Info disclosure	Security bypass
2015	**Symantec**	Security bypass	Remote code	Denial of service
	Kaspersky	Buffer overflow	Use of hard-coded credentials	Cross-site scripting
	Network security device	Cross site scripting	Info disclosure	Security bypass

Adapted from: Symantec (2014, 2015), Kaspersky (2015)

5.4 Framework and Standards Comparison

This section of the study compared available frameworks, standards and international best practices related to Governance, Information security and ICS/SCADA. The sample for the document analysis was chosen by relevance. An initial document, namely COBIT was selected as it is a well-documented control framework aligned with other frameworks and divided into pre-determined categories based on Information Security controls. As more and more documents were analysed the categories expanded. Microsoft Excel were used for the coding and summarising process.

A comparison between seven control frameworks and standards that could be used to protect the ICS/SCADA environment. The following control frameworks or standards were compared:

- COBIT 5 (ISACA 2012);
- NIST SP800-82 Guide to Industrial Control Systems (ICS) Security (Stouffer *et al.* 2015);
- Good Practice Guide Process Control and SCADA Security (CPNI 2008);
- 21 Steps to Improve Cyber Security of SCADA Networks (U.S. Department of Energy 2007);

- ISO 27002:2013 Code of practice for information security controls, (ISO/IEC 2013);
- CIS 20 Critical Controls (SANS Institute 2016); and
- NERC CIP (Knapp 2011).

The standards were coded or rated as follows: red if nothing is mentioned about the control, orange if the control is briefly mentioned, yellow if the control mentioned is partially relevant to ISC/SCADA environment, i.e. the control cannot be implemented immediately and require modification to align to an ICS/SCADA environment and green is the control is relevant (i.e. no modification is required and can be implemented immediately) to an ICS/SCADA environment. Table 5.10 shows a summary of the comparisons and Figure 5.12 a graphical representation of the comparison.

Table 5.10: Comparison of Control frameworks and standards

Controls	COBIT 5	NIST SP800-82	CPNI	DOE 21 steps	ISO 27002	20 critical controls	NERC CIP
Network Architecture							
Segregation from other networks	🟥	🟩	🟩	🟩	🟨	🟩	🟨
Firewalls in place	🟨	🟩	🟩	🟩	🟨	🟩	🟨
Remote Access	🟨	🟩	🟩	🟩	🟨	🟩	🟩
Communication/encryption	🟩	🟩	🟧	🟧	🟩	🟩	🟧
Communication: Wireless and mobile	🟧	🟩	🟩	🟩	🟩	🟩	🟥
Platform Security							
Virus/malware protection	🟨	🟩	🟩	🟥	🟨	🟩	🟩
System Hardening	🟨	🟨	🟩	🟩	🟧	🟩	🟩
Patch Management	🟨	🟩	🟩	🟧	🟨	🟩	🟩
Vulnerability Management/audits	🟧	🟨	🟩	🟧	🟩	🟩	🟩
Logical Access							
User Access Management	🟨	🟩	🟩	🟧	🟨	🟨	🟨
Device Access Management	🟧	🟩	🟩	🟧	🟧	🟧	🟨
Data encryption	🟩	🟩	🟧	🟥	🟩	🟩	🟥
Password policies	🟨	🟩	🟩	🟥	🟩	🟨	🟨
Physical Controls							
Physical access control	🟩	🟩	🟩	🟧	🟩	🟩	🟩
Environmental Standards	🟩	🟩	🟩	🟥	🟩	🟥	🟥
Configuration							
System Change Control	🟩	🟩	🟩	🟧	🟩	🟩	🟩
Configuration Management	🟩	🟩	🟨	🟩	🟧	🟩	🟩
BCM							
Backup and recovery	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Redundancy/resilient infrastructure	🟨	🟨	🟩	🟥	🟩	🟩	🟧
Business Continuity and Disaster Recovery Plans	🟩	🟩	🟩	🟩	🟩	🟥	🟩

Controls	COBIT 5	NIST SP800-82	CPNI	DOE 21 steps	ISO 27002	20 critical controls	NERC CIP
Monitoring							
Audit logs	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Incident response	🟨	🟩	🟩	🟩	🟩	🟩	🟩
SIEM/Security Intelligence Centre	🟧	🟩	🟩	🟩	🟨	🟩	🟩
Governance							
Strategy of ICS/SCADA	🟩	🟨	🟨	🟧	🟩	🟥	🟥
Policies, Procedures, Standards, and Frameworks	🟩	🟨	🟩	🟩	🟩	🟧	🟥
User awareness training	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Project Management	🟩	🟨	🟩	🟥	🟥	🟥	🟥
Risk Management	🟩	🟩	🟩	🟩	🟩	🟧	🟧
3rd Party and vendor management							
3rd party management	🟩	🟨	🟩	🟥	🟩	🟧	🟥
Vendor Management	🟩	🟨	🟩	🟥	🟩	🟥	🟧
3rd party remote access	🟧	🟨	🟩	🟧	🟥	🟩	🟥

Legend	No mention	🟥	Briefly mention	🟧	Partially relevant	🟨	Relevant to ICS/ SCADA	🟩

Source: Author compiled

In order to represent the above table on a graph, the legend was rated and the sub categories was averaged as follows:

- Red/No mention to 0;
- Orange/Briefly mentioned to 1;
- Yellow/Partially relevant to 2; and
- Green/Relevant to ICS/SCADA to 3.

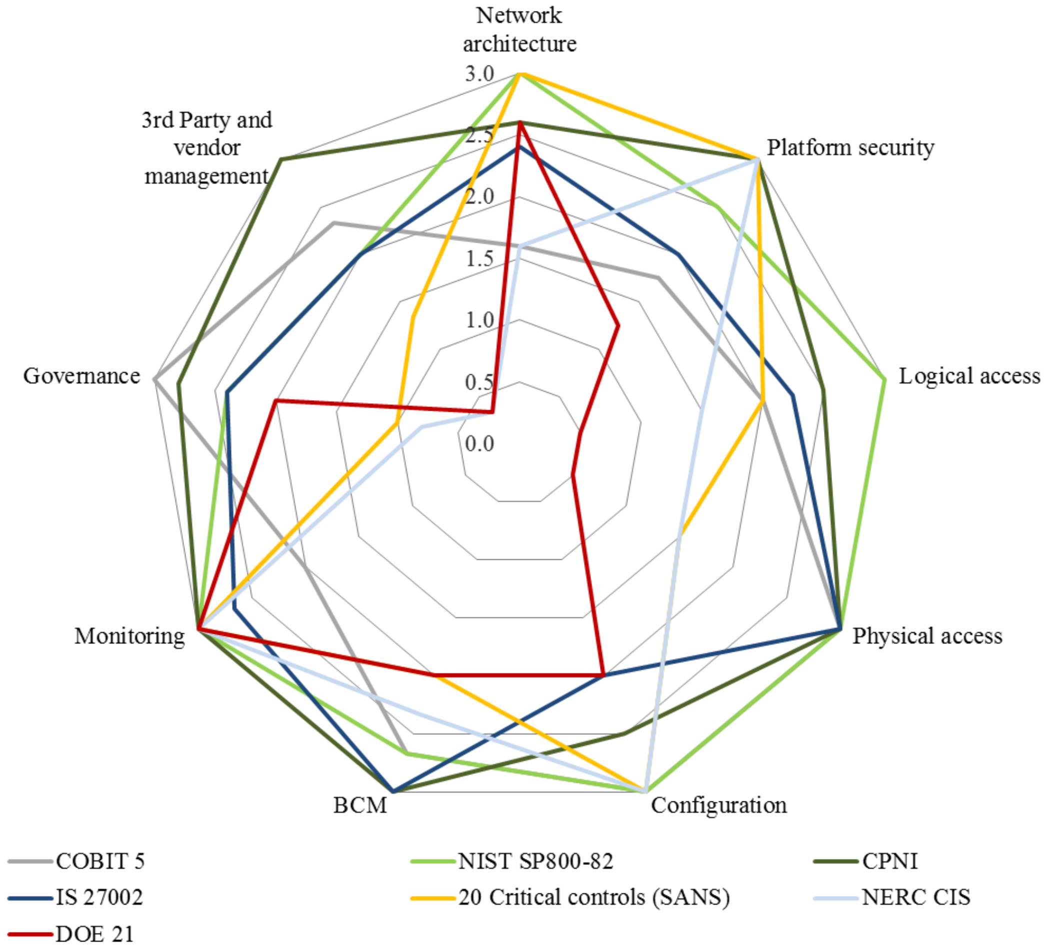


Figure 5.12: Graphical representation of the comparison of Control frameworks and standards

Source: Author compiled

From Table 5.10 and Figure 5.12 it was noted the CPNI framework is best suited overall as it covers all the security areas, secondly the NIST SP800-82 and then the ISO27001/2 series. The DOE 21 steps are the worst suited as it is lacking in a couple of areas, including Platform security, Logical access, Physical security and 3rd party and vendor management. From a governance perspective the COBIT framework (ISACA, 2012) is the best suited as it covers the governance areas substantially. The NERC CIS and SANS's 20 Critical controls are the worst suited in terms of Governance as it fails to cover areas such as Strategy, Policies, standards, Project and Risk Management.

5.5 Default passwords

We noted in Section 2.2.1.4 the security concerns for ICS/SCADA from a password perspective. The list of default passwords from SCADA Strangelove (2015), was obtained and summarised. There are around 234 known ICS/SCADA default passwords. The results were summarised by device type and are displayed in Figure 5.13. It was noted that network devices and PLCs contained the majority of the default passwords.

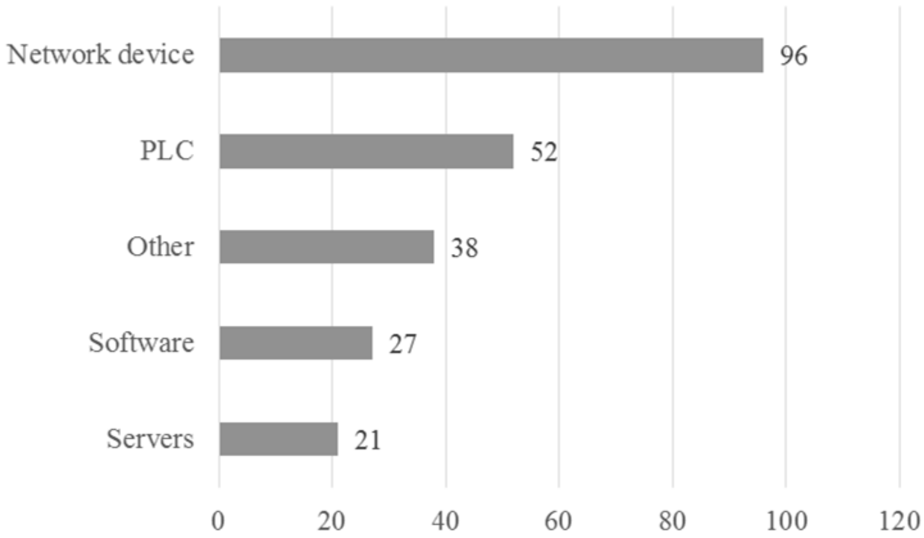


Figure 5.13: ICS/SCADA Device type with known default passwords

Adapted from: SCADA Strangelove (2015)

The ICS/SCADA vendors with the most known default passwords are Schneider Electric with 24, Siemens with 22 and Emerson with 21. Table 5.11 gives a summary of the vendors and know default passwords.

Table 5.11: ICS/SCADA Vendor with known default passwords

Vendor	No of known default passwords
Schneider Electric	24
Siemens	22
Emerson	21
Moxa	16
Rockwell Automation/Allen-Bradley	15
Tecomat	10
Wago	10
Wonderware	10
Others	106
Total	**234**

Adapted from: SCADA Strangelove (2015)

It was noted from the analysis the type of account that was listed. Although it was not possible to determine what type of accounts some of the default passwords and accounts were, it is evident that around 85% of the accounts belonged to an administrator type of account as displayed in Figure 5.14. This would provide the user of that account full access to the ICS/SCADA system/device.

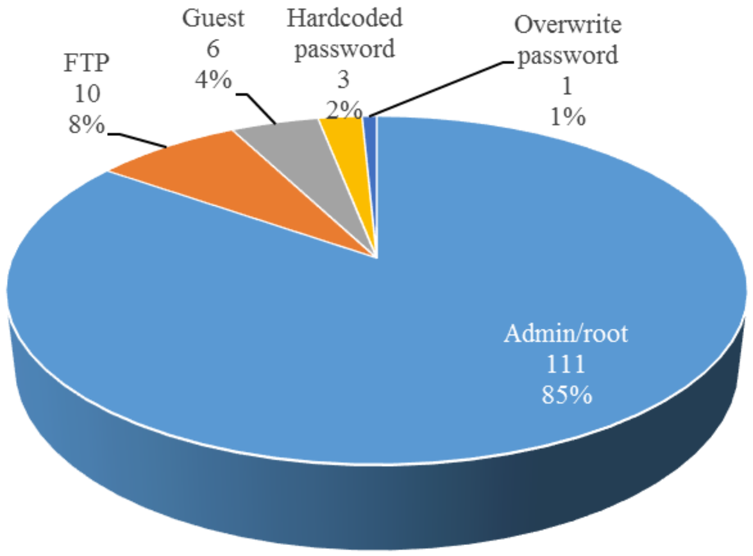


Figure 5.14: ICS/SCADA Account type with known default passwords

Adapted from: SCADA Strangelove (2015)

It can be concluded that the most common known default password would be a Network device from the Vendors, Schneider Electric, Siemens or Emerson, which would have administrator type access. This would make these the most vulnerable devices in the ICS/SCADA environment should the default password not have been changed.

5.6 Shodan

Project SHINE (2014) released a report in 2014 that contained information of ICS/SCADA devices that are directly connected to the Internet. This was partly replicated, but made specific for South Africa. From Section 2.3.1.2, the five most common protocols and ports are Modbus (Port 502), Siemens/ICCP (Port 102), DNP3 (Port 20000), Ethernet/IP (Port 44818) and BACNet (Port 47808).

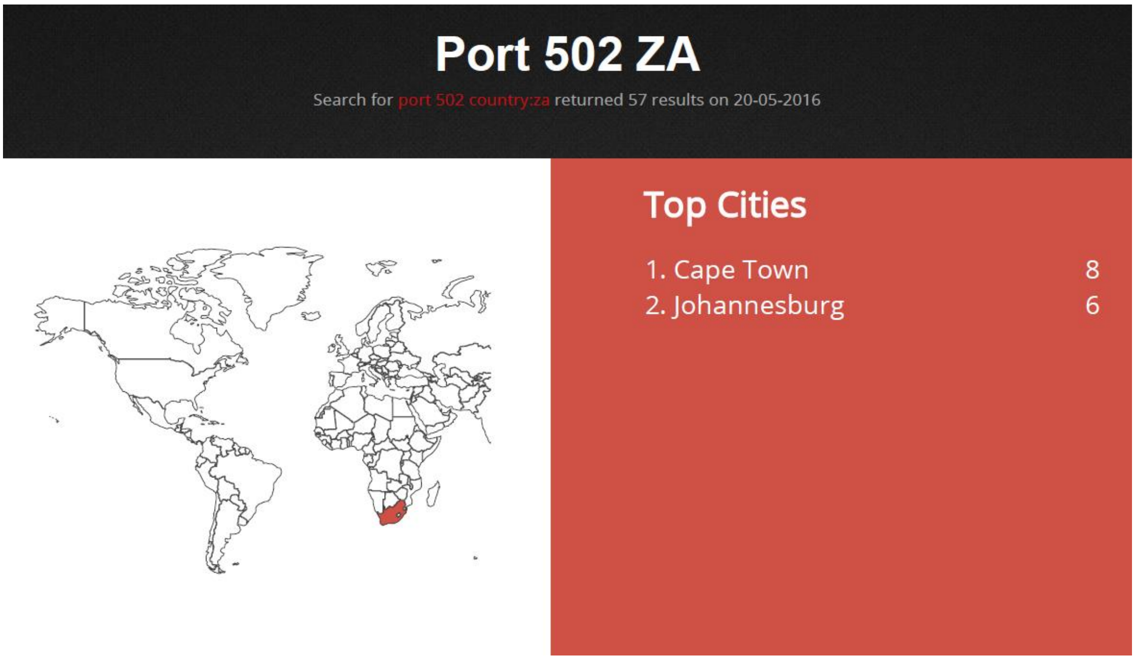
The open source search engine, Shodan (www.shodan.io), was used to search for these protocols and port in order to determine the number of ICS/SCADA devices in South Africa are exposed to the internet. There were 2,213 ICS/SCADA devices in South Africa exposed to the internet. Table 5.12 gives a summary of the results and Figure 5.15 to Figure 5.19 the results from the Shodan searches.

The 2,213 ICS/SCADA devices in South Africa that are exposed to the internet poses a huge risk. This means they are easy accessible to hackers and do not have effective controls in place, such as segregation of ICS/SCADA via a well configured firewall.

Table 5.12: List of ICS/SCADA device exposed to the internet

Protocol	Port	Description	No of ICS/SCADA in South Africa exposed to the internet
Modbus	Port 502	Modbus is commonly used for communication between PLCs and HMIs	57
Siemens/ICCP	Port 102	The ICCP is a protocol used for communication between control centers within the energy industry	6
DNP3	Port 20000	DNP3 us mainly used for communication between master control stations and remote or slave devices	2,097
Ethernet/IP	Port 44818	Ethernet/IP is used in most industries including automotive, manufacturing	39
BACNet	Port 47808	BACNet is a protocol used for communication in building automation.	14
TOTAL			**2,213**

Source: Author Compiled



Port 502 ZA

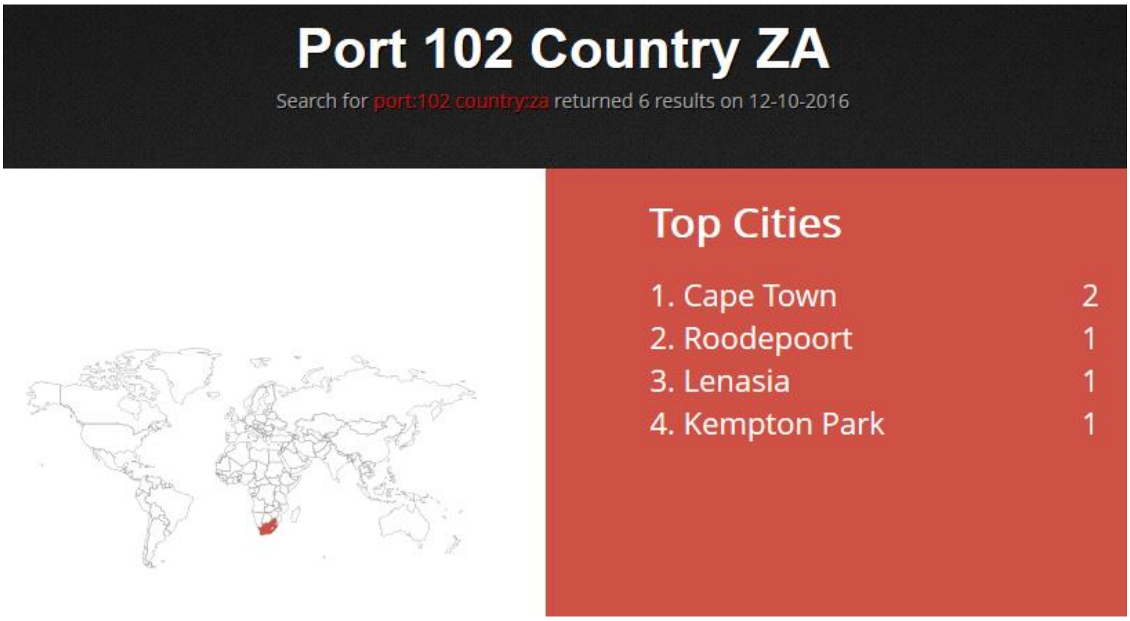
Search for port 502 country:za returned 57 results on 20-05-2016

Top Cities

1. Cape Town	8
2. Johannesburg	6

Figure 5.15: Shodan results for Port 502

Source: Shodan



Port 102 Country ZA

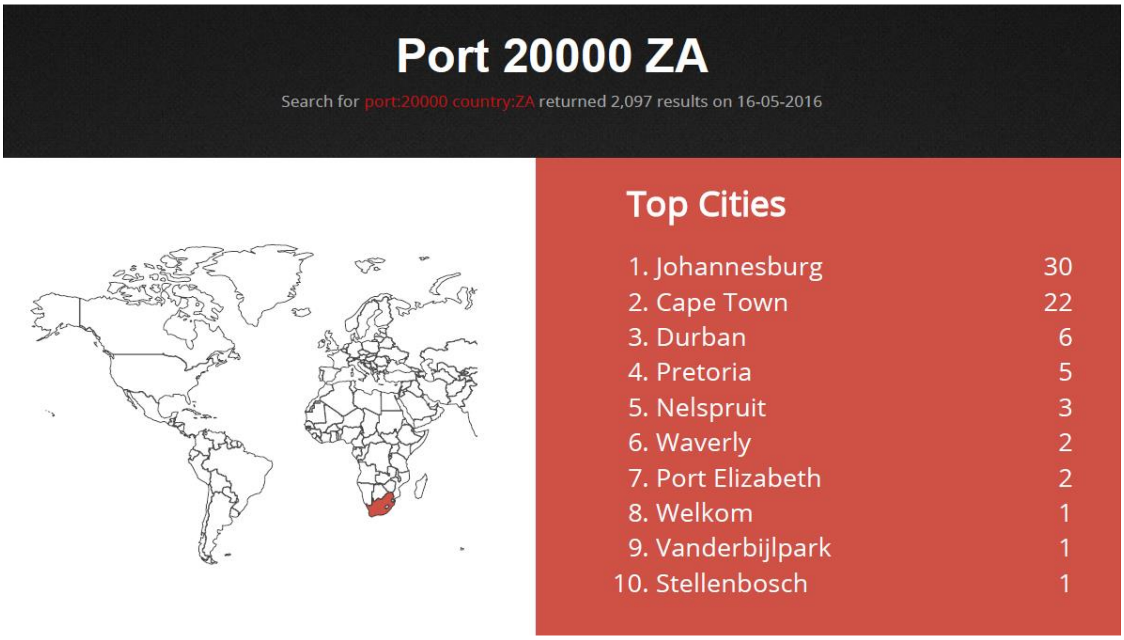
Search for port:102 country:za returned 6 results on 12-10-2016

Top Cities

1. Cape Town	2
2. Roodepoort	1
3. Lenasia	1
4. Kempton Park	1

Figure 5.16: Shodan results for Port 102

Source: Shodan



Port 20000 ZA

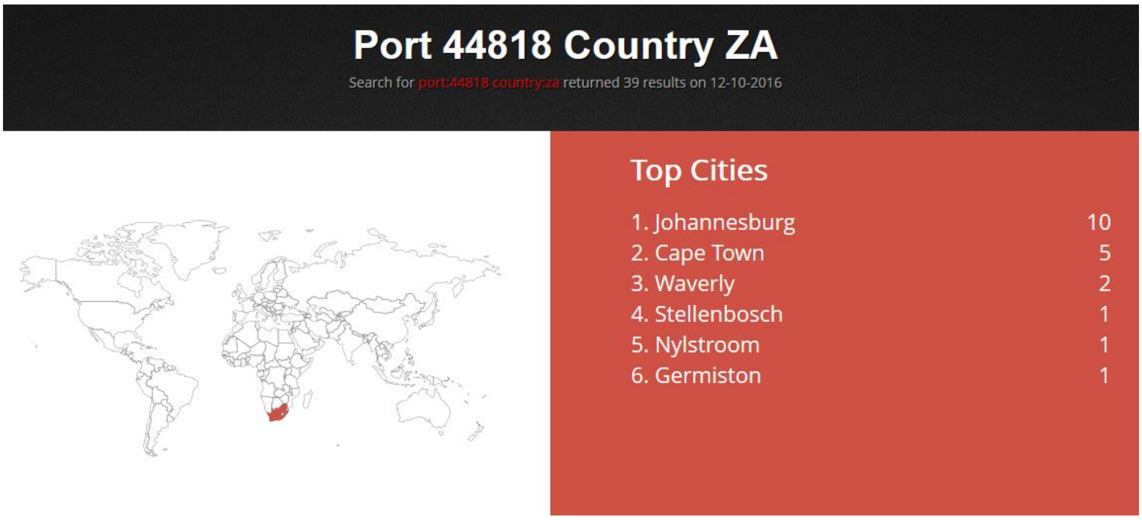
Search for port:20000 country:ZA returned 2,097 results on 16-05-2016

Top Cities

1. Johannesburg	30
2. Cape Town	22
3. Durban	6
4. Pretoria	5
5. Nelspruit	3
6. Waverly	2
7. Port Elizabeth	2
8. Welkom	1
9. Vanderbijlpark	1
10. Stellenbosch	1

Figure 5.17: Shodan results for Port 20000

Source: Shodan



Port 44818 Country ZA

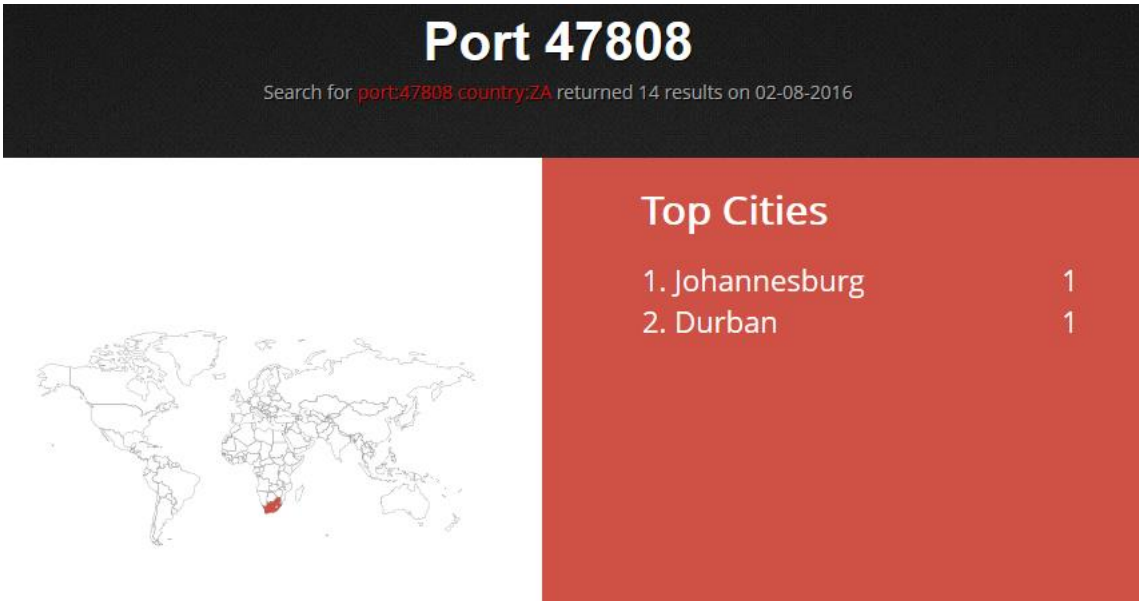
Search for port:44818 country:za returned 39 results on 12-10-2016

Top Cities

1. Johannesburg	10
2. Cape Town	5
3. Waverly	2
4. Stellenbosch	1
5. Nylstroom	1
6. Germiston	1

Figure 5.18: Shodan results for Port 44818

Source: Shodan



Port 47808

Search for port:47808 country:ZA returned 14 results on 02-08-2016

Top Cities

1. Johannesburg	1
2. Durban	1

Figure 5.19: Shodan results for Port 47808

5.7 Summary

The document analysis was conducted on alert reports and trends based on international studies as well as one local study relevant to South Africa. There is consistency across all sets of analysis and results showing high levels of confidence. From the document analysis, it was observed that the most prevalent vulnerabilities are Security Bypass, Remote code execution and Buffer Overflow while the most prevalent Threats are: Internal/Insider threat, External Threat and Malware. The top sectors where incidents occurred were the Energy Sector and Critical Manufacturing Sector.

Comparing international best practices, it was determined that the CPNI framework is best suited overall as it covers all the security areas, and the COBIT framework is the best suited from a governance perspective.

The most common known default password would be a Network device from the Vendors, Schneider Electric, Siemens or Emerson, which would have administrator type access. This would make these the most vulnerable devices in the ICS/SCADA environment should the default password not have been changed. It was noted that 2,213 ICS/SCADA devices in South Africa that are exposed to the internet. These do not have effective controls in place, such as segregation of ICS/SCADA via a well configured firewall.

The next chapter discusses the results from the survey and the document analysis and link them back to the study’s objectives to draw meaningful outcomes.

Chapter 6 Discussion

6.1 Introduction

Chapter 4 presented the results and outcomes of the online survey and Chapter 5 the findings from document analysis. This chapter revisits the study's objectives and discusses the findings and results per research objective. The results are also triangulated and discussed in line with the results from the document analysis in order to draw meaningful implications and comparisons to international studies. Figure 6.1 is a graphical representation of the outline of this chapter and overall structure. The research objectives are listed in Table 6.1 and the study's outcomes in line with each objective follow.

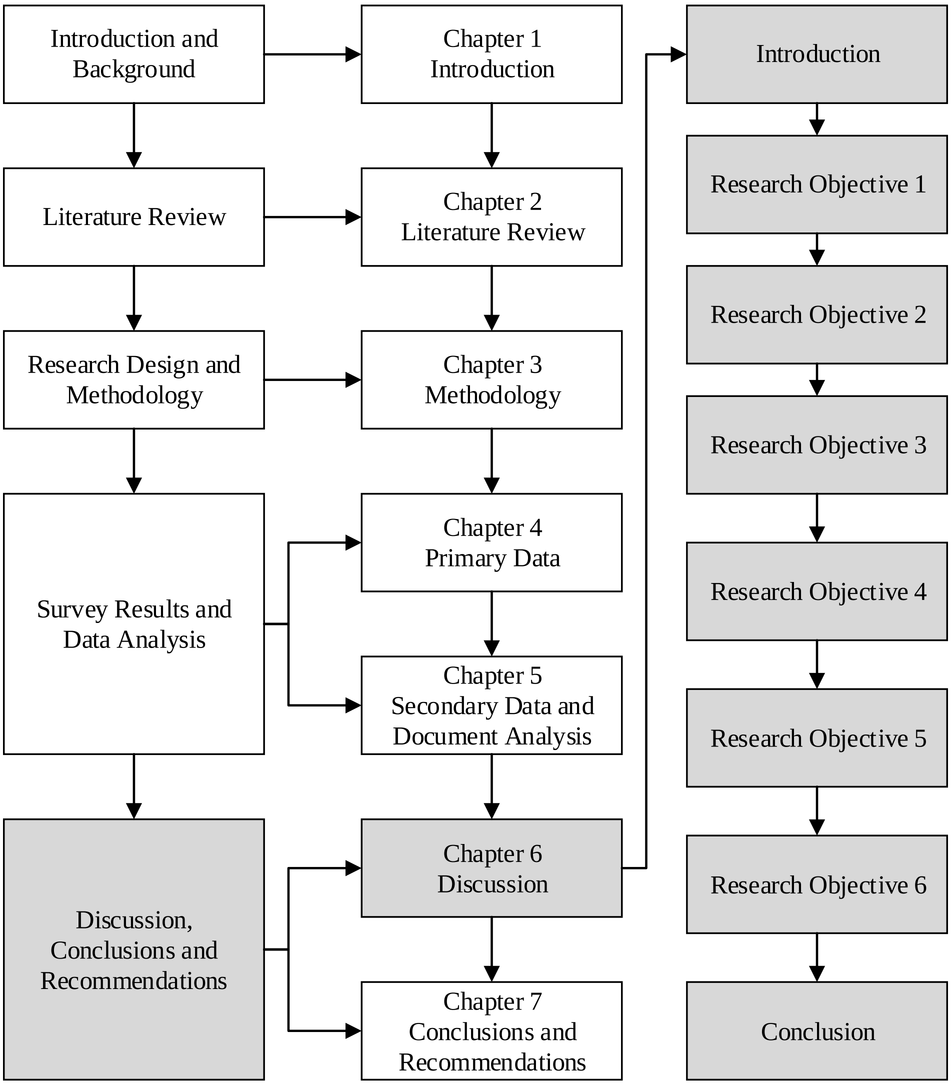

Introduction and Background
Chapter 1 Introduction
Introduction
Literature Review
Chapter 2 Literature Review
Research Objective 1
Research Objective 2
Research Design and Methodology
Chapter 3 Methodology
Research Objective 3
Survey Results and Data Analysis
Chapter 4 Primary Data
Research Objective 4
Chapter 5 Secondary Data and Document Analysis
Research Objective 5
Discussion, Conclusions and Recommendations
Chapter 6 Discussion
Research Objective 6
Chapter 7 Conclusions and Recommendations
Conclusion

Figure 6.1: Graphical representation of Chapter 6 outline

Table 6.1: Summary of Research objectives

	Research objective	Section
RO1	To determine the factors (vulnerabilities and threats) influencing ICS security in South Africa	**6.2**
RO2	To determine what the best mitigating controls to govern and secure ICS/SCADA systems in South Africa are.	**6.3**
RO3	To determine the impact of non-governed ICS	**6.4**
RO4	To determine how ICS in South Africa are secured and governed	**6.5**
RO5	To establish if the confidence levels of implemented controls/measures mitigating the threats and risks are sufficient	**6.6**
RO6	To develop a control framework addressing the shortfalls for ICS security in South Africa	**6.7**

6.2 Research Objective 1 – To determine the factors (vulnerabilities and threats) influencing ICS security in South Africa

This objective aimed to determine the factors (vulnerabilities and threats) influencing ICS security in South Africa. Results from the survey, document analysis, and network device analysis are discussed in the section below.

6.2.1 Vulnerabilities

It was noted in Section 4.3.5 from the questionnaire that the top three vulnerabilities related to ICS/SCADA systems are *outdated or unpatched systems*, *no or limited monitoring*, and *access control (no or weak passwords),* all three listed as a medium vulnerability.

Looking at technical vulnerabilities, in Section 5.3 from the network security device data, it was evident that *cross site scripting* is the top vulnerability, second highest vulnerability is *information disclosure* and third *security bypass*. These technical vulnerabilities take priority above the perceived vulnerabilities as they are actual measured data.

From the document analysis in Section 5.2.6.1, it was evident that the most prevalent vulnerabilities are *security bypass*, *remote code execution* and *buffer overflow*. Others include *denial of service*, *use of hard-coded credentials* and *cross-site scripting*.

The document analysis was conducted on reports based on international studies as well as one local study relevant to South Africa. The document analysis found *security bypass* as the prevalent vulnerability, as discussed in Section 5.2.6.1 while from the network security device in South Africa it was found as the third highest vulnerability. *Cross site scripting* is the highest vulnerability from the network security device in South Africa while internationally it is in the Top 6. *Cross-site scripting* vulnerability may be used by attackers to bypass access controls, the categorisation of the international reports could list a *cross-site scripting* vulnerability under *security bypass*.

There is a challenge that each report categorise the vulnerabilities differently. This might have a small implication on the study as there are no consistency between categories and this could lead to some bias towards certain vulnerabilities and threats. Also this might impact someone in the industry when trying to use various reports to determine the top vulnerabilities and could wrongly place emphasis on controls for vulnerabilities that are not really the most prevalent.

It was also noted that *no or weak passwords*, as listed by the respondents, as the third highest vulnerability coincide with the third highest vulnerability found from the analysis of the network security devices. With *outdated or unpatched systems* and *no or limited monitoring* being the top two vulnerabilities as indicated by the respondents, there are big gaps in terms of securing and having an overview of vulnerabilities for ICS/SCADA in South Africa.

From the document analysis in Section 5.5, it was determined that there are at least 234 known ICS/SCADA default passwords with most having privilege access in the form of administrator or root accounts. This strengthens and align with the third highest vulnerability of *no or weak passwords* from the survey and third highest vulnerability from the document analysis on the network security devices.

It was determined from the analysis in Section 5.6 that a number of ICS/SCADA devices in South Africa are exposed to the internet. At least 2,213 ICS/SCADA devices in South Africa are exposed to the internet and poses as a huge risk. The implication is that they are easy accessible to hackers as these ICS/SCADA device do not have effective controls in place. There is a lack of appropriate segregation of ICS/SCADA networks and IT or corporate networks via a well configured firewall leaving them exposed and easily accessible via the internet.

The vulnerability factors influencing ICS/SCADA in South Africa are *outdated or unpatched systems*, *no or limited monitoring* and *access control* while the technical vulnerabilities are *security bypass*, *cross-site scripting* and *remote code execution*.

6.2.2 Threats

The results in Section 4.3.2 illustrated that the top three threats likely to occur are:

1. *Malware* (medium - expected to occur in some circumstances),
2. *Staff undertaking unintentional unauthorised actions* (leaning towards medium - expected to occur in some circumstances) and
3. *Disgruntled staff* (intentional) (also leaning towards medium - expected to occur in some circumstances).

This was triangulated to the question in Section 4.3.3 as the respondents listed the top 3 threats as: *Staff undertaking unintentional unauthorised actions* (e.g. making changes without following change control process) which 67% of the respondents selected, *malware* (worms/viruses/Trojans/spyware) 63% and *disgruntled staff* (intentional) 48%.

From the document analysis of SANS report in Section 5.2.3 it was noted that the top three perceived threats from an international perspective are *internal threat, external threat* and *malware*. This relates to the top threats selected by the respondents in Section 4.3.2 and 4.3.3. Internal threats can be directly linked to *staff undertaking unintentional unauthorised action* as well as *disgruntled staff*, and *malware* remained in the top three.

From a local perspective, from the Wolfpack report discussed in Section 5.2.5, it was evident the Top threats are: *Insider exploits*, and combined secondly, *external threats*, *attacks originating within the internal network* and *information security policy violations*. *Malware* was in the top 5. This also relates to the top threats selected by the respondents in Section 4.3.2 and 4.3.3. *Internal threats* and *information security policy violation* can be directly linked to *staff undertaking unintentional unauthorised action* as well as *disgruntled staff* while *malware* remained the in the top three. Apart from *malware*, the results are consistent between the local survey conducted by Wolfpack and this study. The survey performed by Wolfpack might have targeted a different audience which perceived *malware* as top 5 threat and not top 3. This is a small deviation and no material impact on the results.

This suggests that from both an international and local perspective the threats are similar and the following three threats are perceived as the Top threats: *staff undertaking unintentional unauthorised actions*, *disgruntled staff* and *malware*. There is consistency across all sets of analysis and results showing high levels of confidence.

6.2.3 Risks

As discussed in Section 3.4, risk is defined as impact times probability/likelihood (Boehm, 1991). The probability/likelihood of threat vs the impact of threat was plotted in Figure 6.2.

The top three risks to ICS/SCADA environment are:

- *Malware*
- *Staff undertaking unintentional unauthorised actions and*
- *Disgruntled staff*

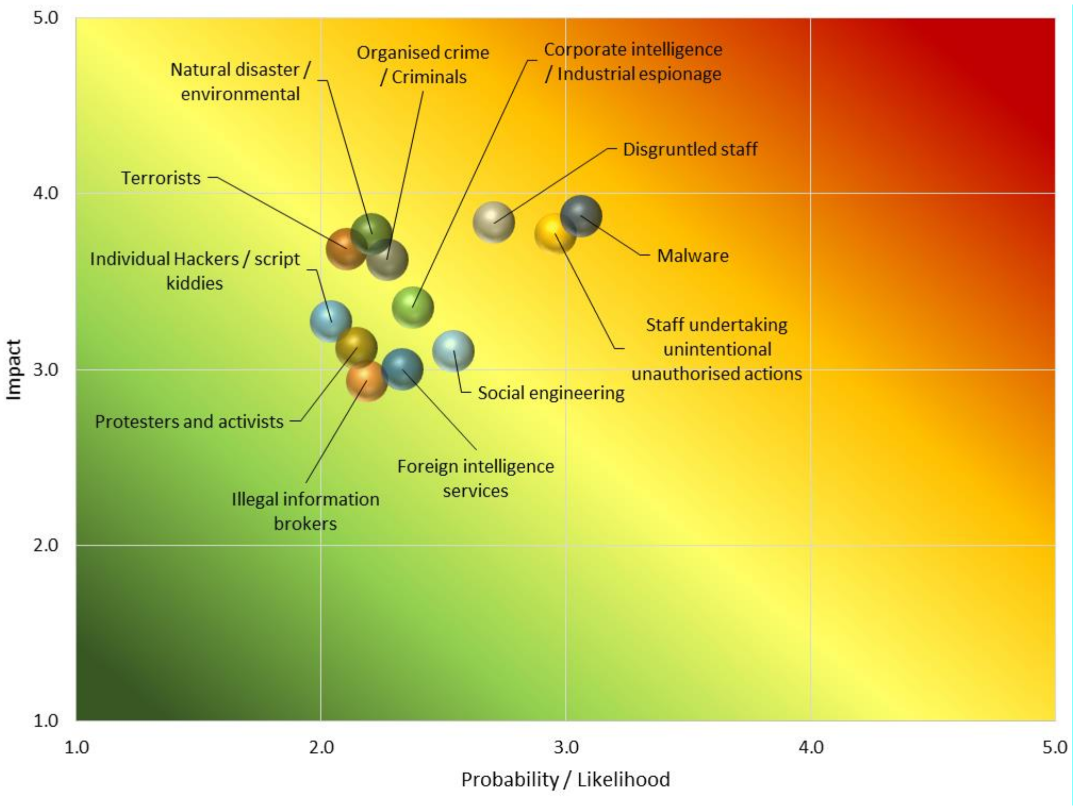


Figure 6.2: Risk (Impact vs Probability/Likelihood)

Source: Author compilation

This aligns to the threats discussed in Section 6.2.2 and strengthen consistency across all sets of analysis and results showing high levels of confidence.

6.2.4 Summary

There are three factors influencing ICS/SCADA in South Africa. They are vulnerabilities, technical vulnerabilities and threats. The vulnerability factor influencing ICS/SCADA in South Africa are *outdated or unpatched systems*, *no or limited monitoring* and *access control* while the technical vulnerabilities are *security bypass*, *cross-site scripting* and *remote code execution*. A number of ICS/SCADA devices are exposed to the internet indicating that there is a lack of appropriate controls to effectively segregate the ICS/SCADA network from IT or corporate network. The threat factor influencing ICS/SCADA in South Africa are *staff undertaking unintentional unauthorised actions*, d*isgruntled staff* and *malware*. These factors could potentially influence the availability of ICS/SCADA systems by causing distribution to operations and the business and ultimately financial loss. There is also a bigger risk if these factors influence the operation of ICS/SCADA systems whereby human life could be at stake.

6.3 Research Objective 2 – To determine what the best mitigating controls to govern and secure ICS/SCADA systems in South Africa are.

In order to determine the best mitigating controls to govern and secure ICS/SCADA systems, the vulnerabilities and threat related to ICS/SCADA needs to be taken into account. The controls should be implemented based on vulnerability and threat priority. Control preference should be given to these technical vulnerabilities as these were detected and not perceived as in the case of the top perceived vulnerabilities and threats.

6.3.1 Controls for vulnerabilities and threats

The results in Section 4.3.6 from the questionnaire illustrated that the top three controls mitigating vulnerabilities in the ICS/SCADA environments are *configuration* (default configuration, no backup of configuration), *physical security* and *network perimeter* (Unsecure, firewall does not exist/misconfigured, direct connections to internet) of which the average of responses all indicated these controls were *partially implemented/in progress*, but leaning strongly towards *implemented control requires improvement*.

It was also noted the bottom three controls mitigating vulnerabilities in the ICS/SCADA environments as selected by respondents in the questionnaire are: *monitoring*, *patching* and *wireless connections* all *partially Implemented/in progress* as indicated by the respondents.

Looking at the vulnerabilities discussed in Section 6.2.1, the top three vulnerabilities related to ICS/SCADA systems are *patching* (outdated/unpatched), *monitoring* (no or limited), and a*ccess control* (no or weak password). The controls to govern or mitigate the vulnerability for *outdated/unpatched* is by implementing *patching control*, which are neither top or bottom three, but the respondents indicated that *patching control* is *partially implemented/in progress*.

Similarly, for the vulnerability in *no or limited monitoring*, the control to govern or mitigate it is to implement a *monitoring control*, which are the bottom control implemented as respondents indicated this is *partially implemented/in progress*. The third top vulnerability is in *access control* (No or weak password), and the control to govern or mitigate is to implement effective *access controls* like passwords and user account management. This control is neither top nor bottom three, but the respondents indicated that *access control* is *partially implemented/in progress*, but leaning strongly towards *implemented control requires improvement*.

Although this is a slightly lesser risk than the other two top vulnerabilities, this is still a risk as the control should be *implemented and operating effectively* in order to successfully govern or mitigate the vulnerability. This shows a clear gap in governing/mitigation of all three the top vulnerabilities.

Table 6.2 show a summary of Top vulnerabilities and the status of controls.

Table 6.2: Summary of Top vulnerabilities and status of relevant controls

Top vulnerability	Control to mitigate	Status of controls
Patching - outdated/unpatched	Patching control	Partially implemented/in progress
Monitoring – no or limited	Monitoring control	Partially implemented/in progress
Access control - no or weak password	Access control	Partially implemented/in progress, but leaning strongly towards implemented control requires improvement

The best mitigating controls to govern and secure the top perceived vulnerabilities for ICS/SCADA systems in South Africa are to *patch* ICS/SCADA systems, to *monitor* them and to ensure appropriate *access control* in the form of user account management is in place.

From the discussion in Section 6.2.2 it was noted that the threat factor influencing ICS/SCADA in South Africa are *staff undertaking unintentional unauthorised actions*, *disgruntled staff* and *malware*. In order to adequately mitigate these, effective *access control* and *anti-virus* software needs to be implemented.

6.3.2 Controls for technical vulnerabilities

It was evident from the network security device data in Section 5.3 that the top three technical vulnerabilities are *cross site scripting*, being the top vulnerability, second highest vulnerability is *information disclosure* and third *security bypass*.

The controls to govern or mitigate the technical vulnerability for *cross site scripting* and *information disclosure* is *configuration management*, which are the top control implemented as indicated by the respondents. They indicated that the *configuration control* was leaning very strongly towards the category of *Implemented control requires improvement*. Although the focus is on mitigating the technical vulnerabilities, the implemented control was still not at optimum level, which were *implemented and operating effectively*.

Similar for the technical vulnerability, *security bypass*, the control to govern or mitigate it is to implement effective *access controls* such as *passwords* and *user account management*. This control is neither top nor bottom three, but the respondents indicated that *access control* is *partially implemented/in progress*, but leaning strongly towards i*mplemented control requires improvement*.

Although all three of these technical vulnerabilities have a slightly less risk than the other vulnerabilities mentioned in Section 6.3.1, there are still a risk as the controls should be *implemented and operating effectively* in order to successfully govern or mitigate the vulnerabilities. This shows a clear risk in governing and mitigation of all three the top vulnerabilities.

Below is a summary of the technical vulnerabilities and the status of controls:

Table 6.3: Summary of Top technical vulnerabilities and status of relevant controls

Top Technical vulnerability	Control to mitigate	Status of controls
Cross site scripting	Configuration	Leaning strongly towards *implemented control requires improvement*
Information disclosure	Configuration	Leaning strongly towards i*mplemented control requires improvement*
Security bypass	Access control	*Partially implemented/in progress,* but leaning strongly towards i*mplemented control requires improvement*

From the document analysis in Section 5.2.6.1, the international reports indicated that the most prevalent vulnerabilities are *security bypass*, *remote code execution* and *buffer overflow*. Others include *denial of service, use of hard-coded credentials* and *cross-site scripting*.

As noted above, *security bypass*, requires *access controls* such as passwords and user account management, to govern or mitigate it. This control is neither top nor bottom three, but the respondents indicated that *access control* is *partially implemented/in progress*, but leaning strongly towards *implemented control requires improvement*. For the technical vulnerability *remote code execution,* the control*, remote access* is neither top nor bottom three, but the respondents indicated that *remote access control* is *partially implemented/in progress*.

The third top technical vulnerability, *memory corruption/buffer overflow* requires effective *configuration management*, which although is the top control implemented, the implemented control is still not at optimum level, which are *implemented and operating effectively*. Respondents indicated that *configuration control* is leaning very strongly towards the category of *implemented control requires improvement*. This shows a clear gap in governing/mitigation of all three the top international technical vulnerabilities.

Table 6.4 provides a summary of the most prevalent international technical vulnerabilities from the document analysis with the status of controls.

Table 6.4: Summary of Top international technical vulnerabilities and status of relevant controls

Top Technical vulnerability	Control to mitigate	Status of controls
Security bypass	Access control	*Partially implemented/in progress,* but leaning strongly towards *implemented control requires improvement*
Remote code execution	Remote access	*Partially implemented/in progress*
Memory corruption/buffer overflow	Configuration	*Partially implemented/in progress,* but leaning strongly towards *implemented control requires improvement*

The focus is wrongly placed on the implementation of *physical security* and *network perimeter* controls. These controls do not however address the technical vulnerabilities in *security bypass*, being the third top vulnerability from the local network security device, and the top technical vulnerability from an international perspective. The focus should also be on the other top two international technical vulnerably (*remote code execution* and *memory corruption/buffer overflow*) as they might come or become relevant to South Africa at a later stage.

From Section 4.6.5 it was noted that the Top 3 priorities when it comes to implementing effective controls for the security of ICS/SCADA systems are: *Preventing control system service interruption*, *preventing financial loss/protecting shareholder value* and *protecting health and safety of employees*. The top threats and vulnerabilities discussed will cause *system service interruption* and possible *financial loss*, thus strengthening the need to shift the focus towards mitigating the top threats and vulnerabilities as a priority.

6.3.3 Summary

The state of ICS/SCADA is one of ungoverned and unsecure systems. The best mitigating controls to govern and secure the top perceived vulnerabilities and threats for ICS/SCADA systems in South Africa are to *patch* ICS/SCADA systems, to *monitor* them and to ensure appropriate *access control* in the form of user account management is in place as well as appropriate *anti-virus software*.

The best mitigating controls to govern and secure the technical vulnerabilities are the implementation of appropriate *access control*, implementation of appropriate and secure *configuration* as well as implementing controls to govern and secure *remote access*. Preference is given to these technical vulnerabilities as these were detected and not perceived as in the case of the top perceived vulnerabilities and threats.

6.4 Research Objective 3 – To determine the impact of non-governed ICS.

In Section 4.3.4 it was observed that the top three threats likely to impact ICS/SCADA systems are *malware* which had a *medium* impact – e.g. some service disruption, but also leaning towards *high* impact – e.g. service disruption), second *disgruntled staff* (intentional) also *medium* impact (expected to occur in some circumstances, but also leaning towards *high* impact – e.g. service disruption), and *staff undertaking unintentional unauthorised actions* with another *medium* impact (expected to occur in some circumstances but also leaning towards *high* impact – e.g. service disruption).

We also saw that the bottom three threats likely to have less impact on ICS/SCADA systems should they occur are: *illegal information brokers*, *foreign intelligence services* and *social engineering* (phishing emails etc.) all leaning strongly towards *low* (Expected to occur in a few circumstances).

In Section 4.4 it was indicated top three impacts of non-governed ICS/SCADA environments should threats and vulnerabilities materialise, are *loss of availability/denial of service*, secondly *loss of* *integrity* and *unauthorised control* all having a *moderate* impact which could lead to some service disruption/potential for adverse publicity.

The author observed in Section 4.4.1 that 37% of respondents did not have a threat occurrence in their ICS/SCADA environment. It was not that 25% of respondents indicated that a threat did occur, 15% cannot disclose, 13% are not sure while 10% indicated maybe. From this it could be concluded that only 37% did not have a threat occurrence in their ICS/SCADA environment, while the remaining 63% might possibly have had a threat that occurred in their ICS/SCADA environment. From the respondents that had a threat occurring in their ICS/SCADA environment, it was noted that 42% of respondents indicated that the threat/event occurred '2 – 4' times in the past 12 months, 41% of respondents had a threat/event occurred once and 17% of respondents had a threat/event occurred '5 – 10' times in the past month.

The top perceived threats and vulnerabilities is expected to *occur in some circumstances* and potentially *lead to loss of availability* or *denial of service*, *loss of integrity* and *unauthorised control*. This impact could cause some *service disruption* or potential for *adverse publicity*.

6.4.1 Summary

The impact of non-governed or unsecure ICS/SCADA is *loss of availability* or *denial of service*. The top perceived threats and vulnerabilities could potentially lead to *service disruption* which could cause *distribution to operations* and the business and ultimately lead to *financial loss*. There is also a bigger risk if these factors influence the operation of ICS/SCADA systems whereby *human life* could be at stake. This could also have a potential for *adverse publicity*.

6.5 Research Objective 4 – To determine how ICS in South Africa are secured and governed

In Section 4.5.1 it was noted that the majority of the respondents (69%) have *control frameworks in place*. 17% of respondents indicated that ICS/SCADA is *regulatory monitored*, 8% were *unsure* how ICS/SCADA systems are secured and governed, 4% indicated that ICS/SCADA systems are *not governed* while 2% indicated other.

The effectiveness of controls is discussed in more detail in Section 6.6.1 and indicate the implementation levels of controls which also have an influence on how ICS/SCADA systems are secured and governed.

We also saw in Section 4.5.2 that the top three frameworks used by the respondents to govern and secure their ICS/SCADA environments are COBIT, ITIL and the ISO 27001 series. The three frameworks that are used the least by the respondents to govern and secure their ICS/SCADA environments are ISA99, ENISA and CPNI.

From the document analysis in section 5.4 it was observed that the CPNI framework is best suited overall as it covers all the security areas, secondly the NIST SP800-82 and then the ISO27001/2 series. From a governance perspective the COBIT 5 framework (ISACA, 2012) is the best suited as it covers the governance areas substantially

From this it was established that the majority of respondents in South Africa have control frameworks in place that mostly govern the ICS/SCADA environment. As the majority indicated they use COBIT, which is the best suited from a governance perspective. However, what is lacking is the security aspect. As per the document analysis the best suited framework, the CPNI, is one of the least used frameworks by respondents in South Africa. This shows a gap in the securing ICS/SCADA systems or environments in South Africa.

In order to fully determine how ICS in South Africa are secured and governed the maturity of governance and security of an ICS/SCADA environment in South Africa was looked at. In Section 4.6 it was noted that 38% of respondents indicated that the maturity of governance and security in their ICS/SCADA environment is *established*, 25% indicated the maturity of their environment is *evolving* and 25% also indicated their environment is *basic*. It was also note that 10% of the governance and security of ICS/SCADA environments are *advanced* and only 2% *leading*. From the responses, it was noted the mean for the responses of the maturity of governance and security for ICS/SCADA environment is 2.40 and that, with 95% confidence, the population mean for the maturity of governance and security for the ICS/SCADA environment is between 2.10 to 2. 70. This indicates that the population mean for the maturity of governance and security for ICS/SCADA environments is between *evolving* (Inconsistently applied controls) leaning slightly towards *established* (Controls in place, but there is a need for enhancement).

The desired state for ICS/SCADA environments are at minimum *advanced* or *leading* (refer to Section 2.2.3.4), however it can be concluded that although a majority of respondents have *control frameworks in place* to govern the ICS/SCADA environment, the maturity of the controls is between *evolving* (Inconsistently applied controls) and *established* (Controls in place, but there is a need for enhancement) as indicated in Figure 6.3.

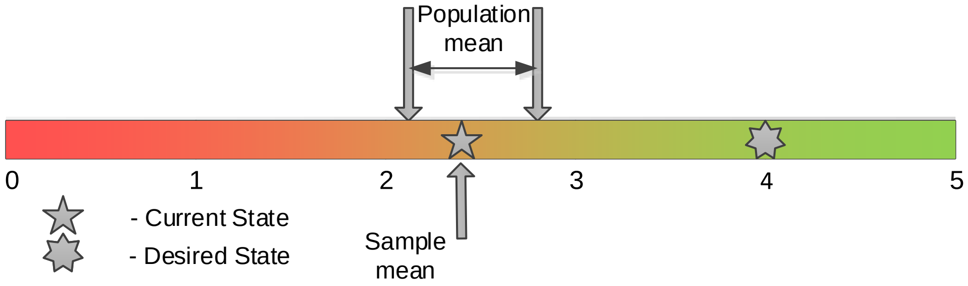


Figure 6.3: ICS/SCADA maturity

6.6 Research Objective 5 – To establish if the confidence levels of implemented controls/measures mitigating the threats and risks are sufficient

In order to establish if the confidence levels of the implemented controls/measures mitigating the threats and risks are sufficient the effectiveness of controls as well as the ease of implementation of controls needs to be look at, which gives us the security confidence as discussed in Section 3.4 and as depicted in Figure 3.2.

6.6.1 Effectiveness of controls

In Section 4.6.1 it was noted the top three effective controls implemented in the ICS/SCADA environments are:

- Firstly*, physical access* control, i*mplemented but requires improvement;*
- Secondly *firewalls*, *implemented but requires improvement*; and
- Thirdly *environmental standards*, *partially Implemented/in progress* but leaning strongly towards *implemented but requires improvement*.

The bottom three effective controls or less effective controls implemented in the ICS/SCADA environments are: *strategy of ICS/SCADA*, *SIEM or security intelligence centre* and *data encryption* which all relates to *partially implemented/in progress*.

Looking at the vulnerabilities from Section 6.2.1, the top three vulnerabilities related to ICS/SCADA systems are *patching* (outdated/unpatched), *monitoring* (no or limited), and *access control* (no or weak password). The controls to govern or mitigate the vulnerability for outdated/unpatched is by implementing *patch management*, which are neither top or bottom three, but the respondents indicated that *patch management* is p*artially implemented/in progress*.

Similar for the vulnerability, *no or limited monitoring*; the control to govern or mitigate it is to implement a *SIEM or security intelligence centre*, which are the second least effective control implemented. The respondents indicated this is *partially implemented/in progress*. The third top vulnerability is in *access control* (no or weak password), and the control to govern or mitigate is to implement effective user access management. This control is neither top nor bottom three, but the respondents indicated that user access management is *partially implemented*/*in progress,* but leaning strongly towards implemented control requires improvement. Although the control, user access management is a slightly lesser risk than the other two top vulnerabilities, this is still not sufficient as the control should be *implemented and operating effectively* in order to successfully govern or mitigate the vulnerability. This shows a clear gap in governing and mitigating of all three the top vulnerabilities.

The threats influencing ICS/SCADA security as discussed in Section 6.2.2, were *malware*, *staff undertaking unintentional unauthorised action* and *disgruntled staff* as the top three threats. Looking at controls to govern or mitigate these threats, the control to govern or mitigate *malware* is *virus/malware protection*. The respondents indicated that *anti-virus/malware control* is *partially implemented/in progress*, but leaning towards *implemented control requires improvement*. This shows a risk in governing and mitigation of the top threat, namely *malware*. Similar gap for the threat, *staff undertaking unintentional unauthorised action*, the control to govern or mitigate it is *policies, procedures, standards and frameworks*. Respondents indicated this is *partially implemented/in progress*. For the third top threat, *disgruntled staff*, the control to govern or mitigate this is to implement effective *user access management* in order to remove the user's account should they be terminated. Effective *policies, procedures, standards and frameworks* is also required to mitigate *disgruntled staff*. For both these controls the respondents indicated that the controls are *partially implemented/in progress*, but leaning strongly towards *implemented control requires improvement* for *user access management*. Although this is a slightly lesser risk than the other two top threats, this is still a risk as the control should be *implemented and operating effectively* in order to successfully govern or mitigate the threat, *disgruntled staff*.

For both the threats and vulnerabilities, the focus might be wrongly placed on the implementation of *physical security* and *network perimeter* controls, and does not however fully address the above threats and vulnerabilities. Although *physical security* might prevent *disgruntled staff* to do physical damage, more emphasis should be placed *access control*, the focus should be shifted towards the threats and vulnerabilities that are relevant to the ICS/SCADA environment.

6.6.2 Ease of implementation of controls

We noted in Section 4.6.2, the top three easiest controls to implement for the ICS/SCADA environment are *physical access control* (*implement with some challenges*), *environmental standards* (*implement with some challenges*), and *virus/ malware protection* all *implement with some challenges*. The bottom most difficult controls to implement for the ICS/SCADA environment are: *systems hardening* (*difficult to implement* leaning highly towards *implement with some challenges*), secondly *remote access* and *3rd party remote access* both control listed as *implement with some challenges*.

Looking at the vulnerabilities from Section 6.2.1, the top three vulnerabilities related to ICS/SCADA systems are *patching* (outdated/unpatched), *monitoring* (no or limited), and *access control* (no or weak password). The controls to govern or mitigate the vulnerability for *outdated/unpatched* systems is by implementing *patch management*, which are neither top or bottom three, but the respondents indicated that *patching control* as *implement with some challenges*.

Similar for the vulnerability, *no or limited monitoring*, the control to govern or mitigate it is to implement *a SIEM or security intelligence centre*, which respondents indicated this as *implement with some challenges*. The third top vulnerability is in *access control* (No or weak password), and the control to govern or mitigate is to implement effective *user access management*. This control is neither top nor bottom three easiest to implement, but the respondents indicated that *user access management* as *implement with some challenges*.

This indicates that the mitigating controls for the top vulnerabilities are not difficult to implement nor is it easy, but that it can be *implemented with some challenges*. This shows that some effort has been made to implement these controls.

The threats influencing ICS/SCADA security from Section 6.2.2, were *malware*, *staff undertaking unintentional unauthorised action* and *disgruntled staff* as the top three threats. Looking at controls to govern or mitigate these threats, the control to govern or mitigate *malware* is *virus/malware protection*. The respondents indicated that *anti-virus/malware* control is the third easiest control to implement and indicated as *implement with some challenges*. This shows that some effort has been made to implement the control to mitigate one of the top three threats, *malware*. Similar risks for the threat, *staff undertaking unintentional unauthorised action*, the control to govern or mitigate it is *policies, procedures, standards and frameworks*. Respondents indicated this as *implement with some challenges*. For the third top threat, *disgruntled staff*, and the control to govern or mitigate this implement effective *user access management* in order to remove the user's account should they be terminated as well as effective *policies, procedures, standards and frameworks*. For both these controls the respondents indicated that the controls as *implement with some challenges*. Similar to the vulnerabilities, this indicates that the mitigating controls for the top threats are not difficult to implement nor is it easy, but that it can be *implemented with some challenges*. This shows that some effort has been made to implement these controls.

6.6.3 How confident/certain are you that the implemented controls mitigating the threats and risks are sufficient?

In Section 4.6.4 it was noted how confident/certain the respondents were that the implemented controls mitigating the threats and risks sufficiently. The average of respondents indicate that they are *somewhat* confident leaning towards *moderately* confident that the implemented controls mitigate the threats and vulnerabilities sufficiently. This indicates that the confident levels are *lower* than it should be.

From Section 4.7.3, the security confidence is made up from *usability of security* and *ease of use of security*, as depicted in Figure 6.3. The top five security confidence controls are: *physical access control*, *environmental standards*, *firewalls in place*, *backup and recovery* and *virus/malware protection*. These controls should be focused on or prioritised when developing a control framework. This relates to similar controls as discussed in Section 6.6.1 and Section 6.6.2.

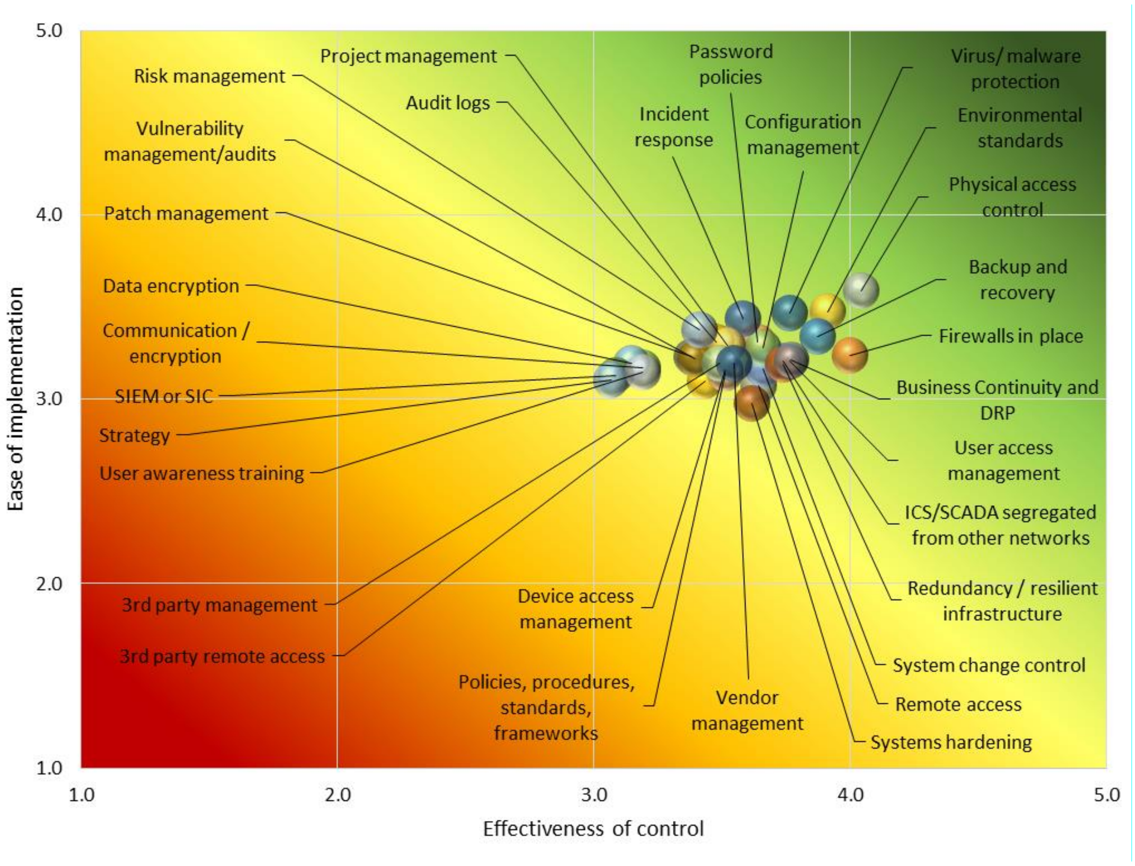


Figure 6.4: Effectiveness of control vs Ease of implementation

Source: Author compilation

6.6.4 Summary

Although focus is placed on certain controls to mitigate the perceived threats and vulnerabilities, more emphasis should be placed on controls that address the threats and vulnerabilities that are relevant to the ICS/SCADA environment.

The perception is that the mitigating controls for the top threats and vulnerabilities are not difficult to implement nor is it easy, but that it can be implemented with some challenges. This shows that some effort has been made to implement these controls. The confident levels of the respondents are *lower* than it should be for the controls that have been implemented to mitigate the threats and vulnerabilities sufficiently.

6.7 Research Objective 6 – To develop a control framework addressing the shortfalls for ICS security in South Africa

The research framework was discussed in Section 3.4, and is populated with the relevant data and results that was found by the study. Refer to Figure 6.2 for the unpopulated research framework.

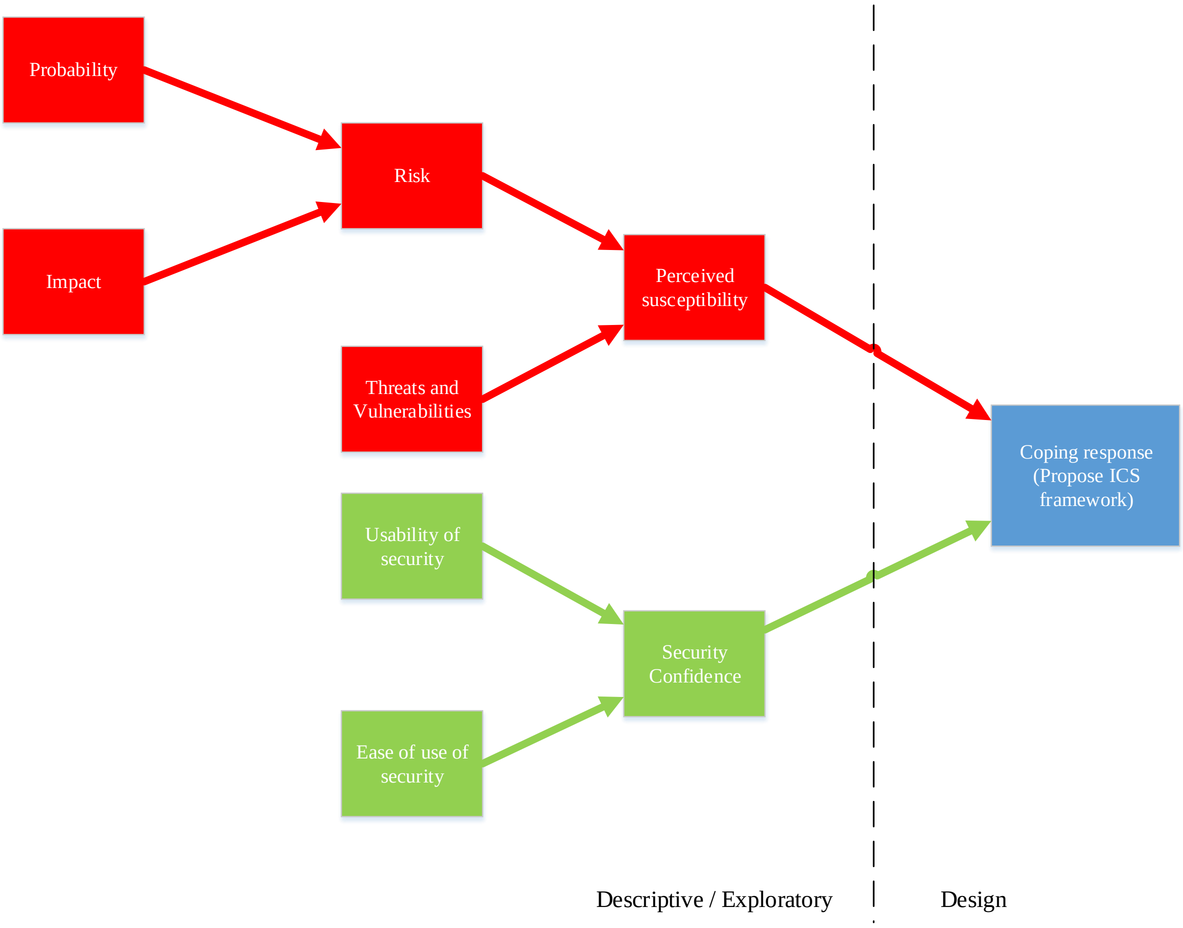


Figure 6.5: Research Framework (unpopulated with results)

Source: Author compilation

In Section 6.7.1 to Section 6.7.8 following, the top results that was used as input into the Research framework listed. The red blocks are represented from Sections 6.7.1 to 6.7.5.

6.7.1 Probability

From the discussion in Section 6.2.2, the top three threats likely to occur are:

- Malware;
- Staff undertaking unintentional unauthorised actions; and
- Disgruntled staff (intentional).

6.7.2 Impact

From the discussion in Section 6.2.2, the top three threats likely to impact ICS/SCADA systems are:

- Malware;
- Disgruntled staff; and
- Staff undertaking unintentional unauthorised actions.

6.7.3 Risks

As discussed in Section 6.2.3, the top three risks to ICS/SCADA environment are:

- Malware;
- Staff undertaking unintentional unauthorised actions; and
- Disgruntled staff.

6.7.4 Threats and Vulnerabilities

6.7.4.1 Threat

From the discussion in Section 6.2.2, the top three threats likely to occur are:

- Malware;
- Staff undertaking unintentional unauthorised actions; and
- Disgruntled staff (intentional).

6.7.4.2 Vulnerabilities

The discussion in Section 6.2.1, indicated that the top three vulnerabilities related to ICS/SCADA systems are

- Outdated/unpatched systems;
- No or limited Monitoring;
- ICS/SCADA not appropriately segregated; and
- No or weak password.

The top three technical vulnerabilities related to ICS/SCADA systems are

- Security Bypass;
- Cross site scripting; and
- Remote code execution.

6.7.5 Perceived susceptibility

The significant perceived susceptibility of ICS/SCADA environments in South Africa are the following risks, threats and vulnerabilities:

- Malware;
- Staff undertaking unintentional unauthorised actions;

- Disgruntled staff;
- Security Bypass;
- Cross site scripting;
- Remote code execution;
- Outdated/unpatched systems;
- No or limited Monitoring;
- No or weak password; and
- ICS/SCADA not appropriately segregated.

The green blocks are represented from Sections 6.7.6 to 6.78 and relate to the TAM model.

6.7.6 Usability of security

From the discussion in Section 6.6.1, the top three effective controls implemented in the ICS/SCADA environments are:

- Physical access control;
- Firewalls in place; and
- Environmental standards.

6.7.7 Ease of use of security

The discussion in Section 6.6.2 indicated that the top three easiest controls to implement for the ICS/SCADA environment are

- Physical access control;
- Environmental standards; and
- Virus/ malware protection.

6.7.8 Security Confidence

From Figure 6.4 the top five security confidence controls are:

- Physical access control;
- Environmental standards;
- Firewalls in place;
- Backup and recovery; and
- Virus/malware protection.

The research framework has been populated with the list of all the relevant input from Sections 6.7.1 to Section 6.7.8. Note that the blocks inside the black dotted line (Probability, Impact, Threats and Risk) have the same list, namely *malware*, *staff undertaking unintentional unauthorised actions* and *disgruntled staff*.

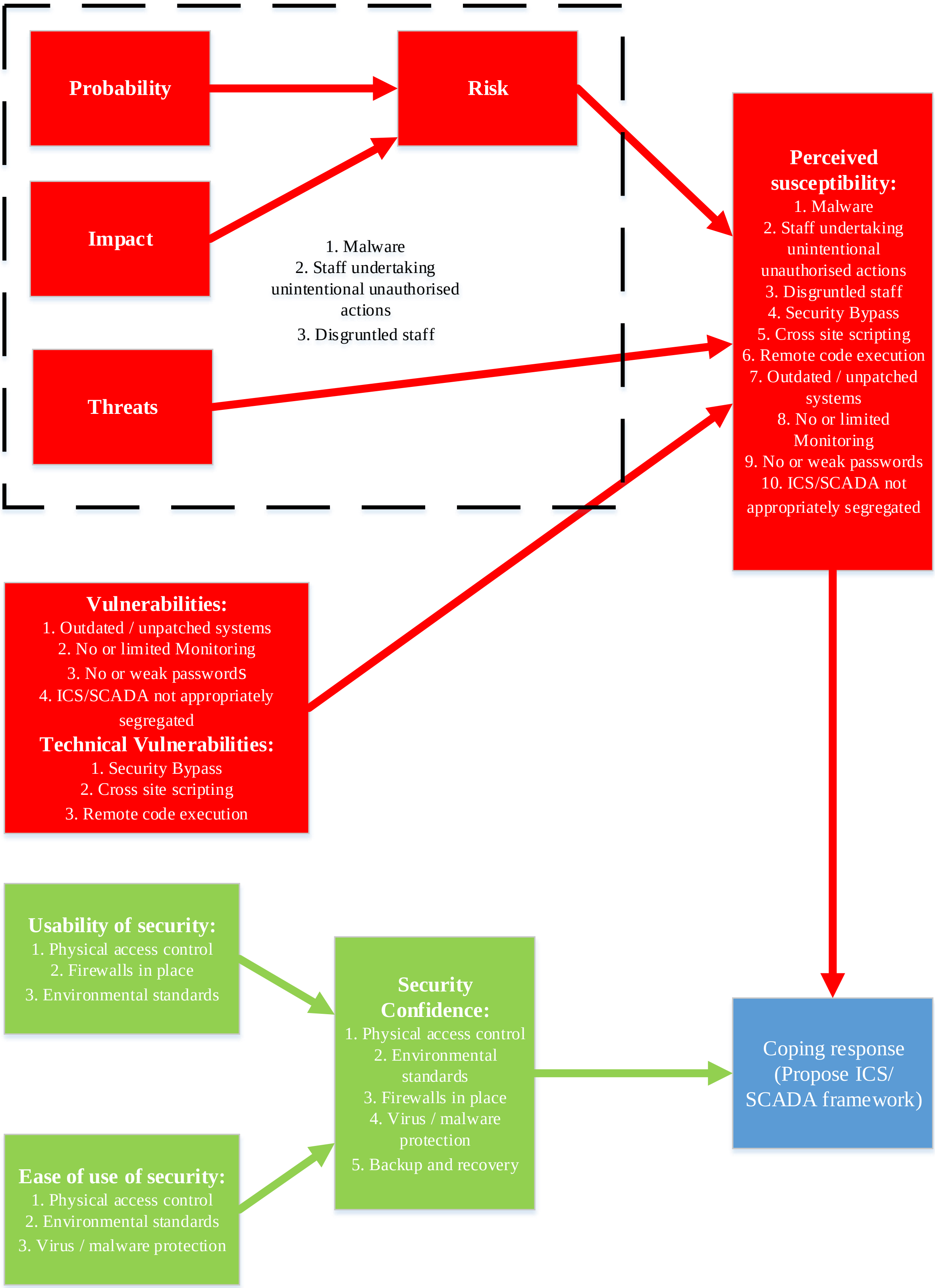

Probability
Risk
Impact
Threats
1. Malware
2. Staff undertaking unintentional unauthorised actions
3. Disgruntled staff
Perceived susceptibility:
1. Malware
2. Staff undertaking unintentional unauthorised actions
3. Disgruntled staff
4. Security Bypass
5. Cross site scripting
6. Remote code execution
7. Outdated / unpatched systems
8. No or limited Monitoring
9. No or weak passwords
10. ICS/SCADA not appropriately segregated
Vulnerabilities:
1. Outdated / unpatched systems
2. No or limited Monitoring
3. No or weak passwords
4. ICS/SCADA not appropriately segregated
Technical Vulnerabilities:
1. Security Bypass
2. Cross site scripting
3. Remote code execution
Usability of security:
1. Physical access control
2. Firewalls in place
3. Environmental standards
Security Confidence:
1. Physical access control
2. Environmental standards
3. Firewalls in place
4. Virus / malware protection
5. Backup and recovery
Ease of use of security:
1. Physical access control
2. Environmental standards
3. Virus / malware protection
Coping response (Propose ICS/ SCADA framework)

Figure 6.6: Research Framework populated with results

Source: Author compilation

6.7.9 Coping response (Propose ICS/SCADA framework)

Taking the perceived susceptibility from Section 6.7.5 and the Security Confidence from Section 6.7.8 as in put into the coping response, the framework for protection of ICS/SCADA in South Africa can be developed.

6.7.9.1 Process of framework development

As discussed in Section 2.5.4, the process to develop a control framework is illustrated in Figure 6.6.

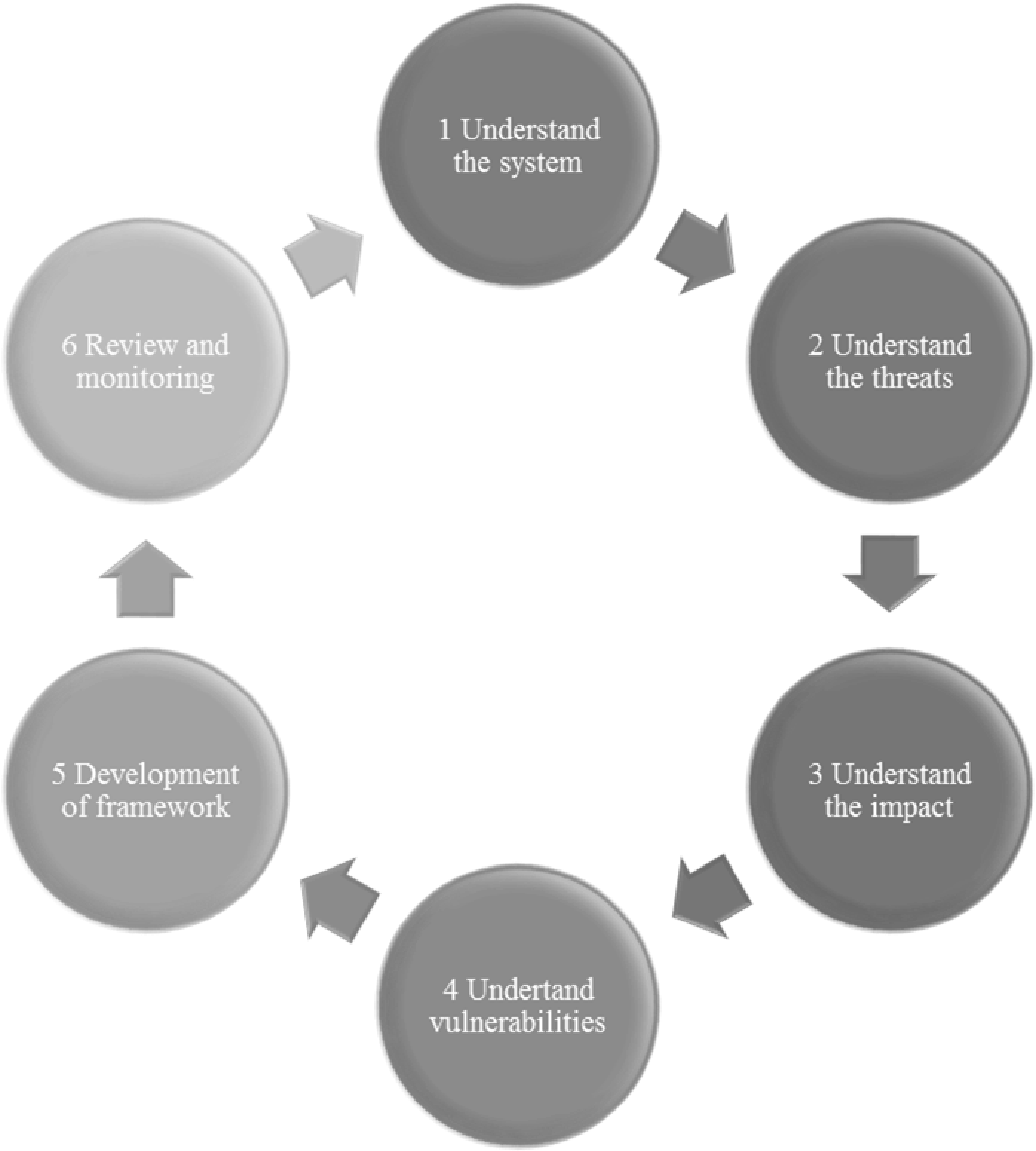


Figure 6.7: Framework Development Methodology

Adapted from: CPNI (2008)

Each of the framework development steps are discussed in Sections A to F.

A. Understand the system

As discussed in Section 2.5.4.1, an organisation or company needs to conduct a formal inventory and analysis of the ICS/SCADA systems and components in the environment. This was excluded as there were various organisations from different industries consisting of multiple ICS/SCADA systems.

B. Understand the threats

Under this step, the organisation needs to assess the threats to the organisation. The threats for ICS/SCADA systems in South Africa was determined, as discussed in Section 6.2.2 and populated in Section 6.7.4.1. The threats are *malware*, *staff undertaking unintentional unauthorised actions*, and *disgruntled staff*.

C. Understand the impact

The impact of the risks, threats and vulnerabilities of non-governed or unsecure ICS/SCADA as discussed in Section 6.4 is *loss of availability* or *denial of service*.

D. Understand vulnerabilities

The vulnerabilities affecting the organisation needs to be assessed under this step. The vulnerabilities for ICS/SCADA systems in South Africa was determined, as discussed in Section 6.2.1 and populated in Section 6.7.4.2.

E. Development of framework

A SCADA control framework was developed taking into account the relevant risks, threats and vulnerabilities to the South African ICS/SCADA environment. From the document analysis in Section 5.4, the CPNI framework is best suited overall as it covers all the security areas and the COBIT framework is best suited from a governance perspective and was also used by most respondents as discussed in Section 6.5. The high level framework is listed in Table 6.5 with prevalent controls to implement based on the *Perceived susceptibility*, as discussed in Section 6.7.5. The time frame for each control is based on priority. Priority 1 controls need to be implemented within three months, priority 2 within six months and priority three within a year. The details of each control is discussed in Section 6.7.9.2 to Section 6.7.9.27

F. Review and monitoring

Regular review of the South African ICS/SCADA environment needs to take place, to identify any new systems changes, threats, vulnerabilities and corresponding update of the control framework should take place at minimum annually. Ongoing testing of the framework in other ICS/SCADA environments will need to be conducted to ensure generalisation and applicability of the framework. Future work will need to include detailed breakdown of the controls as well as analysis of the practicality of implementation and further alignment to South African government legal requirements and international frameworks.

Table 6.5: ICS/SCADA controls prioritised

Control	Justification	Threat/Vulnerability	Priority	Timeframe
Virus/Malware Protection	Top threat	Malware	1	0 – 3 months
	Top 5 security confidence			
Monitoring (SIEM or Security Intelligence Centre and Audit logs)	Top threat	Staff undertaking unintentional unauthorised actions	1	0 – 3 months
	Top vulnerability	No or limited Monitoring		
User and Device Access Management	Top threat	Disgruntled staff (intentional)	1	0 – 3 months
	Top technical vulnerability	Security Bypass		
System Change Control	Top threat	Staff undertaking unintentional unauthorised actions	1	0 – 3 months
Systems hardening and Configuration Management	Top technical vulnerability	Cross site scripting	1	0 – 3 months
Remote Access and 3rd party remote access	Top technical vulnerability	Remote code execution	1	0 – 3 months
Patch Management	Top vulnerability	Outdated/unpatched systems	1	0 – 3 months
Password Policies	Top vulnerability	No or weak password	1	0 – 3 months
Segregation from other networks and Firewalls in place	Top 5 security confidence, ICS/SCADA exposed to internet	Firewalls in place	2	3 – 6 months
Physical Access control	Top 5 security confidence	Physical access control	2	3 – 6 months
Environmental Standards	Top 5 security confidence	Environmental Standards	2	3 – 6 months
Backup and Recovery, Redundancy/resilient infrastructure and Business Continuity and Disaster recovery plans	Top 5 security confidence	Backup and recovery	2	3 – 6 months
Policies, procedures, standards, and frameworks			3	6 – 12 months
Vulnerability Management/audits			3	6 – 12 months
Risk Management			3	6 – 12 months
Incident Response			3	6 – 12 months
User Awareness Training			3	6 – 12 months
Third Party Management			3	6 – 12 months
Project Management			3	6 – 12 months
Vendor Management			3	6 – 12 months
Communication/Encryption, Communication: Wireless and mobile	Bottom 3		3	6 – 12 months
Strategy of ICS/SCADA	Bottom 3		3	6 – 12 months
Data encryption	Bottom 3		3	6 – 12 months

6.7.9.2 Virus/Malware Protection

To ensure that the ICS/SCADA environment is protected against malware and external threats by implementing vendor accredited and configured anti malware software. Where anti malware software cannot be deployed, other protection measures should be implemented, such as gateway anti-virus scanning or manual media checking.

6.7.9.3 Monitoring (SIEM or Security Intelligence Centre and Audit logs)

Ensure that regular system monitoring of ICS/SCADA infrastructure (processes, network, and field devices) is performed. This includes network traffic and user access to detect anomalies, and external threat intelligence to receive early warnings of potential threats or newly discovered vulnerabilities. SIEM or SIC can be used to assist. At minimum Audit logs should be reviewed.

6.7.9.4 User and Device Access Management

To ensure that new employees and terminated employees are managed in the ICS/SCADA environment, this include access to systems, applications, databases, device, switches and PLCs. Ensure the access is minimised to specific job-functions.

6.7.9.5 System Change Control

To ensure that changes to the ICS/SCADA systems are managed and all data conversions are formally managed in accordance with the System Development Lifecycle Methodology, and Change and Release Management Procedure.

6.7.9.6 Systems hardening and security features

Ensure that the ICS/SCADA systems have been hardened: security features activated, unused services and ports have been disabled in the operating systems and applications to prevent unauthorised use, and the use of removable media (such as CDs and USB drives) is restricted where possible. Where use of removable media is necessary, procedures are in place to ensure these are checked for malware prior to use.

6.7.9.7 Configuration Management

Ensure that configuration of ICS/SCADA systems have been documented in a configuration management database (CMDB). No changes are made to the ICS/SCADA configuration without a corresponding update to the CMDB.

6.7.9.8 Remote Access and 3rd party remote access

To ensure that remote access to ICS/SCADA systems is restricted, remote access is managed and regularly reviewed. Appropriate authentication mechanisms (e.g. strong authentication) should be implemented for any remote connections. Security reviews of all third parties having remote access to the ICS/SCADA are performed and managed on a regular basis.

6.7.9.9 Patch Management

To ensure that vendor certified security patches are implemented. Thoroughly test all patches on a test-bed prior to installing on production systems. Where security patching is not possible or practical, alternative appropriate protection measures are considered.

6.7.9.10 Password Policies

To ensure that password policies for ICS/SCADA systems are defined and implemented: applicable users, strength of passwords and expiration times are specified, default vendor passwords are changed where possible from the default settings, and for systems or functions where passwords may not be deemed necessary (such as view only mode) compensating controls are documented (e.g. for control room staff).

6.7.9.11 Segregation from other networks and Firewalls in place

To ensure that ICS/SCADA network is protected or segregated from other networks by appropriately installed, configured and managed firewalls (where connections exist). For extremely sensitive networks, an air gap can be used to separate the ICS/SCADA network from the enterprise network. Email and Internet access from ICS/SCADA systems is minimised and restricted to protect environment from external threats.

6.7.9.12 Physical Access

To ensure that adequate physical security measures are in place to restrict access to areas housing ICS/SCADA equipment and devices.

6.7.9.13 Environmental Standards

Ensure that a resilient infrastructure with necessary facilities are installed to protect the ICS/SCADA systems. Equipment should reside in environmentally controlled areas at appropriate ambient conditions to ensure its proper and sustainable operation.

6.7.9.14 Backup and Recovery

To ensure that effective backups and recovery procedures are in place to safeguard critical data and that the integrity of backups is regularly tested.

6.7.9.15 Redundancy/resilient infrastructure

Redundancy are in place for critical ICS/SCADA systems or ICS/SCADA equipment and components. These include redundant networks, switches, servers, workstation and PLCs.

6.7.9.16 Business Continuity and Disaster recovery plans

A Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP) is developed in cooperation with business process owners and based on risk based approach and should clearly define the roles and responsibilities of the recovery team members. The DRP and BCP should be tested and kept up to date to ensure recovery of ICS/SCADA systems in a way to minimise business impact in the event of a major disruption.

6.7.9.17 Policies, Procedures Standards and Frameworks

To ensure that an effective framework is implemented and communicated to all relevant stakeholders, to govern the ICS/SCADA environment.

6.7.9.18 Vulnerability management

To ensure that vulnerabilities to ICS/SCADA systems are managed and minimised.

6.7.9.19 Incident Response

Ensure that response capabilities to ICS/SCADA system incidents are understood and managed. These include a helpdesk system to prioritise and track incidents and escalation of long outstanding incidents. Procedures should be in place to escalate an incident to a disaster and revert to BCP or DRP should require.

6.7.9.20 User Awareness Training

To ensure that awareness and skills are improved by performing ongoing training for ICS/SCADA system staff. All information security staff who may be required to work with ICS/SCADA should receive the relevant training to do so.

6.7.9.21 Third Party Management

To ensure that third parties applicable to ICS/SCADA systems are managed and security clauses are detailed in all contracts prior to agreements.

6.7.9.22 Project Management

To ensure that the ICS/SCADA projects are managed using recognised methodology.

6.7.9.23 Vendor Management

To ensure that relationship with ICS/SCADA vendors are managed in accordance with organisational policies and procedure that governs the ICS/SCADA. This includes management of contracts, software licenses and employees who work in ICS/SCADA environment.

6.7.9.24 Communication/Encryption

To ensure that critical and confidential communication of the ICS/SCADA network, whether wired or wireless are appropriately encrypted and are regularly monitored and reviewed.

6.7.9.25 Communication: Wireless and mobile

To ensure that wireless networks are minimised and wireless connections are regularly monitored and reviewed. All mobile enabled systems (GSM) must conform to RICA act.

6.7.9.26 Strategy of ICS/SCADA

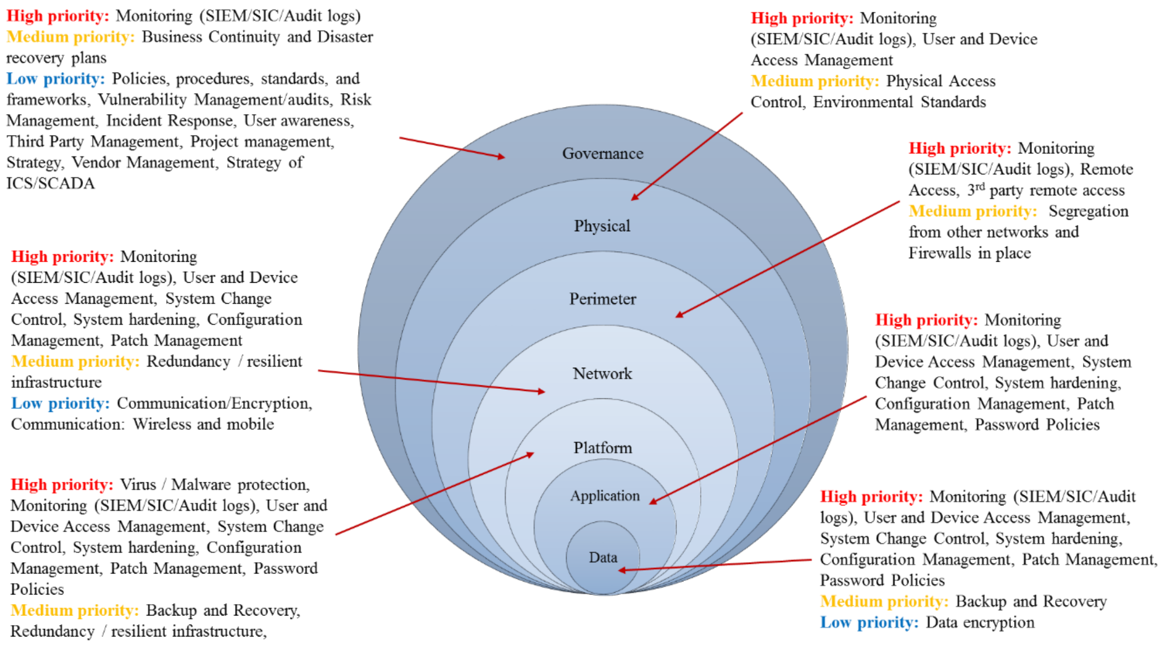
To ensure that the ICS/SCADA strategies and organisational strategies are aligned.

6.7.9.27 Data Encryption

To ensure that critical and confidential data of the ICS/SCADA environment, whether stored in a database, Operating System or Application are appropriately encrypted and are regularly monitored and reviewed.

6.7.10 Application to defence in depth

The controls mentioned in Section 6.7.9.2 to Section 6.7.9.27 have been arranged into a defence in depth approach from the prioritisation in Table 6.5. This is visualised in Figure 6.8. Of the 26 controls listed, a number are relevant to multiple layers in the defence-in-depth model. The purpose of this approach is for the different layers to provide protection against threats which other layers may not protect against. For example, the malware discussed above can circumvent air gaps, therefore additional protection is required in the form of malware, and monitoring for unusual traffic or behaviour. In this way, if the preventative controls (the network segregation and malware protection) fail to prevent the malware infecting, the detective control (monitoring) will then record unusual traffic indicating that a malware infection has occurred. At least one control should be implemented for each layer in Figure 6.8, however more controls will have a higher likelihood of preventing cyber-security incidents. Of the 26 controls listed above, a number are relevant to multiple layers in the defence-in-depth model.



High priority: Monitoring (SIEM/SIC/Audit logs)
Medium priority: Business Continuity and Disaster recovery plans
Low priority: Policies, procedures, standards, and frameworks, Vulnerability Management/audits, Risk Management, Incident Response, User awareness, Third Party Management, Project management, Strategy, Vendor Management, Strategy of ICS/SCADA

High priority: Monitoring (SIEM/SIC/Audit logs), User and Device Access Management
Medium priority: Physical Access Control, Environmental Standards

High priority: Monitoring (SIEM/SIC/Audit logs), Remote Access, 3rd party remote access
Medium priority: Segregation from other networks and Firewalls in place

High priority: Monitoring (SIEM/SIC/Audit logs), User and Device Access Management, System Change Control, System hardening, Configuration Management, Patch Management
Medium priority: Redundancy / resilient infrastructure
Low priority: Communication/Encryption, Communication: Wireless and mobile

High priority: Virus / Malware protection, Monitoring (SIEM/SIC/Audit logs), User and Device Access Management, System Change Control, System hardening, Configuration Management, Patch Management, Password Policies
Medium priority: Backup and Recovery, Redundancy / resilient infrastructure,

High priority: Monitoring (SIEM/SIC/Audit logs), User and Device Access Management, System Change Control, System hardening, Configuration Management, Patch Management, Password Policies

High priority: Monitoring (SIEM/SIC/Audit logs), User and Device Access Management, System Change Control, System hardening, Configuration Management, Patch Management, Password Policies
Medium priority: Backup and Recovery
Low priority: Data encryption

Figure 6.8: Defence in depth approach

Source: Author compilation

6.8 Summary

The factors influencing ICS/SCADA in South Africa are: vulnerabilities, namely, outdated or unpatched systems, No or limited monitoring and Access control; technical vulnerabilities such as Security Bypass, Cross-site scripting and Remote code execution; and threats which include Staff undertaking unintentional unauthorised actions, disgruntled staff and Malware. These factors could potentially cause distribution to operations and the business and ultimately lead to financial loss or possibly human life.

The best mitigating controls to govern and secure the top perceived vulnerabilities and threats for ICS/SCADA systems in South Africa are to patch ICS/SCADA systems, to monitor them and to ensure appropriate access control in the form of user account management is in place as well as appropriate Anti-virus software. While the best mitigating controls to govern and secure the technical vulnerabilities are the implementation of appropriate Access control, implementation of appropriate and secure Configuration as well as implementing controls to govern and secure remote access.

The impact of non-governed or unsecure ICS/SCADA is Loss of Availability or Denial of service. The top perceived threats and vulnerabilities could potentially lead to service disruption to operations and business, financial loss, loss of human life and adverse publicity.

More focus was placed on certain controls to mitigate the perceived threats and vulnerabilities that are relevant to the ICS/SCADA environment. The perception is that the mitigating controls for the top threats and vulnerabilities can be implemented with some challenges. A control framework consisting of governance and security controls, was develop to take into account these perceived threats and vulnerabilities in order to mitigate the risk of ICS/SCADA in South Africa. Priority was given to controls that mitigate the perceived threats, risk and vulnerabilities. The controls were rearranged into a defence in depth model. The next chapter concludes the study and provide recommendations.

Chapter 7 Conclusions and recommendations

7.1 Introduction

The previous chapter interpreted and discussed the results of the analysis of the data gathered by means of the online questionnaire, and secondary data analysis. This chapter concludes the study and examines whether the research objectives were achieved. This dissertation consisted of seven chapters (including this chapter).

Chapter 1 introduced the study and described the research approach. The aim of the study was to assess the current practices of ICS/SCADA in SA, and to develop a consolidated framework aligned to South Africa taken into account new and existing legislation. Chapter 2 presented a literature review on ICS/SCADA. Chapter 3 discussed the research methodology and the research design that guided this study, while Chapter 4 presented the quantitative and qualitative data analysis. Chapter 5 looked at various documents from local and international as well as network security device data, analysed and compared these. Chapter 6 presented a discussion based on the quantitative and qualitative data analysed and in relation to the secondary data analysis.

This chapter concludes the study by presenting the conclusions, the limitations, proposes areas for future research and a final conclusion. Figure 7.1 is a graphical representation of the outline of this chapter and overall structure.

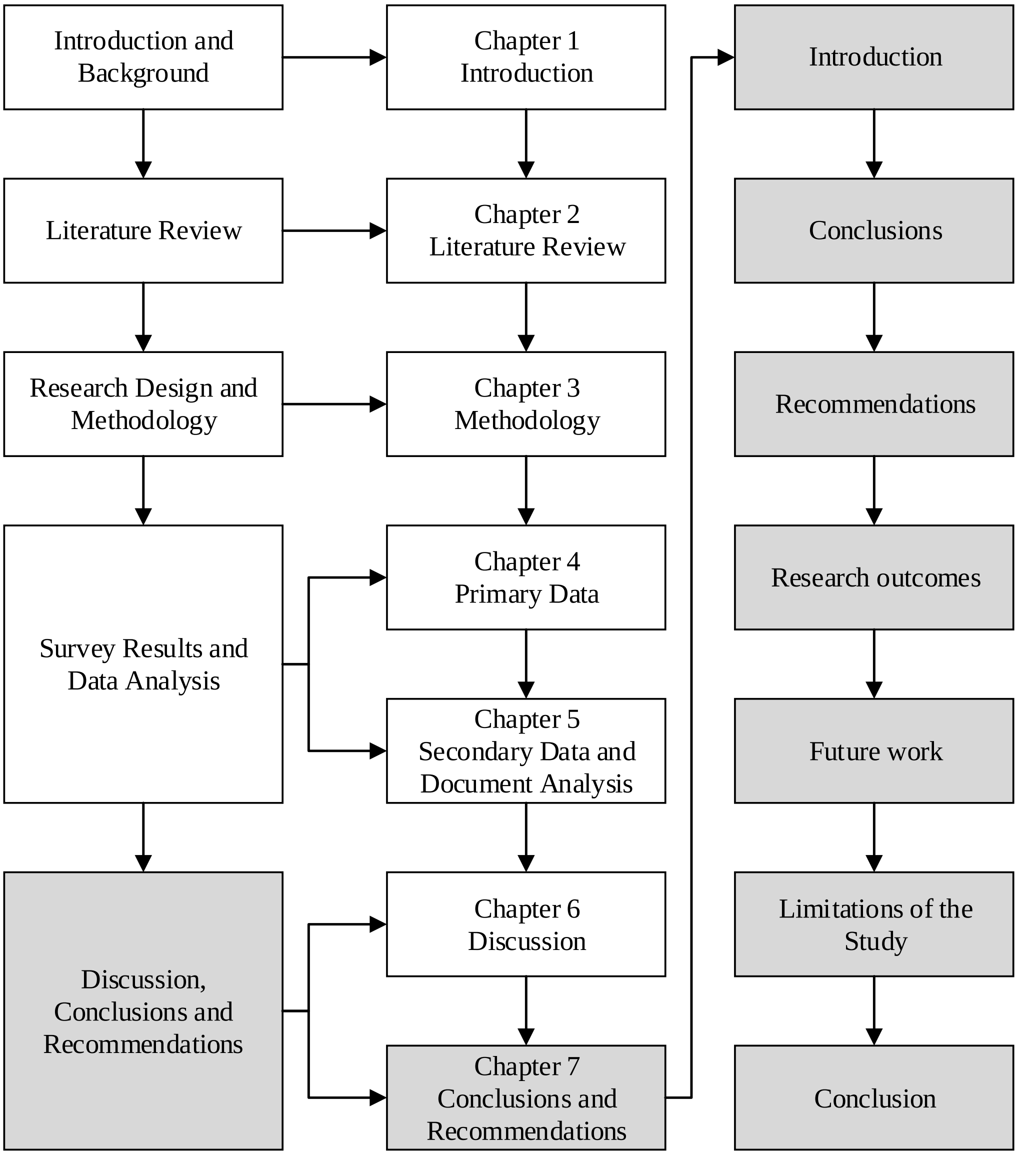

Introduction and Background
Chapter 1 Introduction
Introduction
Literature Review
Chapter 2 Literature Review
Conclusions
Research Design and Methodology
Chapter 3 Methodology
Recommendations
Survey Results and Data Analysis
Chapter 4 Primary Data
Research outcomes
Chapter 5 Secondary Data and Document Analysis
Future work
Discussion, Conclusions and Recommendations
Chapter 6 Discussion
Limitations of the Study
Chapter 7 Conclusions and Recommendations
Conclusion

Figure 7.1: Graphical representation of Chapter 7 outline

7.2 Conclusions

The research objectives were met and are discussed further in the section below.

7.2.1 Research Objective 1 – To determine the factors (vulnerabilities and threats) influencing ICS security in South Africa

The study found that the factors (vulnerabilities and threats) influencing ICS/SCADA environments in South Africa are Patching, Monitoring, and Access control for vulnerabilities and Cross site scripting, Information Disclosure and Security Bypass as technical vulnerabilities. The other factors (threats) that influence ICS/SCADA in South Africa are Malware, Staff undertaking unintentional unauthorised actions and disgruntled staff. Figure 6.1 shows the Risks related to ICS/SCADA. The Top risks are the matching the top threats. Comparing this with analysis of reports from both an international and local perspective it was noted this coincides with the top threats as found by the study showing consistency in the results. These factors could potentially cause distribution to operations and the business and ultimately lead to financial loss or possibly human life.

7.2.2 Research Objective 2 – To determine what the best mitigating controls to govern and secure ICS/SCADA systems in South Africa are

The study found that the top three controls mitigating vulnerabilities in the ICS/SCADA environments as indicated by the respondents were Configuration Management, Physical security and Network perimeter. The respondents indicated these controls were *Partially Implemented/in progress*. This however does not address the top threats and vulnerabilities in the ICS/SCADA environment. It was also noted the controls mitigating the top threats and vulnerabilities were at best *Partially Implemented/in progress*. This shows there are still risks as the controls should be *Implemented and operating effectively* in order to successfully govern or mitigate the top threats and vulnerabilities. The state of ICS/SCADA is one of ungoverned and unsecure systems. The controls need to be prioritised to focus on the top risks, threats and vulnerabilities.

7.2.3 Research Objective 3 – To determine the impact of non-governed ICS.

The respondents indicated the impacts of non-governed ICS/SCADA environments should threats and vulnerabilities materialise, are Loss of Availability/Denial of service, Loss of Integrity and Unauthorised control all having a *Moderate* impact which could lead to Some service disruption/potential for adverse publicity.

The threats (Malware, disgruntled staff (intentional) and Staff undertaking unintentional unauthorised actions) likely to impact ICS/SCADA systems all have a *Medium* impact, which indicate the threats are expected to occur in some circumstances but could also have a *Higher* impact like service disruption.

7.2.4 Research Objective 4 – To determine how ICS in South Africa are secured and governed

The study found that the majority of the respondents in South Africa have control frameworks in place. These frameworks however mostly focus on the governance aspect and not so much on the security aspect of an ICS/SCADA environment. There is a clear gap in securing ICS/SCADA systems or environments in South Africa.

Furthermore, the respondents indicated that the maturity of the controls are between *Evolving*, i.e. inconsistently applied controls, and *Established* i.e. Controls in place, but there is a need for enhancement. It was concluded that although a majority of respondents have a governance framework in place, the controls are not consistently applied or operating effectively.

7.2.5 Research Objective 5 – To establish if the confidence levels of implemented controls/measures mitigating the threats and risks are sufficient

The study found that the confidence levels of implemented control/measures mitigating the threats and risk are low as the respondents are only *somewhat* confident that the implemented controls mitigating the threats and risk are sufficient.

The effectiveness of controls as well as the ease of implementation of controls were also investigated. The top three perceived as effective controls implemented in the ICS/SCADA environments (Physical access control, Firewalls and Environmental standards) were at best *implemented but requires improvement*. This further strengthen the results in Section 7.2.4 which indicates the controls are not consistently applied or operating effectively. Figure 6.3 shows the effectiveness of control versus the ease of implementation. It was observed that the top three easiest controls to implement for the ICS/SCADA environment (Physical access control, Environmental standards and Virus/ malware protection) were at best *implemented with some challenges*. This indicates that not only are the controls difficult to implement, but even if controls are implemented, there still requires improvement as they are not operating effectively.

The confident levels of the respondents are lower than it should be for the controls that have been implemented to mitigate the threats and vulnerabilities sufficiently. From the discussion, the controls that should be prioritised or focused on are: Virus/malware protection, Physical access control, Environmental standards, Firewalls in place, and Backup and recovery.

7.2.6 Research Objective 6 - To develop a control framework addressing the shortfalls for ICS security in South Africa

The ultimate and final objective was to develop a control framework for ICS/SCADA in South Africa addressing the shortfalls. A SCADA control framework was developed taking into account the COBIT and CPNI frameworks. The high level framework is listed in Section 6.7.9 with prevalent controls to implement based on the Perceived susceptibility.

The process for the development of the control framework was discussed in Section 6.7.9.1. The controls were prioritised to focus and address the top risks, threats and vulnerabilities based on the Perceived susceptibility. The control framework was developed with the high priority controls first. From the control framework, the controls were rearranged in a defence-in-depth model as depicted in Figure 7.2.

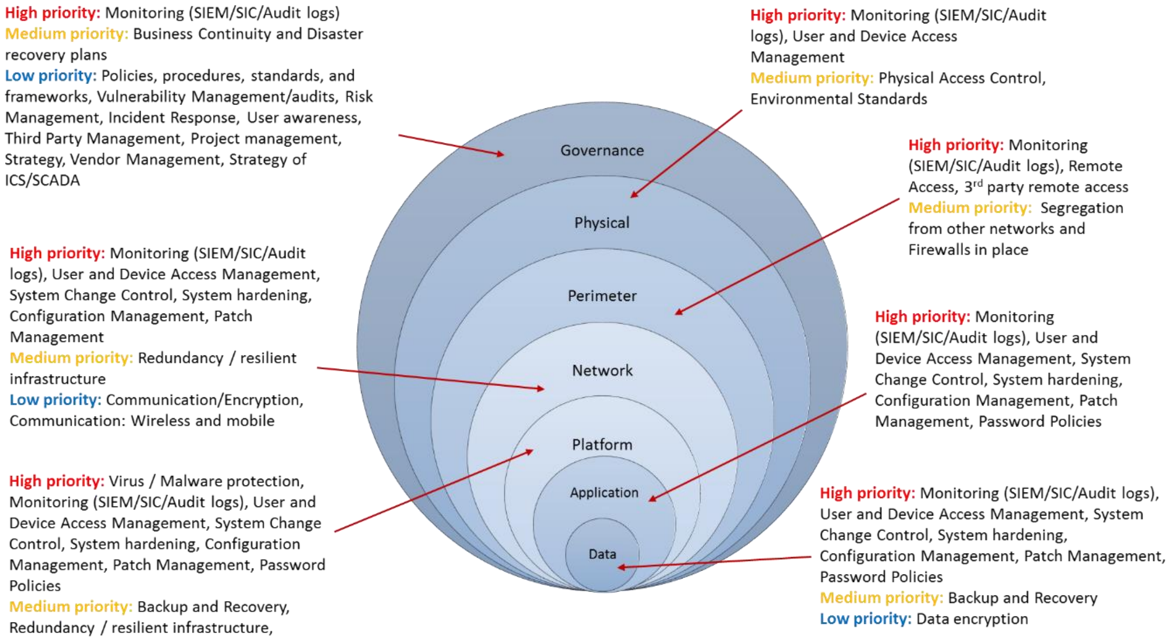

High priority: Monitoring (SIEM/SIC/Audit logs)
Medium priority: Business Continuity and Disaster recovery plans
Low priority: Policies, procedures, standards, and frameworks, Vulnerability Management/audits, Risk Management, Incident Response, User awareness, Third Party Management, Project management, Strategy, Vendor Management, Strategy of ICS/SCADA
High priority: Monitoring (SIEM/SIC/Audit logs), User and Device Access Management
Medium priority: Physical Access Control, Environmental Standards
High priority: Monitoring (SIEM/SIC/Audit logs), Remote Access, 3rd party remote access
Medium priority: Segregation from other networks and Firewalls in place
High priority: Monitoring (SIEM/SIC/Audit logs), User and Device Access Management, System Change Control, System hardening, Configuration Management, Patch Management
Medium priority: Redundancy / resilient infrastructure
Low priority: Communication/Encryption, Communication: Wireless and mobile
High priority: Monitoring (SIEM/SIC/Audit logs), User and Device Access Management, System Change Control, System hardening, Configuration Management, Patch Management, Password Policies
High priority: Virus / Malware protection, Monitoring (SIEM/SIC/Audit logs), User and Device Access Management, System Change Control, System hardening, Configuration Management, Patch Management, Password Policies
Medium priority: Backup and Recovery, Redundancy / resilient infrastructure,
High priority: Monitoring (SIEM/SIC/Audit logs), User and Device Access Management, System Change Control, System hardening, Configuration Management, Patch Management, Password Policies
Medium priority: Backup and Recovery
Low priority: Data encryption
Governance
Physical
Perimeter
Network
Platform
Application
Data

Figure 7.2: Defence in depth model for ICS/SCADA

Source: Author compilation

7.3 Recommendations

7.3.1 Misalignment of controls

From the discussion in Section 6.6.1, it was determined that there is a misalignment between the controls implemented and the ones addressing the Top Risks, Threats and Vulnerabilities. Priority should be given to those addressing the current Top Risks, Threats and Vulnerabilities. These should also be regularly reviewed and ensured it is current. International threats should not be ignored, and should be considered for future as they might come or become relevant to South Africa at a later stage.

7.3.2 Risks and threats

In order to reduce or mitigate the Top three risks and threats to ICS/SCADA environment, the following are recommended as discussed in Section 6.3.

7.3.2.1 Malware

In order to effectively protect the ICS/SCADA environment against malware and external threats, vendor accredited and configured anti-malware software should be implemented and regularly updated. Where anti-malware software cannot be deployed, other protection measures should be implemented, such as gateway anti-virus scanning or manual media checking.

7.3.2.2 Staff undertaking unintentional unauthorised actions

To mitigate staff undertaking unintentional unauthorised actions, first comprehensive Security, Governance, Risk and compliance policies, frameworks and standards must be successfully implemented. These should also be communicated to all relevant stakeholders. In addition, regular system monitoring of the ICS/SCADA infrastructure (including processes, network, and field devices) should be performed. This includes network traffic and user access to detect anomalies, and external threat intelligence to receive early warnings of potential threats or newly discovered vulnerabilities as well as anomalies caused by internal staff undertaking unintentional unauthorised actions.

7.3.2.3 Disgruntled staff

Out-going employees should be managed, this includes removing all access, both physical and logical. This will mitigate the risk of disgruntled staff who have left the organisation. In order to minimise internal disgruntled staff, a similar mitigating action in terms of monitoring should be implemented. This include regular system monitoring of the ICS/SCADA infrastructure, network traffic and user access to detect anomalies of actions performed by disgruntled staff.

7.3.3 Vulnerabilities

In order to reduce or mitigate the vulnerabilities to ICS/SCADA environment, the following are recommended as discussed in Section 6.3:

7.3.3.1 Patching

Implement vendor certified security patches. Thoroughly test all patches on a test-bed prior to installing on production systems. Where security patching is not possible or practical, alternative appropriate protection measures are considered

7.3.3.2 Monitoring

Regular system monitoring of the ICS/SCADA infrastructure (processes, network, and field devices) should be performed. This includes network traffic and user access to detect anomalies, and external threat intelligence to receive early warnings of potential threats or newly discovered vulnerabilities.

7.3.3.3 Access control

Implement mitigating controls to ensure that new employees and out-going employees are managed in the ICS/SCADA environment. Also ensure the access is minimised to specific job-functions, by applying the principle of least privilege access.

Appropriate password policies for ICS/SCADA systems should be defined and implemented. This should include the applicable users, strength of passwords and expiration times, changing of default vendor passwords, and for ICS/SCADA systems or functions where passwords may not be deemed necessary (such as view only mode) compensating controls should be documented (e.g. for control room staff).

7.3.4 Technical vulnerabilities

The following mitigating actions would reduce the following technical vulnerabilities, as discussed in Section 6.3:

7.3.4.1 Cross site scripting

To mitigate cross site scripting ICS/SCADA systems should be hardened. This include activating security features, disabling unused services and ports in the operating systems and applications to prevent unauthorised use.

7.3.4.2 Information Disclosure

Similar to preventing cross site scripting, to mitigate Information Disclosure, ICS/SCADA systems should be hardened as mentioned in Section 7.3.4.1.

7.3.4.3 Security Bypass

To prevent Security bypass, ICS/SCADA systems should have effective user access management and password policies defined and implemented. These should include new users joining and removing users who have left the organisation, strength of passwords and expiration times, and changing of default vendor passwords. For systems or functions where passwords may not be deemed necessary (such as view only mode) compensating controls are documented (e.g. for control room staff).

In addition, security features should be activated, unused services and ports in the operating systems and applications should be disabled. The use of removable media (such as CDs and USB drives) should be restricted. Where use of removable media is necessary, procedures are in place to ensure these are checked for malware prior to use.

7.3.5 Consistency in reporting

From the discussion in Section 6.2.1, it was determined that security vendors should endeavour to improve the consistency of how vulnerabilities and threats are classified and reported. Reports from different years for the same vendor have different naming of vulnerabilities/threats. There are also different naming of vulnerabilities/threats between vendors, making it hard to summarise and correlate. There should be a standard in naming and reporting across security vendors.

7.4 Research outcomes

The research outcome was to address the gap that there is no or limited information available as to the current state of ICS in South Africa including the factors influencing ICS and how they are governed. The mixed methods were used, a survey as well as secondary data pertaining to multiple network security devices. There are contributions are discussed below.

7.4.1 Contribution to Theory

This research developed a conceptual model from two existing models or methodologies which assisted the researched in development of a Security and Governance control framework. The model takes elements from TAM and PMT to develop a model that will take into account Risk, Threats and Vulnerabilities to determine the Perceived susceptibility. The usability of control and the ease of use of the controls will form the Security confidence which will assist together with the Perceived susceptibility to develop and Coping response or Propose ICS/SCADA framework.

7.4.2 Contribution to Global Knowledge

Aspects of this study was published as an academic journal in the *International Journal of Cyber Warfare and Terrorism* (IJCWT) in July 2016 (Pretorius & Van Niekerk, 2016) and the *10th International Conference on Cyber Warfare and Security* (ICCWS) on 24 and 25 March 2015 (Pretorius & Van Niekerk, 2015).

7.4.3 Contribution to Practice

This research also assessed the current practices of ICS/SCADA in South Africa, and developed a consolidated Security and Governance control framework aligned to threats, risks and vulnerabilities relevant to South Africa. The control framework will assist organisations in South Africa to mitigate the risks, threats and vulnerabilities related to their ICS/SCADA environments. Aspects of this study was presented at a practitioner conference, namely at the ISACA South Africa Annual Conference in August 2015 and well as at a KMPG CIO Agenda in June 2016.

7.5 Future work

From this stage, future work will include detailed breakdown of the controls as well as analysis of the practicality of implementation and further alignment to South African government legal requirements and international frameworks. Ongoing testing of the framework in other ICS/SCADA environments will be conducted to ensure generalisation and applicability of the framework. Repeat studies should also be performed at minimum every two years to monitor the progress or lack thereof. As mentioned in Section 7.3.5, security vendors need to improve the consistency of how vulnerabilities and threats are classified and reported. Future research on this could elaborate as to why different vendors use different terminology as well as how these terms can be grouped together for easy interpretation.

7.6 Limitations of the study

It was difficult to determine the exact population. The questionnaire was sent out to the broader community to see the responses. There might be an issue with convenience sampling as the implication would be that other respondents that could have responded have not been fully identified. There is inconsistency of report analysis from the various security vendors discussed in Section 5.2. This included inconsistency between categories which could lead to some bias towards certain vulnerabilities and threats and complicated the overall analysis. Although this might have a small implication on the study, this might impact someone in the industry trying to use various reports to determine the top vulnerabilities. They might wrongly place emphasis on controls for vulnerabilities that are not really the most prevalent.

7.7 Summary of Conclusions and Recommendations

This research explored the threat, vulnerabilities, risks and challenges related to the ICS/SCADA environment in South Africa. The study found that the factors (vulnerabilities and threats) influencing ICS/SCADA environments in South Africa are Patching, Monitoring, and Access control for vulnerabilities and Cross site scripting, Information Disclosure and Security Bypass as technical vulnerabilities. The other factor (threats) that influence ICS/SCADA in South Africa are Malware, Staff undertaking unintentional unauthorised actions and disgruntled staff. These factors could potentially cause distribution to operations and the business and ultimately lead to financial loss or possibly human life.

The state of ICS/SCADA is one of ungoverned and unsecure systems. Controls needs to be prioritised to focus on the top risks, threats and vulnerabilities. Although a majority of respondents have a governance framework in place, the controls are not consistently applied or operating effectively. The confident levels of the respondents are lower than it should be for the controls that have been implemented to mitigate the threats and vulnerabilities sufficiently.

A SCADA control framework was developed taking into account the COBIT and CPNI frameworks. The control framework gave prevalent controls to implement based on the Perceived susceptibility. The controls were prioritised to focus and address the top risks, threats and vulnerabilities based on the Perceived susceptibility. The control framework was developed with the high priority controls first. From the control framework, the controls were rearranged in a defence-in-depth model.

References

Abrams, M., & Weiss, J., 2008, *Malicious Control System Cyber Security Attack Case Study - Maroochy Water Services, Australia*, Computer Security Resource Centre, National Institute of Standards and Technology, viewed 30 December 2015, from http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf.

Acohido, B., 2015, *Improving Detection, Prevention and Response with Security Maturity Modeling*, SANS Institute InfoSec Reading Room, viewed 12 October 2016, from https://www.sans.org/reading-room/whitepapers/analyst/improving-detection-prevention-response-security-maturity-modeling-35985.

Alfreds, D., 2016, *SA business 'unprepared' for cybercrime*, Fin24.com, viewed 12 October 2016, from http://www.fin24.com/Tech/Cyber-Security/sa-business-unprepared-for-cybercrime-20160609.

Amoroso, E.G., 2013, *Cyber Attacks: Protecting National Infrastructure*, Student edition. Waltham, Butterworth-Heinemann., MA.

Andress, J., & Winterfield, S., 2011, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Waltham, Elsevier, MA.

Ashford, W., 2013, *Cyber attack shuts down Israeli toll road tunnel*, Computer Weekly, viewed 29 October 2015, from http://www.computerweekly.com/news/2240207924/Cyber-attack-shuts-down-Israeli-toll-road-tunnel.

BBC., 2014, *Hack attack causes 'massive damage' at steel works*, bbc.com, viewed 17 July 2015, from http://www.bbc.com/news/technology-30575104.

Beggs, C., & Warren, M., 2008, 'Safeguarding Australia from Cyberterrorism: A Proposed Cyber-terrorism SCADA Risk Framework for Australia', *Journal of Information Warfare* 7(1), 24-35.

Boehm, B. W., 1991, Software Risk Management: Principles and Practices, *IEEE Software* 8(1), 32-41.

Bowen, G. A., 2009, 'Document Analysis as a Qualitative Research Method', *Qualitative Research Journal* 9 (2), 27-40.

Brodsky, J., & Radvanovsky, R., 2013, 'Sociological and Cultural Aspects', in R. Radvanovsky & J. Brodsky (Eds.), *Handbook of SCADA/Control Systems Security*, CRC Press, Boca Raton, pp. 15-28.

Brook, C., 2015, *Polish Planes Grounded After Airline Hit With DDoS Attack,* Threatpost, viewed 22 June 2015, from https://threatpost.com/polish-planes-grounded-after-airline-hit-with-ddos-attack/113412.

Brook, C., 2016, *Nuclear Power Plant Disrupted by Cyber Attack*, Threatpost, viewed 13 October 2016, from https://threatpost.com/nuclear-power-plant-disrupted-by-cyber-attack/121216/.

Byres, E., 2012, *SCADA Security Basics: SCADA vs. ICS Terminology*, Tofino Security, viewed 6 September 2015, from https://www.tofinosecurity.com/blog/scada-security-basics-scada-vs-ics-terminology.

Carroll, J., 2014, *Computer Security, 2nd ed*. Butterworths, USA.

Cheng, W. & Shi-bo, W., 2014, 'User Behavior Research of Information Security Technology Based on TAM', *International Journal of Security and Its Applications* 8 (2), pp. 203-210.

Chileshe, G., & van Heerden, R., 2012, 'SCADA Systems in South Africa and their Vulnerabilities', in V. Lysenko (eds.), *Proceedings of the 7th International Conference of Information Warfare and Security*, Reading, Academic Publishing Limited, UK, pp. 90-97.

Chiloane, M., 2016, *Cybercrimes cost SA economy R35 Billion in 2015*, EWN, viewed 21 October 2016 from http://ewn.co.za/2016/07/06/Cybercrime-cost-SA-economy-R35-billion-in-2015.

Control Global., 2008, *ISA95 Levels for Enterprise Integration*, viewed 15 September 2015, from http://www.controlglobal.com/articles/2008/isa95enterpriselevels/.

CPNI., 2008, *Good practice guide Process Control and SCADA Security, Guide 1: Understand the business risk*, viewed 14 October 2015, from http://www.cpni.gov.uk/Documents/Publications/2008/2008024-GPG_SCADA_Business_Risk.pdf.

Cusimano., 2010, *DCS Virus Infection, Investigation and Response: A Case Study*. ICSJWG Fall Conference, viewed 6 January 6 2016, from https://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/F2010/Cusimano_ICSJWG%20DCS%20Virus%20Case%20Study.pdf .

Dahbur, K., Mohammad, B. & Tarakji, A. B., 2011, 'A survey of risks, threats and vulnerabilities in cloud computing', *Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications*, Amman, ACM, Jordan.

Davis, F. D.; Bagozzi, R. P.; Warshaw, P. R., 1989, *"User acceptance of computer technology: A comparison of two theoretical models*, Management Science 35, pp 982–1003.

Davis, G., 2015, *Cyber Security a top priority for state security*, Eyewitness News, viewed 8 June 2015, from http://ewn.co.za/2015/05/06/Mahlobo-Cyber-security-a-top-priority.

Day, J., 2015, *How did Ashley Madison get hacked?*, Quora, viewed 12 October 2016, from https://www.quora.com/How-did-Ashley-Madison-get-hacked

Dunn, J.E., 2013, *Hackers planted remote devices to smuggle drugs through Antwerp port*, Techworld.com, viewed 11 July 2015, from http://news.techworld.com/security/3474018/hackers-planted-remote-devices-to-smuggle-drugs-through-antwerp-port-europol-reveals/.

Elkind, P., 2015, *Inside the hack of the century*, Fortune, viewed 12 October 2016, from http://fortune.com/sony-hack-part-1/.

ENISA., 2011, *Protecting Industrial Control Systems: Recommendations for Europe and Member States*, European Network and Information Security Agency, viewed 13 October 2016, from https://www.enisa.europa.eu/publications/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states.

ESRI., 2014, *The Geospatial Approach to Cybersecurity: An Executive Overview*, viewed 12 October 2016, from http://downloads.esri.com/support/whitepapers/other_/geospatial-approach-cybersecurity.pdf.

Federal Bureau of Investigation, 2014, *2014 Internet Crime Report*, Internet Crime Compliant Centre, viewed 13 October 2016, from https://pdf.ic3.gov/2014_IC3Report.pdf

Fripp, C., 2016, *Anonymous hacks Armscor website with simple SQL injection*, htxt.africa, viewed 19 October 2016, from http://www.htxt.co.za/2016/07/12/armscor-website-hacked-sql-injection/

Government of Republic of South Africa, 2002a, *Electronic Communications and Transactions Act*, Act 25 of 2002, Pretoria.

Government of Republic of South Africa, 2002b, *Regulation of Interception of Communications and Provision of Communication-Related Information Act*, Act 70 of 2002, Pretoria.

Government of Republic of South Africa, 2013, *Protection of Personal Information Act*, Act 4 of 2013, Pretoria.

Government of Republic of South Africa, 2015, *Cybercrimes and Cybersecurity Bill*, Draft for Public Comment, Pretoria.

Groden, C., 2015, *Here's who's been hacked in the past two years*, Fortune, viewed 12 October 2016, from http://fortune.com/2015/10/02/heres-whos-been-hacked-in-the-past-two-years/.

Higgins, K.J., 2015, *State Trooper Vehicles Hacked*, Dark Reading, viewed 2 October 2015, from http://www.darkreading.com/attacks-breaches/state-trooper-vehicles-hacked-/d/d-id/1322415.

Howley, D., 2015, *The Biggest Computer Hack Attacks of the Last 5 Years*, Yahoo! Tech, viewed 12 October 2016, from https://www.yahoo.com/tech/the-biggest-computer-hack-attacks-of-the-last-5-125449860474.html.

Hubeschle, A., 2011, *The Dark Side of the Internet: Cybercrime*. Institute of Security Studies, viewed 12 October 2016, from http://www.issafrica.org/iss-today/the-dark-side-of-the-internet-cybercrime.

ISACA., 2012, *COBIT 5 for Information Security*, viewed 6 June 2016, from http://www.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf.

ISO/IEC., 2013, *ISO 27002:2013 Code of practice for information security controls*, Pretoria: SABS Standards Division.

IT News., 2016, *8.8 Million South Africans have fallen victim to cybercrime*, IT News Africa, viewed 21 October 2016, from http://www.itnewsafrica.com/2016/07/8-8-million-south-africans-have-fallen-victim-to-cybercrime/.

Jones, A., 2013, *Information Security Incident Management Procedures*, Heriot-Watt University, viewed 20 October 2016, from https://www.hw.ac.uk/documents/information-security-incident-management-procedures.pdf.

Jones, G., 2014, *South Africa neglects alarming effect of cybercrime,* BusinessLive, viewed 15 July 2015, from http://www.bdlive.co.za/business/2014/01/14/south-africa-neglects-alarming-effect-of-cybercrime.

Kaspersky., 2016, *Industrial Control Systems Vulnerabilities Statistics*, viewed 2 October 2016, from https://kas.pr/KL_ICS_vulnerabilities.

Kinnunen, S., 2016, ‘Exploring Determinants of different Information Security Behaviors’, Master’s thesis, University of Jyväskylä.

Kirk, J., 2009, *Virus Attacks Ministry of Defence*, CIO.co.uk, viewed 19 October 2016, from http://www.cio.co.uk/news/3460/virus-attacks-ministry-of-defence/.

Knapp, E. D., 2011, *Industrial Network Security*, Syngress, Waltham.

Kovacs, E., 2014, *Several Siemens Industrial Products Affected by ShellShock Bug*, Securityweek, viewed 13 October 2015, from http://www.securityweek.com/several-siemens-industrial-products-affected-shellshock-bug.

Kovacs, E., 2016, *BlackEnergy Malware Used in Ukraine Power Grid Attacks*, Securityweek, viewed 4 January 2016, from http://www.securityweek.com/blackenergy-group-uses-destructive-plugin-ukraine-attacks.

Krebs, B., 2014, *Target Hackers Broke in via HVAC Company*, Krebs on Security Blog, viewed 12 February 2016, from http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.

Krutz, R.L., 2006, *Securing SCADA Systems*, Wiley, Indianapolis.

Leyden, J., 2008, *Polish teen derails tram after hacking train network*, The Register, viewed 4 January 2016, from http://www.theregister.co.uk/2008/01/11/tram_hack/.

Leyden, J., 2012, *Saudi oil giant seals off network after mystery malware attack*, The Register, viewed 20 August 2015, from http://www.theregister.co.uk/2012/08/16/saudi_aramco_malware/.

MathBits, 2016, *Correlation Coefficient*, MathBits.com, viewed 4 November 2016, from http://mathbits.com/MathBits/TISection/Statistics2/correlation.htm

Miller, B., & Rowe, D.C., 2012, ‘A Survey of SCADA and Critical Infrastructure Incidents’, in *Proceedings of the 1st Annual conference on Research in information technology*, ACM, New York, pp. 51-56.

Mills, E., 2012, *Saudi Oil firm says 30,000 computers hit by virus*, CNet, viewed 4 September 2015, from http://news.cnet.com/8301-1009_3-57501066-83/saudi-oil-firm-says-30000-computers-hit-by-virus/.

Mkhwananzi, S., 2015, *Roads agency account hacked for R8.5m*, iol.co.za, viewed 12 October 2016, from http://www.iol.co.za/capetimes/roads-agency-account-hacked-for-r8-5m-1.1928834.

Nakashima, E. & Warrick, J., 2012, *Stuxnet was the work of U.S. and Israel, officials say*, Washington Post, viewed 7 June 2015, from http://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

Nakashima, E., Miller, G. & Tate, J., 2012, *U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say*, Washington Post, viewed 21 June 2015, from http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html.

National Cybersecurity and Communications Integration Center., 2014, *ICS-CERT Monitor May-August 2014*, US Department of Homeland Security, viewed 14 October 2015, https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_May-Aug2014.pdf.

National Cybersecurity and Communications Integration Center., 2015, *ICS-CERT Monitor November-December 2015*, US Department of Homeland Security, viewed 2 October 2016, https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Nov-Dec2015_S508C.pdf.

Neitzel, L., & Huba, B., 2014, *Top ten differences between ICS and IT cybersecurity*, International Society of Automation Intech magazine, viewed 9 September 2015, from https://www.isa.org/standards-and-publications/isa-publications/intech-magazine/2014/may-jun/features/cover-story-top-ten-differences-between-ics-and-it-cybersecurity/.

Norton Rose Fulbright., 2012, *Cyber crime at a tipping point*, viewed 14 October 2016, from http://www.nortonrosefulbright.com/knowledge/publications/72312/cyber-crime-at-a-tipping-point.

Online Tenders., 2014, viewed 9 September 2015, *eThekwini/Durban Electricity SCADA audit*, onlinetenders.co.za, from https://www.onlinetenders.co.za/show-tender.aspx?s=s&tid=591811.

Paganini, P., 2013, *Improving SCADA System Security*, Infosec Institute, viewed 14 October 2015, from http://resources.infosecinstitute.com/improving-scada-system-security/.

Paganini, P., 2016, *Modern railroad systems vulnerable to cyber attacks*, Security Affairs, viewed 4 January 2016, from http://securityaffairs.co/wordpress/43196/hacking/railroad-systems-vulnerabilities.html.

Patrick, H., 2016, ‘Security information flow in the public sector: KZN Health and Education’, PhD Thesis, School of Management, Information and Governance, University of KwaZulu-Natal.

Patton, M.L., 2005, *Understanding research methods*, Pyrczak, Glendale, California.

Pella, B., 2013, ‘Obsolescence and Procurement of SCADA’, in R. Radvanovsky & J. Brodsky (Eds.), *Handbook of SCADA/Control Systems Security*, CRC Press, Boca Raton, pp. 245-254.

Pretorius, B., & Van Niekerk, B., 2016, ‘Cyber-Security for ICS/SCADA: A South African Perspective’, *International Journal of Cyber Warfare and Terrorism (IJCWT)* 6(3), pp. 1 – 16, viewed on 12 September 2016, from http://www.igi-global.com/article/cyber-security-for-icsscada/159880.

Pretorius, B., Van Niekerk, B., 2015, ‘Cyber-Security and Governance for ICS/SCADA in South Africa’, in *The Proceedings of the 10th International Conference on Cyber Warfare and Security*, Academic Conferences and Publishing International Limited, UK, pp 241-251.

Project SHINE., 2014, *Project SHINE (SHodan INtelligence Extraction) Findings Report*, scadahacker.com, viewed 13 October 2016, from https://scadahacker.com/library/Documents/ICS_Vulnerabilities/Infracritical%20-%20Project%20SHINE%20Findings%20Report%20-%20Oct%202014.pdf.

Quinn, B., Arthur, C., 2011, *PlayStation Network hackers access data of 77 million users*, The guardian, viewed 12 October 2016, from https://www.theguardian.com/technology/2011/apr/26/playstation-network-hackers-data.

Rasool, F., 2012, *KPMG investigates Postbank theft*, ITWeb Security, viewed 12 October 2016, from http://www.itweb.co.za/index.php?option=com_content&view=article&id=50919:kpmg-investigates-postbank-theft&catid=234.

Rhodes-Ousley, M., 2013, *The Complete Reference: Information Security 2nd edition*, The McGraw-Hill Companies.

Riley, M., Elgin, B., Lawrence, D., Matlack, C., 2014, *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, Bloomberg, viewed 12 October 2016, from http://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data#p4.

Roane, B., 2013, *SAPS website hacked*, iol.co.za, viewed 12 October 2016, from http://www.iol.co.za/news/crime-courts/saps-website-hacked-1520042.

Robertson, J., & Riley, M., 2014, *Mysterious ’08 Turkey Pipeline Blast Opened New Cyberwar*, Bloomberg, viewed 5 January 2016, from http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.

Rodionov, E., 2012, *Interconnection of Gauss with Stuxnet, Duqu & Flame*, ESET Blog, viewed 22 August 2015, from http://blog.eset.com/2012/08/15/interconnection-of-gauss-with-stuxnet-duqu-flame.

Rogers, R.W., 1975, 'A protections motivation theory of fear appeals and attitude change', *Journal of Psychology* 91, pp 93 - 114.

Rogers, R.W., 1983, 'Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation', in J.T. Cacioppo and R.E. Petty (eds), *Social Psychophysiology: A Source Book*, pp 153 -176, Guilford Press, New York.

RSA., 2014, *RSA Security Awareness Program*, EMC, viewed 12 November 2015, from http://www.emc.com/collateral/data-sheet/h13289-ds-rsa-security-awareness-program.pdf.

Rubin, A., 2008, *Practioner's guide to using research for evidence-based practice*, John Wiley, Hoboken, New Jersey.

SANS Institute., 2006, *An Introduction to Information System Risk Management*, viewed 12 October 2016, from https://www.sans.org/reading-room/whitepapers/auditing/introduction-information-system-risk-management-1204.

SANS Institute., 2012, *Insider Threat Risk Formula: Survivability, Risk and threat*, viewed 12 October 2016, from https://cyber-defense.sans.org/blog/2012/10/23/insider-threat-risk-formula-survivability-risk-and-threat.

SANS Institute., 2013, *Results of the SANS SCADA Security Survey*, viewed 14 October 2015, from http://www.sans.org/reading-room/whitepapers/analyst/results-scada-security-survey-35135.

SANS Institute., 2014, *Breaches on the Rise in Control Systems: A SANS Survey*, viewed 14 September 2015, from https://www.sans.org/reading-room/whitepapers/analyst/breaches-rise-control-systems-survey-34665.

SANS Institute., 2015, *The State of Security in Control Systems Today*, viewed 14 September 2016, from https://www.sans.org/reading-room/whitepapers/analyst/state-security-control-systems-today-36042.

SANS Institute., 2016a, *SANS 2016 State of ICS Security Survey*, viewed 14 September 2016, from https://www.sans.org/reading-room/whitepapers/analyst/2016-state-ics-security-survey-37067.

SANS Institute., 2016b, *CIS Critical Security Controls*, viewed 20 July 2016, from https://www.sans.org/critical-security-controls.

Saunders, M., & Tosey, P., 2013, *The Layers of Research Design*, Rapport, Winter 2012/2013, viewed 13 July 2015, from https://www.academia.edu/4107831/The_Layers_of_Research_Design.

SCADA Strangelove., 2015, *SCADAPASS #32C3 Release,* SCADA.SL, viewed 2 August 2016, from http://scadastrangelove.blogspot.co.za/2015/12/scadapass.html?_sm_au_=i5VvZvHQ66NjvPJf.

Sentrillion., 2012, *Safeguarding your information with a "Defense in Depth" architecture,* viewed 10 October 2016, from http://www.sentrillion.com/cyber/secure-architecture.php.

Shahriar, H. & Zulkernine, M., 2012, 'Mitigating program security vulnerabilities: Approaches and challenges', *ACM* 44**,** 1-46, viewed 10 October 2016, from http://dl.acm.org/citation.cfm?id=2187673.

Solomon, M., 2016, *Anonymous Africa cyber hackers shut down Gupta-linked websites*, Mail and Guardian, viewed 12 October 2016, from http://mg.co.za/article/2016-06-15-anonymous-africa-cyber-hackers-shutdown-gupta-linked-websites.

Sommestad, T., Karlzen, H., & Hallberg, J., 2015, 'A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour', *International Journal of Information Security and Privacy* 9 (1), pp. 26 – 46.

Stamp, J., Dillinger, J., Young, W., & DePoy.J., 2003, *Common Vulnerabilities in Critical Infrastructure Control Systems*, Sandia Corporation, Albuquerque.

Stouffer, K., Falco, J., Kent, K., 2006, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security*, National Institute of Standards and Technology Special Publication 800-82.

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

Susanto, H., Almunawar, M. N. & Tuan, Y. C., 2012, 'Information Security Challenge and Breaches: Novelty Approach on Measuring ISO 27001 Readiness Level', *International Journal of Engineering and Technology* 2, 67-75.

Symantec., 2014a, *2014 Internet Security Threat Report, Volume 19*, viewed 14 October 2015, from http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf.

Symantec., 2014b, *2014 Internet Security Threat Report, Volume 19, Supplemental Data*, viewed 14 October 2014, from http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_appendices_v19_221284438.en-us.pdf.

Symantec., 2015, *2015 Internet Security Threat Report, Volume 20, Supplemental Data*, viewed 6 January 2016, from https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347931_GA-internet-security-threat-report-volume-20-2015-appendices.pdf.

Symantec., 2016a, *2016 Internet Security Threat Report, Volume 21*, viewed 6 July 2016, from https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf.

Symantec., 2016b, *2016 Internet Security Threat Report, Volume 21, Appendices*, viewed 6 July 2016, from https://www.symantec.com/content/.../symantec/.../reports/istr-21-2016-appendices-en.pdf.

U.S. Department of Energy., 2007, *21 Steps to Improve Cyber Security of SCADA Networks*, Infrastructure Security and Energy Restoration Committee, viewed 25 April 2016, from www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf.

Van Zyl, G., 2016, *Anonymous 'hacks' Armscor website*, Fin24.com, viewed 12 October 2016, from http://www.fin24.com/Tech/News/anonymous-hacks-armscor-website-20160712.

Vermeulen, J., 2016a, *Anonymous hacks SA government database*, Mybroadband.co.za, viewed 18 October 2016, from http://mybroadband.co.za/news/security/155030-anonymous-hacks-sa-government-database.html.

Vermeulen, J., 2016b, *This is how I took down the SABC: Anonymous hacker*, Mybroadband.co.za, viewed 12 October 2016, from http://mybroadband.co.za/news/security/168303-this-is-how-i-took-down-the-sabc-anonymous-hacker.html.

Vicente, A., 2016, *SA is top cyber crime target in Africa*, ITWeb, viewed 21 October 2016, from http://www.itweb.co.za/index.php?option=com_content&view=article&id=150566.

Wagstaff, J., 2014, *All at sea: global shipping fleet exposed to hacking threat*, Reuters, viewed 24 April 2016, from http://www.reuters.com/article/2014/04/24/tech-cybersecurity-shipping-graphic-pix-idUSL3N0NG0GP20140424.

Walker, D., 2014, *'Havex' malware strikes industrial sector via watering hole attacks*, SC Magazine, viewed 27 July 2015, from http://www.scmagazine.com/havex-malware-strikes-industrial-sector-via-watering-hole-attacks/article/357875/.

Weiss G., 2008, *The Farewell dossier: Duping the Soviets*, Central Intelligence Agency, viewed 6 September 2015, from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm.

Whitman, M.E., & Mattord, H.J., 2012, *Principles of Information Security 4th edition*, Course Technology Cengage Learning, Boston.

Willsher, K., 2009, *French Fighter Planes Grounded by Computer Virus*, The Telegraph, viewed 19 October 2015, from http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html.

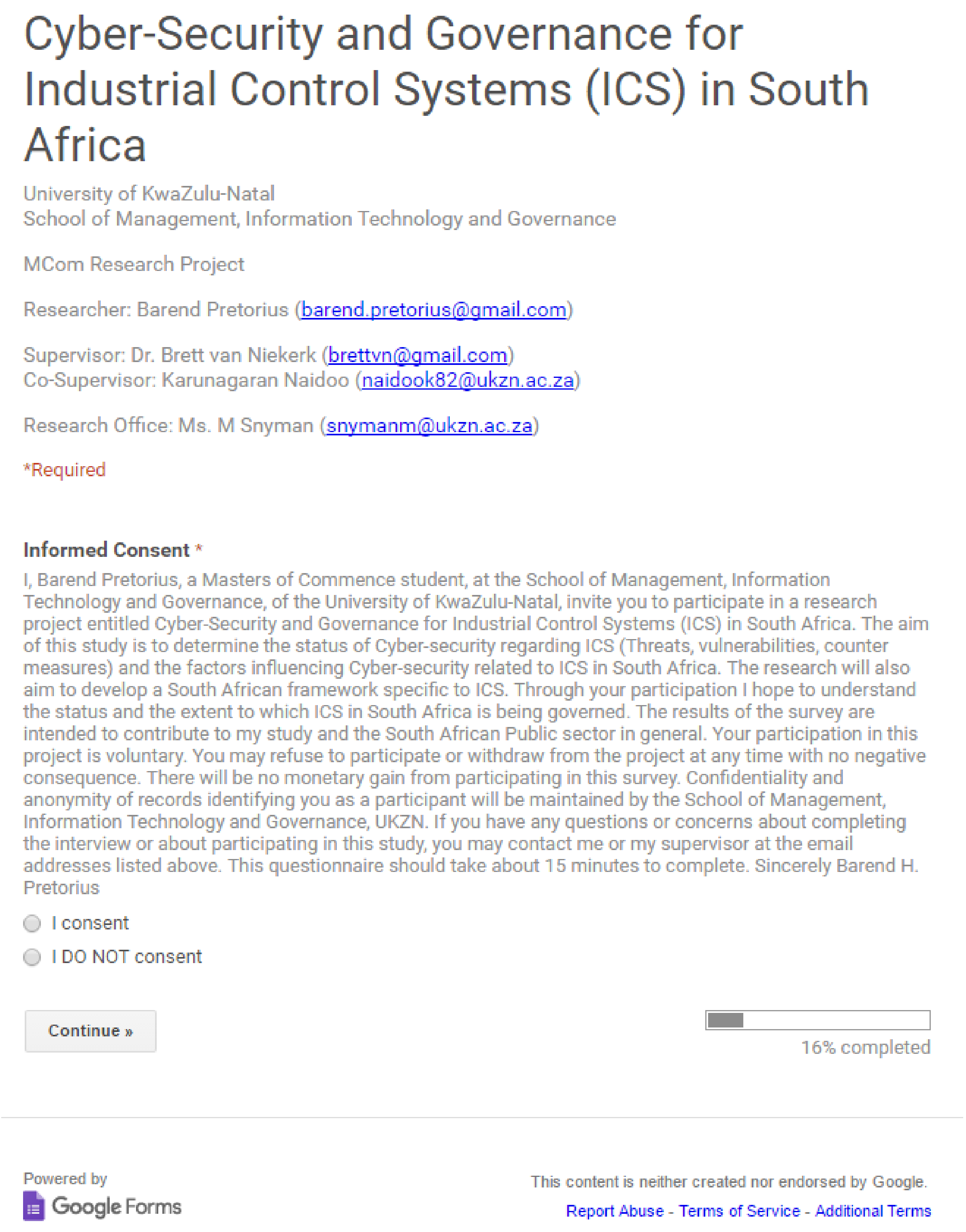
Wolfpack., 2016, *Critical Information Infrastructure Protection Report*, viewed 15 July 2016, from https://wolfpackrisk.com/wp-content/uploads/2016/05/CIIP_Full_Report-final.pdf.

Wyld, B., 2004, *The Fear Factor*, The Age, viewed 31 July 2015, from http://www.theage.com.au/articles/2004/07/16/1089694549469.html.

Yin, R.K., 2009, *Case study research: Design and methods*, Nelson Press. Los Angeles.

Zetter, L., 2015, *Is it Possible for Passengers to Hack Commercial Aircraft*, Wired, viewed 5 January 2016, from http://www.wired.com/2015/05/possible-passengers-hack-commercial-aircraft/.

Appendix A Questionnaire



Cyber-Security and Governance for Industrial Control Systems (ICS) in South Africa

University of KwaZulu-Natal
School of Management, Information Technology and Governance

MCom Research Project

Researcher: Barend Pretorius (barend.pretorius@gmail.com)

Supervisor: Dr. Brett van Niekerk (brettvn@gmail.com)
Co-Supervisor: Karunagaran Naidoo (naidook82@ukzn.ac.za)

Research Office: Ms. M Snyman (snymanm@ukzn.ac.za)

*Required

Informed Consent *

I, Barend Pretorius, a Masters of Commence student, at the School of Management, Information Technology and Governance, of the University of KwaZulu-Natal, invite you to participate in a research project entitled Cyber-Security and Governance for Industrial Control Systems (ICS) in South Africa. The aim of this study is to determine the status of Cyber-security regarding ICS (Threats, vulnerabilities, counter measures) and the factors influencing Cyber-security related to ICS in South Africa. The research will also aim to develop a South African framework specific to ICS. Through your participation I hope to understand the status and the extent to which ICS in South Africa is being governed. The results of the survey are intended to contribute to my study and the South African Public sector in general. Your participation in this project is voluntary. You may refuse to participate or withdraw from the project at any time with no negative consequence. There will be no monetary gain from participating in this survey. Confidentiality and anonymity of records identifying you as a participant will be maintained by the School of Management, Information Technology and Governance, UKZN. If you have any questions or concerns about completing the interview or about participating in this study, you may contact me or my supervisor at the email addresses listed above. This questionnaire should take about 15 minutes to complete. Sincerely Barend H. Pretorius

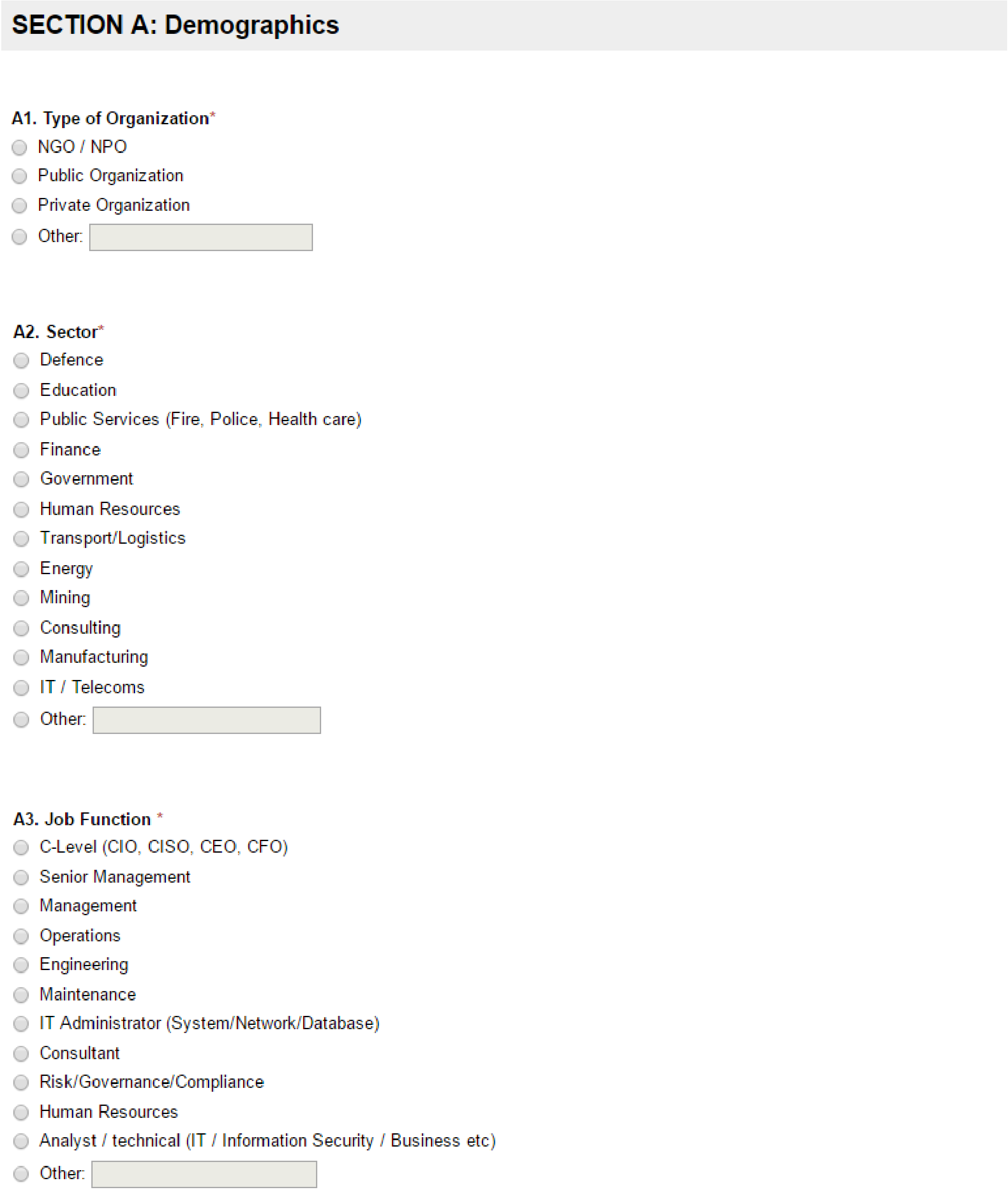
○ I consent

○ I DO NOT consent

16% completed

This content is neither created nor endorsed by Google.

QUESTIONNAIRE



SECTION A: Demographics

A1. Type of Organization*

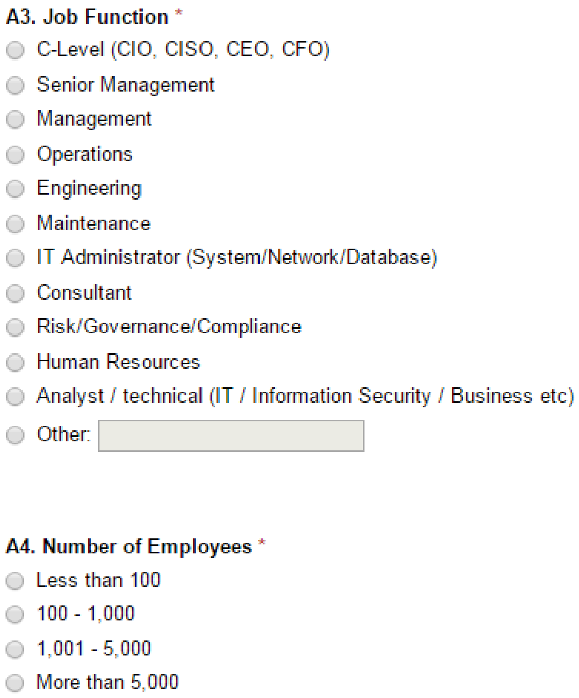
○ NGO / NPO
○ Public Organization
○ Private Organization
○ Other:

A2. Sector*

○ Defence
○ Education
○ Public Services (Fire, Police, Health care)
○ Finance
○ Government
○ Human Resources
○ Transport/Logistics
○ Energy
○ Mining
○ Consulting
○ Manufacturing
○ IT / Telecoms
○ Other:

A3. Job Function *

○ C-Level (CIO, CISO, CEO, CFO)
○ Senior Management
○ Management
○ Operations
○ Engineering
○ Maintenance
○ IT Administrator (System/Network/Database)
○ Consultant
○ Risk/Governance/Compliance
○ Human Resources
○ Analyst / technical (IT / Information Security / Business etc)
○ Other:



A3. Job Function *

○ C-Level (CIO, CISO, CEO, CFO)

○ Senior Management

○ Management

○ Operations

○ Engineering

○ Maintenance

○ IT Administrator (System/Network/Database)

○ Consultant

○ Risk/Governance/Compliance

○ Human Resources

○ Analyst / technical (IT / Information Security / Business etc)

○ Other: ________

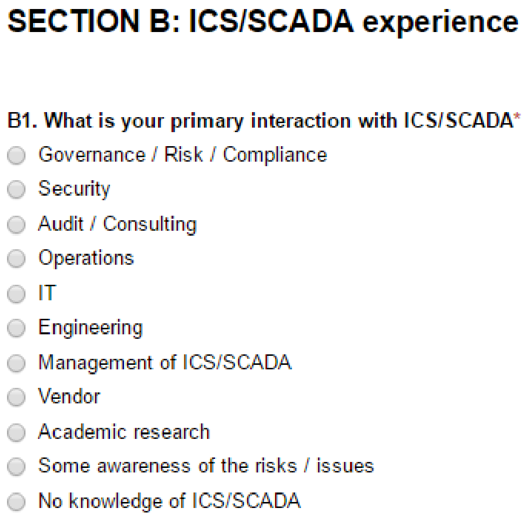
A4. Number of Employees *

○ Less than 100

○ 100 - 1,000

○ 1,001 - 5,000

○ More than 5,000



SECTION B: ICS/SCADA experience

B1. What is your primary interaction with ICS/SCADA*

○ Governance / Risk / Compliance

○ Security

○ Audit / Consulting

○ Operations

○ IT

○ Engineering

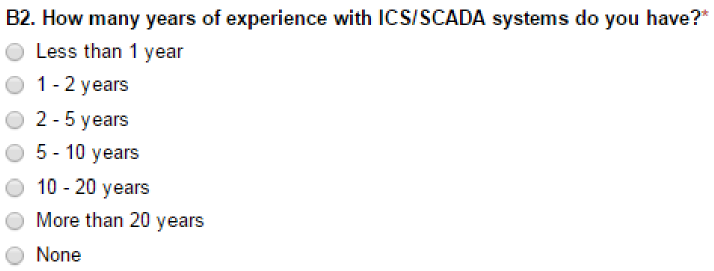
○ Management of ICS/SCADA

○ Vendor

○ Academic research

○ Some awareness of the risks / issues

○ No knowledge of ICS/SCADA



B2. How many years of experience with ICS/SCADA systems do you have?*

○ Less than 1 year

○ 1 - 2 years

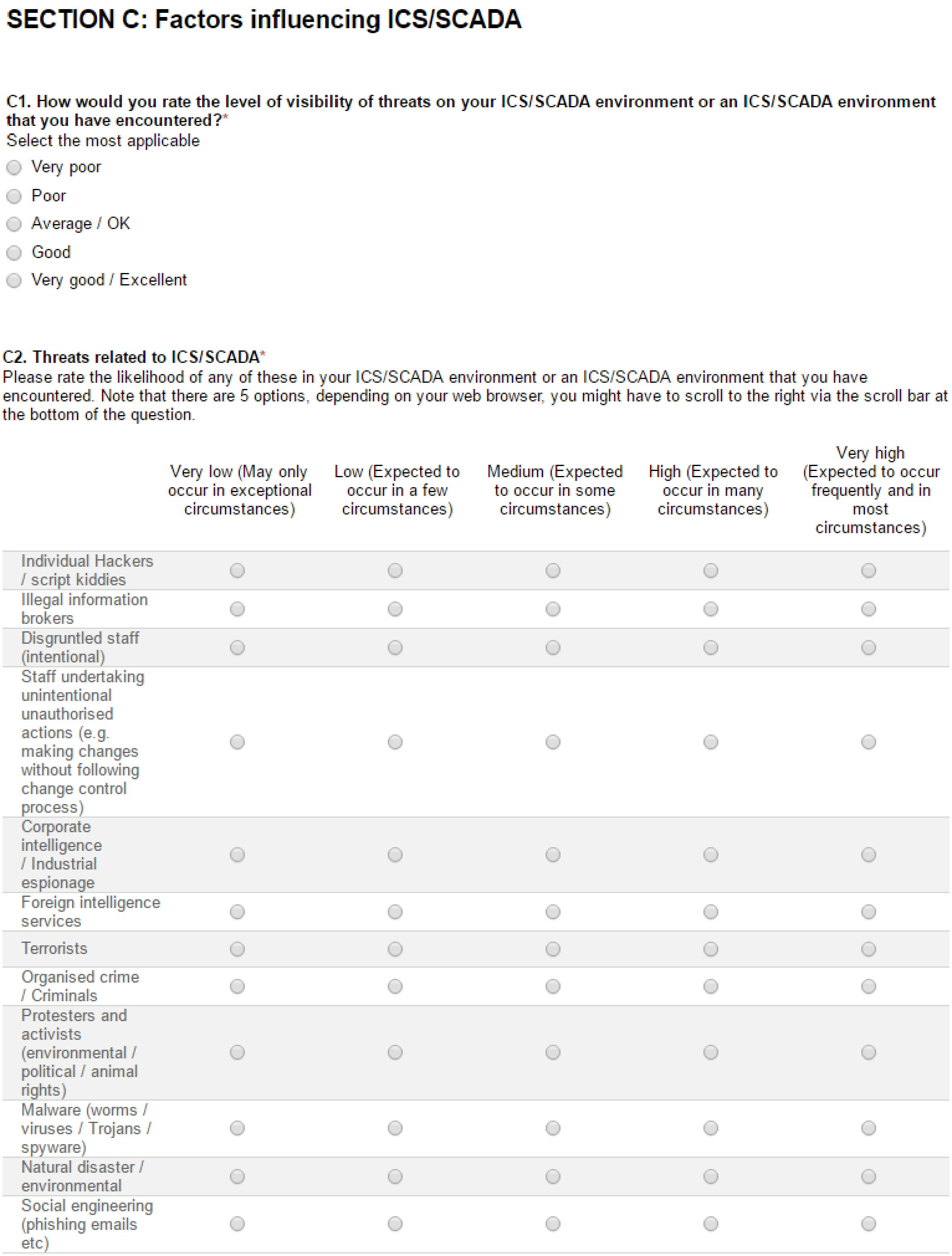
○ 2 - 5 years

○ 5 - 10 years

○ 10 - 20 years

○ More than 20 years

○ None



SECTION C: Factors influencing ICS/SCADA

C1. How would you rate the level of visibility of threats on your ICS/SCADA environment or an ICS/SCADA environment that you have encountered?*
Select the most applicable

○ Very poor

○ Poor

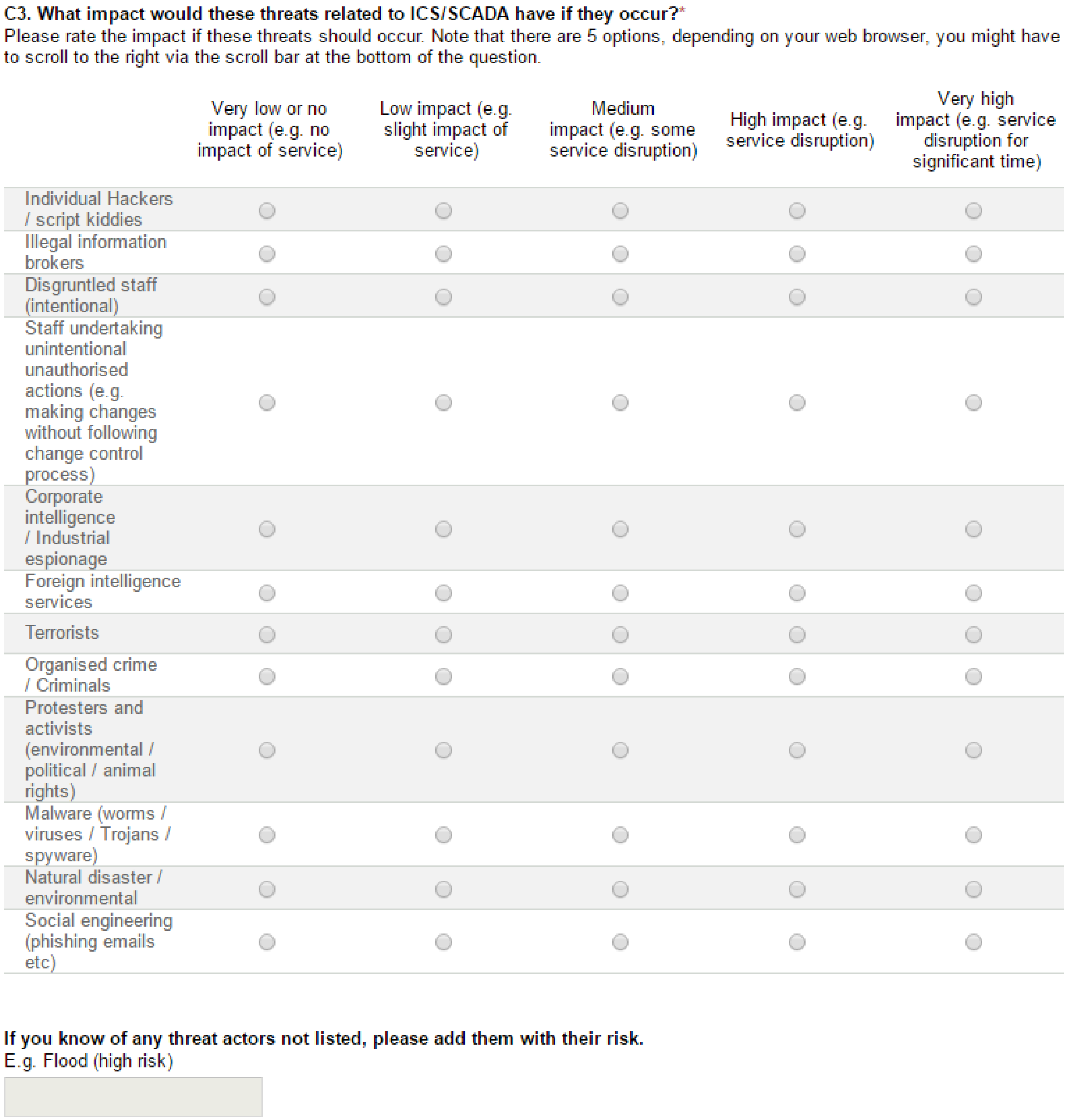
○ Average / OK

○ Good

○ Very good / Excellent

C2. Threats related to ICS/SCADA*
Please rate the likelihood of any of these in your ICS/SCADA environment or an ICS/SCADA environment that you have encountered. Note that there are 5 options, depending on your web browser, you might have to scroll to the right via the scroll bar at the bottom of the question.

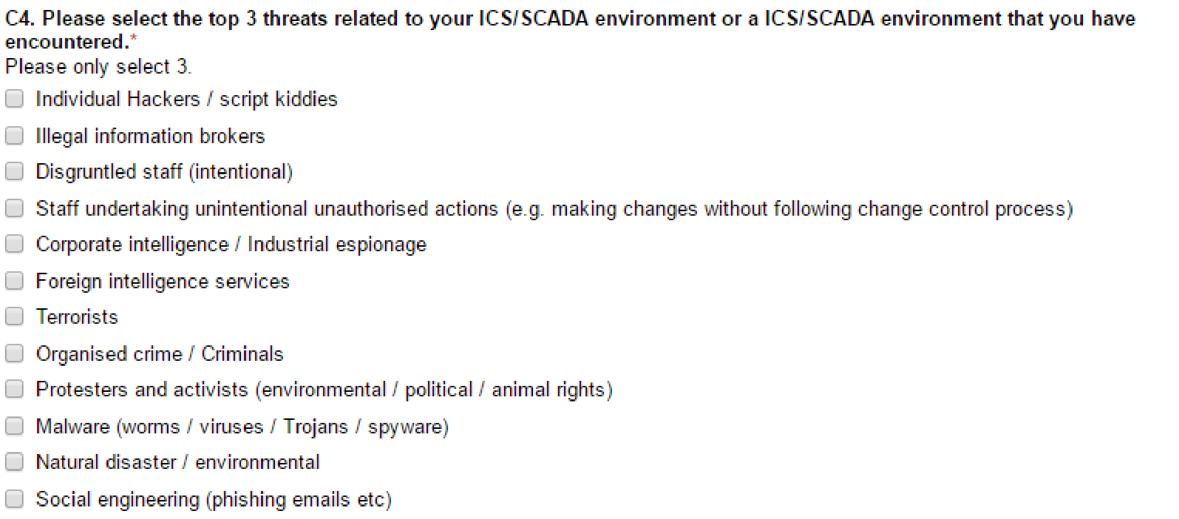
	Very low (May only occur in exceptional circumstances)	Low (Expected to occur in a few circumstances)	Medium (Expected to occur in some circumstances)	High (Expected to occur in many circumstances)	Very high (Expected to occur frequently and in most circumstances)
Individual Hackers / script kiddies	○	○	○	○	○
Illegal information brokers	○	○	○	○	○
Disgruntled staff (intentional)	○	○	○	○	○
Staff undertaking unintentional unauthorised actions (e.g. making changes without following change control process)	○	○	○	○	○
Corporate intelligence / Industrial espionage	○	○	○	○	○
Foreign intelligence services	○	○	○	○	○
Terrorists	○	○	○	○	○
Organised crime / Criminals	○	○	○	○	○
Protesters and activists (environmental / political / animal rights)	○	○	○	○	○
Malware (worms / viruses / Trojans / spyware)	○	○	○	○	○
Natural disaster / environmental	○	○	○	○	○
Social engineering (phishing emails etc)	○	○	○	○	○



C3. What impact would these threats related to ICS/SCADA have if they occur?*
Please rate the impact if these threats should occur. Note that there are 5 options, depending on your web browser, you might have to scroll to the right via the scroll bar at the bottom of the question.

	Very low or no impact (e.g. no impact of service)	Low impact (e.g. slight impact of service)	Medium impact (e.g. some service disruption)	High impact (e.g. service disruption)	Very high impact (e.g. service disruption for significant time)
Individual Hackers / script kiddies	○	○	○	○	○
Illegal information brokers	○	○	○	○	○
Disgruntled staff (intentional)	○	○	○	○	○
Staff undertaking unintentional unauthorised actions (e.g. making changes without following change control process)	○	○	○	○	○
Corporate intelligence / Industrial espionage	○	○	○	○	○
Foreign intelligence services	○	○	○	○	○
Terrorists	○	○	○	○	○
Organised crime / Criminals	○	○	○	○	○
Protesters and activists (environmental / political / animal rights)	○	○	○	○	○
Malware (worms / viruses / Trojans / spyware)	○	○	○	○	○
Natural disaster / environmental	○	○	○	○	○
Social engineering (phishing emails etc)	○	○	○	○	○

If you know of any threat actors not listed, please add them with their risk.
E.g. Flood (high risk)



C4. Please select the top 3 threats related to your ICS/SCADA environment or a ICS/SCADA environment that you have encountered.*

Please only select 3.

□ Individual Hackers / script kiddies

□ Illegal information brokers

□ Disgruntled staff (intentional)

□ Staff undertaking unintentional unauthorised actions (e.g. making changes without following change control process)

□ Corporate intelligence / Industrial espionage

□ Foreign intelligence services

□ Terrorists

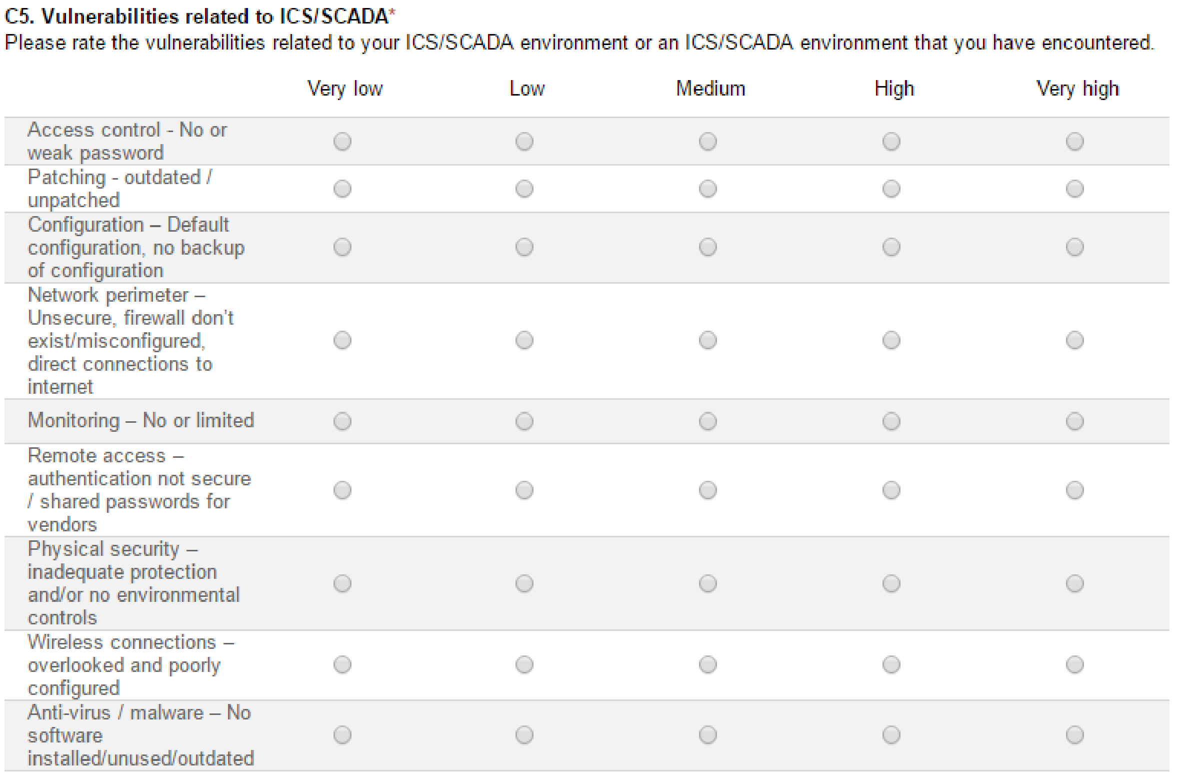
□ Organised crime / Criminals

□ Protesters and activists (environmental / political / animal rights)

□ Malware (worms / viruses / Trojans / spyware)

□ Natural disaster / environmental

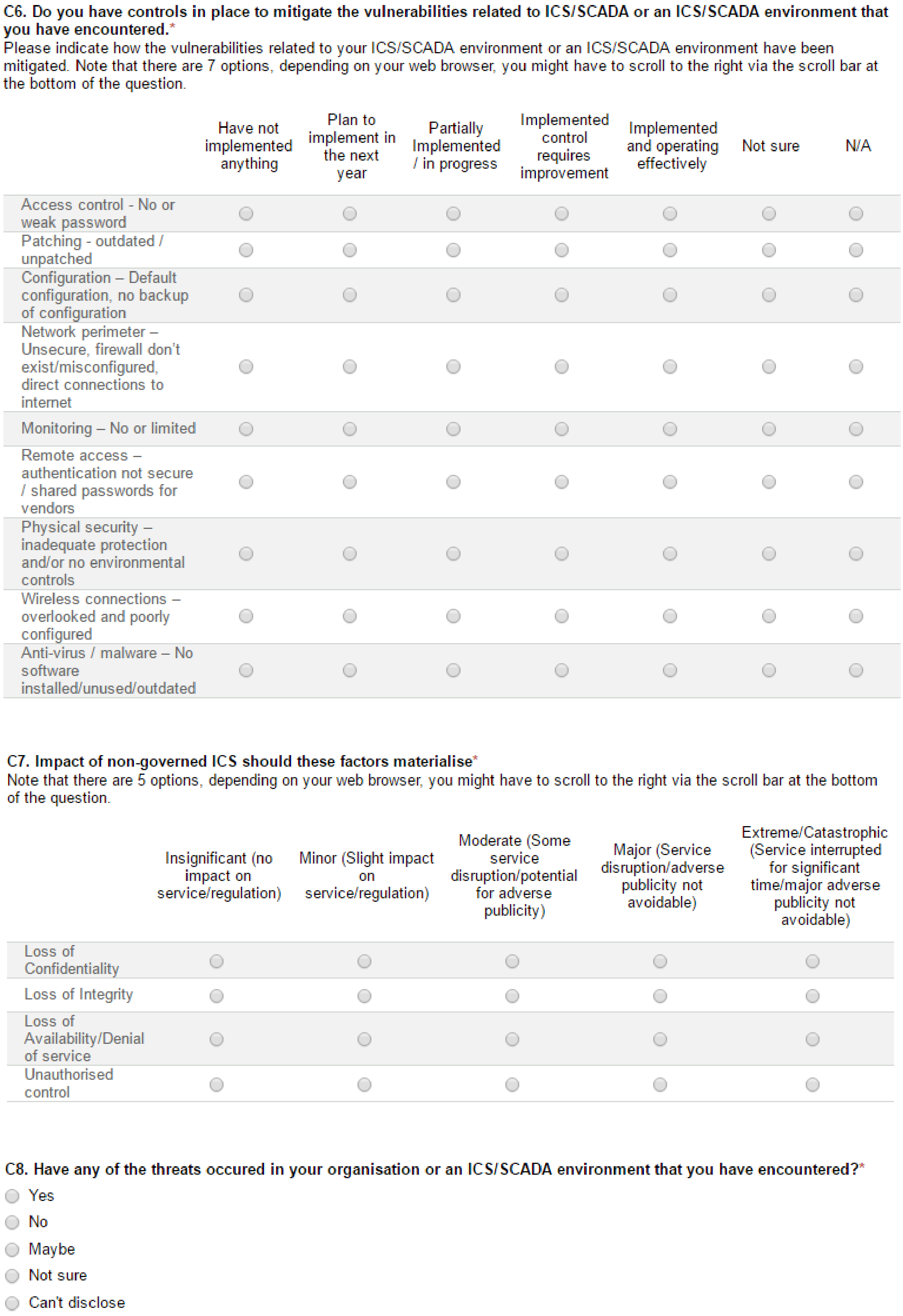
□ Social engineering (phishing emails etc)



C5. Vulnerabilities related to ICS/SCADA*

Please rate the vulnerabilities related to your ICS/SCADA environment or an ICS/SCADA environment that you have encountered.

	Very low	Low	Medium	High	Very high
Access control - No or weak password	○	○	○	○	○
Patching - outdated / unpatched	○	○	○	○	○
Configuration – Default configuration, no backup of configuration	○	○	○	○	○
Network perimeter – Unsecure, firewall don't exist/misconfigured, direct connections to internet	○	○	○	○	○
Monitoring – No or limited	○	○	○	○	○
Remote access – authentication not secure / shared passwords for vendors	○	○	○	○	○
Physical security – inadequate protection and/or no environmental controls	○	○	○	○	○
Wireless connections – overlooked and poorly configured	○	○	○	○	○
Anti-virus / malware – No software installed/unused/outdated	○	○	○	○	○



C6. Do you have controls in place to mitigate the vulnerabilities related to ICS/SCADA or an ICS/SCADA environment that you have encountered.*

Please indicate how the vulnerabilities related to your ICS/SCADA environment or an ICS/SCADA environment have been mitigated. Note that there are 7 options, depending on your web browser, you might have to scroll to the right via the scroll bar at the bottom of the question.

	Have not implemented anything	Plan to implement in the next year	Partially Implemented / in progress	Implemented control requires improvement	Implemented and operating effectively	Not sure	N/A
Access control - No or weak password	○	○	○	○	○	○	○
Patching - outdated / unpatched	○	○	○	○	○	○	○
Configuration – Default configuration, no backup of configuration	○	○	○	○	○	○	○
Network perimeter – Unsecure, firewall don't exist/misconfigured, direct connections to internet	○	○	○	○	○	○	○
Monitoring – No or limited	○	○	○	○	○	○	○
Remote access – authentication not secure / shared passwords for vendors	○	○	○	○	○	○	○
Physical security – inadequate protection and/or no environmental controls	○	○	○	○	○	○	○
Wireless connections – overlooked and poorly configured	○	○	○	○	○	○	○
Anti-virus / malware – No software installed/unused/outdated	○	○	○	○	○	○	○

C7. Impact of non-governed ICS should these factors materialise*

Note that there are 5 options, depending on your web browser, you might have to scroll to the right via the scroll bar at the bottom of the question.

	Insignificant (no impact on service/regulation)	Minor (Slight impact on service/regulation)	Moderate (Some service disruption/potential for adverse publicity)	Major (Service disruption/adverse publicity not avoidable)	Extreme/Catastrophic (Service interrupted for significant time/major adverse publicity not avoidable)
Loss of Confidentiality	○	○	○	○	○
Loss of Integrity	○	○	○	○	○
Loss of Availability/Denial of service	○	○	○	○	○
Unauthorised control	○	○	○	○	○

C8. Have any of the threats occured in your organisation or an ICS/SCADA environment that you have encountered?*

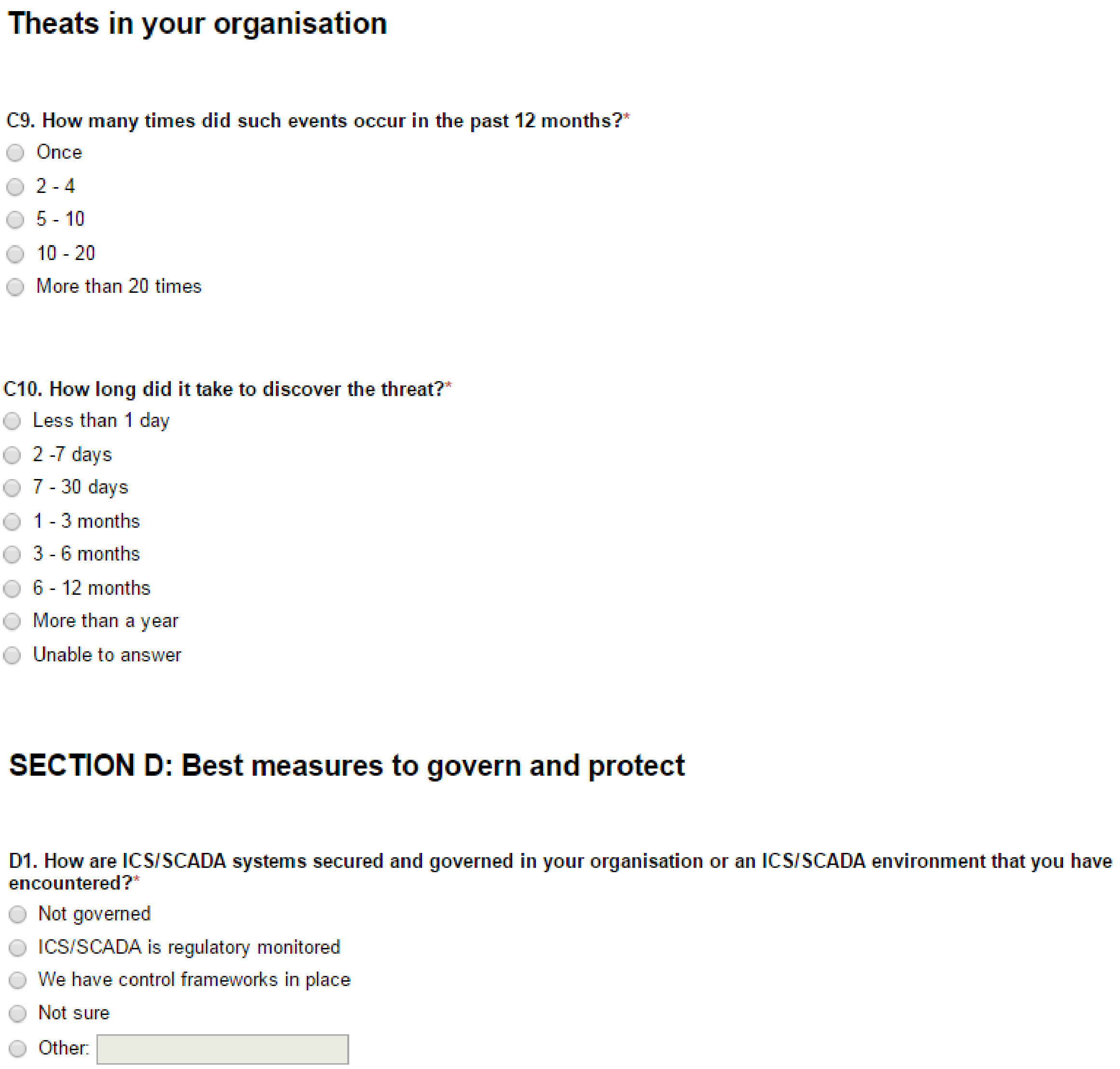
○ Yes

○ No

○ Maybe

○ Not sure

○ Can't disclose



Theats in your organisation

C9. How many times did such events occur in the past 12 months?*

○ Once
○ 2 - 4
○ 5 - 10
○ 10 - 20
○ More than 20 times

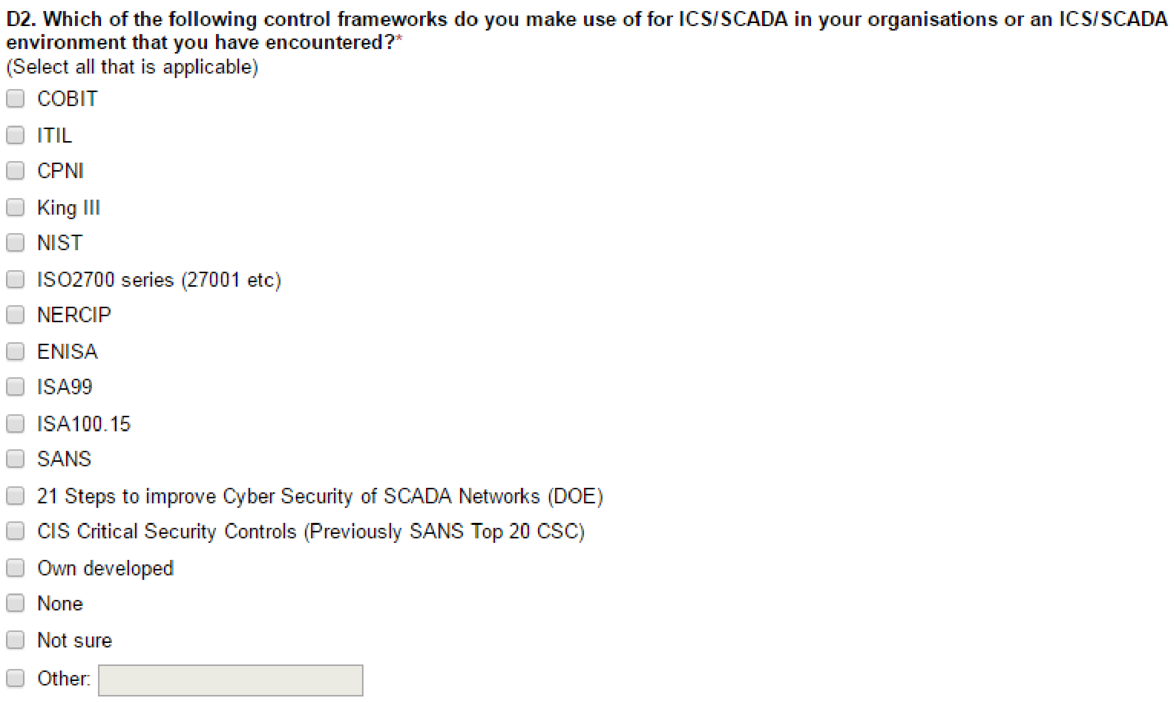
C10. How long did it take to discover the threat?*

○ Less than 1 day
○ 2 -7 days
○ 7 - 30 days
○ 1 - 3 months
○ 3 - 6 months
○ 6 - 12 months
○ More than a year
○ Unable to answer

SECTION D: Best measures to govern and protect

D1. How are ICS/SCADA systems secured and governed in your organisation or an ICS/SCADA environment that you have encountered?*

○ Not governed
○ ICS/SCADA is regulatory monitored
○ We have control frameworks in place
○ Not sure
○ Other: ▭



D2. Which of the following control frameworks do you make use of for ICS/SCADA in your organisations or an ICS/SCADA environment that you have encountered?*
(Select all that is applicable)

□ COBIT

□ ITIL

□ CPNI

□ King III

□ NIST

□ ISO2700 series (27001 etc)

□ NERCIP

□ ENISA

□ ISA99

□ ISA100.15

□ SANS

□ 21 Steps to improve Cyber Security of SCADA Networks (DOE)

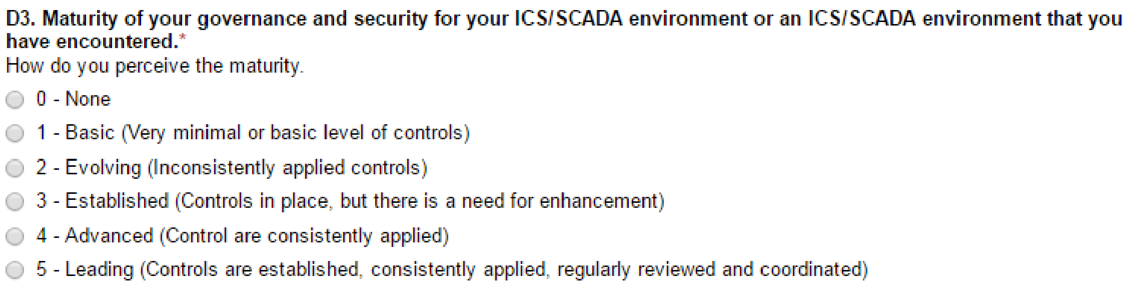
□ CIS Critical Security Controls (Previously SANS Top 20 CSC)

□ Own developed

□ None

□ Not sure

□ Other: ________



D3. Maturity of your governance and security for your ICS/SCADA environment or an ICS/SCADA environment that you have encountered.*
How do you perceive the maturity.

○ 0 - None

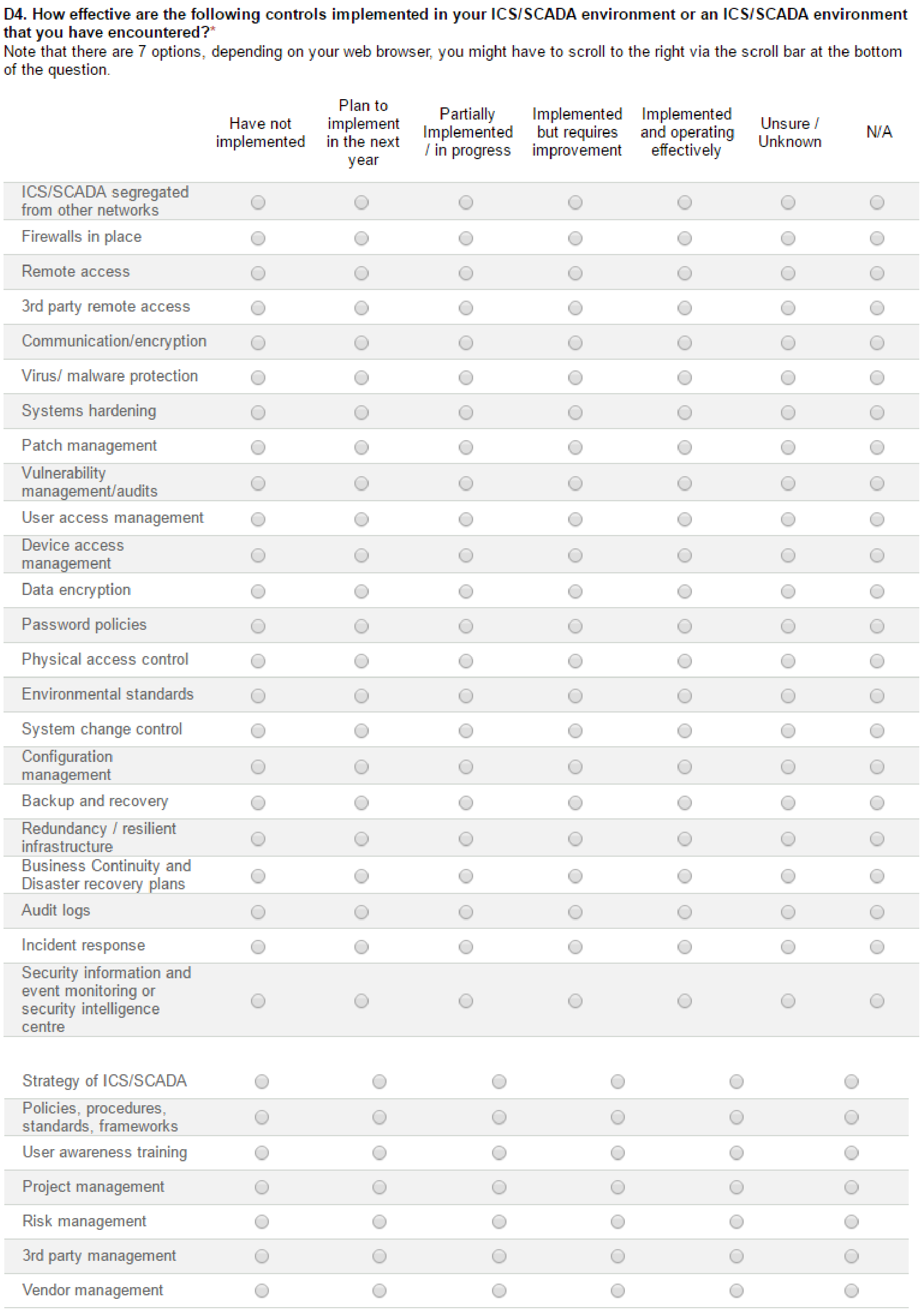
○ 1 - Basic (Very minimal or basic level of controls)

○ 2 - Evolving (Inconsistently applied controls)

○ 3 - Established (Controls in place, but there is a need for enhancement)

○ 4 - Advanced (Control are consistently applied)

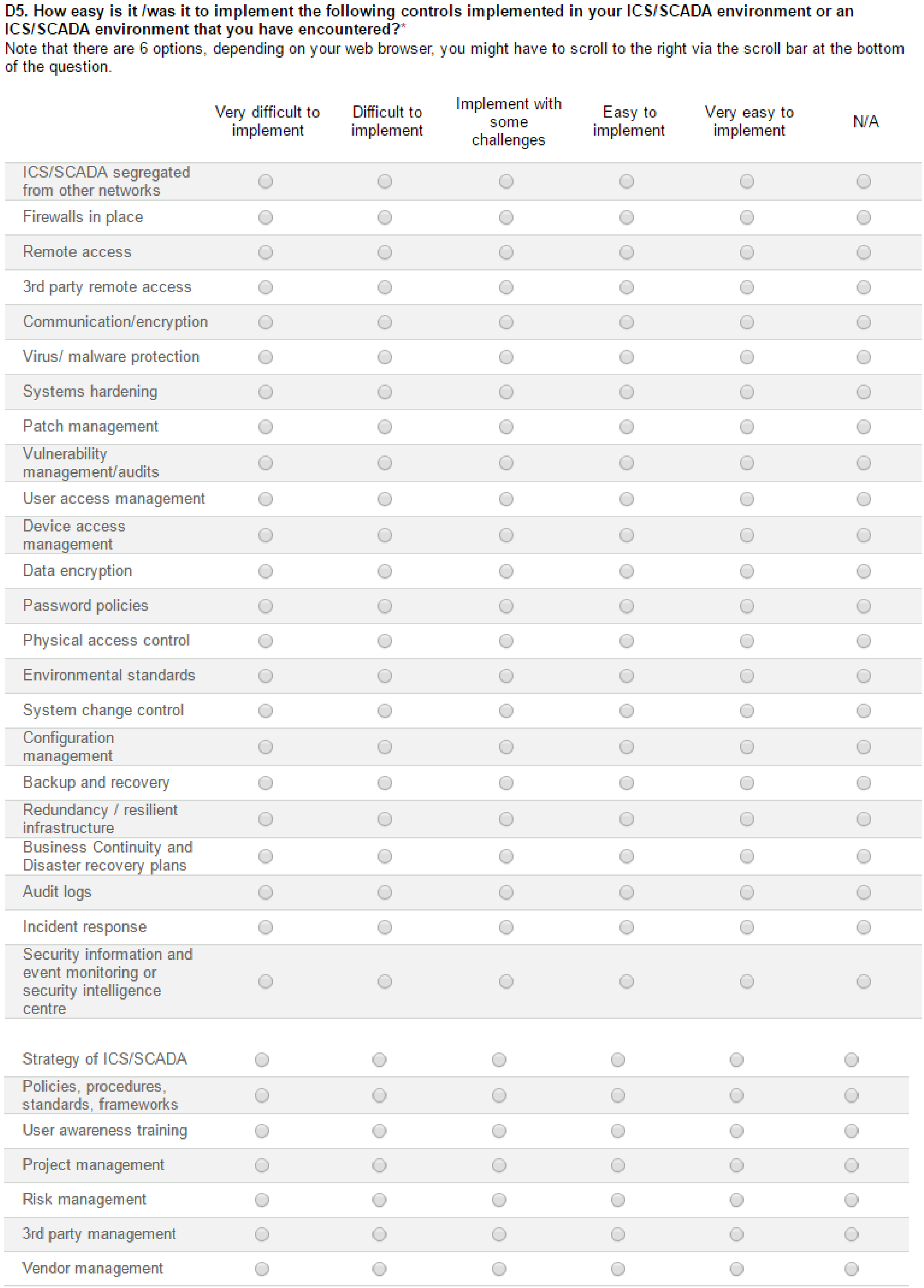
○ 5 - Leading (Controls are established, consistently applied, regularly reviewed and coordinated)



D4. How effective are the following controls implemented in your ICS/SCADA environment or an ICS/SCADA environment that you have encountered?*
Note that there are 7 options, depending on your web browser, you might have to scroll to the right via the scroll bar at the bottom of the question.

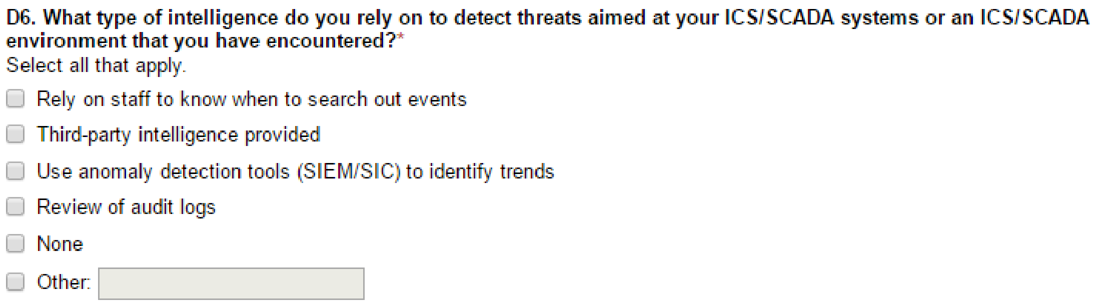
	Have not implemented	Plan to implement in the next year	Partially Implemented / in progress	Implemented but requires improvement	Implemented and operating effectively	Unsure / Unknown	N/A
ICS/SCADA segregated from other networks	○	○	○	○	○	○	○
Firewalls in place	○	○	○	○	○	○	○
Remote access	○	○	○	○	○	○	○
3rd party remote access	○	○	○	○	○	○	○
Communication/encryption	○	○	○	○	○	○	○
Virus/ malware protection	○	○	○	○	○	○	○
Systems hardening	○	○	○	○	○	○	○
Patch management	○	○	○	○	○	○	○
Vulnerability management/audits	○	○	○	○	○	○	○
User access management	○	○	○	○	○	○	○
Device access management	○	○	○	○	○	○	○
Data encryption	○	○	○	○	○	○	○
Password policies	○	○	○	○	○	○	○
Physical access control	○	○	○	○	○	○	○
Environmental standards	○	○	○	○	○	○	○
System change control	○	○	○	○	○	○	○
Configuration management	○	○	○	○	○	○	○
Backup and recovery	○	○	○	○	○	○	○
Redundancy / resilient infrastructure	○	○	○	○	○	○	○
Business Continuity and Disaster recovery plans	○	○	○	○	○	○	○
Audit logs	○	○	○	○	○	○	○
Incident response	○	○	○	○	○	○	○
Security information and event monitoring or security intelligence centre	○	○	○	○	○	○	○

Strategy of ICS/SCADA	○	○	○	○	○	○
Policies, procedures, standards, frameworks	○	○	○	○	○	○
User awareness training	○	○	○	○	○	○
Project management	○	○	○	○	○	○
Risk management	○	○	○	○	○	○
3rd party management	○	○	○	○	○	○
Vendor management	○	○	○	○	○	○



D5. How easy is it /was it to implement the following controls implemented in your ICS/SCADA environment or an ICS/SCADA environment that you have encountered?*
Note that there are 6 options, depending on your web browser, you might have to scroll to the right via the scroll bar at the bottom of the question.

	Very difficult to implement	Difficult to implement	Implement with some challenges	Easy to implement	Very easy to implement	N/A
ICS/SCADA segregated from other networks	○	○	○	○	○	○
Firewalls in place	○	○	○	○	○	○
Remote access	○	○	○	○	○	○
3rd party remote access	○	○	○	○	○	○
Communication/encryption	○	○	○	○	○	○
Virus/ malware protection	○	○	○	○	○	○
Systems hardening	○	○	○	○	○	○
Patch management	○	○	○	○	○	○
Vulnerability management/audits	○	○	○	○	○	○
User access management	○	○	○	○	○	○
Device access management	○	○	○	○	○	○
Data encryption	○	○	○	○	○	○
Password policies	○	○	○	○	○	○
Physical access control	○	○	○	○	○	○
Environmental standards	○	○	○	○	○	○
System change control	○	○	○	○	○	○
Configuration management	○	○	○	○	○	○
Backup and recovery	○	○	○	○	○	○
Redundancy / resilient infrastructure	○	○	○	○	○	○
Business Continuity and Disaster recovery plans	○	○	○	○	○	○
Audit logs	○	○	○	○	○	○
Incident response	○	○	○	○	○	○
Security information and event monitoring or security intelligence centre	○	○	○	○	○	○
Strategy of ICS/SCADA	○	○	○	○	○	○
Policies, procedures, standards, frameworks	○	○	○	○	○	○
User awareness training	○	○	○	○	○	○
Project management	○	○	○	○	○	○
Risk management	○	○	○	○	○	○
3rd party management	○	○	○	○	○	○
Vendor management	○	○	○	○	○	○



D6. What type of intelligence do you rely on to detect threats aimed at your ICS/SCADA systems or an ICS/SCADA environment that you have encountered?*

Select all that apply.

□ Rely on staff to know when to search out events

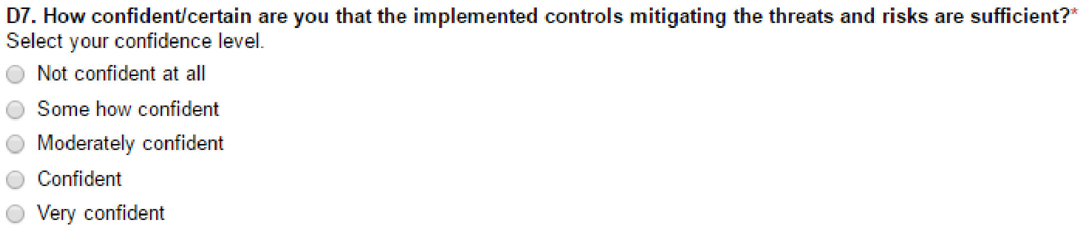
□ Third-party intelligence provided

□ Use anomaly detection tools (SIEM/SIC) to identify trends

□ Review of audit logs

□ None

□ Other:



D7. How confident/certain are you that the implemented controls mitigating the threats and risks are sufficient?*

Select your confidence level.

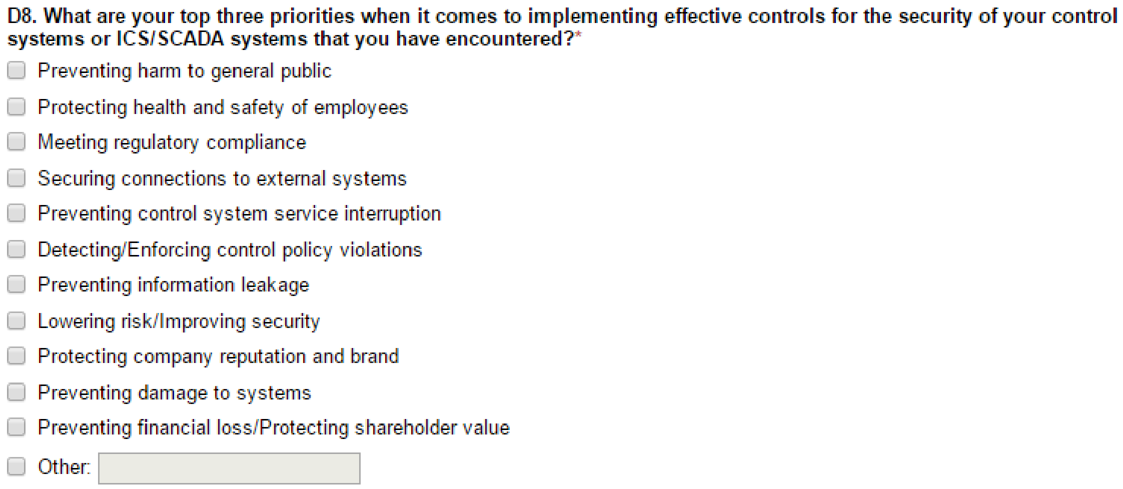
○ Not confident at all

○ Some how confident

○ Moderately confident

○ Confident

○ Very confident



D8. What are your top three priorities when it comes to implementing effective controls for the security of your control systems or ICS/SCADA systems that you have encountered?*

□ Preventing harm to general public

□ Protecting health and safety of employees

□ Meeting regulatory compliance

□ Securing connections to external systems

□ Preventing control system service interruption

□ Detecting/Enforcing control policy violations

□ Preventing information leakage

□ Lowering risk/Improving security

□ Protecting company reputation and brand

□ Preventing damage to systems

□ Preventing financial loss/Protecting shareholder value

□ Other:

Appendix B Additional Tables: Effectiveness of controls

Table B1: Frequency and descriptive statistics for effectiveness of controls implemented in ICS/SCADA environment

	Segregated from other networks	Firewalls in place	Remote access	3rd party remote access	Communication/encryption	Virus/ malware protection	Systems hardening	Patch management	Vulnerability management/audits	User access management
Have not implemented	3	2	2	4	12	4	3	4	7	3
Plan to implement in the next year	3	2	3	6	4	3	3	5	4	1
Partially Implemented/in progress	13	11	15	10	6	6	14	14	10	13
Implemented but requires improvement	11	11	14	15	13	21	16	17	17	17
Implemented and operating effectively	16	21	11	9	12	13	11	7	10	13
Unsure/Unknown	1	0	2	3	1	1	1	1	0	1
N/A	1	1	1	1	0	0	0	0	0	0
Count (n-N/A - Unsure/Unknown)	46	47	45	44	47	47	47	47	48	47
Mean*	3.74	4.00	3.64	3.43	3.19	3.77	3.62	3.38	3.40	3.77
Std Deviation*	1.20	1.12	1.07	1.23	1.56	1.18	1.11	1.13	1.32	1.09
Variance*	1.44	1.26	1.14	1.51	2.42	1.40	1.24	1.28	1.73	1.18
Kurtosis*	-0.27	0.32	-0.03	-0.61	-1.43	0.53	0.07	-0.24	-0.67	0.69
Skewness*	-0.68	-0.96	-0.51	-0.51	-0.33	-1.08	-0.65	-0.54	-0.61	-0.89
Rank		2								

Table B1 (Continued)

	Device access management	Data encryption	Password policies	Physical access control	Environmental standards	System change control	Configuration management	Backup and recovery	Redundancy/resilient infrastructure	Business Continuity and Disaster recovery plans
Have not implemented	4	12	7	2	4	5	6	3	4	5
Plan to implement in the next year	6	2	1	2	2	4	4	2	2	2
Partially Implemented/in progress	10	10	11	9	7	8	5	10	12	9
Implemented but requires improvement	16	15	11	14	14	15	17	16	12	15
Implemented and operating effectively	11	9	17	21	19	15	15	17	16	17
Unsure/Unknown	1	0	1	0	2	1	1	0	2	0
N/A	0	0	0	0	0	0	0	0	0	0
Count (n-N/A - Unsure/Unknown)	47	48	47	48	46	47	47	48	46	48
Mean*	3.51	3.15	3.64	4.04	3.91	3.66	3.66	3.88	3.74	3.77
Std Deviation*	1.23	1.46	1.39	1.09	1.24	1.31	1.36	1.14	1.24	1.28
Variance*	1.52	2.13	1.93	1.19	1.55	1.71	1.84	1.30	1.53	1.63
Kurtosis*	-0.56	-1.21	-0.51	0.80	0.46	-0.40	-0.42	0.54	-0.09	0.05
Skewness*	-0.57	-0.39	-0.78	-1.11	-1.13	-0.79	-0.87	-1.00	-0.80	-0.96
Rank				1	3					

Table B1 (Continued)

	Audit logs	Incident response	SIEM or security intelligence centre	Strategy of ICS/SCADA	Policies, procedures, standards, frameworks	User awareness training	Project management	Risk management	3rd party management	Vendor management
Have not implemented	6	3	11	9	6	6	5	6	4	3
Plan to implement in the next year	4	6	3	6	3	5	2	2	3	3
Partially Implemented/in progress	10	12	11	9	12	15	12	13	13	14
Implemented but requires improvement	14	14	15	15	13	16	18	17	17	15
Implemented and operating effectively	12	13	7	6	13	5	9	8	8	9
Unsure/Unknown	2	0	1	2	1	1	2	2	3	3
N/A	0	0	0	1	0	0	0	0	0	1
Count (n-N/A - Unsure/Unknown)	46	48	47	45	47	47	46	46	45	44
Mean*	3.48	3.58	3.09	3.07	3.51	3.19	3.52	3.41	3.49	3.55
Std Deviation*	1.33	1.20	1.40	1.36	1.32	1.17	1.19	1.22	1.14	1.11
Variance*	1.77	1.44	1.95	1.84	1.73	1.38	1.41	1.49	1.30	1.23
Kurtosis*	-0.68	-0.57	-1.14	-1.15	-0.57	-0.47	0.08	-0.19	0.04	0.05
Skewness*	-0.60	-0.51	-0.36	-0.30	-0.62	-0.47	-0.80	-0.71	-0.69	-0.60
Rank										

* The table of frequencies listed. The mean, Standard Deviation, Variance, Kurtosis, Skewness and Confidence Level have been calculated by removing the N/A and Unsure/Unknown responses.

Appendix C Additional Tables: Ease of implementation

Table C1: Frequency and descriptive statistics for how easy it is/was to implement controls in ICS/SCADA environment

	Segregated from other networks	Firewalls in place	Remote access	3rd party remote access	Communication/encryption	Virus/ malware protection	Systems hardening	Patch management	Vulnerability management/audits	User access management
Very difficult to implement	0	0	2	1	0	1	1	1	0	1
Difficult to implement	9	8	7	6	7	6	12	9	8	7
Implement with some challenges	20	19	20	23	17	14	19	15	19	21
Easy to implement	10	12	10	10	9	16	9	15	11	12
Very easy to implement	4	3	2	1	2	6	2	3	3	3
N/A	5	6	7	7	13	5	5	5	7	4
Count (n-N/A)	43	42	41	41	35	43	43	43	41	44
Mean*	3.21	3.24	3.07	3.10	3.17	3.47	2.98	3.23	3.22	3.20
Std Deviation*	0.89	0.85	0.91	0.77	0.82	0.98	0.89	0.95	0.85	0.88
Variance*	0.79	0.72	0.82	0.59	0.68	0.97	0.79	0.90	0.73	0.77
Kurtosis*	-0.38	-0.43	0.27	0.75	-0.22	-0.31	-0.13	-0.49	-0.37	0.12
Skewness*	0.42	0.26	-0.15	-0.17	0.34	-0.29	0.26	-0.14	0.32	0.01
Rank						3				

Table C1 (Continued)

	Device access management	Data encryption	Password policies	Physical access control	Environmental standards	System change control	Configuration management	Backup and recovery	Redundancy/resilient infrastructure	Business Continuity and Disaster recovery plans
Very difficult to implement	0	0	1	1	1	2	0	2	1	0
Difficult to implement	8	9	8	4	4	5	6	4	5	9
Implement with some challenges	22	13	13	15	16	23	24	20	23	19
Easy to implement	13	12	17	19	16	10	8	13	11	10
Very easy to implement	1	2	3	7	5	3	5	5	2	4
N/A	4	12	6	2	6	5	5	4	6	6
Count (n-N/A)	44	36	42	46	42	43	43	44	42	42
Mean*	3.16	3.19	3.31	3.59	3.48	3.16	3.28	3.34	3.19	3.21
Std Deviation*	0.75	0.89	0.95	0.93	0.92	0.90	0.85	0.96	0.80	0.90
Variance*	0.56	0.79	0.90	0.87	0.84	0.81	0.73	0.93	0.65	0.81
Kurtosis*	-0.41	-0.85	-0.44	0.16	0.18	0.66	-0.02	0.31	0.78	-0.45
Skewness*	0.08	0.11	-0.32	-0.44	-0.33	-0.13	0.62	-0.26	-0.07	0.40
Rank				1	2					

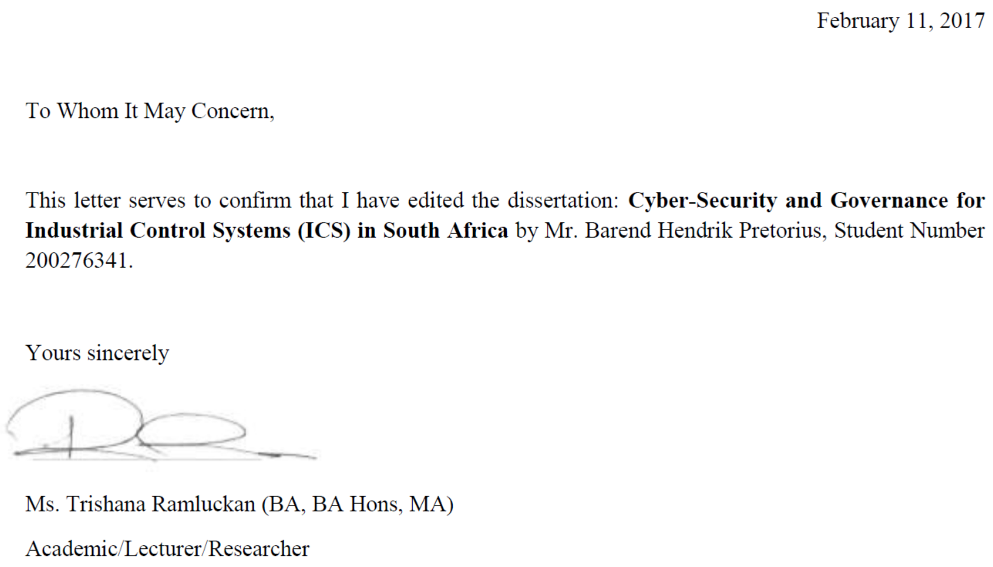
Table C1 (Continued)

	Audit logs	Incident response	SIEM or security intelligence centre	Strategy of ICS/SCADA	Policies, procedures, standards, frameworks	User awareness training	Project management	Risk management	3rd party management	Vendor management
Very difficult to implement	1	0	0	0	1	3	1	0	1	2
Difficult to implement	5	4	10	8	10	7	6	5	6	6
Implement with some challenges	19	18	15	20	17	16	18	19	21	19
Easy to implement	9	16	11	8	12	11	12	12	10	10
Very easy to implement	5	3	2	2	3	4	4	4	3	4
N/A	9	7	10	10	5	7	7	8	7	7
Count (n-N/A)	39	41	38	38	43	41	41	40	41	41
Mean*	3.31	3.44	3.13	3.11	3.14	3.15	3.29	3.38	3.20	3.20
Std Deviation*	0.95	0.78	0.88	0.80	0.94	1.06	0.93	0.84	0.87	0.98
Variance*	0.90	0.60	0.77	0.64	0.88	1.13	0.86	0.70	0.76	0.96
Kurtosis*	0.01	-0.26	-0.71	0.09	-0.41	-0.30	-0.05	-0.33	0.35	0.07
Skewness*	0.10	0.04	0.24	0.48	0.07	-0.17	-0.04	0.28	0.07	-0.08
Rank										

* The table of frequencies listed. The mean, Standard Deviation, Variance, Kurtosis, Skewness and Confidence Level have been calculated by removing the N/A responses.

Appendix D Index

Appendix E Letter from the Language Editor



February 11, 2017

To Whom It May Concern,

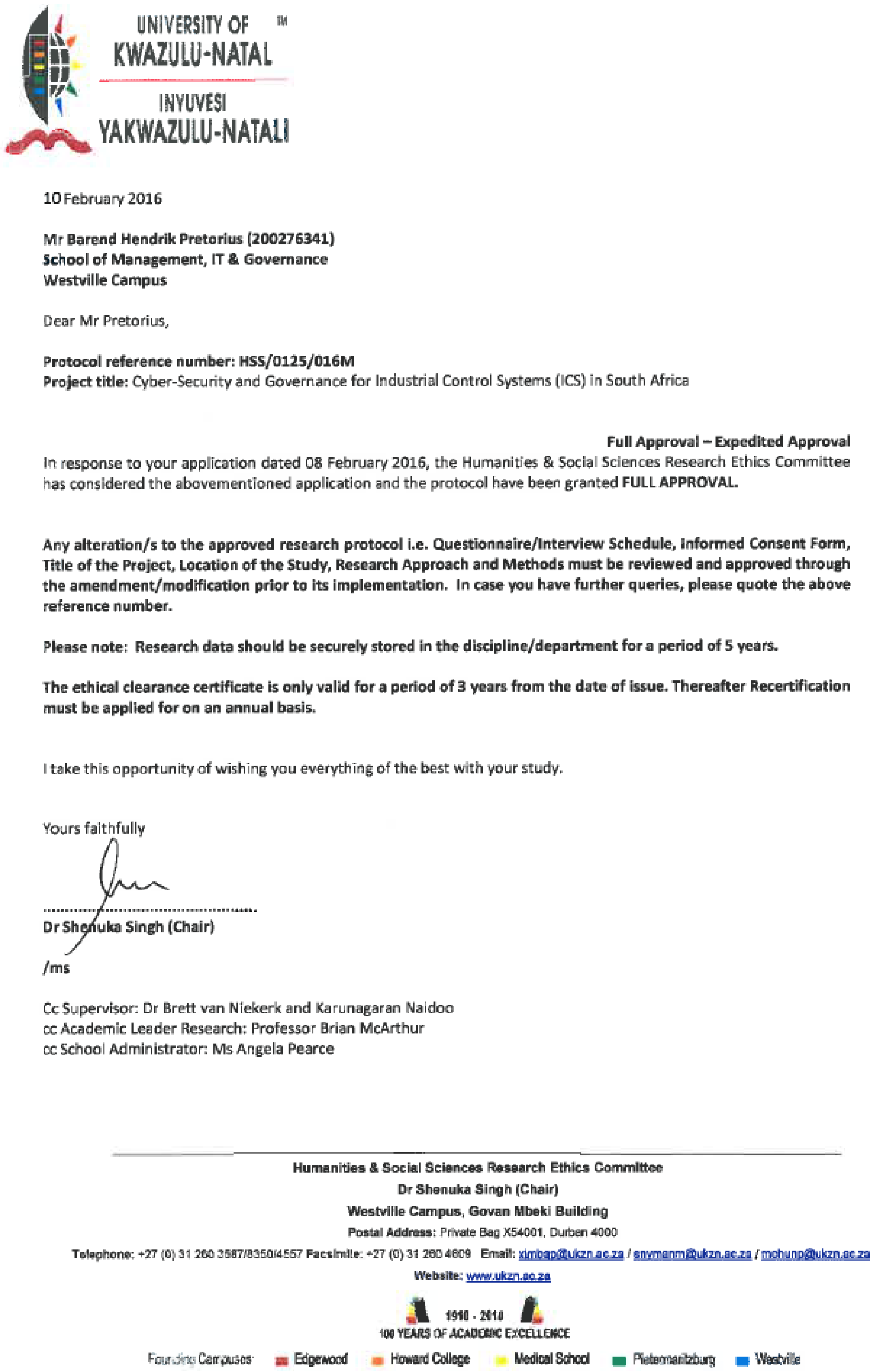
This letter serves to confirm that I have edited the dissertation: **Cyber-Security and Governance for Industrial Control Systems (ICS) in South Africa** by Mr. Barend Hendrik Pretorius, Student Number 200276341.

Yours sincerely

Ms. Trishana Ramluckan (BA, BA Hons, MA)

Academic/Lecturer/Researcher

Appendix F Ethical Clearance



UNIVERSITY OF KWAZULU-NATAL
INYUVESI YAKWAZULU-NATALI

10 February 2016

Mr Barend Hendrik Pretorius (200276341)
School of Management, IT & Governance
Westville Campus

Dear Mr Pretorius,

Protocol reference number: HSS/0125/016M
Project title: Cyber-Security and Governance for Industrial Control Systems (ICS) in South Africa

Full Approval – Expedited Approval

In response to your application dated 08 February 2016, the Humanities & Social Sciences Research Ethics Committee has considered the abovementioned application and the protocol have been granted **FULL APPROVAL.**

Any alteration/s to the approved research protocol i.e. Questionnaire/Interview Schedule, Informed Consent Form, Title of the Project, Location of the Study, Research Approach and Methods must be reviewed and approved through the amendment/modification prior to its implementation. In case you have further queries, please quote the above reference number.

Please note: Research data should be securely stored in the discipline/department for a period of 5 years.

The ethical clearance certificate is only valid for a period of 3 years from the date of issue. Thereafter Recertification must be applied for on an annual basis.

I take this opportunity of wishing you everything of the best with your study.

Yours faithfully

....

Dr Shenuka Singh (Chair)

/ms

Cc Supervisor: Dr Brett van Niekerk and Karunagaran Naidoo
cc Academic Leader Research: Professor Brian McArthur
cc School Administrator: Ms Angela Pearce

Humanities & Social Sciences Research Ethics Committee
Dr Shenuka Singh (Chair)
Westville Campus, Govan Mbeki Building
Postal Address: Private Bag X54001, Durban 4000
Telephone: +27 (0) 31 260 3587/8350/4557 **Facsimile:** +27 (0) 31 260 4609 **Email:** ximbap@ukzn.ac.za / snymanm@ukzn.ac.za / mohunp@ukzn.ac.za
Website: www.ukzn.ac.za

1910 - 2010
100 YEARS OF ACADEMIC EXCELLENCE

Founding Campuses: 🟥 Edgewood 🟧 Howard College 🟨 Medical School 🟩 Pietermaritzburg 🟦 Westville