Faculty of Computing and Informatics

Department of Computer Science

A Bio-Immunology Inspired Security Model to Defend Industrial Control Systems from Advanced Persistent Threats

Thesis submitted in fulfilment of the requirements for the degree of

Doctor of Philosophy in Computer Science

at

Namibia University of Science and Technology

Submitted by:	**Mercy Chitauro**
Student Number:	**200731939**
Supervisor:	**Prof H. N. Muyingi**
Co-Supervisor:	**Dr S. John**
Submission Date:	**January 2019**

METADATA

TITLE:	Mrs
STUDENT NAME:	Mercy Chitauro
SUPERVISOR:	Prof. H. N. Muyingi
CO-SUPERVISOR:	Dr S. John
DEPARTMENT:	Computer Science
QUALIFICATION:	Doctor of Philosophy (PhD) in Computer Science
SPECIALISATION:	Cyber Security
STUDY TITLE:	A Bio-Immunology Inspired Security Model to Defend Industrial Control Systems from Advanced Persistent Threats
MAIN KNOWLEDGE AREA:	Information Assurance and Security
KEYWORDS:	Industrial Control System, Advanced Persistent Threat, Immune System, Artificial Immune System, Security, Control System
TYPE OF RESEARCH:	Experimental Research
METHODOLOGY:	Design Science Research
STATUS:	Final Thesis
SITE:	Main Campus Windhoek
DOCUMENT DATE:	October 2018
RESEARCH LAB:	Digital Forensics and Information Security

DECLARATION

I, Mercy Chitauro hereby declare that the work contained in this report is presented for the Doctor of Philosophy (PhD) in Computer Science at the Namibia University of Science and Technology, entitled:

A Bio-Immunology Inspired Security Model to Defend Industrial Control System from Advanced Persistent Threats,

is my own original work and that I have not previously in its entirety or in part submitted it at any university or other higher education institution for the award of a degree. I further declare that all sources cited or quoted are indicated and fully acknowledged by means of a comprehensive list of references in accordance with the institution rules.

Signature: 

Date: 31 January 2019

ABSTRACT

Industrial Control Systems (ICS) control critical industrial processes. For example, there are ICS networks that control electricity, water distribution, food, and pharmaceutical and beverage production. Historically, ICS networks were safe from network attacks because they were not interconnected to business Information Technology (IT) networks and the Internet. However, with the passage of time, ICS were interconnected to business networks. Because traditional IT networks are built on the TCP/IP suite, ICS became susceptible to network attacks that already existed in TCP/IP networks and to ICS specific attacks.

Successful attacks in ICS networks may compromise the ICS infrastructure, system configurations and components. ICS security standards and frameworks were drafted and approved by different organisations for use in the implementation of ICS security. ICS can be secured using these standards or any other means as recommended by ICS security experts. Even though ICS are secured using these recommended methods, they are still being successfully attacked by Advanced Persistent Threats (APTs). APTs are targeted attacks which are successful because they do not attack any system that they might be in but become active in only those systems they were designed for. APTs have the ability to circumvent available security control and regular intrusion detection systems, and in addition, antiviruses are not able to detect APTs.

There is no known technique available to identify APTs that attack ICS because APTs are discovered after they have been in the system for some time and usually only after they have executed their payload. Subsequently, this means that present ICS security implementations are not capable of defending ICS when they are attacked by APTs.

By design, ICS security systems should be capable of defending ICS components from any attacks. They are likened to the biological immune system which is responsible for detecting and protecting the biological body from harmful microorganisms. The biological immune system's most crucial function is that of preventing infections and eradicating already established

infections. The biological immune system can identify unknown and harmful pathogens and eliminate them by continuously evolving in anticipation of new pathogens.

Thus, the research endeavoured to design a bio-immunology inspired security model to harden existing ICS defence from APTs, with the aim that the new ICS security system will constantly evolve in anticipation of new attack scenarios.

Design science research, which is a mixed method approach, was used because it is a problem solving paradigm. To find out how, where and why APTs attack ICS, systematic analysis of literature on APTs was used. Systematic analysis of literature on current ICS defence mechanisms was used to inform the theories, frameworks, instruments, models, methods and weaknesses of current ICS defence mechanisms. Finally, systematic analysis of biological immune systems and artificial immune systems was used to find out how the biological immune system defends the body from pathogens and to find out about the theories, models, methods and weaknesses of current artificial immune systems.

It was discovered that the biological immune system properties such as the fact that it is environmentally self-aware, distributed, intelligent, capable to do message transfers and that it is resilient, enable it to identify unknown but harmful pathogens and to eliminate them. Armed with these properties, it was possible in this research to design a bio-immunology inspired ICS security model. Even though all the identified properties were used to design the bio-immunology inspired security, it was established that collaboration, defence-in-depth and decentralisation properties were already established security parameters in ICS security. Thus, only the property of environmental self-awareness and its enhancement to resilience were tested within the model.

A Model Predictive Controller (MPC) was used as a device that can showcase environmental self-awareness by using prediction intelligence in an ICS depicted by a continuously stirred tank reactor simulation experiment using MATLAB. Demonstration and evaluation of the bio-immunology inspired security model results show that the MPC controlled process does detect APTs effects and can stop APTs from affecting the process when the attack happens before the process starts. MPC is not able to stop attacks after the process has started, but is able to return

the process to a steady state in a short time. Therefore, it was inferred to mean that if few biological immune system properties are used in a security system like in the case of this experiment, then APT will be able to attack ICS but if defence-in-depth strategies are used, then better results are expected.

Keywords: Industrial Control System, Advanced Persistent Threat, biological Immune System, Artificial Immune System, security, control system

DEDICATION

To the Almighty God for giving me life and for making this thesis possible - Philippians 4:13; “I can do all things through Christ who strengthens me”. It was only through Him that I got the strength and the perseverance to start and finish this research

To my husband Shadreck Chitauro for his support throughout the whole process; I would like to commend his technical prowess, because of this, all experiments and any technical requirements were realised easily.

To Nathaniel and Yevedzo for giving mummy time to write up by managing on their own, may God continue to bless these two lovely children.

To Fungai Bhunu Shava who is always lending a helping hand and always finding the right words to encourage one into accomplishing their task, her selfless drive to see others succeed is more than appreciated. Let her not do this for me only but for all that require her guidance and support.

To Mr Attlee Gamundani, who is always ready to lend a helping hand and ready to listen to one’s problems, his determination and never ending ideas always gave me the strength to continue with my research.

To my friends and family who supported me throughout my study; thank you for the moral support and your prayers. Special mention goes to my mum (elder Bere), the Nyandoro family and Dr Blessing Chiripanhura.

ACKNOWLEDGEMENTS

I would like to profoundly thank Professor Hippolyte Muyingi for his guidance throughout my study. I would like to acknowledge and thank Prof for his genius ideas, his never ending patience and timely feedback. Professor Muyingi has a wealth of knowledge, humility and wisdom. Thank you for the five years you have spent on my work, your support, your kindness and believing that I could make it.

I would also like to thank Dr Samuel John. Though he got involved at a much later stage of my research, his guidance on control systems was invaluable; thank you Dr for your support, guidance and support.

I would also like to acknowledge Dr Colleen Sheridan for her guidance on biological immune systems. Thank you for reviewing my work and for guiding me on some misunderstandings I had about the immune system.

I would also like to thank the Faculty of Computing and Informatics at the Namibia University of Science and Technology for their support and for giving me the platform and opportunities to present my research work locally and at international conferences. In this regard, special mention goes to NUST's Digital Forensics and Information Security Research Cluster, which always found time to peer review my work.

Publications arising from this thesis

JOURNAL PAPERS

1. Bere, M., Bhunu Shava, F., Gamundani, A. M., & Nhamu, I. (2015). How advanced persistent threats exploit humans. *IJCSI, 12*(4), in print. doi:IJCSI-2015-12-4-10601

PEER REVIEWED CONFERENCE PAPERS

2. Bere-Chitauro, M., Muyingi, H., Gamundani, A., & Chitauro, S. (2015). *Advanced persistent threat model for testing industrial control system security mechanisms*. Proceedings of the International Congress on Information and Communication Technology. *Advances in Intelligent Systems and Computing,* 438. Singapore: Springer.

3. Bere M. (2015). *A preliminary review of ICS security frameworks and standards vs. advanced persistent threats*. Proceedings of the 10th International Conference on Cyber Warfare and Security held on the 24th to the 25th of March 2015 in South Africa. ISBN 978-1-910309-97-1.

4. Bere, M. (2015). *Initial investigation of Industrial Control System (ICS) security using Artificial Immune System (AIS).* Proceedings of International Conference on Emerging Trends in Network and Computer Communication held on 18- 21 May 2015 in Namibia. Pages: 79 - 84, DOI: 10.1109/ETNCC.2015.7184812

5. Chitauro, M., Muyingi, H., John, S. & Chitauro, S. (2019). *A survey of APT defence techniques.* In Proceedings of 14th International Conference on Cyber Warfare and Security, 28 February – 1 March, Stellenbosch, South Africa. In press.

6. Chitauro, M., Muyingi, H., John, S. & Chitauro, S. (2019). *A bio-immunology inspired*

industrial control system security model. In Proceedings of First International Conference on Sustainable Technologies for Computational Intelligence (ICTSCI-2019), 29-30 March, Jaipur, Rajasthan, India. In Press.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

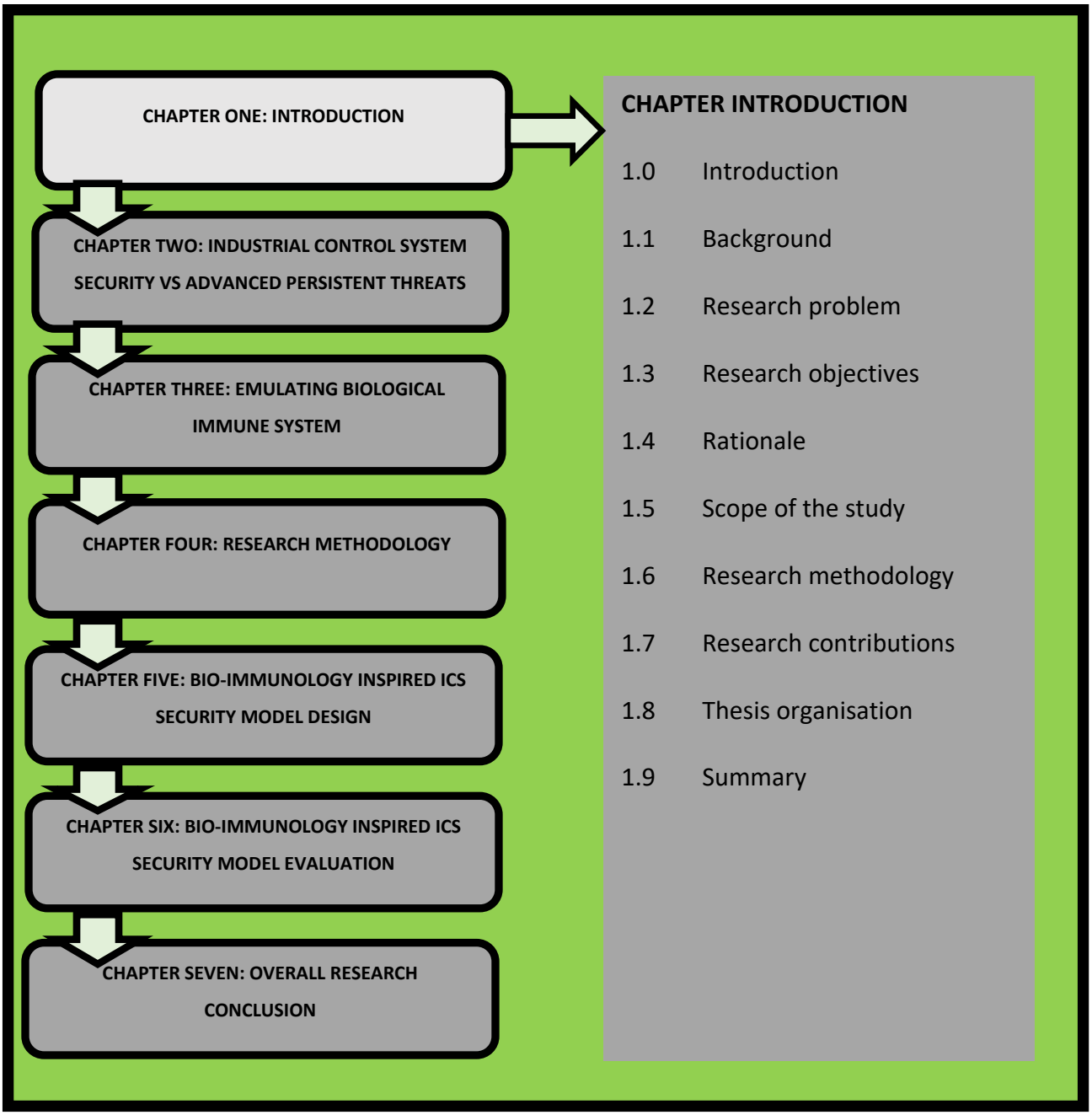
LIST OF ACRONYMS AND ABBREVIATIONS

AIS	Artificial Immune Systems
APT	Advanced Persistent Threat
BIS	Biological Immune System
C&C	Command and Control
CHARE	Configurable Hardware Assisted Application Rule Enforcement
CSTR	Continuously Stirred Tank Reactor
CVE	Common Vulnerabilities and Exposures
DAMPS	Damage Associated Molecular Patterns
DC	Dendritic Cell
DCS	Distributed Control System
DNS	Domain Name System
e_{ss}	steady state error
HMI	Human Machine Interface
ICS	Industrial Control System
IDS	Intrusion Detection System
IKC	Intrusion Kill Chain
IED	Intelligent Electronic Device

IPS	Intrusion Prevention System
IS	Immune System
ISA	International Society of Automation
IT	Information Technology
LAN	Local Area Network
LQG	Linear Quadratic Gaussian
MATLAB	Matrix Laboratory
MPC	Model Predictive Controller
MTU	Master Terminal Unit
PAMPS	Pathogen-Associated Molecular Patterns
PID	Proportional-Integral-Derivative
PCS	Process Control system
PDF	Portable Document Format
PLC	Programmable Logic Controller
PPT	PowerPoint
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information Event Management
SIS	Safety Instrumented System
TAIGA	The Autonomic Interface Guardian Architecture
T_h	Helper T Cell
t_r	Rise time

t_s	Settling time
TCP/IP	Transmission Control Protocol/Internet Protocol
TTP	Tactics, Techniques and Procedures
UBA	User Behaviour Analytics
USB	Universal Serial Bus
XML	eXtensible Markup Language

CHAPTER 1 : INTRODUCTION



CHAPTER OUTLINE

Industrial Control Systems (ICS) and Advanced Persistent Threats (APT) are introduced in this chapter. The chapter gives an overview of ICS, ICS security and how APT are attacking ICS. This leads to a description of the research problem and research objectives. This chapter is an overarching description of the whole research process. It outlines how the research was carried out, the methodology used, the scope of the study and research contributions. Finally, the chapter outlines and summarises the rest of the remaining chapters in the thesis document.

1.0 Introduction

ICS is a generic term for a variety of control systems that include Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS), Process Control Systems (PCS), and smart grid. ICS automate the generation, transportation and distribution of electricity. ICS automate the industrial manufacturing of food, beverages and chemicals. ICS are also used in mining industries, transportation systems, distribution of water, natural gas and oil, in communication systems and in specialised facilities such as nuclear plants. Many ICS typically automate facilities that are part of national critical infrastructures such as electricity grids. The malfunctioning of ICS can lead to detrimental environmental effects such as nuclear waste leakage. This study focuses on how to enhance ICS security from advanced persistent threats. A bio-immunology inspired ICS security model was designed for use as a security baseline for ICS security. This chapter gives an overview of how the research problem, the objectives and how a bio-immunology inspired ICS security model was conceptualised, designed and validated.

Section 1.1 provides the background to the research; Section 1.2 outlines the research problem; Section 1.3 presents the research objectives and formulation of the research questions; Section 1.4 presents the rationale and Section 1.5 describes the scope. An overview of the research design and methodology is given in Section 1.6. Section 1.7 summarises research contributions and finally section 1.8 presents the organisation of the rest of the thesis and finally section 1.9 summarises Chapter One.

1.1 Background

In the past ICS were thought to be safe from attacks because they were air gapped from other information technology (IT) networks. This meant that they were not secured like other IT networks (CPNI, 2008; Stouffer, Pillitteri, Lightman, Abrams, & Hahn, 2015). By following trends, ICS were eventually connected to their corporate networks, which therefore, meant that ICS became vulnerable to common, new and ICS specific network attacks.

There are many ICS security specifications like ICS security standards and frameworks which an ICS security practitioner can use to safeguard ICS from network attacks. Many a time ICS security standards are used as a building block to designing security implementations for ICS because they generally offer best practice guidelines on ways to secure ICS from computer threats.

Despite the existence of and implementation of security measures in ICS, they are still being successfully attacked by sophisticated attacks termed Advanced Persistent Threat (APT). APTs typically successfully attack an ICS because they are persistent targeted attacks that are not detectable in ICS. Normal intrusion detection systems are not capable of detecting APT because APTs use camouflaging techniques and exploit previously unknown ICS vulnerabilities. Table 1.1 shows some of the APTs that have been discovered lurking in ICS.

Table 1.1: Examples of APT in ICS ("Targeted cyberattacks logbook," n.d.)

	APT		**Intention**	**Infection method**	**Year Discovered**	**First known sample**
	Stuxnet		Cybersabotage	File infection, LAN spreading, USB cables	2010	2007
	Shamoon		Data wiping	LAN spreading	2012	2012
	Wiper		Data wiping	unknown	2012	2011
	Miniduke		Cyberespionage	Spear phishing	2013	2008
	The Mask/Careto		Cyberespionage	Spear phishing	2013	2007

	Desert Falcons		Cyberespionage, data theft, survellaince)	Social engineering (spear phishing, facebook	2014	2011
	Poseidon		Cyberespionage, Remote control, Surveillance	Social engineering, Exploits	2015	2015
	Ghoul		Cyberespionage	Social engineering	2016	2015
	Shadowpad		Remote control	Trojanized software installers	2017	2017
	Expetr		Data wiping, stealing money	Exploits, watering hole attacks	2017	2017

Unlike typical worms and viruses which target as many victims as possible, APTs only attack specific and selected targets. An APT is executed in several stages (Virvilis et al., 2013). An APT's execution stages are (Fortinet, 2013; Giura & Wang, 2012; Virvilis et al., 2013):

- reconnaissance,
- delivery,
- exploitation,
- operation,
- data collection, and
- exfiltration.

At the very beginning of an APT attack, the attackers choose their victims. After they have identified a target, the attackers launch reconnaissance attacks to gather information about their target. After gaining enough data, the attackers deliver their malware into the ICS. This is followed by the exploitation of the system whereby the APT strategically positions itself by taking advantage of ICS vulnerabilities. Once it is where it needs to be, an APT can now execute its operation and in most cases steal data to send to a remote command and control centre (Bencsáth, Pék, Buttyán, & Félegyházi, 2012; Falliere, Murchu, & Chien, 2011; Virvilis & Gritzalis, 2013).

To exemplify the concepts about APT described above, let us take the example of Stuxnet. Stuxnet was discovered in 2010. It was designed to attack the Iranian Natanz Nuclear Enrichment Facility (Falliere et al., 2011). Stuxnet gained entry into the system through a USB stick. It infected Microsoft Windows machines by presenting false digital certificates. Stuxnet would then find out if the machine infected was part of the Siemens component of the ICS. If the machine was not part of the Siemens ICS component, Stuxnet would remain idle. If the machine connected was part of the Siemens ICS components Stuxnet would use zero-day exploits to infect the connected Programmable Logic Controller (PLC). At first, Stuxnet would do nothing but just gather information and then eventually it would change the frequency settings in a cycle so that centrifuges would spin out of control. From the time of entry into the system to the time it would execute its payload of changing centrifuges frequency cycles, Stuxnet would provide false feedback that everything is fine to the outside controllers so that the controlled operation would appear normal.

Another example of an APT is Crounching Yeti or Energetic bear. Crounching Yeti which was discovered in 2014 targeted industrial/machinery, manufacturing, pharmaceutical, and construction sites. It was delivered into the target systems by way of:

- Spear-phishing e-mails using PDF documents embedded with an Adobe Flash exploit (CVE-2011- 0611)
- Trojanised software installers
- Waterhole attacks using a variety of re-used exploits

Once in the system, Crounching Yeti APT used several malwares/Trojans; Havex Trojan, Sysmain Trojan, The ClientX backdoor and karagany backdoor that target Windows systems only. The malware is used to analyse servers, to find and steal information. Additionally, original files were replaced.

APTs will pursue their objective until it is reached even if it takes a long time. Also, APTs can adapt to the system environment in order to bypass security parameters (Falliere et al., 2011; Bencsath et al., 2012). That is why most APTs are not delivered using one method. If one method fails, then another one is sought until one of the methods succeeds. Furthermore, APTs have the

ability to act stealthily in a system to avoid detection or they can suspend their objective until certain conditions are met.

1.1.1 ICS security mechanisms bypassed by APT

1.1.1.1 Access and identity security

ICS security recommendations state that ICS personnel should be trained on the importance of keeping ICS safe (CPNI, 2008; QNCIS, 2014; Stouffer et al., 2015). It should also be the norm that the ICS personnel should know that they must not divulge ICS information to unauthorised people. However, APT developers are very determined and they usually socially engineer ICS personnel so that they can gather information and also to gain entry into the ICS (Bere, Bhunu-Shava, Gamundani, & Nhamu, 2015). Although social engineering gives an APT attacker vital information about ICS, they add to this information by mining for information on social websites where sharing information is the standard thing to do. Access control mechanisms can also be easily bypassed by the disgruntled employee who already has access to the system. A disgruntled employee can also willingly give out information to whoever needs it. A typical example is seen in the case of the attack in the Maroochy water plant incident in Australia (Slay & Miller, 2008).

1.1.1.2 Data security

In most instances when APT gains entry into a system, it escalates its rights so that it can install whatever malicious software its needs to operate. This is because they have rootkit functionalities. This means that those conditions that state that authorised software should only be installed by authorised entities is easily circumvented by APTs. Data security makes sure that data is not corrupted but as we saw in the examples of Stuxnet and Crounching Yeti, APT corrupted data and changed PLC configurations without the system noticing.

1.1.1.3 Network security

Firewalls, antivirus applications, intrusion detection systems (IDS) and intrusion prevention mechanisms (IPS) are easily circumvented by APTs yet these are the applications that are commonly used for network security. Antivirus and IPS that rely on malware signatures and known attack footprints to detect intrusion are not able to detect APT because APT uses zero-day exploits to compromise the system. Zero-day exploits do not have previously recorded

signatures and thus, cannot be detected by signature based antiviruses and IDSs where the signatures used for detection would be non-existent. Even if the signature were known, APT like Stuxnet exhibited different behaviour in the presence of diffident antivirus software (see section 2.4.2.2). Some IPSs depend on the use of anomalous behaviour in the system to detect intrusion. Although such IPS tend to have a high rate of false positives, it is highly unlikely that they would be able to detect APT because APTs have camouflage capabilities which enable them to hide their presence in a system (Virvilis & Gritzalis, 2013).

The implementation of firewalls in ICS has its shortfalls also because APTs are not blocked by firewalls. They enter into the system and are allowed through the firewall as genuine ICS traffic. This is mainly because they enter into the system by socially engineering the personnel and thus they are introduced in the system by users somewhere behind the firewalls. Furthermore, APTs once in the system communicate with their command and control centre outside the ICS. The communication between APT and its command and control centre is through a firewall, which means that the firewall rules are not adequate to stop this communication.

1.1.2 Current ICS security research

The problem of APT attacking ICS needs to be addressed as a matter of urgency. In line with this, several researches have been undertaken in order to improve ICS security in the face of APT attack. The work by Averbuch and Siboni (2013), de Vries, Hoogstraaten, van den Berg, and Daskapan (2012), and Skopik, Friedberg, and Fiedler (2014) suggest the use of anomalous IDS to detect APT. They argue that since APTs are foreign in the system, they should exhibit anomalous behaviour at some point in the system which should be detected by the IDS.

Other works by Virvilis et al. (2013) and Bhatt et al. (2014) put forward the idea of improving security controls in existence. They suggest looking at APT stages and tweaking the security controls that APT bypass at each stage. This method of increasing security layers is known as the defence-in-depth strategy.

Yet other work by Virvilis and Gritzalis (2013), and Giura and Wang (2012) suggest combining anomalous IDS and the defence-in-depth strategies.

In summary, it can be generalised that APTs are sophisticated cyber-attacks that are able to bypass most security configurations in a system. APTs successfully attack ICS because they are persistent and are not detectable in ICS. APT are not detectable with normal detection systems because APTs exploit previously unknown ICS vulnerabilities. APTs are mainly used for data exfiltration but the most dangerous APTs would be like the ones that act like Stuxnet. These APTs change ICS configurations so that they can sabotage normal operations. It is also quite apparent that current detection mechanisms are slow to detect APTs in the system. If we look at Table 1.1, we can see that it normally takes up to a year for an APT to be detected in the system. Current research on the improvement of ICS defence from APTs is centred on improving intrusion detection systems so that they are able to detect APTs in the system before they have realised their objective. The problem with these innovations is that they propose to detect an APT when it has already had some damage in the system.

1.2 Research problem

Hardening ICS with the use of classic or best practices recommended by ICS security frameworks and standards is clearly not enough to deter APTs from gaining access to ICS. Traditional ways like the use of IDS, IPS, firewalls and antivirus software not really useful in defending an ICS from APTs. These traditional methods which are also endorsed for use by ICS standards and frameworks are not really useful because attackers understand how an ICS is secured. Therefore, attackers, are able to exploit ICS security configurations. Furthermore, to gain access attackers social engineer humans to gain access to ICS. Current ICS security researches suggest solutions that will detect an APT after it has been in the system for a while (Bere, 2015; de Vries, Hoogstraaten, van den Berg, & Daskapan, 2012; Piggin, 2012; Virvilis & Gritzalis, 2013).

There is no known solution for access control, identity control, and data security against APTs. Current access control mechanisms used in ICS security would only be helpful if there were flawless means by which to isolate completely all access methods to unauthorised people. But, even if this was true APTs are persistent, which means they will ultimately bypass access control mechanisms and gain access into the system one way or another (Bere, 2015).

There was no known technique available to identify APTs that attack ICS, because APTs are discovered after they have been in the system for some time and usually only after they have executed their payload (Virvilis & Gritzalis, 2013) . Subsequently, this means that present ICS security implementations are not capable of defending ICS when they are attacked by APTs.

1.3 Research objectives and questions

The main objective of this research was to develop a bio-immunology inspired ICS security model for improving existing ICS defence from APTs through an early detection approach of APT. In order to achieve this objective, the following sub objectives were realised.

1. Analyse where, how and why APTs attack ICS
2. Evaluate current ICS defence mechanisms
3. Design a bio-immunology inspired ICS security model
4. Validate the bio-immunology inspired ICS security model

The main research question answered in this research is:

- How can ICS be secured to avoid APT attack?

To answer the main question, the following sub-questions were answered:

1. Where and how do APTs attack ICS?
2. Why do APT attacks happen: Are ICS vulnerabilities from ICS inner workings / operations, security strategy site or something else?
3. What approach can be considered in either case to avoid APT attacks?
4. What are the components of a bio-immunology inspired ICS security model?
5. How can a bio-immunology inspired ICS security model be validated?

1.4 Rationale

The outcomes of this research add to the knowledge of ICS network security and vulnerabilities in that:

1. Significant contribution is made to the advancement of ICS security. Improvements in ICS security mean that ICS are less vulnerable to APT attacks. When ICS are less vulnerable to APT attacks or any other attack, then the negative effects of APT attacks will be greatly improved.

2. Improving ICS security has an effect in reducing cybercrime. For example, a reduction in unauthorised access to systems, stealing confidential data, etc. will subsequently be reduced as well. A reduction in cybercrime is an advantage to ICS system administrators, law enforcement agencies, society and business. The possibility of a reduction in any form of crime is definitely an advantage to any society, business, country, continent, and the world that would have been affected by the crime.

1.5 Scope

1. Security mechanisms try to completely prevent intrusions from entering the system or they detect those that have already invaded and they then eliminate them. APTs are finding entry to ICS through the exploitation of human weaknesses. This means that in most cases APTs do find a way of gaining entry into ICS. Thus, this research focused on APTs that have already gained entry into the system.

2. Many APTs are designed to steal data in the system, hence this research focused on those APT that cause changes to how an ICS will operate as these were understood to be the most dangerous kinds of APTs.

3. Although APTs do not only attack ICS, this research concentrated only on those APTs that are attacking ICS.

4. APTs may attack ICS because ICS components and protocols have weaknesses or they may attack ICS because of the fact that ICS components are networked and the security mechanisms of the networked components are failing. The focus was on the issues of weak security mechanisms in ICS.

1.6 Research methodology

1.6.1 Research paradigms and philosophies

The research paradigm adopted for this research is the pragmatist paradigm whereby the design science research methodology was the overarching methodology used to conduct this research. Thus, the design science research methodology was chosen with an ontological view that it would best answer the research question (*How can ICS be secured to avoid APT attacks?*) and an epistemological belief that both observable phenomena and or subjective meanings can provide acceptable knowledge dependent upon the research question.

This research used design research methodology with simulation and experimentation of quantitative data.

1.6.2 Theoretical assumption: The bio-immunology similarities

The biological immune system is tasked with detecting and protecting the body from harmful microorganisms. As such, it was equated to ICS security systems which are tasked to detecting and protecting ICS from intruders and malicious activity. The biological immune system is capable of identifying known and unknown pathogens. The capability of the immune system to identify previously unknown attacks was deemed as lacking in ICS security.

The biological immune system has the following properties, namely that it:

- is distributed,
- uses intelligence and collaboration,
- can communicate (message transfer),
- uses defence in depth,
- enables environmental self-awareness, and

- is resilient.

A mapping of the biological immune system properties to ICS security mechanisms was done. After identifying those security properties of the biological immune system that were lacking in ICS security properties, the researcher emulated the missing properties of the biological immune system to ICS security mechanisms.

1.6.3 Design research methodology

The research fell under the constructive research methodology or research by proof of concept whereby something novel is researched, designed, implemented, and evaluated, then theorised about. Design research uses the mixed method approach that relies on natural science and design science. In the case of solving APT in the ICS problem, answers to how, where and why APT attacks ICS were given by conducting data analysis of literature on APT. Data analysis of current ICS defence mechanisms was done to inform on the theories, frameworks, instruments, models, methods and weaknesses of current ICS defence mechanisms.

In order to verify and evaluate the model, design science conceptual frameworks suggest the use of case studies, experiments, field study or simulation. In this research, a real ICS was simulated in an experiment which was used to test the effectiveness of the new model. Figure 1.1 illustrates the research process.

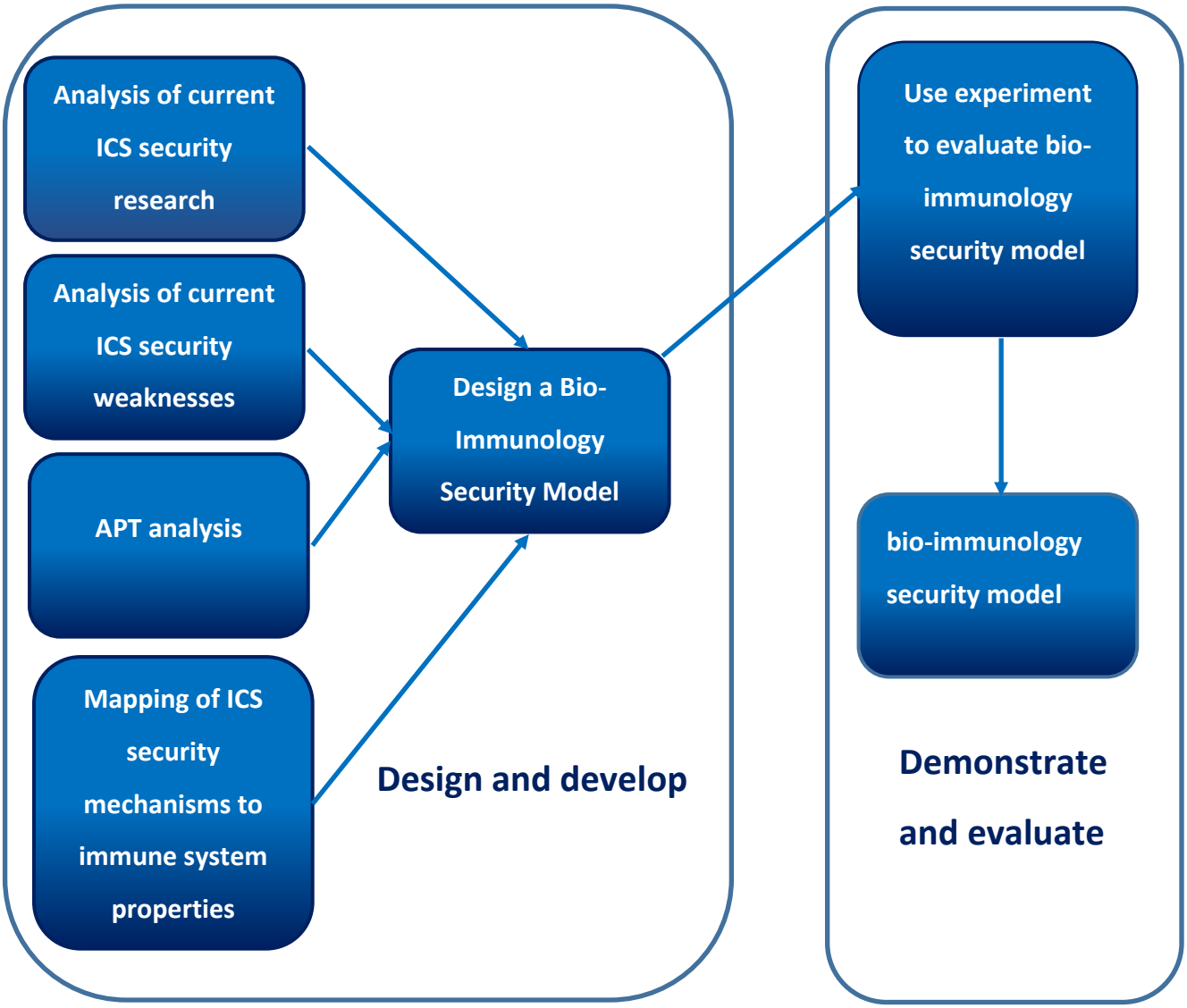


Figure 1.1 Research Process

1.7 Research contributions

This research designed and demonstrated a bio-immunology inspired ICS security model. The model can be used in cases where there is a need to prevent attacks on ICS that alter how the ICS behaves.

This research has brought about the thinking of emulating the biological immune system properties instead of the more commonly known ideology of modelling immune system functionalities into mathematical models. Most artificial immune systems that are in existence today endeavoured to model immune system functionalities like the negative selection and clonal selection principle. This study proposes that it is worthwhile to emulate immune system properties by using computational means that are already understood in computer science.

Ultimately, this research contributes to the field or domain of ICS security which transitively implies that it also contributed to the field of IT security. Finally the research also had book contributions through publications listed on page ix.

1.8 Thesis organisation

This thesis has seven chapters. Chapter one: ***Introduction,*** presents a background of the study, research problem, research objectives and questions, rationale, research scope, research methodology overview, research contributions, summary and the thesis organisation.

Chapter two: ***Industrial Control System Security Vs Advanced Persistent Threats,*** contains an introduction to the chapter, description of ICS, ICS networks and ICS networks security. After the description of ICS networks security follows a description of APTs, current ICS research and finally the summary of the chapter.

Chapter three: ***Emulating Biological Immune System,*** starts with the introduction to the chapter followed by a description of innate immune system, followed by a description of the adaptive immune system. A description of the biological immune system properties comes next which is followed by an outline of the artificial immune systems and their challenges. After this is an outline of how to emulate the biological immune system to solve APT problem in ICS. This section is followed by a comparison of the ICS security and biological immune system. The summary of the chapter comes right at the end.

Chapter four: ***Research Methodology*** consists of an introduction to the chapter, research paradigms and philosophies, design research methodology, qualitative research methodology,

quantitative research methodology, research methodology adopted for this research and finally the summary of chapter four.

Chapter five: ***Bio-immunology Inspired ICS Security Model Design*** begins with an introduction to the chapter followed by a model justification, model description, model development methodology, designing a bio-immunology inspired ICS security model, description of how to use a bio-immunology inspired ICS security model, evaluation of the bio-immunology inspired ICS security model and finally a summary of chapter five.

Chapter six: ***Bio-immunology Inspired ICS Security Model Evaluation*** commences with an introduction of the chapter which is followed by demonstration and evaluation steps, the results analysis follows and then finally a summary of the chapter.

Chapter seven: ***Overall Research Conclusion***, like all the other chapters commences with an introduction of the chapter which is followed by research contributions, reflection, lessons learnt, research limitations, recommendations for future research and the final concluding remarks

1.9 Summary

Chapter one is an overview of the research and outlines background information on ICS and how they are secured. It is shown in this chapter that ICS are being attacked by advanced persistent threats and the identification of the problem that was under investigation:

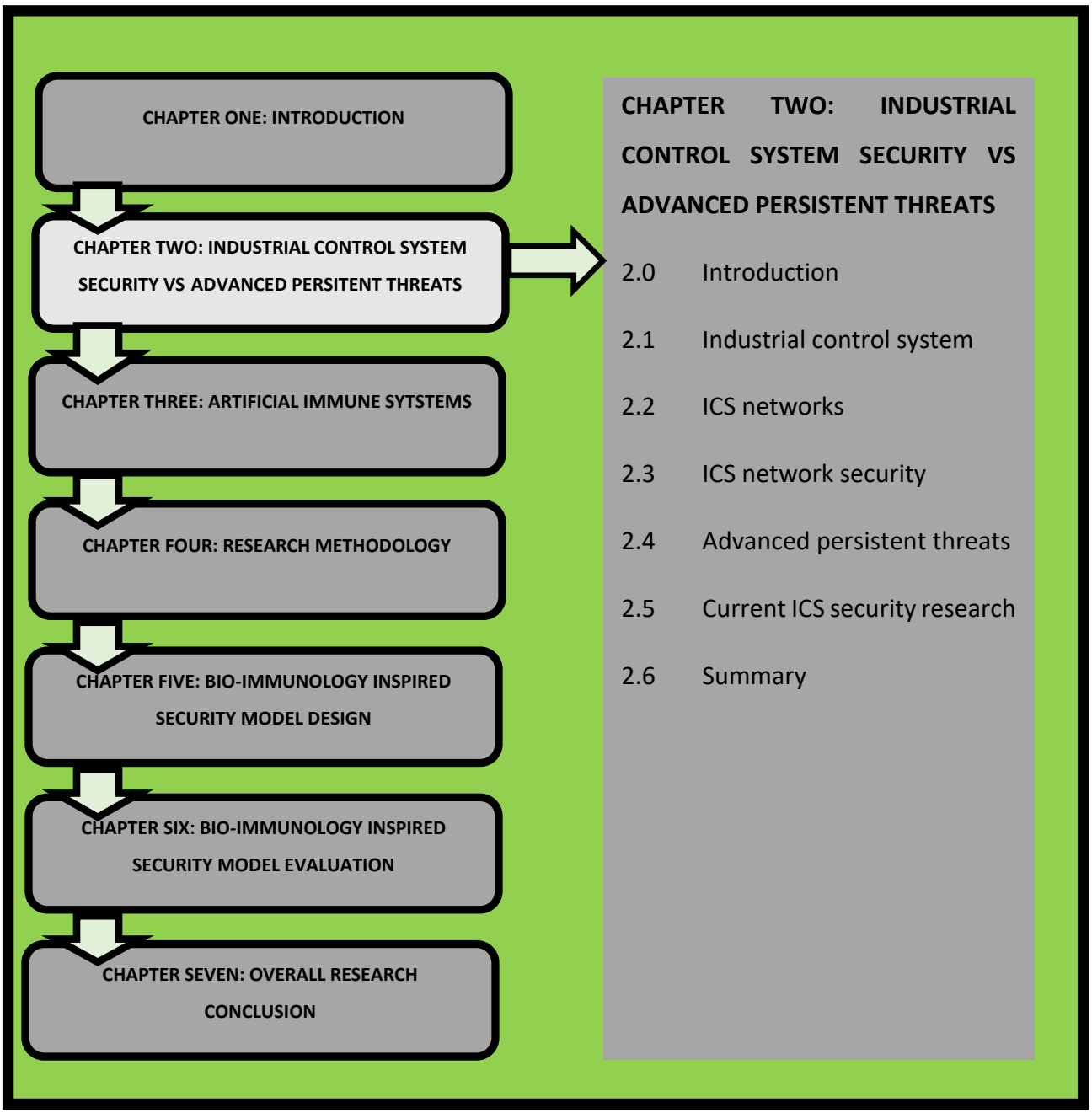
There was no known technique available to identify APTs that attack ICS because APTs are discovered after they have been in the system for some time and usually only after they have executed their payload

The problem was addressed using design science research methodology to answer the questions:

1. Where and how do APTs attack ICS?
2. Why do APT attacks happen: Are ICS vulnerabilities from ICS inner workings / operations, security strategy site or something else?
3. What approach can be considered in either case to avoid APTs attacks?

The chapter also outlined the rationale of the study, scope of the study, and research contributions.

CHAPTER 2 : INDUSTRIAL CONTROL SYSTEM SECURITY VS ADVANCED PERSISTENT THREATS



CHAPTER OUTLINE

The first section discusses ICS operations in general so that the reader can get an overview of how an ICS operates. Following is a discussion on ICS networks and ICS security in its current form. It is established at the end of this section that even though ICS are secured, they are being attacked by APT. This leads to a discussion of APT, what they are, how they attack ICS and why they are successful in ICS. To conclude the chapter, current ICS security research is discussed in view of how it can be used to circumvent APT from attacking ICS.

2.0 Introduction

This chapter discusses Industrial Control Systems (ICS) and Advanced Persistent Threats. In general, an ICS produces a desired output through a controlled process. ICS are networked systems which need to be segmented so that business operations do not overlap with supervisory and control segments. ICS are now connected to business operations, thus it was imperative that they be secured from attacks. Thus, ICS security standards evolved in an effort to secure ICS from attacks. However, despite the security implementations, ICS are being attacked by APT which are persistent and they will almost always achieve their objective.

2.1 Industrial Control System (ICS)

ICS manage the automation of many industrial processes like food manufacturing, air traffic control, mining industries, wastewater treatment and nuclear plants.

"A control system is a device, or set of devices, that manages, commands, directs or regulates the behaviour of other devices or systems" ("Control System | Closed Loop Open Loop Control System," n.d., para. 2). An ICS environment is made up of several control components (e.g., electrical, mechanical, hydraulic, pneumatic) that interact to attain an industrial objective (Stouffer et al., 2015). According to Stouffer et al. (2015):

- Output is the result of the process;
- The control part can be fully automated or manual;
- Has requirements of the desired output or performance;
- Systems can be configured to operate in the open-loop, closed-loop, and manual mode

    - The output for open-loop control systems is managed by pre-determined settings;
    - In closed-loop control systems, the output has an effect on the input in such a way as to maintain the desired objective;
    - Humans control the system in the manual mode.
- The controller is responsible for specification maintenance;
- A characteristic of ICS is that they may have a number of control loops, Human Machine Interfaces (HMIs), and remote diagnostics and maintenance tools connected via network protocols.

The term ICS is actually a generic term encompassing different variations of control systems namely SCADA, DCS, PCS and smart grid. ICS are used to perform monitoring, data logging, alarming and diagnostic functions so that large and complicated processes can be operated in a safe manner and be maintained by a relatively small staff (Sosik, 2003). Sosik (2003) defines monitoring, alarming, data logging, and alarming functions as follows:

- Monitoring functions provide a visual interface between the controlled process and operator;
- Data logging means storing all control system data into electronic records;
- Alarming functions which are integrated into the graphical user interfaces are functions that set off and display alarms as they happen and in some cases they automatically notify operating staff; and
- Diagnostic functions are statistical functions that are used for online analysis of process data to detect when it has been changed for no reasons.

2.1.1 SCADA

SCADA systems are distributed control systems that are used to control processes that are situated far from each other. SCADA is often used by utilities to automate the distribution of water, electricity, natural gas, oil, wastewater collection and in transportation. Critical data acquisition from remote stations, sensors, control devices and monitoring systems are integrated into one control system. SCADA system components frequently consist of Programmable Logic Controllers (PLC).

2.1.2 DCS

A DCS is a system deployed and controlled in a distributed manner. This means that various distributed control systems or processes are controlled individually (Knapp & Langill, 2015a). DCS controls industrial processes located on a site like electricity generation, water treatment, beverages and food production. DCS are most commonly found in process based industries (Stouffer et al., 2015). In addition, a DCS typically communicates with LAN networks.

2.1.3 Smart grid

The smart grid, another type of ICS, is a computer based remote control and automation of electricity transmission, distribution, delivering and metering system. When the smart grid is connected to other ICS modules, the smart grid is a bit more critical than other ICS elements in that the other types of ICS like SCADA, DCS and PCS will depend on it for supplying energy.

Stouffer et al. (2015) state that the largest number of ICS implementations is a hybrid of SCADA and DCS.

The way ICS operates can best be explained by understanding how the different control components work together.

2.1.4 Programmable Logic Controllers (PLC)

A PLC is a dedicated industrial computer for automating functions. PLCs are special purpose computers that can be deployed in a production environment. PLCs are usually designed for specific industrial uses. They have multiple specialised inputs and outputs. Commercial off the shelf operating systems (OS) are usually not available for PLCs, therefore they have application programmes that are developed particularly for them in such a way as to automate the expected outputs (Knapp & Langill, 2015).

Since PLC control real-time processes, they are designed for simple efficiency, therefore logic is simple and programmed by following an international standard set of languages as defined by IEC-61131-3 (Knapp & Langill, 2015). A PLC may replace a Remote Terminal Unit (RTU) or it can work in conjunction with one (Macaulay & Singer, 2012).

PLCs are connected to sensors and actuators. Most of the time PLCS are designed in such a way that if contact is lost with the main SCADA or DCS, it can safeguard the assets under management (Macaulay & Singer, 2012). Modern day PLC have advanced architecture which does not only have processing capabilities but might also have human-machine interfaces (HMIs), convergence of multiple process types, the ability to either receive and respond to process events, and more.

PLCs are not only used in SCADA control systems but they are also used in DCS and PCS control systems where they regulate, monitor and evaluate industrial processes like water temperature. PLC normally interfaces with LAN networks.

2.1.5 Intelligent Electronic Device

The IED is "Any device incorporating one or more processors with the capability to receive or send data/control from or to an external source (e.g., electronic multifunction meters, digital relays, controllers)" (Stouffer et al., 2015, p. B-8). Various industries have distinct physical and logical requirements; therefore, each industry has its own set of IED. "IEDs provide a direct interface to control and monitor equipment and sensors may be directly polled and controlled by the control server and in most cases have local programming that allows for the IED to act without direct instructions from the control center" (Stouffer et al., 2015, p. 2-5)

2.1.6 Data historian

A data historian is a device with a centralised database that is used for data analysis and statistical process control techniques (Stouffer et al., 2015).

2.1.7 Remote Terminal Unit (RTU)

An RTU is also known as a remote telemetry unit is a specialised data acquisition and control unit remote field device that has inbuilt wired or wireless network capabilities to communicate to the supervisory controller which can be a master terminal unit (MTU), a central PLC or an HMI (Knapp & Langill, 2015; Stouffer et al., 2015). An RTU resides in substations, along pipelines, or other distant sites (Knapp & Langill, 2015). The capability and functionality of the RTU and PLC often overlaps (Knapp & Langill, 2015; Macaulay & Singer, 2012).

2.1.8 Supervisory workstation

A supervisory workstation presents information about the controlled purpose for supervisory purposes only. They have no control functions like an HMI and they are primarily read only.

2.1.9 Human Machine Interface (HMI)

An HMI can either be hardware, software or a combination of both, which allows humans to interface with the controlled process. HMIs substitute physically activated switches, dials, and other electrical controls with software parameters which allow for easy adaption and adjustment. This means that they enable control engineers to adjust settings, configure set points and control algorithms. In case of an emergency, an HMI can be used to bypass automatic control operations. HMIs graphically represent the controlled process along with sensor values and other measurements, historical information, reports and output state. The HMI interacts with ICS servers or controllers through industrial protocols (Knapp & Langill, 2015; Macaulay & Singer, 2012; Stouffer et al., 2015). They come in two form-factors (E. D. Knapp & Langill, 2015a):

- On systems like Windows OS, and
- A combination of an industrial hardened computer, local touch panel, packaged to support door or direct panel mounting.

The security of ICS is largely dependent on access control and the host security of an HMI (Knapp & Langill, 2015a).

Thus to sum it up, any type of ICS works as depicted in Figure 2.1. ICS components are the different devices interconnected to form different types of ICS as indicated in Figure 2.1.

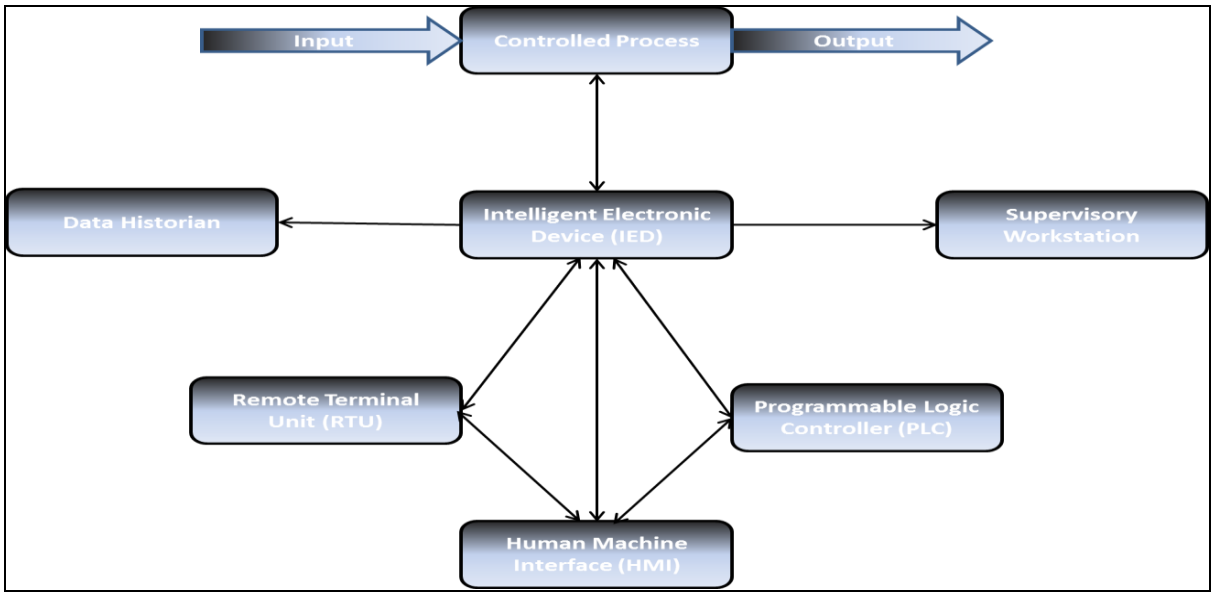


Figure 2.1: ICS Components Operation (Knapp & Langill, 2015)

For any controlled process, IED devices like sensors collect the data about the controlled processes for local processing to send to the RTU or PLC. If data from IED is sent to an RTU then it is a SCADA system. If data from IED is sent to the PLC, then the system is DCS. PLC or RTU make decisions on the controlled process or send the information to the Human Machine Interface (HMI). The HMI will give humans capabilities to make decisions on the controlled process. While all of this is happening in the ICS, data is being captured and sent to the data historian for capturing in a database for further use and to the supervisory workstations for supervisory purposes only.

2.2 ICS networks security

CPNI (2008) and Stouffer et al. (2015) state that before the internet and the World Wide Web existed, ICS were not secured because they were air gaped from other systems. Radvanovsky and Bodsky (2013) highlight that ICS are not secure anymore because:

- ICS are moving away from using vendor specific technologies to commercial off the shelf technologies;
- Control systems are now interconnected to unsecure networks and unsecure remote devices; and

- Control system technical data is now available on the internet.

If ICS vulnerabilities are exploited, then according to Stouffer et al. (2015), there would be denial of service to system operators and DNS services due to control systems disruption, delaying and blocking. This could also cause information transfer bottlenecks. Secondly, unauthorised configurations in the ICS can result in inappropriate plant behaviour like shutting down of processes. Thirdly, if system operators receive inaccurate data they might initiate wrong activities that might negatively impact the system. Forth, infected and modified ICS software will also have negative effects. Fifth, life is endangered if safety systems are tampered with. Sixth, malicious software might find its way into the system, and lastly, incorrect changes to product formulae will result in wrong industrial products.

In general, ICS are designed in such a way that they are reliable and durable (Krotofil & Gollmann, 2013). Another design requirement for ICS is that they must be easy to use (Krotofil & Gollmann, 2013). Taking these requirements into consideration and the ICS security concerns, it became obvious that ICS needed to be secured. Consequently, ICS security standards and frameworks were designed to give best practice guidelines and recommendations on how to secure ICS (Piggin, 2012). Security 'standards' are rigorous security recommendations because they have been proven through research and evaluation (Piggin, 2012).

The recommendations from ICS security standards can be summed into several categories. CPNI categories are that organisations should understand business risk, implement secure architecture, establish response capabilities, improve awareness and skills, manage third party risks, engage projects and establish third party risk (CPNI, 2008). Another example of ICS security standards is NIST SP800-82 Guide to Industrial Control Systems (ICS) Security (Stouffer et al., 2015). In this document, ways to secure the systems using a blend of security policies and carefully configured security measures to form defence-in-depth layering is recommended. QCERT - National ICS Security Standard from Qatar also recommends the use of security policies for each ICS facet which includes the procurement process, organisational security, physical and environmental security, communications and operations management, access control,

information security incident management, business continuity management and compliancy (QNCIS, 2014). Other ICS security standards include:

1. System Protection Profile – Industrial Control Systems - published by National Institute of Standards and Technology (NIST);
2. Cyber Security Procurement language for Control Systems – published by Department of Homeland Security;
3. 21 Steps to improve Cyber Security of SCADA networks – published by U.S department of Energy;
4. NERC CIP standards published by North American Electric Reliability Corporation;
5. ISA-99 Industrial Automation and Control System Security published by US International Society of Automation (ISA).

A typical characteristic observed in the standards is that whenever ICS are secured, a risk based approach to securing systems can be used. This approach must be informed by a balance with operational, business and security requirements (Piggin, 2012). Following is a summary of some of the security recommendations from the ICS standards.

2.2.1 Mitigating reconnaissance attacks

System users must be taught about security issues to increase security awareness. Training and awareness programmes must help teach personnel on the importance of ICS security. Personnel should be trained that they should never reveal data related to ICS like names and contact information over telephones or any other means unless they have been instructed to do so. Organisations should work towards uplifting employee morale, loyalty and retention. Enforcement of when, which, who and how to train on security awareness should be initiated from policies and procedures that the organisation has (CPNI, 2008; Stouffer et al., 2015; USDoE, n.d.).

2.2.2 Access control mechanisms

This section is summarised from a compilation of CPNI (2008), QNCIS (2014), Stouffer et al. (2015), and USDoE (n.d.). Access to the system should be given only after supplying the correct identification material like passwords, biometric identification, identity cards etc. When users gain access they should only access authorised applications. Only applications that are relevant

to ICS operations should be installed in the system. Users accessing the control system from the corporate network should only do so through a firewall in demilitarised zones. The firewalls should have appropriate rules to enable filtering unwanted access. Email and internet access should never be initiated from the control system. Remote access to the system should only be if specific machines for specific services and at specific times have been given access otherwise it should never be allowed. Physical controls must be in place to protect systems from unwanted physical access, and finally, physical access controls to restrict physical access to those devices that display ICS information

2.2.3 Auditing, monitoring and accountability

This section is summarised from a compilation of CPNI (2008), QNCIS (2014), Stouffer et al. (2015), and USDoE (n.d.). An intrusion detection system should be used to monitor access to ICS and devices. The intrusion detection system should alert administrators of behaviour variations in the system and ICS are required to conduct regular vulnerability and risk assessment checks. The tests should check operating systems, infrastructure, network access, processes and procedures. In this way, vulnerabilities should be kept at minimum. Communication channels between ICS administrators with vendors supplying systems must exist to enable reporting of any vulnerabilities discovered. Real time monitoring of firewalls and other security sensors should also be implemented. System configurations should be monitored for any unauthorised changes. There are recommendations that organisations must conduct regular audits of the ICS systems. Auditing results should verify that correct access is being given to the authorised users and processes. In addition, audit results should give a clear picture of applications existing in the systems, the role of each system, their business, where they are in the system and the owners and managers of each system.

From the discussion given in section 2.2 it is apparent that ICS are now being designed with security in mind. ICS networks are segmented, meaning that the business part of the network and the control and supervisory part of the network are not connected. This means that if there are any problems in one segment of the system then it should not affect the other parts. In line with this is that ICS security standards have been developed and if followed they should be able to sufficiently defend ICS from any attack. But the reality is that in most cases best practice

guidelines are not followed and vulnerabilities are introduced in the network. That is why ICS are being attacked by Advanced Persistent Threats (APT). APT have been discovered in ICS since 2010 with the discovery of Stuxnet APT. Stuxnet sought to sabotage the Iranian Natanz Nuclear Enrichment Facility operations. The ultimate goal for Stuxnet was to change the frequency settings in a cycle so that centrifuges would spin out of control. After the discovery of Stuxnet, many other APTs like Shamoon, Wiper, miniduke, NetTraveler, Equation, etc. have been found lurking in ICS. Therefore pertinent to ask is: What is an advanced persistent threat?

2.3 Advanced persistent threats

2.3.0 Introduction

One of the biggest threats to ICS has been the advent of APT. APT are very sophisticated attacks which do not find glory in the number of sites attacked like the normal worms and viruses we are used to. APT are targeted attacks that are tailor made to attack only certain sites at the right time and conditions. If the time, site and conditions are not met an APT will never execute. APT were first discovered in 2010 with the discovery of Stuxnet. Ever since, there have been quite a number that have been discovered. Table 2.1 shows a list of APT that were targeting ICS exclusively or as one of the targets. Table 2.1 also lists, the year the APT was discovered, the infection method used by the APT to gain entry into its target system. Table 2.1 was mainly compiled from Kaspersky's Targeted Cyberattacks Logbook ("Targeted cyberattacks logbook," n.d.). From the table it can be derived that the average time taken to discover APTs is 3.4 years.

Table 2.1: Advanced Persistent Threats in ICS

APT	Intention	Infection method	Year Discovered	First known sample
Stuxnet	Cybersabotage	File infection, LAN spreading, USB cables	2010	2007
Shamoon	Data Wiping	LAN spreading	2012	2012
Wiper	Data wiping	unknown	2012	2011
Adwind	Cyberespionage, surveillance	Exploits, Social engineering	2013	2012

Cosmicduke	Data wiping	Trojanised software installers	2013	2012
Miniduke	Cyberespionage	Spear Phishing	2013	2008
TeamSpy	Cyberespionage, data wiping	Social engineering - spear phishing, Exploits	2013	2004
NetTraveler	Cyberespionage, data wiping	Social engineering – spear phishing, Watering hole attacks, Exploits	2013	2004
The Mask/Careto	Cyberespionage	Spear phishing	2013	2007
Equation	Cyberespionage, data theft, surveillance	USB drives, Exploits, Self-replication, Physical media, CD-ROMs	2014	2002
Blue Termite	Cyberespionage, data theft, surveillance	Social engineering Exploits, Watering hole attacks	2014	2013
Crounching Yeti	Data wiping	Spear phishing using PDF documents embedded with a flash exploit (CVE-2011-0611), Trojanised software installers, Waterhole attacks using a variety of re-used exploits	2014	2010
Desert Falcons	Cyberespionage, data theft, survellaince)	Social engineering (spear phishing, facebook	2014	2011
Poseidon	Cyberespionage, Remote control, Surveillance	Social engineering, Exploits	2015	2015
Ghoul	Cyberespionage	Social Engineering	2016	2015
Shadowpad	Remote control	Trojanized software installers	2017	2017
Expetr	Data wiping, Stealing money	Exploits, Watering hole attacks	2017	2017

2.3.1 APT description

APT are designed in a way that makes them very sophisticated multistep cyberattacks (Virvilis, Gritzalis, & Apostolopoulos, 2013). They target only specific targets unlike the normal worms and viruses which leverage on targeting as many victims as possible. APT are multistep attacks that follow a specific set of steps in order to successfully penetrate a target network. The steps that an APTs typically follows are (Fortinet, 2013; Giura & Wang, 2012):

- Choosing a victim,
- Reconnaissance,
- Delivery,
- Exploitation,
- Operation, and
- Data collection and exfiltration

2.3.1.1 Choosing a victim

The first stage of an APT attack is when the attacker chooses their victim. They select which entities they intend to attack. At this point the attacker makes a decision on the ultimate goal of their attack. For example, the attacker will decide that they want to steal data, spy on the organisation, get remote control capabilities, wipe data or sabotage operations (Virvilis et al., 2013).

2.3.1.2 Reconnaissance

Just as the name of the stage implies, at this stage the attacker gains as much information about their target as possible. Network scanning and mapping techniques can be used to gather intelligence about their target. Also at the attacker's disposal is the use of social engineering, social networks, employee profiling, and phone directories to get information (Virvilis et al. 2013). After this investigation, the attacker will now have a way to penetrate their victims' organisation.

2.3.1.3 Delivery

After the reconnaissance step, the attacker will now know the vulnerabilities that exist in the target organisation's network. They will use the vulnerabilities to develop exploits that will be attached to pdfs, docs, ppts, etc. These exploits are delivered to the attacker's victim (Bhatt, Yano, & Gustavsson, 2014). Several injection methods as shown in Figure 2.2 are used by APT to gain access (Ponemon Institute LLC, 2013).

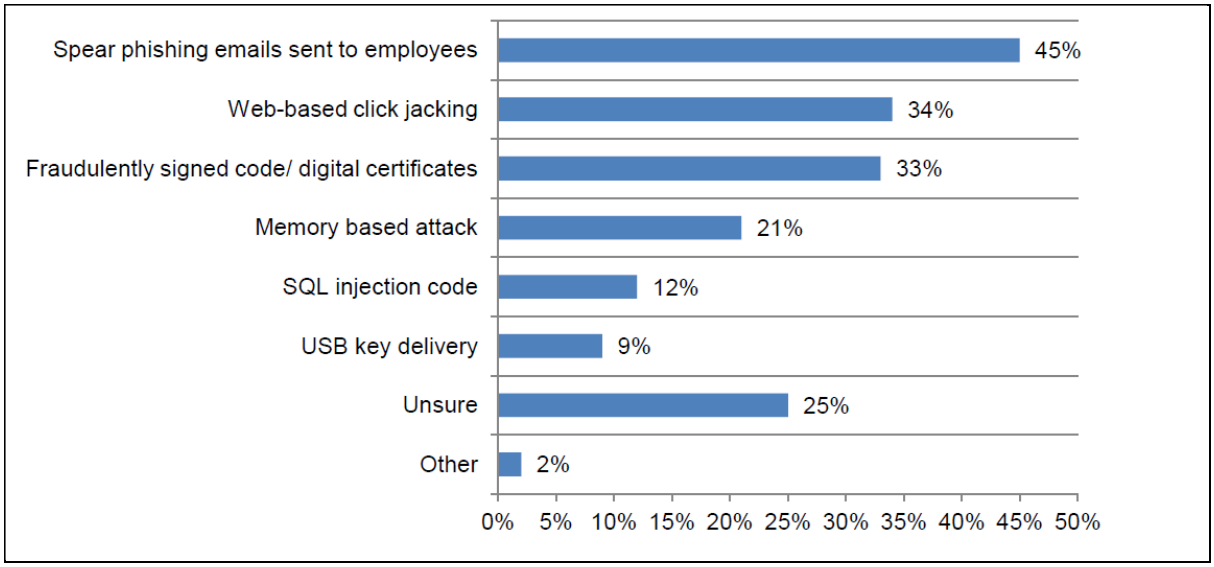


Figure 2.2: Advanced Persistent Threats in ICS

2.3.1.4 Exploitation

Once the APT is now in the system, it forms a communication channel with its command and control centre. Data about the victims' computers is gathered and sent to the command and control centre (Giura & Wang, 2012). Since the APT will now be in the system, it is at liberty to unleash its payload (Bhatt et al, 2014).

2.3.1.5 Operation

This is the stage when the attacker persistently remains present in the system. If required, the attacker might move laterally in the network to strategic positions, for example servers with sensitive or important information (Giura & Wang, 2012). The APT might also move laterally to gain access to compromise other devices in the system (fortinet, 2013).

2.3.1.6 Data collection and exfiltration

Data is collected, segmented and encrypted. During the time the APT is establishing a redundant connection with the command and control centre as data is kept in temporary servers in the system. The last thing to be done is to send data over encrypted channels to several command and control centres so that it is not clear to which destination the data is going to be kept (Giura & Wang, 2012).

2.3.2 How APT attack ICS

Table 2.1 shows that twelve out of the seventeen listed APT got into systems through the use of social engineering and that counts for approximately 71% percent of the total. The APT stages of reconnaissance and delivery use the art of social engineering to manipulate humans. Top, as highlighted by Figure 2.2 is a spear phishing email, click jacking and USB key delivery. Other methods used are USB key delivery, fraudulently signed code or digital certificates, sql injection and memory base attacks. We look in detail at two APT namely, Desert Falcons as an example of APT that used social engineering to get access, and Stuxnet which used USB key delivery. Stuxnet is also described in detail because it is an example of an APT that managed to sabotage an ICS operation.

2.3.2.1 Desert Falcons

Desert Falcons APT used 4 social engineering tricks; spear phishing, targeted Facebook attacks, just click the shortcut: the rar/lnk trick and fake RealPlayer plugin trick (Kaspersky, 2015) to gain entry into the target system.

1. The first social engineering trick used by Desert Falcon was spear phishing e-mails that aimed to trick the victim into opening a malicious attachment. The targeted people were in government or high profile media. The attachments sent with the mail were well structured and suited to each victim. Take for instance a PDF of a meeting record that was used to target senior politicians in Egypt and Palestine that seemed to contain minutes for a very important meeting between Egypt and Palestine.

2. Just click the shortcut: the rar/lnk trick was the second method used to get access by Desert Falcon APT. The rar file was extracted to many files and had a small shortcut icon. Once clicked, a command to extract, setup and run the malware was invoked.
3. The third method employed was the use of targeted Facebook attacks aimed at specific people. They created Facebook accounts to use for chatting with victims until they gained their trust. They eventually sent them Trojan files hidden as images or other things.
4. The fourth and last social engineering trick used by desert falcon was the fake RealPlayer plugin trick. Here malware was delivered as a "plugin" for a "banned video" of a famous political show in Egypt.

We can therefore conclude that attackers exploited victims' trust in social networking forums and victims' curiosity about news relating to political conflict in their country (Kaspersky, 2015).

The fifth way used by Desert Falcons was the Right-to-left extension override trick was an exploit that preyed on the Unicode. What the attackers did was to reverse the order of characters in a file name by exploiting Unicode special characters. By doing this, dangerous file extensions were hidden and only fake trustable file extensions were visible (Kaspersky, 2015).

2.3.2.2 Stuxnet

The description of Stuxnet was compiled from Falliere, Murchu, and Chien(2011) and Nachenburg (2010).

Stuxnet was actually designed to physically damage an actual running process. Stuxnet which was discovered in 2010 is the only APT discovered that actually sabotaged an ICS facility. Stuxnet targeted the Iranian Natanz Nuclear Enrichment Facility. Stuxnet can be viewed as a worm because of its capabilities to spread on its own, a Trojan horse because it could hide its true intentions or it could be a parasitic virus because it could attach itself to programmes and could infect any Windows PC but it would only infect PLC from Siemens. So how did Stuxnet achieve this fit?

It is believed that Stuxnet gained entry into the system through USB sticks. Once it got in the facility it would spread on its own. It used 7 ways to spread to new computers and six of the methods were zero-day exploits. Zero-day exploits take advantage of previously unknown

vulnerabilities to software vendors. Stuxnet did not just activate; it made sure that it was on the correct target. The correct target:

- must be running STEP7 software from Siemens,
- must be directly connected to an S7-315 Programmable Logic Controller from Siemens,
- its PLC must further be connected to at least six CP-342-5 Network Modules from Siemens, and
- must have network module connected to ~31 Fararo Paya or Vacon NX frequency converters.

When all of these are met, Stuxnet triggers its payload. First it delivers its malicious logic to the PLC, then checks to see that the motors are running between 807 and 1210hz. For thirteen days Stuxnet would measure normal operating speed of the frequency converters. Next it would increase the spin rate to 1410hz for fifteen minutes then sleep for twenty seven days. After twenty-seven days Stuxnet would reduce the spin rate to 2hz for 50 minutes. This process is repeated many times over. The safety instrumented systems failed to detect a problem because Stuxnet recorded the correct settings which it sent whenever it launched an attack. This false feedback would make it look as if the operation is running normally. In addition, Stuxnet had disabled the emergency kill switch.

How did Stuxnet hide from detection? It used five ways to conceal its presence:

1. Used stolen digital certificates from RealTek and Jmicron to appear as if it is legitimate software,
2. Concealed malicious change to PLC logic from the operators,
3. It would delete itself from a USB if it had infected three machines,
4. Hide its files on USBs by using two rootkits, and
5. It exhibited different behaviours in the presence of different antivirus applications.

2.3.3 Why APT are successful in ICS

We can derive from the examples given that ICS security in its current form is not sufficient to detect APT. It would seem that if best practice guidelines (standards) are followed then it would be difficult for APTs or any malware to gain access. However, it was shown in Table 2.1 that most

APT target human weaknesses to gain entry into systems. Desert Falcons and Stuxnet discussed in section 2.4.2.1 and 2.4.2.2 respectively clearly show human involvement in the propagation of APT. Thus, even though there might be well articulated technical security configurations, humans would still introduce APTs in systems. Humans are easily fooled into revealing sensitive information and into doing things that are contrary to security best practices.

Although security recommendations clearly spell out that personnel should be taught on the importance of keeping ICS safe and not to divulge information to unauthorised people, if the attackers are determined enough, then they will most definitely catch a person off guard. Learning about ICS is also made easy by social websites where information sharing is the norm. Not only can information be found using reconnaissance techniques but the disgruntled worker can be a willing participant in sharing information or might just be the executor of the attack as was seen in the Maroochy water plant incident in Australia (Slay & Miller, 2007).

Although humans have their weaknesses that make them download files from unsecure sites and use unscanned USBs, it can be argued that even if this is the case, technical security controls should detect APT once in the system. Firewalls, intrusion detection systems and access control mechanisms should detect that there is a problem in the system. But why do all these security parameters not detect APT? This is because:

1. APT have sophisticated camouflaging techniques like rootkits and 'legitimate' digital signatures that enable them to stay under the radar;
2. They delete all evidence of ever being present in a system after a certain time or after certain conditions have been met;
3. They present fake information to monitoring personnel or monitoring systems so that everything appears normal;
4. APT have rootkit functionalities, thus when APT have successfully infiltrated into a system they escalate their rights in order to install additional software required. Thus, security conditions that only authorised software should be installed in the systems are bypassed by this APT functionality;

5. Antivirus, intrusion detection systems (IDS) and prevention mechanisms are easily circumvented by APTs because they rely on previously known malware signatures in order to detect intrusion. APTs use zero-day exploits to compromise the system whose signatures are not recognised by these systems. Thus, relying on already known signatures to detect an attack that is not yet documented is fruitless. Some IDS that depend on the use of anomalous behaviour in the system to detect intrusion in most instances such IDS have proved to give false positives and thus they cannot really be relied on in securing systems. The fact that many APTs also have the capability to hide their presence in the system or to camouflage their use of the system, activities emanating from APT may not be detected as anomalous behaviour in the system; and
6. APTs once in the system communicate with their command and control centre outside the ICS for further instructions or updates.

Network segmentation and zoning is implemented to increase security but what this means in as far as protecting ICS from APTs is that since APT will get into the system and pose as legitimate entries, segmentation barriers will not really indicate when an APT is in the system. What can be monitored as far as segments are concerned is the traffic between the segments. The system can be monitored to find out whenever there is a difference in traffic flow between the segments. In this way normal traffic can be differentiated from what is not normal and if there is a change then it must be raised as an alarm or reported as an anomaly.

After all, if the security controls have failed the safety instrumented systems should still be capable of detecting problems and they should transition the process to a safe state but as we can see from Stuxnet, APT would also present fake information to these systems so that everything would appear as if it is normal. If a situation which is not rated as dangerous occurs, like data theft, then the SIS system treats this as normal and continues operations and does not generate any alarms. Because SIS use the same technology as the control system, an attacker compromising ICS by exploiting ICS vulnerabilities that are similar to SIS vulnerabilities might as well compromise SIS because the vulnerabilities are similar.

2.4 Current ICS security research

2.4.0 Introduction

The increase in the number of APT meant that current ICS security implementations were not effectively deterring APT. Therefore, research to improve ICS security is being carried out. These studies aim to find ways in which APT can be detected and stopped. The approaches that are being taken to solve the APT problem in ICS can be grouped into five subcategories:

2.4.1 Anomaly detection

Averbuch and Siboni (2013), de Vries et al. (2012), Skopik, Friedberg, and Fiedler (2014) propose the use of anomalous Intrusion Detection Systems (IDS). An anomaly based IDS builds a baseline system behaviour that is used as a basis for detecting behaviour that deviates from the norm. When deviation from normal behaviour is detected an alarm is sounded. What differs in the approaches taken by the researcher mentioned above is in how and which information should be used as a baseline. For example, Skopik et al. (2014) propose the use of "system events, their dependencies and occurrences", while De Vries et al. (2012) propose to use "network traffic, client data at multiple locations in a network" and Averburch and Siboni (2013) propose the use of big data analysis of normal network traffic.

De Vries et al. (2012), propose that the reference point should be built from "network traffic, client data at multiple locations in a network". de Vries et al. (2012) developed an analysis framework to relate attack characteristics to detection and location methods. The framework can be used to design sophisticated IDS and also on where in the network an IDS should be placed and what the IDS should detect. McLaren, Russell and Buchanan (2017)'s anomaly detection technique utilises data mining and classification algorithms.

Because ICS normally exude predictable behaviour, detecting APT using the anomalous detection mechanisms should be effective. A flaw with the approaches described above is that most of them propose to sound the alarm after the APT has been in the system for a while because they believe a false alarm might be raised if they are raised earlier. Since ICS behaviour is known and

predictable, we believe that raising alarms earlier in the APT lifecycle should still be accurate for the most part.

2.4.2 Tweaking security controls

This approach which can be exemplified by Virvilis et al. (2013) and Bhatt et al. (2014) hinges on refining and tightening existing security configurations. The aim is to make sure that those security controls that are already available are implemented as they should. This method also recommends hardening security controls circumvented by APT. This means that all vulnerabilities exploited at each APT stage can be hardened.

Ussath, Jaeger, Feng Cheng and Meinel (2016) propose tightening already existing security controls focusing on special characteristics of APT. As an example, they suggest the use of tools like the Enhanced Mitigation Experience Toolkit (EMET), hash and password dumping and the use of Standard Tools and Techniques like log data to detect characteristics that are peculiar to APT. Paradise et al. (2017) propose tightening security by using social network honeypots which would aid in detecting APT at the reconnaissance stage.

In this anomaly detection technique, Siddiqui, Khan, Ferens and Kinsner (2016) introduce a fractal based classification mechanism. The technique utilises a machine learning algorithm for fractal dimension representation of the network layer level C&C communication protocol of APTs that use TCP based network connections.

2.4.3 Anomaly detection and tweaking security controls

This approach presented by Virvilis and Gritzalis (2013), and Giura and Wang (2012), involves combining the methods in section 2.5.1 and 2.5.4. This means combining the defence-in-depth (explained in section 2.5.4) strategy and anomaly based IDS. The system will use anomaly intrusion detection methods and defence-in-depth approaches, thus inheriting the advantages of both methods. This can be viewed as the best approach to detecting APTs because it combines many methods, making it difficult for an APT to exploit the system.

2.4.4 Defence-in-depth

The defence-in-depth strategy is recommended as a means to secure ICS by many ICS security standards. Chapple and Seidl (2015, Chapter 9: Defence-In-Depth Strategies: Overview; para. 4)

say that “Defence-in-depth is the idea that defences should have more than a single layer of protection between an attacker and the protected systems, data, or networks”. Employing this method means that the ICS has different layers and methods that prevent attackers from gaining entry. This is because when a layered approach is used an attacker does not only have to compromise a single point of weakness but several (Chapple & Seidl, 2015). Using the defence-in-depth strategy implies that several security implementations must be layered between a protected asset and the attacker (Amoroso, 2011).

Figure 2.3 is a depiction of a common defence-in-depth model. (E. Knapp, 2011) states that since ICS are segregated, then defence-in-depth should be applied in the following contexts:

- The layers of the Open Systems Interconnection (OSI) model, from physical (Layer 1) to application (Layer 7);
- Physical or Topological layers consisting of subnetworks and/or functional groups;
- Policy layers consisting of users, roles, and privileges;
- Multiple layers of defence devices at any given demarcation point (such as implementing a firewall and an IDS or IPS).

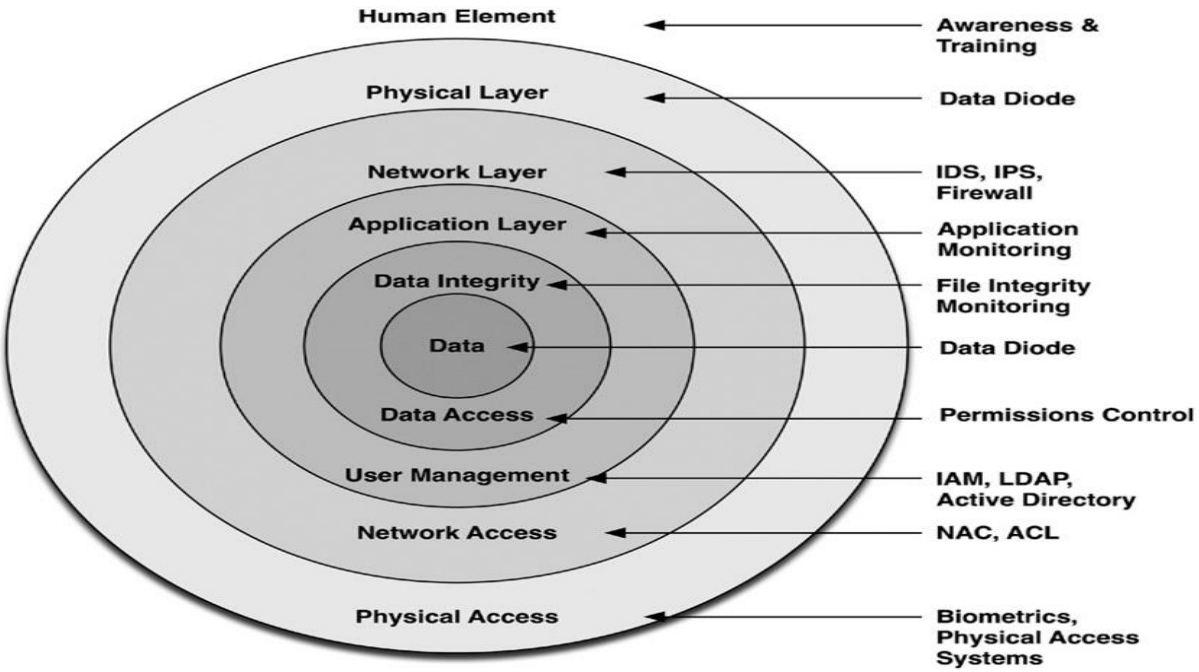


Figure 2.3: Defence in Depth with Corresponding Protective Measures (Knapp, 2011)

Tankard (2011) states that the layered security approach requires organisations to do log analysis, file integrity checking, registry monitoring, rootkit detection, outbound traffic analysis and to encrypt databases, files, backup and storage systems. Tankard (2011) suggests outbound traffic analysis because many APT have been designed to steal data out of the system.

Baize (2012) puts forward the idea that defensive software must be enhanced by developing attack-aware software. Attack-aware software would enable early APT detection but this should not work on its own, secure software must have the capability to "log and report incidents that have been prevented" (Baize, 2012, p. 90). This means that in addition to what the software does, it becomes a threat intelligence source for better monitoring.

Giura and Wang's (2012) APT detection framework gathers data from all attack planes and links that data in order to detect an APT within a context.

DNS intelligence communication patterns and domain and net-block reputation, geo-location and data origin should be used on intelligent systems that detect malicious traffic to dissect command and control protocols (C&C) (Sood & Enbody, 2012). The perfect scenario of the above

would be when a suspicious code is executed in a virtual environment. Other layers of security that Sood and Enbody (2012) suggest are to educate users and to include traditional security measures, patching operating systems, updating software, etc.

In this multi-layered approach, Fortinet (2013) suggests a protection mechanism characterised by among others:

- security partnerships with security organisations that provide threat intelligence,
- network segregation,
- web filtering ,
- application whitelisting,
- network access control, and
- user education.

Bhatt et al. (2014) also believe in solving the APT problem by using a layered security approach. They designed a framework that uses Intrusion Kill Chain (IKC) to detect APT early in their lifecycle. This framework works by increasing the complexity that would be required to carry out multi-stage attacks. In addition, the framework mentions that data logs from the layered approach should be correlated. Similarly, Saud and Islam (2015) propose correlating network events by using a honeypot and network IDS. Brewer (2014) also adds to this notion of correlating network activity. Brewer (2014) points out that 360-degree visibility network activity by analysing logs that are kept during APT stages. Lu, Chen, Zhuo and Zhang (2017) also suggest collecting and correlating temporal-related features and traffic-related features in a big data analytic filter for APT traffic. This method of correlating seemingly unrelated data is put forth by Zhang, Li and Hu (2017) who used OpenIOC for a detection framework that is established for characteristics based on IKC and a calculation based on Tactics, Techniques and Procedures (TTPs). OpenIOC is an extensible XML schema that is used to give a technical characteristic description to detect a known threat, an attacker's methodology or other evidence of compromise.

Every APT attack stage should be viewed as a different attack (Brogi & Tong, 2016). These different attacks can be detected by an IDS. They developed a tool called TerminAPTor that correlates the different attacks by using Information Flow Tracking (IFT). Messaoud, Guennoun, Wahbi, and Sadik (2016) also proposed using the different APT stages to detect them. Messaoud et al. (2016) proposed to use various security measures like sandboxing, honeypots, Security Information Event Management (SIEM) and User Behaviour Analytics (UBA) to detect different APT phases.

Layering security parameters makes it difficult for APT to bypass all of them to gain entry into a system. This approach we believe is the future of ICS security. In as far as APTs are concerned, a shift from the much used signature detection IDS to anomalous detection IDS should be employed. The only problem with the anomalous detection mechanisms being designed for APT detection is that they sound an alert late in the APT lifecycle. Normally an ICS system remains constant for extended periods and it has predictable behaviour. As such, it should be possible to design an anomalous detection IDS which sounds an alarm in APT initial stages. Thus, this research contributes to the development of a bio-immunology inspired early alert security model for protecting ICS. When this model is employed, then APTs should be detected much earlier in their lifecycle

2.4.5 Controller run-time security

One other evolving way to protect ICS from Stuxnet-like APT is that of modelling the controlled process and then using it to compare with the actual process to discover deviations from normal behaviour. One such work is that of Lerner, Farag and Patterson (2012) who presented a run-time security technique to protect ICS from "Stuxnet-like (APT) cyber-attacks.

Lerner at al. (2012) state that "Regardless of how the threat originated, the role of the trusted protection system is to anticipate and deter consequences to the controlled process" (p. 138). Their work hinges on finding malicious or non-malicious action that if accepted and implemented would cause deviations from normal behaviour.

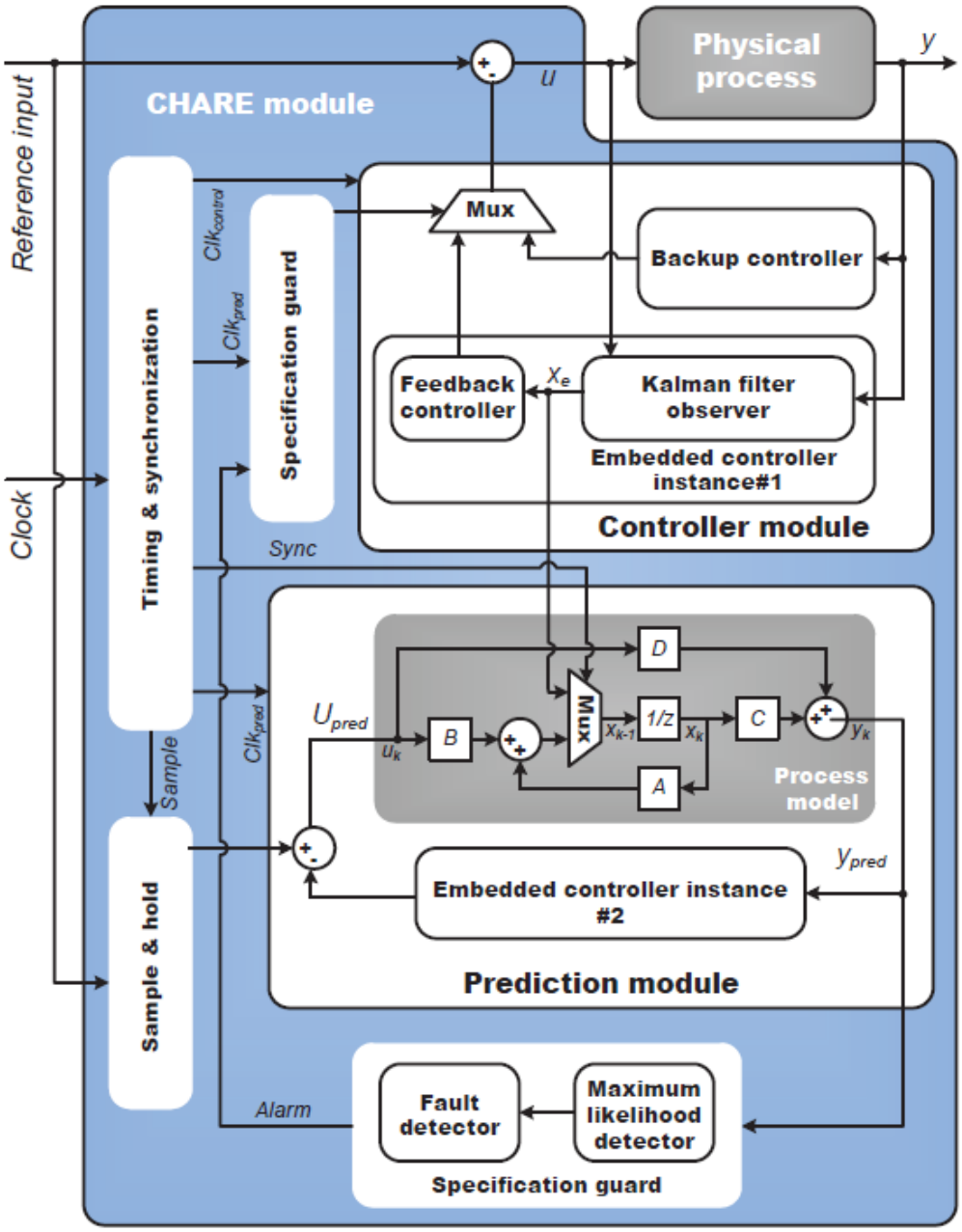


Figure 2.4: Predictive and pre-emptive security architecture (Lerner et al., 2012)

Figure 2.4 shows the security architecture developed by Lerner et al. (2012). The major components of their model are:

- The original controller module containing an active controller-to-be-protected, a high assurance, stability preserving controller, and a mechanism to switch between them. This embedded system module runs at the typical sampling rate of the physical process.
- A prediction module consisting of a process model and a second instance of the active controller. This subsystem runs *n* times faster than the active control system module.
- A CHARE (Configurable hardware assisted application rule enforcement) module that warps the controller and prediction modules. This subsystem consists of specification guards as well as a specialized model synchronisation and timing tools.

A model of the process is used to continuously match the behaviour of the actual process state and expected states. There are three controllers in the whole system: one connected to the actual physical process, the second one is for testing instructions (prediction controller), measurements, etc. before they are sent to the actual controller (controller number one). This controller is exactly the same as the one connected to the physical process. The third one is the backup controller which is trusted to have the correct set of instructions at any given time. The second one which is *n* times faster than the first one compares results with expected results that are recorded in the process model.

Follow up work to this research by Harshe, Chiluvuri, Patterson and Baumann (2015) and Lerner, Franklin, Baumann and Patterson (2014) hinges on modelling the entire ICS operation and then using the model to compare with the current ICS plant state at a particular time. Lerner et al. (2014) used this kind of method to predict software attacks on ICS. They used a backup controller hardcoded to resist software reconfiguration attacks. A production controller is implemented on a soft chip that is connected to the model of the physical process which works ahead of the normal process to know in advance what the controller will do. Franklin, Patterson, Lerner and Prado (2014) used The Autonomic Interface Guardian Architecture (TAIGA) for the same purpose. The difference with what is presented by Lerner et al. (2014) and theirs is that theirs separates

the trusted components by redistributing responsibilities between the Programmable logic Controller (PLC) and hardcoded controllers.

This work by Lerner et al. (2012), Lerner et al. (2014), Harshe et al. (2015) and Franklin et al. (2014) concentrated only on making the process stable.

1. It does not address those attacks that seem to makes changes to the process but at a later stage execute something else. Depending on the actual time between the controlled model and the actual process, a command might be set in such a way that it executes something in the first instance but will later on execute something else.
2. It does not deeply protect the actual process controller because they believe that once the predictive module has detected an attack then there is no way the actual physical controller can be affected.
3. It does not look at the possibility of actually denying input that will potentially harm the system. That is to say, all input is accepted and run by the predictive controller then compared to the physical model for any deviations.

We propose to use a model of the system with a filter such that if the filter already sees a deviation from normally accepted instances then it can already discard these changes before they can be sent to the process.

2.5 Summary

This chapter discussed industrial control systems. It was noted that ICS is a generic term for several systems which encompass SCADA, DCS and PCS. In general, an ICS is composed of PLC, RTU, HMI, supervisory workstations, data historians and IED working hand in hand to produce a desired output through a controlled process

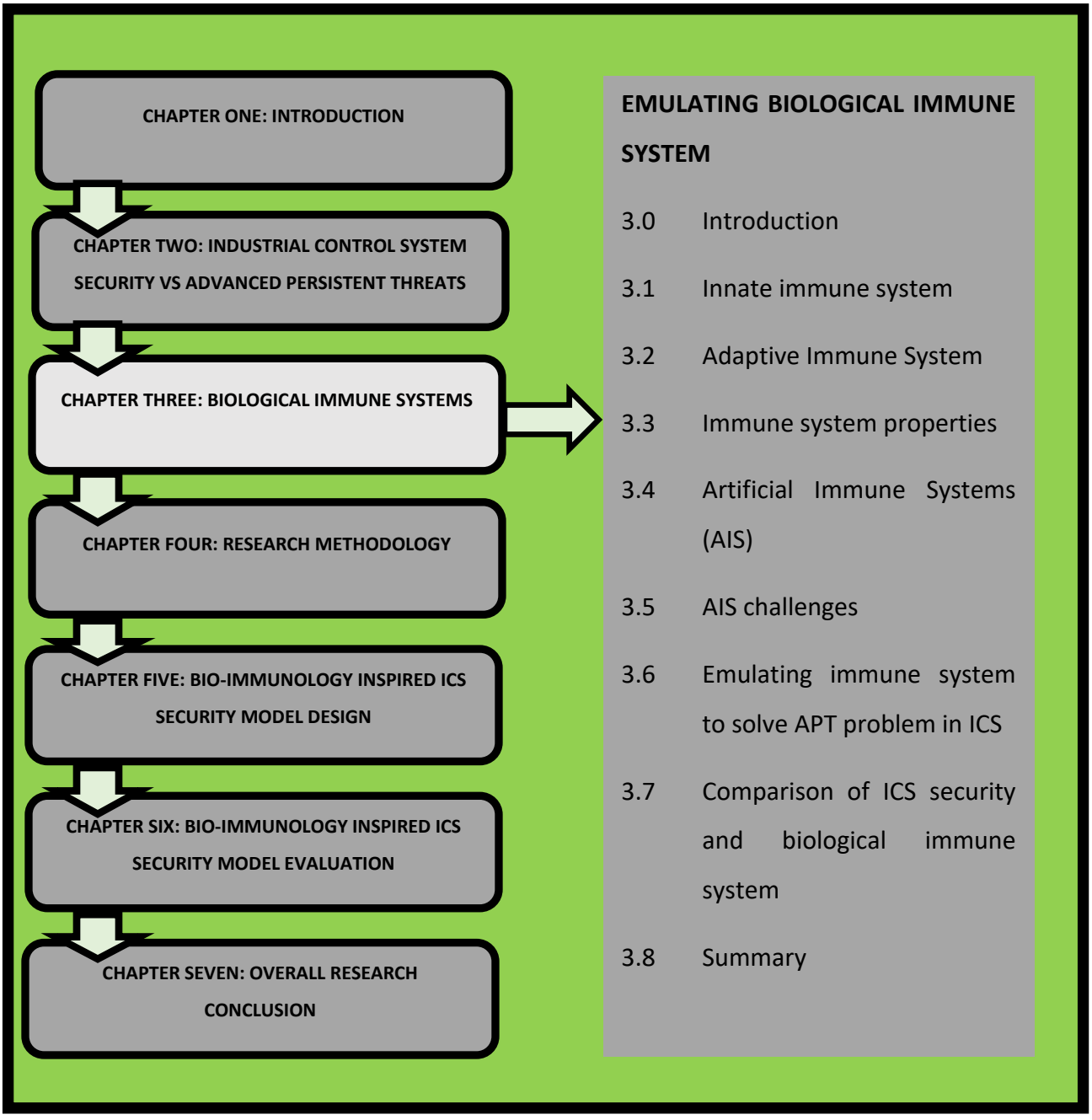
ICS are networked systems. It is recommended that the networks be designed in segments so that business operations do not overlap with supervisory and control segments. In addition, SIS are connected to ICS so that whenever there is a problem SIS would transition the controlled

process to safe conditions. Because ICS are now networked, it was imperative that they be secured from attacks. Thus, ICS security standards evolved in an effort to secure ICS from attacks.

However, despite the security implementations, ICS are being attacked by APT, an APT which is a targeted multistep attack. APT are particularly problematic because they are persistent and will almost always achieve their objective. APT prey on human weaknesses to get access in the systems but despite tricking humans, it is still possible to have technical measures that should detect and stop APT. In light of this, it became necessary to advance ICS security hence the last section of the chapter that discussed current ICS security research which the researcher believed can be further improved to increase ICS security by studying and emulating the biological immune system

The biological immune system is tasked with detecting and protecting the body from harmful microorganisms. As such, it is equated to ICS security systems. ICS security should be capable of detecting and protecting ICS from intruders and malicious activities. Thus, a mapping of the immune system to ICS security mechanisms is proposed and was used to allow ICS computing systems to emulate key functions and components in the immune system for ICS security mechanisms. A discussion of the immune system follows in the next chapter.

CHAPTER 3 : EMULATING BIOLOGICAL IMMUNE SYSTEM



CHAPTER OUTLINE

The Biological Immune System (BIS) is a system that functions as a defender of the body from pathogens through a combination of physical, chemical and cellular components. The innate immune system and the adaptive immune system are two components of the immune system. Actions undertaken between the innate and adaptive immune system to defend the body can be imagined to be in four layers. These layers of biological immune systems security enable it to exude the properties of being distributed, enabling environmental self-awareness, resiliency, intelligence and collaboration, communicating messages and defence-in-depth. Artificial immune systems (AIS) which model operations of the immune systems are used in computer systems. AIS have not been applied successfully in computer systems mainly because they are misunderstood thus, this research proposes to use the properties of a biological immune systems as building blocks for securing ICS instead of trying to model the biological immune system operations.

3. 0 BIOLOGICAL IMMUNE SYSTEM

The biological immune system is a system that functions as a defender of the body from pathogens through a combination of physical, chemical and cellular components (Edgar, 2005). Pathogens are categorised into 4 general categories known as viruses, bacteria, fungi and eukaryotic organisms called parasites. Eukaryotic organisms are those with cells much like ours, with compartmentalised functions all in one cell. Eukaryotes divide different functions of the cell to different locations of the cell, for example, mitochondria which are cellular energy exchangers and lysosome that dispose cellular waste.

The biological immune system is of two types, namely the innate immune system and the adaptive immune system. The innate immune system is responsible for physically blocking and chemically destroying pathogens. On the other side of the immune system is the adaptive immune system which is responsible for humoral immunity; cell mediated immunity and is part of the complement system (Abbas, Lichtman, Pillai, Baker, & Baker, 2016; David Edgar, 2005; K. P. Murphy, Travers, Walport, Ehrenstein, & Janeway, 2008; Segel & Cohen, 2001). These two

make up four layers of security for the body as shall be discussed in the next sections. After this the chapter will discuss artificial immune systems and their use in computer systems. At the end of the chapter a comparison of ICS security and immune system is undertaken in the view of identifying the best possible way of emulating the biological immune system so that the emulation will be able to solve the problem of APT attacking ICS.

3.1 Innate immune system

Innate immunity, which is also known as natural or native immunity is determined by the genes inherited from parents and is always present in healthy individuals (Abbas et al., 2016; Parham, 2009). The innate immune system is responsible for physically blocking and chemically destroying pathogens.

The innate immune system is also responsible for inflammation in the biological immune system. Inflammation is a process which involves recruiting to the infected site, cells and molecules of the innate immune system(Murphy et al., 2008). Inflammation, which can manifest as heat, pain, redness and swelling, is caused by tissue injury and/or microbial invasion that causes the release of inflammatory mediators that increase both blood flow and blood vessel permeability. Inflammation has 3 key roles, namely to:

- Deliver more effector molecules and cells to sites of infection;
- Induce blood clotting which provides a physical barrier to the spread of the infection in the blood stream;
- Repair injured tissues.

The innate immune system is responsible for immediate combatting of pathogens upon infection. It does not keep a record of previous encounters with pathogens and it resets to baseline after each encounter. *Thus, innate immune system is responsible for early detection of pathogens. This functionality would be the most useful to ICS security. That would mean all APT will be detected immediately upon invading an ICS.* How does the innate system recognise pathogens if it does not keep a record of the encounters? The innate immune system recognises common structures that are shared by common pathogens, but which would not be present in normal host cells. For

example, phagocytes recognise bacterial endotoxin and peptidoglycans each of which are not present in mammalian cells but are components of bacterial cell walls. In addition Innate IS responds to double stranded RNA which is found in many viruses but not in mammalian cells (Abbas et al., 2016).

Figure 3.1 is a diagram of the researcher's understanding of the immune system components, what they do and the actual cells and process that achieve the effects. Next is the researcher's overview of how the immune system functions. The immune system is a distributed system that protects the body by local interactions of different layers of the immune system protections.

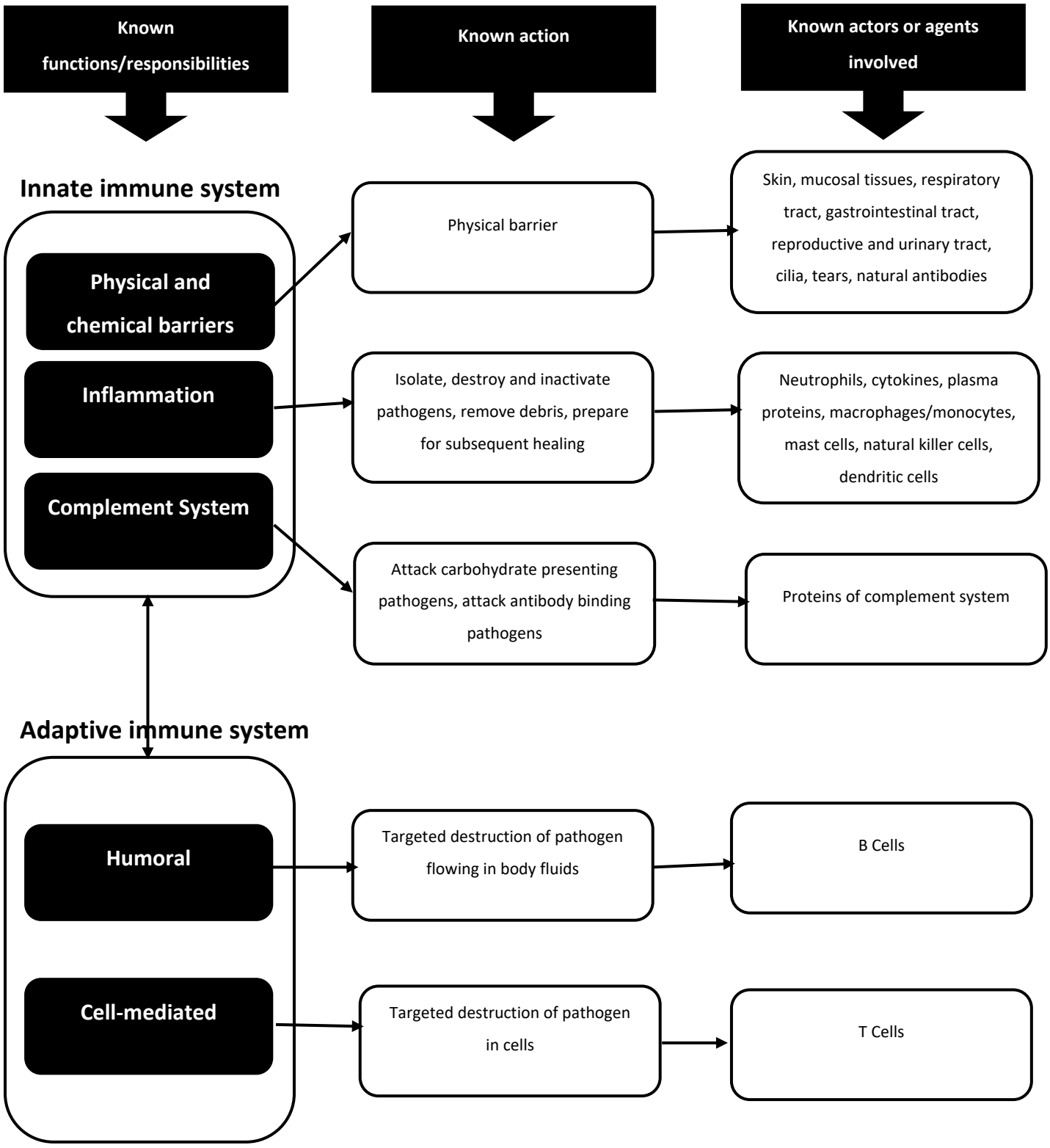


Figure 3.1: Immune System Operations

3.1.1 Layer 1

The first layer of protection consists of physical and chemical barriers which are afforded by:

- The skin which blocks pathogens from entering the body;
- Mucus which traps pathogens;
- lysozymes in tears, saliva, fatty acids on the skin and low PH of the vagina and stomach and chemicals in sweat.

This layer serves to physically block or chemically deter pathogens.

3.1.2 Layer 2

If pathogens have successfully gone past the first layer, phagocytes respond to the infection. All phagocytes ingest pathogens. The first type of phagocyte to respond to an infection after physical and chemical barriers have failed or when physical and chemical barriers have been circumvented are neutrophils. Neutrophils which are resident in blood fluids are not long living phagocytes. When they die they collect into what is called pus. At this stage most cells release histamine which starts a fever which inhibits pathogens.

Another type of phagocyte at the site of infection is a macrophage. Macrophages are resident in body tissues and they generally encounter pathogens first but are soon re-enforced by neutrophils. Macrophages and other phagocytes like neutrophils detect and engulf extracellular bacteria and debris and they also destroy dead cells. This is because macrophages have receptors for certain kinds of bacteria. Molecules (debris) that are released from damaged or necrotic host cells are called damage associated molecular patterns (DAMPS). Macrophages are resident in tissue which means they are sentinel security agents in tissues that are always ready to pounce on invaders. *Which means that all functional areas and all components of ICS security should have such kind of security functionality that is always present to sense any invasions.*

Macrophages and other cells of the biological immune system release cytokines that have a variety of important functions during an immune response. They are the signals that induce inflammation, fever, and modulation of immune responses. Dendritic cells, macrophages, mast cells and other cells secrete cytokines that mediate many of the cellular reactions of the innate immunity. Most are called interleukins by convention, meaning that they are produced by

leukocytes and act on leukocytes. Cytokines recruit neutrophils and monocytes to sites of infection and induce fever.

Microbial molecules that are detected by the innate immune system are called Pathogen-Associated Molecular Patterns (PAMPS). Receptors of the innate immunity that recognise these shared structures are called pattern recognition receptors. A pathogen cannot evade immunity simply by mutating or not expressing the targets of the innate immune recognition. Microbes that do not express functional forms of these structures lose their ability to infect the host; whereas microbes frequently evade adaptive immunity by mutating their antigens that are recognised by lymphocytes because these antigens are usually not required for the life of microbes. *Thus, if we extend this to ICS security we should be looking for something that will always be present in all malware such that if that functionality is not there the malicious software becomes useless*. In *addition, innate immune systems know to recognise that which is not of self. This is a kind of whitelisting in which known functions and or cells are allowed to be but the rest is marked as dangerous.*

Involved also in this second line of defence is the complement system. The complement system is a collection of plasma proteins whose role is to mark pathogens for eradication (Parham, 2009). Complement proteins in plasma bind to bacteria and eliminate them through lysis or opsonisation. Lysis is a process in which complement ruptures the bacterial membrane. Opsonisation refers to the coating of bacteria with complement or antibodies enabling bacteria to be detected by macrophages. Healthy cells exhibit many complement regulatory proteins on their surface which prevent complement proteins from binding to them.

Also in the second line of defence are natural killer cells which target cancerous and virally infected cells. They release perforins that create pores on the cell membranes which allow more water and ions into the cell eventually causing the cell to swell and burst. Virally infected cells produce interferons (a type of cytokine) which stop viral replication by binding to healthy cells. Interferons promote production of proteins that will hinder viral replication in these cells.

Found also in action at the site of infection are dendritic cells that are another type of phagocyte. After engulfing bacteria dendritic cells, act as antigen presenting cells by shredding the pathogen

and presenting portions of the pathogen (now called antigens) on its surface. Antigen presenting cells use this to communicate with the adaptive immune system. Thus, dendritic cells act as the messengers between the innate and the adaptive immune system.

The innate immune system creates time for the adaptive immune system to start by working to contain the infection. When the message gets through to the adaptive immunity/ specific immunity via the dendritic cells or macrophages, then either B lymphocytes or T lymphocytes work towards eliminating the pathogen. B or T lymphocytes recognise specific antigens from pathogens.

3.2 Adaptive immune system

On the other side of the immune system is the adaptive immune system which is responsible for humoral immunity and cell mediated immunity (Abbas et al., 2016; Edgar, n.d.; Segel & Cohen, 2001). The adaptive immune system works differently in that it does not mount the same kind of defence against all pathogens like the innate system. The adaptive immune system gets intelligence about pathogens keeps a record of the information and finds ways to defend the body. To do this are two lymphocytes named T cells and B cells. Antibodies which are found in blood fluid or plasma are the main actors of humoral immunity. Humoral immunity (layer 4) is named as such because historically blood fluids where known as humors (Murphy, Travers, Walport, Ehrenstein, & Janeway, 2008). Cell mediated immunity (layer 3) which is championed by T cells involves targeted destruction of pathogens in cells.

3.2.1 Layer 3

The third layer overlaps with the second layer. When an antigen presenting cell, like a dendritic cell, engulfs a pathogen it presents specific antigens from the pathogen (signal 1) and expresses a costimulatory molecule (signal 2) that are both required to activate the helper T cell (T_h). After binding the dendritic cell, the T_h releases interleukin 2 which is a final signal that activates the T_h cell to clone itself and produce either effector T_h cells or memory T_h cells. Effector T_h cells stimulate other lymphocytes to take action and memory T_h cells keep a record of the pathogen

for future immunity. Effector T_h cells produce cytokines that activate phagocytes to destroy and ingest microbes. They are also required to activate both humoral and cell-mediated immunity.

3.2.2 Layer 4

The fourth layer also overlaps with the second layer. The fourth layer, termed humoral adaptive immune response, or humoral immunity, makes use of B cells in an immune response against pathogens that are floating in the body fluids. B cells have receptors that recognise pathogens. The recognition involves B cells binding to the pathogens. Once the B cell binds to a pathogen it waits to be activated by a T_h cell (this is so that B cells do not react to self-cells). Once activated, a B cell will immediately start cloning itself into effector B cells called plasma cells and memory B cells. Plasma cells will create antibodies that will bind to pathogens. Antibodies are not cells but specialised proteins that bind to pathogens to mark them for phagocytes to ingest them or for complement to bind and lyse them. Antibodies are not able to destroy pathogens on their own. Memory B cells will keep a record of the pathogen for future encounters.

Normal cells that have been infected by pathogens present the pathogens on their surface and this gets detected by cytotoxic T cells which kill the infected cells. Cytotoxic T cells are activated by T_h cells.

The biological immune system knows to recognise particular things as dangerous. For example, when tissue damage occurs; things that are normally found inside of a cells are now outside of a cell and are viewed as dangerous or when particular conserved microbial structures that humans don't have, like cell wall components or flagella, enter the body and are seen as dangerous. Mature B and T cells are also educated to know what is not dangerous, like self-antigens. There exists a large pool of T and B cell receptors whose antigen binding sites were created randomly. And with billions of B and T cells in the human body, this creates an enormous amount of pre-existing variations that could recognise billions of different random molecular structures. Because many of these randomly generated receptors could recognise self-antigens, B and T cells must go through a maturation process that ensures that each randomly generated receptor is functional (positive selection) and does not recognize self-antigens (negative selection). Thus giving rise to a population of B and T cells that could conceivably respond to any

possible non-self-antigen entering the body. Each of these cells must then go through a series of steps in order to be activated. These steps provide important checkpoints to activation of the immune response, in order to ensure it is not activated by non-dangerous or self-antigens.

All the functions of the immune system are enabled because of the properties the immune system exhibits. Because of these properties, the biological immune system is able to detect and eradicate pathogens that invade the body.

3.3 Immune system properties

Six immune system properties were identified. These properties enable the biological immune system to be a robust security system that functions to defend the body from pathogens. These six properties are; the immune system is distributed, it uses intelligence and collaboration, it can communicate message transfer, uses defence-in-depth, enables environment self-awareness and it is resilient.

3.3.1 Distributed control

One property of the immune system is that it is distributed. The distributed control of the immune system means that there is no central control that governs how immune cells work but rather it works by local interactions of the cells and antigens (Aickelin, Dasgupta, & Gu, 2014). Immune System responses as we have seen in the descriptions given above are not governed by a central entity rather by different elements working together to achieve one goal. Take for instance when a pathogen enters the body many different immune system elements like inflammation, activation of neutrophils, macrophages begin to act on the pathogen so that it is contained.

3.3.2 Intelligence and collaboration

The immune system also utilises intelligence and collaboration properties. Immune System elements are intelligent entities which can respond to various situations and past responses and collaboratively work together to eliminate pathogens (Abbas et al., 2016; Parham, 2009; Murphy et al., 2008). Both the innate immune system and adaptive immune system intelligently

recognise or sense presence of pathogens and act on them. They use intelligence to know that these patterns that come before them are those of dangerous elements that should not be allowed. To achieve this, elements of the immune system collaborate by secretions of different signals that act as messages between elements so that they may know how to cooperate in order to eliminate pathogens.

3.3.3 Message transfer

In can be viewed as being capable of communicating messages transferred through physical and chemical entities and can be exemplified by cytokines, opsonisation, antigen presentation, etc. (Abbas et al., 2016; Parham, 2009; Murphy et al., 2008)

3.3.4 Resilient

The immune system is a resilient system which can develop large rescue resources whilst fighting against attacks. This means that IS enables the body to completely recover after attack by pathogens (Abbas et al., 2016; Murphy et al., 2008; Parham, 2009). The immune system is capable of mounting a defence against many attacks and still return to baseline, mount another defence, bounce back to baseline for a very long time. Actually the biological immune system can do this for an average of 75 years which is the average life span of a human ("WHO | Life expectancy," n.d.).

3.3.5 Environmental self-awareness

When a pathogen tries or successfully tries to enter the body through a cut on the skin, on the hand, through the respiratory system, etc. the immune system will act in the best possible way to eradicate all invasions. Because macrophages are resident in tissues looking out for dangerous invaders, whenever these dangerous situations arise and abnormalities are detected the immune system functions to contain the infection. Neutrophils floating and other immune system elements in blood or strategically positioned in other regions such as in lymph nodes are always ready to act on pathogens, that have infected any part of the body. There are no special parts that get the most or the best defence each body part is linked to the best possible defence mechanisms via the biological immune system. Thus, this means that all body components have some kind of localised defence strategies.

3.3.6 Defence-in-depth

The biological immune system uses a layered defence approach. The layers involved in immune system defence have been described above. It has been established that there are four layers of defence. Physical and chemical barriers make up the first layer. Phagocytes such as neutrophils, macrophages and dendritic cells makeup the second layer which is involved in early detection of pathogens. The second layer is that which targets pathogens that have infected cells and the last layer involves eradication of pathogens floating in blood fluid. By having a layered defence approach a pathogen actually has to bypass several defence mechanisms for it to successfully invade the body. Thus, we extended this to mean that the biological immune system applies the defence-in-depth strategy.

The processes and the operations of the biological immune system have inspired the emergence of artificial immune systems (AIS). AIS are "computational systems inspired by the principles of the natural immune system" (Mohamed Elsayed, Ammar, & Rajasekaran, 2012a). Most of the models emulating the immune system model the processes of the adaptive immune system. Immune network theory, Negative selection, clonal selection theory and the danger theory were all derived from the adaptive immune system. The theories used to design AIS are explained next.

3.4 Artificial Immune Systems (AIS)

Clonal selection theory, negative selection, the danger theory, Immune network theory, and dendritic cell theories are some of the most widely applied AIS. A brief description of these theories follows.

3.4.1Clonal selection principle

"The clonal selection principle is used to explain the basic features of an adaptive immune response to an antigenic stimulus. It establishes the idea that only those cells that recognise the antigens are selected to proliferate"(Castro & Zuben, 2002). Key features of the clonal selection principle are that:

- new cells are clones of their parents subjected to a mutation mechanism with high rates (somatic hypermutation)
- newly differentiated lymphocytes carrying self-reactive receptors are eliminated
- mature B cells proliferate and differentiate on contact with antigens

3.4.2 Negative selection mechanism

This is based on the generation of T cell generation. T cells receptors are made through pseudo random genetic rearrangement process. Then they undergo a genetic rearrangement process in the thymus called negative selection. T-cells that react to self-proteins are destroyed and only those that do not bind to self-proteins leave the thymus. Negative selection is the method that the biological immune system uses to protect the body from reacting to self. Only matured T-cells circulate throughput the body to perform immunological functions and protect the body against pathogens (Aickelin, Dasgupta, & Gu, 2013)

3.4.3 Danger theory

The key idea in the danger theory is that the biological immune system does not respond to non-self but to danger. It states that an immune response is due to danger instead of foreignness. In this theory danger is measured by damage to cells indicated by distress signals that are sent out when cells die an unnatural death cell stress or lytic cell death , necrosis (uncontrolled cell death) (Aickelin & Cayzer, 2008).

3.4.4 Immune network theory

Immune network theory hypothesises that the biological immune system maintains an idiotypic network of interconnected B cells for antigen recognition. This is because paratopes (molecular portions of antibody) bind to idiotope (shared characteristic between a group of T cell receptor). The binding stimulates B cells because reaction between paratopes and idiotopes of similar B cells is similar to how they would react to antigen (Jerne, 1974, as cited by Andrews & Timmis, 2005). “These cells both stimulate and suppress each other in certain ways that lead to the stabilisation of the network. Two B cells are connected if the affinities they share exceed a certain threshold and the strength of the connection is directly proportional to the affinity they share” (Dasgupta, 2006).

3.4.5 Dendritic cells

Dendritic cells (DCs) come into contact with various signals and antigens at their immature state in tissues. The signals the DCs come into contact with include pathogen-associated molecular patterns (PAMP), danger signals which result from necrosis, and safe signals derived from programmed cell death (apoptosis). If there are more PAMP signals and danger signals than safe signals interacting with DCs then DCs mature and report an anomalous status in tissue. Conversely, if there are more safe signals than PAMP and danger signals, DCs transform into semi-mature state and report a normal status in tissue. After DCs mature they migrate through blood cells from tissue to lymph nodes for further interaction with T-cells (Aickelin et al., 2013).

3.4.5 Artificial immune systems use in computer systems

The idea of using the biological immune system is not a new idea but has been used over the years to solve computer science and engineering problems in what are known as Artificial Immune Systems (AIS). AIS are "computational systems inspired by the principles and processes of the natural immune system" (Mohamed Elsayed, Ammar, & Rajasekaran, 2012b). AIS principles and mechanisms have been modelled in several ways to solve various computing problems. Most of the computing problems that have been solved by AIS can be summed to include learning, anomaly detection and optimisation (Hart & Timmis, 2008).

In AIS infancy mostly negative selection, clonal selection and immune network theories were being used to solve the problems. The AIS community was mostly inspired by the adaptive immune system to solve computational problems. Over the years there has been an analysis on the usefulness and effectiveness of AIS. With this analysis came some recommendations on how to successfully implement AIS. The following sections will summarise the recommendations from 2005 to present day.

3.5 AIS challenges

There has been some negative hype around AIS for several years after its deployment. Several authors have summarised reviews of AIS over the years in order to evaluate if there have been improvements on AIS development and to find out ways to develop a highly effective AIS by

trying to integrate recommendations for improvement to AIS suggested by the several studies highlighted in this paper. Only AIS reviews were considered in this review in order not to replicate work that has been done so that this work focuses on trying to consolidate what has already been done before.

Hart and Timmis (2005) state in their paper that AIS systems were not very successful. They state that for AIS to improve, they must be developed following the Stepney conceptual framework (Stepney, Smith, Timmis, & Tyrrell, 2004). They also add that for AIS to be distinct then it must borrow some more principles from immune system such as; homeostasis, interactions between innate and adaptive immune system which would consist of multiple, interacting communicating, components.

Garrett (2005) embarked on a journey to evaluate AIS. The author states that for an application to be useful then it must both be distinct and effective. From the tests that were done on AIS Garrett (2005) notes that the biggest challenge for AIS is that it has a few applications for which it is undisputedly the most effective. The other problem with AIS according to Garrett, (2005) was that the innate immune system had been completely ignored. To improve AIS the author suggests that as the field matures then AIS will become useful.

According to Andrews and Timmis (2005), AIS were originally designed by paying attention to the biology from which the inspiration was drawn but focus has shifted only to the engineering aspects. This meant that AIS were designed from 'naïve biological models' which suffer from 'reasoning by metaphor'. They stressed that the theory chosen for inspiration should be appropriate. Andrews and Timmis (2005) argue that for the AIS practitioner to be successful then the theories presented by the immunologist should be sound. They noted that the problem with this requirement is the fact there was no agreement among immunologist about key immune system principles. The other problem that they highlighted was the fact that it is difficult to choose which aspect of the immune system will generate the required right behaviour. They note that since the clonal selection and the immune network theory were not being successful then there was need to look to alternative theories for inspiration like the Cohen model in the hope of developing new AIS models. To solve the problem of not being able to select the right IS for

inspiration, Andrews and Timmis (2005) recommend the use of Stepney's Conceptual Framework which promotes an interdisciplinary approach to developing AIS.

Stepney et al. (2005) in their paper state that AIS models that are developed were naïve in respect to biology as such naivety of the models blocks the understanding of the development and analysis of computations. Consequently, to develop more sophisticated AIS models, they must be developed using a conceptual framework that will also aid in the analysis of computational metaphors and algorithms.

Dasgupta (2006) stated that AIS lack uniqueness and usability. The paper notes that if AIS was to be unique and usable then; AIS algorithms must improve efficiency, enhance representation, introduce other immune mechanisms and development of unified architecture that integrate several AIS.

Liu, Wang, and Gao (2006) highlight that from IS artificial immune networks and artificial immune algorithms have been developed. They state that the problem with AIS by then is that there was no analytic design guidance. To solve this problem they state that IS fundamentals must be studied in further detail to exploit new artificial immune models, use AIS in more application areas like systems sciences, electronics, etc., prove AIS algorithms and models convergence, analyse AIS algorithm and models efficiency to understand the functions and the principles, exploit hybrid AIS merged with neural networks, fuzzy logic and genetic algorithm.

Somayaji, Locasto and Feyereisl (2008) outlined a panel discussion at a workshop on new security paradigms. The discussion was centred on the future of computer security and biology. The discussions conclude that there was a need to learn more biology and there was a need to improve communication to others of the field's fundamentals. The discussion also concluded that the differences between evolution and intelligence needed to be properly understood. They state that if an approach is to be adopted then it must be well evaluated. Hence their solution is to develop better evaluation methodologies for biological mechanisms.

Timmis, Hone, Stibor, and Clark (2008) stated in their paper that up until 2008, AIS algorithms were mainly being developed in an ad hoc manner. This meant that there was a lack of theoretical justification for the use of AIS. They emphasise that theoretical work done thus far is only the

beginning of a more meticulous and thorough foundation to the area because as it is AIS are no longer rooted in biology. Timmis et al. (2008), state that explorations in the use of DCs should address this imbalance. DCs should provide means to recognise anomalous behaviour in a network. The paper concludes that growth of AIS should be based on good methodology that result in full exploitation of the paradigm by:

- Use modelling techniques – computational and mathematical models – focusing on the biological aspects of interest;
- Adoption of a theory first approach starting with detailed theoretical models of the biology, will provide a sound basis for algorithms developed.

Moreover, Zheng, Chen and Zhang (2010) note that AIS do not have unique applications and concentrate on what other paradigms do. They state that there is need to look for a de facto application for AIS or use AIS in cases were benefits of adopting AIS are clear. Zheng et al. (2010) state that in developing AIS in addition to studying the immune system, systems like the neural and endocrine systems must also be considered because the biological immune system does not work independently. In addition, AIS do not have a general purpose framework from which to design AIS (Zheng et al., 2010).

Furthermore, Dasgupta, Yu and Nino (2011) say that their review of artificial immune networks and the clonal selection algorithm, concluded that the many studies of AIS are applications of existing algorithms instead of extensions and improvements of the algorithms. They state that future AIS research and studies should design unique immune systems algorithms that do not intersect with features from other methods. In addition they state that there should be greater interaction and collaboration amongst biologists, computer scientists and engineers if the AIS field is to be advanced.

In addition, Elsayed et al. (2012) also agree that AIS are reasonably effective in a moderately few problems but do not add any distinctive significance over other paradigms. They state that AIS should adopt a problem oriented approach instead of an algorithm oriented approach. We are in agreement here.

While investigating the use of AIS to secure industrial control system Bere and Muyingi (2015) conclude that AIS have not been successful in the implementation because biological immune systems that are being used are not fully understood. To design better AIS, Bere and Muyingi (2015) recommend that the immune system functionality that is being emulated should be fully understood, translate the immune system functionalities into mathematical models and then, translate the mathematical models into computational models. Table 3.1 summarises the challenges that have been identified in AIS over the years.

Table 3.1: AIS Challenges Summary

Author, year of publication	**AIS Challenge**	**Recommendations**
Hart and Timmis, 2005	• AIS not very successful	• Develop AIS following Stepney's Conceptual framework • Borrow some more IS principles
Garett, 2005	• A few application types for which AIS is the most effective method • Innate IS has been ignored	• As the field Matures AIS will improve
Stepney et al, 2005	• Developing naïve AIS in respect to the biology blocks understanding development and analysis of computations	• Develop a conceptual framework that helps analysis of computational metaphors and algorithms
Andrews and Timmis, 2005	• Biological models suffer from reasoning by metaphor • No agreement among immunologists about key IS principles • Difficult to choose which aspect of IS generates the required right behaviour	• Look into alternative IS theories like Cohen Model • Use Stepney's conceptual framework to promote interdisciplinary approach to developing AIS • Use modelling techniques – computational and mathematical models • Adopt theory first approach starting with detailed theoretical biological models

Dasgupta, 2006	• AIS not unique and not usable	• Improve AIS algorithm efficiency • Introduce other IS mechanisms • Enhance representation • Develop a unified architecture that integrate several AIS
Liu, Wang ans Gao, 2006	• AIS lack analytic design guidance	• Study IS further • Use AIS in more application areas • Prove AIS algorithms and models convergence • Analyse AIS algorithms and models efficiency • Exploit hybrid AIS
Somayaji, Locasto, and Feyereisl, 2008	• Need to learn more about biology and need to learn how to learn to communicate the fundamentals of their field to others • Differences between evolution and intelligence should be better understood • Need to clarify goals	• Develop better evaluation methods
Zheng, Chen and Zhang, 2010	• AIS do not have unique application and it concentrates on what other applications do • Lacks a general framework in which to design AIS	• Design killer AIS application • Use AIS in cases were benefits of adopting AIS are clear • Attention should also be paid to other systems which IS interacts with like the neural and endocrine system
Dasgupta, Yu and nino, 2011	• Majority of AIS are applications of already developed algorithms rather than extensions and improvements	• Develop distinctive AIS that do not logically and technologically overlap with other existing paradigms • More communication among biologists, computer scientists and

		engineers to explore and move forward in the AIS field
Mohamed Elsayed, Ammar, Rajasekaran, 2012	• AIS successful in a narrow range of problem but do not add sufficient value over other paradigms	• AIS should adopt a problem oriented approach instead of an algorithm oriented approach
Bere and Muyingi, 2015	• immune systems that are being used for inspiration are not fully understood	• Fully understand immune system functionality that will be emulated • Translate the immune system functionalities into mathematical models • Translate the mathematical models into computational models.

3.6 Emulating immune system to solve APT problem in ICS

By looking at its design and the way it functions it is clear that many useful inspirations can be drawn from the biological immune system. However, over the years the use of biological immune systems has not been particularly successful as we have seen in the previous section. Some major problems of biological immune system application to solving computational problems have been highlighted. These include problems like:

- The biology from which the inspiration is drawn is not fully understood;
- Majority of AIS applications do not solve a unique problem but rather compete with already established paradigms;
- It is difficult to choose which immune system functionality will solve the current problem;
- Ignoring innate immune system and only modelling adaptive immune system.

To solve these problems major recommendations can be summarised to; there is a need to fully understand the immune system. This transitively implies that the biological immune system functionality that will be emulated is also needs to be fully understood. When the functionality

is fully understood, model the functionality in such way that it can be thoroughly proven that the functionality has been totally understood and it is functioning according to design specifications.

The problem with this kind of approach is that one can never be too sure that the immune system has been fully understood. It is still possible to misunderstand the biological immune system or even if it is understood it might be wrongly implemented. This stems from the fact that biologists that are the experts in the field do not even agree on how the immune system functions. It thus proves difficult to fully understand a phenomenon in which there is no agreed convention as to the way it operates. To improve this scenario the researcher proposes to look at the biological immune system properties.

A high level understanding of the biological immune system makes it obvious that its main function is that of detecting and eradicating infection. This should be the perfect inspiration for any security applications that need to be developed. But, as we have seen this is not the case. Thus, we propose to understand those properties that enable it to secure the body and make sure those properties are also introduced in ICS security. We propose that the implementations of these properties be not be modelled from the immune system but adopt those methods that achieve the same properties but are well established already. From the problems of AIS implementation it is pointed out that AIS applications are not really successful because they are competing with already established paradigms. Thus, it would be appropriate to measure which property is appropriate for which problem and then use an already established method to achieve the property so that AIS applications do no compete with other paradigms but rather complement them.

In the case of APT in ICS we proposed that all six biological immune system properties identified in section 3.3 be adopted for ICS security so that ICS security can be enhanced to be resilient and robust like the biological immune system. The next section will compare ICS security with immune system security.

3.7 Comparison of ICS security and biological immune system

This section compares ICS security and biological immune system in order to find any similarities and differences between the two. To compare the biological immune system and ICS security, the notion of layers developed in section 3.2 and 3.3 and the IS properties, discussed in section 2 will used.

3.7.1 Layer one

Layer one introduced the notion that the biological immune system has physical and chemical barriers like skin, lysosomes in tears and saliva, mucus, etc. that inhibit pathogens from attacking the body. These barriers make the environment which the pathogen wants to attack hostile to pathogens. That is to say the environment becomes pathogen unfriendly because the physical and chemical barriers exhibit unfavourable conditions for pathogens. This same kind of security is found in ICS security. In ICS security, we have physical barriers like physical locks and cameras that prevent physical intrusion into ICS. ICS have physical as well as logical access control mechanisms that spell out who or what has access to what part of the physical or logical part of the ICS. ICS also have firewalls which logically block unwanted access into ICS.

3.7.2 Layer two

Layer 2 of the biological immune system functionalities mounts a phagocytic response on pathogens that have bypassed physical and chemical barriers. They identify pathogen and go to work to eliminate them or communicate messages to layer three and four about them. This kind of scenario is also found in ICS security. In ICS security antivirus software and Intrusion Prevention Systems (IPS) detect intrusions that bypass access control mechanism, physical barriers and logical barriers of ICS. Antivirus and IPS detect and contain the attack, whilst intrusion detection systems just detect and sound an alarm about the intrusion which is similar to what would happen with dendritic cells that display antigen to layer 4 and three.

3.7.3 Layer three and four

Layer 3 and 4 introduce the concept of identifying structures of pathogens. After identifying them, keep a record of the pathogen so that the next time it tries to attack, it is quickly destroyed.

This concept is the same as that which is used by antiviruses, IDS and IPS that rely on virus signatures and known intruder patterns to positively identify malicious entry in ICS.

3.7.4 Intelligence and collaboration

The biological immune system also utilises intelligence and collaboration properties. Immune System elements are intelligent entities which can respond to various situations and past responses and collaboratively work together to eliminate pathogens. Both innate immune system and adaptive immune system intelligently recognise or sense presence of pathogens and act on them. They use intelligence to identify patterns of dangerous elements that should not be allowed. To achieve this, elements of immune system collaborate by secretions of different signals that act as messages between elements so that they know how to cooperate in order to eliminate pathogens. This behaviour is similar to IDS and IPS in ICS. For example, a cell that has been attacked by a virus will release interferons which signal other cells to up the defence.

The biological immune system allows pathogens that do not cause harm to the body to co-exist in the body. Biological immune system does not destroy all pathogens but only those that cause harm because some of the pathogens if not present will make the body sick. In the same manner SIS monitor ICS to make sure that they are always in a safe state.

3.7.5 Resilience

Being resilient enables the biological immune system to mount large rescue resources when fighting attacks and enables it to mount defences again and again when needed. Therefore, the biological immune system withstands adverse conditions enabling the body not to succumb to all infections. This is somewhat different in ICS security as sometimes ICS suffer damage that result in reconfiguration in order to return to correct controlled process state. Take for example the case of Stuxnet.

3.7.6 Distributed control

It was already noted that the biological immune system has distributed control, which means that separate networked immune system components coordinate and pass messages to achieve one goal. Failure of one component does not bring the whole system down. Take the example of a pathogen that enters the body, many different immune system elements like inflammation,

activation of neutrophils, macrophages begin to coordinate and pass messages in order to contain the pathogen.

3.7.7 Environment self-awareness

Environment self-awareness can be summed to mean that whenever a part of the body is attacked biological immune system knows to recognise that the situation is no longer normal and begin to act on the attackers. There are always localised security entities on guard to detect attack. This is not the case in ICS. ICS typically employ perimeter only security and actual components of ICS do not have local resident security to protect or prevent attack.

3.7.8 Way forward

APTs use any access method to gain access into ICS where they eventually execute their payload. In the biological immune system pathogens have many entry points and in the majority of cases the pathogens are detected. One vulnerable point of failure is when the biological immune system itself is attacked, for example when the biological immune system is attacked like in the case of the HIV virus which attacks the biological immune system. When the biological immune system is attacked by the HIV virus it will no longer be capable of detecting pathogens. If anything else other than the biological immune system is attacked, the biological immune system can kick in and defend the body from invasion. However, there are a lot of diseases that still kill people because the biological immune system was not able to start up quickly enough and many pathogens hide from the biological immune system instead of attacking it directly. Despite these conditions in the majority of cases, the immune systems work correctly and defend the body from being attacked.

This behaviour is unlike in ICS, where despite which point is used to gain access by APT, the attack is almost always successful. We believe that this is where the biological immune system champions ICS security. This is because the biological immune system knows to recognise particular things as dangerous regardless of where in the body the attack occurs. Take for instance when tissue damage occurs, things that are normally found inside of cells are now outside of cells; or when particular conserved microbial structures that humans don't have, like cell wall components or flagella, enter the body the biological immune system is able to detect

all of these invasions. Mature B and T cells are also educated to know what is not dangerous, like self-antigens. This means from any point of malicious entry the body is secured or has security agents on guard but for any point of entry in the ICS some components are not secured or guarded by security agents.

ICS security systems are not resilient and do not enable ICS components to be environment aware. These two properties are not inherent in ICS security as derived between the comparison of ICS security and biological immune system. The other properties already exist to some extent in ICS security. We proposed that in order to successfully emulate immune system to ICS security then we need to incorporate all IS properties in ICS security. Therefore, for ICS security, in addition to already existing properties, there is need to add the properties to be resilient and to be environmentally self-aware.

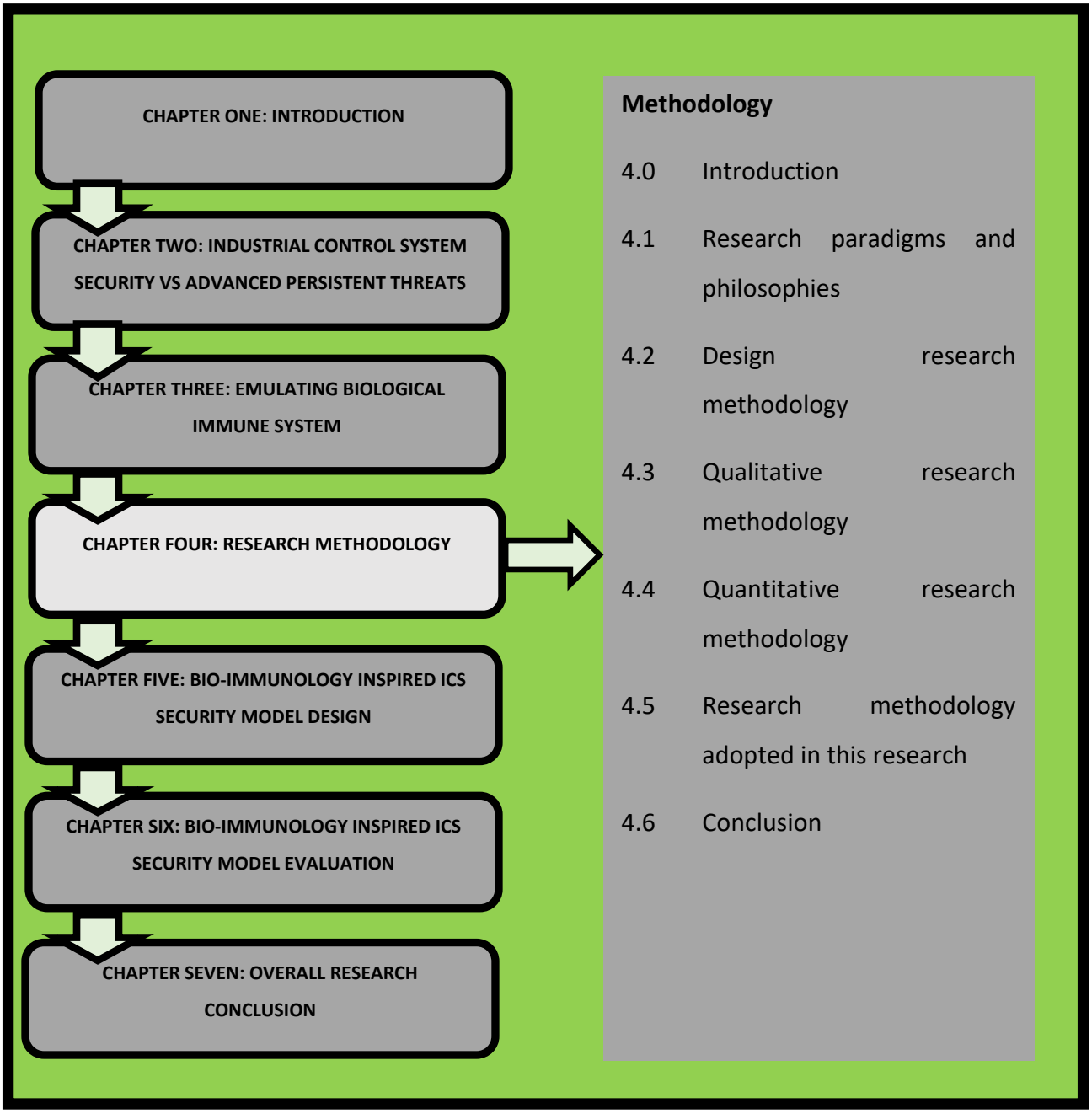
3.8 Summary

The Biological Immune System (BIS) is a system that functions as a defender of the body from pathogens through a combination of physical, chemical and cellular components. The immune system is of two types, namely the innate immune system and the adaptive immune system. Actions undertaken between the innate and adaptive immune system to defend the body can be imagined to be in four layers. These layers of the biological immune system security enable it to display the properties of being distributed, enabling environmental self-awareness, resiliency, intelligence and collaboration, communicating messages and defence-in-depth.

The operations of the immune systems have been modelled and employed in computer systems through an architype termed AIS. AIS have not been applied successfully in computer systems mainly because they are misunderstood. This research proposes to use the properties of the biological immune systems as building blocks for securing ICS mechanisms instead of trying to model the biological immune system operations. This research proposes to identify the properties required and use already established means of achieving the property. Thus, by comparing ICS security and biological immune system it was established that the properties of resilience and environmental self-awareness are not obvious in ICS security. Thus, it would be

useful to incorporate these two missing security properties and if possible reinforce the already existing properties.

CHAPTER 4 : RESEARCH METHODOLOGY



CHAPTER OUTLINE

The research paradigm adopted for this research is the pragmatist paradigm, whereby design science research methodology was chosen as the overarching methodology to conduct this research. Design science research methodology was chosen with an ontological view that it would best answer the research question (*How can ICS be secured to avoid APT attack)* and an epistemological belief that both observable phenomena and subjective meanings can provide acceptable knowledge dependent upon the research question.

4.0 Introduction

This chapter presents the methodology that was used in this research. Design science research methodology was chosen on the basis of it being the methodology that would best answer the research questions. The chapter first describes research philosophies then research methodologies and finally research methodology adopted for this research

4.1 Research paradigms and philosophies

Guba and Lincoln (1994) define research paradigms as the "basic belief systems that guide research, not only in choices of methods but in ontologically and epistemologically fundamental ways" (as cited by Saunders, Lewis, & Thornhill, 2009, p. 106). Different philosophical dimensions distinguish research paradigms (Wahyuni, 2012). Research philosophy relates to how knowledge is developed and the nature of that knowledge (Saunders et al., 2009). Wahyuni (2012), states that the two most important dimensions that distinguish research paradigms are ontology and epistemology.

4.1.1 Ontology

Ontology deals with nature of reality. Two ontological positions are objectivism and subjectivism. "Objectivism is the position that believes that social entities exist in reality external to social actors concerned with their existence" (Saunders et al., 2009 p. 110). That is to say reality exists independent of any social actors. Objectivism is a simple statement that a fact is a fact.

Subjectivism is a position that states that social phenomena exist as a perception of and consequent actions of those social actors concerned with their existence (Saunders et al., 2009). Subjectivism means social phenomena are a subject to how an individual interprets them.

4.1.2 Epistemology

Epistemology is the view on what constitutes acceptable knowledge (Saunders et al., 2009). It also addresses how that acceptable knowledge is acquired. Positivism, realism, interpretivism are three epistemological views (Saunders et al., 2009). Positivism is an epistemological stance that acceptable knowledge is only derived from scientific evidence (Ritchie & Lewis, 2003). That is to say, true knowledge can only be obtained from observable phenomena. Realism is philosophical position that objects exist independent of how they are perceived or theorised by the human mind (Maxwell, 2012). Interpretivism opposes positivism. Interpretivism is the view that humans cannot be studied in the same way as objects are studied. Thus, understanding others, the world and ourselves is mainly influenced by who we are and how we perceive the world (Robert Wood Johnson Foundation, 2008).

As stated above, research paradigms are frameworks which inform on which methods and ontological and epistemological positions the research will follow. Wahyuni (2012) identifies four research paradigms namely; positivism, post positivism, interpretivism and pragmatism. Table 4.1 below highlights the ontological and epistemological viewpoints of the different research paradigms.

Table 4.1: Ontological and Epistemological Views

	Research Paradigms			
	Positivism (naïve realism)	Post-positivism (Critical Realism)	Interpretivism (Contructivism)	Pragmatism
Ontology: the position on the nature of reality	External, objective and independent of social actors	Objective. Exist independently of human thoughts and beliefs or knowledge of their existence, but is interpreted through social conditioning (critical realist)	Socially constructed, subjective, may change, multiple	External, multiple, view chosen to best achieve an answer to the research question
Epistemology: the view on what constitutes acceptable knowledge	Only observable phenomena can provide credible data, facts. Focus on causality and law-like generalisations, reducing phenomena to simplest elements	Only observable phenomena can provide credible data, facts. Focus on explaining within a context or contexts	Subjective meanings and social phenomena. Focus upon the details of situation, the reality behind these details, subjective meanings and motivating actions	Either or both observable phenomena and subjective meanings can provide acceptable knowledge dependent upon the research question. Focus on practical applied research, integrating different perspectives to help interpret the data

Two other research philosophies are axiology and methodology. Axiology is concerned with the role our values and ethics play in the research process (Saunders et al., 2009). Methodology is defined as the "macro-level framework that offers principles of reasoning associated with particular paradigmatic assumptions that legitimate various schools of research" (O'Leary, 2014, p. 10).

4.1.2 Pragmatism

Pragmatism paradigm argues that it is not the research paradigm that is important but the research question. Epistemology, ontology and axiology that the research will follow are determined by how best to answer the research question. Pragmatism believes that it is possible to mix epistemology, ontology methodology and axiology by choosing the best way to solve the imminent research problem. Saunders et al. (2009) state that pragmatists believe that a researcher values play a significant role in interpreting results. The pragmatist researcher will take both the objective and subjective viewpoints. The authors also state that pragmatists use both qualitative and quantitative research methodologies.

The discipline in which the research will be conducted determines the research methodology to be used. In the Information Technology (IT) disciplines Design Research, theoretical research, experimental research, quantitative research, qualitative research, case study, action research, etc. are examples of methodology that can be used.

4.2 Design research methodology

Design research uses the mixed method approach. Design research supports the pragmatist research paradigm with emphasis on the development of new products and outcomes that solve current problems (Hevner & Chatterjee, 2010). Design research evolved from the facts that; information systems are implemented in order to better business efficiency and effectiveness (Hevner et al., 2004). Design science paradigm is a problem-solving paradigm. It is particularly useful in solving "wicked problems" which are characterised by Hevner et al. (2004) as:

- unstable requirements and constraints based on ill-defined environmental contexts,
- complex interactions among subcomponents of the problem,

- inherent flexibility to change design processes as well as design artefacts (i.e., malleable processes and artefacts),
- a critical dependence upon human cognitive abilities (e.g., creativity) to produce effective solutions, and
- a critical dependence upon human social abilities (e.g., teamwork) to produce effective solutions.

4.2.1 Design research methods

4.2.1.1 Case study

Case studies are a thorough contextual analysis in an organisation where the nature and definition of the problem are being experienced currently (Sekaran & Bougie, 2010). A case study involves studying the problem in its real life context. It can be used in both qualitative and quantitative research.

4.2.1.2 Simulations

A simulation is an experiment conducted in an artificial environment that resembles the natural environment in which the problem activities typically occurs (Sekaran & Bougie, 2009). Sekaran and Bougie (2009) argue that simulations are better suited to establishing cause-and-effect relationships. They also state that simulations are popularly used in accounting and finance and that many prototypes of machines and instruments are a result of simulation.

4.2.1.3 Experiments

Experiments are normally used when the researcher wants to investigate cause and effect relationships (Sekaran & Bougie, 2009). In this type of research, conclusions are based on measurements observed. Experimental research can be subdivided into two. The first type of experiment is a formal experiment where observations are made in a controlled environment like a lab. In this type of experiment, a variable is manipulated to find its effect on the dependent variable(s). The second category of experiment research is a field experiment. In this scenario, the researcher observes and/or takes measures in a natural environment.

4.3 Qualitative research methodology

"Qualitative research is a term used as an overarching category, covering a wide range of approaches and methods found within different research disciplines"(Ritchie & Lewis, 2003, p. 2).

According to Creswell (2013), qualitative research design has the following characteristics:

- Qualitative research is conducted in a natural setting where the researchers collect data on the site where participants experience the problem.
- Qualitative researchers collect their own data from observations and interviews.
- Qualitative researchers gather multiple forms of data which is reviewed and organised into categories or themes.
- Themes, patterns or categories are built from bottom up.
- Focus is kept on learning the meaning that the participants hold about the problem issues not that of the researchers.
- Initial plan for the research cannot be tightly prescribed.
- Researchers position themselves in a qualitative study.
- Qualitative researchers report multiple perspectives of the problem, identifying the many factors involved in a situation.

4.3.1 Qualitative research methods

4.3.1.1 Observation

This method phenomenon is perceived in its natural setting. The researcher registers experiences, activities and behaviours and any other interesting phenomena (Sekaran & Bougie, 2009). Layout of the environment is recorded. The researcher can be a non-participant observer who does not become part of the organisational system under observation or the researcher can be a participant observer who becomes a part of the inner circle of group or event being observed (Welman & Kruger, 1999).

4.3.1.2 Interviews

Interviews which can be structured on unstructured are a way of gathering data by conversing with participants about the problem at hand. A structured interview is one in which questions are pre-planned in sequence. Conversely, unstructured interviews questions are not pre-planned. Interviews may be conducted face-to-face, by telephone or by video conferencing. (Sekaran & Bougie, 2009).

4.3.1.3 Focus groups

A focus group is a group of eight to ten members with a moderator leading the discussion on the pertinent topic, concept or product. Members are chosen because of their expertise in the topic under discussion. The moderator should guide the discussion to keep it on track and to get genuine opinions, feelings, etc. from the group (Sekaran & Bougie, 2009).

4.4 Quantitative research methodology

Quantitative research deals with structured research where everything in the research process is predetermined. It is commonly referred to as hypothesis-testing research. In a typical quantitative research, the research begins with theory statements from which hypothesis can be derived. An experiment is then conducted to test the effects of the independent variable on the dependant variable (Jha, 2008). Quantitative research answers cause and effect questions by quantifying a variation. Muijs (2004), states that quantitative research involves collecting numerical data to explain a particular phenomenon. Muijs (2004) highlights the following four types of questions that quantitative research can answer.

- When we want a quantitative answer. For example; how many students chose to study computer science?
- Numerical change. For example; is achievement going up or down?
- Finding out about something's state that when we want to explain phenomena. For example, what factors are related to student's achievement over time.
- Hypothesis testing.

4.5 Research methodology adopted in this research

The problem that was addressed in this research is:

There is no method or way of identifying that an ICS is being attacked by an APT

Thus the research aims to design a bio-immunology inspired security model for effective ICS defence from APT. To achieve this objective, the research generally asks:

How can ICS be secured to avoid APT attack?

To answer this question these two further questions were asked;

1. *Why, where and how do APTs Attack ICS?*
2. *What are the weaknesses of current ICS security strategies in defence from APT?*

The main goal of the research is to design a bio-immunology inspired security model which means that the main emphasis of this goal is to design a security model for protecting ICS from APT. To achieve this objective design science research methodology was chosen. The reasons why design science research was chosen are discussed but before that a discussion on why qualitative and quantitative research methodologies were not suitable as overarching methodologies for this research are made.

4.5.1 Why qualitative research methodology is not suitable for designing a ICS security model

Qualitative research has several characteristics as described by Creswell (2007, p. 45) and stated in section 4.3. Table 4.2 lists the characteristics of qualitative research methodology and the nature of the research to be conducted.

Table 4.2: Evaluation of Qualitative Research Methodology as a Suitable Research Methodology for this Research

Qualitative research property	Designing a bio-immunology inspired security model
Conducted in a natural setting where the researcher collects data on the site where participants experience the problem.	Not possible because to gauge when an APT will attack which APT and even when known it is not guaranteed that ICS owners will grant permission for the study to be carried out on their site.

Researcher collects their own data from observations and interviews	Can only collect data from interviews otherwise observing APT in action in an ICS is difficult to time correctly
Researcher gathers multiple forms of data which is reviewed and organised into categories or themes	Can be done by collecting forensics of discovered APT
Research methods used are observation, interviews, focus groups, life histories and narratives and analysis of documents and text	All possible except observation as highlighted above
Themes, patterns or categories are built from bottom up	
Focus is kept on learning the meaning that the participants hold about the problem issues not that of the researcher	Cannot be fulfilled because focus is participant views but on finding a way to detect APT
Initial plan for the research cannot be tightly prescribed	Cannot be fulfilled because initial plan is clear and that is design a security model that enables ICS to detect APT
Researcher report multiple perspectives of the problem, identifying the many factors involved in a situation	Possible because there is need to identify factors involved when APT attack ICS

As can be concluded by the information given in Table 4.2, qualitative research was not a suitable choice for this research.

4.5.2 Why quantitative research methodology is not suitable for designing a ICS security model

Quantitative research described in section 4.4 is a structured research framework where everything in the research process is predetermined. It typically deals with hypothesis-testing. Quantitative research entails the use of an experiment to test the effects of an independent variable on a dependant variable.

Quantitative research was clearly not suitable as this research required a problem solving approach that enables design of an artefact to solve the problem, hence the choice of design science research.

4.5.3 Mapping design science to research objectives

This investigation falls under Constructive Research Methodology or Design Research, or Research by Proof of Concept. Muyingi (2009) states that in such an investigation, something

novel is researched, designed, implemented, evaluated then theorised about, which may be a new sorting algorithm, or new process. Design research uses the mixed method approach and it supports the pragmatist research paradigm with emphasis on the development of new products and outcomes that solve current problems (Hevner & Chatterjee, 2010). In this research, a new ICS security model was going to be designed to solve the prevailing problem of APT attacking ICS. To understand why, where and how APT attack ICS and to gain an understanding of current ICS security one needed to analyse what is currently on the ground. Analysis of current ICS defence mechanisms would inform on the theories, frameworks, instruments, models, methods and weaknesses of current ICS defence mechanisms. Doing this gave the researcher much needed insights on what kind of functionalities would be needed in a security solution for ICS. But it is clear that the method that is needed to understand the underpinning data would not be the same as the method needed for the design of the actual security model thus a need to employ a mixed method approach.

Design science tools include analytical, empirical and software tools and methods. Evaluation tools include statistical, mathematical simulation and equipment for experiments. Evaluation uses criteria which are based on a theoretical understanding of the problem situation (Muyingi, 2009). The analytical method was used to discover underpinning data about APT and ICS security. And the evaluation of the model using MATLAB was based on the theoretical understanding of how security implementation should behave in the face of APT. It is said that design research evolved from the fact that; information systems are implemented in order to better business efficiency and effectiveness (Hevner et al., 2004). This was the goal of this research, to improve ICS efficiency and effectiveness. That is to say, by achieving our objective, the ICS business would be more efficient as it would not be prone to disturbances from APT.

As was stated earlier, design science research is a 'wicked problem' solving paradigm characterised by:

1. unstable requirements and constraints based on ill-defined environmental contexts,
2. complex interactions among subcomponents of the problem,

3. inherent flexibility to change design processes as well as design artefacts (i.e., malleable processes and artefacts),
4. a critical dependence upon human cognitive abilities (e.g., creativity) to produce effective solutions, and
5. a critical dependence upon human social abilities (e.g., teamwork) to produce effective solutions.

In a view to measure the suitability of design science to solving the problem, the researcher had to compare design research problem characteristics with the problem that was going to be solved.

1. A 'wicked problem' that design science must solve a problem with unstable requirements and constraints based on ill-defined environmental contexts. The requirements of a solution to detect APT in ICS are not clear and they are not always the same. In the case of APT, what was known was that when an APT invades an ICS, it will be detected after some time in the system. APTs do not have the same characteristics between different APT because they are targeted attacks that attack only specific entries. Thus it is difficult to have a generic APT. Which, also makes it difficult to measure what exactly will be required in a solution that will detect APT
2. The other characteristic to be exuded by a problem that design science will solve is that of complex interactions among subcomponents of the problem. This is very much the case in this context because execution of APT in ICS requires complex methods that might constitute having knowledge on how to efficiently combine ICS and computing systems. On the other hand, the solution of trying to emulate biological immune system to ICS security is a very complex operation that requires diversifying phenomena to be compared and merged together.
3. Design science can solve a problem that relies on human intellectual and social abilities to produce effective solutions. In the case of APT attacking ICS relies heavily on human intellectual abilities to design a solution. An ICS is a man-made phenomenon in which the only way to have change or to improve conditions can only be possible by employing human thinking capabilities to solve the problem and effectively implement it.

Thus the problem exhibits four of the five characteristics of design science.

4.5.4 Design science research

Design science research process has 6 steps namely; identify the problem, describe the objectives, design and develop the artefact, demonstrate, evaluate, communicate. Design science research emphasises on the development of new products and outcomes that solve current problems (Hevner & Chatterjee, 2010). Design research evolved from the facts that; information systems are implemented in order to better business efficiency and effectiveness (Hevner, March, & Ram, 2004). Design science paradigm is problem solving paradigm. It is particularly useful in solving "wicked problems" which are characterised by (Hevner et al., 2004) in section 4.2.

In the case of this research, the bio-immunology inspired security model was designed to better the efficiency and effectiveness of ICS security systems. The efficiency and effectiveness of the model means that ICS are better equipped to defend themselves from APT and any other attacks that would attempt to change PLC logic. In addition, the design of the model was best done following design research methodology because the solution to APT attacking ICS was largely dependent on human cognitive abilities and human social abilities to produce effective solutions; which is a characteristic of problems that design science should be able to solve.

When design science research is used to solve a research problem it is important to consider use of design science conceptual framework proposed by Hevner et al. (2004). It is also important that the problem conforms to the design science research guidelines on use of design research. The seven guidelines are shown in Table 4.4.

Table 4.3: Design science guidelines

Design Science Research Guidelines		
Guideline	**Description**	**Suitability to designing a bio-immunology inspired security model**
Design as an Artefact	Design science research must produce a viable artefact in the form of a construct, a model, a method, or an instantiation.	A model will be the outcome.
Problem relevance	The objective of design science research is to develop technology-based solutions to important and relevant business problems.	The model is a technological model that is used in ICS to solve the issue of invasion from unauthorised entries.
Design evaluation	The utility, quality, and efficacy of a design artefact must be rigorously demonstrated via well-executed evaluation methods.	Efficiency and quality were demonstrated in a simulated environment of MATLAB.
Research contributions	Effective design science research must provide clear and verifiable contributions in the areas of the design artefact, design foundations, and/or design methodologies.	Research contributes to domain of design artefact and design foundations because it is based on novel integration of concepts from the biological immune system, industrial control system security and advanced persistent threats.
Research rigor	Design science research relies upon the application of rigorous methods in both the construction and evaluation of the design artefact.	Rigorous methods applied in identifying components and their relationships as well as an extensive evaluation procedure was anticipated in the design of model. Rigorous evaluation will be described in chapter 6.
Design as a search process	The search for an effective artefact requires utilising available means to reach desired ends while satisfying laws in the problem environment.	Design of a bio-immunology inspired security model was a search process in ICS security domain.
Communication of research	Design science research must be presented effectively to both technology-oriented and management-oriented audiences.	Research papers on the entire research were published in an academic journal and peer-reviewed conferences.

Peffers, Tuunanen, Rothenberger and Chatterjee (2007)) point out that literature on design research has a wealth of ideas on how to conduct research. They point out that some researchers on design science provide concepts from which the research process can be derived but there is lack of literature on the actual design research processes. Peffers et al. (2007) propose a design science research process as depicted in Figure 4.1.

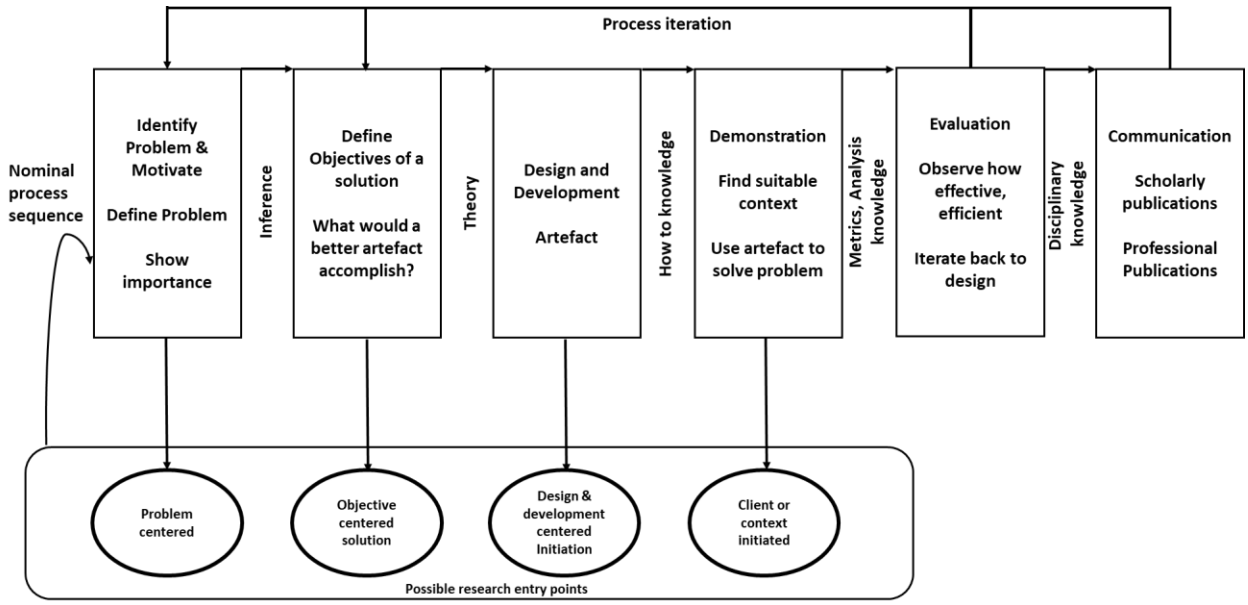


Figure 4.1: Design Science Research Process

The process by (Peffers et al., 2007) was the one adopted in this research.

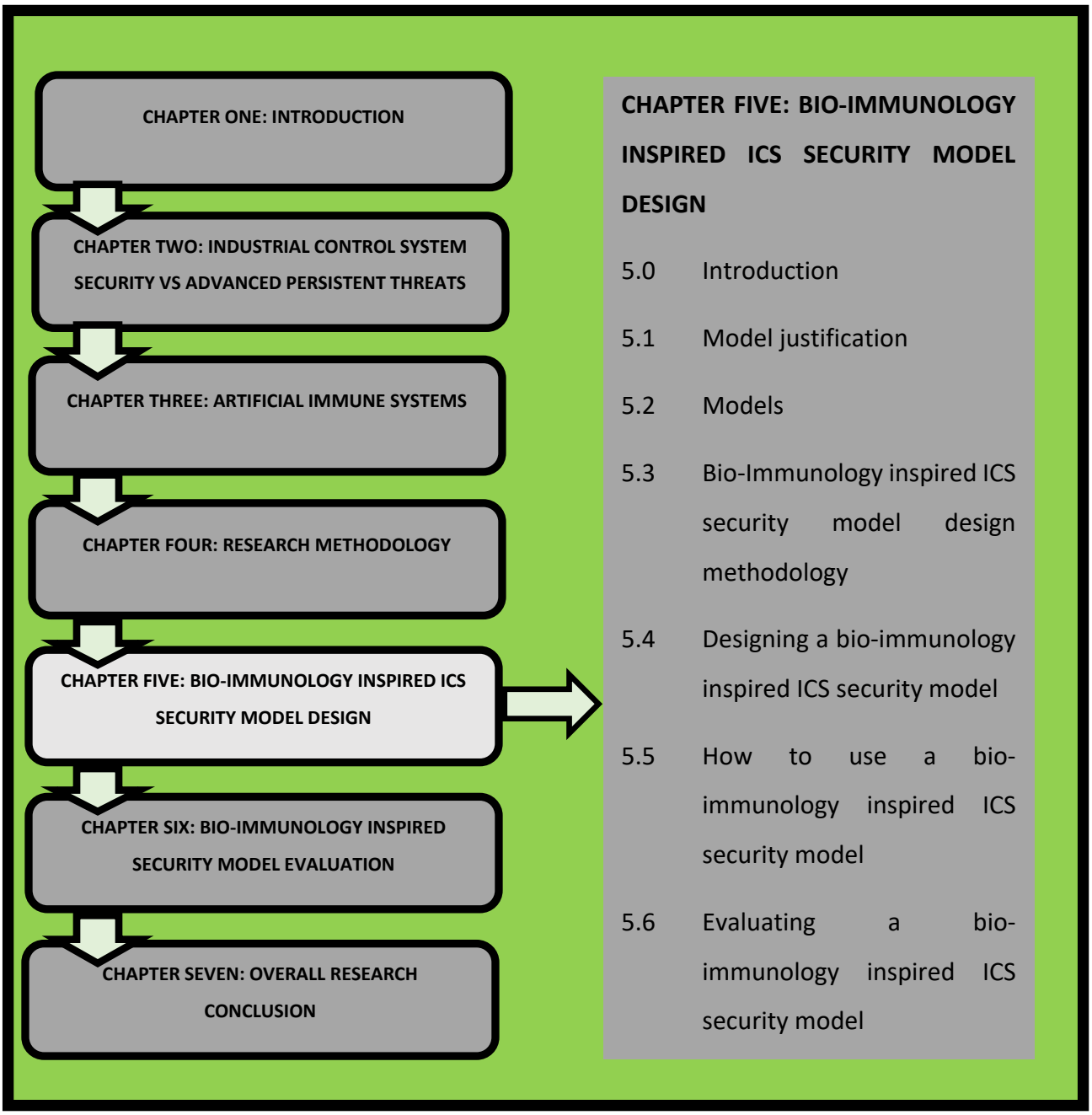
4.6 Summary

The research paradigm adopted for this research is the pragmatist paradigm whereby the design science research methodology was the overarching methodology to conduct this research. Thus, design science research methodology was chosen with an ontological view that it would best answer the research question (*How can ICS be secured to avoid APT attack)* and an epistemological belief that either both observable phenomena and subjective meanings can provide acceptable knowledge dependent upon the research question. Since design science research methodology is a mixed method approach, Table 4.4 shows a mapping of the research objectives and the mixed methods used to achieve them.

Table 4.4: Mapping of Research Objectives and Methods

	Research Objective	**Method**	**Outcome**
1	Analyse where, how and why APT attack ICS	Literature analysis	APT attack model
2	Evaluate current ICS defence mechanisms	Literature analysis	ICS security strategies
3	Design bio-immunology inspired ICS security model	Design science	bio-immunology inspired ICS security model
4	Validate bio-immunology inspired ICS security model	Design science	Validated bio-immunology inspired ICS security model functionalities

CHAPTER 5 BIO-IMMUNOLOGY INSPIRED ICS SECURITY MODEL DESIGN



CHAPTER OUTLINE

Chapter four outlined how the research was conducted. It outlined how the concepts from chapter three and five were used to design a bio-immunology inspired security model. The model design process and the model components are discussed in this chapter. The chapter is organised in two parts. The first part of the chapter discusses the model design process that was used to design the model. Subsequent sections of the chapter zoom in on the model components and their relationships. At the end of the chapter is the summary.

5.0 Introduction

ICS are critical systems that need to be protected from APT, thus it is important to design a bio-immunology inspired model to secure ICS from APT. Models are outlines of how things ought to be and how things are which implies that a model can be used to describe systems, in this case a security system. Design science research methodology was used to design a bio-immunology inspired security model by following design science research process (Peffers et al., 2007). The components of a bio-immunology inspired security model discovered are a firewall, process controller, prediction controller, fall-back controller, process model, intrusion detection system and root of trust.

5.1 Model justification

ICS are critical systems that need to be protected from APT. Findings in chapter two section 2.3.3 show that despite all security controls that are implemented in ICS, APTs still manage to bypass them and enter into the system. APTS manage to bypass access, auditing, monitoring and accountability security controls. At present ICS are secured by following ICS security standards like the NIST Guide to Industrial Control Systems Security and by following best practice procedures from ICS security experts. ICS security controls include raising user security awareness and having policies and procedures that enforce security training. Access control mechanisms implemented in ICS mandate that users must be identified and they should be given

access to only what they need. Further, access to the control system from the corporate network should be through a firewall. Emails should not be allowed in the control system. Physical access to control systems and to devices that display control systems should be restricted. To audit and monitor systems ICS security, ICS conduct regular risk vulnerability and risk management, use intrusion prevention systems, monitor firewalls and security monitors to verify ICS systems are working as they should. To enhance security ICS networks are segmented, the most rudimentary segmentation is that the corporate network has its own segment, the supervisory control has its own segment and the control has its own segment.

Current research on ICS security recommend the use of the defence-in-depth method and using anomaly detection mechanisms as shown in section 2.4.2. Additionally, current researches on ICS security are proposing methods as discussed in section 2.4.6 that focus on keeping the process stable. Checks are done to verify whether new commands are correct or appropriate in accordance with how the process should behave. These methods strive to keep the running process stable by verifying current input and resultant states.

The biological immune system enables the body to block, deflect, detect, mitigate and recover from attacks because it is decentralised and there is no perimeter security. Which means that if a pathogen tries or successfully tries to enter the body through a cut on the skin on the hand and if a pathogen tries or successfully enters the body through the respiratory system, the immune system will act in best possible way to eradicate all invasions. There are no special parts that get the most or the best defence as each body part is linked to the best possible defence mechanisms via the immune system. Thus, this means all body components have some kind of localised defence strategies.

The biological immune system uses a layered defence approach, whereby a pathogen actually has to bypass several defence mechanisms for it to successfully invade the body. Thus, we extended this to mean that the biological immune system applies the defence-in-depth strategy.

There is need to extend current ICS security research that is proposing methods that keep the process stable by adding filtering parameters that apply security policies to incoming commands. In addition to this, employing defence-in-depth, marrying all these concepts into one security

tool that promised to give exciting results that would fare much better than any other system in terms of detecting advanced persistent threats. It was also vital to make sure that the tool designed conforms to biological immune system specifications because this research acknowledges that the biological immune system does an excellent job at detecting and eradicating pathogens consequently, it would be useful also to extend the feature by emulating these capabilities to ICS security mechanisms. Thus, to explain the marriage of ideas, a model was designed to explain the relationships and the components that make up the proposed ICS security tool in the form of a model.

5.2 Models

According to Tomhave (2005, p. 8), "a model is an abstract, conceptual construct that represents processes, variables, and relationships without providing specific guidance on or practices for implementation." Models are outlines of how things ought to be and how things are (Hevner & Chatterjee, 2010). Modelling is a diagramming technique used to describe systems (Models and modelling, n.d.). One of the major steps is determining what the system should do. A model is key in the development of an artefact. Two distinctions about models are common (Models and modelling, 2018). These distinctions are that;

- static models, describe a set of elements and any relationships that exist between them;
- dynamic models, describe the behaviour of one or more elements over time

Furthermore, Models and modelling (n.d.) highlight that a model is machine that exemplifies the simulation of the real thing.

Thus, in this research a model means a conceptual construct that simulates how an ICS security system should function in order to defend itself from APT.

Lethbridge and Laganière (2005) mention three modelling approaches; use case modelling, structural modelling, dynamic and behavioural modelling. Where, dynamic and behavioural modelling means to represent system states, activities and how its components interact. Lethbridge and Laganière (2005) highlight that:

- An interaction model shows a set of actors and objects interacting by exchanging messages and
- A behaviour model shows how an object or system changes state in reaction to a series of events.

The bio-immunology inspired security model designed in this research is a descriptive behaviour model that is a simulation of how ICS security entities change state when it is under attack from APT. From the definition given above and corroborated by Johnson and Henderson (2002), the model components are participating variables, relationship between variables, and a non-specific implementation guideline. Non-specific by definition meaning not specific to any technology but non – specific in this research meaning it should be applicable to any ICS security system.

5.3 Model development methodology

This section describes how the model was designed using design science research and also on the basis of a model definition given in section 5.2. The section explores how the bio-immunology inspired security model was designed following design science research processes.

5.3.1 Design science research process

The design science research process has 6 steps namely; identify the problem, describe the objectives, design and develop the artefact, demonstrate, evaluate, communicate. A brief explanation of each of the six steps will follow.

5.3.1.1 Identify the problem

Ellis and Levy (2010) state the importance of starting with a well-defined problem that cannot be understated. However, they note that not all problems are research worthy and not all problems can be solved by design research methods. They point out that all problems that should be solved by design research have characteristics as pointed out by Hevner (2004):

1. Environmental factors such as requirements and constraints are poorly defined
2. An inherent complexity in the problem and possible solutions
3. A flexibility and potential for change of possible solutions
4. A solution at least partially dependent on human creativity

5. A solution at least partially dependent on collaborative effort

5.3.1.2 Describe the objectives

The next step is to define the objectives of the research. The objectives must be deducted from the problem and also from understanding what can and what cannot be. The objectives can be quantitative, meaning that there is a degree to which there must be a change or they can be qualitative with regards to 'how' the artefact is supposed to behave (Peffers et al., 2007). The research questions must according to Ellis and Levy (2010):

1. be clearly related to that problem, and
2. not already have known and/or documented answers.

5.3.1.3 Design and develop the artefact

It is important to base the designing phase of the artefacts (models, constructs, methods, or instantiations) in literature (Ellis & Levy, 2010; Peffers et al., 2007). At this stage, we determine what the artefact should do and what artefact should look like and actually bringing the artefact to life.

5.3.1.4 Demonstrate

The forth step is to demonstrate the usefulness of the artefact. It must be proven that when the artefact is applied it will solve one or more cases of the problem. This can be achieved by experimenting, simulating, case studying, proving, or any other appropriate activity.

5.3.1.5 Evaluate

The fifth step is to evaluate the artefact. At this stage, care must be taken to compare objectives to what is actually achieved using relevant metrics and analysis techniques by using accepted literature processes (Ellis & Levy, 2010; Peffers et al., 2007). Evaluation could be such as (Peffers et al., 2007):

- a comparison of the artefact's functionality with the solution objectives
- quantitative performance measures

- quantifiable measures of system performance, such as response time or availability.

Depending on the results and venue the researchers can iterate back to step three (5.3.1.3) to improve the effectiveness or continue to step six (5.3.1.6) to communicate the results.

5.3.1.6 Communicate

The last step in a design science research process is to disseminate the problem, its relevance, the artefact, its usefulness, research rigor to the appropriate audiences and to other researchers in the same domain. In academic papers the structure should follow the structure of the design science research process so that it conforms to design science research disciplinary culture (Peffers et al., 2007).

5.4 Designing a bio-immunology inspired security model

Industrial Control Systems (ICS) control critical automated industrial processes like food, chemical, pharmaceutical and beverages manufacturing. ICS are vulnerable to APT attacks which can compromise the infrastructure of the ICS system or compromise the system components of ICS. This can negatively affect the process being controlled which, in turn might negatively affect business or have negative environmental effect. It is of paramount importance to have an early detection mechanism for detecting APT in ICS before they can cause harm. Thus, the purpose of this study, is to propose a model of early detection of APT. Steps that were undertaken were the ones discussed in section 5.3.

5.4.1 Identifying the problem

This was based on literature reviews of existing literature as highlighted in chapter 1 and 2. Literature pertaining to APTs attacking ICS was considered. In addition, literature pertaining to ICS security mechanisms was also considered to have a clear understanding of ICS security arsenal. Thus, the problem identified was the following:

There was no known technique available to identify APTs that attack ICS, because APTs are discovered after they have been in the system for some time and usually only after they have executed their payload

Consequently, this meant that ICS security configurations were inadequate in defending ICS from APT attacks. As such, the study was undertaken to find a solution to the problem of APT attacking ICS.

5.4.2 The objectives

According to the guidelines at this stage, it is important to derive the objectives from the problem and by knowing what can be done and what cannot be done. Following this the main objective of the research was:

To develop a bio-immunology inspired security model for improving existing ICS defence from APT

5.4.3 Designing and developing the bio-immunology inspired security model

The recommendation at this stage is to determine what the artefact should do and what the artefact should look like and then actually bringing the artefact to life.

5.4.3.1 What the bio-immunology inspired security model should do

What should the model accomplish? After it has been deployed what should it achieve? What are the metrics that are going to be used to measure that it is effective? This is what was done at this stage.

Extensive literature reviews were conducted at this stage. Chapter two and Chapter three identified what the model should accomplish and the metrics for effectiveness. The steps taken are listed below

1. First it was established that for APT to gain access into the ICS they bypass access, auditing, monitoring and accountability controls.
2. Then it was established that APT had three most common payloads, cyberespionage, data wiping and data theft. But the worst payload with most dangerous effect was that of Stuxnet which had been designed for cyber sabotage. Thus, Stuxnet was studied further so as to find solutions that would deter future Stuxnet like attacks.
3. It was discovered that Stuxnet had altered the PLC logic to make the centrifuges spin faster at some time and spin slower at other times in a way that did not follow the approved

specification of the affected centrifuges. To do this, Stuxnet managed to get to the engineering workstations and modified the PLC logic.

4. This meant there was need to further secure control part of an ICS. *Thus, the model needed to detect attacks that are targeting PLC.*
5. After this, the researcher had to find the shortcomings of the current ICS security in deterring APTs. It was established that ICS security measures were not quick enough to detect APTs and that ICS security measures were not verifying configuration change parameters from the engineering workstations which changed the behaviour of the controlled process. *Thus, the model had to be able to verify configuration changes and process input parameters*.
6. How can an ICS verify that it is under attack in a prompt manner? Because it was not feasible to look at the already established ICS verification methods as they were failing, the researcher studied the bio-logical immune system to discover how it was able to quickly discover pathogens and effectively defend the body from invasions.
7. By looking at the biological immune system, the researcher derived that to be secure or to be able to detect intrusion is derived from the fact that every body part should essentially be connected to the immune system. Thus, all body parts can block, deflect, detect, mitigate and recover from attacks because there is no central control for security and because the BIS does not have 'perimeter' only security. *Thus, from this we can derive the fact that each critical part of the industrial control system must have many security controls (defence-in-depth).*
8. For the immune system to achieve all this (step 7), it inhibits properties that enable it to work in such a manner. Those properties of immunity are that it is decentralised, an intelligent and collaborative system, and self-aware. Collaboration, defence-in-depth and decentralization properties are already established security parameters in ICS security. *Thus, the model had to add the notion of self-awareness.*
9. How does a controlled environment become self-aware and 'know' that the controlled process in now behaving wrongly? This can be done by creating a model of the controlled process and connecting it to parts of the controlled process so that any deviations can be known. *Thus, the model had to have prior knowledge of how the controlled process should behave.* Work by (Lerner at al., 2012) was doing just this. It consists of the following:

a. The controller module containing process controller-to-be-protected, a high assurance, stability preserving controller (fall-back controller), and a mechanism to switch between the process controller and the fall-back controller. This embedded system module runs at the typical sampling rate of the physical process
b. A prediction module consisting of a process model and a second instance of the process controller. This subsystem runs n times ahead of the active control system module
c. A CHARE (Configurable hardware assisted application rule enforcement) module that wraps the controller and prediction modules. This subsystem consists of specification guards as well as a specialised model synchronisation and timing tools.

10. The model had to benchmark with ICS security standards and from these it was established that effective security means we had to implement a defence in depth strategy. *Thus the model had to display defence-in-depth properties*

5.4.3.2 Anatomy of the bio-immunology inspired model

At this stage the researcher had to establish how the model should look like. At this stage we had to establish what exactly would accomplish the discovered functionalities that are discussed in section 5.4.3.1 and how would it all work.

In summary, section 5.4.3.1 establishes that:

- The model needed to detect attacks that are targeting PLC *(in a way that was quicker than existing detection mechanisms)*
- Each critical part of the industrial control system must have many security controls. (defence-in-depth) *(from biological immune system)*
- Model had to add the notion of self-awareness by having prior knowledge of how the controlled process should behave *(from biological immune system)*
- Display defence-in-depth properties *(from ICS security standards)*

Putting all this together would yield the following:

1. There are three controllers in the whole system:
    a. one connected to the actual physical process which is housed in the controller module (process controller),
    b. a second one (prediction controller) is used for testing instructions, measurements, and other parameters before they are sent to the actual controller. This one is in the prediction where also a model of the process is used to continuously match behaviour of the actual process state and expected states.
    c. the third controller is the fall back which is trusted to have the correct set of instructions at any given time.
2. A process model runs N minutes/seconds/hours (unit of time) ahead of the actual physical process.
3. Prediction controller compares results of current input with expected results that are recorded in the process model deviations.
4. Input for the controlled process configuration changes for the controllers goes through the filter to make sure they are authentic. The filter is used to check whether input or configuration changes comply with specifications. This means that the firewall is configured in such a way to know plant operations. Thus, it should make sure it has verified that the event is correct, the identities and the times for input and configuration change is correct. If any is not correct then it will not be allowed to pass the firewall.
5. Additionally, an IDS is connected to the prediction controller to detect those input and configuration changes that are not authentic but have somehow bypassed the firewall. When an alarm is detected control should be switched to the fall-back controller which is trusted to have the correct set of logic at any given time. IDS should also protect prediction controller from attacks targeting it.
6. The IDS is also connected to the actual controller to detect events that might still not have been detected in the prediction module. Again, if there is an alarm the control should be shifted to the fall-back controller. As in five IDS should also protect process controller from attacks targeting it.

7. The root of trust validates that future system states will not violate system-level policies. Root of trust should be able to guarantee that application's security and reliability specifications are adhered to.

5.4.3.3 Model explanation

Figure 5.1 explains the model components as they were identified in section 5.4.3.2:

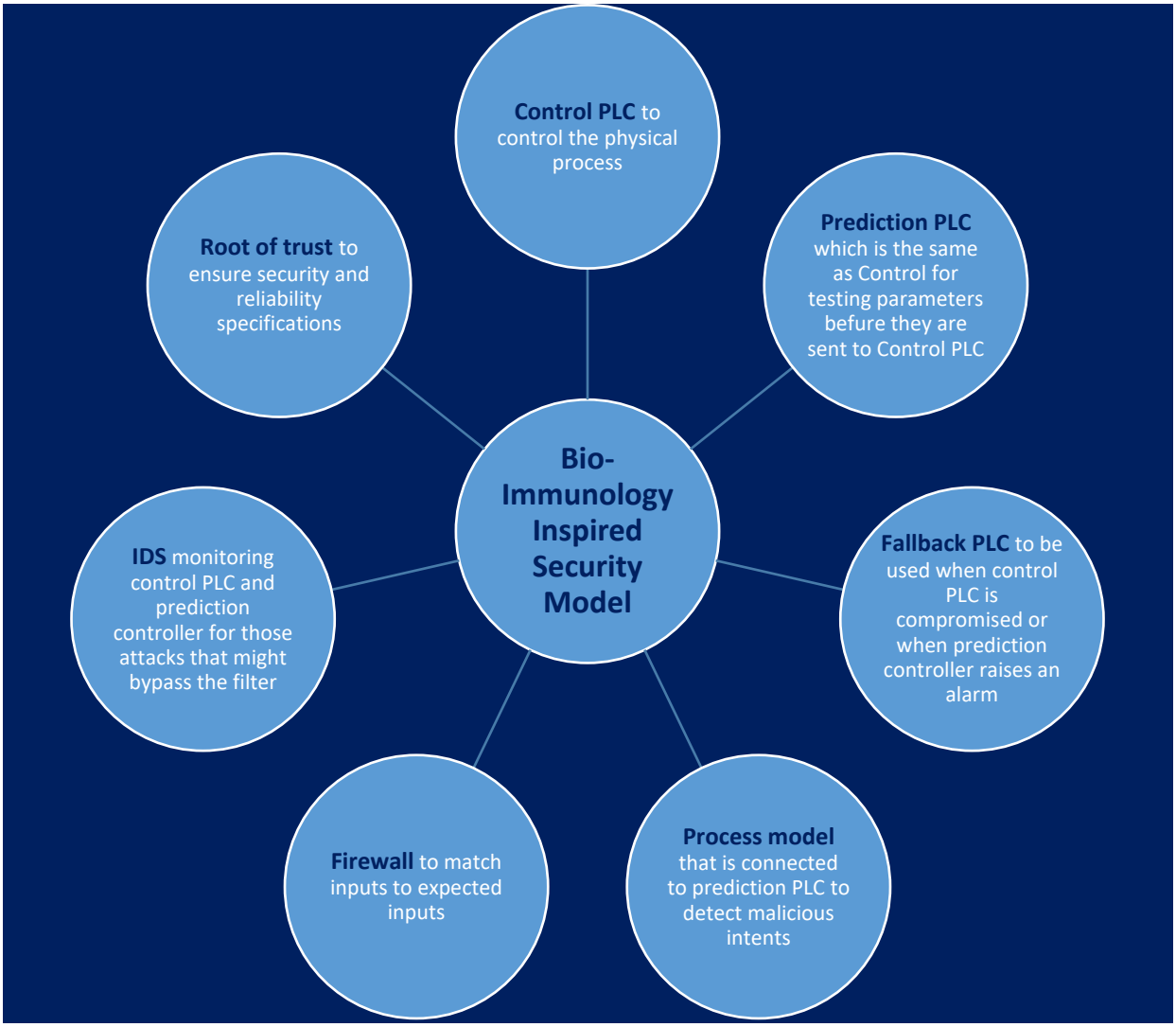


Figure 5.1: Bio-Immunology Inspired Security Model Components

The identified components of the bio-immunology inspired security model are a firewall, control PLC (process controller), prediction controller, fall-back controller, root of trust, process model and intrusion detection system and will be explained next.

Firewall

In an ICS, PLCs are used to automate functions. PLC may be specialised for specific industrial uses with multiple specialized inputs and outputs. PLCs normally do not use commercially available operating system and they usually depend on specific application programs that allow the PLC to function automatically. The automated functions generate as a result of specific inputs (see chapter 2 for more detail).

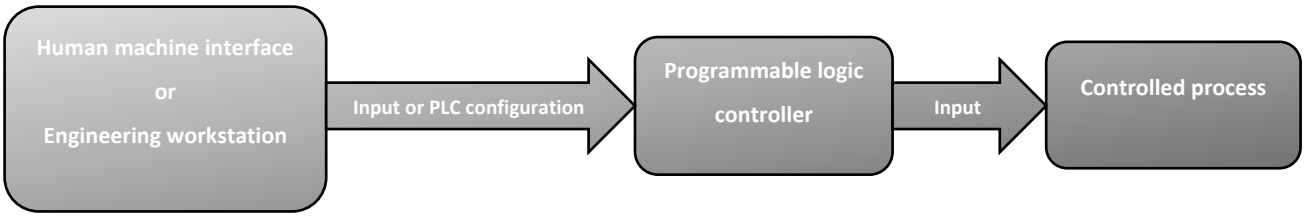


Figure 5.2: Typical PLC connections

Input to the PLC is normally from the different sensors depending on the actual process running. But sometimes input comes from engineering workstations (Figure 5.2). In addition, change to the PLC logic and updates on applications running on a PLC come from the engineering workstations. It is workstations like these that Stuxnet took advantage of and it is anticipated that APT that would attempt to alter automated process results will also take advantage of these kinds of work stations. Thus, to ensure that input and any other change is correct at any specific time there needs to be a firewall to filter input and any changes to make sure that they are legitimate. The setup would be like Figure 5.3.

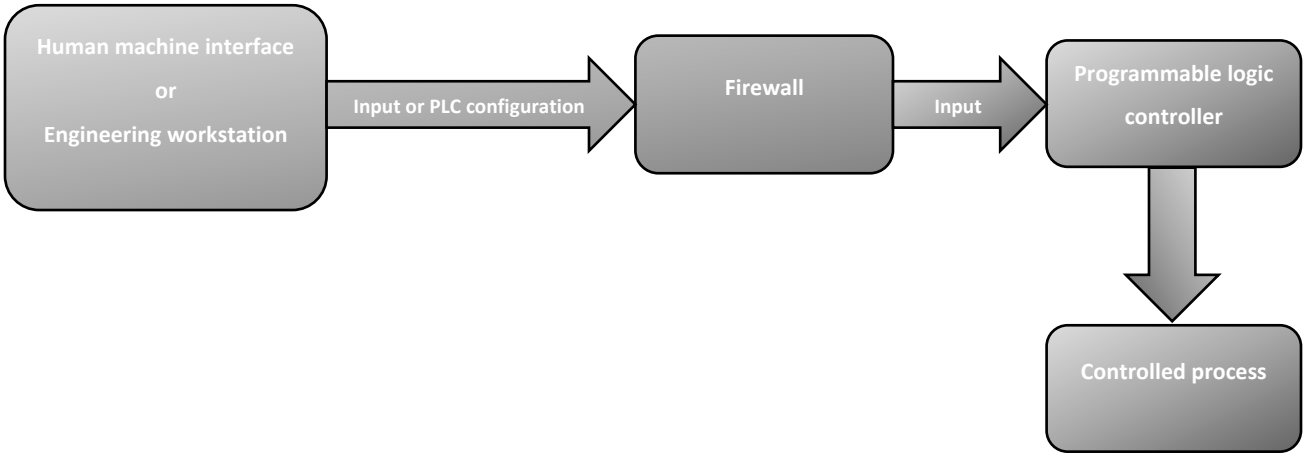


Figure 5.3: Typical PLC connections with a firewall

Process controller

The process controller will be responsible for the automated functions. It will take input for the controlled process. Input will have to be approved by the firewall before it can reach the process controller.

Process model

A process model is a prediction of the controlled process. It runs ahead of the actual process and is connected to the prediction PLC.

Prediction controller

The prediction controller will be connected to a model of the controlled process. By being connected to the model of the process being controlled, it will be possible to predict or to discover that wrong input has been accepted. This is because the output generated as a result of the current input will be compared to what is expected to happen basing on the events that have been pre run in the process model.

Root of trust

The root of trust ensures that security and reliability specification are adhered to. By being connected to the prediction controller, the root of trust validates that future system states will not violate system-level policies. If any violations are detected, control is redirected to the fall-back controller.

Fall-back controller

The fall-back controller is trusted to always have the correct set of logic. It will be used when process controller is compromised, when prediction controller raises an alarm or is compromised and when called for by the root of trust.

Intrusion detection system

This is a monitoring device to further protect the controlled process. The IDS will make sure that the PLC are working as they should and further it will protect them against attacks that might be

targeting the PLCs. This means that some attacks might not necessarily alter the controlled process behaviour but will target the PLC so that it can begin to malfunction and thereby indirectly affect the process.

5.4.4 Bio-immunology inspired security model

The bio-immunology inspired security model was designed to detect APTs before they can affect the controlled process in an ICS. The components and how the model was designed have been highlighted in the previous sections of this chapter. The components have been described and their relationships have also been enumerated. The arrangement of the components in the model is shown in Figure 5.4.

Figure 5.4: Bio-Immunology Inspired Security Model

5.5 How to use a bio-immunology inspired ICS security model

The target users of the bio-immunology inspired security model are ICS security personnel. As they design and implement security for controlled processes they must make sure that their security design has all the components in the model. The security personnel must make sure that their ICS security design will have:

- A firewall connected to process controllers to verify input is correct at any given time.
- A process model that predicts future behaviour of the controlled process. It is used to benchmark correct controlled process behaviour with current process states and inputs.
- A process controller to automate processes
- A prediction controller for testing input before it is applied to the actual process
- An IDS to further monitor the process and prediction controllers for malicious input targeting the controlled process. Moreover, the IDS should monitor the process and prediction controllers for attacks that are targeting them
- A fall-back controller to be used when there are any violations detected

By doing this it becomes highly probable that an APT will be detected before its payload affects the controlled process.

5.6 Evaluating a bio-immunology inspired ICS security model

The fifth step of design science research is to evaluate the designed artefact. This stage will be discussed in detail in the next chapter. Care was taken to compare objectives to what was actually achieved using relevant metrics and analysis techniques. The evaluation compared the model functionality with the objectives set in section 5.4.2. Evaluation also measured the timely response of the model.

5.7 Summary

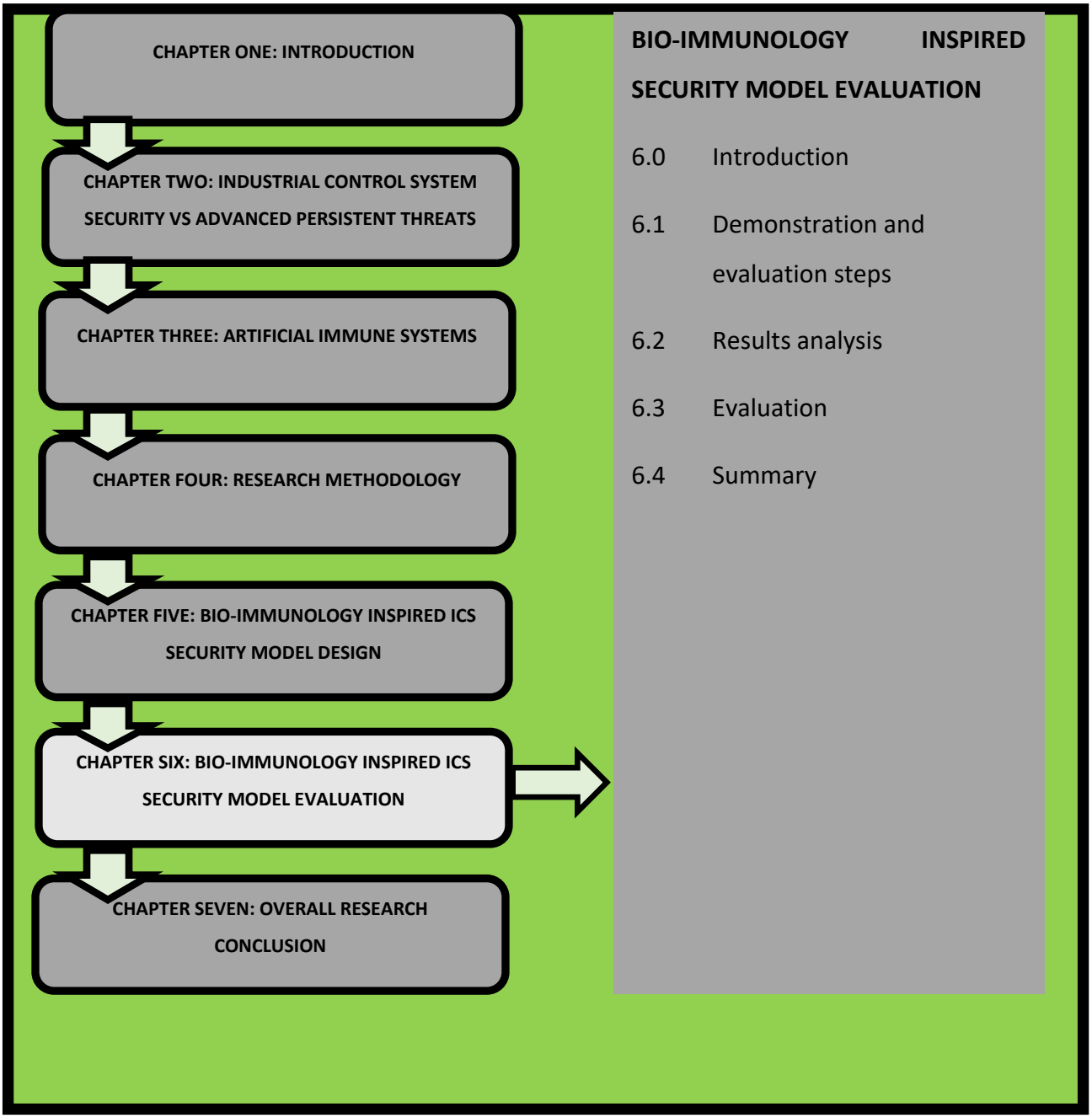
This chapter outlined the bio-immunology inspired security model. First a brief discussion that noted that it was of utmost importance to design an ICS security model to defend ICS from APT was undertaken and it showed why a model needed to be designed. Following a summary of models was given. The designed science research methodology that was used to design the

model was discussed next and then design science research process was discussed. The chapter showcased how the model was designed by following the design science research process. Discovered components of the model and how they must inter relate are discussed. The components of the bio-immunology inspired security model are

- a firewall,
- process controller,
- prediction controller,
- fall-back controller,
- process model,
- intrusion detection system, and
- root of trust.

The chapter highlighted that the model should be used by ICS security personnel to make sure that the ICS they are protecting are able to defend themselves from APT.

CHAPTER 6 : BIO-IMMUNOLOGY INSPIRED SECURITY MODEL EVALUATION



CHAPTER OUTLINE

In order to verify a design research artefact, it needs to be demonstrated and evaluated. A demonstration of the artefact shows that it works according to specifications, an evaluation shows that it works according to certain criteria that are set. At the beginning, this chapter outlines how the bio-immunology inspired security model was demonstrated and evaluated. Towards the end is an analysis of the findings of the evaluation and demonstration steps.

6.0 Introduction

As stated in section 5.4, the design of a bio-immunology inspired security model was done following the design science research process. The fourth and fifth stages of the design science research process are to demonstrate and evaluate the designed artefact respectively. In this case that is to demonstrate and to evaluate the bio-immunology inspired security model.

As is stated in section 5.2.3.4 demonstrating the model means:

"Demonstrating the usefulness of the artefact. It must be proven that when the artefact is applied it will solve one or more cases of the problem. This can be achieved by experimenting, simulating, case studying, proving, or any other appropriate activity."

Demonstration can be carried out either by simulation on an appropriate software environment or on hardware. For this work, the demonstration was done using the Matlab/Simulink environment. **At the evaluation stage of the design science research, it must be shown that the model, when applied in its context, will produce the desired output.** This meant the need to show that the bio-immunology inspired security model when implemented in an ICS environment would:

- Enable detection of APT before it executes its payload and
- Reduce APT effects as quickly as possible.

At the evaluation stage **"Comparison is made between set objectives and what is actually achieved based on the design specifications and using relevant metrics and analysis techniques**

found in relevant literature related to the control plant used as a case study." The metrics to measure are:

- does the model implementation enable detection of APT before it executes its payload and
- does the model implementation reduce APT effects as quickly as possible?

In addition, as specified in section 5.4.3 points 4, 5, 8 and 9 (respectively) the model had to:

- Detect attacks that are targeting Programmable Logic Controller (PLC).
- Be able to verify configuration changes and process input parameters.
- Add the notion of environmental self-awareness.
- Have prior knowledge of how the controlled process should behave

As established in Chapter three, section 3.6 in this research, the researcher did not model how the immune systems work but rather emulated the biological immune system properties to ICS security. It was reasoned that in order to effectively secure an ICS, all biological immune system properties identified in this research must also be exuded by the ICS that needs to be secured. BIS properties of being intelligent, having distributed control, being collaborative, having defence-in-depth, being resilient and being able to do message transfer were identified.

ICS security implementations as they are currently show that distributed control, intelligence, collaboration, message transfer, and defence-in-depth are already well-established security parameters in ICS and what needed to be added to the security of ICS were the notions of environmental self-awareness to add to the defence-in-depth and resiliency properties. Thus, the usefulness of environmental self-awareness was demonstrated and evaluated in this research as the other elements were already established elements in ICS security.

In order for an ICS security system to be environmentally self-aware, it has to have the ability to pre-empt or predict its future state. Pre-empting and predicting future states is a form of artificial intelligence which can be achieved by having a model of how the ICS process should behave in the future that is known and understood by the ICS. This means that the ICS security system can predict the future state and be able to carry out corrective measures when and if necessary. This

type of artificial intelligence and is achieved by using the previously computed model of the process to compare with the predicted future states. As shown in Figure 6.1 the future states at different times will be used to inform the controller on what actions should be taken in order to keep the controlled process in its desired state.

In Figure 6.1:

- $F_{1m}T_{1m}$, $F_{2m}T_{2m}$, $F_{3m}T_{3m}$,..., $F_{nm}T_{nm}$ represent ICS process model states as they have been precomputed in the future.
- $F_{1p}T_{1p}$, $F_{2p}T_{2p}$, $F_{3p}T_{3p}$,..., $F_{np}T_{np}$ represent ICS predicted model states.

Figure 6.1 illustrates how we can use a model of how the process should function and predicted future time states to inform the controller on control decisions to take. When a model future state $F_{1m}T_{1m}$ is compared to predicted future time states $F_{1p}T_{1p}$ in the predictive module, if $F_{1p}T_{1p}$ deviates from $F_{1m}T_{1m}$ the controller should make corrective measures on the controlled process to keep it in steady state and operating as it should. This is repeated at the other time steps $F_{2m}T_{2m}$, $F_{3m}T_{3m}$, until $F_{nm}T_{nm}$ when the process should stop. For the process to be operating normally this means that it should always be behaving as in the $F_{1m}T_{1m}$, $F_{2m}T_{2m}$, $F_{3m}T_{3m}$, until $F_{nm}T_{nm}$ states . Thus if an APT attacks the controlled process $F_{1p}T_{1p}$, $F_{2p}T_{2p}$, $F_{3p}T_{3p}$, until $F_{np}T_{np}$ will deviate from the $F_{1m}T_{1m}$, $F_{2m}T_{2m}$, $F_{3m}T_{3m}$, until $F_{nm}T_{nm}$ model states thus indicating the presence of an APT. The APT will be circumvented because the controller will return the controlled process to $F_{1m}T_{1m}$, $F_{2m}T_{2m}$, $F_{3m}T_{3m}$, until $F_{nm}T_{nm}$ states as these are the desired steady states

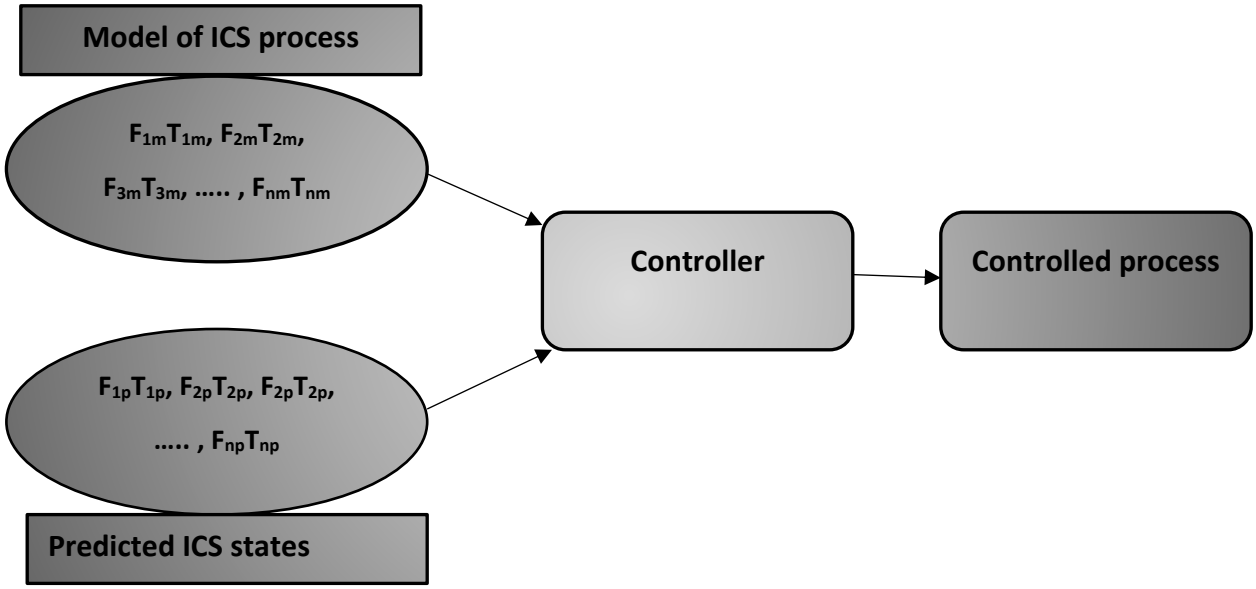


Figure 6.1: How Prediction and ICS model are used to inform the controlled process

The prediction of the future states of an ICS can be achieved using predictive features somewhere in the ICS. This is normally achieved by having the prediction occurring in the process controller, which is able to immediately carry out corrective measures on the controlled process whenever an error occurs. Figure 6.2 which is an extraction of part of Figure 2.1 shows where in the ICS the prediction will be happening. In this research, prediction of the controlled process was obtained from the use of a Model Predictive Controller (MPC). An MPC described in section 6.0.3 is able to predict future outputs based on a process model.

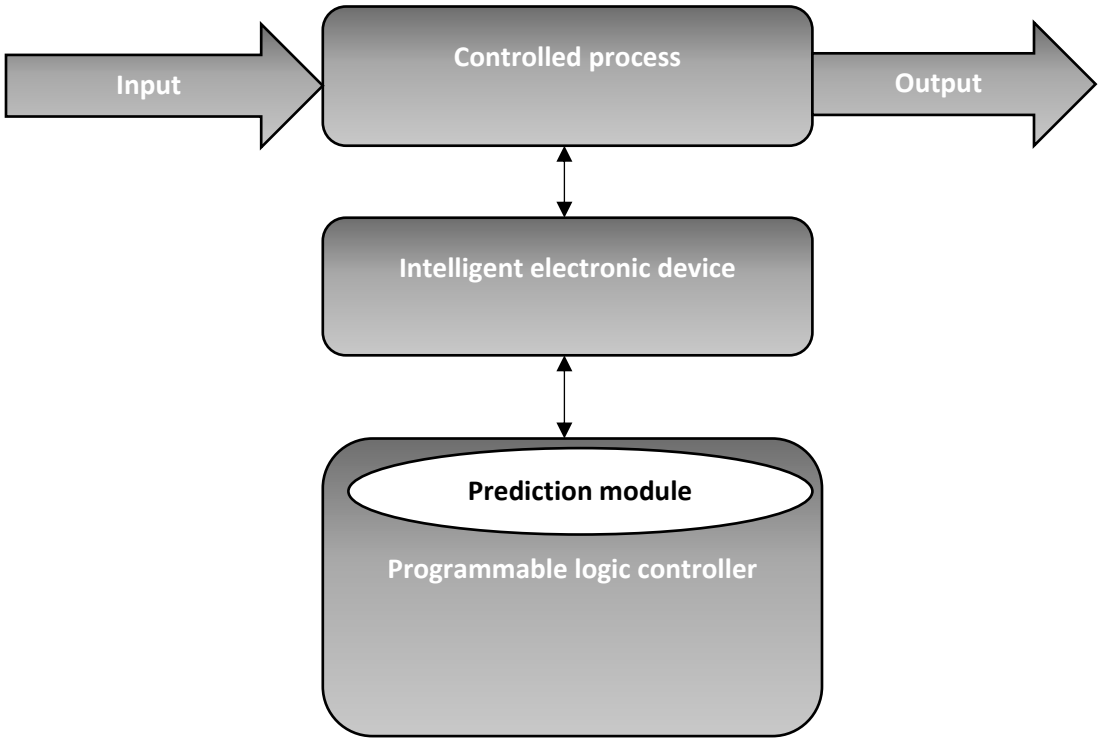


Figure 6.2: Prediction module position in ICS

Earlier in the chapter, it was stated that "The metrics to measure are that an APT is detected before it executes its payload and its effects are reduced as quickly as possible". Environmental self-awareness in BIS means local states of body parts are known and when invasion occurs, localised defence mechanisms kick into play because it is understood by BIS elements at that site that what will be happening at that particular moment is not the correct behaviour. This implies that environmental self-awareness is a property that works to detect pathogens that have already invaded the body.

Similarly, in our ICS environment having environmental awareness should enable ICS security parameters to immediately detect the effects of attacks when they occur. This means the ICS has already been compromised and the ICS security system that implements the bio-immunology inspired security model would be detecting security attacks that are already in the system. Thus, for the case of this evaluation we assumed that the APT has already gained entry into the system by some means or the other. At this point, the APT is already in the system and it is ready to execute its payload. **The demonstration carried out needed to determine if the APT payload will**

be detected. This implies that the demonstration described in this chapter were those of APTs that have already gained access into the system and have the capability to change system dynamics (Stuxnet like APT).

In the evaluation stage what needed to be measured was the capability to reduce APT effects as quickly as possible. In addition evaluation should establish whether the bio-immunology inspired ICS security will be robust enough for the plant processes to run normally even in the presence of attacks or disturbances.

Putting everything into perspective from the beginning, the demonstration and evaluation process followed the following logical steps illustrated in Figure 6.3.

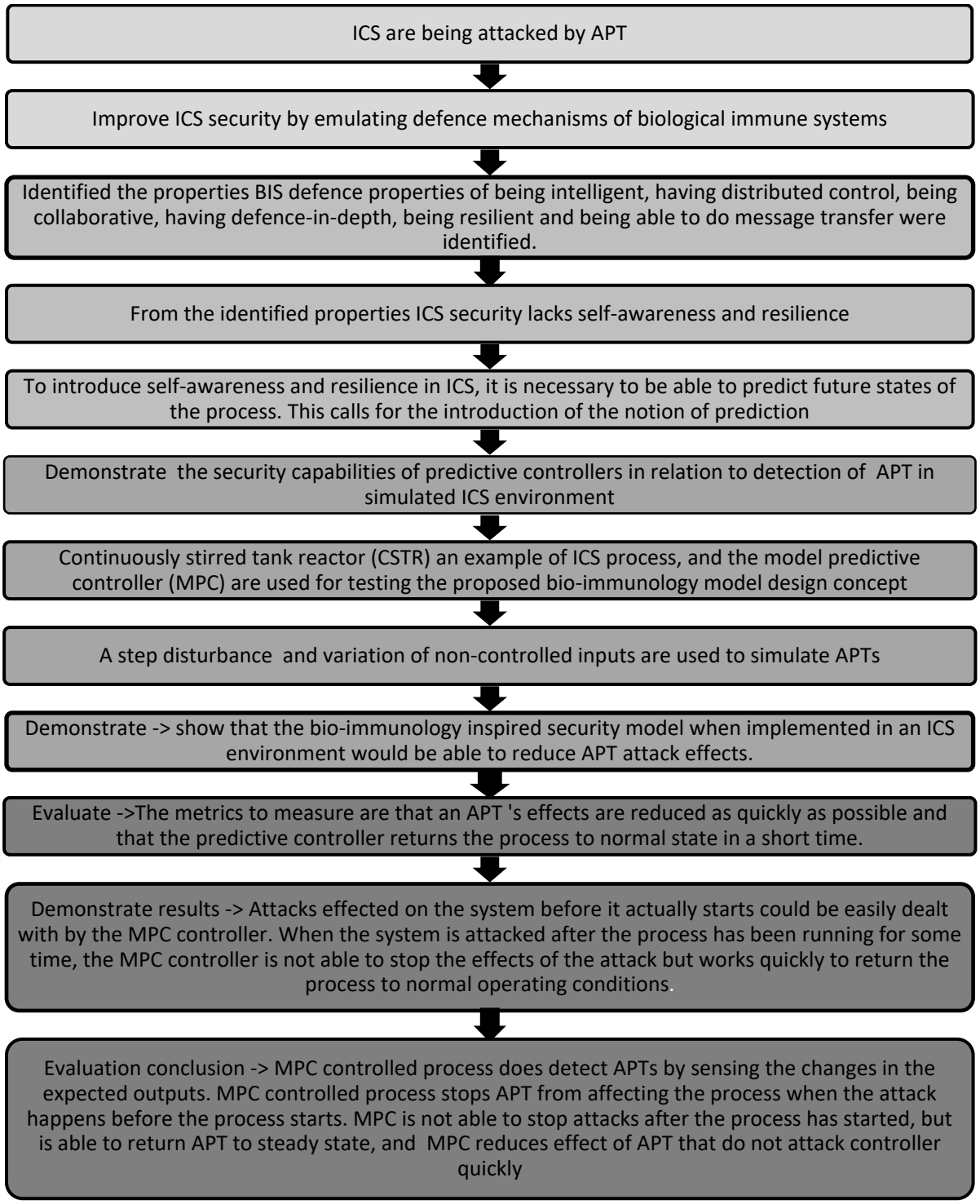


Figure 6.3: Evaluation Process Logic

In summary the usefulness of the bio-immunology inspired security model was demonstrated and evaluated in ICS simulated process called a continuously stirred tank reactor (CSTR) and by the use of step disturbances in the CSTR. Step disturbances represented APT that have already invaded an ICS process. In addition, the Model Predictive Controller (MPC) was used to show the effects of prediction. The suitability of simulations, MPC, CSTR and step disturbances is discussed next.

6.0.1 Simulations

A simulation is an experiment that is conducted in an artificial environment that resembles the natural environment in which the problem activities typically occur (Sekaran & Bougie, 2009). Sekaran and Bougie (2009) say that simulations are better suited to establishing cause-and-effect relationships. They also state that many prototypes of machines and instruments are a result of simulation. A simulation experiment was conducted because:

- The current research aimed at demonstrating the feasibility of the proposed concept and not to test it on an actual process plant,
- The simulation software chosen (MATLAB) is a powerful simulation environment, which had all the features that provide a fairly accurate system dynamics, and
- A simulation environment has the advantage of being risk-free, possibility of several simulation runs save on the cost of conducting trial and error experiments on an actual process plant. Added to this are the lack of risks to the environment and life in case of incorrect parameters being used.

In this case a simulation was seen as the best choice because it enabled the researcher to demonstrate the bio-immunology inspired security model in a fairly accurate implementation on an ICS in a risk-free manner. **In addition, the process simulated in the experiments described here actually simulates the mixing of many substances that are used in real life. For example the CSTR is used for mixture of beverages as well as in the production of chemicals.**

6.0.2 Simulation Experiments

Experiments are normally used when the researcher wants to investigate cause and effect relationships (Sekaran & Bougie, 2009) and conclusions are based on measurements observed. Experimental research can be subdivided into two. The first type of experiment is a formal experiment where observations are made in a controlled environment like a laboratory whereby an experiment variable is manipulated to find its effect on the dependent variable(s). The second type of experiment is a field experiment which involves observing and/or taking measurement in a natural environment.

In this case, the simulation experiment was a formal experiment where observations were made on how an APT attack would affect a process that is controlled by a model predictive controller. The simulation of the CSTR was done in MATLAB (Matrix Laboratory), which is a programming platform for technical computing. With MATLAB one can analyse data, develop algorithms and create models and applications (MathWorks, 2018).

The description of an MPC controller and the controlled process (CSTR) the normal process simulated in the experiments follows.

6.0.3 Model Predictive Controller (MPC)

The mathematical model of the MPC is given as:

Equation 1

$$J = \sum_{i=1}^{N} \omega_{T_i}(T_d - T_i)^2 + \sum_{i=1}^{N} \omega_{u_i} \Delta u_i^2$$

Where:

- T_d is reference variable (for example the desired/required temperature for the process)
- T_i is the controlled variable (for example measure temperature at the i-time step)
- u_i is the control input at the i-time step
- ω_{T_i} weighting coefficient reflecting the relative importance of T_i
- ω_{Td} weighting coefficient reflecting the relative importance of u_i

Following is an explanation of MPC from Matlab uploaded on Youtube (Matlab, 2018). This is an illustration to assist in understanding how the prediction module and model of the process interact in order to control the process so that it stays within the desired process states.

"An MPC is a feedback controller algorithm that uses a previously computed model of the process to make predictions about future outputs about the process. If a person is driving a car their goal as they are driving is to keep the car within their lane. The decisions the driver makes is similar to how an MPC works. The driver knows how fast her car goes, how much it turns based on the control actions they take. Based on this knowledge she does simulations in her head about her car's position in the future. These simulations give her predictions about the future car positions based on the control actions she is taking. From these simulations she selects the control actions that keeps predicted simulation car positions as close as possible to the desired car position.

In a controlled problem the goal of the controller is to calculate the input to the plant such that the plant output follows a desired reference. An MPC's strategy to compute this input is to predict the future. How? MPC uses the model of the plant to do predictions about the future plant behaviour. It also uses an optimizer which ensures that predicted future plant output tracks the desired reference.

P is a measure of how far ahead MPC looks into the future and is referred to as the prediction horizon. **P** is often represented by the length of time into the future or the number of future time steps. At the current time the MPC controller uses the car model to simulate the car's path in the next **P** time steps if the steering wheel is turned a certain angle.

The MPC controller needs to find the best predicted path that is the closest to the reference. So, it simulates multiple future scenarios (by choosing different steering wheel angles to use, in the prediction horizon (P)). However, it does not do these simulations in a random order instead it does it in a systematic way and this is where the optimizer comes into the picture. By solving an online optimisation problem, the MPC controller tries to minimise the error between the reference and predicted path of the car. It also tries to minimise the change in the steering wheel angle from one time step to the next. The cost function **J** of this optimisation problem includes both these terms and is represented as a weighted square sum of the predicted errors and

steering wheel angle increments. While minimising the cost function MPC also makes that the steering wheel angle and car's position stay within prescribed limits.

At the current time step the MPC controller is solving the optimisation problem over the prediction horizon whilst satisfying the constraints. The predicted path with the smallest **J** gives the optimal solution and therefore determines the optimal steering wheel angle sequence that will get the car as close as possible to the reference (the desired trajectory). At the current time step MPC applies only the first step of this optimal sequence to the car and disregards the rest." For example, if the best J is the one as shown in Figure 6.4. MPC will apply the step at K+1 only and recomputes **J** again. Description of MPC in the case of CSTR used in this research is given in section 6.0.4.1.

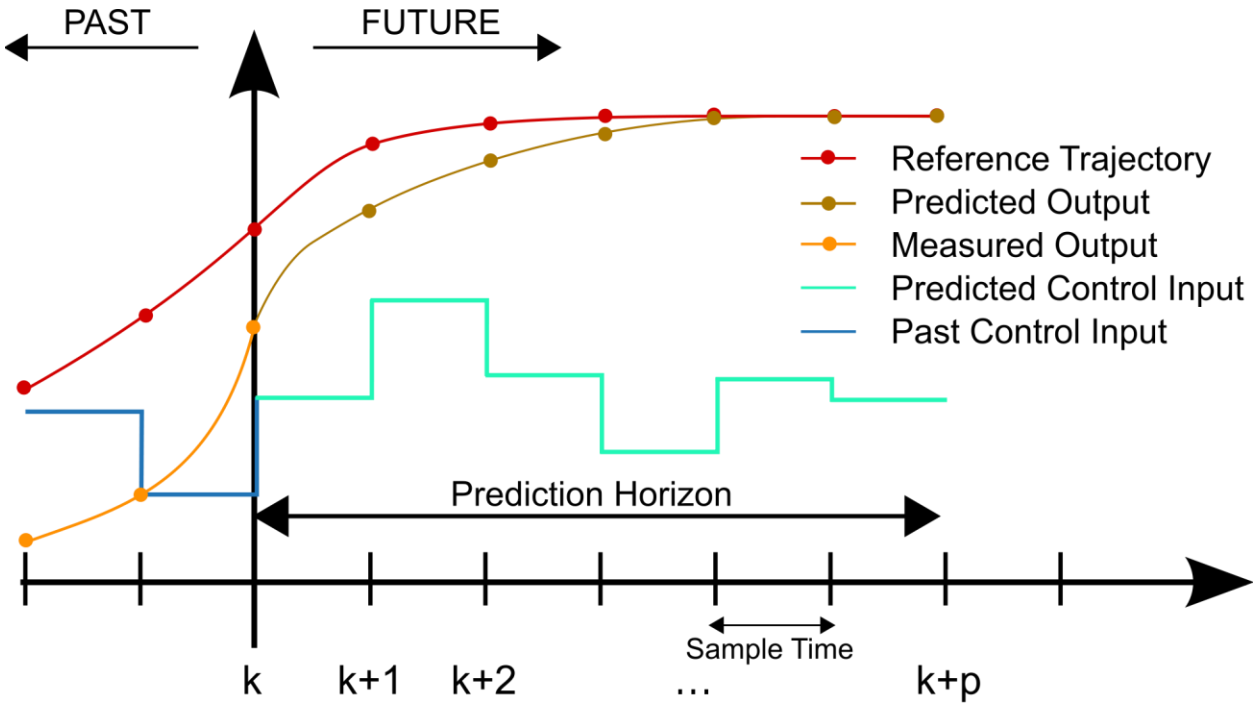


Figure 6.4: MPC scheme

To summarise in the car scenario given:

- J gives the best simulated path that will keep the car within the lane

- T_d is the desired position of the car in the desired path
- T_i is the controlled variable which is the current position of the car at the i_{th} timestep
- u_i is the steering wheel angle input at the i-time step
- ω_{T_i} weighting coefficient reflecting the relative importance of T_i *(current car position)*
- ω_{Td} weighting coefficient reflecting the relative importance of u_i *(steering wheel angle)*

6.0.4. Test Plant: Continuously Stirred Tank Reactor (CSTR)

It was stated in section 1.0 that "ICS automate the generation, transportation and distribution of electricity. ICS automate the industrial manufacturing of food, beverages and chemicals. ICS are also used in mining industries, transportation systems, distribution of water, natural gas and oil, in communication systems and in specialised facilities such as nuclear plants." That means ICS are used in a variety of industries which in many cases represents the mixing of substances or reagents to output certain outputs such as chemicals, beverages and other substances. The Continuously Stirred Tank Reactor (CSTR) is commonly used in the industrial control processes to output chemicals, beverages and others. Its primary use is that of mixing, therefore, it can be said to be a reactor. Thus, it was a good example of an industrially controlled process to use for testing. It was also easy and well documented in the simulation environment for the researcher.

This research used jacketed non-adiabatic tank CSTR model commonly used in the process industry as depicted in Figure 6.5. An adiabatic process is one that occurs without the transfer of heat or matter between a thermodynamic system and its surroundings; that means in an adiabatic process, no heat is gained or lost by the system and its surroundings.

The actual CSTR model used was extracted from the **Simulink library (Matlab, 2019)** this was chosen because the MPC used here had already been tuned and tested for efficiency by professionals designing processes for Simulink. Thus, the controlled process used in the experiments is an example of how MPC works found in Simulink library of Matlab. The description of the process as extracted from Simulink follows:

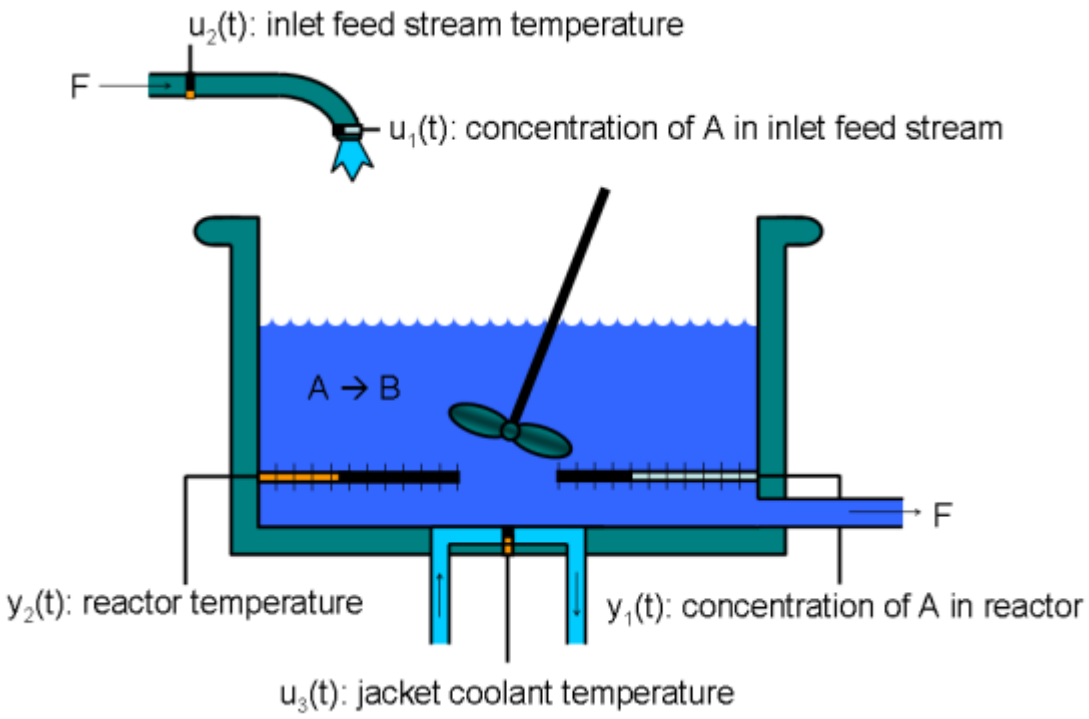


Figure 6.5: Continuously Stirred Tank Reactor (CSTR)

An inlet stream of reagent *A* feeds into the tank at a constant rate. A first-order, irreversible, exothermic reaction takes place to produce the product stream, which exits the reactor at the same rate as the input stream.

The CSTR model has three inputs:

- Feed Concentration (C_{Ai}) — The concentration of reagent *A* in the feed stream (kgmol/m^3)
- Feed Temperature (T_i) — Feed stream temperature (K)
- Coolant Temperature (T_c) — Reactor coolant temperature (K)

The two model outputs are:

- CSTR Temperature (T) — Reactor temperature (K)
- Concentration (C_A) — Concentration of reagent A in the product stream, also referred to as the residual concentration (kgmol/m^3)

The control objective is to maintain the residual concentration, C_A, at its nominal set-point by adjusting the coolant temperature, *Tc*. Changes in the feed concentration, C_{Ai}, and feed temperature, *Ti*, cause disturbances in the CSTR reaction.

For this experiment, the reactor temperature was not controlled; it was assumed that the residual concentration is measured directly.

We assume that the product B is a drink and that the concentration C_A cannot be changed to anything else. This is to maintain the taste and quality of the drink. If the concentration strays beyond this, then the drink will not be suitable for human consumption and will not taste as it should.

In Simulink, one can trim the model to conform to input and output specifications. This is known as trimming. In the experiments described below, C_A was the output constraint used to trim the model so that C_A is always kept at 2kgmol/m^3

The Simulink model of the CSTR is shown in Figure 6.6.

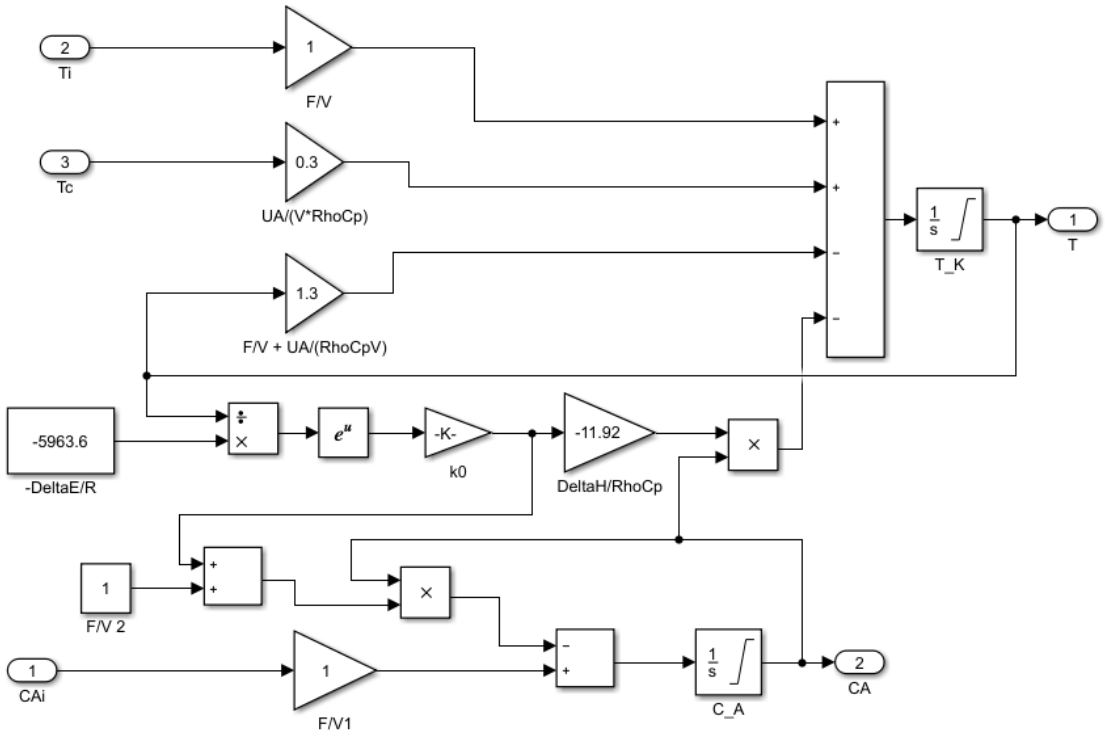


Figure 6.6: CSTR Simulink model

Putting this into MPC equation (equation 1) we have:

- J gives the best simulated feed concentration that will keep the product within the desired concentration
- T_d is the desired Concentration (C_A) that is the concentration of reagent A in the product stream
- T_i is the is the current concentration of reagent A in the product stream at the i_{th} timestep
- u_i is the Coolant Temperature (T_c) input at the i-time step
- ω_{T_i} weighting coefficient reflecting the relative importance of T_i *(concentration of reagent)*
- ω_{Td} weighting coefficient reflecting the relative importance of u_i *(coolant temperature)*

6.0.4.1 Description of MPC in the case of CSTR

In this case the MPC uses a previously computed model of the CSTR process to make predictions about the future concentration. The goal is to keep the concentration at 2kgmol/m^3. The MPC simulates future concentration based on the future coolant temperature. From these computations the MPC selects the control actions that keeps predicted concentration simulation as close as possible to the desired 2kgmol/m^3.

P in this case was 20. Therefore at the current time the MPC controller uses the concentration model to simulate the concentration in the next 20 time steps based on future coolant temperatures. By solving an online optimisation problem, the MPC controller tries to minimise the error between the 2kgmol/m^3 the desired concentration and predicted concentration of the mixture. It also tries to minimise the change in the coolant temperature from one time step to the next. While minimising the cost function MPC also makes sure that the coolant temperature and concentration stay within prescribed limits (constraints).

At the current time step the MPC controller is solving the optimisation problem over the prediction horizon whilst satisfying the constraints. The predicted path with the smallest J gives the optimal solution and therefore determines the optimal coolant temperature sequence that will get the concentration as close as possible to the 2kgmol/m^3 (the desired concentration). At

the current time step MPC applies only the first step of this optimal sequence to the CTRS process and disregards the rest. And recomputed for the next time step.

6.0.5 Step disturbances

A disturbance Input is an unwanted external or environmental factor that affects plant behaviour. Once added to a system it will affect the system's output, thus increasing errors. The step disturbance changes the input size of the process to that of the final step value in a very short time. Stuxnet like APTs want to alter system outputs thus, can be represented by step disturbances in the system. This simulates well APTs that already have access into the system whose goal is to affect or modify plant behaviour.

A step disturbance at time zero seconds, four seconds and eight seconds were considered. The final step values for all step times considered are 20, 60, 100, 180, 240 and 300.

In other experiments (Figure 6.15 and Figure 6.16) APTs were also modelled by changing non controlled system parameters. In the MPC used in the experiments; sample time = 0.1s, control horizon =5 and prediction horizon 20.

6.1 Demonstration and evaluation steps

Section 3.3 established that the biological immune system exudes the properties of decentralisation, intelligence, message transfer, collaboration and environmental self-awareness. It was established in section 5.4.3.1 that all the other properties except environmental self-awareness and resilience were already established security parameters in ICS security. All these properties from the BIS were included in the bio-immunology inspired security model, but only environmental self-awareness was tested for its effectiveness because the other BIS components of collaboration, defence-in-depth and decentralisation are already established and used in ICS security. Piggin (2012) states that ICS security standards and frameworks provide reliable methods to securing systems and the standards' recommendations have been proven through research and evaluation. ICS standards (CPNI, 2008; QNCIS, 2014; Stouffer et al., 2015)

already recommend the use of firewalls and intrusion detection systems in ICS thus, their usefulness has already been established.

Thus, section 5.4.3.2 established the need to evaluate the model by investigating whether implementing the model would:

1. Enable the detection of APTs before they execute their payloads,
2. Stop APT from affecting the controlled process, and
3. Show that a predictive controller detects APTs and return process to steady state quickly.

It has been established earlier in the chapter that by having prediction at the controller level it means we have assumed that the APT entry into the system has not been detected but we wanted to establish if its effects can be reduced as it executes its payload by using the environmental self-awareness property which in this case would be implemented in the MPC controller. Table 6.1 summarises the steps taken in the demonstration and evaluation of the bio-immunology inspired security model.

Table 6.1: Demonstration and Evaluation steps

Bio-immunology inspired model demonstration and evaluation steps using CSTR and MPC		
Step	**What was done**	**Results demonstration**
Step 1	Demonstrate how a normal MPC controlled process behaves	Figure 6.9
Step 2	Demonstrate effect of APT on controlled process	Figure 6.12, Figure 6.13, Figure 6.14 (six iterations for each step value
Step 3	Demonstrating effect of APT by changing system inputs	Figure 6.15 and Figure 6.16
Step 4	evaluation	6.3 EVALUATION

6.1.1 Step 1: Demonstrate how a normal MPC controlled process behaves

At this stage, the aim was to run a normal process and observe how a normal process without any disturbances operates. That is to say, we observed the output of the system as it is shown in Figure 6.7.

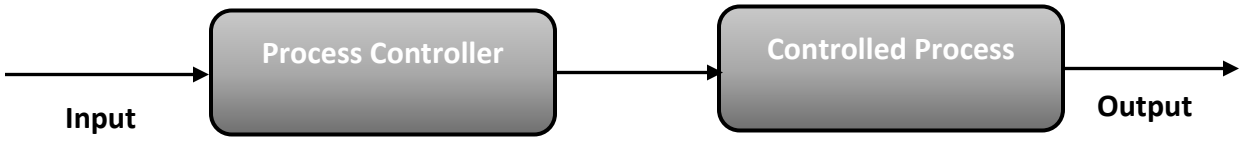


Figure 6.7: Normal Process Behaviour

Moreover, at this stage, baseline behaviour was being established. The output at this stage was going to be used to compare with any changes that might be incurred after introducing any changes. The output at this stage shows how the system behaves normally. The implementation of the model in Simulink is shown in Figure 6.8 and the results are shown in Figure 6.9.

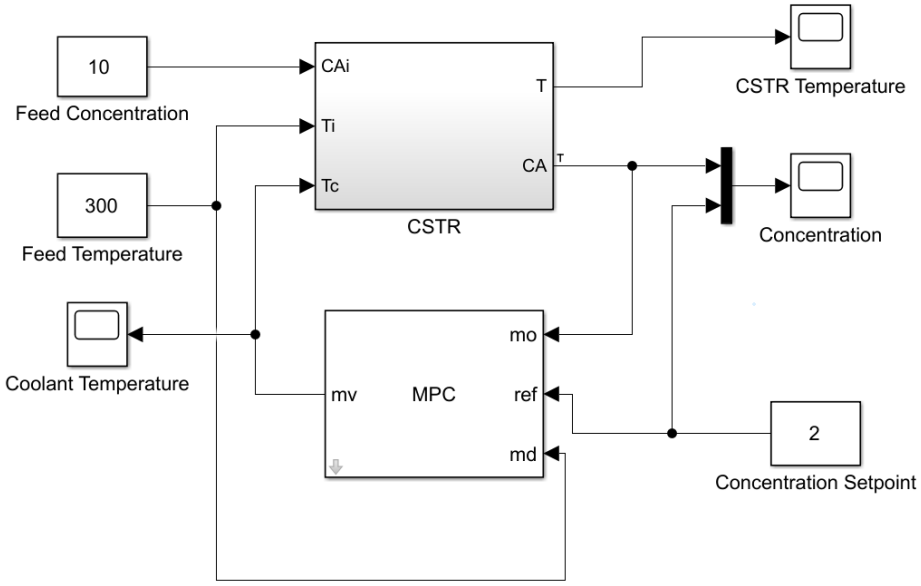


Figure 6.8: CSTR Model Predictive Control

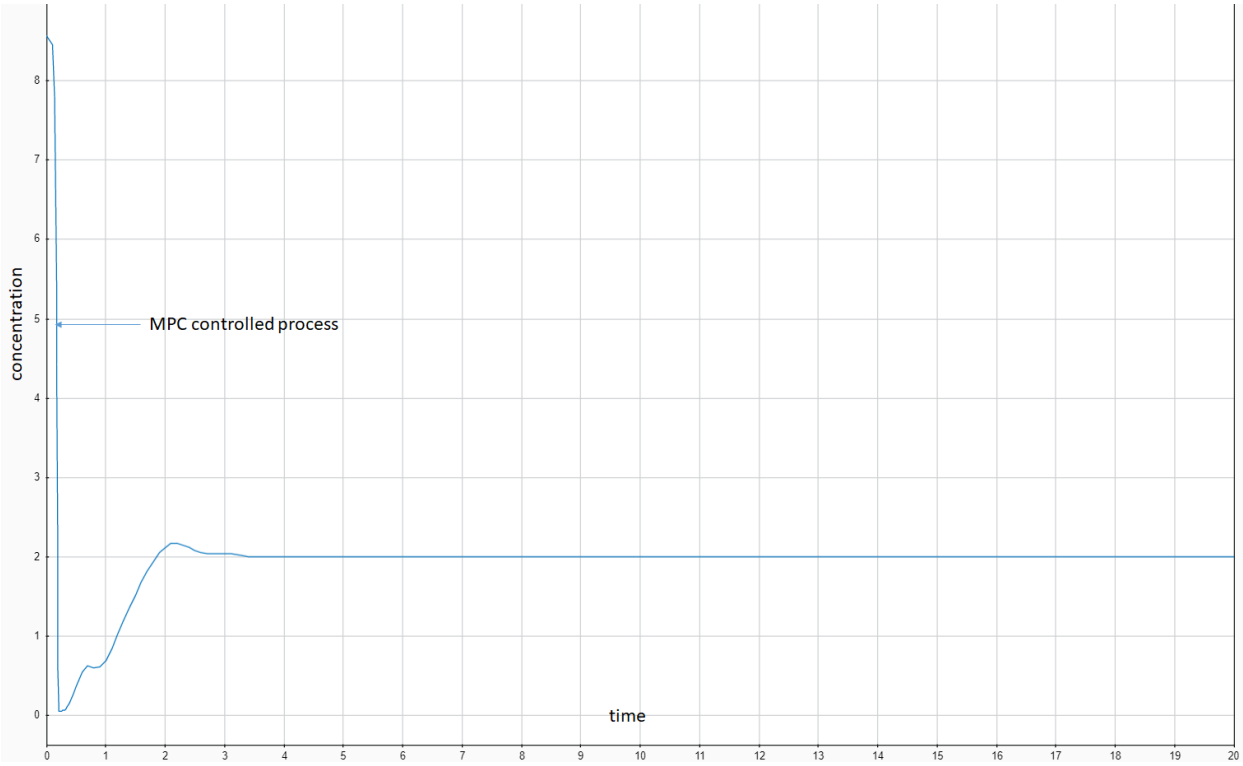


Figure 6.9: CSTR-MPC-Control Concentration

In process control systems settling time is the time taken for the process signal to be bounded to within a tolerance of 98% of the steady state value. For the CSTR example the residual concentration was set to 2kgmols/m^3. Therefore, CSTR will reach steady state when concentration is 1.96kgmols/m^3. It was observed and can be seen in Figure 6.9 that the settling time of the CSTR MPC controlled process is **3.5s**. To compare the results of the different stages, settling time is used to find out how the process fares after it has been attacked.

6.1.2 Step 2: Demonstrate effect of APT on controlled process

As was stated earlier, the ultimate goal of a Stuxnet resembling APT (section 2.4.2.2.) would be to change how the process behaves. A Stuxnet like attack aims to deviate the controlled process from normal behaviour. Thus, at this stage a step disturbance was introduced into the controlled process to observe the effects of introducing conditions that aim to alter process outputs of the controlled process. In this instance, the APT is matched to a significant disturbance on the system. A step disturbance as was highlighted in section 6.0.5 exemplifies the ultimate goal of an APT that will attack an ICS (that of changing how the process behaves). Figure 6.10 shows the

conceptual diagram of how a Stuxnet like APT attacks a controlled process. Figure 6.11 shows the actual Simulink implementation of APT attacking MPC controlled CSTR process.

In addition, the feed concentration (C_A) and feed temperature (T_i) were also varied to observe the effects of an attack that can alter other parameters of a system.

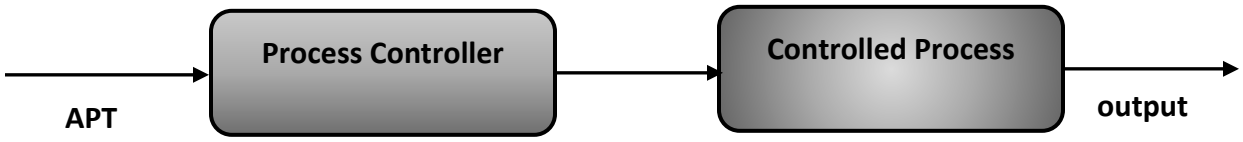


Figure 6.10: APT effect on controlled process

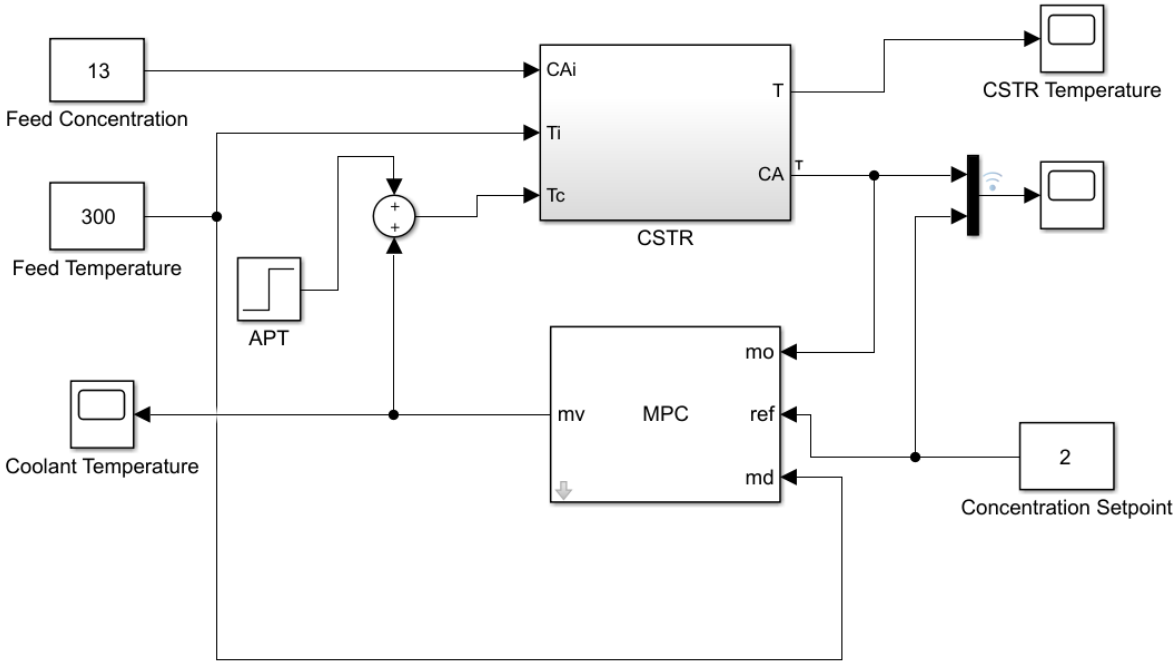


Figure 6.11: APT attack

For the Step disturbance, 3 step time intervals were considered for the MPC controlled processes;

- 0s,
- 4s and
- 8s,

For all these step times, final step values were varied as follows:

- 20
- 60
- 100
- 180
- 240 and
- 300

This means for each time interval the process was runs six times (six iterations at all the time intervals). That is at time t=0 a step disturbance of 20 was tested and recorded and repeated at time t=0 with a step disturbance of 60 was tested and recorded. Again at time = 0 a step disturbance of 100 was tested and recorded and repeated at step values 180, 240, and 300. 300 was the last unit chosen as anything above this would be above the feed temperature and thus would no longer be a coolant temperature as required. Temperatures above 300 were tested

when feed temperature was varied. Figures 6.12-6.14 show 6 different plots in different colours which show the different iterations done at each step

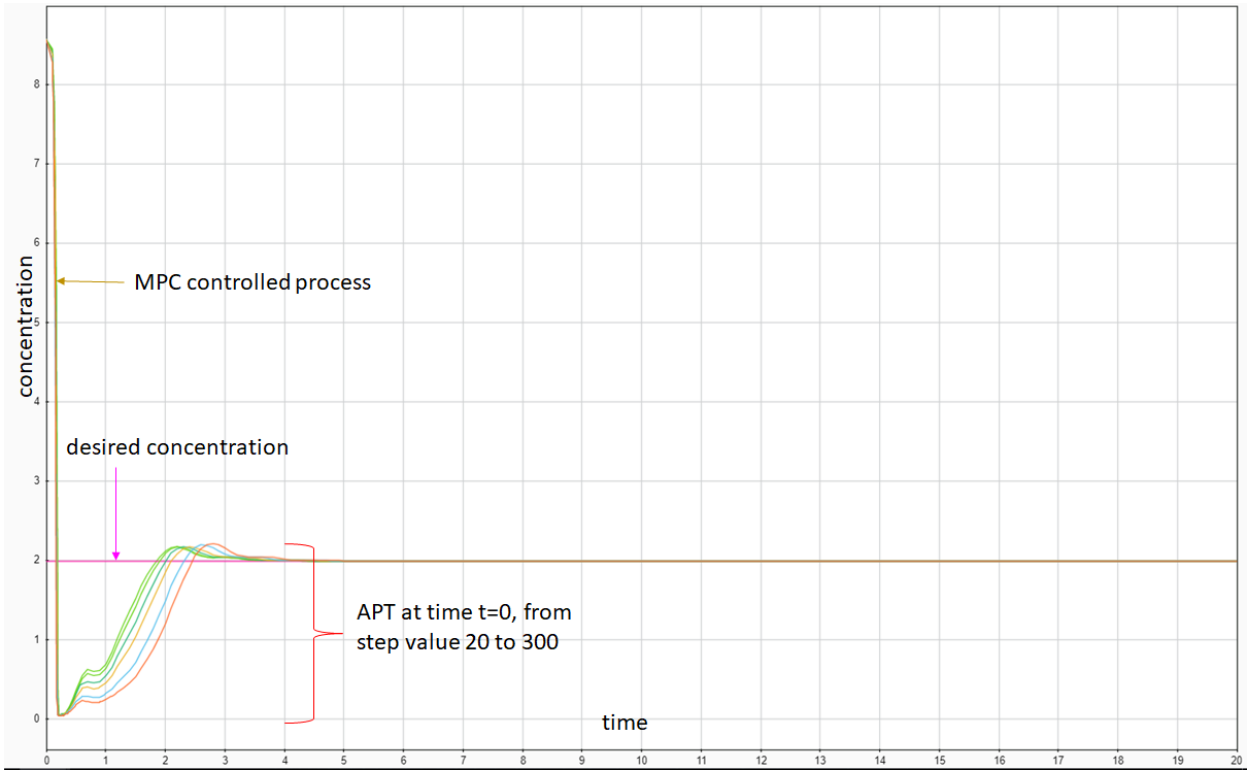


Figure 6.12: MPC controlled process APT attack at step time = 0

Figure 6.12 shows the results of attacking an MPC controlled CSTR process at the beginning of the process by using a step disturbance. Six different step values as described above were used. Results for step the values of 20, 60, 100, 180, 240 and 300 at time t=0 are shown in Figure 6.12. The graph shows that as the step disturbance value increases (as the intended effect of the APT increase), the overshoot value is not affected; it remains the same as that of the normal system. The settling time is affected and averages 4s after an attack at the beginning of the process. The average time is an increase of 0.5s from the normal settling time of the process. The MPC does reduce the effects of the APT because it does bring the process back to steady state.

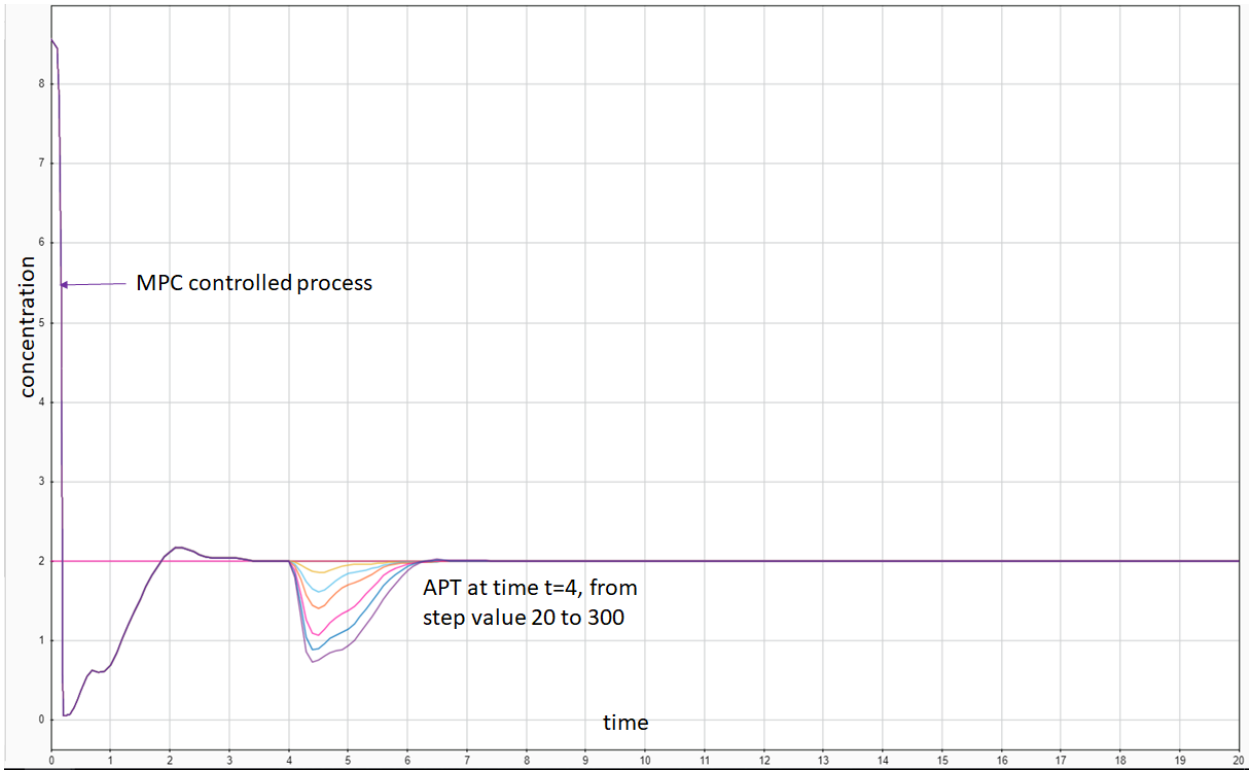


Figure 6.13: MPC controlled process APT attack at step time = 4

Figure 6.13 shows the results of attacking an MPC controlled CSTR process 4 seconds after it has started. Description of the experiment is the same as the one given for Figure 6.12. The difference is that for the experiment results shown on Figure 6.13 step times is 4s after the process has started. The graph shows that after an attack the process is affected, an undershoot is observed (the concentration goes below the desired concentration). It is also seen that as the step value increases from 20-300 so does the undershoot. The effect of the attack is immediately dealt with by the MPC as it immediately tries to bring the process back to steady state. For each attack value considered average time taken to return process to steady state is 2.5s. The time to return the process to steady state is not affected by the size of the step value, that means despite the intended impact of the APT the MPC would still be able to return the process to steady state as this is the desired feature of a controller. Figure 6.13 shows that 2.5 seconds is the average time needed to return the process to the steady state after an APT attack.

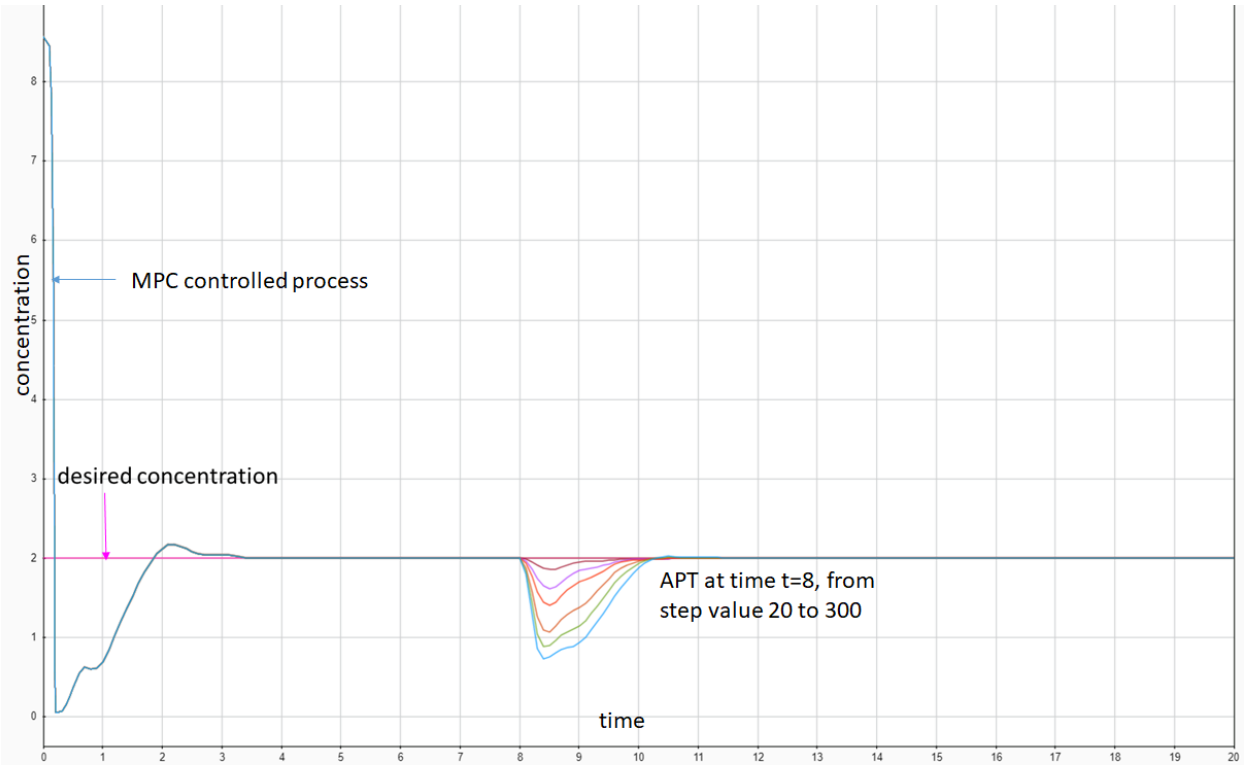


Figure 6.14: MPC controlled process APT attack at step time = 8s

Figure 6.14 shows the results of attacking an MPC controlled CSTR process 8 seconds after it has started. Description of the experiment is the same as the one given for Figure 6.13. The difference is that for the experiments depicted in Figure 6.14 step time (attack time) is 8s after the process has started. The graph shows that as the step value increases so does the undershoot. The average time taken to return process to steady state is 2.5s. The time to return the process to steady state is not affected by the size of the step value. Figure 6.14 shows that 2.5 seconds is the average time needed to return the process to the steady state, which is less than the desired settling time of 3.5 seconds and it is much less than the average time of 3.4 years shown in Table 2.1 section 2.3.0.

To summarise, when the process is attacked at the beginning, the overshoot of the system is unchanged, but the settling time increases to 4.0 seconds. In general, for the MPC controlled process (exemplified by Figures 6.12-6.14) when the process is attacked after the settling time, the process undershoots and settles after 2.5 seconds.

Repeating these attacks at any other time after settling time were depicting the same pattern.

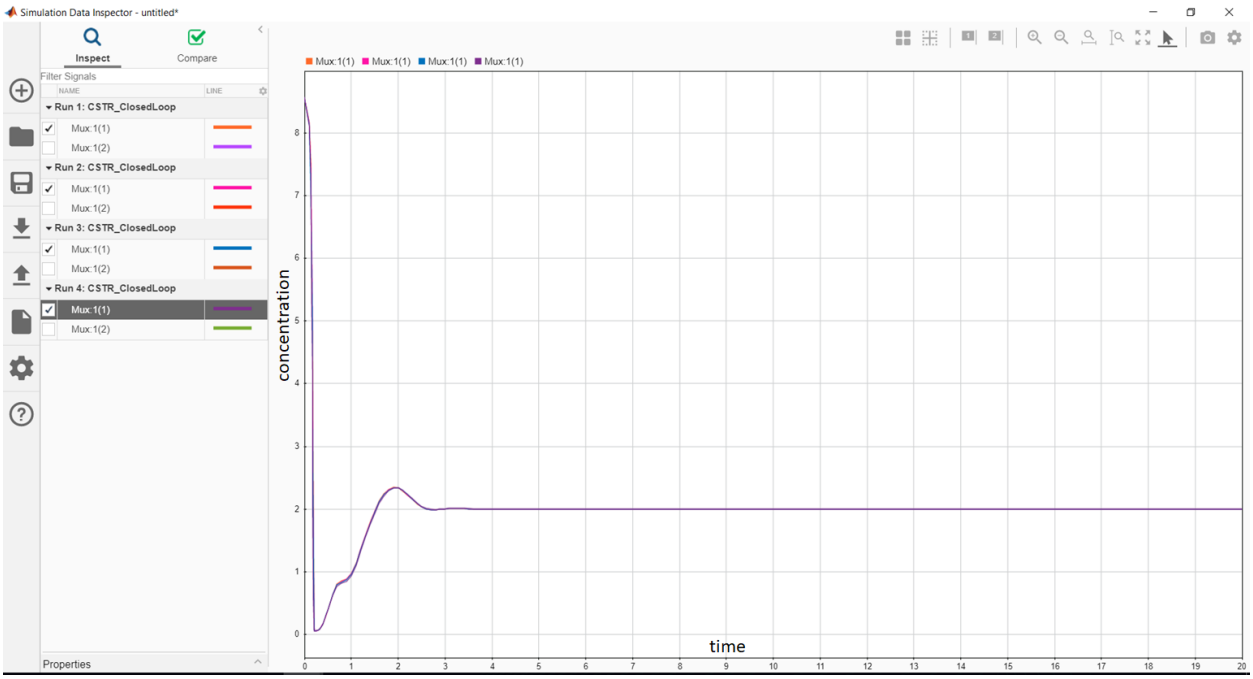


Figure 6.15: Changing feed temperature

Figure 6.15 shows the results of attacking an MPC controlled CSTR process by changing one of the non-controlled parameters (feed temperature). APTs in this scenario were changing the system input values. In this case, the feed temperature was varied from 300K to 400K as follows:

- Run 1 - 300K is the normal feed temperature
- Run 2 – 320K
- Run 3 – 350K
- Run 4 – 400K

The results of these tests show that if an APT managed to change the feed temperature it would have no effect on the process as the graph is exactly the same for all cases shown in Figure 6.9 which depicted how the process runs normally.

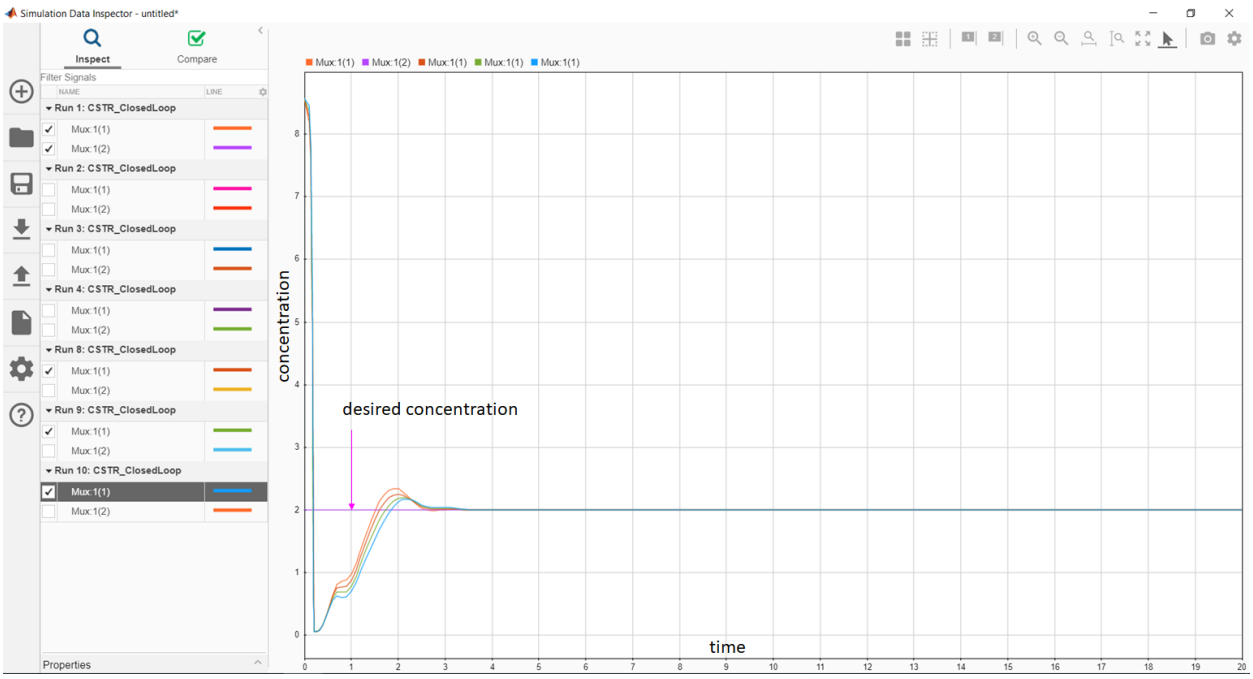


Figure 6.16: Changing feed concentration

Figure 6.16 shows the results of attacking an MPC controlled CSTR process by changing one of the non-controlled parameters. Here, the feed concentration was varied from 10kgmol/m^3 to 13 Kgmol/m^3 as follows:

- Run 1 - 10Kgmol/m^3 is the normal feed concentration
- Run 8 – 11Kgmol/m^3
- Run 9 – 12Kgmol/m^3
- Run 10 – 13Kgmol/m^3

The results of these tests show that if any APT managed to somehow alter the feed concentration, this would have no effect on settling time and overshoot of the process.

6.2 Results analysis

In section 6.0, it was stated that the experiment aimed to establish that a bio-immunology inspired security model secured system is able to stop APT affecting the controlled process and

that the model predictive controller returns the process to a normal state in a short time. APTs were modelled by step disturbances to the system and by varying non-controlled process inputs. An APT was introduced at the times 0s, 4s, and 8s. To re-iterate APTs like Stuxnet aim to change the process output by manipulating variables in an authorised manner. In this case the effect of an APT that of trying to change system variables is what was simulated by step functions and by the change in the feed temperature as well as the feed concentration. It was assumed that the APT is already in the system and is trying to alter system condition.

It was observed that:

- When the MPC controlled system was attacked at the beginning of the process, the settling time was affected by 0.5 seconds, but the concentration was not affected (Figure 6.12). This means the final product concentration was unaffected, but it happened 0.5s later than the usual time.
- When the MPC controlled system is attacked after the process had reached a steady state, it took 2.5seconds to return to a steady state (Figures 6.12-6.14). This is not a desirable condition because the concentration cannot be anything other than 2Kgmol/m^3. The controller will return the process to steady state but only after 2.5s.
- When the APT changes, the feed concentration settling time is not affected (Figure 6.16).
- When APT changes the feed temperature, there is no change on any process dynamics, and the settling time is also not affected (Figure 6.15).

The set metrics were to demonstrate:

- if the MPC controlled is able to stop APT affecting the controlled process, and
- the time that the predictive controller requires to returns the process to normal state. The process must be returned to steady state in a short time.

When the MPC controlled system was attacked at the beginning of the process, the biological immune system inspired ICS security implementation was able to circumvent the APT effects completely before it affected the process. These are the desired metrics, which mean that the

biological immune system inspired ICS security implementation of environmental self-awareness was working as desired.

When the MPC controlled system is attacked after settling time, it took 2.5seconds to return to the steady state then the biological immune system inspired ICS security implementation of environmental self-awareness is not able to stop the APT from affecting the process. The system undershoots and the drink concentration goes below the required levels. The system however, returned to steady state after 2.5 seconds, which means that the biological immune system inspired ICS security implementation of environmental self-awareness is able to return the process to a steady state. In addition, 2.5seconds is a short time to recover from an APT attack in relation to the time that it took for other APTs to be discovered in other security systems (table 2.1). These times are shown in Table 2.1 in section 2.3.0. The average time to discover an APT was shown as three years. Even though the APT had managed to penetrate the system, the MPC controlled process is able to return the process to steady state in 2 secs.

When the MPC controlled system's uncontrolled variables are altered, the biological immune system inspired ICS security implementation is able to stop the APT completely before it affects the process. These are the desired metrics.

The results stated above show that any changes effected on the system before it actually starts could be easily dealt with by the MPC controller. When the system is attacked after the process has been running for some time, the MPC controller is not able to stop the effects of the attack but works quickly to return the process to normal operating conditions. It has been highlighted in chapter three that the immune system is a system that has many layers that interact together. The fact that it is effective is brought about by these facts; that the different immune system parts do not work in isolation but work together in a distributed manner to achieve a security goal. The goal of the immune system is to defend the body from pathogens. For it to work effectively it has these properties, intelligence and collaboration, message transfer, resilience, distributed control and defence in depth.

Some of the negative results observed (Figures 6.12-6.14) were actually quite exciting because they actually showed that a bio-immunology inspired security system must not rely on one

security aspect. The BIS properties do not work in isolation but collaborate to eliminate invasions. It was stated that bio-immunology inspired security works best when all security properties are implemented and working in collaboration. The experiments described in this section were only testing the security property of being environmentally self-aware. The MPC could return the process to a steady state in a reasonable time but it was not able to actually stop the APT. This meant that optimum security conditions are only realised after working in collaboration with other layers of security. It can be said that when the security depends only on a few parameters like environmental self-awareness, which was tested in the experiments described in sections 6.1.1 and 6.1.2, then the results are sometimes acceptable but not always desirable.

6.3 Evaluation

6.3.1 Model behaviour in ICS

According to design science research process at the evaluation stage of the design science research It must be shown that the model, when applied in its context, will produce the desired output- this meant the need to show that the bio-immunology inspired security model when implemented in an ICS environment would be able to reduce the effects of an APT once it has entered the system. *Environmental self-awareness is a property of the biological immune system that enables the body to recognise or to be aware of the correct behaviour of the body at any particular time. This means when an invasion occurs, and a pathogen is affecting a body part/section it is understood or known by local biological immune agents that what is occurring in that part/section is not correct and corrective measures should be taken.* Therefore, if the bio-immunological immune system model is applied in an ICS it should be able to reduce the effects of an APT attack.

An ICS can have processes like the CSTR running producing some outputs like a drink, chemicals, and many other substances. When we add an MPC which adds the notion of environmental self-awareness in the ICS process of CSTR we observe that the MPC controller is able to detect the changes in the process and adjusts the input in such a way as to return the process to the required

state. In most processes of CSTR processes the concentration of the product cannot be anything other than the desired residual concentration. Thus, at the time of attack the product will have to be discarded. Normal APT attacks are normally detected after 3.4 years (section 2.3.0) thus the 2.5 seconds that the MPC controlled process took in the experiments depicted in figures (6.12-6.14) to return to normal conditions is a significant improvement. Thus, we can loosely say in the case of the CSTR used instead of taking 3.4 years to correct the effects of the APT then we would need 2.5 seconds by implementing the notion of environmental self-awareness via MPC.

6.3.2 Model evaluation against set objectives

Design science research also mandates that when evaluating the designed artefact comparison be made between set objectives and what is actually achieved based on the design specifications and using relevant metrics and analysis techniques found in relevant literature related to the control plant used as a case study.

> *The metrics to measure are that an APT 's effects are reduced as quickly as possible and that the predictive controller returns the process to normal state in a short time (section 6.0).*

In addition from section 5.4.3 points 4, 5, 8 and 9 (respectively) established that the model had to:

- *Detect attacks that are targeting Programmable Logic Controller (PLC).*
- *Be able to verify configuration changes and process input parameters.*
- *Add the notion of environmental self-awareness.*
- *Have prior knowledge of how the controlled process should behave*

The overall evaluation questions asked were:

1. Does the model implement the notion of environmental self-awareness?
2. Does the notion of adding of adding environmental self-awareness enable the system to have prior knowledge of how the controlled process should work?
3. Does the notion of adding environmental self-awareness enable detection of attacks targeting PLC?

4. Does the notion of adding of adding environmental self-awareness enable verification of configuration and process input parameter changes?
5. Does the notion of adding environmental self-awareness reduce APT effects as quickly as possible?

It was possible to use the experiments conducted in section 6.1, some additional experiments and the understanding of how some of the components used in the experiment work to answer the evaluation questions. The answers to the questions are described in the next sections

6.3.3 Does the model implement the notion of environmental self-awareness?

What is environmental self-awareness? Section 3.7.7 showed that environmental self-awareness can be summed to mean that whenever any part of the ICS system is attacked it knows to recognise that the situation is no longer normal and begin to act on the attackers. It implies that there are always localised security entities on guard and detect attacks anywhere on the system. In any ICS this is the work of any controller (PLC). As described in section 2.1.4 A PLC is a dedicated industrial computer deployed in a production environment for automating specific functions. They are used in such a way as to automate the expected outputs.

For any process controlled by a controller whenever there is a problem its job is to adjust system parameters so that the output remains constant or as the expected product. Despite the source of the disturbance on the controlled process the controller must always work to make sure that the process continues to run as is expected. The controller always has intelligence on the system by knowing the reference output and tracking that reference. This is similar to what the property of environmental self-awareness does in the immune system. The only difference between the controllers is the way that they control the process. And since an MPC is a type of controller then it does implement the notion of environmental self-awareness.

6.3.4 Does the notion of adding environmental self-awareness enable the system to have prior knowledge of how the controlled process should work?

How does the ICS have prior knowledge of the process? In most cases the controllers used in the control process only know the final output. Therefore, they control the process by tracking the output and the expected output reference. In the case of MPC the process is actually controlled

by having prior knowledge about the future process through the use of the controlled process's model. MPC uses the model of the plant to do predictions about the future process behaviour. It compares the model of expected process behaviour by calculating what will be the future outputs based on current inputs and make adjustments accordingly.

What is the importance of having prior knowledge about how the ICS controlled process should work? This is because, by knowing future outputs of the process if an ICS controlled process is attacked by a Stuxnet like APT that alters system inputs and parameters by comparing to the expected model of the system then it would be possible to correct the effects because the attack would have made the outputs deviate from the expected model behaviour. Therefore, the model of the system that is implemented within the workings of the MPC enables the system to have prior knowledge about the entire controlled process (inputs, outputs and any other process behaviours).

6.3.5 Does the notion of adding environmental self-awareness enable detection of attacks targeting PLC?

Sometimes a Stuxnet like attack aims to alter system outputs by attacking the controller itself. In the case of the MPC because the notion of environmental self-awareness is within the workings of the MPC if the attack aims for the PLC itself then the notion of adding environmental self-awareness will not enable the detection of attacks targeting PLC. The researcher proposes that in order for environmental self-awareness to work in favour of PLC the model of the process must be elsewhere in the controlled process not within the PLC like the case of MPC. It would be interesting to see how other predictive algorithms like the neural networks would fare against attacks aimed at the PLC.

6.3.6 Does the notion of adding environmental self-awareness enable verification of configuration and process input parameter changes?

Verification of configuration and input parameter changes can be verified by adding environmental self-awareness only if it is not within the PLC for the same reasons as explained in section 6.3.5. Thus, verification will only work if the attack did not target the controller itself.

6.3.7 Does the notion of adding environmental self-awareness reduce APT effects as quickly as possible?

In a separate CSTR experiment as described by (Bequette, 2002). The researcher carried the experiments as published in (Chitauro, Muyingi, John, & Chitauro, 2019). The experiments that were carried were used to compare a Proportional–Integral–Derivative (PID) controller and an MPC. A PID controller is also commonly used in the process industry (Terrence Blevins, 2012). In the experiment:

1. At first the process was run as normal using both a PID controller and MPC controller without an attack to build baseline behaviour.
2. A step disturbance as an APT was then introduced at the beginning of the process, i.e. at t=0s. To compare the results of the different stages the following parameters where chosen for comparison.

- Rise Time (tr) - the time taken for the output to go from 10% to 90% of the final value.
- Settling Time (ts) - The time taken for the process signal to be bounded to within a tolerance of 99% of the steady state value.
- Steady State Error (e_{ss}) - The difference between the input step value and the final value. This is the difference between the desired value and the final signal value.
- Overshoot - (max value − final value)/final value × 100.

Table 6.2 (Chitauro et al., 2019) shows the results obtained.

After the APT attack it showed that the PID controlled process could return the process to steady state in 3.5 seconds which was a better time than that of the MPC but the overshoot was significantly higher which shows that the product wasted (unwanted) is much more for PID controlled process. Having less overshoot means that when APT attacks a controlled process MPC will reduce the attack effects and not allow the final values of the process to go way beyond the expected parameters. This is the more desirable condition in our case because we aimed at reducing APT effects.

Table 6.2: Comparison of PID and MPC when attacked by APT

		Normal Controlled process		APT attacked Process	
		PID	MPC	PID	mpc
t_r	3	0.7	0.5	1	0.5
t_s	9	3.5	1.1	3.5	4
e_{ss}	0	0	0	0	0
overshoot	0	8%	0.1%	8%	3.2%

Taking into consideration also the experiments in section 6.1 that show that the notion of adding environmental self-awareness reduces APT effects as quickly as possible.

6.3.8 Evaluation Summary

Table 6.3 highlights the summary of the evaluation process. Here we were considering MPC controlled process.

Table 6.3: Summary of Evaluation process

Evaluation metric	Evaluation
Does the model implement the notion of environmental self-awareness?	Yes
Does the notion of adding of adding environmental self-awareness enable the system to have prior knowledge of how the controlled process should work?	Yes
Does the notion of adding environmental self-awareness enable detection of attacks targeting PLC?	No
Does the notion of adding of adding environmental self-awareness enable verification of configuration and process input parameter changes?	Yes and No
Does the notion of adding environmental self-awareness reduce APT effects as quickly as possible?	Yes

At the beginning of the experiments, the goal was to test if the MPC controlled process:

1. enables the detection of APTs before they execute their payloads,
2. stops APT from affecting the controlled process, and
3. shows that a predictive controller detects APTs quickly.

It was shown that the;

- MPC controlled process does detect APTs by sensing the changes in the expected outputs,
- MPC controlled process stops APT from affecting the process when the attack happens before the process starts,
- MPC is not able to stop attacks after the process has started, but is able to return APT to steady state, and
- MPC reduces effect of APT that do not attack controller quickly

As stated above, this outcome actually highlights what the immune system is all about. The biological immune system is a distributed collaborative system that works well when all the different defence mechanisms work together in a layered manner. The biological immune system is a robust system because all of its security elements work in collaboration. The fact that the predictive environment could achieve all three things that it was being tested for, but not at the best rates (could not stop APT when attacked after the process is already running) could mean that when other security parameters are introduced and work together, then it will yield better results. These results were transitively inferred to mean that when the bio-immunology inspired security model is implemented in full then the ICS security system would be able to:

- detect APT,
- stop APT from affecting the process, and
- have superior detection times than other detection mechanisms.

Looking at the set metrics to evaluate the bio-immunology inspired security model which in the experiments carried out was evaluating one parameter for the reasons explained in section 6.0. It can said that if environmental awareness is added to the controlled process in the controller part then everything as desired would be achieved but if the attack attacks the controller itself then it would not be detected.

6.4 Summary

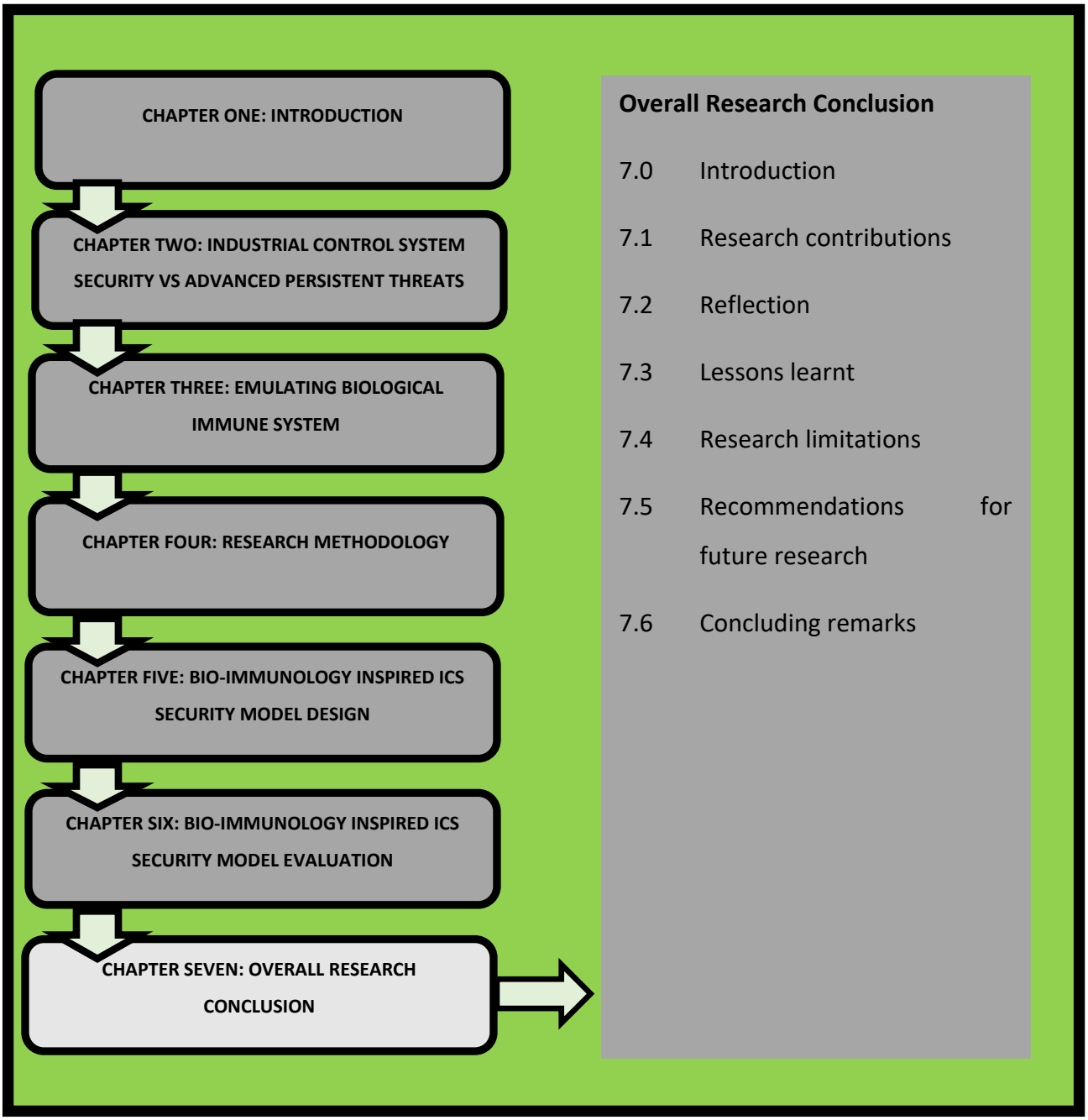
Chapter 6 demonstrated and evaluated the effectiveness of the proposed bio-immunology inspired security model design. Because other components of the bio-immunology inspired security model are tried and tested, the demonstration and evaluation concentrated on the use of environmental self-awareness. The demonstration and evaluation were carried out using a CSTR controlled process which simulates an ICS in MATLAB Simulink.

It was shown that;

- MPC controlled process does detect APTs by sensing the changes in the expected outputs,
- MPC controlled process stops APT from affecting the process when the attack happens before the process starts,
- MPC is not able to stop attacks after the process has started, but is able to return APT to steady state, and
- MPC reduces effect of APT that do not attack controller quickly.

The best defence system is one that has many security parameters in it or we can say the one that employs a defence-depth strategy and that which displays all the immune system properties. Thus, a bio-immunology inspired security model implemented in an ICS would have better performance according to the experiments carried out in this research.

CHAPTER 7 : OVERALL RESEARCH CONCLUSION



CHAPTER OUTLINE

After following the design science research methodology, this chapter concludes the research process. A design science research methodology was used to solve the problem of APT attacking ICS. The problem was solved by designing a bio-immunology inspired security model that can be adopted for use to enhance ICS security. To achieve this, research objectives were set. This chapter gives a reflection of how the research objectives were met through the research findings. In addition, research contributions and research limitations are discussed in this chapter. Furthermore, recommendations for future research directions are highlighted.

7.0 Introduction

The previous chapters discussed ICS, ICS security, APT, immune systems, research methodology, design and validation of a bio-immunology inspired security model to defend ICS from APT. ICS were characterised as critical systems that need to be protected from APTs that attack them. The problem to solve was that there was no clear and quick method to identify when an ICS is under attack from an APT as most APTs are discovered after some time in the system or only after they have realised their objective.

Although it was shown in Chapter two that ICS are secured using standards and many other security mechanisms from security experts, the security afforded by such efforts was not adequate to protect ICS from APT. Thus, this research proposed to study and emulate the biological immune system in order to enhance ICS security. The study of the biological immune system culminated in the design of a bio-immunology inspired security model to use when securing ICS.

Many other studies of the biological immune system have ended by modelling one or more components of the immune system into mathematical models that can later on be transformed to computational models. This research diverted from this normal status quo and suggested that we need to understand the properties of the biological immune system, instead of modelling them mathematically as is the typical with many researchers, the researcher emulated them in

ICS security. The biological immune system properties were emulated by using already established computational ways of having these properties in security implementations. What we needed to make sure is that all the properties of the biological immune system are available in the system that needs to be protected.

Design science research was used to design the bio-immunology inspired security model. Design science research, a mixed method approach, was used because it is problem solving paradigm. Demonstration and Evaluation of one component the model (environmental self- awareness) was done in MATLAB Simulink using a continuously stirred tank reactor (CSTR) model. The other components of the model where already proven for effectiveness.

The objectives of this research were:

1. Analyse where, how and why APT attack ICS
2. Evaluate current ICS defence mechanisms
3. Design bio-immunology inspired ICS security model
4. Validate bio-immunology inspired ICS security model

Following is a description of how the objectives were met.

1. APTs mostly attack ICS through the use of social engineering through things like spear phishing, click jacking and USB key delivery. More detailed information about this is given in section 2.4.2. APTs mostly attack ICS for the more common reason of stealing data and more scary reason like that of cyber sabotage as highlighted in Table 2.1. Finally APTs' point of entry is through humans and sometimes using camouflaging techniques to bypass security mechanisms like that of a firewall. More detail about this is covered in section 2.4.3.
2. ICS mechanisms derived from standards and security best practices are not adequate to deter APT. More detail in section 2.3.
3. Design of a bio-immunology inspired ICS security model was done using the design science research methodology motivated in Chapter four and the actual design steps are described in Chapter five.

4. Demonstration and evaluation of the bio-immunology inspired ICS security model is described in Chapter six which showcased that ICS security that is derived from the bio-immunology inspired security model yields better results than those that have not.

The next section discusses in summary the research journey and findings from each chapter as written in this document. The section also highlights contributions to the body of knowledge.

7.1 Research contributions

7.1.1 Findings from chapters

7.1.1.1 Findings from Chapter one: Introduction

Contribution of Chapter one towards the overall research is that of identification of the research area and identification and description of the problem to be solved.

7.1.1.2 Findings from Chapter two: Industrial Control System Security vs Advanced Persistent Threats

Chapter two discusses ICS, ICS security and APT through a critical literature review of available data on ICS security and APT. In this chapter, an evaluation of current ICS security indicated that the current ICS security is not adequate to defend ICS from APT. It was shown in this chapter that the APTs, which are targeted attacks, gain access into the ICS by bypassing access, auditing, monitoring and accountability controls. It was established that APT had three most common payloads namely, cyberespionage, data wiping and data theft and that the worst payload is that of cyber sabotage like that of Stuxnet.

This chapter also discussed the fact that APT like Stuxnet alter PLC logic to attain their goals. From this it was shown that to protect ICS from the most dangerous type of attack then the security mechanism designed would need to focus on those methods that can improve security around a PLC. Thus to address ICS security shortcomings it was suggested in this chapter to design ICS security by emulating the biological immune system.

7.1.1.3 Findings from Chapter three: Emulating Biological Immune System

This chapter discovered why biological immune system quickly discovers pathogens and effectively defend, the body from invasions. This is because every body parts can block, deflect,

detect, mitigate and recover from attacks; there is no central control for security and the BIS does not have 'perimeter' only security. For the biological immune system to achieve all this, it exhibits properties of being decentralised, intelligent and collaborating system, and environmentally self-aware. Collaboration, intelligence and decentralisation are already established in ICS security. Thus, the model had to add the notion of environmental self-awareness to ICS security.

Chapter Three also highlighted the existence of AIS which are computational systems derived from immune system operations. Current AIS challenges that have made them unsuccessful were also highlighted. It is this chapter that shows that there is no need to mathematically model the immune system in order to be able to design an ICS security solution that can be used to detect APT.

7.1.1.4 Findings from Chapter four: Research Methodology

Chapter four highlighted the research paradigm and methodology adopted in this research. The research paradigm adopted was the pragmatist paradigm and design science research methodology was highlighted as the overarching methodology for the research. Chapter four showed that design science research methodology would suffice to answer the main research question (How can ICS be secured to avoid APT attack?)

7.1.1.5 Findings from Chapter five: Bio-Immunology Inspired Security Model Design

Chapter five outlined design science research in general and how design science was applied in this research to design a bio-immunology inspired ICS security model. It showed the model development stages using ICS security literature, APT literature and biological immune system literature. It was also established in this chapter that the model that was to be designed had to benchmark with ICS security standards and this meant that the model had to include defence-in-depth strategies. It then identified the components that must be incorporated in a bio-immunology inspired security model, like a firewall, process controller, prediction controller, fall-back controller, process model, intrusion detection system and root of trust.

7.1.1.6 Findings from Chapter six: Bio-Immunology Inspired Security Model Evaluation

Chapter six contributed to the overall research by giving a description of how a bio-immunology inspired ICS security model was demonstrated and evaluated through the implementation of a

CSTR controlled process in MATLAB Simulink. The MPC controller used in the CSTR experiment showcased the use of environmental self-awareness which adds prediction to the security. This chapter demonstrated that the designed bio-immunology inspired ICS security model does detect the effects of APT and it enables the minimisation of the effects of the APT attack on the controlled process.

7.1.2 Contributions to the body of knowledge

7.1.2.1 Survey of ICS security

It was discovered that common defence techniques that are used to defend ICS from APT are the following: tweaking existing security controls, anomaly detection techniques, defence-in-depth techniques and securing the user plane. The defence-in-depth method was highlighted as the most commonly used method.

The survey of ICS security was published in two papers, the first one Bere & Muyingi, 2015, A preliminary review of ICS security frameworks and standards Vs. Advanced persistent threats and the second one Chitauro et al., 2019, A survey of APT defence techniques.

7.*1.2.2 Emulating biological immune system properties*

AIS challenges culminate to the fact that the biological immune system is not fully understood and therefore, it is not possible to correctly mathematically model it. Moreover, it is difficult to choose which immune system functionality will solve the current problem and that most AIS techniques ignore innate immune systems and mostly model adaptive immune system. The researcher argued that you do not need to fully understand how the biological immune system, but you need to fully understand the properties that enable it to protect the body and emulate those in the security solution proposed.

Benefits would be that we eliminate the need to understand all the under-pinnings of how the biological immune system works and rely on a high level understanding of the immune system only. Achieving the different biological immune system phenomena using paradigms that are already understand would be more beneficial and easier to execute. Therefore, to get best defence mechanisms from the biological immune system it is not always necessary to mathematically model the biological immune system desired phenomena. It would suffice to

understand what the desired phenomenon achieves in the immune system then use the already established methods of having the same effect and then implement the phenomena using already established mechanisms. The benefits would be that instead of starting from scratch to solve a problem, one simply uses tried and tested mechanisms.

The concept of using the biological immune system was published in Bere & Muyingi, 2015, Initial investigation of Industrial Control System (ICS) Security Using Artificial Immune System (AIS).

7.1.2.3 Bio-immunology inspired ICS security model

The bio-immunology inspired security model designed to detect APT before they can affect the controlled process in an ICS. The components are a firewall, process controller, prediction controller, fall-back controller, process model, intrusion detection system and root of trust. The model focuses on enhancing ICS security from APT by emulating biological immune system.

Benefits of the model are the improvement of ICS security. ICS are better prepared to defend themselves from APT. The Bio-immunology inspired ICS security model was published in (Chitauro et al., 2019) A Bio-Immunology Inspired Industrial Control System Security Model.

7.1.2.4 Model use

How stakeholders can use bio-immunology inspired ICS security model in ICS context. The target being ICS security personnel for use when they design and implement security for ICS

Benefits would be that all aspects of security required in ICS as prescribed by bio-immunology inspired security model would be incorporated and the reason why they need to be included is well understood.

7.2.1.5 How APT exploit humans

A description of how APTs get entry into systems mainly by exploiting humans was also done in this research. The methods of how APT gain entry into organisations was already well documented in literature but it was pointed out in the paper “How advanced persistent threats exploit humans (Bere et al., 2015) ” that these methods are mainly a resultant of exploiting humans. The mains methods used by APT to exploit humans identified in the paper are spear phishing and click jacking.

7.2.1.6 Advanced Persistent threat model for testing industrial control system security mechanisms

APT testing model for ICS security implementations was developed. The identified model components were reconnaissance, injection, installation, operation and command and control. The model was proposed as a systematic approach to testing and validating APT security mechanism for ICS. It was shown that in order to efficiently manage testing of ICS security mechanisms it would be useful to test for APT in an incremental manner. That means instead of having a full blown APT for testing rather test for APT in flow progression from the reconnaissance step all the way to the command and control step. This testing model was published in the paper (Chitauro et al., 2019)

7.2 Reflection

7.2.1 Methodological reflection

Design science research methodology adopted in this research falls under pragmatist paradigm which does not conform to one philosophy or reality (Hevner & Chatterjee, 2010). Instead it is a problem based approach which uses mixed methods to find means and ways to best solve the problem at hand (Hevner et al., 2004). Design science research emphasises the development of new products and outcomes that solve current problems (Hevner & Chatterjee, 2010 and Muyingi, 2009). Design science particularly came to life when information systems were implemented in order to better business efficiency and effectiveness

This research focused on designing a security model that can be deployed for use in ICS. This was a mixed methods problem which focused on solving the current problem of enhancing ICS security. To solve the problem content, documents analysis was used to design the security model and simulation experiments were used to validate the model. Focus was on how best to solve the problem at hand. Thus, design science research methodology was suited to solve the problem identified.

Acknowledging the fact that design science research is a problem solving approach that focuses on ways that best solve the problem at hand, the researcher is cognisant of the fact that other approaches might be taken to solve the same problem.

7.3 Lessons learnt

More knowledge and skills in the field of study were gained. It was only when I undertook this research when I appreciated the interdisciplinary nature of research. This meant we could use MATLAB/ Simulink control functionality to display biological immune system properties. To me research could be computer science, engineering, business, and so on with may be a few interactions here and there. I only fully grasped how many fields can be fully meshed when doing this research.

7.4 Research limitations

The research intersected three knowledge fields, computer science, control systems and biological immune systems. It was difficult to find experts who were well versed with all three. It would have been interesting to have experts with a holistic view of the research from all angles of expertise required.

The strength of the model emanates from the fact that it was designed from a strong computer science background with a broad understanding of network security and threats. However, its application domain was in an ICS and inspiration was drawn from the biological immune system which are not the researcher's strong points and relied on external expertise. Although this is also the research's novelty, that of merging the different fields of study.

7.5 Recommendations for future research

Since this research was conducted in an ICS environment, it would be interesting to bring the same type of security consideration in computer networks. The study should focus on how immune system properties can be incorporated in a typical computer network to achieve

intelligence through prediction, resilience and defence-in-depth capabilities in order to detect APT in IT legacy systems and other types of threats to information technology systems.

Simulation experiments were conducted to validate the model. Although MATLAB is a powerful simulation software, it is worthy to understand and know how the model would behave in a live lab experiment. This would yield results that would show how it behaves in real scenario.

Simulation experiments also focused on the use of a step disturbance. It would also be useful to vary the kind of disturbance in the system.

It would also be useful to use real APT data sets in conducting the simulation experiment. This research used a step disturbance to emulate an APT.

7.6 Concluding remarks

The main objective of this research was to develop a bio-immunology inspired ICS security model for improving existing ICS defence from APT. Four sub-objectives were articulated to achieve the main objective and they were achieved through research and experiments that intended to answer the research questions outlined in section 1.3. Table 7.1 presents the research questions and their answers.

Table 7.1: Research Questions Answers

Question	Answer	Evidence
Where and how do APTs Attack ICS?	By exploiting human weaknesses and weak security configurations. APT use social engineering, USB key delivery, fraudulently signed code or digital certificates, sql injection and memory based attacks	Figure 2.1, 2.2, and section 2.4 Paper 1: Appendix B Paper 3: Appendix C Paper 4: Appendix E
Why do APT attacks happen: Are ICS vulnerabilities from ICS inner workings/ operations, security strategy site or else?	APT attacks ICS for cyberespionage, data wiping, data theft and the most dangerous for cyber sabotage.	Figure 2.1 Paper 3: Appendix D

What approach can be considered in either case to avoid APTs attacks?	Develop a bio-immunology inspired ICS security model	Design security by emulating biological immune system properties to ICS security Paper 4: Appendix E Paper 5: Appendix F

The research followed design science research methodology which is a mixed method approach. Data collection was done through literature reviews and the final artefact developed was the bio-immunology inspired security model which was demonstrated and evaluated through the use of Simulink simulation experiments.

Research findings were published in peer reviewed conference proceedings and journals that focus on computer science, information security and control systems. First pages of the published papers are presented in Appendices B - G

A presentation of the model development and validation is found in chapters five and six. The model marries the defence strategies required in ICS security as identified in Chapter 2 and the properties of the immune system that makes it a versatile tool for defending the body from pathogens. Security requirements in a robust security ICS environment are layered together in the model to achieve better ICS security implementations. Having properties like defence-in-depth, resilience, intelligence and collaboration, being distributed, environmental self-awareness makes an ICS security system better suited to defending itself from APT.

The environmental self-awareness property that was investigated in this research meant that the prediction used draws from intelligence. Intelligence in this case was drawn from the use of previously computed model of the system and is used to make control decisions about the process. Self-awareness is a type of artificial intelligence, thus it is in line with emerging disruptive technologies. As was noted that it can be evaluated against neural networks as stated in section 6.3.5 which are vastly in used in artificial intelligence.

Well, coming to an end after a great and long journey in which a problem was identified and solved in five good years was worth it all. A Shona proverb says 'chisingaperi chinoshura' which directly translates to; "that which does not come to an end is like a bad omen"; but which actually means everything comes to an end, I conclude by saying:

GLORY BE TO GOD THE ALMIGHTY!!

References

Abbas, A. K., Lichtman, A. H., Pillai, S., Baker, D. L., & Baker, A. (2016). *Basic immunology: Functions and disorders of the immune system* (5th ed.). St. Louis, MI: Elsevier.

Aickelin, U., & Cayzer, S. (2008). The danger theory and its application to artificial immune systems. *ArXiv Preprint ArXiv:0801.3549*. Retrieved from http://arxiv.org/abs/0801.3549

Aickelin, U., Dasgupta, D., & Gu, F. (2013). Artificial immune systems (intros 2). *ArXiv Preprint ArXiv:1308.5138*. Retrieved from http://arxiv.org/abs/1308.5138

Aickelin, U., Dasgupta, D., & Gu, F. (2014). Artificial immune systems. In *Search methodologies* (pp. 187–211). Town, Country: Springer.

Amoroso, E. G. (2011). *Cyber attacks: Protecting national infrastructure*. Amsterdam: Butterworth-Heinemann/Elsevier.

Andrews, P. S., & Timmis, J. (2005a). Inspiration for the next generation of artificial immune systems. In C. Jacob, M. L. Pilat, P. J. Bentley, & J. I. Timmis (Eds.), *Artificial Immune Systems* (Vol. 3627, pp. 126–138). https://doi.org/10.1007/11536444_10

Andrews, P. S., & Timmis, J. (2005b). *Inspiration for the next generation of artificial immune systems.* International Conference on Artificial Immune Systems, 126–138. Retrieved from http://link.springer.com/10.1007%2F11536444_10

Averbuch, A., & Siboni, G. (2013). The classic cyber defense methods have failed–what comes next? *Military and Strategic Affairs*, *5*(1), 45-58.

Baize, E. (2012). Developing secure products in the age of advanced persistent threats. *IEEE Security & Privacy Magazine*, *10*(3), 88-92. https://doi.org/10.1109/MSP.2012.65

Bencsáth, B., Pék, G., Buttyán, L., & Félegyházi, M. (2012). The cousins of stuxnet: Duqu, Flame,

and Gauss. *Future Internet*, *4*(4), 971–1003. https://doi.org/10.3390/fi4040971

Bequette, B. W. (2002). *Process dynamics: Modeling, analysis, and simulation*. Upper Saddle River, NJ: Prentice Hall PTR.

Bere, M., & Muyingi, H. (2015). *Initial investigation of Industrial Control System (ICS) security using Artificial Immune System (AIS)*. *2*015 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), 79-84. https://doi.org/10.1109/ETNCC.2015.7184812

Bere, Mercy. (2015). *A preliminary review of ICS security frameworks and standards vs. advanced persistent threats*. Iccws 2015 - The Proceedings of the 10th International Conference on Cyber Warfare and Security: ICCWS2015. Presented at the Iccws 2015 - 10th International Conference on Cyber Warfare and Security: ICCWS2015.

Bere, M., Bhunu-Shava, F., Gamundani, A., & Nhamu, I. (2015). How advanced persistent threats exploit humans. *International Journal of Computer Science Issues*, *12*(6), 170-174.

Bhatt, P., Yano, E. T., & Gustavsson, P. (2014). *Towards a framework to detect multi-stage advanced persistent threats attacks*. Retrieved from https://doi.org/10.1109/SOSE.2014.53

Brewer, R. (2014). Advanced persistent threats: Minimising the damage. *Network Security*, *2014*(4), 5-9. https://doi.org/10.1016/S1353-4858(14)70040-6

Brogi, G., & Tong, V. V. T. (2016). TerminAPTor: Highlighting advanced persistent threats through information flow tracking. *2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 1-5. Retrieved from https://doi.org/10.1109/NTMS.2016.7792480

Castro, L. N. de, & Zuben, F. J. V. (2002). Learning and optimization using the clonal selection

principle. *IEEE Transactions on Evolutionary Computation*, *6*(3), 239–251. Retrieved from https://doi.org/10.1109/TEVC.2002.1011539

Chapple, M., & Seidl, D. (2015). *Cyberwarfare: Information operations in a connected world*. Burlington, MA: Jones & Bartlett Learning.

Chitauro, M., Muyingi, H., John, S., & Chitauro, S. (2019). *A survey of APT defence techniques*. Presented at the 14th International Conference on Cyber Warfare and Security ICCWS 2019 (pp. 46-57), Stellenbosch, ACPIL.

Chitauro, M., Muyingi, H., John, S., & Chitauro, S. (2019, March 29). *A bio-immunology inspired industrial control system security model.* Presented at the First International Conference on Sustainable Technologies for Computational Intelligence (ICTSCI—2019), (pp. 823-835) Jaipur, Rajasthan, India.

Control System | Closed Loop Open Loop Control System. (n.d.). Retrieved from https://www.electrical4u.com/control-system-closed-loop-open-loop-control-system/

CPNI, C. for the P. of I. (2008). *Good practice guide, process control and SCADA security*. Retrieved from http://www.cpni.gov.uk/documents/publications/2008/2008031-gpg_scada_security_good_practice.pdf

Dasgupta, D. (2006). Advances in artificial immune systems. *IEEE Computational Intelligence Magazine*, *1*(4), 40-49. https://doi.org/10.1109/MCI.2006.329705

Dasgupta, D., Yu, S., & Nino, F. (2011). Recent advances in artificial immune systems: Models and applications. *Applied Soft Computing*, *11*(2), 1574-1587. https://doi.org/10.1016/j.asoc.2010.08.024

de Vries, J., Hoogstraaten, H., van den Berg, J., & Daskapan, S. (2012). *Systems for detecting*

advanced persistent threats: A development roadmap using intelligent data analysis. Retrieved from https://doi.org/10.1109/CyberSecurity.2012.14

Edgar, D. (2005). *Master medicine: Immunology*. Edinburgh, UK: Elsevier.

Falliere, N., Murchu, L. O., & Chien, E. (2011). W32. Stuxnet dossier. *White Paper, Symantec Corp., Security Response*, *5*(6).

Fortinet. (2013). *Threats on the Horizon: The rise of the advanced persistent threats*. Retrieved from http://www.fortinet.com/sites/default/files/solutionbrief/threats-on-the-horizon-rise-of-advanced-persistent-threats.pdf

Franklin, Z. R., Patterson, C. D., Lerner, L. W., & Prado, R. J. (2014). *Isolating trust in an industrial control system-on-chip architecture.* Resilient Control Systems (ISRCS), 2014 7th International Symposium On, 1–6. IEEE. https://ieeexplore-ieee-org.eresources.nust.na/document/6900096

Garrett, S. M. (2005). How do we evaluate artificial immune systems? *Evolutionary Computation*, *13*(2), 145-177.

Giura, P., & Wang, W. (2012). *A context-based detection framework for advanced persistent threats*. Retrieved from https://doi.org/10.1109/CyberSecurity.2012.16

Harshe, O. A., Chiluvuri, N. T., Patterson, C. D., & Baumann, W. T. (2015). *Design and implementation of a security framework for industrial control systems.* Industrial Instrumentation and Control (ICIC), 2015 International Conference On, 127–132. IEEE. https://ieeexplore-ieee-org.eresources.nust.na/document/7150724

Hart, E., & Timmis, J. (2008). Application areas of AIS: The past, the present and the future. *Applied Soft Computing*, *8*(1), 191–201. https://doi.org/10.1016/j.asoc.2006.12.004

Hevner, A., & Chatterjee, S. (2010). Design science research in information systems. In A.

Hevner & S. Chatterjee, *Design research in information systems* (Vol. 22, pp. 9-22). https://doi.org/10.1007/978-1-4419-5653-8_2

Hevner, A. R., March, S. T., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, *28*(1), 75–105.

Ellis, J. , T., & Levy, Y. (2010). *A guide for novice researchers: Design and development research methods*. Retrieved from https://doi.org/10.28945/1237

Jha, N. K. (2008). *Research methodology*. Chandigarh, India: Abhishek Publications.

Johnson, J., & Henderson, A. (2002). Conceptual models: Begin by designing what to design. *Interactions*, *9*(1), (25-32). https://doi.org/10.1145/503355.503366

Kaspersky. (2015). *The desert falcons targeted attacks*. Retrieved from https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064309/The-Desert-Falcons-targeted-attacks.pdf

Knapp, E. (2011). *Industrial network security: Securing critical infrastructure networks for Smart Grid, SCADA , and other industrial control systems*. Amsterdam: Elsevier/Syngress.

Knapp, E. D., & Langill, J. T. (2015a). *Industrial network security: Securing critical infrastructure networks for Smart Grid, SCADA, and other industrial control systems* (2nd ed.), R. Samani (Ed.). Amsterdam Boston Heidelberg London: Elsevier, Syngress.

Knapp, E. D., & Langill, J. T. (2015b). *Industrial network security: Securing critical infrastructure networks for Smart Grid, SCADA, and other industrial control systems* (2nd ed.), R. Samani (Ed.). Amsterdam Boston Heidelberg London: Elsevier, Syngress.

Krotofil, M., & Gollmann, D. (2013). *Industrial control systems security: What is happening?* Industrial Informatics (INDIN), 2013 11th IEEE International Conference On, 670–675. IEEE. https://ieeexplore-ieee-org.eresources.nust.na/document/6622964

Lerner, L. W., Farag, M. M., & Patterson, C. D. (2012). *Run-time prediction and preemption of configuration attacks on embedded process controllers*. Proceedings of the First International Conference on Security of Internet of Things, 135–144. Retrieved from http://dl.acm.org/citation.cfm?id=2490447

Lerner, L. W., Franklin, Z. R., Baumann, W. T., & Patterson, C. D. (2014, June). *Application-level autonomic hardware to predict and pre-empt software attacks on industrial control systems*. Retrieved from https://doi.org/10.1109/DSN.2014.26

Lethbridge, T. C., & Laganière, R. (2005). *Object-oriented software engineering: Practical software development using UML and Java* (2. ed.). London, UK: McGraw-Hill.

Liu, F., Wang, Q., & Gao, X. (2006). *Survey of artificial immune system*. *Systems and control in aerospace and astronautics, 2006.* ISSCAA 2006. 1st International Symposium on, 5–pp. http://ieeexplore.ieee.org/abstract/document/1627489/

Lu, J., Chen, K., Zhuo, Z., & Zhang, X. (2017). *A temporal correlation and traffic analysis approach for APT attacks detection*. Cluster Computing. https://doi.org/10.1007/s10586-017-1256-y

Macaulay, T., & Singer, B. (2012). *Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS*. Boca Raton, FL.: CRC Press.

Maxwell, J. A. (2012). *A realist approach for qualitative research*. Thousand Oaks, CA: SAGE Publications.

McLaren, P., Russell, G., & Buchanan, B. (2017). *Mining malware command and control traces.* 2017 Computing Conference, 788–794. Retrieved from https://doi.org/10.1109/SAI.2017.8252185

Messaoud, B. I. D., Guennoun, K., Wahbi, M., & Sadik, M. (2016). *Advanced persistent threat:*

New analysis driven by life cycle phases and their challenges. *2*016 International Conference on Advanced Communication Systems and Information Security (ACOSIS), 1–6. https://doi.org/10.1109/ACOSIS.2016.7843932

Models and Modelling. (n.d.). Retrieved May 12, 2018, from OpenLearn website: http://www.open.edu/openlearn/science-maths-technology/computing-and-ict/models-and-modelling/content-section-0

Mohamed Elsayed, S. A., Ammar, R. A., & Rajasekaran, S. (2012a). *Artificial immune systems: Models, applications, and challenges*. Retrieved https://doi.org/10.1145/2245276.2245326

Mohamed Elsayed, S. A., Ammar, R. A., & Rajasekaran, S. (2012b). *Artificial immune systems: Models, applications, and challenges.* Proceedings of the 27th Annual ACM Symposium on Applied Computing - SAC '12, 256. Retrieved from https://doi.org/10.1145/2245276.2245326

Muijs, D. (2004). *Doing quantitative research in education with SPSS*. London, UK: Sage Publications.

Murphy, K. P., Travers, P., Walport, M., Ehrenstein, M., & Janeway, C. (Eds.). (2008). *Janeway's immunobiology* (7th ed.). New York, NY: Garland Science.

Muyingi, H. (2009). *How to do research when there's no-one much to help you*. in press

Nachenburg, C. (2010). *A forensic dissection of Stuxnet*. https://cisac.fsi.stanford.edu/multimedia/forensic-dissection-stuxnet

O'Leary, Z. (2014). *The essential guide to doing your research project* (2nd ed.). Los Angeles, LA: SAGE.

Paradise, A., Shabtai, A., Puzis, R., Elyashar, A., Elovici, Y., Roshandel, M., & Peylo, C. (2017).

Creation and management of social network honeypots for detecting targeted cyber-attacks. *IEEE Transactions on Computational Social Systems*, *4*(3), 65-79. https://doi.org/10.1109/TCSS.2017.2719705

Parham, P. (2009). *The immune system* (3rd ed.). London, UK: Garland Science.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, *24*(3), 45-77. https://doi.org/10.2753/MIS0742-1222240302

Piggin, R. S. H. (2012). *Emerging good practice for cyber security of industrial control systems and SCADA.* System Safety, Incorporating the Cyber Security Conference 2012, 7th IET International Conference, 1–6. IET. https://ieeexplore-ieee-org.eresources.nust.na/document/6458961

Ponemon Institute LLC. (2013). *The state of advanced persistent threats*. Retrieved from http://informationsecurity.report/Resources/Whitepapers/b92cfb99-1e2b-4c3d-9803-4720b7bb0d36_state-advanced-persistent-threats-pdf-6-w-1053.pdf

QNCIS, Q. N. C. for I. S. (2014). *National ics security standard v.3*. Retrieved from http://www.scadahacker.com/library/Documents/Standards/QCERT%20-%20National%20ICS%20Security%20Standard%20v.3%20-%20March%202014.pdf

Ritchie, J., & Lewis, J. (Eds.). (2003). *Qualitative research practice: A guide for social science students and researchers*. Thousand Oaks, CA: Sage Publications.

Saud, Z., & Islam, M. H. (2015). *Towards proactive detection of advanced persistent threat (APT) attacks using honeypots*. Proceedings of the 8th International Conference on Security of Information and Networks - SIN '15, 154–157. https://doi.org/10.1145/2799979.2800042

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2009). *Research methods for business students* (5th ed.). New York, NY: Prentice Hall.

Segel, L. A., & Cohen, I. R. (Eds.). (2001). *Design principles for the immune system and other distributed autonomous systems*. Oxford, UK: Oxford Univ. Press.

Sekaran, U., & Bougie, R. (2010). *Research methods for business: A skill-building approach* (5th ed.). Chichester, UK: Wiley.

Siddiqui, S., Khan, M. S., Ferens, K., & Kinsner, W. (2016). *Detecting advanced persistent threats using fractal dimension based machine learning classification*. Proceedings of the 2016 ACM on International Workshop on Security and Privacy Analytics - IWSPA '16, 64–69. Retrieved from https://doi.org/10.1145/2875475.2875484

Skopik, F., Friedberg, I., & Fiedler, R. (2014). Dealing with advanced persistent threats in smart grid ICT networks. *Innovative Smart Grid Technologies Conference (ISGT), 2014 Ieee Pes*, 1–5. IEEE. https://ieeexplore-ieee-org.eresources.nust.na/document/6816388

Slay, J., & Miller, M. (2007). Lessons learned from the maroochy water breach. *International Conference on Critical Infrastructure Protection*, 73-82.

Somayaji, A., Locasto, M., & Feyereisl, J. (2008). *The future of biologically-inspired security: Is there anything left to learn?* Proceedings of the 2007 Workshop on New Security Paradigms, 49-54. Retrieved from http://dl.acm.org/citation.cfm?id=1600185

Sood, A. K., & Enbody, R. (2012). Targeted cyber-attacks - A superset of advanced persistent threats. *IEEE Security & Privacy Magazine*, 1–1. https://doi.org/10.1109/MSP.2012.90

Sosik, S. J. (2003). *SCADA systems in wastewater treatment*. https://ieeexplore-ieee-org.eresources.nust.na/document/6231617

Stepney, S., Smith, R. E., Timmis, J., & Tyrrell, A. M. (2004). *Towards a conceptual framework for artificial immune systems.* International Conference on Artificial Immune Systems, 53-64. Retrieved from http://link.springer.com/chapter/10.1007/978-3-540-30220-9_5

Stepney, S., Smith, R. E., Timmis, J., Tyrrell, A. M., Neal, M. J., & Hone, A. N. (2005). Conceptual frameworks for artificial immune systems. *IJUC*, *1*(3), 315 - 338.

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). *Guide to industrial control systems (ICS) Security* (No. NIST SP 800-82r2). Retrieved from https://doi.org/10.6028/NIST.SP.800-82r2

Tankard, C. (2011). Advanced persistent threats and how to monitor and deter them. *Network Security*, *2011*(8), 16-19. https://doi.org/10.1016/S1353-4858(11)70086-1

Targeted Cyberattacks Logbook. (n.d.). Retrieved from https://apt.securelist.com/#!/threats/

Terrence Blevins. (2012). *PID advances in industrial control*. Presented at the Conference of Advances in PID Control, Brescia. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.476.8972&rep=rep1&type=pdf

Timmis, J., Hone, A., Stibor, T., & Clark, E. (2008). Theoretical advances in artificial immune systems. *Theoretical Computer Science*, *403*(1), 11 - 32. https://doi.org/10.1016/j.tcs.2008.02.011

Tomhave, B. L. (2005). *Alphabet soup: Making sense of models, frameworks, and methodologies*. https://www.secureconsulting.net/Papers/Alphabet_Soup.pdf

USDoE, U. S. D. of E. (n.d.). *21 Steps to Improve Cyber security of SCADA Networks*. Retrieved from http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf

Ussath, M., Jaeger, D., Feng C., & Meinel, C. (2016). *Advanced persistent threats: Behind the scenes.* 2016 Annual Conference on Information Science and Systems (CISS), 181–186. Retrieved from https://doi.org/10.1109/CISS.2016.7460498

Virvilis, N., & Gritzalis, D. (2013). *The big four - What we did wrong in advanced persistent threat detection?* 248–254. Retrieved from https://doi.org/10.1109/ARES.2013.32

Virvilis, N., Gritzalis, D., & Apostolopoulos, T. (2013). *Trusted computing vs. advanced persistent threats: Can a defender win this game?* Retrieved from https://doi.org/10.1109/UIC-ATC.2013.80

Wahyuni, D. (2012). The research design maze. *Understanding Paradigms, Cases, Methods and Methodologies*, *10*(1), (pp. 69-80).

Welman, J. C., & Kruger, F. (1999). *Research methodology for the business and administrative sciences*. Halfway House: International Thomson Pub. (Southern Africa).

WHO Life Expectancy. (n.d.). Retrieved from http://www.who.int/gho/mortality_burden_disease/life_tables/situation_trends_text/en/

Zhang, Q., Li, H., & Hu, J. (2017). *A study on security framework against advanced persistent threat*. 2017 7th IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC), 128–131. https://doi.org/10.1109/ICEIEC.2017.8076527

Zheng, J., Chen, Y., & Zhang, W. (2010). A Survey of artificial immune applications. *Artificial Intelligence Review*, *34*(1), 19-34. https://doi.org/10.1007/s10462-010-9159-9

APPENDIX A

HIGHLINE COLLEGE

May 29, 2018

Mercy Chitauro
PhD Candidate
Computer Science
Namibia University of Science and Technology

Dear Committee Members:

I am writing this letter in support of Mercy Chitauro, a PhD Candidate in your Computer Science Program at Namibia University of Science and Technology. I read Mercy and her colleague's paper titled, "Anatomy of a Bio-Immunology Inspired Security Architecture to Defend Industrial Control Systems from Advanced Persistent Threats," and am impressed with her abundant knowledge of the immune system and how it works. I am particularly impressed with her vision of how the immune system can help us to learn how to make better industrial control systems. When she said,

"Some of the properties that make the immune system robust are:
- it is decentralised,
- it is an intelligent and collaborative system
- and self-aware,"

I was positively struck with the choice of wording "self-aware" and how that describes such an amazingly complex and vital system to human well-being. I made a few minor suggestions on the paper and they were well received. From my background, where I earned a B.S. in Bioengineering from the University of California at Berkeley, USA, and later went on to earn a Ph.D. in Immunology from Stanford University in Stanford, CA, USA, I am VERY excited to see Mercy and her colleagues translate how the immune system works to keeping computer systems safe from advanced persistent threats.

In summary, I am writing with enthusiastic support of Mercy Chitauro and her work on using the immune system as a model for designing advanced computer systems security technology. If you have any questions, please feel free to contact me.

Sincerely,

Colleen Sheridan, PhD, MEd
Biology Faculty
Highline College
Phone: 1 (206) 592-4009
Email: csheridan@highline.edu

highline.edu (206) 878-3710 (206) 870-3782 P.O. Box 98000, Des Moines WA 98198-9800

APPENDIX B: PAPER 1

IJCSI International Journal of Computer Science Issues, Volume 12, Issue 6, November 2015
ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784
www.IJCSI.org

How Advanced Persistent Threats Exploit Humans

Mercy Bere[1], Fungai Bhunu-Shava[2], Attlee Gamundani[3], Isaac Nhamu[4]

[1, 2, 3, 4] Computer Science Department, Polytechnic of Namibia, Windhoek Namibia

Abstract

Advanced Persistent Threats (APT) are a fast growing security concern for ICT users in homes, governments and other organisations. Initial delivery of APT in computer systems is achieved by social engineering people within the organisations. This research employed a preliminary desktop review of how APTs are delivered in organisations' computer systems and discovered that spear phishing is the leader in social engineering techniques used in APTs to compromise industrial control systems security. A description on how APTs operate and how spear phishing and click jacking are used as tools to successfully exploit organisational security is presented. In addition the paper briefly describes implications of successful APT attacks in organisations. Further the paper proposes use of the APT awareness stages in order for organisations to improve their security posture through user security awareness

Keywords: *Advanced Persistent Threats; Industrial Control Systems, social engineering; security awareness; organisational security*

networking security model for securing industrial control systems from APTs.

The following sections of the paper are organised as follows. The next section will outline APT and the APT lifecycle. Section 3 and 4 will discuss the social engineering methods used by APTs to attack IP networks. Section 5 will give a brief overview of the implications of successful APT attack. Section 6 will show some of the security aspects organisations need to beef up on, in order to increase user security awareness. Section 7 will be the conclusion.

2. Advanced Persistent Threats

Advanced Persistent Threats are sophisticated multistep cyberattacks which are designed in such a way that they only attack specific targets [5]. In order to successfully infiltrate a network APTs usually follow the following attack stages [2, 5, 6]:

APPENDIX C: PAPER 2

Advanced Persistent Threat Model for Testing Industrial Control System Security Mechanisms

Mercy Bere-Chitauro, Hippolyte Muyingi, Attlee Gamundani, Shadreck Chitauro
Polytechnic of Namibia transforming into Namibia University of Science and Technology,
Computer Science Department, Windhoek, Namibia
{mbere, hmuyingi, agamundani,schitauro}@polytechnic.edu.na

Abstract: An APT is a targeted multi-step attack that uses zero day exploits to achieve its objectives. In order to find solutions to mitigate APT attacks it is important to understand APT anatomy. This paper proposes an APT testing model developed using design research methodology that can be used to develop Industrial Control Security (ICS) mechanisms. The model development followed three steps; identifying the components; identifying and explaining the characteristics in each component and developing the model. 6 components were identified to be included in the model; reconnaissance, injection, installation, operation, command and control and termination. The model proposed is envisaged as systematic approach to testing and validation of security mechanisms that are aimed at APT detection in ICS.

Keywords: Advanced Persistent threats, industrial control system, security, attacks, threats

1. Introduction

Advanced Persistent Threats (APT) are persistent cyber-attacks that stealthily infiltrate a network [1]. APT use reconnaissance attacks to gain information about their targeted networks. The information from the reconnaissance attack is used to find ways and methods to gain access into the system. Once an APT has found its entry point and positioned itself

APPENDIX D: PAPER 3

A Preliminary Review of ICS Security Frameworks and Standards Vs. Advanced Persistent Threats

Mercy Bere

Polytechnic of Namibia, Windhoek, Namibia

mebshc@yahoo.com

Abstract

Industrial Control Systems (ICS) control critical industrial processes. Just like any other computer system ICS are vulnerable to attacks which can compromise the infrastructure and or the system components of ICS. Consequently the process being controlled is affected by the attacks. ICS are secured by following best practices and recommendations from ICS security frameworks and standards. It would seem that after implementing and adhering to best practices ICS would be secure and difficult to gain access to, but this is not the case because ICS are being compromised by a new kind of threat christened "Advanced Persistent Threats" (APT). An APT is a multi-step attack designed to realise a particular objective. All the traditional methods of detecting attacks like firewalls, intrusion detection systems and antivirus scanners fail to detect APTs before they have realised their objective. This implies that following ICS security best practices which recommend the use of firewalls, intrusion detection systems, and antivirus scanners is not enough to deter APTs. This paper will highlight why ICS security frameworks and standards are not sufficient for securing ICS from APTS and will propose possible methods of securing ICS from APTs.

Keywords – Industrial Control Systems, Advanced Persistent Threat

Introduction

ICS are used in automatic distribution of water, electricity, natural gas and they are also used in industrial processes like food, beverage and pharmaceutical production. In addition they are used in many mining operations. ICS were not normally secured like other information technology systems because they were supposedly safe from attacks since they were not connected to other IT networks and the internet. (National Institute of Standards and Technology, 2011). Eventually ICS were connected to their corporate networks which are linked to internet and thus also became vulnerable to the network attacks that are prevalent in most IT networks. As a result standards and frameworks were designed to secure ICS from these threats. Whilst utilities and processing industries are still trying to effectively secure their operations from network attacks and bringing them up to par with corporate networks a new kind of threat to ICS called Advanced Persistent Threats (APT) was unleashed.

APPENDIX E: PAPER 4

Initial Investigation of Industrial Control System (ICS) Security Using Artificial Immune System (AIS)

Mercy Bere
Computer Science. Polytechnic of Namibia
Windhoek, Namibia
mbere@polytechnic.edu.na

Hippolyte Muyingi
Computer Science. Polytechnic of Namibia
Windhoek, Namibia
hmuyingi@potechnic.edu.na

***Abstract*—Industrial Control Systems (ICS) which among others are comprised of Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS) are used to control industrial processes. ICS have now been connected to other Information Technology (IT) systems and have as a result become vulnerable to Advanced Persistent Threats (APT). APTs are targeted attacks that use zero-day attacks to attack systems. Current ICS security mechanisms fail to deter APTs from infiltrating ICS. An analysis of possible solutions to deter APTs was done. This paper proposes the use of Artificial Immune Systems to secure ICS from APTs.**

Keywords—industrial control system; advanced persistent threat; artificial immune system; security systems

I. INTRODUCTION

Industrial Control System (ICS) is a generic term for various control systems. ICS control systems include Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS), Process control Systems (PCS), Programmable Logic Controllers (PLC) and Smart grid. SCADA systems are control systems that are used to control processes geographically spaced from each other. PLCs manage the state of input and output devices in both

The researchers believe and expect that after securing an ICS network following whichever method that a high degree of security is attained and it should be difficult for any attack to compromise ICS. This high level of security is however easily circumvented by Advanced Persistent Threats (APT) which, manage to gain entry and manipulate ICS. To solve the problem of APT attacking ICS we propose to design an ICS security model which is inspired by the immune system.

The mechanisms that defend the body from different microorganisms are result of combination of multiple physical, chemical and cellular components called the immune system [4]. Since the immune system is responsible for detecting and protecting the body from harmful microorganism it is likened to ICS security systems which; should be capable of detecting and protecting ICS components from harmful intrusions like APT. As such, it is proposed to design an ICS security model that emulates how the immune system functions to a new bio-immunology inspired ICS security model.

The next section will describe briefly APTs attacking ICS. The next sections (III and IV) will discuss ICS security and its shortfalls. Section (V) will describe current ICS security research. Following that will be sections (VI and VII) on bio-

APPENDIX F: PAPER 5

A Survey of APT Defence Techniques

Mercy Chitauro, Hippolyte Muyingi, Samuel John, Shadreck Chitauro
Namibia University of Science and Technology, Windhoek, Namibia

mchitauro@nust.na
hmuyingi@nust.na
sjohn@nust.na
schitauro@nust.na

Abstract: Since the discovery of Stuxnet in 2010, there have been a plethora of Advanced Persistent Threats (APT) that have been discovered in regular IT networks and in critical infrastructure such as Industrial Control Systems (ICS). ICS is a general term for different control systems like Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS), Process Control Systems (PCS), and Smart grid. ICSs are used in mining industries, transportation systems, and for the distribution of water, natural gas, oil, electricity, and communications, in specialised facilities such as nuclear plants and for automating many other facilities. In a quest to find tangible solutions to the APT problem in information technology systems, many solutions have been designed to detect and protect against, as well as recover from APT. This paper endeavoured to survey the different techniques that have been designed to solve APT problems and their levels of success. This paper therefore discusses APT defence techniques. It is noted that many APTs use social engineering techniques to gain entry into systems; however, technical solutions are being developed to try and correct human errors that enable APTs to infiltrate ICS. Technical solutions include tweaking existing security controls, anomaly detection techniques and defence-in-depth techniques. The researchers believe that the defence-in-depth approach is the future of security and thus, suggest further improvements in defence-in-depth approaches by emulating the immune system which uses a layered defence mechanism to protect the human body from pathogens. Since the main research focused on APTs that are attacking ICS, a control system was setup to find the level of effectiveness of emulating immune system properties. This paper gives some preliminary results on how ICS which exhibit immune system properties perform better than those that are not.

Keywords: advanced persistent threat, security, immune system, defence-in-depth, industrial control system

1. Introduction

The year 2010 saw the discovery of Stuxnet, a deadly malware that was capable of attacking the Iranian Natanz Nuclear Enrichment Facility by changing the frequency settings in a cycle so that centrifuges would spin out of control. Since its discovery, many similar malwares known as Advanced Persistent Threats (APT) have been discovered. Figure 1 and 2 show some of the APTs that have been discovered and how long it took to discover them as detailed by Targeted cyberattacks logbook, (n.d.). Appendix A shows the data derived from ("Targeted cyberattacks logbook," n.d.).

APPENDIX G: PAPER 6

A Bio-Immunology Inspired Industrial Control System Security Model

Mercy Chitauro[1], Hippolyte Muyingi[1], Samuel John[1], Shadreck Chitauro[1]
[1] Namibia University of Science and Technology, Windhoek, Namibia

{mchitauro, hmuyingi, sjohn, schitauro}@nust.na

Abstract. Industrial Control System (ICS) security is inadequate to protect ICS from Advanced Persistent Threats (APT). APTs attack ICS in such a way that they are detected after a long time in the system. This paper proposes the use of the biological immune system as a foundation for developing ICS security architecture because the biological immune system is renowned for defending the body from pathogens. The paper compares how the Biological Immune System (BIS) defends the body from pathogens and how ICS are secured from invasion by any attack. By considering the similarities and differences between ICS security and the BIS operation and taking into consideration current research on ICS security a bio-immunology inspired security model to defend ICS was designed. The proposed model was designed using design science research and initial results are presented in this paper.

Keywords: Industrial Control System, Security, Biological Immune System, Advanced Persistent Threats.

1 Introduction

Industrial Control Systems (ICS) is a generic term for systems that manage the automation of industry processes. ICS are vulnerable to network attacks and thus, robust mechanisms for securing ICS; ICS security standards and frameworks were drafted are used as general guidelines on the best way to secure ICS [1]. ICS security and frameworks guidelines provide a basis for securing ICS from any computing related threats.

Although, the guidelines mentioned in ICS standards and frameworks are good recommendations for securing ICS, their implementation still keeps ICS vulnerable to

APPENDIX F: LANGUAGE EDITOR'S LETTER

ACET Consultancy
Anenyasha Communication, Editing and Training
Box 50453 Bachbrecht, Windhoek, Namibia
Cell: +264814218613
Email: mlambons@yahoo.co.uk / nelsonmlambo@icloud.com

30 November 2019

To whom it may concern

LANGUAGE EDITING – MERCY CHITAURO

This letter serves to confirm that a Doctor of Philosophy in Computer Science at the Namibia University of Science and Technology entitled ***A Bio-Immunology Inspired Security Model to Defend Industrial Control Systems from Advanced Persistent Threats*** by Mercy Chitauro was submitted to me for language editing.

The thesis was professionally edited and track changes and suggestions were made in the document. The research content or the author's intentions were not altered during the editing process and the author has the authority to accept or reject my suggestions.

Yours faithfully

Mlambo

DR NELSON MLAMBO
PhD in English
M.A. in Intercultural Communication
M.A. in English
B. A. Special Honours in English – First class
B. A. English & Linguistics