BEHAVIOURAL OBSERVATION FOR CRITICAL INFRASTRUCTURE SECURITY SUPPORT

William Hurst BSc(Hons), MSc

A thesis submitted in partial fulfilment of the
requirements of Liverpool John Moores University
for the degree of Doctor of Philosophy

July 2014

To my lovely wife Anna

and

to my Mum and Dad

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

I would like to start by thanking my amazing supervisory team, Professor Madjid Merabti and Dr Paul Fergus, who provided me with unparalleled guidance throughout the course of my PhD research. Professor Merabti I would like to thank you for your exceptional supervision, your time, your encouragement, and for sharing your knowledge with me as I progressed in my research. Dr Fergus I would like to also thank you for your exceptional supervision, encouragement, patience and for also sharing your knowledge with me over the last three years. You both have my immense gratitude.

I would also like to thank my wife Anna for her support, encouragement and patience throughout the completion of my PhD. I would like to thank my parents for inspiring me to progress with my education and encouraging me as I did.

I would also like to thank my colleagues and friends Chris, Nathan, Laura, Mike, Mohssen, Andrew, Aine, Ibrahim, Nut, Paul and also my excellent office mate Chelsea, for their friendship and advice throughout the last three years.

Finally, I would like to thank the admin staff, Lucy, Tricia and Carol for all the hard work they do and all the administration help they have given me during my time at Liverpool John Moores University.

ABSTRACT

Critical infrastructures include sectors such as energy resources, finance, food and water distribution, health, manufacturing and government services. In recent years, critical infrastructures have become increasingly dependent on ICT; more interconnected and are often, as a result, linked to the Internet. Consequently, this makes these systems more vulnerable and increases the threat of cyber-attack. In addition, the growing use of wireless networks means that infrastructures can be more susceptible to a direct digital attack than ever before.

Traditionally, protecting against environmental threats was the main focus of critical infrastructure preservation. Now, however, with the emergence of cyber-attacks, the focus has changed and infrastructures are facing a different danger with potentially debilitating consequences. Current security techniques are struggling to keep up to date with the sheer volume of innovative and emerging attacks; therefore, considering fresh and adaptive solutions to existing computer security approaches is crucial.

The research presented in this thesis, details the use of behavioural observation for critical infrastructure security support. Our observer system monitors an infrastructure’s behaviour and detects abnormalities, which are the result of a cyber-attack taking place. By observing subtle changes in system behaviours, an additional level of support for critical infrastructure security is provided through a plug-in device, which operates autonomously and has no negative impact on data flow.

Behaviour is evaluated using mathematical classifications to assess the data and detect changes. The subsequent results achieved during the data classification process were high and successful. Our observer approach was able to accurately classify 98.138 % of the normal and abnormal system behaviours produced by a simulation of a critical infrastructure, using nine data classifiers.

INDEX OF TERMS

Critical Infrastructure, Behavioural Observation, Cyber-Attack, Security, Data Analysis, Data Classification, Cascading Failure, Interconnectivity, Intrusion Detection System, Unified Threat Management System, Security, Control System, Cyber Security, Defence in Depth, Layered Architecture, Linear Discriminant Classifier, Quadratic Discriminant Classifier, Uncorrelated Normal Density based Classifier, Polynomial Classifier, Decision Tree, Parzen Classifier, k-Nearest Neighbour, Support Vector Classifier, Naïve Bayes Classifier

GLOSSARY

- Alert: The sounding of an alarm as a result of abnormal system activity or a detected cyber-threat.

- Advanced Persistent Threats (APT): Cyber-attacks which have increased dramatically in sophistication and are able to infiltrate critical infrastructures in spite of the cyber defences in place are referred to as APT threats.

- Behavioural Observation: The processing of gathered data to assess the state of a situation or a system.

- Control System: A control system is real-time based system regulator, which has a critical response time, sequential tasks, important security issues and has a continuous operation requirement.

- Critical Infrastructure (CI): Critical Infrastructures are controlled by networked computers and can be defined as sectors that would have a debilitating impact on national security if destroyed. Certain infrastructures, in particular national ones, are extremely vital and incapacitating them would result in devastating impact on defence, economics, communication, government systems and society as a whole.

- Critical Infrastructure Protection (CIP): Critical Infrastructure protection refers to the preparedness to an attack on a critical infrastructure and the response taken in order to protect the infrastructure.

- Cyber-Attack: A digital attack on a system reliant on information and communication technology (ICT) networks to function.

- Cyber Security: The measures taken to protect against cyber-attacks using digital safety standards.

- Defence in Depth (DiD): Different technology is used on each layer of the infrastructure to ensure that if an attacker penetrates one layer they are not automatically able to access the next one. This is known as defence in depth.

- Decision Tree: Decision Tree is a classifier which uses decision rules (referred to as branches) to divide data into classes (represented by leaves) based on criteria for splits.

- Distributed Control System (DCS): DCS is used world-wide and consists of a number of controllers connected together through use of networks. In other words, the system has no central controller but is operated by various control components working together to decide the required action.

- Distributed Denial of Service (DDoS): A DDoS or distributed denial of service attack refers to an attack that makes routers and intermediate links deal with enormous volumes of network traffic.

- Distributed Network Protocol 3.0 (DNP3): DNP3 is a protocol that provides interoperability between equipment from different manufacturers. It also supports multiple-slave, peer-to-peer and multiple-master communications.

- Graphical User Interface (GUI): A GUI is the way a human can interface with a system through use of an operating system.

- Infrastructure Failure Interdependencies (IFI): Critical infrastructures can supply services cross boarders and often multiple countries consider the same infrastructure as critical. IFIs are potential cascading failures, which could occur as a result of cross-border interconnectivity. This impacts large sectors resulting in devastating consequences.

- Intrusion Detection System (IDS): Intrusion Detection Systems provide a sense of security for computers and network data by identifying, in real-time, misuse or unauthorised use, whilst allowing the system to continue functioning as normal. IDSs typically use statistical anomaly and rule-based detection to detect intrusion attempts and act accordingly.

- Layered Architecture: Critical infrastructures are constructed in layers, which include the following: a User Interface layer, a Management System, a Control layer, a Network layer, and a Hardware layer.

- Linear Discriminant Classifier (LDC): LDC is a mathematical classifier, which works by sorting or dividing data into groups based on characteristics in order to create a classification. It performs an ordered transformation of unknown quantities, using a linear approach.

- k-Nearest Neighbour (k-NNC): k-NNC is a mathematical classifier which functions by grouping data based on the 'k-closest' values from the training set. In other words, it groups data based on dominant coefficients from the dataset, referred to as the 'k' values.

- Modicon Communication Bus (Modbus): A protocol used by PLC devices to communicate. It is an application layer messaging protocol, which provides communication between different types of buses or networks in an infrastructure.

- Man In the Middle Attack (MITM): A man in the middle attack is where false commands or system instructions and false responses are maliciously inserted into the system.

- Master Terminal Unit (MTU): An MTU acquires data from and sends instructions to components. In addition, it is equipped with a Human Machine Interface; uses databases for storing past information and is linked to workstations for engineers and business information systems for industrial applications.

- Naïve Bayes Classifier (NAIVEBC): NAIVEBC is a mathematical classifier which operates by applying Bayes' theorem to a set of data with independent suppositions, to sort variables into groups based on characteristics.

- Parzen Classifier (ParzenC): ParzenC is a mathematical classifier which functions by including aspects of the training data when the classifier is built up. It is a non-linear classifier

- Polynomial Classifier (PolyC): PolyC is a mathematical classifier which sorts data by evaluating the weighting, using a linear combination of features and considering the variables of the objects.

- Programmable Logic Controller (PLC): A programmable controller is used for automation, for example in manufacturing and production. A PLC is a physical digital unit which controls and automates components such as valves, pumps and sensors.

- Protocol: A protocol is a behaviour or set of guidelines that is adopted by a network to use as standards for their data communication. It defines physical media and communication procedures.

- Quadratic Discriminant Classifier (QDC): QDC is a mathematical classifier which works by sorting or dividing data into groups based on characteristics in a multi-dimensional approach.

- Risk: The danger of damage as a result of an activity.

- Remote Terminal Unit (RTU): RTU's are used to gather information, which is then passed on to the MTU.

- Supervisory Control & Data Acquisition System (SCADA): An industrial infrastructure control system software, commonly used in critical infrastructures for the automation of services such as water distribution, oil pipelines, transport systems and electrical power distribution.

- Simulation Environment: An emulated system using simulation software.

- Support Vector Classifier (SVC): SVC is a mathematical classifier which functions by predicting two possible outputs from a given training feature.

- Threats: The risk of impending danger of harm from cyber-attacks or natural phenomenon.

- Uncorrelated Normal Density Based Classifier (UDC): UDC works in a similar way to the QDC classifier but computation of a quadratic classifier, between the classes in the dataset, is done by assuming normal densities with uncorrelated features.

- Unified Threat Management System (UTM): Unified threat management systems use firewalls, pattern recognition, IDS and embedded analysis middleware. They are widely used to enhance network security in critical infrastructures.

- Vulnerabilities: Weaknesses in the system, which attackers look to exploit, are referred to as vulnerabilities.

- Wireless Sensor Network (WSN): A wireless sensor network consists of individual independent sensors that co-operate to monitor real world physical conditions. Wireless sensor networks have many uses including monitoring environments such as temperature and weather patterns, as well as industrial and military uses.

PUBLICATIONS RESULTING FROM THIS THESIS

JOURNAL PAPERS

1. Hurst, W., Merabti, M., Iram, S & Fergus, P. *Protecting Critical Infrastructures through Behavioural Observation*. Inderscience International Journal of Critical Infrastructures. 2013 (In Press)

2. Hurst, W., Merabti, M. & Fergus, P. *Behavioural Classification for Enhancing Critical Infrastructure Security*. Inderscience International Journal of Critical Infrastructures. 2013 (Accepted with minor changes).

3. Pla Beltran, L., Merabti, M & Hurst, W. (2013). *Using Behavioural Observation and Game Technology to Support Critical Infrastructure Security*, Inderscience International Journal of System of Systems, 2013 (Accepted with minor changes).

CONFERENCE PAPERS

4. Merabti, M., Kennedy, M., & Hurst, W. *Critical Infrastructure Protection: A 21st Century Challenge*. Proceedings of the First IEEE International Conference on Communications and Information Technology (ICCIT), pp. 1-6, 2011

5. Hurst, W., Merabti, M & Fergus, P. *Operational Support for Critical Infrastructure Security*. Proceedings of the Ninth IEEE International Conference on Embedded Software and Systems (ICESS), 2012

6. Hurst, W., Merabti, M & Fergus, P. *Managing Critical Infrastructures through Behavioural Observation*. Proceedings of the Third IEEE International Conference on Networked Embedded Systems for Every Application (NESEA), 2012.

7. Hurst, W., Merabti, M & Fergus, P. *Behavioural Observation for Critical Infrastructure Security Support*. Proceedings of the Seventh IEEE European Modelling Symposium, EMS201. November 2013.

8. MacDermott, A., Hurst, W., Shi, Q & Merabti, M. *Simulating Critical Infrastructure Cascading Failure*. The Sixteenth IEEE International Conference on Modelling and Simulation. March 2014.

9. Hurst, W., Merabti, M & Fergus, P. (2014). *Critical Infrastructure Security: A Survey*. Proceedings of the Eighth Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection. March 2014.

10. Hurst, W., Merabti, M & Fergus, P. *Big Data Analysis Techniques for Cyber-Threat Detection in Critical Infrastructures*. Proceedings of the Eighth IEEE International Workshop on Telecommunication Networking, Applications and Systems, May 2014. (accepted).

11. Hurst, W., Merabti, M & Fergus, P. *Towards a Framework for Operational Support in Critical Infrastructures*. Proceedings of the Twelfth Annual Post Graduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting, June 2011

12. Hurst, W., Merabti, M & Fergus, P. B*ehavioural Observation for Critical Infrastructure Support*. Proceedings of the Thirteenth Annual Post Graduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting, 2012

13. Hurst, W., Merabti, M & Fergus, P. *Behavioural Analysis for Supporting Critical Infrastructure Security*. Proceedings of the Fourteenth Annual Post Graduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting, June 2013

POSTERS

14. Hurst, W., Merabti, M & Fergus, P. (2011) Critical Infrastructures, Science and Technology for Security: Harnessing Innovation from Academia (RUSI 2011)

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1.1 FOREWORD

As technology has rapidly changed over recent decades, the functioning of society has evolved to depend on a number of key infrastructures [1]. These key infrastructures, referred to as critical infrastructures, work together to provide a continuous flow of goods or services [2], which range from food and water distribution, power supply, military defence and transport, to health and government services, to name but a few [3], [4]. Failure in one directly impacts the other [5].

Furthermore, beyond these traditional critical infrastructures, non-traditional ones have also emerged, which include telephone systems, banking, electrical energy distribution and manufacturing [6]. Having a well-established critical infrastructure network is often considered a sign of civilized life, and nations are usually judged by the strength of their critical infrastructure network and the services they can provide to their inhabitants [7]. However, dependence on these infrastructures is one of society's greatest weaknesses, due to the fact that a disruption to a single critical infrastructure can result in life-threatening and general debilitating consequences on the population, economy and government [8], [9]. As dependence on these critical infrastructures increases it is important that the ability to avoid disasters is enhanced [10]. Consequently, the research presented in this thesis offers a way of supporting critical infrastructure security by building on the defence in depth.

In this chapter critical infrastructures are introduced, along with a discussion on the motivation behind the research in this thesis. The contributions to knowledge are also presented, in addition to the aims and objectives of the work; the methodology taken and the thesis structure.

1.2 Critical Infrastructures

Critical infrastructures consist of a network of interdependent man-made systems that work together to provide a continuous flow of goods or services that are essential for economic development and social well-being [2]. One of the key defining factors of a critical infrastructure is society's dependence on the services provided by the infrastructure and the loss that would be encountered if the infrastructure was shut down through a successful physical or cyber-attack.

Critical infrastructures are key service providers and are greatly relied upon by governments and the general population. All critical infrastructure areas are now becoming heavy Information and Communication Technology (ICT) users, with automation playing a key role in production [11]. ICT has also begun to increase in areas such as; agriculture, food and water, where control systems and the use of sensor equipment is helping to facilitate production and become more adaptive to the growing demands being placed on them [12], [13]. The use of robotics in farming to assist with labour-intensive work, is helping to revolutionise the way in which crops are grown and maintained [14], [15]. Clearly, the use of ICT is becoming more pervasive in all areas of critical infrastructure.

With increased ICT usage, infrastructure interdependencies have grown and, along with them, the risk that a disruption or a critical failure to one infrastructure can directly lead to disruptions in others [16], [17]. Critical infrastructures are heavily interconnected, meaning any damaging impact would result in devastating consequences.

The increase in digitisation and interconnectivity has also meant that such failures could be deliberately implemented from a remote location by a cyber-attack, which has the potential to bring operations to a halt with devastating consequences.

1.3 Motivation

When critical infrastructures first started being built the main focus was how to develop an infrastructure that would be resilient to the threat of changing environmental conditions [18] and potential natural disasters. One only has to look to the recent example of the devastating earthquakes and tsunami, which hit Japan in March 2011 to see the scale of destruction natural phenomenon can cause and why they are planned for [19].

This natural disaster threat is further reflected in numerous other examples including an impact on a European power grid in November 2006 which, originating in Germany, resulting in 10 million people being out of power in Germany, France, Austria, Belgium and Spain [20]. The incident in the Torness nuclear power station in Scotland in 2011, for example, which experienced a shut down due to a large bloom of jellyfish, blocking the plant’s water intake system, further demonstrates the unpredictable side of nature, which critical infrastructures have to cope with. All of these examples demonstrate the potential damage to critical infrastructures and reflect the need to remain at least one step ahead of potential threats, whatever their source [21]. However, failures are not always the result of changing environmental conditions and can often be the result of human error [22] and cyber-attacks.

Technology in critical infrastructures has evolved [23] and reliance on digital industrial controls and wireless networking for providing fast and effective communication has increased, consequently, the main focus for critical infrastructure protection has been diverted from how critical infrastructures are kept environmentally safe to how best to keep them digitally secure [24]. This is because these key service providers present a tempting target for terrorists, military strikes, and hackers wanting to find a way to cause disruption, steal information or incapacitate a country remotely. The ability to attack a critical infrastructure from a distant location provides a new and emerging way of conducting warfare with the potential to cause more damage than a physical attack could. With this ability, incapacitating a country or causing harm to the population can be done without the victim knowing where the attack is coming from, making defence or retaliation difficult.

In addition to the threat of failure to an individual critical infrastructure, there is a risk that one failure can escalate rapidly [22]. This is as a direct result of the close interconnectivity of the infrastructures with each other and the many facets of life which depend on them [25]. As Schlapfer *et al.*, discuss, certain infrastructures are highly interconnected and, in result, are linked through busy communication channels [26]. For that reason, it is often the case that breakdowns result in cascading failures due to the close links created for the facilitation of the services provided [27], [28].

Managing critical infrastructures under the growing cyber-threat is becoming a matter of international urgency. The volume and frequency of cyber-related incidents is on the rise yearly, and the level of sophistication is increasing.

1.3.1 GROWING CYBER-THREAT

The interconnectivity of critical infrastructures and the risk of cascading breakdown is a growing concern when factoring in the cyber-threat. The topic has, in result, become a key issue for debate in many governments and in growing frequency by chief executive officers (CEO) of global corporations [29], [30], as well as, being at the forefront of many news articles. In the early months of 2013, the USA defence secretary Leon Panetta highlighted the risk cyber-attacks could have on a nation, comparing the potential impact of a successful attack to that of the terrorist attacks of 9/11 [31]. The United Kingdom, particularly in 2011, has also been very vocal on the large volume of cyber-attacks that occur daily, which are aimed at government services and global corporations, with the Secretary of State for Foreign Affairs, William Hague, highlighting the volume and variety of cyber-threats being encountered. Whilst many of the attempted attacks remain small, for example, malicious emails [32], [33] containing Trojan horses [34], the sheer volume of the attacks occurring, regularly poses a cause for concern.

As emailing has become indispensable to the operation of businesses, a threat of malicious emails has also grown exponentially [32], [33]. This threat is particularly difficult to counter as their contents may seem genuine making them challenging to identify. Often malicious emails either contain links to external unsafe websites or contain attachments that, once opened, could infect the user’s computer system. In the last few months of 2011 for example, several attempted attacks on the British Government were conducted, where emails were sent containing viruses from fake sources disguised to look like they had been sent from the White House and from other internal staff members.

1.3.2 COST OF FAILURE

Critical infrastructures are faced with the unexpected when it comes to the levels of cyber-threats that exist. As previously mentioned the cost of critical infrastructure failure due to environmental disasters is high and it is conceivable that the consequences of digital failure could have a similar devastating impact.

Attackers are starting to find increasingly ingenious ways of causing disruptions in infrastructures [35]. Physical parameters, such as temperatures, pressure, speed and flow rate factors are all controlled digitally, offering tempting targets. A weakness that can result in a physical failure must be quickly identified and addressed prior to there being grave consequences.

Examples of failures which had real world physical impact due to digital failure include the Galaxy 4 satellite failure, albeit over a decade ago in 1998, where an outage of nearly ninety per cent of all pagers worldwide impacted several banking and financial services as well as disrupting communications with doctors and emergency workers [5].

Electrical failures caused by natural phenomenon are generally fixed within short periods of time yet in this short period of time there is usually impact on the economy. The heavy snow fall in the UK in the December of 2010 is said to have resulted in lost revenue for shops, business and airports. Given the impact a relatively small failure, caused by natural occurrences had on the economy, it is fair to say that the result of a long-term failure as a result of an attack on a power-related critical infrastructure would be devastating.

The consequences of digital failure are diverse, a further example in New Zealand in 1998 when a power outage in Auckland Central Business District resulted in 50,000 inner-city workers and 6,000 residents being without power for five weeks, demonstrates this. The power outage caused substantial disruption to businesses and the general population [36] and had a severe impact on the economy due to the long period of time the power was off for. Five weeks without power has the potential to ruin businesses and cause a lasting effect on the economy, not to mention affecting the provision of the services offered by other infrastructures.

In addition to the above accidental digital failures, which occurred, in the last decade in particular, there have been several successful high profile cyber-attacks that have caused disruption and had a lasting effect on their target. Some of these cyber-attacks are discussed in more detail in chapter 3 of this thesis.

High profile attacks have tended to be well documented in the news, and none more so than the Stuxnet virus [37]. Designed to target Siemens' industrial software and equipment, this is a good example of a cyber-attack where a Nuclear power plant in Iran was shut down, damaging Iran's progress with their nuclear program. The reports on the Stuxnet virus have been well documented and helped fuel the fear of the level of sophistication cyber-attacks can have [37]. The worrying factor behind the success of this security breach is that, despite being unique in its sophistication, it is not the only example of such an attack that has taken place. One of the benefits of using a cyber-attack, especially a sophisticated one like Stuxnet, is that it allows an attacker to have deniability, making it difficult for the victim to retaliate.

One other example of a successful cyber-attack is the Slammer worm [38]. In Ohio USA in 2003, this worm breached a private computer network in Ohio's Nuclear power plant. Upon entering the network it disabled a safety monitoring system for over five hours. The plant was already offline and unused but the presence of a worm, that can disable a safety monitoring system, reflects the current dangers and importance of cyber security. It is clear that, as threats grow, the risk of physical consequences caused by digital failure are worrying.

One further example seen in recent months is Flame [39]. Similar to Stuxnet, Flame has a high level of sophistication and was used to collect data from computers across the Middle East. Without being able to accurately identify and confirm where such an attack originated, there is a worry that a sophisticated attack of this magnitude was created by a national state.

1.3.3 MOTIVATION SUMMARY

The research in this thesis is motivated by the real risk posed by a growing cyber-threat which critical infrastructures must now contend with. During their lifetime, critical infrastructures can expect to face a variety of threats from natural phenomenon. However, it is the digital threat, which is now the main focus of critical infrastructure protection.

Cyber-attacks are increasing at an alarming rate. The need to remain one step ahead of the attacker is becoming more and more important. The consequences of failure can produce unexpected results and must be planned for in order to prevent disasters escalating. The cost of physical consequences reflects the ever-growing need for effective critical infrastructure protection for the future safeguarding of the services, which are heavily relied upon by the population.

Despite the need to develop effective methods for protecting critical infrastructures, the task is a difficult one. The protection of these important infrastructure systems is becoming exceedingly complex due to the sheer size involved, and the technologies used.

1.4 Aims and Objectives

The motivation behind this thesis, is to detail the development of an approach called ‘Behavioural Observation for Critical Infrastructure Security Support’ (BOCISS); that will support security and the secure running of an infrastructure during real-time operation using behavioural observation and data classification techniques.

Modern banks currently monitor credit card activity and develop a patterns of acceptable behaviour for the user of the card [40]. The model for correct behaviour is based on demographic and economic information combined with a database of historical behaviour, thus combing a variety of information to devise a pattern of expected activity [41]. The concept for our idea is the same. If a pattern of correct behaviour can be determined for a critical infrastructure, then threats and anomalies can be quickly identified through real-time monitoring of the system and comparing with models of expected performance. As BOCISS has the role of adding to critical infrastructure security’s defence in depth, the following project aims are considered:

- The recognition of unusual activity: If patterns of behaviour are detected [42] based on the functioning of an infrastructure, then any malicious or out of the ordinary activity taking place can be quickly identified and investigated [43]. Changes in behaviour that would be detected would ideally include:
    - Unauthorised Changes in System Behaviour.
    - Changes in Data Patterns.
    - Detecting Unexpected System Behaviours.
- To draw from multiple sources of information: Using physical data collected from multiple components in a critical infrastructure, patterns of behaviour are established and the operator is presented with an informed overview of the operation of the system. The aim of this is to provide:
    - Real-time analysis: The creation of a more effective critical infrastructure security environment using the data collected from a huge variety of components, such as pressure gauges and nodes, to provide real-time analysis and identify threats.
    - Model correct behaviour: The development of a model of expected system behaviour, taking into account data collected from physical processes [44] and any other sources of information that would be beneficial.

    - Proactive security: The provision of a support system that is continually looking to identify patterns. The recognition of unusual activity is the key to the improvement of critical infrastructure security. No matter what type of attack occurs, if the security is looking only at the continued acceptable operation of the system, then attacks can be identified by recognising subtle behavioural pattern changes and events that are out of the ordinary.

These project aims are achieved through the completion of multiple research objectives, which include the following:

- Research into related work surrounding critical infrastructure protection, cyber-security, behavioural observation, simulation and data analysis.

- The evaluation of current methods for improving critical infrastructure security, in order to conduct an analysis of how BOCISS compares to other existing approaches being developed to support critical infrastructure security.

- The investigation of how behaviour can be modelled by testing methods for gathering data in a way that can be processed and evaluated. In addition, the assessment of what sources would be ideal for data collection, and how physical data can be collected.

- Research into data classification and the selection of suitable data classification techniques for modelling behaviour and identifying changes in behaviour patterns.

- Research into how an operator will communicate with BOCISS. The system must communicate with an operator using user interface and have effective data management in order to store the data in a way that allows a model of correct behaviour to be formed and compared with, using a database of known behavioural patterns.

- A case study into the development of a simulation to construct realistic critical infrastructure data, which can be used for the development of BOCISS and for testing its effectiveness in identifying cyber-threats.

- The evaluation of the results, through suitable approaches, in order to discover the effectiveness of the design based on testing and case studies.

- The publication of results obtained during the research.

1.5 Approach

The solution focuses on developing a system that operates with a much broader view of the critical infrastructure to provide a coordinated response and alerts through behavioural observation services. The aim of the research within these areas is to have an impact on national security for critical infrastructures such as power plants, transport systems and industrial production to name a few, and improve on the security each currently uses.

The aim will be to carry out various functions such as Data Processing, Observing and Diagnosis as well as to store a Database of patterns of information about the system. The objectives are to provide an alternative method of safeguarding systems that is more resilient and builds on the security that is already currently in place.

The human brain makes decisions through drawing from multiple sources of information, such as sensory organs, and in doing so is able to avoid threats and devise effective conclusions [45]. The storing and retrieving of information learnt provides a way of keeping the body safe from harm [46]. The solution being developed will create a more effective critical infrastructure security environment through monitoring a huge variety of components such as pressure gauges, nodes, etc.

Thus in the same way our brain makes informed decisions from drawing from multiple sources of information, BOCISS provides enhanced security by identifying threats in a more informed way. The approach for the development of BOCISS requires the involvement of various key aspects, which include:

- The development of a realistic critical infrastructure simulation.

- Data construction through simulation.

- The use of an observer system for extracting and collecting data.

- The use of data classification techniques to analyse the data and identify threat behaviour.

Schweitzer et al., present a theoretical approach to improving critical infrastructure protection. Referring to a fictitious attack on a critical infrastructure, they discuss how an attack would leave behind fingerprints, which can be used to recognise when systems have been attacked or compromised [47]. They present the use of existing tools, which are used to recognise when such fingerprints have been left behind, and propose a theoretical approach to improving security.

They use a fictitious incident in order to explain how an attack would be detected. The incident they refer to involves an outage on a modern control system architecture. Following the incident, several components are checked to understand why a fault had taken place. All these checks had to be done individually and manually in order to try and work out what was taking place.

Their research reflects the need for a supportive system, which constantly provides operators with information. One of the aims of BOCISS is to provide the operator with an overall image of the events taking place in the system, which is independent of the control system, and the information displayed within. The result is, the provision of separate views of the system functioning provided to the operator.

1.6 Novel Contributions

This research offers an unconventional approach for supporting critical infrastructures by building on existing security [48]. The main novel contributions of our work are discussed below:

- The observation of physical data makes BOCISS stand out from other approaches to critical infrastructure security, which have a heavy focus on using network data. Using component behaviour data, our observer device can accurately identify threats to the system and security breaches using behavioural observation and big data analysis techniques [48]. This approach is reliant on a list of dependents for providing data and support is offered through intelligent observation and reactive services [49]. The gathering of information from various modules and sources, provides an insight into the bigger picture of the events taking place [50]. In turn, BOCISS is able to identify threats going beyond the ability of current IDSs. The technique proposed differs from UTM devices as it looks to develop a pattern of overall behaviour of the infrastructure. Whereas, UTMs and IDSs tend to have a heavy focus on network activity and overlook other potentially relevant data. BOCISS has no control over the data but uses it for behavioural observation purposes [51], [52].

- This work presents a novel approach to supporting critical infrastructures by identifying malicious activity, using an observer unit and data classification techniques. The use of data classification techniques, which identify when subtle changes in system behaviours have occurred, is a point of novelty in our system design [48]. Our choice of data classification algorithms have not been used in a critical infrastructure or security environment. Using the classifiers to achieve real-time security through pattern detection means that security does not have to remain one-step ahead of new and emerging threats to be effective. Our real-time security approach will be active, continually processing data to identify changes in behaviour, as opposed to existing passive systems which are reliant on being given the data from the network or control systems rather than extracting autonomously [51], [55].

- BOCISS can be applied to multiple critical infrastructures as it goes through a learning or training phase to make it adaptable to the specific infrastructure type rather than being constructed with a single critical infrastructure in mind. Many of the existing solutions against cyber-threats focus on one specific area such as power networks, smart grids or water distribution. Our approach provides a novelty in its generic and adaptive approach for use in multiple critical infrastructure types [54], [56]. The choice of data extracted from the system can be customised by the operator, allowing the system to be adaptive to different environments [50].

1.7 Thesis Structure

The research detailed in this thesis is divided into 8 chapters. An overview for each of the remaining chapters is provided.

Chapter 2 – Background on Critical Infrastructures: This chapter will define what critical infrastructures are, how they function, what weaknesses they tend to have and how they are currently protected against cyber-attack.

Chapter 3 - Cyber-Threat: This chapter will draw on examples of past and existing cyber-threats, digital breakdown, and critical infrastructure failures, which have taken place over the last decade, to justify this research being conducted. The motivation behind our research will be presented along with a discussion on existing cyber-threats and what challenges are faced as a result of their increasing prominence.

Chapter 4 – Related Research: In this chapter, associated research into critical infrastructure protection will be discussed. This chapter will also provide an insight into why simulation is an important factor in the future development on critical infrastructure protection and how behavioural observation is currently implemented in other areas of research.

Chapter 5- Behavioural Observation for Critical Infrastructure Security Support: In this chapter, our system design will be presented. It will entail an outline of the specification; a detailed discussion on the system architecture and an explanation of the system modes of operation.

Chapter 6 –Nuclear Power Plant Case Study: This section will contain the development of a simulation of a nuclear power plant using Siemens Tecnomatix Plant Simulator and the programming language SimTalk. Its use for both normal and abnormal data construction will also be presented. There will also be a focus on methodologies used for the evaluation stage of our research. This chapter will, therefore, contain an account of the pre-processing of the dataset generated by our nuclear power plant simulation in addition to the methodology for classification.

Chapter 7 - Evaluation: The evaluation chapter will involve a detailed analysis of the data classification results. A visual interpretation of the classification process and a justification of the results obtained will also be put forward in this chapter.

Chapter 8 - Conclusion and Future Developments In the final chapter of this thesis, the research will be concluded by discussing the accomplishments of the research. This chapter will, also, highlight how the work can be built on for future research purposes.

CHAPTER 2

CRITICAL INFRASTRUCTURES

2.1 INTRODUCTION

The worldwide growth in the use of ICT has seen a drastic change in the way critical infrastructures operate. The digitisation of service provision and the growth in the use of automation are examples of this. The benefits of using computerised approaches for service provision far outweigh the risks. However, with the increased use of digital systems, it is important to consider the security of critical infrastructures and ensure that effective multilayer security is in place to safeguard against failures which could have a debilitating impact on society as a whole.

In this section, critical infrastructures are discussed in depth. There is a focus on control systems and automation, as well as the security currently in place and why the use of defence in depth is an important issue in the protection against cyber-attacks.

2.2 CRITICAL INFRASTRUCTURE STRUCTURE

As demand grows, the continued provision of services is dependent on effective organisation in critical infrastructures, which is a long process involving multiple levels of design, planning and research due to the large volume of components involved [57]. It is, of course, possible to divide a critical infrastructure into various layers, which are responsible for different provisions of services. This organisational technique can benefit the development of security systems.

2.2.1 CRITICAL INFRASTRUCTURE LAYOUT

The different layers, displayed in Figure 1, include a Business Layer; a Management System or User Interface; a Control layer; a Network layer and a Hardware layer. Firstly, the Business layer (taking the example of an industrial production infrastructure) would be responsible for the intake of new manufacturing orders for production, including orders taken directly from the Internet.

Modern day control systems (as discussed in section 2.4) use open or standard protocols and the Remote Terminal Units (RTU) interpret the protocol commands from the control system on behalf of components such as sensors. RTUs also collect data in the form of analogue signals and converts them into a digital format which is sent back to the control system for interpretation [58].

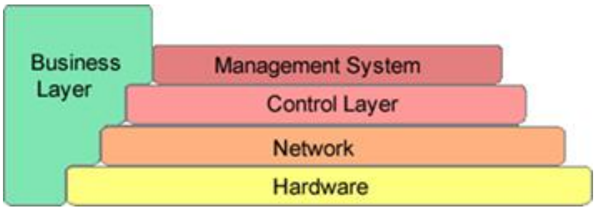


Figure 1 Critical Infrastructure Layers

Next the Management System, also known as the User Interface Layer, allows an operator to interact with the infrastructure in order to open or close valves remotely, monitor alarms, gather information and control switches [59]. This communicates directly with the Control Layer, which consists of a Programmable Logic Controller (PLC) used for automation, for example, in manufacturing and production.

A PLC is digital and uses logic to allow for multiple input and output operations [60]. PLC devices are usually small and compact and are most effectively used in an environment where timing and automation is essential. A PLC conducts a process repeatedly, executing the logic through what is known as a scan time. Much like a critical infrastructure, a PLC can be divided into several layers including: Power, CPU, Input/Output (also known as I/0) and the Rack which holds the components together. PLCs are often programmed in multiple ways. The most common of which include the use of ladder logic [61]; function blocks [62] and high level programming languages [63], [64].

PLCs are extremely popular and this is mostly due to its various advantages over the use of a standard PC. One such advantage is that PLCs are robust and able to operate in difficult environments, as well as being flexible and easy to repair.

The Network Layer covers how all the various components that make up an infrastructure are linked and connected with each other [65]. It has three main functions, which include the Connection Model, Host Addressing and Message Forwarding. The Connection Model is the way in which packets are sent and delivered. Packets are sent to their destination with a packet header that acts as a label for the packet. The Host Addressing involves the system hierarchy and tags the network with a unique address (e.g. IP address). The Message Forwarding is associated with the connection of the various parts of the network though the use of routers, which ensure the packets, can be sent between networks [65].

The Hardware Layer consists of components used to operate the infrastructure. These components include hardware such as nodes, valves and sensors, (as discussed later in the thesis) which work together to allow the system to function. The hardware used is relevant to the type of infrastructure [66].

2.2.2 Critical Infrastructure Layer Interaction

Figure 2 displays a more detailed view of the interaction between the different layers and the infrastructure components.

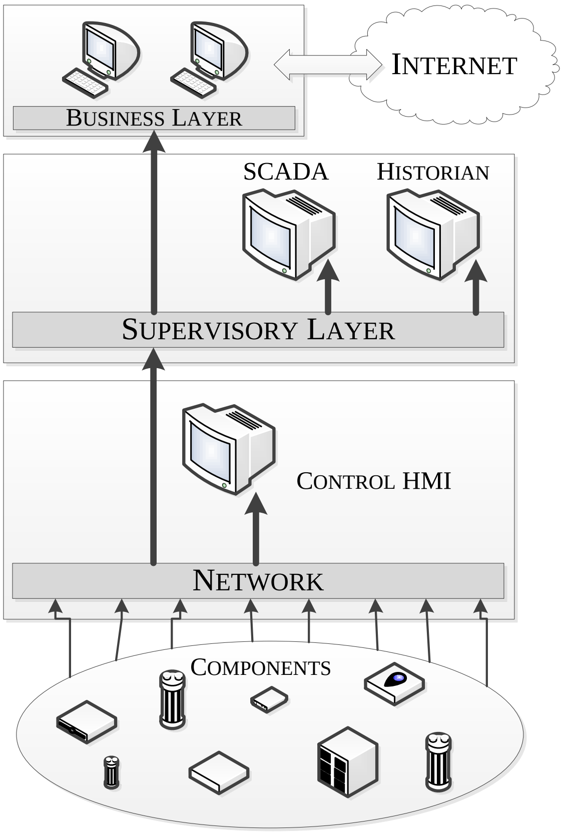


Figure 2 Critical Infrastructure Layout

All components in a critical infrastructure are controlled by a PLC or RTU and connected to the network, which in turn is connected to a control user interface. Above the network, the supervisory layer houses the control system and system historian. The historian stores system data, which is used for analysis [67]. The top tier is the business layer and it is connected to the internet to process orders for the infrastructure to complete.

Due to the complexities in each layer of the infrastructure, there is an emphasis on the development of effective control systems that are able to adapt and manage the sheer volume of data being processed by the infrastructure and their various layers. There are, however, numerous vulnerabilities, which, as threats grow, are starting to increase and put a strain on control systems and security.

2.3 AUTOMATION

Throughout the critical infrastructure layers, automation has become an indispensable part of service provision and has increased exponentially, as demand for digital services and interconnectivity has increased. The reliance on these systems has resulted in ICT playing a key role in the provision of services that critical infrastructures deliver to the general population.

2.3.1 AUTOMATION BENEFITS

The benefits of being able to allow an infrastructure to operate and communicate self-sufficiently include, saving on costs, labour, and time. Outside orders are processed automatically and controlled remotely [68] without the need to pay staff to take orders manually and enter functions. However, it is because of this, critical infrastructures find that they are in some way connected to the Internet [69]–[71].

Automation is a key issue in attracting business. In the USA, for example, many businesses have shifted their production over to China where the use of automation allows for fast and cheap production of goods through automation services. This is an issue currently being addressed by the US government as they attempt to bring manufacturing back to the USA [72].

Having a link with the Internet means that these infrastructures have seen one of their most valuable strengths become one of their greatest weaknesses as the cyber-threat increases [73]. In light of that fact, the motivation for critical infrastructure protection is now focused on cyber security and the devastating effects a man-made attack could have [74]. The potential for destruction caused by a human controlled attack could have more of an impact than a natural disaster would, as the destruction would tend to be orchestrated. With key knowledge of the workings of an infrastructure, a guided attack could be targeted to cause the most damage possible. This is especially the case when considering an attack on a nuclear power plant where the damage could be widespread and catastrophic with the potential for lasting environmental consequences. The meltdown, which occurred at Chernobyl power station, is a clear example of this, where resulting devastation to the surrounding environment means that even after 25 years it is still not possible to return to within 30km of the power station without proper anti-radiation protection.

2.3.2 AUTOMATION ADVANCES

One new area of automation is smart meters. Infrastructures will soon be fitted with smart meters which will allow customers to use services on a prepay tariff [75]. This however, as Anderson et al., discuss, will pose a new cyber-threat as attackers, now have the ability to directly disrupt electricity supplies to civilians [75].

Smart metres are being introduced in USA and Europe. The main aim is to allow users to have more control over the amount of energy they can afford to use and avoid users defaulting on their bills by using more electricity than they can afford to pay for. The key aspect is that they have a remote off-switch, which is controlled by the infrastructure. Anderson et al., point out that this is the cyber equivalent to a nuclear strike: If a way is found to successfully attack and shutdown electricity essentially every electronic device is stopped [75]. As Anderson *et al.*, discuss, the worst-case scenario is that millions of smart meters are installed and controlled by a switch, without a detailed counter attack planning.

2.4 CONTROL SYSTEMS

As automation grows in all areas of critical infrastructures [76], increased pressure is put on control systems to oversee and monitor operations at all times.

The way critical infrastructures function is through the use of networked computers and control systems, which allow operators to control components (such as valves, pressure gauges, switches and nodes) from remote locations without physically needing to be there [77]. The requirement of operators having to travel to distant locations has been replaced by carefully designed user interfaces to allow the operator to interact with the system [59].

2.4.1 CONTROL SYSTEM TYPES

One example of such a control system is SCADA (Supervisory Control and Data Acquisition), which is one of the most commonly used in critical infrastructures and is often constructed through the purchase of off-the-shelf components to a specification suitable to the type of infrastructure being used [78].

Supervisory Control and Data Acquisition (SCADA) systems play a vital role in the digital control and automation of the services provided by critical infrastructures. A central control unit has the job of governing the behaviour of a vast system, ensuring the infrastructure is run smoothly and automated efficiently [79].

In recent months, we have seen how important SCADA systems are to a critical infrastructure where cyber-attacks such as Stuxnet and Flame, as previously mentioned, are being specifically designed to have the goal of incapacitating a SCADA control system and bring a critical infrastructure to a halt by causing disruption.

Another type of control system is a DCS (Distributed Control System) which tends to have no central controller but is operated by various control components working together to decide the required action [80], [81]. SCADA systems, however, are not divided up but rather operate from one sole location. The use of off-the-shelf components does pose some cause for concern as the technology used in infrastructures is readily available for anyone to use, which can make them more vulnerable to attack [78].

A typical modern SCADA system consists of a network of sensors acquiring data, and actuators, which are used to control devices using PLCs. SCADA devices are usually composed of three parts, including the master terminal unit (MTU), the remote terminal units (RTU) and the communication links. The MTU acquires data and sends instructions between various components such as a Human Machine Interface (HMI), databases for storing past information, workstations for engineers and business information systems for industrial applications.

The remote terminal unit (RTU) has the role of interfacing the SCADA system with the hardware components. RTUs are essentially PLC devices that automate the actions ordered by the master terminal unit. The communication links are responsible for proficient communication and usually consist of fibre optics, microwave, telephone lines, pilot cables, radio or satellite [61], [66].

Figure 3, displays a simplified view of a control system where the RTU provides the communication link between various components of the infrastructure and the MTU, which is linked to the graphical user interface.

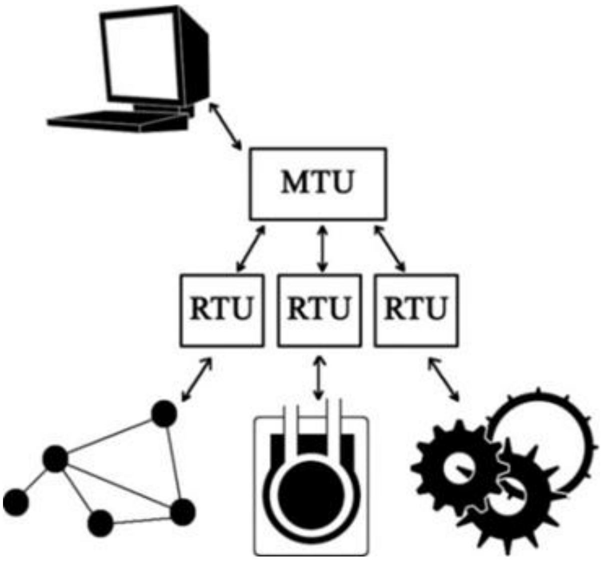


Figure 3 SCADA Overview

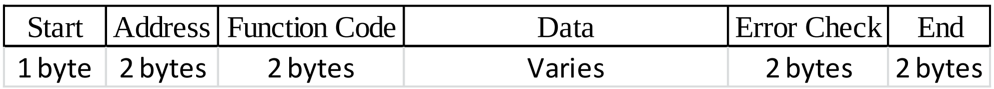
The SCADA system is typically software, which enables the operator to interact with the MTU and observe the on-going activities in the infrastructure [82]. In the following subsection, a discussion is presented on the data, which facilitates the communication process through the network layer.

2.4.2 NETWORK DATA AND PROTOCOLS

Control system data is coded in protocol format to exchange information with components and RTUs. The protocol formats provide automation and send information back to the control user interface to deliver a status of system operations. Communication protocols are designed for real-time operation [83]. Two examples of industrial control network protocols include Modbus (Modicon Communication Bus) and DNP3 (Distributed Network Protocol). Each are commonly used in modern day critical infrastructures are able to match the specific requirements of the system, however they are susceptible to disruption and security breaches [83].

DNP3 is a protocol that provides interoperability between equipment from different manufacturers. It also supports multiple-slave, peer-to-peer and multiple-master communications. Modbus, on the other hand, is an application layer messaging protocol, which provides communication between different types of buses or networks [84]. As Modbus is one of the most common in use, it will be our focus as an example of network data protocol.

Modbus communicates without the need for authentication and is well known for its ease of use [83]. It is used to send information collected by the RTUs back to the control system, in addition to conveying instructions from the control system to components. This is known as a master and slave relationship. Figure 4 displays an example of a Modbus data packet.



Start	Address	Function Code	Data	Error Check	End
1 byte	2 bytes	2 bytes	Varies	2 bytes	2 bytes

Figure 4 Network Data Format

Modbus is deployed on a TCP/IP network. Each component using Modbus has a unique ID address. The address then forms part of the data packet allowing only the component with the right address to receive the information [83]. The data content varies in size but other aspects of the packet consist of one or two bytes.

The variety of digital technologies and the growing use of automation services leaves critical infrastructures with various vulnerabilities and considerable weaknesses.

Interior network weaknesses exist in the form of protocol security concerns. Modbus, in particular, has various weaknesses, which attackers exploit. Because Modbus was designed for isolated systems, security was not taken into consideration. Two such weakness are the lack of authentication and the lack of encryption [83]. Modbus data can be easily extracted from the network and replaced with false commands.

As Modbus travels through the entire network, one other clear weakness is the lack of broadcast suppression. In other words, Modbus has access to all recipients or connected devices and therefore, malware inserted into a Modbus packet would be able to reach multiple targets. As the targets are critical components and have potential control over key mechanisms, consequences of an attack could be direct and life threatening.

The following subsection provides a discussion on the vulnerabilities critical infrastructures have, as well as, a literature review of some of the research being conducted to counter such weaknesses.

2.5 VULNERABILITIES

Critical infrastructure vulnerabilities are weaknesses in the system, which attackers look to exploit. The difference between threats and vulnerabilities is that threats are the people or attackers who are looking to find a way of exploiting the existing weaknesses [85]. As previously mentioned, cascading failure is one particular weakness of critical infrastructure networks. The result of a failure spreading from one infrastructure to another due to the high level of interdependency between the infrastructures can be catastrophic.

2.5.1 CASCADING FAILURE

Critical infrastructures are the supporting mechanisms of modern society and cyber-attacks are increasing at an alarming rate. Critical infrastructure security experts around the globe are now recognising the importance of effective simulation in planning the fight against the growing cyber-threat [86]. The need to remain one-step ahead of the attacker is becoming more and more important.

The consequences of failure can produce unexpected results and must be planned for in order to prevent disasters escalating [87], particularly in light of the potential cascading effect. The close interconnectivity of these vital service providers means that failures impact the provision of other services, affecting multiple systems through a single failure [88].

An example of this is displayed in Figure 5, which shows the impact of a hypothetical power plant fault on telecommunications. The thicker red arrows show the impact of failure caused by the power plant fault on the telecommunications and the cascading effect this produces.

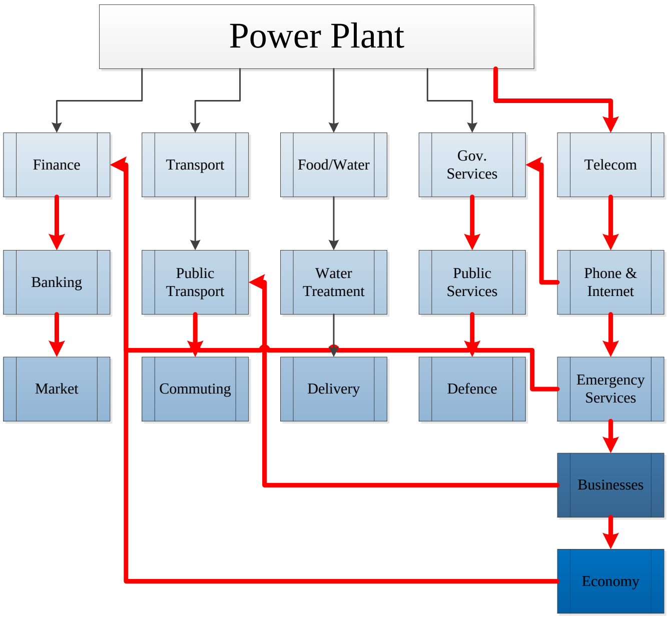


Figure 5 Cascading Failure

The failure has direct impact on phone and Internet connections. As a result, the Finance sector is affected, causing disruption to banking and markets. In addition, the emergency service which would no longer be contactable by the population and unable to offer their services where needed. Government Services are also impacted, which in turn, affects national defence. It is clear from the above that failure in one critical infrastructure leads either directly or indirectly to all the others.

In addition, the impact of an orchestrated attack on a nuclear power plant could have serious consequences due to the nuclear element involved [83]. A successful attack could not only affect the population but also the environment. Nuclear power plants are prime targets for cyber-attacks [83].

The dependencies one critical infrastructure has on another can be categorised into four groups, including Physical Interdependencies, Cyber Interdependencies, Geographic Interdependencies and Logical Interdependencies. Each are explained below:

- Physical Interdependency: Where infrastructures are dependent on physical output from each other. An example would be material output from one infrastructure that is required in another.
- Cyber Interdependency: Where the state of an infrastructure depends on information that has been transmitted. An example of this is in automation or the use of SCADA systems.
- Geographic Interdependency: Infrastructures that are dependent on environmental events or where natural occurrences can affect the infrastructure. An example would be a geographical event which would create changes in all the nearby infrastructures. An example could be a hurricane.
- Logical Dependency: Where infrastructures are linked by states such as politics, legal or regulatory regimes or any events, which are not physical or cyber [71].

2.5.2 INTERDEPENDENCIES

The high level of interdependency has been highlighted by the EU who discuss that one of the underlying reasons for potential cascading failures occurring are due to a lack of co-operation between European Member States when it comes to improved protection methods. Specifically, they identify the following weaknesses as areas which are damaging for the future of critical infrastructure security [89]:

- Member states having uneven approaches to security and resilience. Visibly, the disparity between Member State capabilities means that different approaches to security are subsequently adopted.

- With the introduction of new proposed governance models, a challenging volume of difficulties could be faced in some countries as, inevitably, some countries have weaker capabilities when it comes to critical infrastructure security
- Limited early-warning capabilities between European countries. Given the cross-border interconnectivity, the ability to warn neighbouring countries is essential.
- Low awareness of the growing threats. Despite the volume of cyber-attacks occurring on a daily basis the awareness of existing threats to critical infrastructures remains fairly low [30].

The infrastructure vulnerabilities are further enforced by the impact frequent unexpected natural disasters can have on infrastructure operations. One such example of this, is the impact of volcanic ash in 2010 across Europe [90]. Wilson *et al.*, discuss the implications of the wide range of hazards posed by volcanic eruptions and the impact on critical infrastructures, focusing, in particular, on volcanic ash.

Electricity networks are noted to be particularly vulnerable to ash disruptions since it tends to adhere to power lines and substation insulators where it can cause unintended electrical discharge and result in disruption to power distribution. On becoming wet the ash becomes heavier and can also cause line breakage or tower collapse. In addition to the impact on electricity distribution, falling ash can impact on water treatment plants or enter the water distribution network and contaminating the water supply. The disruption caused by ash clouds is not limited to affecting only water supplies as the volcano emissions from Iceland during the early months of 2011 demonstrated. For a substantial period of time, air travel was affected by large ash clouds which covered a large part of northern Europe impacting air travel and subsequently affecting the economy.

It is in light of the numerous vulnerabilities that Rong *et al.*, propose an effective technique that aids with planning for critical infrastructure protection by providing a way of analysing the interdependency of crucial systems using interpretive structural modelling (ISM) [21]. They, similarly to others, point out what a critical system is and why it is so important to protect them. However, they take the next step of detailing how one infrastructure can depend on another in an ISM relationship and how, if one fails, another can be affected. Furthermore, they consider the interrelationships between networks when developing the subsequent generation of critical system networks, as understanding the interaction between networks can lead to better efficiency and more effective network security. Because of the clear impact natural phenomenon have on critical infrastructures there will always be a risk of cascading failure occurring.

Their model is based on the use of assigning values to show the weight of the consequences of an infrastructure failure. In addition, the use of an impact index and extent indexes which ranges from 1 to 9 combine weighting of the failure duration and severity. The example given is that of the analysis of the 2008 Chinese winter storms where large portions of southern and central China were affected by heavy snow and cold temperatures, causing disruptions in power supply and the provision of other critical infrastructure services [21]. The representation of critical infrastructure interdependencies through the use of a model which provides an impact index is an effective way of demonstrating the extent of cascading failures. Using this method it would be possible to aid failure planning and the prioritisation of protecting critical infrastructures that would be deemed a high risk.

Continuing the research into critical infrastructure interdependencies, Barrett *et al.*, present a study of human-initiated cascading failures between critical infrastructures. They present a model for studying human-initiated interdependencies between societal infrastructures and how they respond to cascading failures. The systematic study of human-initiated cascading failure presented focuses on several closely critical infrastructure sectors, including two forms of telecommunications and transport. It is noted that during periods of crisis, there are individual behavioural changes in the patterns of activity, which affect the provision and demand for the services. The aim of the work of Barrett *et al.*, is to study the potential impact a chemical attack in a densely populated area could have on the use of telecommunications and the subsequent cascading failure of the critical infrastructure networks. They also present a representation of the behaviours of individuals and how their actions depend of the person’s demographics, such as age and gender during the event of a crisis occurring [91].

The impact of a chemical attack is highlighted by the changes in call patterns. Given that when call patterns are normal, the area that has the highest volume of calls is in the region of the city centre. However, as evacuation begins the locations of the users' changes as they try to avoid the disaster and this impacts demand on fixed based stations. The main contribution and results is the demonstration of the change in the use of loads put on the communication network. The model they describe is based on the combination of several models, including an evacuation model, a mobility model, the changes in calling patterns and the addition of multi-hop mesh networks which can be used to increase the capacity of cellular infrastructures.

The interactions between critical infrastructures are a complex mixture of adaptive dependencies and changing demands, which produce many different forms of services and result in, complex challenges.

Not only do the interdependencies between critical infrastructures produce design challenges, the sheer volume of components and technologies used within all add to the overall complexities involved. In response to this issue, critical infrastructure complexities are discussed in the following section.

2.6 Critical Infrastructure Complexity

Due to the advantages of using control systems, critical infrastructures have become increasingly reliant on automation, wireless networking and interconnectivity [47]. This reliance on automation has resulted in challenging design complexities as a large infrastructure tends to consist of thousands of nodes and components across a vast area all connected to a control station [92].

2.6.1 Design Complexities

The topological growth of networks also means that individual components inside an infrastructure end up being integrated by mutually incompatible information systems in order to control operations [93]. There is an emerging issue that the problems surrounding complexity are being exacerbated by the fact that interconnectivity is becoming fundamental for automation to be effective. In India, for example, there has been a large investment over the last decade into the private sector for infrastructure development to increase automation and production. In result, there are inadequate measures in place for disaster planning and preparedness should a failure occur and spread between infrastructures due to the diversity and lack of co-operation in technologies used [94].

In addition, reliability is affected by the fact that critical infrastructures are in some cases overloaded and have increased in complexity due to the growing demand of the services they offer. Subsequently, complex networks consisting of a vast number of components mean that there are more potential targets for attack [95]. Clearly, the more automation is used the more the resilience is reduced, and weaknesses emerge caused by the design complexities and dependence on computerisation, [96] especially as new technologies are integrated [75].

In addition, the reliance on wireless networking has brought about additional problems and design complexities of its own. Using wireless networks and wireless nodes, specifically, mean that more potential entry points into the system are offered. The energy requirements of wireless nodes, in particular, mean that when depleted, they can no longer conduct their designated task and are therefore, useless until the energy is replenished [97]. Attackers have recognised that one way of attacking a WSN (Wireless Sensor Networks) is to detect which nodes have ‘special roles’ and exploit them in order to increase the efficiency of an attack. If one node has a key role in the functioning of the infrastructure functioning and is often overburdened, then the attacker can have more success at causing disruption if that particular node is the target of the attack than if a random node was picked.

The result of this is a weakness to Sleep Attack, which involves denying energy-constrained sensor networks the ability to sleep. Sleep attacks prevent packets from reaching their destination meaning that commands can be sent without being able to reach their destination [98]. With the use of WSN, reliability must be invested in as critical infrastructures are required to provide their service 24 hours 365 days a year and failures caused by WSN errors are not acceptable [99]. WSNs are, in particular, expected to be energy efficient due to long-lasting life requirements and ultra-low power communication [97].

The complexity is reflected in the layout of wireless nodes, especially when designing a critical infrastructure where the topology is required to be robust [100]. If the network is not designed to cope with the loss of several nodes, the infrastructure will fail. The layout of the nodes makes the difference between a network continuing to function or completely falling apart.

Reliability is becoming an increasingly difficult task, as in most developed countries, large segments of components of critical infrastructures are becoming old and out-dated, which increases their vulnerability to failure. It is quite often the case that less-modern infrastructures have been adapted through an increase in demand for their services over the years and have been expanded and developed without careful planning when it comes to security. In addition to this, many have had to incorporate and adapt to the use of new security techniques despite the fact they may have been built long before this was an issue worth consideration. It is fair to say that because of the need for older infrastructures to adapt to keep up with modern demands, the complexity of the system has increased to a point where developing effective security techniques has become difficult as the systems are so complex.

2.6.2 Technologies Used

In addition to the use of control systems, various other components provide key functions towards the provision of the services, which critical infrastructures provide to the population. Different types of technologies are used to compose the hardware layer of the infrastructure and are vulnerable to both cyber and physical attack as well as the changing environmental occurrences.

An effective example of this can been seen in an airbase where a combination of optoelectronics and sensors offer a network of movement detection [66]. Loroch *et al.*, discuss this use of optoelectronics hardware for defending an airbase, which consists of a mass observation system, including a mast and infra-red sensors; a radiolocation observation system used to track and detect mobile objects. One other common piece of technology used in critical infrastructures are sensors, which perform the task of acquiring data. The model of the use of optoelectronics is an example of the effective use of sensors inside an infrastructure.

Many infrastructures, particularly in the industrial sector rely on the use of nodes. Nodes can perform multiple services, either acting as sensors to indicate what is happening inside an infrastructure, or provide a way of relaying information to components in the system.

To carry the data packets across infrastructure networks, the communication links used usually consist of fibre-optic cables and Ethernet. They are generally used in the telecommunications network where large companies are installing it to provide efficient Internet services. Fibre-optic cables provide extremely fast communication links. Ethernet also provides the ability to communicate information at high speeds and stream data which helps with remote monitoring and maintenance in that problems can be diagnosed and fixed from a distance and, in doing so, improve interoperability since multiple infrastructures use this type of communication link.

Power plants are particularly vulnerable infrastructures due to the sheer number of components involved and the reliance on automation. From the loss of power, all infrastructures would be affected and in the case of hospitals or transport control, this would be extremely damaging. The different technology used in power plants provides a good example of the combination of components required to provide a service.

Power plants operate through a process which involves heating up water and using the steam produced to power a turbine, which in turn generates power. The water is pumped into the reactor and heated up by nuclear fuel elements. This also serves to cool down the core and prevent it from overheating. The water is pumped using a system of water pumps where a PLC is used to monitor through the use of battery-powered sensors. This is known as a boiling water reactor [101]–[104] and water is used both as a coolant and for generating energy [101].

Inside the reactor core, pressure is very high, about 155 times the atmospheric pressure, and its controlled by a pressurizer which controls the flow of steam into the creation of energy and the secondary loop where it is turned back into water [101].

The recent trouble experienced by the Fukushima power plant in March 2011 in Japan provides an effective example of the reliance on multiple components inside a power plant. The Fukushima power plant was hit by a tsunami caused by a 9.0-magnitude earthquake. After the tsunami, the water pumps which are used to provide water to cool the core inside the power plant failed, resulting in the core overheating and causing an explosion and radiation leak. In result, a 20km exclusion zone was imposed around the power plant to minimise the health risk to the general population.

The number of components used are heavily relied upon and prone to individual weaknesses. Monitoring and operating these multiple components in real-time requires complex control systems, which have the ability to keep track of the demands of operating a critical infrastructure. Clearly, security is a very important issue for the safeguarding of the technologies used.

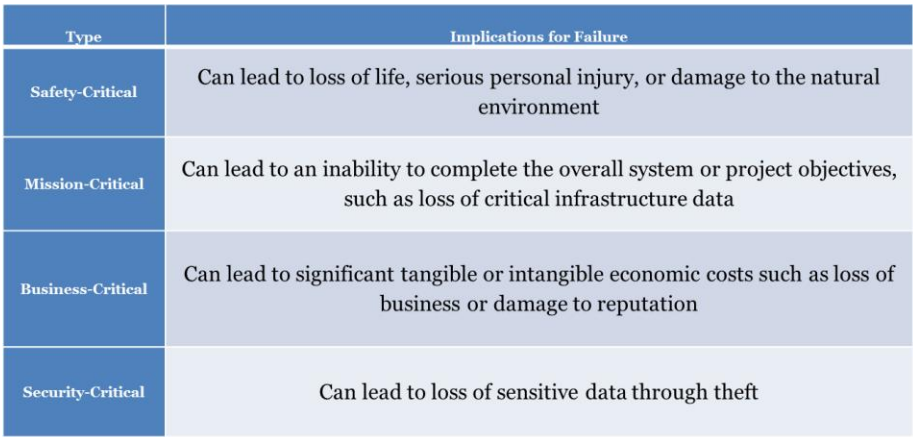
2.7 Security

Critical infrastructures tend to be civilian owned by commercial companies that operate competitively with limited capital for spending on security. The result of this is that security can be put at a disadvantage as, different technologies may be used in each and infrastructure owners are hesitant to share or co-operate with others as business information or strategy can be given away by the actions it takes to secure the infrastructure [105].

2.7.1 Defence in Depth

Despite there being multiple types and levels of sophistication of cyber-attacks, there are four different types of possible failures in total, as a result of a successful breach of security. These failures are displayed in Table 1.

Table 1 Implications for Failure



Type	Implications for Failure
Safety-Critical	Can lead to loss of life, serious personal injury, or damage to the natural environment
Mission-Critical	Can lead to an inability to complete the overall system or project objectives, such as loss of critical infrastructure data
Business-Critical	Can lead to significant tangible or intangible economic costs such as loss of business or damage to reputation
Security-Critical	Can lead to loss of sensitive data through theft

The aim of dividing failures into four groups is to categorise the critical infrastructure through the services provided and ensure that the correct type of security is in place to combat the category of failure that can occur.

Due to the cost of failure, most critical infrastructures take the approach of building their security with a Defence in Depth (DiD) approach [113], [114]. DiD is an important aspect to a critical infrastructure, and it involves various layers of security with different technologies and Intrusion Detection Systems (IDS) on each layer to ensure that if an attacker penetrates one layer, they are not automatically able to access the next one [115].

Hitchins *et al.*, details the theory of DiD and how there are several advantages in using this approach. The advantages include: good organisation resulting in fewer system parts and reduced complexity, efficient co-ordination of the parts of the infrastructure, good interaction and optimisation of the overall system [113].

As Kumar *et al,*. discuss, DiD is most effective when layers are created that are independent of each other. These various levels of security would, for example, include Low levels, Medium levels and High levels. The Low levels would be accessible by general employees who require basic security clearance to the infrastructure to perform their tasks and have access to only a small amount of necessary data. The high levels, however, would only be accessible by management and system administrators due to the fact that the contents would be of a more sensitive nature.

2.7.2 SECURITY

Inside the DiD approach, IDS have the role of detecting the hostile activities in a network and signalling alarms when attacks are identified [116]. There are multiple types of IDS, which are widely used to enhance network security [117] and provide a sense of security for computers and network data by identifying in real time misuse or unauthorised use, whilst allowing the system to continue functioning. Considering that different types of IDS exist it is possible to categorise them into two distinct groups: Host-based and Network-based IDSs. Host-based IDS have the task of monitoring resources such as logs and application activity in real-time. Whereas Network-based IDS continually scan the network in order to detect intrusions [118].

Two common types of IDSs which are used for the identification of intrusion attempts include anomaly detection and signature-based detection. Anomaly detection involves the detection of abnormal network activities. Such an anomaly may include, for example, a sudden increase in a data flow in a certain part of the system, which is unexpected [119]. Signature-based detection is the use of a pattern to identify data that stands out as being an intrusion [116]. The pattern is based on the comparison of the attack with known attack signatures. Signature-based detection, however, is non-adaptive and cannot detect attacks which don't have a signature making it ineffective when used by itself [120]. To cover for various forms of attack, critical infrastructures typically use a combination of multiple types of IDS to ensure that the infrastructure is as protected as possible from the many threats that can originate from external network connections.

Building on the success of using IDS, recent years have seen the introduction of Unified Threat Management Systems (UTM) for critical infrastructure protection. UTMs use a combination of firewalls, pattern recognition, IDS, embedded analysis middleware to implement a deep level of security. UTMs first appeared in 2004 and are now widely used to enhance network security [117]. The combination of these various protection techniques means that UTMs are able to offer a level of protection to the Hardware, Software and Network layers in one [117]. However, although they are equipped to monitor multiple layers, critical infrastructures also tend to use many types of UTMs in the same infrastructure for defence in depth purposes. If one type of UTM is compromised during the course of an attack, there is a different type as a backup, which the attacker has to compromise separately.

UTMs in general integrate multiple security technologies such as control interfaces, message formats; communication protocols and security policies and for that reason the management of security technologies in UTMs presents a major challenge. The current importance of UTMs for critical infrastructure protection is enforced by Zhang *et al*., who discuss that UTMs provide a combination of multiple security features, which creates a level of protection through the use of a unified security architecture [117].

The benefits of using a UTM system include cost benefits, as the number of appliances is reduced and therefore, there are lower management and support costs. UTMs are easy to use making them ideal for organisations who do not have technical capabilities. However, similarly to other technologies being used, UTMs are prone to several weaknesses, none more so than being the single point of failure in the security system [121]–[124]. A UTM is effectively a security gateway, which filters and monitors network flows between Internet and Enterprise Networks [121].

UTMs tend to be divided into two groups including loosely-coupled and tightly coupled:

- Loosely-coupled UTMs integrate security products from various manufacturers meaning that interoperability between the components is an issue.
- Tightly-coupled UTMs are when the UTM has been developed by a single manufacturer meaning all the security functions have been developed by a single vendor with no interoperability support [5].

2.8 SUMMARY

Despite large investments into critical infrastructure protection techniques, there are still a large number of weaknesses, which need to be addressed. It is clear that infrastructures face significant threats. The growth in the use of SCADA and control systems and the fact that networks are becoming integrated in some way with public networks, are making critical systems more vulnerable to cyber-attacks.

In addition, the growing use of wireless networks means that infrastructures can be more vulnerable to direct attack than previously. It is essential to evaluate critical infrastructure protection levels and address how security can be improved. This is further enforced by a growing volume and level of sophistication of cyber-attacks.

In this chapter, critical infrastructures were presented in detail, along with the technologies used inside them and their existing weaknesses and vulnerabilities. Security currently used for safeguarding these vital service providers was also presented, as was a discussion on their existing flaws. In the following chapter, the growing cyber-threat is present along with their origins and some examples of where attacks have been successful.

CHAPTER 3

CYBER-THREAT

3.1 INTRODUCTION

Critical infrastructures are under constant cyber-attack from hackers, foreign nations and cyber-terrorists (to name but a few sources) who attempt to disrupt and steal information or inflict damage on crucial and vulnerable resource providing services. Amidst increasing threats of cyber-attack and cyber-based warfare, critical infrastructure protection is becoming a growing concern for governments and organisations around the globe, with experts disagreeing on whether the potential scale of impact from failure could affect millions or billions.

In this chapter, the threats posed by cyber-attacks are presented. Numerous, past, successful cyber-attacks are offered as examples of why there is such a concern about what the future holds in the digital environment. Topics, such as the growth in cyber-attack sophistication and future global challenges for defence systems, are investigated in depth. In addition, future challenges and the importance of increasing cyber-threat awareness is highlighted and presented in this chapter.

3.2 THE THREAT OF CYBER-ATTACK

Many forms of cyber-attacks are currently being encountered around the globe [127], [128]. These attacks have mixed and varied degrees of success. Along with the potential of physical damage caused by an attack on a critical infrastructure, as touched upon earlier in this thesis, there is also a strong threat of losing sensitive information. This has already been demonstrated in the well-known Night Dragon cyber-attacks [129] in which oil, petrol and chemical companies around the globe were targeted through the use of a series of complex hacking techniques in order to gather information on financial data and company strategies. Information, such as bids on oil and gas fields, were targeted along with company project-financing information, which is usually treated as highly sensitive [129].

3.2.1 CYBER-THREAT EXAMPLES

As a result of examples, such as the Night Dragon cyber-attacks, M15 has recently said that it is astonished with the level of cyber-attacks on British industries occurring daily and with the UK announcing their intention to invest millions into cyber-defence to combat their vulnerabilities and counter the threats, clearly governments are beginning to recognise the real threat that exists [87]. The UK, however, is not alone in experiencing cyber-attacks and other countries have reported an increase in the number of threats being encountered [130]. For example, China was widely reported to have experienced millions of attempted cyber-attacks, which were targeted at the Beijing Olympic Games in 2008 on a daily basis [131]. Despite not being considered an infrastructure of importance the Olympic Games represent an identifiable iconic gathering and would be a high profile target if successfully attacked. A breach at such an event would result in an increase in fear of the consequences of a successful attack on a critical infrastructure network and demonstrates the real danger that currently exists.

In response to the increased threat, the European Union has recognised that international partnerships are one of the ways forward and, in Europe in 2010; the Cyber Europe 2010 exercise took place. With the aim of boosting communication and co-operation through a simulation of over three hundred hacking attacks, the exercise involved national and cross-border communication to counter attacks [86], [132]. Such activities as Cyber Europe 2010 emphasise the key role a community approach could have towards the level of critical infrastructure security. Despite the fact this exercise was one of the first steps towards cultivating the way critical infrastructures are secured, it provided an effective insight into how European member states manage incidents.

Through the exercise, the main objectives were to boost the level to trust and augment the level of understanding of difficulties that can be encountered when infrastructures operate across borders [86], [133]. This idea of strengthening Europe’s incident response through international partnerships was again seen in 2011 in the first joint cyber-security exercise between the EU and the USA. During this exercise, two simulated cyber-crisis events were devised to discover how the EU, and the USA, would interact in the case of a real-life event taking place [86], [133]. Clearly, for security to improve, it is imperative that isolation from other parts of the world is avoided so that there is coherence for the defence measures being devised and put in place [134]. It is clear that the cyber-arms race is beginning.

3.2.2 Cyber-Threat Growing Concern

With the volumes of complex attacks starting to increase and present a real threat to critical infrastructures, in this subsection various existing cyber-attack types are presented as a demonstration of the variety of attacks facing critical infrastructures on a daily basis.

One of the most common methods of attack is the Distributed Denial of Service (DDoS) attack [135] where systems are sent large volumes of traffic, which is intended to make the system fail by overloading it. This attack is so effective as there is no way to distinguish between good requests and bad requests, making attacks difficult to block [136], [137].

Another common technique is the Man in the Middle attack (MITM) [138] where false commands or system instructions and fake responses are inserted into the system. Not only can a MITM attack be used to cause disruption; it can also be used to provide a way of eavesdropping making it important to use authentication protocols to ensure the communication is reaching its intended destination [139].

MITM attacks can occur in various forms, one such form of attack, which is starting to become a well-known threat to Internet users as well as critical infrastructure operators, is the Phishing attack. Phishing attacks are engineered to steal information, which can subsequently be used for identity theft and financial profit. They operate in many forms but one of the most common is the use of a fake website, which closely resembles the website the user is trying to find. The counterfeit website is then used to gather information such as usernames and passwords as well as sending out spam emails. Banking information, such as credit card details, is usually the primary target and the success Phishers tend to have means this type of attack has become the most popular way of conducting cyber-crime [140].

This is reinforced by the fact that online financial transactions such as banking, shopping and money transfer have dramatically increased over recent years. Joshi *et al.*, discuss that in the USA in 2008 over 5 million users were victims and were affected financially as a result of successful Phishing attacks [141]. Whilst security is steadily improving for combatting attacks such as these, there is a real need for alternative approaches to defence.

Phishing attacks are becoming increasingly numerous and one specific type of phishing attack is known as a Spear-Phishing attack. This involves a targeted form of a phishing attack [142], where the success rate of the attack is higher compared with the generic bulk approach often used. Spear phishing attacks are designed with a specific target in mind and rely on human error to be successful. Their aim is to trick the victim into thinking an email-based scam is legitimate by ensuring the information inside is specific to that person or organisation [143].

One growing method of attack is the use of Botnets. A Botnet is a malicious network of compromised computers. These computers are referred to as bots and are controlled by a human operator. The operator uses the controlled computers as a distributed platform for conducting cyber-crimes such as Distributed Denial of Service (DDoS) attacks [144]. Using botnets allows the operator to have a fairly high level of anonymity. It also, effectively, functions as a cyber-army, which can span across the globe, without the user having to invest in their own hardware or own any physical components. Botnets have been specifically identified by the European Commission as a major growing threat to cyber safety. Feily *et al.*, also discuss that currently very little is known about botnet behaviour. Botnets also tend to demonstrate strong synchronization in the responses [144].

Another of the most common cyber-attacks critical infrastructures are having to cope with is an SQL (Structured Query Language) Injection attack. A successful SQL injection attack allows data to be stolen from a database [145]. It functions by using original SQL queries to the database to change, obtain or view data [145] making the SQL query malicious [146]. Such types of attacks typically target systems, which use significant database services, which require continuous user inputs to and from the database using SQL [146].

Some types of cyber-attacks are specific to individual parts of critical infrastructures. For example, Igor Nai Fovino *et al.*, discuss various attacks which are designed with the precise intention of disrupting or infiltrating SCADA systems [85]. One such attack is known as a Process Network Malware Infection (PNMI) and it involves injecting a worm into the process network. The process network is often used for hosting the whole of the SCADA where communication is conducted through protocols like ModBus or DNP3 (as discussed in section 2.4.2) [85].

The worrying factor about PNMI attacks is that they have the ability to spread using the hosts resources. The Slammer worm, previously mentioned in the Introduction, functions in the same was as a process network malware infection [85].

3.2.3 Cyber-Threat Sources

The increased variety and sophistication of cyber-attacks is, in part, due to the variety of attack sources. Ranging from insider-threats to Hacktivists the sources of attacks can vary depending on the situation [147]. Nicholson A, *et al.*, highlight some of the various culprits of cyber-attacks, each of are discussed below:

- States or Governments: With the ability to disable or severely cripple a country's ability on the other side of the globe through use of a remote computer, it is clear to see why governments are currently investing heavily in cyber-warfare technologies. As news agencies frequently highlight, state created viruses can potentially be the major threat to SCADA systems due to the level of sophistication and financial investment, which has gone into its development [147].

- Insider attack: Attacks occurring from inside an infrastructure are a problem, which infrastructures are becoming increasingly aware of and preparing for. An attack, which originates from the inside of an infrastructure, has the advantage that security measures can be bi-passed and damage can be done before security has a chance to respond [147]. Often such attacks would occur as a result of an employee being disgruntled or upset with the organisation.

- Organised Crime: Any attacks, which originate as part of organised crime are usually motivated by money. As Nicholson *et al.*, discuss, attackers often have access to substantial amounts of money and target banks or large companies, which can be held at ransom.

- Hobbyists: An unusual threat critical infrastructures face comes from individuals who see a cyber-attack on a system as a challenge or thrill or something, which is simply curiosity motivated [147].

- Script Kiddies: Similarly to hobbyists, script kiddies tend to be individuals who have limited access to sophisticated technologies and perform their attacks through use of limited scripts.

- Hacktivists: Attacks which originate from Hacktivists tend to be individuals or groups who have political reasons for the their attacks [147]. For example, if a group wish to protest over the implementation of a new law, or make a political statement, then often cyber-attacks are conducted as a means to gain attention. One group known as Anonymous, have successfully conducted several high profile attacks, such as, targeting the UK police web forum in order to make a political statement.

The problems current control systems experience, enforce the need for an improvement in the technology used. However, critical infrastructures do not only have to cope with multiple control system vulnerabilities, they are also facing various type of SCADA system perpetrators, as Nicholson *et al.* discuss [147].

The result of the variety of threats control systems face in the immediate future signifies that there is a clear need for a high level multifaceted security system to safeguard critical infrastructures. This factor results in cyber-threat challenges, which are discussed in the following section.

3.3 Cyber-Threat Challenges

The improvement of cyber-defences is of huge importance to safeguard the increasing use of ICT, automation services and dependence on interconnectivity. However, countering the growth of cyber-attacks and their numerous sources is faced by various challenges, which must be addressed. This includes weaknesses in control systems and diverse problems with cross-border co-operation. In this section, some of the challenges being faced are presented along with why these problems exist and how they can be addressed for the benefit of improving cyber-defences.

3.3.1 Control System Weaknesses

As it is one of the main control systems used in critical infrastructures, it is important to, first of all, discuss the problems with SCADA. One of the main problems is the overload of data which the operator has to deal with [148]. Due to the size and complexity of the systems being controlled the volume of data being processed is vast. SCADA operators tend to organise the information gathered for the forecasting of future control of the system [149]. Similarly to how an airline would forecast future revenues and passenger levels based on a huge variety of data through use of mathematical models [150]. Forecasting is the future prediction of system requirements based on current and past values [151].

An example of this in a critical infrastructure environment, would be the forecasting of errors that can occur, or more specifically changes, which could occur in physical parameters that would affect the operating of the system, such as, the forecasting of water loss based on a water distribution control system. Using the information gathered, adjustments are made to the system and the user must decide how much of the collected information should be used to do this effectively.

Another problem often encountered is the number of incorrect readings, which can affect the forecasting results. Due to the sheer volume of components being used it is inevitable that some of them tend to malfunction and cause errors or fail to provide feedback altogether. These missing values are, however, very difficult to detect given that the volume of data being gathered is so great it can be challenging to identify when values have not been collected. SCADA systems can also fall victim to time-scale errors and faults, which are caused by computational delay as a result of the volume of network traffic making real-time analysis of results hard to process [152].

3.3.2 Security Weaknesses

Continuing the discussion on vulnerabilities, it is important to, subsequently, address weaknesses in security systems such as UTMs and IDSs. IDS is not a vulnerability but it has susceptibilities of its own. The main problem with IDS and UTMs is there is too much information and therefore to reduce the amount of information an architectural approach is taken. UTM's also reduce the number of false positives by operating behind a firewall, meaning that the firewall acts as a filter.

Another problem with using IDS in critical infrastructures, however, is that they often tend not to be advanced enough to detect sophisticated cyber-attacks and where advanced security is used there are usually compromises such as slowed network activity caused by data being analysed in real time [153]. IDS are the only gateway into the infrastructure, and their continuous monitoring of network activity means that performance is slowed due to the sheer volume of data requiring analysis [121].

It is often discussed that one of the weaknesses of an IDS is that they tend to become the bottle-neck of the whole network [122]. In addition, IDS tend to generate a high level of false positives meaning that frequently an alarm could be signalled incorrectly. Considering the sheer size of critical infrastructures and the number of components, a large scale distributed IDS will produce a large number of alerts [154]. The risk with this problem is that real incoming attacks can get masked, and in result, operators misled [155], [156].

One of the main problems with UTMs is the use of a combination of different technologies. Multiple types of technologies are used and combined to form a UTM due to the variety of functions it is required to perform. However, the result of this is that applications tend to work independently of each other.

Deng *et al.*, discuss the limitations of current UTM devices and how the weaknesses impact performance. UTMs do not guarantee performance and quite often slow the network activity. This problem is generally caused by the network operating in layers causing increased costs. UTMs can also, only catch packets from specific IP addresses and cannot devise the user identity of packets [121]. UTMs have the tendency to become the bottle-neck of the whole network [122], as they tend to be composed of multiple applications that tend to work independently of each other resulting in slow processing [123].

In the work being conducted by Y. Zhang *et al.*, [117] they address the issue of the design and implementation and configuration and management of UTM security through proposing a practical control mechanism. They present a solution to improving the control and management mechanisms of UTMs. The control system is designed to be easy to use, have high interoperability and high efficiency among other improvements. Their solution, UTM-Configuration and Management, or UTM-CM, consists of three layers: the configuration layer, the enforcement layer and the communication layer. The configuration layer allows for human interaction, the enforcement layer is the layer which processes control messages and the communication layer provides the machine-to-machine communication and interaction. Each layer combines multiple utilities such as Graphical User Interfaces (GUI), Configuration Managers (CM), Message Protocols and Notification processes.

The work conducted by Y. Zhang *et al.*, [117] is detailed in a high level manor and under experiment the results showed that the system is easy to use and provides high efficiency. The solution they provide differs to how a UTM currently works in that it offers greater scalability and ease of use than current UTMs provide.

3.5 SUMMARY

Cyber-attacks are increasing at an alarming rate. The need to remain one step ahead of the attacker is becoming more and more important. Clearly, the consequences of failure can produce unexpected results and must be planned for in order to prevent disasters escalating. The cost of physical consequences reflects the ever growing need for effective critical infrastructure protection for the future safeguarding of the services which are heavily relied upon by the population.

Despite the clear need to develop effective methods for protecting critical infrastructures, the task is a difficult one. The protection of these important infrastructure systems is becoming exceedingly complex due to the sheer size involved, and the technologies used. The problem highlighted is that infrastructure security must always attempt to remain one step ahead of attacks. We propose our method of using behavioural observation and pattern detection in order to add to the defence in depth currently in place. In the following chapter, we present researched related to this. An overview of our system design and its evaluation will then form the remainder of this thesis.

CHAPTER 4

BEHAVIOURAL OBSERVATION AND SIMULATION

4.1 INTRODUCTION

Improving the level of support for security systems helps towards the evolution of cyber-attack defences. Our approach for supporting critical infrastructure security against cyber-attacks involves behavioural analysis and data classification techniques. The use of each of these has a key role in how our system functions. In addition, a simulation is also used to construct the data we use for evaluating our approach. Simulation is an effective tool in the development of critical infrastructure security systems and provides an effective way of testing the effect of implementing new technologies without consequence. For that reason, in this section, we present a literature survey of behaviour analysis, the benefits of simulation and current areas of research employing data classification techniques.

4.2 BEHAVIOURAL OBSERVATION

Many research areas currently explore the use of behavioural analysis to achieve an improved level of performance in their field. Some infrastructures already implement their own behavioural observation techniques for security purposes. One example of this is seen in banks where credit card patterns are analysed to offer a level of fraud or theft detection. Using the example of bank card misuse detection, two different categories of behaviour, normal behaviour and abnormal behaviour are explained using the following examples.

- Normal behaviour: In a bank system, this model for normal behaviour is based on demographic and economic information combined with a database of historical behaviour. Combining such sources of information to devise a pattern of expected activity is used as a template for the expected behaviour or the user [166].

- Abnormal behaviour: In a bank system, if the pattern of activity deviates, from the expected, the bank then flags it up as a potential card theft. Abnormal behaviour consists of data generated by behaviour, which is out of the ordinary, such as a significant change in location of the card or a sudden increase in the use of the card, over a short period.

In our approach, the reasons these two different types of behaviours are needed are to show how our threat-detection approach will operate. In a critical infrastructure, correct behaviour will be clearly defined when the infrastructure is being built. Systems will be set up with clear defined tasks of what they are required to do and when. The reality is, however, that the system will function correctly but slightly outside of what is expected. It is this behaviour, which is classified as normal behaviour. Therefore, abnormal behaviour will subsequently, refer to changes in the expected patterns of the normal behaviour of the infrastructure [167].

We are taking the approach of measuring behaviour to identify attacks which occur on critical infrastructures. The following section highlights a specific area in which pattern detection is currently used with effect for security purposes.

4.2.1 BEHAVIOUR TYPES

Bank security has been using behavioural observation for several years for the identification of card theft and fraud. Most banks currently monitor credit card activity and develop a pattern of what would be considered normal behaviour for the user of the card [40]. The aim of this is to identify when the card is misused because of a change in patterns of behaviour. As protecting against a digital threat is, of course, a growing concern for the banking industry, there is currently a large amount of research into improving and enhancing the existing methods used for safeguarding credit cards and bank accounts.

One approach taken by Chan *et al.*, is the use of fuzzy logic rules to mine data collected about a user's bank activity [168]. For these purposes, they present the development of their FARM II (Fuzzy Association Rule Mining) technique. The approach involves three steps. Firstly, both relational and transactional data is combined, secondly it identifies fuzzy attributes, and finally, it uses a rule-search process. Their work, in particular, focuses on the mining of data to detect patterns of activity and in doing so learn as much as possible about the customer. The aim is to provide more information, which the bank can use to devise new products.

Their technique combines fuzzy logic with the association rule to mine data. Despite this, the principle behind developing patterns of activity based on analysing data is comparable with security research into pattern detection.

In another approach, Ma *et al*., discuss the use of mining through historical customer data in a bank to propose their own approach to identifying credit card fraud and offering support to banks to counter this problem. Their approach involves the analysis of past data. Using a genetic algorithm, which is an algorithm used in artificial intelligence applications, to learn the natural process of things, they aim to propose a method for preventing credit card fraud. As Ma *et al*., discuss, genetic algorithms aim to solve and optimise problems through methods based on the theory of a simulation of evolution. The goal is to develop a model, which is adaptive that can detect card misuse through using a genetic algorithm to develop a confidence level, which will allow them to classify the data [169]. Their model uses real-life data, gathered from a user's behaviour, to judge whether a new, unknown, customer will be fraudulent [169].

Fu *et al*., also discusses the use of a genetic algorithm in a bank system. In their paper, the use of a genetic algorithm, in a financial institution, for the supervision of new credit card applicants [170] is presented. The algorithm is trained using 'good' examples to devise a rule set. The system is then tested by evaluating applicants against their behaviour, stored in the database. The approach is similar to the approach posited in this thesis in that patterns of behaviour are observed in order to determine whether or not there is a threat. In this case, however, the data used is information, which has been previously collected and the process is not done in real-time. Furthermore, the evaluation is not performed using a comparison of past data and current. It is solely based on the users' past actions to decide whether they will be a threat in the future. The approach taken by Fu *et al*., demonstrates the efficient use of genetic algorithms. However, as the author points out, more sources of information would be ideal to present a clearer picture of the system.

Algorithms have multiple applications in computing, as Li *et al*., discuss. They highlight network vulnerabilities and how they are a direct result of malicious nodes, which do not comply with network protocols [171]. As they discuss, nodes operate as part of a network and are required to follow protocols, in order to work together and achieve a common goal. However, similar to every IT system, interactive node networks also face various cyber-threats. One such threat is that of a pollution attack where a malicious node may upload a malicious piece of information to the network, in order to, disrupt operations. Such an attack can be found in an online social network where there is peer-to-peer interaction. Their research aims to develop an algorithm to detect malicious nodes so as to block communication, and reduce their impact inside the network, by designing a distributed detection algorithm. The algorithm is given to every good node so that it can detect which of its neighbours are malicious.

4.2.2 USING BEHAVIOURAL OBSERVATION

The area of bank security is just one area where using behaviour analysis, in particular pattern recognition, is currently being used. As previously mentioned, other areas of research are investigating behavioural observation techniques. An example of this is reflected in the work being carried out in real-time event monitoring by Sekar *et al.*, as a way of developing effective critical infrastructure security [119]. In their approach, Sekar *et al.*, propose the use of real-time analysis, in contrast to the post-attack evidence analysis technique other security systems adopt. Their approach involves the tracking of problems inside an infrastructure through the use of automatically initiated reactions, which are programs developed to respond to attacks. In their approach, they aim to isolate compromised components to prevent the problem from spreading and also trace the origins of incoming attacks.

Their approach requires the use of a human operator who has to respond when abnormal behaviour is identified in order to have an expert who can identify whether the threat is real or not and thus minimising false positives occurring. Furthermore, their approach involves the comparison of behaviour with events known to be unacceptable. Our approach differs from theirs as they have developed programs, which look to respond to attacks and trace the origin of occurring attacks. Their aim is also to isolate components which have been attacked and only look at system calls which are involved with how components request a service from a control system. Our approach focuses on developing a whole picture of the infrastructure, fusing data to develop a detailed portrait of the events taking place and using that to identify changes in behaviour.

Our approach is also different to Bass *et al.*, who proposes the use of situational awareness for securing cyber space where the use of data gathering from multiple sources (data-fusion) can help security systems be more effective [153],[172],[45]. The fusion of data requires gathering from a variety of sources of information. One such technique discussed by Bass *et al.*, is data mining. Data mining is the detection of hidden patterns based on previously undetected intrusions, where data gathered beforehand is filtered and organised into sets in order to detect previously unidentified situational patterns and then used to develop new detection templates. This concept of using situational awareness is similar, however Bass *et al*., focuses in post event analysis in contrast to real-time data processing.

Blauensteiner *et al*., discusses one other approach using behaviour observation, and look into the use of pattern recognition in banks to improve security [173]. Their research is based on looking for abnormal or suspicious behaviour in events and a system designed to detect them. The aim of their research is to develop a way of detecting security breaches in critical infrastructures based on automated recognition of human behaviour. They state it is important to define abnormal behaviour to be able to detect it effectively and to identify what exactly abnormal behaviour is. In the case of humans, this is particularly difficult. Our research, however, does not take into account human behaviour but rather focuses on the system and infrastructure events as a whole.

On the subject of pattern recognition, Fernandez, E *et al*. discuss its use for SCADA security [174]. The aim of their proposed technique is to apply a pattern to a SCADA system to identify threats that have occurred at a software level and to guide security at each stage. The main problem with their approach is that their proposed technique does not take into account the effect their idea will have at slowing network activity on the system.

Critical infrastructures are growing in size and importance every year as the population grows and puts increasing demand on the unseen services provided. Protecting these infrastructures is clearly a key issue. One which our research, using behavioural observation, aims to address.

4.2.3 Behavioural Observation Challenges

To accomplish the role of adding to critical infrastructure security's defence in depth using behavioural observation, various challenges are faced. Drawing from multiple sources of information is one of the challenges. Using the data collected a model for correct behaviour will take into account any beneficial sources of information in order to accomplish its task. Components such as pressure gauges, nodes, network activity and physical processes, will be monitored.

Proactive security is another challenge. Through using the vast data collected by the SCADA, real-time analysis will be provided. The continuous identification of patterns, and the subsequent recognising of unusual activity, is the key to our design. Attacks can be identified through monitoring continued acceptable operation and recognising events that are out of the ordinary.

It is fair to say if there is a reliance on one method of security for defending an infrastructure, then compromising that method will result in devastating consequences. Security needs to be adaptive and take on board other methods for securing an infrastructure. This is essential in order to take the next step in the evolution of critical infrastructure security. Our approach is beneficial and complements current existing security. It ensures that the defence does not have to adapt continually to new and emerging threats. This is because our system looks for breaches in the pattern for correct behaviour. Security is offered through ensuring that the status quo is being kept.

Scalability and data processing speed are other issues to be contended with when implementing behavioural observation techniques in a critical infrastructure environment. The collection of data could take place from potentially millions of components meaning data processing time could be slowed. This would require our approach to employ a decomposition approach. Decomposition refers to the breaking down of data into smaller, more comprehensible representations of the dataset [175], [176]. An effective data extraction process can make the system scalable for national critical infrastructures. This will be presented in the system design.

4.3 Simulation in Critical Infrastructures

To combat the increase in cyber-threats many industries are taking the approach of using a testbed to assess infrastructure vulnerabilities. A testbed is a simulation environment, where a simple system is created to represent a larger project or infrastructure to allow for testing or experimentation to take place [92]. As Davis *et al.*, state, assessing the vulnerabilities in a system can be difficult due to the amount of complex software and hardware interactions that take place. It is because of this that the use of a testbed is ideal for assessing vulnerabilities.

4.3.1 Simulation for Security

This is reflected in the work being done by Wang *et al.*, who focus on simulation experiments [3] and the use of simulation techniques in order to assess the security of a SCADA system. In their approach, experimental attacks are used to evaluate the various vulnerabilities of the SCADA system. This includes an analysis of the impact of a cyber-attack on a critical infrastructure or SCADA system. In total, Wang *et al.*, investigate several SCADA security simulation methods and propose the implementation of a more flexible simulation environment. Whilst this is effective, their approach only focuses on one type of attack, therefore, to test the true flexibility of the approach, different attack scenarios need to be considered.

A simulation experiment is an effective way of analysing the security of a SCADA system. It works by creating an environment in which experimental attacks can be conducted in order to evaluate the various vulnerabilities of the SCADA system. The sheer size of infrastructures means that modelling and simulation are becoming an increasingly important factor. Simulations are an essential step when developing a system to ensure correctly configured instruments [5].

Critical infrastructures are faced with increasingly challenging cyber-attacks and simulation provides an effective role in testing the capabilities infrastructures have in facing the growing cyber-threat. Using emulators can provide an effective ways of developing new approaches to secure critical infrastructures [29]. Its use is becoming a common technique for the testing of cyber-attack prevention measures and for developing improved security techniques [132], [86]. A simple system can be created to represent a larger infrastructure and allow for realistic testing to take place [92].

Given their highly sensitive nature, organisations are often unwilling to part with data or detailed information about how their systems function. This poses difficulties for independent researchers and security companies to find an effective way of developing new approaches to securing critical infrastructures. As critical infrastructure data is highly sensitive, it is clear that simulation can provide realistic data without being restricted by security constraints. Furthermore, not only is effective security costly, the requirements individual critical infrastructures have are often unique meaning their security systems have to be tailored to match their specific needs. As a result of these factors, simulation can play a key role in the advancement of security measures in a cheap, safe and effective way.

It is clear that there are many benefits of using simulation. Most notably is that conducting experimentation can be done on a realistic representation of a system without the worry that any damage done would have a real impact [92]. In particular, when testing against cyber-attack resilience and developing new approaches to security, critical infrastructure simulation is of great benefit. Aspects such as cost can be kept to a minimum and new technologies to be introduced to the system can be tested through simulation prior to being put into practice in a real-life situation.

The aim of the simulation work presented in this thesis is to develop an emulator where data could be constructed, which would be consistent, yet, to some extent differ slightly every time the system is run. The benefits of using simulation can offer effective ways of developing new approaches to secure critical infrastructures.

4.3.2 Simulation for Co-Ordination

The previously mentioned Cyber Europe 2010 exercise which took place involving a simulation of over three hundred hacking attacks is clear example of this. However, further to this, in 2011 the first joint cyber-security exercise between the European Union and the United States took place. During this exercise, there were two simulated cyber-crises in order to discover how the EU and US would interact in the case of a real-life event taking place. The first simulation was based on an Advanced Persistent Threat (APT) whereas the second was based on SCADA disruption [86].

The recognition that simulation is the best approach to preventing cyber-attacks and improving responses is clearly identified as the best way forward by governments and organisations around the globe. Using simulation is beneficial in that it can be an effective tool for implementing new approaches to security in a realistic environment. It can also provide an insight into how effective a new approach to security would be and provide proof of applicability and performance evaluation.

4.4 Related Approaches

Based on the aims and objects of this research, which uses behavioural and simulation based research, in this section, a comparison with other similar approaches provides a critical discussion on how our approach compares with other research being conducted into security support. It is essential to draw from other research in the area of behavioural observation, as examples of how behaviour monitoring in critical infrastructures can be achieved. The other approaches discussed either involve behaviour or security enhancement research for securing critical infrastructures.

Schweitzer *et al.,* discuss the question: How would we know if an attack was taking place [62]? The reliance of the modern critical infrastructures on ICT and the increasing risk of sophisticated cyber-attack makes this question and an important one to ask. The aims set out for BOCISS were to allow the operator to identify attacks on the system in real-time by providing an overall view of the system and detecting anomalies in behavioural patterns. One of the main aims was to identify subtle changes in behaviour, which could be missed, and support the security currently in place.

4.4.1 Existing Behavioural Research

However, measuring behaviour is challenging, as Hernantes *et al*., discuss. They, consider the importance of situational awareness in critical infrastructures. Their research puts emphasis on behaviour monitoring to make the operator aware of triggering events that result in disastrous incidents taking place for disaster prevention. They recognise that 60% of all accidents tend to be caused by recurring disruptions due to un-identified attacks [177]. The study highlights the importance of being aware of dangers that could cause cascading failure. Critical infrastructure protection requires that managers and operators understand system vulnerabilities. Furthermore, they must comprehend their interaction with other infrastructures in order to assess properly the weaknesses a system has. Despite the investment into more advanced forms of security, success cannot be possible without a competent user.

For that reason, user awareness is a factor, which can play a key role in infrastructure defence. The Awareness Ladder is a two-tier model of Projection, which relates to the users' ability to see indicators and predict the events that could occur. It consists of two stages; Firstly, Comprehension which is the users' ability to understand the system behaviour, and the information displayed on the system. Secondly, Perception which is the users' ability to be aware of sensors that are of importance. The aim of this Awareness Ladder is to equip managers to act proactively to reduce the impact of a failure [177].

Developing a security based on awareness is an important issue for identifying security breaches or errors. A key way of quantifying behaviour is through the use of behavioural patterns which is the identification of trends in a dataset. Behaviour, however, is a difficult entity to quantify and a particularly challenging task.

Firstly, Singh et al., discuss how infrastructures worldwide are facing a very real threat from terrorist activity [178]. Their research focuses on the prediction of threat events from occurring using a semi-automated tool to perform analysis. They propose a model to track and detect terrorist activities and discuss terrorist tactics. To do this, they use two probabilistic methods: Bayesian networks (BNs) and Hidden Markov Models (HMMs). The HMMs have the role of detecting and measuring local threat levels and the BNs are used to combine the data collected from HMMs to evaluate the probability of an event taking place. Using their approach they evaluate the potential threat level to the 2004 Olympics.

The HMMS are fed data based on terrorist activity, which has been gathered from detectable clues left in cyber-space. Using the data collected over time, patterns of behaviour are formed using HMM and then a BN uses the data to predict the likelihood of an attack taking place. As terrorist groups tend to be elusive, decentralised and seemingly unconnected, behaviour can be difficult to predict, long periods of time are required in order to collect effective data for the Bayesian Networks to classify.

Despite taking a different approach to safeguarding the general population, the methods used by Singh *et al.*, are comparable with our approach in that behaviour is monitored and predicted using data classification through a Bayesian Network. Their approach also requires two phases of a learning or training phase for model construction to act as an inference model for their behavioural analysis. They refer to this as a maximum-likelihood estimation to obtain a reference point for when behaviour is not as it should be.

Our research differs from their approach as BOCISS is focused solely on critical infrastructure behavioural data. Our pattern detection approach, through use of observers and data classification, makes BOCISS dissimilar from the 'behaviour analysis for security' approach adopted by Singh *et al*.

Secondly, the use of anomaly detection in water management systems is discussed by Raciti *et al.*, [179]. Their research is motivated by the concern over the quality of drinking water and as part of the critical infrastructure grouping, water supply security is at risk from cyber-threats. Whilst security has improved and techniques, such as anomaly detection and misuse detection, are in place there is still weaknesses that need addressing. They detail that the use of SCADA systems offer a 'natural' opportunity to increase vigilance against threats.

Two of such weaknesses can be found in misuse detection and anomaly detection methods. In the case of misuse detection, the inability to identify attacks, which have not previously taken place meaning that it is always one step behind new and emerging attacks, is the main problem. However, in the case of anomaly detection, new attacks can be uncovered but there is a dependence on referencing behaviour back to a control model of normality [179].

Water provision is measured through a network of data sensors, which detect changes in quality and alert an operator. In their approach, Raciti *et al.*, propose the use of ADWICE (Anomaly Detection With fast Incremental ClustEring), a clustering algorithm, for the detection of anomalies in real-time. Much in the same way as BOCISS, ADWICE uses real-time data to detect changes rather than using past data-mining techniques [179]. The difference between ADWICE and BOCISS, is that ADWICE was developed for IP network anomaly detection. It also uses clustering as opposed to data classification techniques and feature selection must be pre-defined rather than the customisability provided by BOCISS through the use of an observer.

ADWICE develops a model of normality consisting of a set of clusters that represent all the observed normal behaviour. Each of the clusters is presented through a cluster feature which is a multidimensional and numeric vector consisting of a representation of feature in the data. Threats are subsequently identified by comparing whether the real-time clustered data is close to the existing model of normal behaviour clusters or not. ADWICE achieves this through the use of BIRCH which is a data mining algorithm used to conduct clustering over a hierarchy.

Sekar *et al*., present the use of real-time event monitoring in their research. Their approach can be developed into an effective way to secure critical infrastructures. It functions through the use of real-time analysis as opposed to post-attack evidence analysis. It involves the tracking of problems inside an infrastructure through the use of automatically initiated reactions which are programs they have developed to respond to occurring attacks.

They aim to isolate compromised components to prevent the problem from spreading and also trace the origins of incoming attacks. The use of a human operator is required, who has to respond when abnormal behaviour is identified in order to have an expert who can identify whether the threat is real or not and thus minimising false positives occurring. Their technique differs to BOCISS in that their approach focuses on the use of system-call observations through the development of their own specification langue called ADL (Auditing Specification Language). Using this language normal and abnormal behaviours are processed by monitoring system calls rather than monitoring physical behaviour and creating patterns through data classification techniques.

Sekar *et al*., refer back to the work of Ko *et al.,* who discuss the use of identifying changes in behaviour to identify previously un-encountered attacks [180]. In their research, Ko *et al*., present the use of analysing audit trails generated by the operating system to detect actions, which are specified as abnormal behaviour. Audit trails are records, which refer to instances where expected activities have been affected. They focus on the modelling of system behaviour by looking at the expected privileged programs and monitoring if the behaviour remains consistent. While there are certain similarities in their work, such as the reference to correct behaviour compared to actual behaviour, there are fundamental differences in their behaviour observation approach to that of BOCISS. Their approach differs to BOCISS in that it specifically monitors privileged program behaviours which are allowed to bypass that kernel's security mechanism in order to accomplish its take [180]. Their approach is low-level focusing specifically on the internal behaviour of specific programs, whereas BOCISS monitors the system behaviour as a whole.

Continuing the discussion on related research, Bass *et al*., discusses that much like how a human brain draws from multiple sources of information through use of sensory organs in order to make an informed decision, the use of data gathering from multiple sources (data-fusion) can help security systems be more effective. Confirming that current real-time IDSs are not advanced enough to detect many professional cyber-attacks, Bass *et al*., argue that the next generation of cyberspace IDSs will require the use of situational awareness in order to improve security. The fusion of data requires gathering from a variety of sources of information. One such technique discussed is Data Mining. Data Mining is the detection of hidden patterns based on previously undetected intrusions, where previously gathered data is filtered and organised into sets in order to detect previously undetected situational patterns and then used to develop new detection templates [45].

Data fusion combines data to create a clear picture. The data is combined so operators do not have to look at individual pieces of information but instead can get a clear picture from information being organised. In other words, large data are converted into manageable amounts. Large data is put into meaningful and smaller amounts. The concept of using situational awareness is an aspect, which BOCISS uses however, in the research being conducted by Bass *et al*., the focus is on post event analysis in contrast to real-time data processing. The technique of constructing the situational awareness is also fundamentally different in its approach.

Igor Nai Fovino *et al*, discuss that a standard NIDS (Network Intrusion Detection System) is composed of distributed sensors that are used for analysing traffic flow and that traditional NIDSs, such as Snort, are unable to understand application level protocols. However, recently a set of ad-hoc rules have been released in order to detect attacks on SCADA [85].

In addition to this, they propose an innovative approach to the design of IDSs with the aim of being able to detect complex attack on SCADA systems. Their approach combines signature-based intrusion detection with State-Analysis in order to provide security by keeping track of the state of the system. They mix together various countermeasures in order to develop an architecture for a SCADA communications system which is based on integrity, authentication, filtering, state detection and K survivability [85]. It functions by creating a secure channel between master and slaves with the addition of a filtering mesh, which operates with a SCADA and detects attacks through the analysis of packets of data. SCADA attacks can be considered extremely complex and are rarely composed of just one step [84], [181] which is one reason why a system which helps present an overall picture of events taking place by drawing from different sources of information would be ideal for combating complex multistep attacks.

Their approach differs to BOCISS in that, two specific types of intrusion detection approaches are combined to detect intrusions inside a secure channel, which has been created between the RTU and SCADA control. BOCISS simply builds on existing systems as they function to add to defence in depth. No alteration of system function is required. Their research also has a heavy focus on network data and packet analysis, whereas BOCISS relies on physical data and an observer unit to collect it.

4.4.2 EXISTING SECURITY RESEARCH

One of the main comparisons of BOCISS is with anomaly detection, which, as previously mentioned, is currently implemented by both IDS and UTM systems for safeguarding critical infrastructures. It functions by identifying security threats through detecting events which are out of the ordinary. However, it is prone to false positives due to the fact that unlearned behaviour can occur [119]. Specifically it functions by sifting through datasets and searching for patterns of data, which do not coincide with patterns which are expected [182].

There tends to be three different approaches to achieving anomaly detection. These include model-based, proximity-based and density-based. Model-based refers to the development of a model and the identification of objects which do not fit into the model as being anomalies. Proximity-based refers to the identification of objects which are far from other objects and thus being anomalies as they are irregularities in the clustering. Density-based refers to objects that are of low density and distant from their neighbours.

Each of these three techniques can be applied in three different types of anomaly detection which include unsupervised supervised and semi-supervised. Unsupervised refers to the construction of a dataset of behaviour based on how the system is functioning and anything which deviates from that function is anomalous. Supervised refers to the training of a data set based on two sets of data, normal and anomalous. BOCISS would mostly be comparable with supervised anomaly detection. Semi-supervised would be a combination of both approaches.

Anomaly detection operates by using a database of known behaviours and signals an alarm when changes occur. It is, however, prone to false positives due to subtle normal changes in behaviour when the system is functioning. Anomaly detection, however, is prone to several weaknesses [144], [179], which is why there is a significant amount of research being conducted into improving its effectiveness. The known weaknesses include: performing poorly when given high dimensional data; being prone to false positives and being overloaded with data.

Feily *et al.*, discuss the specific weakness anomaly detection has. They discuss that using it as an IDS results in the inability to detect IRC-based (Internet Relay Chat) attacks. Anomaly detection functions through identifying changes in network traffic anomalies however, in the case of IRC-based operations a threat such as a botnet, which has never been used before maybe be introduced the system and the anomaly detection may be unable to detect it [144].

Anomaly detection differs to BOCISS in that, anomaly detection looks for ‘outliers’ which is data that lies far away from other data points. BOCISS looks to identify more subtle changes in data and the classifiers used are able to be trained to identify more subtle changes in patterns of behaviour. Our system also filters the data through feature extraction and effective data classification to reduce false positive rates. BOCISS also looks at physical rather than both the network data and the data collected by the control system.

Other IDS techniques are not comparable with BOCISS. Misuse detection, for example, another IDS technique, relies on information from previous attacks to function meaning they are prone to less false positives but are one step behind new and emerging attacks. Signature-based detection, another common IDS technique, relies on a database of known attack signatures and it blocks known attacks from taking place. Whilst having the ability to counter existing threats and simple cyber-attacks, this approach also finds that it will always one-step behind new emerging attacks as their signatures will be unknown to it.

4.5 SUMMARY

Using behaviour analysis for security has effective results, as does using simulation for testing new and adaptive approaches to security. In an industrial environment, real-time monitoring is essential. Large numbers of physical parameters, such as temperatures, pressure, speed and flow rate factors must be taken into account. Using behavioural observational services would allow for fast identification of anomalies by monitoring the system functions and recognising patterns of behaviour.

The construction of a simulation allows for the generation of significant realistic data sets. Using this data we will propose a behavioural-based observation system which will support security in critical infrastructures. The data constructed through our simulation will be used for evaluating our system. In the following chapter, our system design, specification and functionality is put forward.

CHAPTER 5

BEHAVIOURAL OBSERVATION FOR CRITICAL INFRASTRUCTURE SECURITY SUPPORT

5.1 INTRODUCTION

The research presented in this thesis offers a way of supporting the security currently in place in critical infrastructures by using behavioural observation to add to the Defence in Depth (DiD). As this work demonstrates, applying behavioural observation to critical infrastructure protection has effective results [53], [167], [183]. Our approach is proactive and continually looks to identify patterns or behaviour, which is out of place in the ordinary operations of the infrastructure. In this chapter, our design for Behavioural Observation for Critical Infrastructure Security Support (BOCISS) is presented. This entails an outline of the design specification; a detailed discussion on the system architecture and an explanation of the system modes of operation.

5.2 APPROACH FOR BOCISS

The main aim of BOCISS is to provide operators with the ability to detect abnormal behaviours and identify subtle changes in activity. The system collects data and acts as a plug-in device, where it trains itself to identify normal behaviour and sound alarms when anomalous behaviour is detected. In addition, a user interface layer provides the user with the ability to interact with BOCISS and view alarms, in a similar approach to how current SCADA systems allow the operator to view system functions.

5.2.1 Design Specification

The system functions by registering itself with the infrastructure and extracting data from the network layer in blocks. Using this data to train classifiers, threats to the system are identified by analysing changes in behavioural patterns. Security is provided by maintaining the status quo rather than striving to be one-step ahead of new and emerging cyber-attacks. To achieve this, our system is required to:

- Be generic and adaptable to different critical infrastructure systems
- Provide the operator with an alternative view of system activity
- Act as a plug-in service
- Collect data from the system autonomously
- Learn system behaviour
- Identify system anomalies
- Identify specific attacks
- Alert the operator of attacks on the system

BOCISS offers an alternative approach to cyber-attack detection by operating independently of the control system and the security in place. Existing threat management systems are supported by using effective data classifiers to detect subtle behavioural changes in system behaviour. Issues, such as network slowing, are avoided by the fact that BOCISS has no control over network activity and therefore does not inhibit processing. In addition, there is no need to remain one-step ahead of existing attacks, as security is offered by maintaining the status quo of operational performance.

5.2.2 BOCISS Location

BOCISS fits into the control layer, which has direct cabled access to the network for data extraction. The network is generally closed and local to the infrastructure. Typically, physical data is collected from a huge variety of sources meaning different types of data will form part of the data collection. This data is also encoded in the required infrastructure protocol format.

It is this data, collected by the RTUs, which is extracted from the network and used to perform behaviour analysis. The active nature of BOCISS (unlike the passive technique used by many honeypots and UTMs) means that it actively searches and identifies patterns that stand out as being abnormal. Figure 6 displays how BOCISS fits into a critical infrastructure layout.

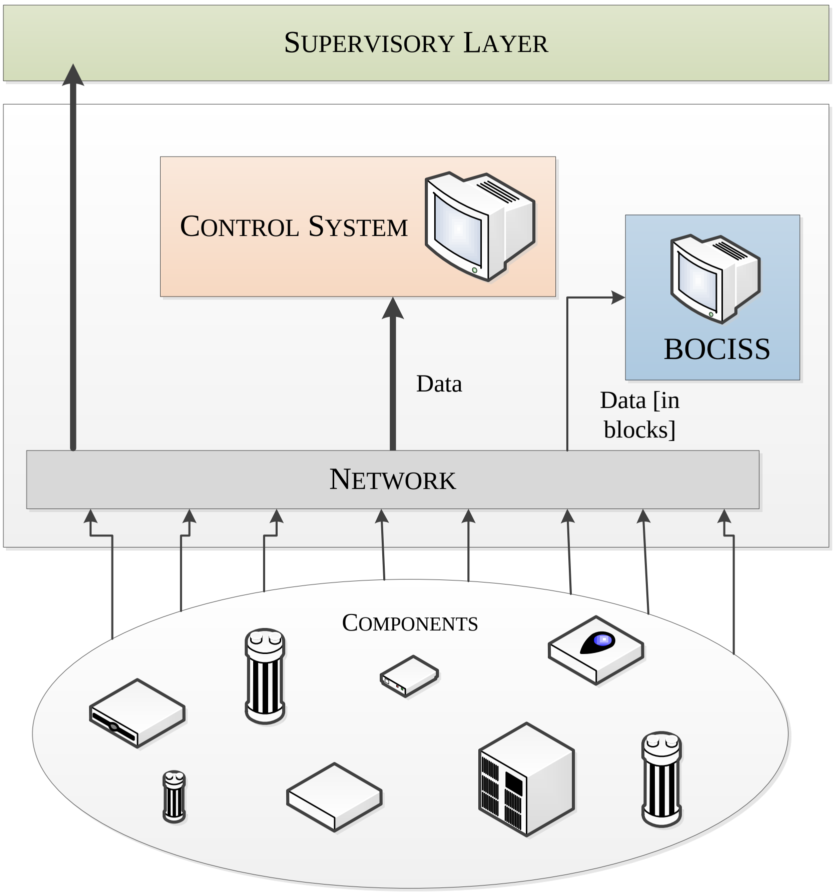


Figure 6 BOCISS Location

Figure 6 displays a snapshot of part of a critical infrastructure layout with the addition of BOCISS as a plug-in observer. Data collection continues as normal for the control system and BOCISS extracts data separately. Extracted blocks or windows of data are of a predesigned size and prevent data overload from occurring during extraction from the network. In acting as an observer and a separate entity to the control system, BOCISS provides autonomous system analysis.

5.2.3 DESIGN FUNCTIONALITY

In order to achieve its functionality, BOCISS operates in three different modes, all of which take place inside one observer, which extracts windows of data from the network. The modes of operation include: Data Collection, Training and Prediction. Each are discussed as follows:

Mode 1 - Data Collection: Once a substantial amount of data has been extracted, which accurately reflects infrastructure behaviour, collection is stopped. Two types of datasets are required, one when the system is functioning as normal and one when the system is under attack or behaving anomalously. The collection of abnormal behaviour data would be reliant on an operator or a piece of code running automated attacks and causing system disruptions. This could be, for example, changing component behaviour and causing system changes. The data sets are labelled as either normal or abnormal and stored in separate data stores.

Mode 2 - Training: This entails removing both the normal and abnormal data from the store and using extracted data features to train classifiers, which identify normal and abnormal system behaviour. This process is conducted autonomously after data collection is completed.

Mode 3 - Prediction: This is the real-time detection of system behaviour that is achieved by analysing data produced by system operation. The trained classifiers have the ability to detect abnormal behaviour and alert the operator if the classifiers detect abnormal behaviour. The extracted data is provided by multiple system components from the network layer. Figure 7 displays, in brief, the processes involved in the three modes.

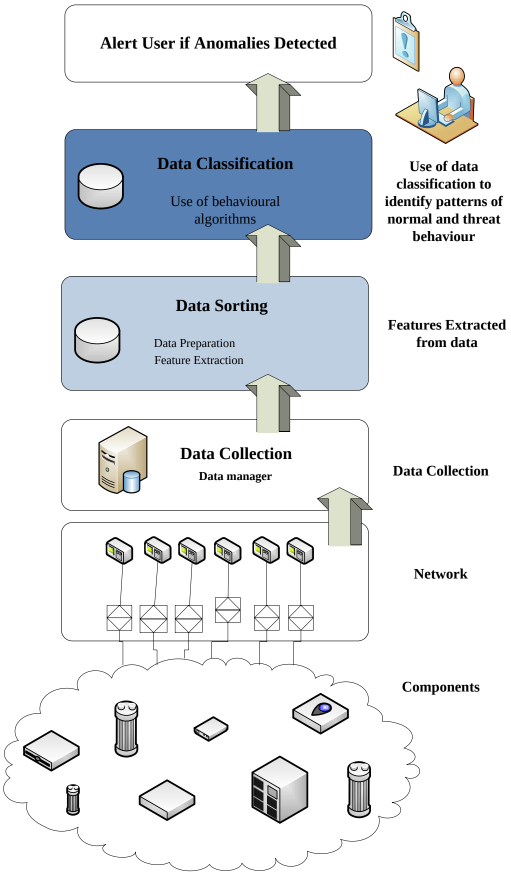

Alert User if Anomalies Detected
Data Classification
Use of behavioural algorithms
Use of data classification to identify patterns of normal and threat behaviour
Data Sorting
Data Preparation
Feature Extraction
Features Extracted from data
Data Collection
Data manager
Data Collection
Network
Components

Figure 7 BOCISS Process

The diagram shows how the system collects data, then sorts and classifies it, in order to identify normal and abnormal system behaviour.

5.3 BOCISS Architecture

A high-level view of the BOCISS observer design is shown in Figure 8, which displays the system architecture and interaction between the components.

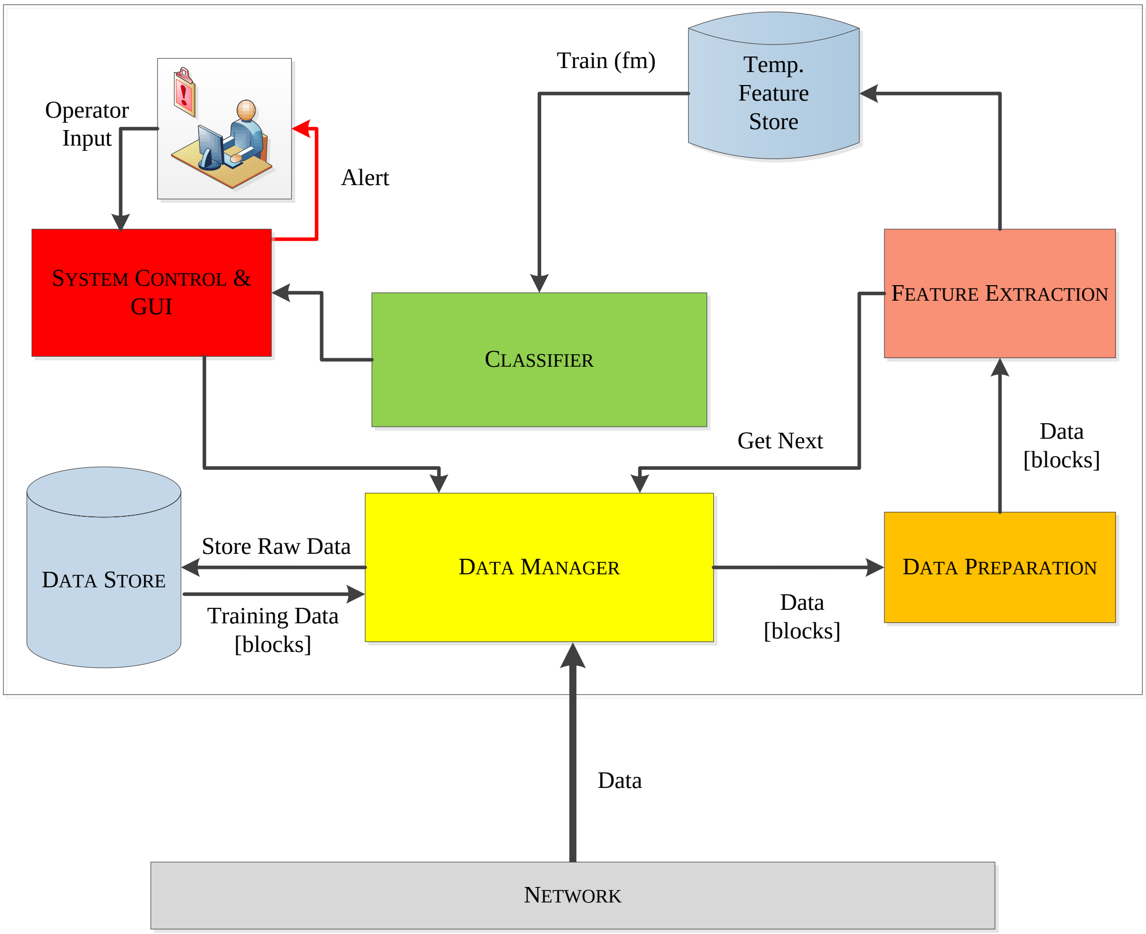


Figure 8 High Level System Design

BOCISS is composed of various mechanisms and data stores. After connecting to the Network Layer, BOCISS registers itself and begins data collection. Extracted network data is converted in the data manager and, depending on the mode of operation, is directed to the data store or for feature extraction. Features, initially sent to a temporary data store are used to create feature vectors and train classifiers to identify system behaviours. A system control governs the operations and interprets the classification results for the UI.

5.3.1 BOCISS PROCESS

Figure 9 displays a structural unified modelling language (UML) diagram for BOCISS and presents how the observer architecture functions when processing the infrastructure data. In the remainder of this section, each of the components are discussed in depth.

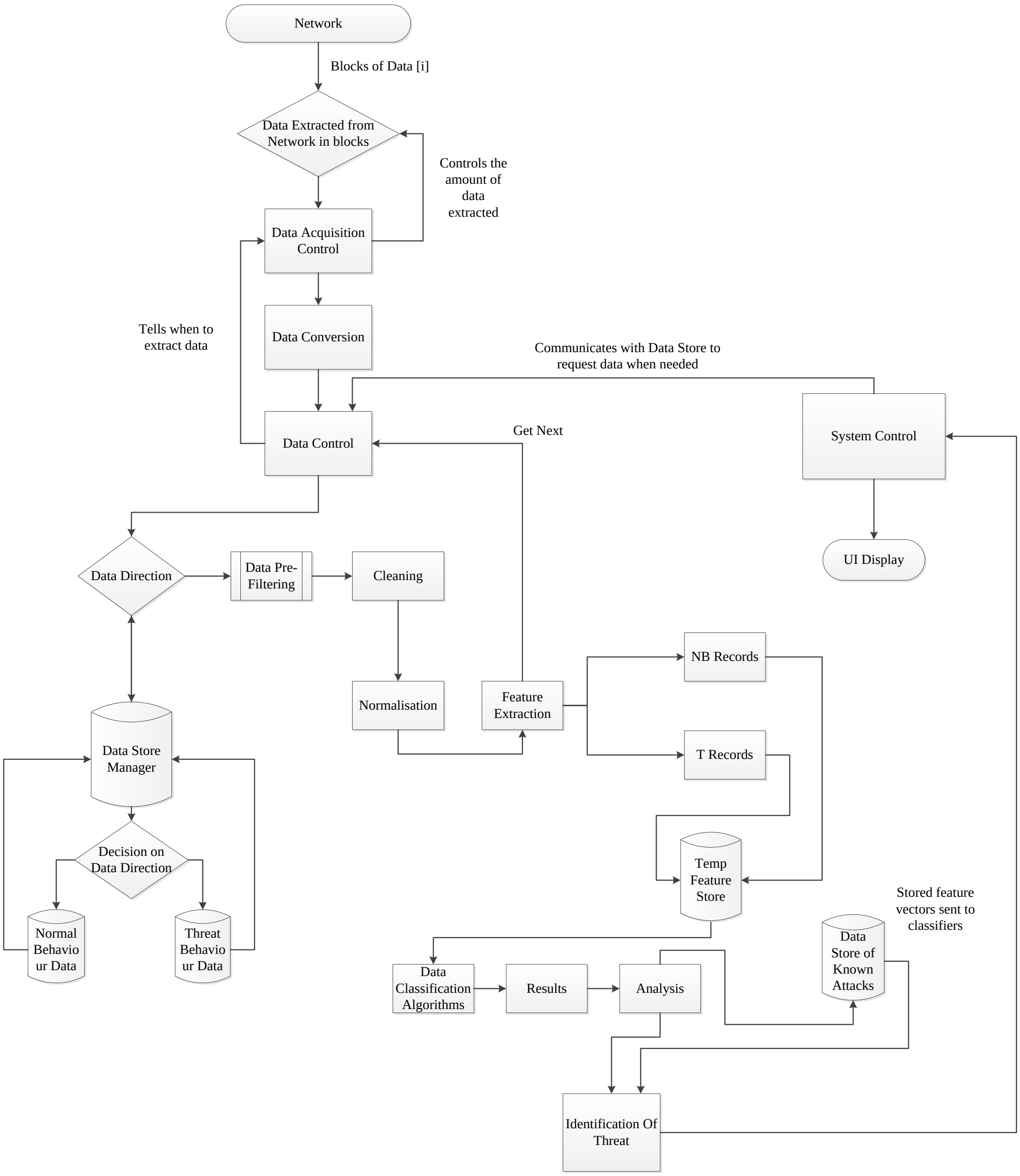


Figure 9 UML of BOCISS

5.3.2 DATA MANAGER

The use of a data manager enables BOCISS to act as a plug-in service. The data manager uses a data acquisition application (DAQ) and interprets the protocol-formatted data extracted from the network. A data acquisition application is constructed from a hardware component complete with a piece of software, which extracts data from a source.

Analogue values → RTU Conversion to Protocol Format → Data Sent to Network as I/O → BOCISS DAQ Data Collection

Two examples of protocol data formats include DNP3 and Modbus. Both are particularly used if the critical infrastructure uses a SCADA system. The data manager converts it to raw data using the data acquisition application and sends it either to a database, which is able to store both normal and threat behaviour separately, or to a feature extraction process.

Data I/O → DAQ Services → Raw Normal/Abnormal Data

Data extraction is an important procedure, which affects the scalability of BOCISS. Extracting data in blocks allows a control over the volume of data being collected and prevents data overload. Each of the processes, which take place inside the data manager, are shown in Figure 10.

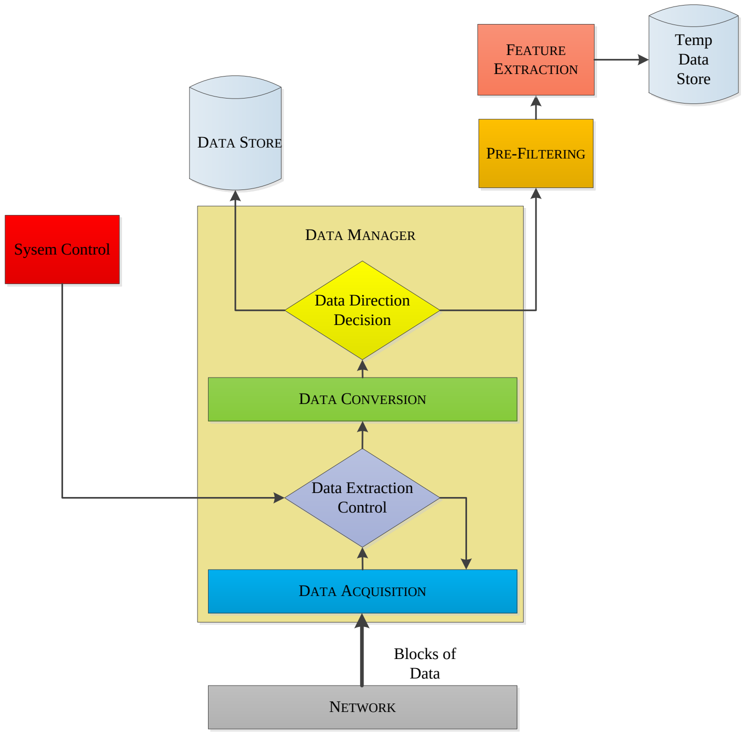


Figure 10 Data Manager

The data extraction control regulates the extraction of data from the network and informs the DAQ when data collection is required. Initially, converted raw data is given an ID tag for identity, depending on the BOCISS mode of operation. For example, if in training mode the data will be tagged as either normal behaviour or abnormal behaviour. This process is displayed in the class diagram in Figure 11.

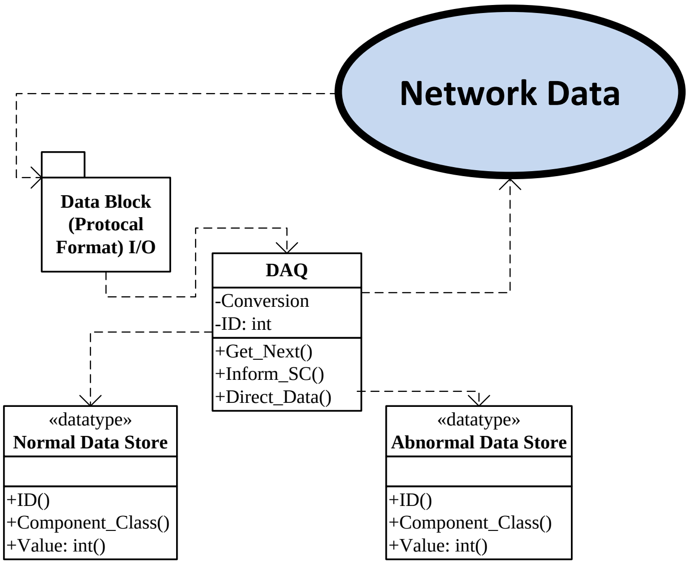


Figure 11 BOCISS DAQ Class Diagram

Protocol formatted data is extracted via a 'Get_Next' command and the collection process is governed by the system control.

5.3.3 System Control

One of the principal components is the system control, which regulates operations and notifies the data manager when to perform its data processing functions. The system control is required to execute a variety of functions, which include several key aspects, such as:

- Instructing the data manager to start or stop data collection.
- Allowing the user to input data collection requirements.
- Converting classification results to a format to present system behaviour via a user interface.
- Presenting threat identification to the operator.
- Comparing a detected threat with a database of known threat behaviours.

During each mode the system control is kept informed about system progress, in order to autonomously switch BOCISS between its three modes of operation. Figure 12 displays the system control.

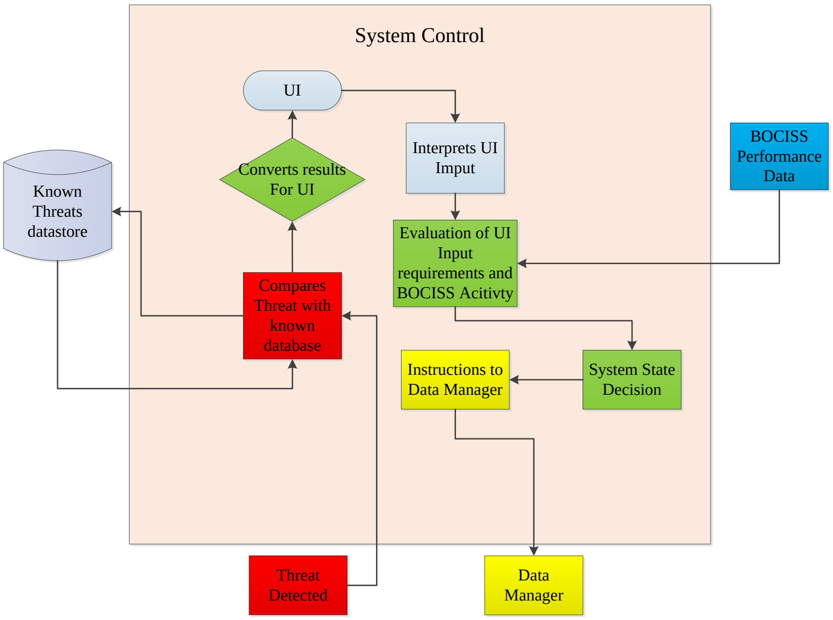


Figure 12 BOCISS System Control

Initially, the operator will define a period of time for the data collection mode. The system control will switch BOCISS to training mode once predefined data collection is completed. Prediction mode is enabled once the data classifiers have been successfully trained. If anomalous system behaviour is detected during run-time, the system control also compares behavioural patterns with a stored known database of threat behaviours and alerts the operator. This process is displayed in a class diagram in Figure 13.

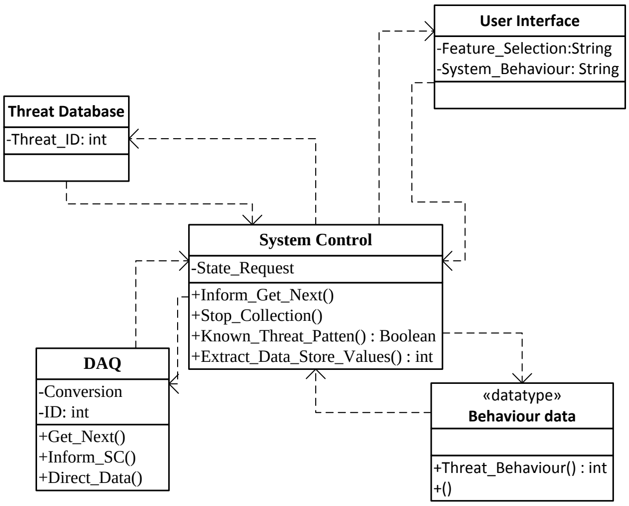


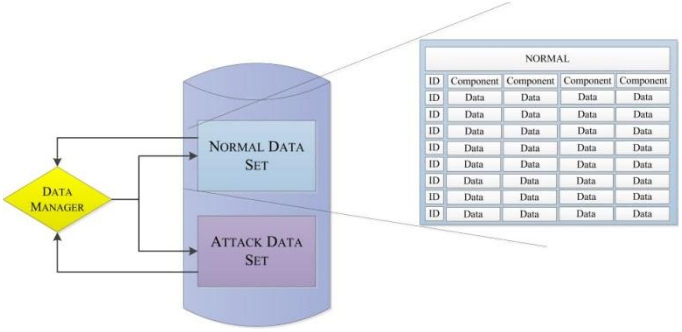
Figure 13 System Control Class Diagram

The system control requests the various system states, notably from the data manager and classifiers. Commands, including start/stop data collection are also issued by the system control.

5.3.4 Data Store

Once data extraction has been established by the DAQ, the data manager makes a decision about its destination. Data sent to the database will be directed to one of two deposits; one for normal behaviour and one for threat behaviour. The use of a database was chosen for several reasons. Mainly, because critical infrastructures commonly use databases for storing a retrieving data so its implementation offers consistency for a critical infrastructure.

The data is required to have an ID and specified location in the database. Each block of collected data is positioned in a row with a column for each component data is collected from. This is demonstrated in Figure 14.



NORMAL				
ID	Component	Component	Component	Component
ID	Data	Data	Data	Data
ID	Data	Data	Data	Data
ID	Data	Data	Data	Data
ID	Data	Data	Data	Data
ID	Data	Data	Data	Data
ID	Data	Data	Data	Data
ID	Data	Data	Data	Data
ID	Data	Data	Data	Data

Figure 14 BOCISS Data Store

The data manager extracts the data sequentially, based on the IDs, when the command to enter training mode is executed by the system control. The database process is displayed in Figure 15.

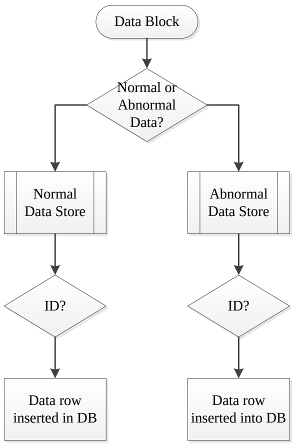


Figure 15 BOCISS Database Process

5.3.5 Data Pre-Processing

When in training or prediction mode, data requires pre-processing. This acts as a filter to remove unwanted values and clean the data prior to feature extraction. Pre-filtering the data extracts any elements that are not required by the feature extraction stage. Redundant values, which do not conform to the filter parameters and irrelevant aspects of the data are removed.

This process includes various stages, such as: cleaning and normalisation of raw data. Cleaning involves verifying that there are no missing values and smoothing data. Noisy data, which refers to corrupt and meaningless values, are also removed. The cleaning process also removes duplicated values; otherwise, the results of the data classification would be compromised. This could also include specifying a value range to cut out coefficients, which are outside the scope of our requirement. This process is displayed in Figure 16.

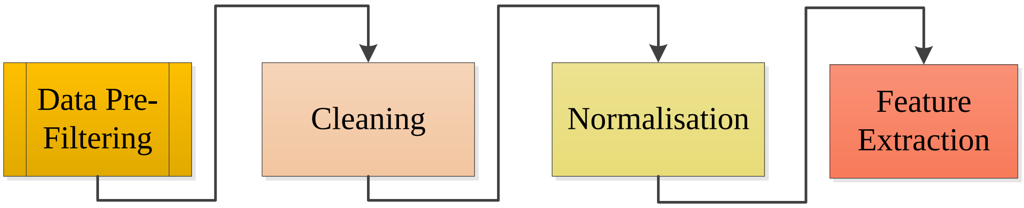


Figure 16 Data Pre-Filtering

In our system, normalisation is used to allow the classifiers to treat the data equally. In other words, the data is manipulated so that coefficients in the dataset are standardised. This prevents raw data values from over contributing to the classification process and affecting the results.

5.3.6 Feature Extraction

Features are aspects of the data, which allow for a representation of overall system behaviour. In the training mode, extracted features form feature vectors for both normal and abnormal behaviour. An example of a feature vector is displayed, which would contain information about system and individual component behaviour. The [id] labels the vector as either normal or abnormal behaviour.

[[id][component feature][component feature][component feature][component feature][component feature]…[.]]

The feature vectors are then stored in a temporary feature store until the data processing is complete. Once all the required data has been processed, a signal is sent to inform the temporary feature store to transfer its contents onto the data classifiers.

The features selected are unique for each critical infrastructure but they could include, for example, aspects such as: overall water volumes; steam output; energy creation; water tank levels or speed of water flow. They are constructed by cataloguing the data into designated representations of the dataset. This process is displayed in Figure 17.

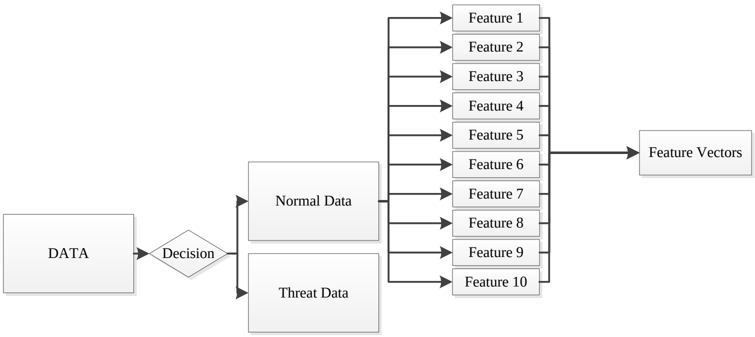


Figure 17 Feature Extraction

During training mode, a feature vector would be labelled with an ID, which would identify it as either part of the data set belonging to normal behaviour or abnormal behaviour. During prediction mode, the label would be unknown to the classifier and decisions would be made based on the patterns in the feature vector.

5.3.7 CLASSIFICATION

Classification is achieved using the feature vectors from the temporary feature store and by training the chosen classifiers to identify normal and abnormal system behaviour. Figure 18 displays this process, known as supervised learning.

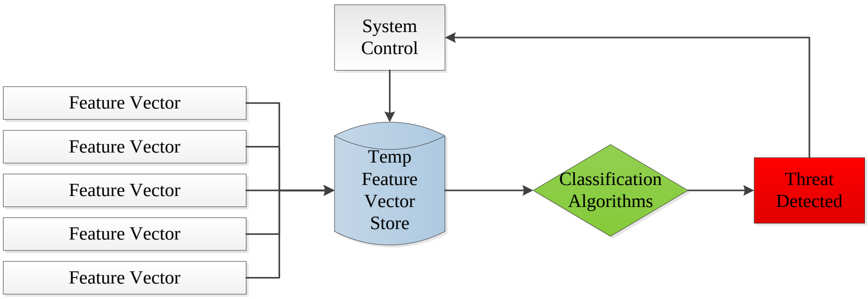
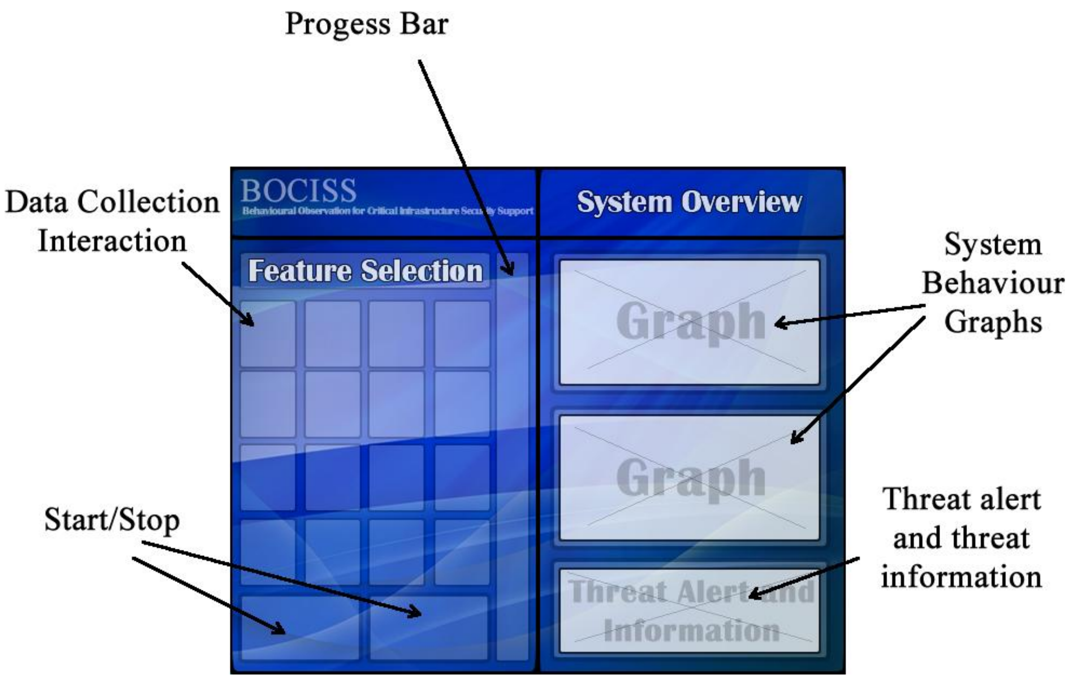


Figure 18 BOCISS Data Classification

Linear classifiers accurately provide a discrete output and divide the data into groups based on characteristics to identify changes in patterns of behaviour, which would otherwise be difficult to observe. Once the classifiers are trained, they are able to function self-sufficiently during run-time.

5.3.7 User Interface

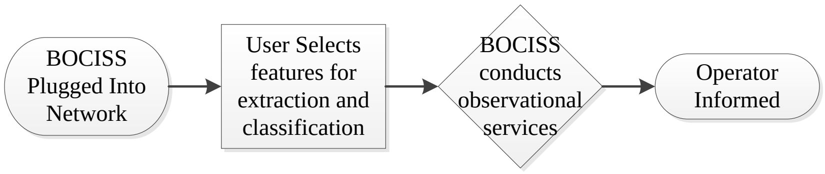
BOCISS has its own user interface, which allows the operator to interact with the system. The design of the user interface would be divided into two parts, as displayed in Figure 19. One to permit the user to insert system commands. The other to enable BOCISS to present system behaviour and threat alerts. Figure 19 displays how the user interface would function.



Progess Bar
Data Collection Interaction
BOCISS
Behavioural Observation for Critical Infrastructure Security Support
Feature Selection
System Overview
System Behaviour Graphs
Graph
Graph
Start/Stop
Threat alert and threat information
Threat Alert and Information

Figure 19 BOCISS UI Overview

The ability to insert data collection commands enables BOCISS to be generic and applicable to multiple types of infrastructure. Commands may include, the type of data extracted from the network or which features to construct from the dataset. Figure 20 displays the process flow for the user interface.



BOCISS Plugged Into Network
User Selects features for extraction and classification
BOCISS conducts observational services
Operator Informed

Figure 20 BOCISS UI UML

When threats are detected, an alarm is signalled. Details about the intrusion are displayed in the threat alert information box.

5.4 BOCISS Modes

The components discussed in the system architecture work together autonomously. In this section, a description on the three modes of operation, and how they function, is provided.

5.4.1 Data Collection

The data collection mode requires the use of the data manager, the system control and the data store. Data collection is conducted in two phases, when the system is functioning normally and when abnormally. Evenly sized datasets of both normal and abnormal behaviour are stored in the database. The stored data is used to supply data to the classifiers during training mode. The high-level view of the process, which takes place during the data collection mode, is shown in Figure 21 below.

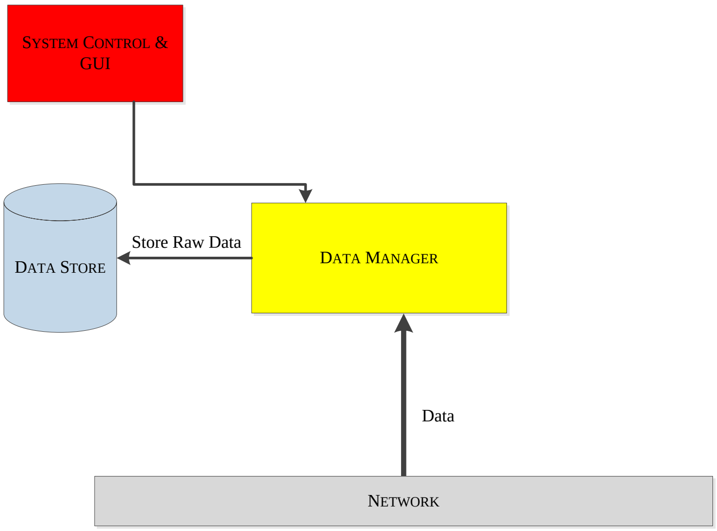


Figure 21 BOCISS Data Collection

Data collection is performed over a pre-defined time, for example a week or a month. The period is application specific, in order to establish an accurate overview of how the system behaves. As each is different, the period chosen will depend on what services are provided by the critical infrastructure.

Executing the data collection process is reliant on receiving a ‘collect data’ command from the system control. As previously mentioned, both normal and attack behaviour data are required. Both are collected during this stage. The data manager controls the flow and direction of data to the database. Figure 22 displays a class diagram for the data collection process.

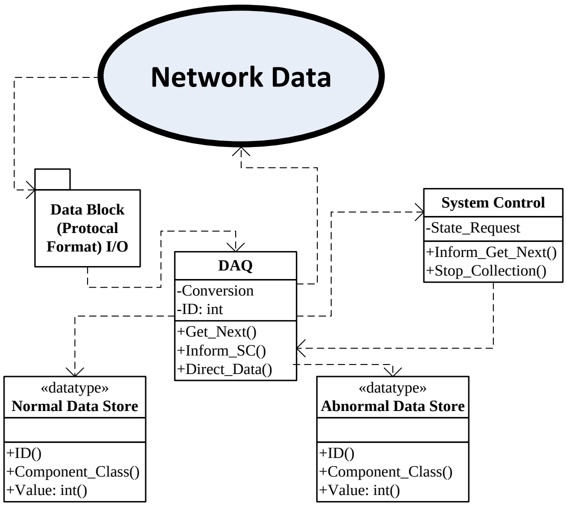


Figure 22 Data Collection Class Diagram

The system control monitors the level of data collection and terminates the process once the pre-defined level of data has been collected. Figure 23 illustrates the data storage process and how data is filtered to two separate storage locations depending on its type.

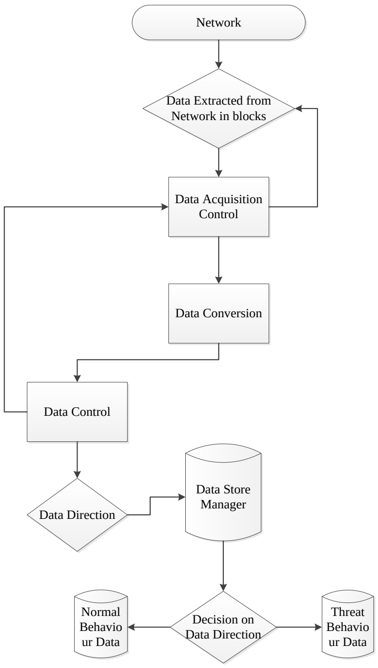


Figure 23 BOCISS Data Collection UML

Once the database is filled, the command is given by the system control to begin the training process.

5.4.2 TRAINING

The training mode involves extracting features from stored datasets. When the command is executed to begin training mode, data is extracted from the database and pre-processed. A ‘get next’ message is sent from the feature extraction process to the data manager until the data store has been fully processed. The extracted feature vectors, which have been stored in the temporary data store, are used to train the classifiers. The training process and the components involved, is displayed in Figure 24.

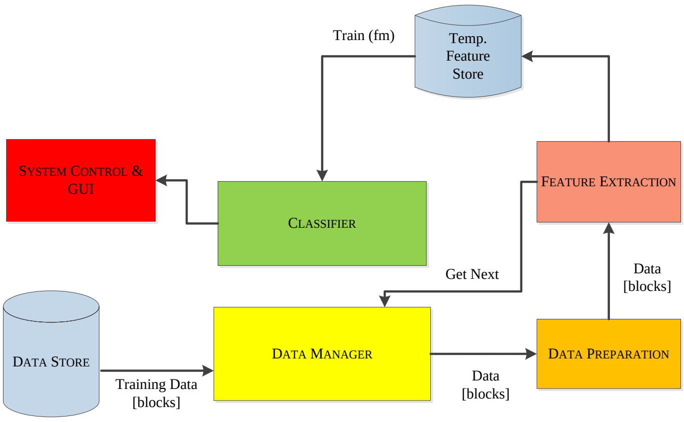


Figure 24 BOCISS Training Stage

This supervised learning stage requires the evenly sized data sets of both the normal behaviour and attack data. Figure 25 displays the processes involved in the training mode.

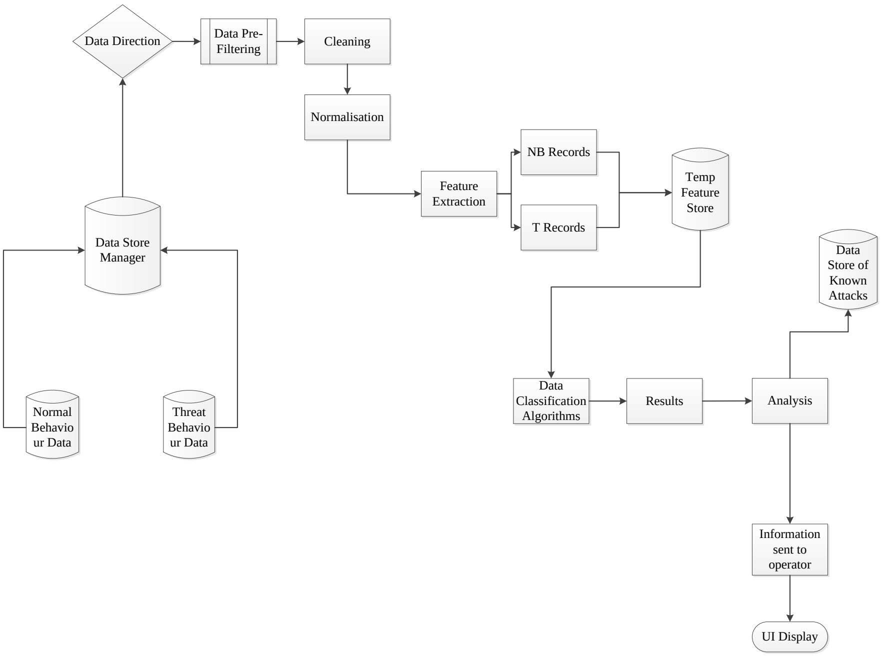


Figure 25 BOCISS Training Stage UML

When the classifiers are trained, they are able to operate autonomously and detect anomalies in data collected from the network in real-time. Completion of the data classification process is monitored by the system control, which sends a signal to the UI upon completion. Figure 26 displays a class diagram of this process.

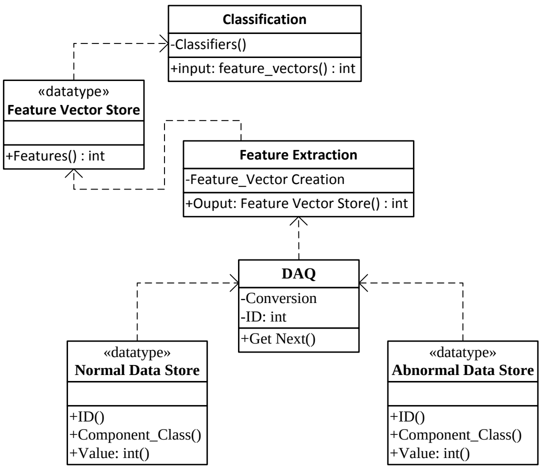


Figure 26 Training Class Diagram

Once the training is completed, BOCISS changes to prediction mode and operates in run-time to evaluate system behaviour.

5.4.3 Prediction

The prediction mode involves transferring real-time data to the classifiers, via the feature extraction process, in order to identify any changes in system behaviour. Figure 27 displays this mode of operation.

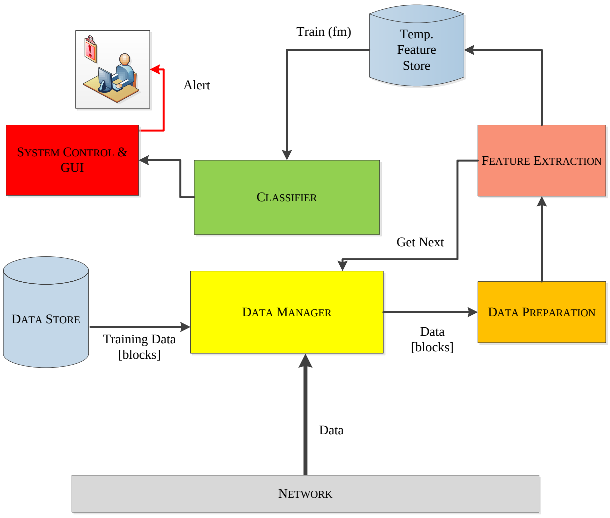


Figure 27 BOCISS Prediction Mode

Any detected changes in system behaviour would be the result of a cyber-attack taking place on the infrastructure. Data is, again, mined in window blocks from the network. Firstly it is pre-processed then features are constructed. These real-time features are then pre-trained by classifiers for analysis. Figure 28 displays the prediction mode process.

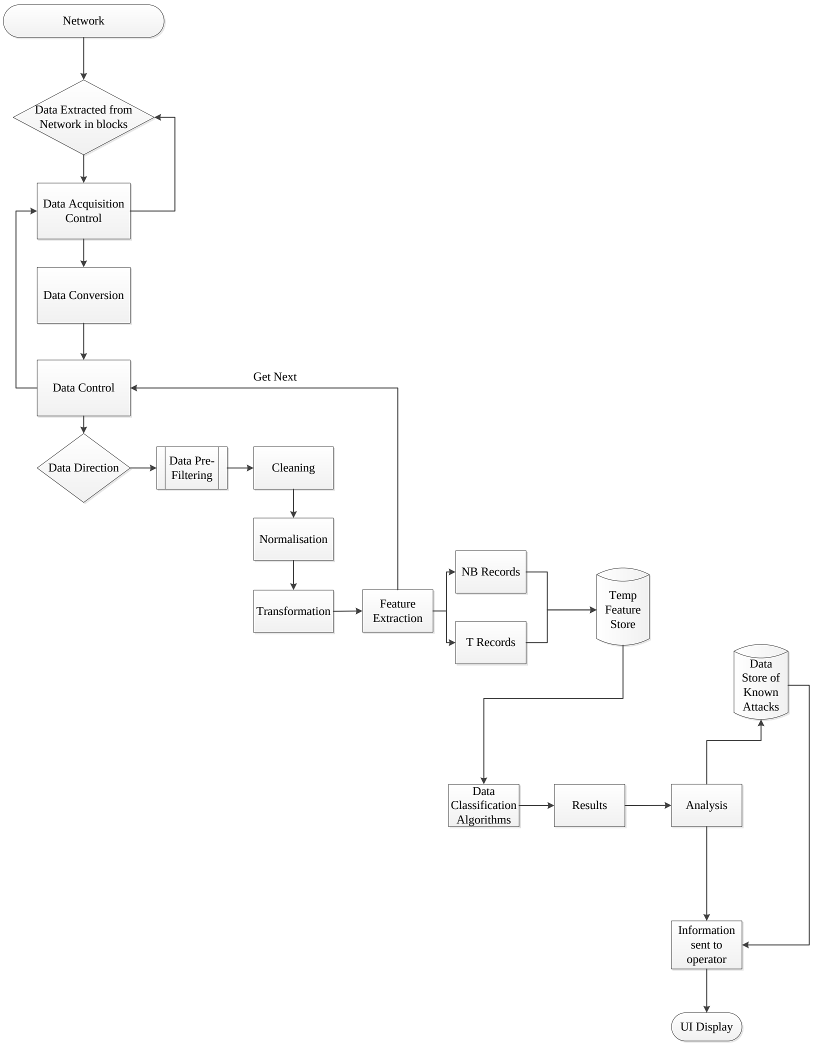


Figure 28 BOCISS Prediction Mode UML

The prediction mode is one of the aspects, which distinguishes BOCISS from other approaches to intrusion detection. Applying effective data classification algorithms to real-time data allows for the identification of subtle system changes in behaviour.

5.4.4 Attack Evaluation

As well as having the ability to detect threats, which are the result of anomalous behaviour, BOCISS can be adapted to identify specific attacks by recognising known behaviour changes and what is causing them. This approach differs from signature-based detection as it looks at physical changes in component behaviour and uses them to identify attacks, which are known to cause those changes. Traditional signature-based detection identifies known data signatures, such as globally known viruses.

The addition of a data store of known system behaviour when under specific attacks, allows for a comparison between identified threats and known threat behaviour. Information in the database would only be drawn from once a threat has been identified. If a comparison can be found then the operator is informed about the specifics of the attack taking place. Figure 29 displays how the added database of stored known patterns of behaviour is used to implement a known behaviour-based detection. The system control would perform the threat comparison function.

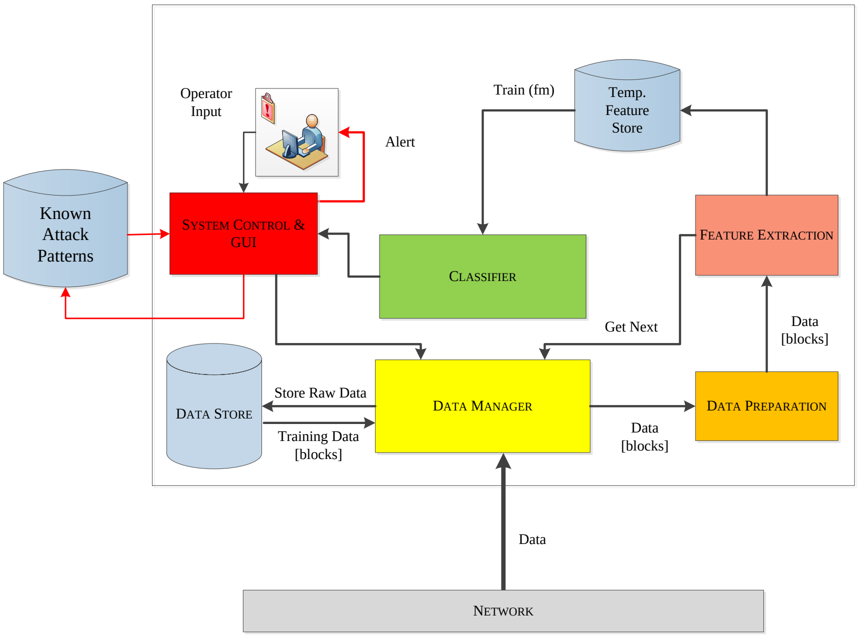


Figure 29 Signature Identification Addition

The database would consist of various sets of signatures, for example {A} to {Z}. If the identified threat set of signatures {C} matched one of the sets in the database then the operator would be provided with more information.

5.5 SUMMARY

The system presented in this chapter, improves critical infrastructure security by identifying threats, and unusual activity, through behavioural observation. Using this novel approach to identify system threats, a layer of security is added to the defence in depth.

In the following chapter, the development of a simulation of a nuclear power plant for the purposes of realistic critical infrastructure data construction is presented. The data is used for the evaluation of our system.

CHAPTER 6

NUCLEAR POWER PLANT CASE STUDY

6.1 INTRODUCTION

BOCISS requires a significant amount of realistic critical infrastructure data. This is provided by the development of a nuclear power plant simulation using Siemens Tecnomatix Plant Simulator and the programming language SimTalk. Using this simulation, realistic data is constructed and collected, when both functioning as normal and during a cyber-attack scenario. In this chapter, the assembly of the simulation is presented along with an account of how data is constructed. In addition, the data-preparation, feature extraction and classification stages of our system design are presented.

6.2 SIMULATION ARCHITECTURE

Pre-defining the design for the system is an essential first stage in simulation development. In particular, formulating a specification allows the architecture to be specified prior to the system being constructed. Our simulation is required to:

- Provide realistic critical infrastructure data.
- Provide consistent datasets that differ slightly each time the simulation is run.
- Allow the operator to extract large datasets in short periods of time.
- Allow data to be extracted from a large number of components.
- Provide physical system behaviour data.

- Be a process flow.
- Represent a critical infrastructure type.

Our aim was to construct a system, which can be used to provide realistic data about the behaviour of a nuclear power plant. Attacking a nuclear power plant has the potential to have a huge impact. For this reason, a simulation of a nuclear power plant would be ideal for constructing data and evaluating our system.

6.2.1 Simulation Design

The simulation provides different sources of data, as can be seen in Figure 30. The system consists of several mechanisms including, an external water source, two water storage tanks, a condenser, two pumps, a nuclear reactor, an emergency water tank, and a steam generator. Pipes are also included, which carry the water throughout the system where necessary. The design is based on a realistic nuclear power plant, which would contain each of the components in the design.

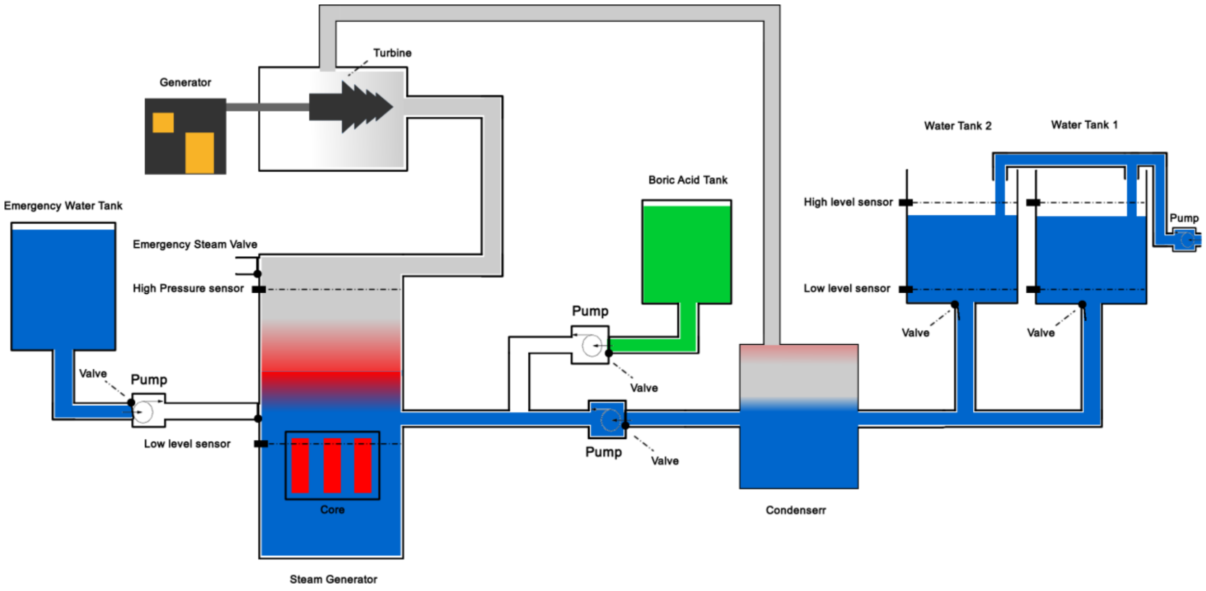


Figure 30 Power Plant Design

Each of the major system mechanisms are constructed by using a variety of components. The specifications for each are displayed in Figure 31 to Figure 35.

Firstly, the water source requires and infinite supply of water which is filtered for impurities before being passed to the water pipes. It would therefore consist of a network of pipes and a filtration system as displayed in Figure 31.

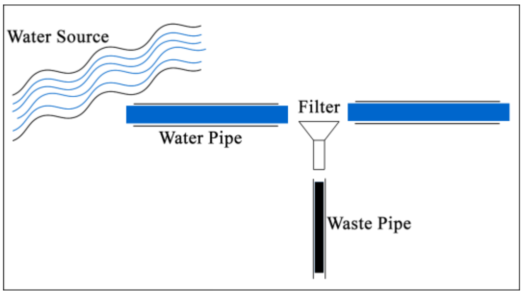


Figure 31 Water Source Design

Figure 32 displays the specification for the water tanks. The aim is to have two water tanks, which supply water to generate steam in the reactor, as well as acting as a coolant in both the condenser and reactor.

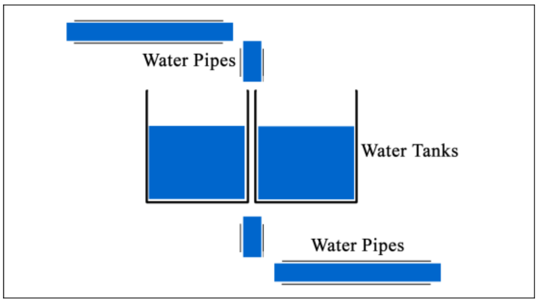


Figure 32 Water Tanks Design

A network of pipes maintains the flow of water to and from both tanks. Two pumps remove the water from the tanks at a steady rate into a pipe, which leads to the compressor where it cools the steam produced in the reactor core. The steam produced by the heat from the nuclear reaction is cooled in the condenser as displayed in Figure 33.

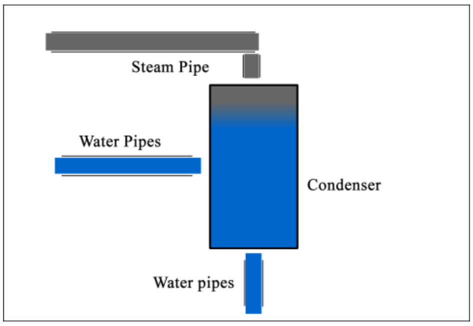


Figure 33 Condenser Design

Once cooled it is pumped back into the reactor where it is once again heated up into steam. Figure 34 displays the reactor system. The steam is released into a steam pipe and directed to the generator.

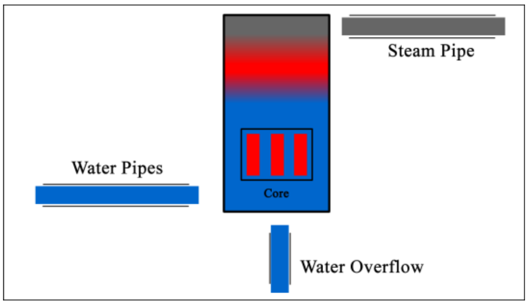


Figure 34 Reactor Design

The generator uses the steam to create electricity. The steam is returned to the condenser and turned back into water once cooled. Figure 35 displays the components, which make up the generator mechanism.

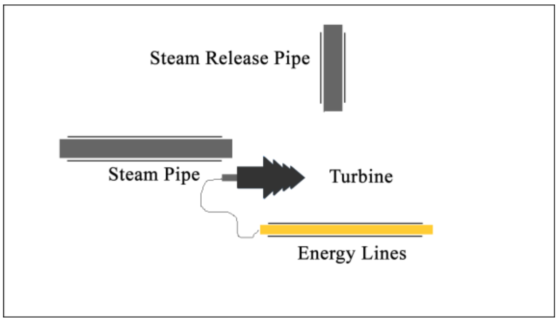


Figure 35 Generator Design

The steam then turns a turbine, which creates electric energy. This is known as a boiling water reactor (PWR) and is used to cool water and generate energy. Two further additions to the design include an acid tank and an emergency coolant tank both displayed in Figure 36

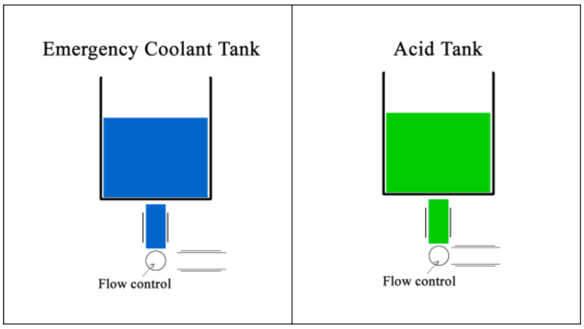
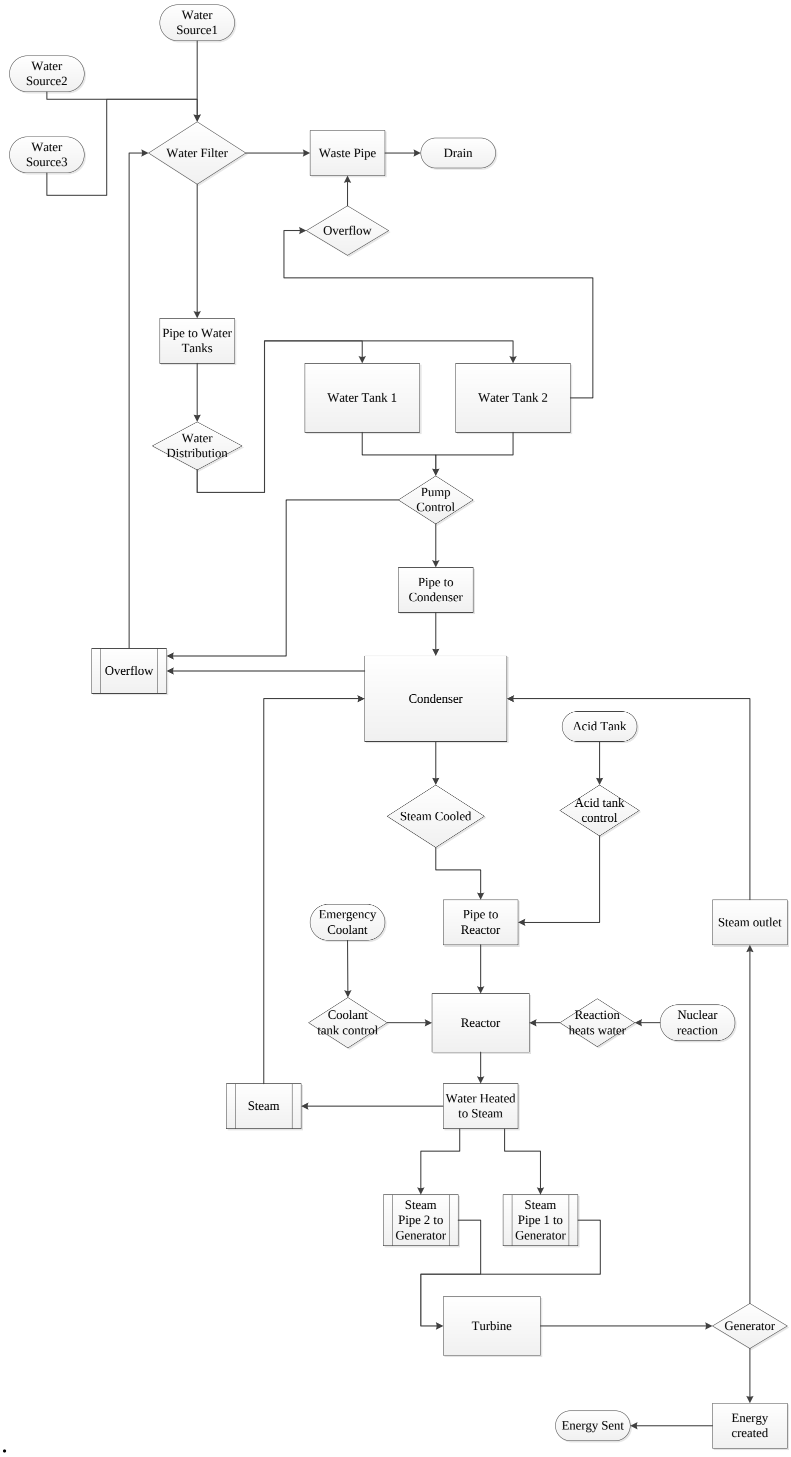


Figure 36 Coolant and Acid Tanks

Both the creation of energy and the cooling of the reactor are created using closed loops, which will be reflected in our simulation.

6.2.2 SIMULATION PROCESS

The process flow, displayed in Figure 37, sets out the various procedures, which are involved when the system is functioning.



.

Figure 37 Simulation Process Flow UML

The process flow identifies the simulation processes. In total, the system operates using four loops for water flow. There is a loop between the water sources and the water tanks. A second loop, between the water tanks and the condenser. A third loop between the condenser and the reactor and a final loop involving the reactor, generator and the condenser, where the water is in the form of steam. Figure 38 displays these four different loops and demonstrates how they are interconnected, with the arrows representing water flow.

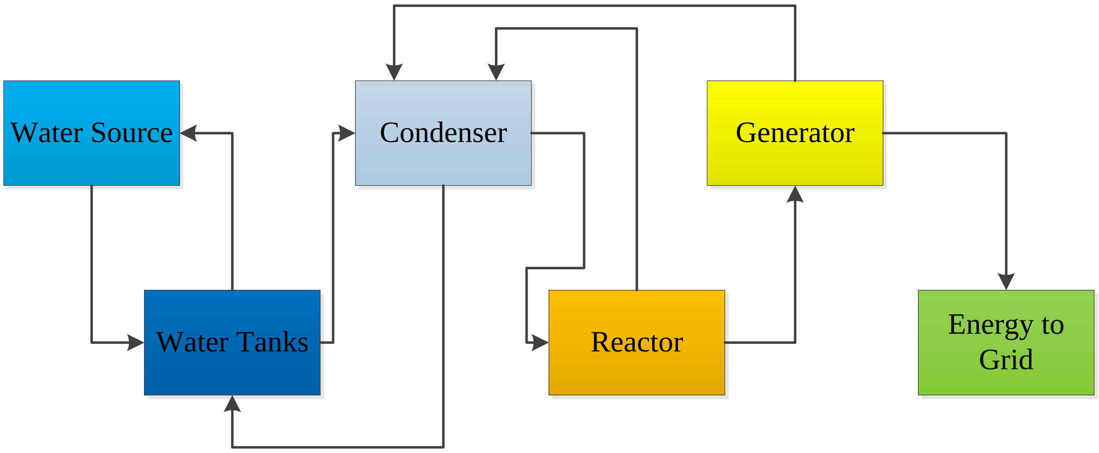


Figure 38 Simulation Process Loops

Errors or anomalous behaviour in one loop will have direct impact on another. A component failure in our simulation should allow the infrastructure to keep functioning but the effects of the fault will be visible in the dataset. In the following section, the construction of the simulation is presented using the Siemens Technomatix Plant Simulation Tool.

6.3 Power Plant Simulation

The Siemens Tecnomatix Plant Simulator is based on object-oriented modelling, where each component inserted is an individual object, which can be adjusted and used to construct data. In order to simulate our design we create and insert objects for each of the components, which together form our emulator.

6.3.1 Simulation Overview

Figure 39 displays our Tecnomatix interpretation of the system design. The diagram displays an overview of the whole system. Each of the mechanisms has a graphical icon to represent its function more clearly. They can also be expanded to detail their interconnectivity and the various components, which allow the system to operate. Each of the mechanisms are explained below.

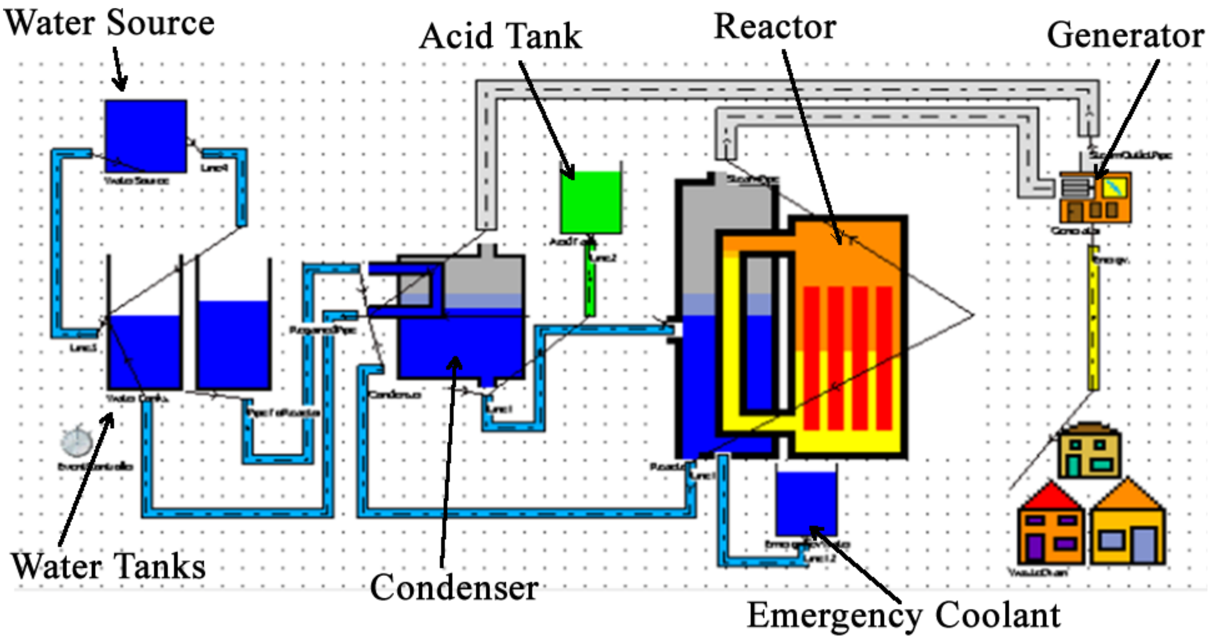


Figure 39 Simulated Power Plant

- The Water Source: The production of water is supplied by three sources including two infinite sources, representing a lake or ocean, and one water tower. The water requires filtering. It is, therefore, supplied to one large pipe, which is then sifted for impurities before being pumped into the Water Tanks.
- The Two Water Tanks: Water produced by the water source is collected in two tanks. This effectively acts as a buffer and controls the water flow in the system. Two pumps are used to send water from the tanks to the Condenser.
- The Condenser: One of the most complex mechanisms in the simulation is the condenser which consists of an interaction between two system loops. In the condenser, steam is cooled and converted to water and the water is subsequently sent to the reactor to be heated.
- The Reactor: The intake of water is combined with heat from a nuclear reaction to produce steam in the reactor mechanism. The steam is sent to the generator mechanism via two steam pipes.
- The Generator: Steam sent from the reactor rotates a turbine. Each unit of steam turns the turbine once and energy is produced. Excess steam is directed via a network of pipes to the condenser system for cooling.
- Acid Tank and Emergency Coolant: In case of system failure, two storage tanks, one containing Boronic Acid and one containing emergency coolant, are in place. The emergency coolant is required in the case of a failure in the provision of water to the reactor. The Acid is needed for emergency situations such as core overload as a result of cascading system failure.

The simulated power plant consists of a large number of components, including connections and interfaces. Its assembly, configuration and each of the components, is discussed below.

6.3.2 Controlled System Failures

In the simulation, each of the components has a random failure implemented and a specified time to repair. However, the system should not stop functioning if one of the minor components has a fault. Random failures are implemented using an Availability Percentage. The Availability Percentage refers to the chances of a machine or component being ready to use at any given time taking into account failures and blockages. It is calculated using the formula:

$$Availability = MTBF/(MTBF + MTTR) \tag{1}$$

Where MTTR is the Mean Time To Repair and MTBF is the Mean Time Between Failures. The implementation of random failures is intended to reflect realistic unexpected component malfunctions, which occur in all infrastructures. However, due to the fact that power plant systems are designed to be enduring, the failure percentage in the system components was kept low.

When constructing the anomalous behaviour dataset, this approach allowed us to affect system behaviour and the data produced. By implementing more extensive system failures, orchestrated attacks can be conducted on the simulation in order to construct a data set, which would be similar to that of a cyber-attack taking place.

In the following subsection, the power plant mechanisms are presented in detail along with their customisation, coding and availability percentage.

6.3.3 Power Plant Mechanisms

The mechanisms used to form the simulation are created by editing and linking together objects from the Siemens Tecnomatix Simulator Toolbox. The objects in the toolbox are customised and attached together using the Connector tool which creates a relationship between the entities. After adding all the required components to form each of the mechanisms, the settings of each require defining. Aspects such as processing times, capacity, failures and repair times are adjusted by double clicking on an object. In this section, the set up for each of the individual components used to form the system mechanisms are presented.

The following, Figure 40 to Figure 51, display the components, which constitute the mechanisms in the simulation. Initially, the Water Source is displayed in Figure 40. Water generation consists of two infinite sources of water, for example the sea or a lake, and a third source, a Water Tower. Generated units of water circulate around the power plant via a network of pipes. The water is supplied into one large pipe, which is then filtered for impurities and pumped into the Water Tanks. All waste removed from the water is sent down a drain and discarded.

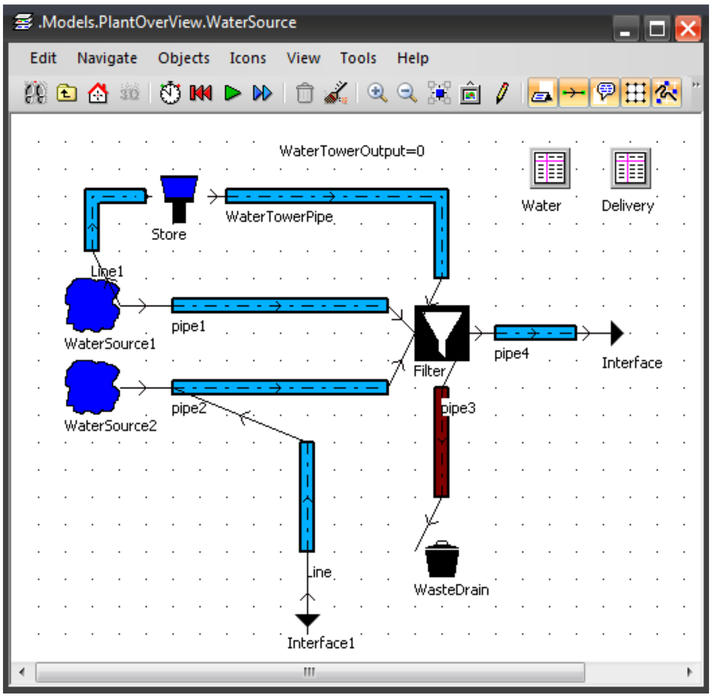


Figure 40 Simulation Water Source

Water is produced by the first infinite source at a rate of one unit every 0.2 of a second with a regular and constant stream. The second infinite source produces water every 0.5 of a second. The water tower only produces water if needed and acts as a backup for discrepancies in the collection of water from natural sources. The Water Tower has a flow rate of one unit every 10 seconds.

However, the Water Tower has a limited production of water and can only supply for the duration of 10 hours if needed. 1 unit of water represents 1 litre in our system. The generation of impurities in the water was set to 1% meaning that the level of discrepancies remained small but had to be monitored by the water filter.

The provision of water to a power plant is highly critical and for that reason systems are developed to be fault resistant. However, the intake of water is dependent on the natural environment remaining constant. For that reason faults in the water intake do occur but remain rare. The previously mentioned example of a jellyfish bloom blocking up a water intake pipe at the Torness nuclear power plant is a good example of this.

In order to reflect this in our simulation, the fault level for the water intake mechanisms were set to a low level to ensure faults were possible but extremely exceptional. It would also be the case that water intake faults would be costly and require a considerable amount of time to fix. For that reason faults would be extremely rare, occurring only 0.01% of the time during simulation, but take 1 hour to repair.

The process involved in the production of water is displayed in Figure 41 and in a class diagram in Figure 42.

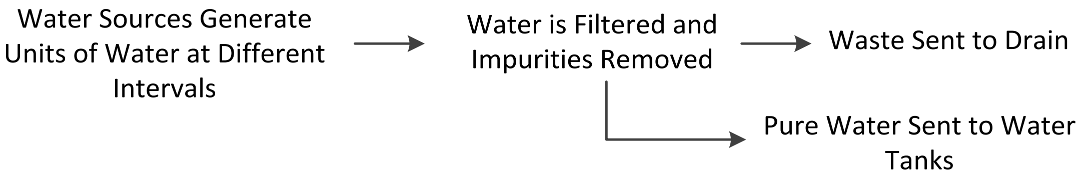

Water Sources Generate Units of Water at Different Intervals
Water is Filtered and Impurities Removed
Waste Sent to Drain
Pure Water Sent to Water Tanks

Figure 41 Water Source Process

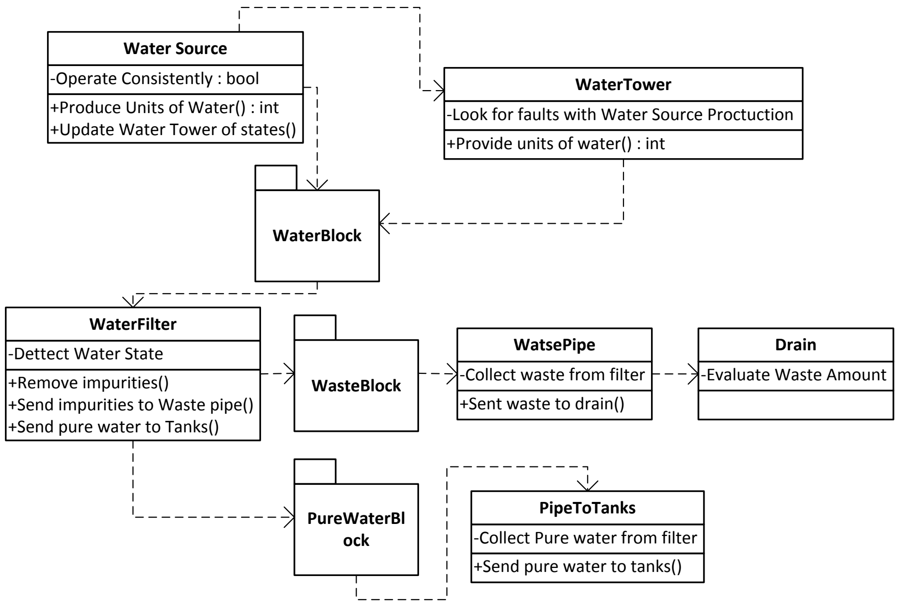

Water Source
-Operate Consistently : bool
+Produce Units of Water() : int
+Update Water Tower of states()
WaterTower
-Look for faults with Water Source Proctuction
+Provide units of water() : int
WaterBlock
WaterFilter
-Dettect Water State
+Remove impurities()
+Send impurities to Waste pipe()
+Send pure water to Tanks()
WasteBlock
WatsePipe
-Collect waste from filter
+Sent waste to drain()
Drain
-Evaluate Waste Amount
PureWaterBl ock
PipeToTanks
-Collect Pure water from filter
+Send pure water to tanks()

Figure 42 Water Source Class Diagram

Using a FlowControl ensures that a constant stream of water is sent to the water tanks via one main pipe. Figure 43 displays the components, which constitute the Water Tank grouping. It consists of two storage tanks, with a pipe leading from each tank and the flow controlled by two pumps. The pumps are implemented using Pick and Place objects from the Toolbox. The tanks provide water, in a steady stream, which is used for cooling the reactor. The storage size of each tank is set to 100 units, in our simulation this refers to a capacity of 100 litres of water.

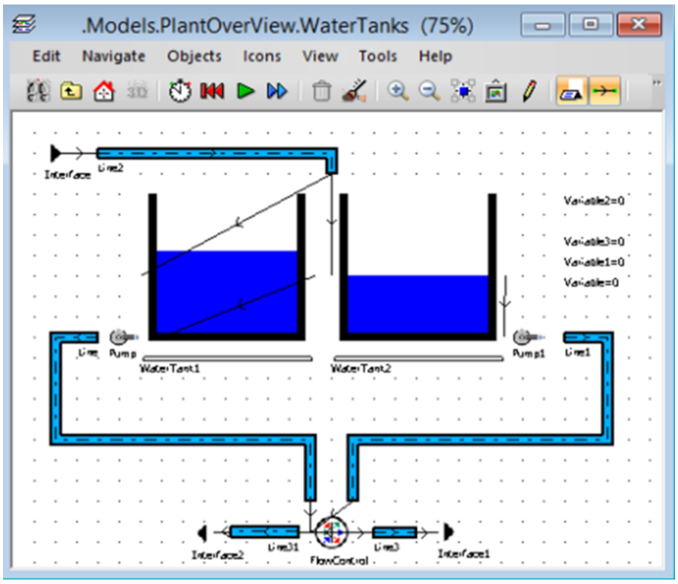


Figure 43 Simulation Water Tanks

The water is also pumped into the condenser to cool the steam. The water distribution is controlled by an additional FlowControl, which gives tank 1 priority over tank 2. The water flow process for the water tank system is displayed in Figure 44. One additional aspect is the collection of overflow water from the tanks, which is offloaded to an overflow drain.

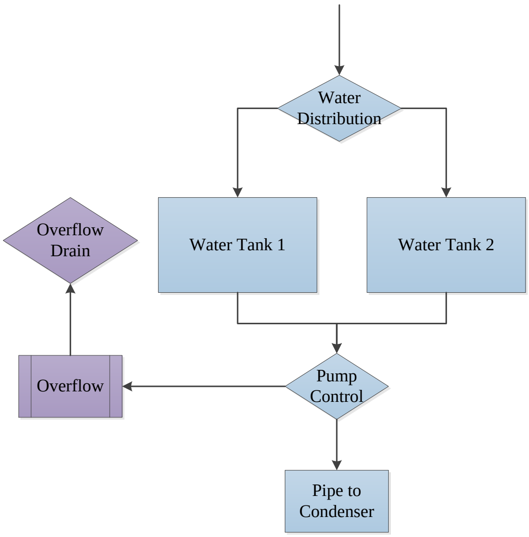


Figure 44 Water Tanks UML

Similarly to the water source production, the failure level in the water tank system is expected to be extremely low so failures were set at 0.01%. The system is able to function sufficiently with only one of the tanks in operation. The likelihood of both tanks failing is extremely low. Water from the tanks, is pumped to the condenser and then to the reactor core. Figure 45 displays the condenser system and Figure 46 displays the processes, which take place.

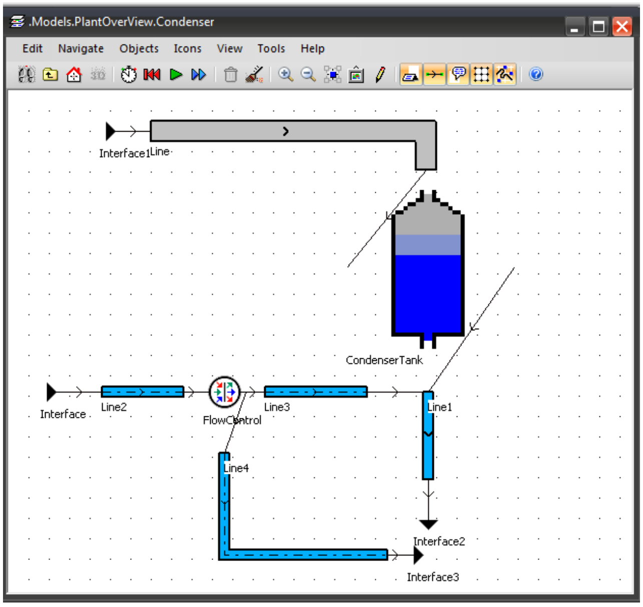


Figure 45 Simulation Condenser

Steam passed on from the generator is cooled in the condenser. The water from the condenser is also used to maintain temperature in the reactor and prevent it from overheating. In doing so the water is also turned into steam which is used by the generator to create electricity.

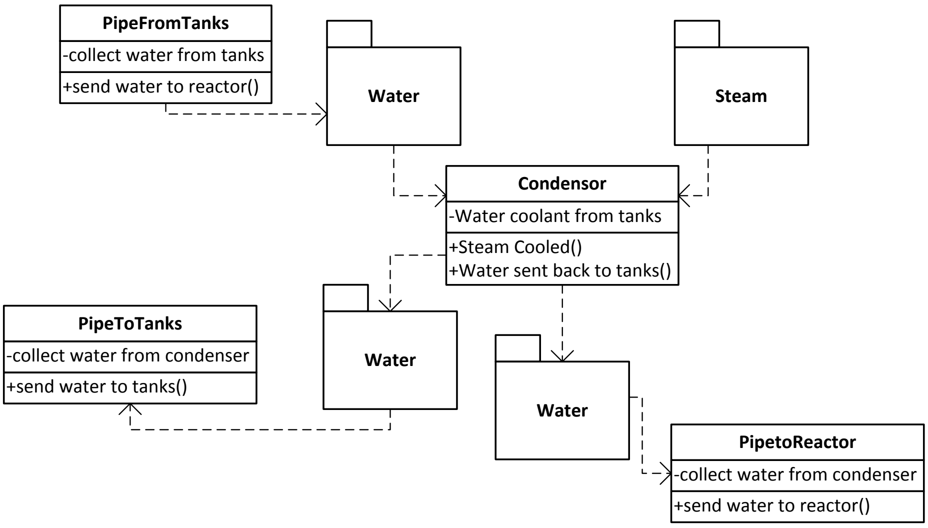


Figure 46 Condenser Class Diagram

The condenser system is made up of a steam pipe and four water pipes created using Conveyor Lines from the Siemens Toolbox. The main condenser unit consists of an Assembly Station, which combines one unit of steam with two units of water to cool the steam and turn it back into water.

Nuclear power plants have storage tanks containing Boronic Acid. In cases of emergency, the reactor core is flooded with the acid to prevent extensive radiation leakage. Figure 47 displays the acid storage and emergency water tanks, which is connected directly to the reactor.

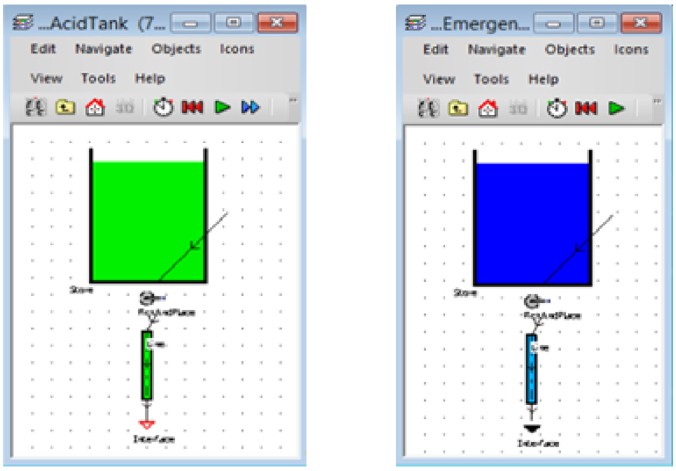


Figure 47 Simulation Acid and Emergency Water Tanks

Both mechanisms consist of a storage unit containing 100 units of the relevant liquid and are controlled by separate Methods, which instruct pumps to distribute the liquid into the system if needed. The code for both the emergency and acid tanks is similar and available in the appendix.

The Reactor combines the intake of water with heat from a nuclear reaction to produce steam and supply it to a generator via a steam outlet pipe. Figure 48 displays the construction of the reactor.

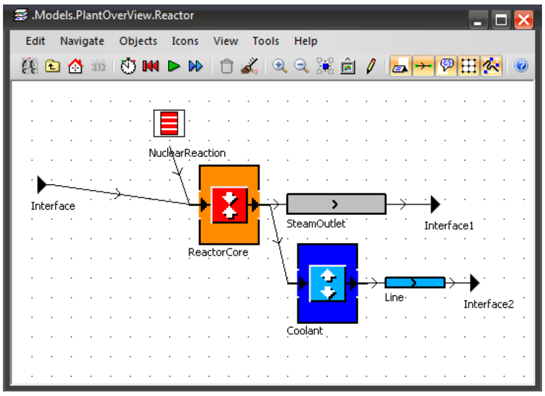


Figure 48 Simulation Reactor

A Source component is inserted to generate the Nuclear Reaction, which is combined with units of water in an Assembly Station to produce units of steam. The steam is output to the main steam outlet pipe, consisting of a Conveyor Line. In a nuclear power plant the water acts as a coolant for the reactor, some water is therefore recaptured as it is not turned into steam and sent back for reuse in the condenser mechanism. The recaptured water is extracted using a disassembly station, which removes units of water from the reactor assembly station output.

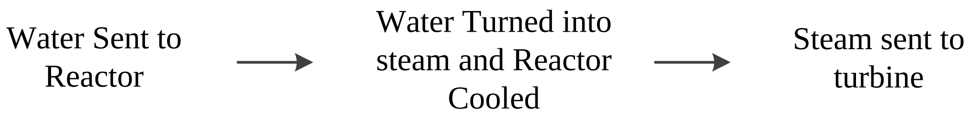


Figure 49 Simulation Reactor Process

In the reactor grouping, this is achieved using a disassembly station to collect left over units of water. The water is released back to the condenser via a pipe. This process is displayed in a class diagram in Figure 50. Any errors occurring in the reactor core would be catastrophic. However, errors are possible but often the result of a failure from a natural phenomenon. For that reason, the likelihood of errors occurring in the reactor core components are set at 0.01% as with the other components

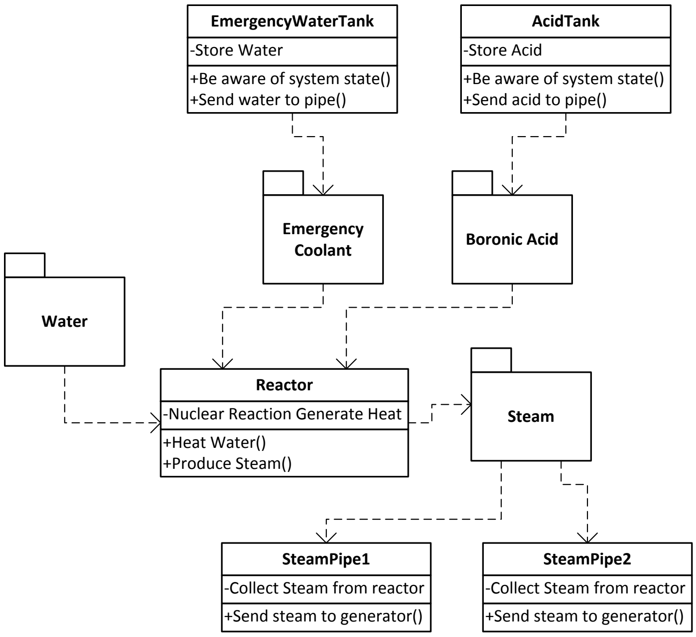

EmergencyWaterTank
-Store Water
+Be aware of system state()
+Send water to pipe()
AcidTank
-Store Acid
+Be aware of system state()
+Send acid to pipe()
Emergency Coolant
Boronic Acid
Water
Reactor
-Nuclear Reaction Generate Heat
+Heat Water()
+Produce Steam()
Steam
SteamPipe1
-Collect Steam from reactor
+Send steam to generator()
SteamPipe2
-Collect Steam from reactor
+Send steam to generator()

Figure 50 Simulation Reactor Class Diagram

In this case, the component repair times are a lot lower and set to 15 minutes. This is to represent an operator reacting quickly to a critical component malfunction.

The Generator and Turbine mechanisms are displayed in Figure 51. The grouping consists of two steam pipes into which the reactor supplies steam and a turbine, which is turned by the steam entering the system. Each unit of steam turns the turbine once.

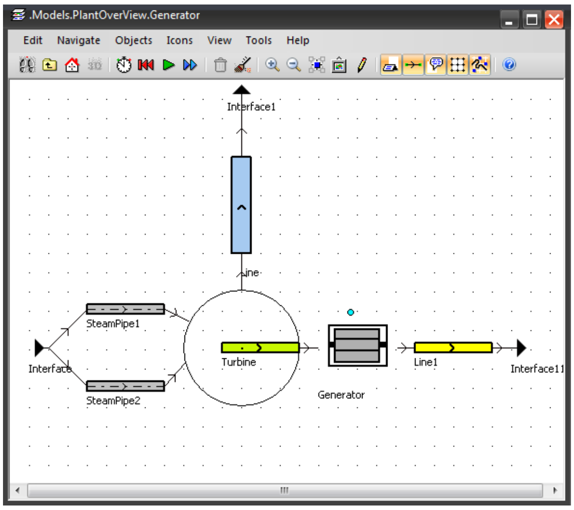


Figure 51 Simulation Energy Generator

The action of rotating the turbine produces energy in the generator, which consists of an assembly station combining units of steam to create electricity. The amount of energy produced can be measured. The excess steam is offloaded into a steam pipe and directed to the condenser where it is cooled and turned back into water. This is achieved by creating a distribution table to instruct the turbine to offload 75% of units into the generator and 25% of units into the steam outlet. This prevents the generator from being overloaded and unable to process all the units of steam. This system process is displayed in Figure 52.

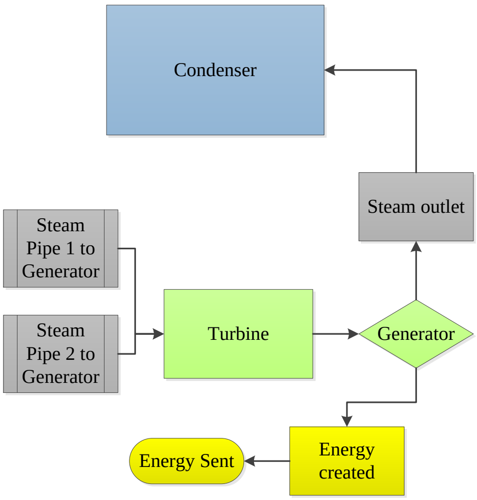


Figure 52 Generator UML

As the reactor core produces a large volume of steam very quickly, there is a risk that pressure in the steam pipes could become too high. For that reason, if an overload of steam is detected, the steam is diverted to the steam outlet pipe and sent back to the condenser. The code to achieve this is available in the appendix.

6.3.4 Simulation Visualisation

When linked together, the system functions, as shown in Figure 53. The individual blue blocks represent a visualisation of water flow. The grey/blue blocks represent steam and the yellow blocks represent units of energy. Exiting the generator, the energy is supplied to the output (represented by houses) and productivity is measured.

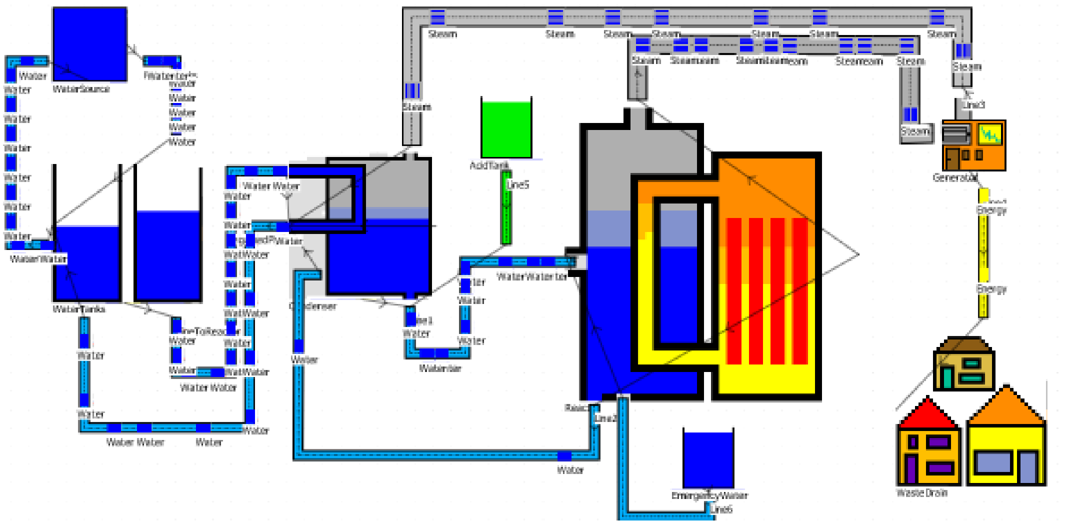


Figure 53 Simulation System Functioning

The system functions smoothly and consistently. However the output and behaviour differs slightly every time the system operates resulting in variance in datasets. The flow of material in the system can be demonstrated in a Sankey Diagram, represented by the thick redlines, which is a way of providing a quick visualisation and flow of the system.

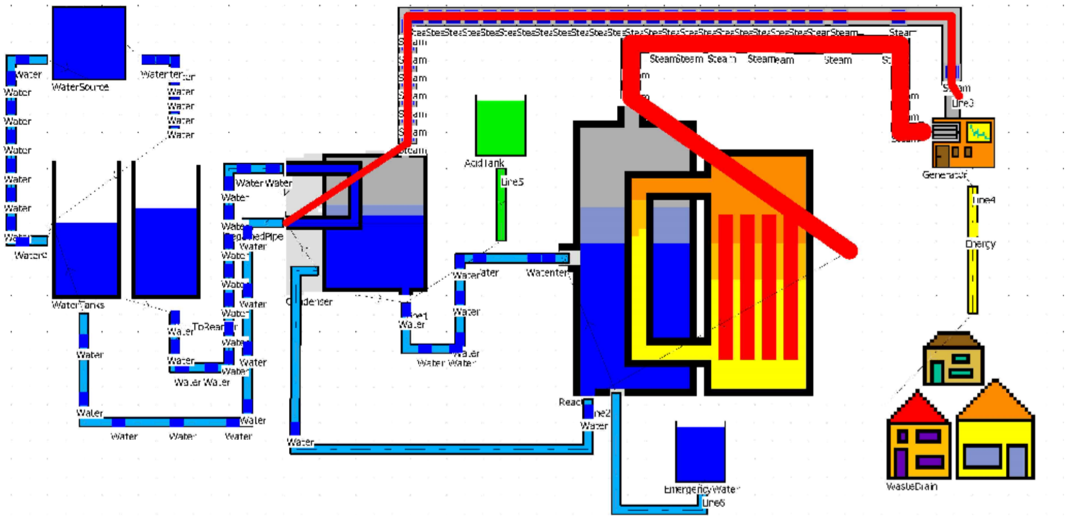
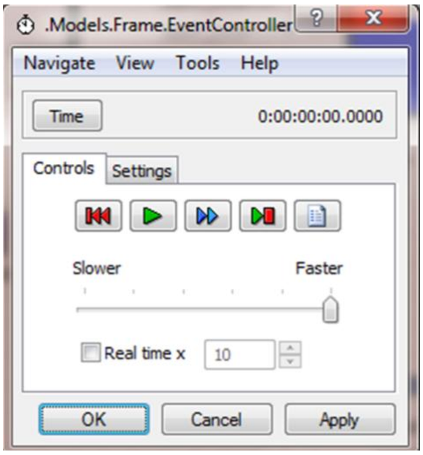


Figure 54 Simulation Sankey Diagram of Steam Flow

In Figure 54, the Sankey diagram shows the flow of steam throughout the system represented by the thickness of the red lines. The thicker the line, the more traffic passes between the connection. As Figure 54 displays, the heaviest traffic can be seen on the pipes heading from the reactor to the generator and from the generator to the condenser.

6.3.5 Simulation Mode of Operation

The simulation is operated by implementing an event controller, which governs the operational speed. Figure 55 displays the event controller interface.


.Models.Frame.EventController

Time 0:00:00:00.0000

☐ Real time x 10

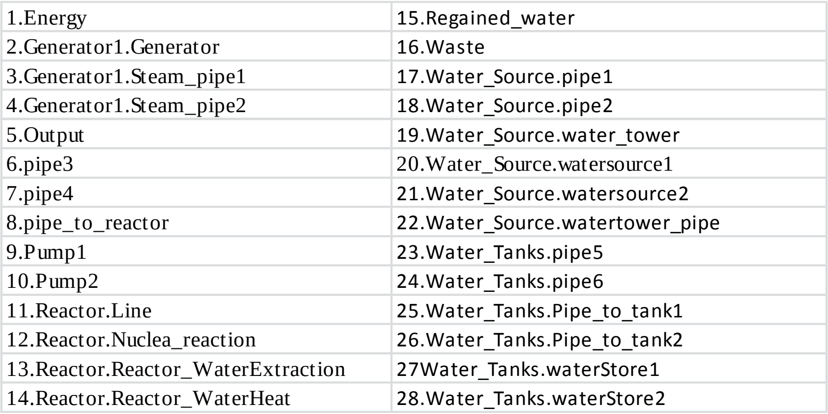
Figure 55 Simulation Event Controller

Figure 55 shows a speed control, start/stop function and a reset control. The duration of the simulation can be input into the event controller to allow for self-governing operation and automatic completion after the allotted time has passed.

6.3.6 SYSTEM BEHAVIOUR CONSISTENCY

The behaviour of the system remains consistent during each simulation however subtle changes in data patterns can be seen due to the random factors introduced. The data set generated by this simulation is used to evaluate BOCISS.

When running the simulation, data can be collected from any of the components. This is comparable with the collection of data from mechanisms, such as a pump, in a real nuclear power plant. A selection of the simulation components data is extracted from are displayed in Table 2.



1.Energy	15.Regained_water
2.Generator1.Generator	16.Waste
3.Generator1.Steam_pipe1	17.Water_Source.pipe1
4.Generator1.Steam_pipe2	18.Water_Source.pipe2
5.Output	19.Water_Source.water_tower
6.pipe3	20.Water_Source.watersource1
7.pipe4	21.Water_Source.watersource2
8.pipe_to_reactor	22.Water_Source.watertower_pipe
9.Pump1	23.Water_Tanks.pipe5
10.Pump2	24.Water_Tanks.pipe6
11.Reactor.Line	25.Water_Tanks.Pipe_to_tank1
12.Reactor.Nuclea_reaction	26.Water_Tanks.Pipe_to_tank2
13.Reactor.Reactor_WaterExtraction	27Water_Tanks.waterStore1
14.Reactor.Reactor_WaterHeat	28.Water_Tanks.waterStore2

Table 2 Simulation Components Example

The components displayed constitute the key objects within the system and make an ideal choice for collecting data from, as their behaviour changes during simulation and they present an effective example of the overall behaviour of the system.

When the simulation is running, behaviour can be actively monitored in order to view the operation of the system. Figure 56 displays the behaviour of the system after 40 simulated minutes. Numbers 1 to 28 on the x-axis signify the various components from Table 2, which the data is collected from to present a view of the system.

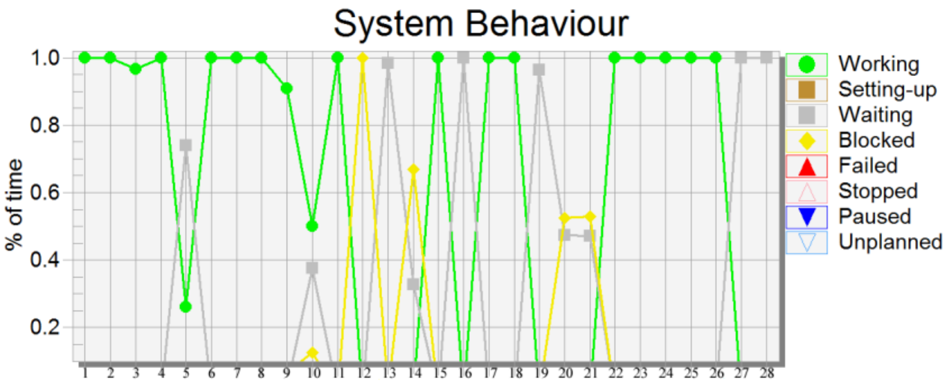


Figure 56 Line Graph Snapshot of Simulation Behaviour (40 mins)

The y-axis refers to the percentage of operation over a period of time. For example, pipe 4 (number 7) was operational 100% of the time after 40 minutes. Pump2, however (number 10) was blocked 50% of the time as a result of the pipe to the reactor being full. After 1 hour, the behaviour remained constant.

Figure 57, displays this behaviour in the form of a bar chart. In this case, there have been failures in two components: steam pipe 1 and the water tower both for short periods of time.

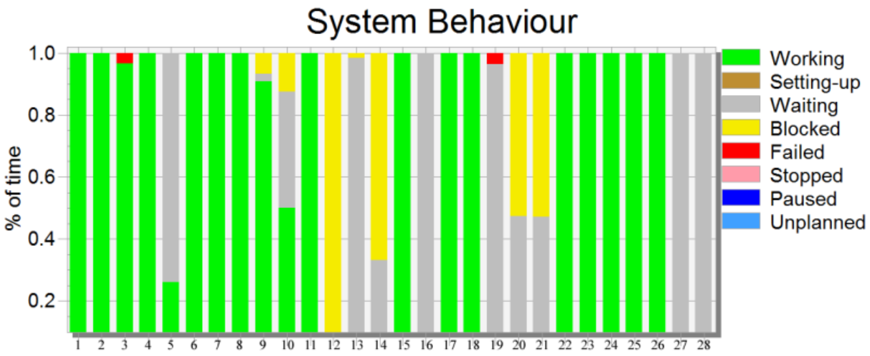
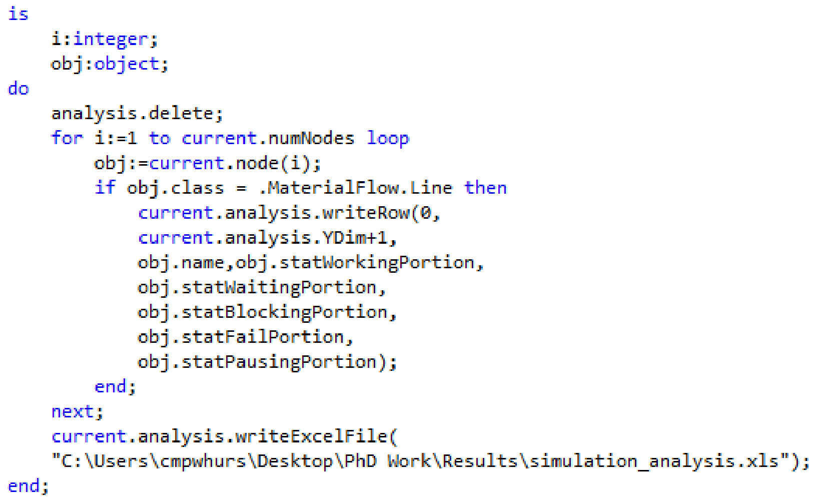


Figure 57 Bar Chart Snapshot of Simulation Behaviour (1 hr)

The simulated errors in system components are a result of the afore mentioned availability percentage which defines how likely a failure is to occur in a specific component.

6.3.7 Data Extraction Methods

Data can be extracted from the nuclear power plant simulation by implementing a method in order to export data as a set. An example of the coding for this is displayed below.



```
is
    i:integer;
    obj:object;
do
    analysis.delete;
    for i:=1 to current.numNodes loop
        obj:=current.node(i);
        if obj.class = .MaterialFlow.Line then
            current.analysis.writeRow(0,
            current.analysis.YDim+1,
            obj.name,obj.statWorkingPortion,
            obj.statWaitingPortion,
            obj.statBlockingPortion,
            obj.statFailPortion,
            obj.statPausingPortion);
        end;
    next;
    current.analysis.writeExcelFile(
    "C:\Users\cmpwhurs\Desktop\PhD Work\Results\simulation_analysis.xls");
end;
```

Figure 58 Simulation Data Export Code

Another approach is to insert an entity referred to as a 'TimeSequence' to act as an observer for a specific system component and extract pre-specified data. The types of data we can collect include: performance data, material flow data, resource allocation, and system load data. In our simulation we used this second approach as it allowed for more flexibility during data collection and allowed us to target specific system components for data extraction. Using this approach we were able to construct a large customised dataset which matched our requirements for the evaluation of BOCISS.

Taking pipe4 as an example, an inserted TimeSequence acts as an observer, and it records the values for the number of units of water passing through pipe4. Active sampling was done at 0.1 seconds. The code used to accomplish this is displayed below:

$$pipe4.NumMU$$

This code effectively tells the TimeSequence to record data exclusively about the number of units of water. In the following section, a sample data set is presented to demonstrate the data constructed using our simulation.

6.4 Data Construction For BOCISS

To evaluate BOCISS, we constructed two data sets: one for normal behaviour and one for abnormal behaviour. These two equally sized data sets are required for the training of the data classifiers.

6.4.1 Data Extraction

Data is collected using TimeSequences, which act as observers for individual system components. Figure 59 displays the observers represented by black-squared icons. Arrows demonstrate the observers' corresponding component for data extraction.

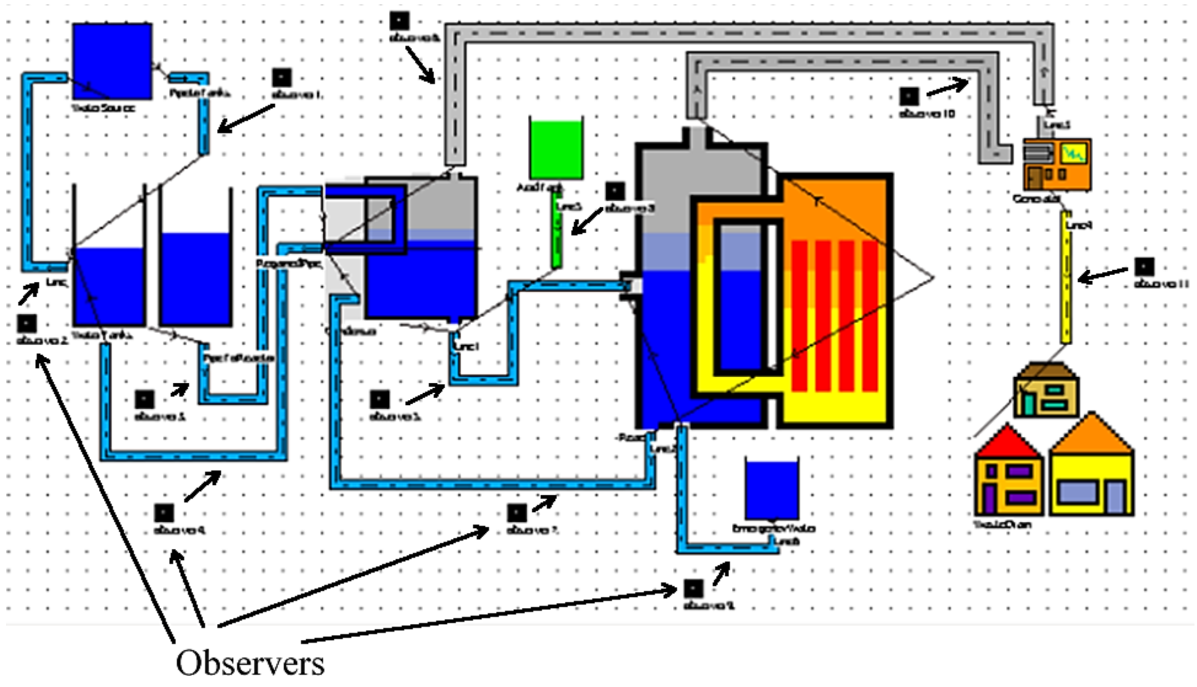


Figure 59 Simulation with Observers

Inside each of the mechanisms, the observers can be seen more clearly. Figure 60 displays the water source mechanism, which contains 14 observers. Again, several arrows are added to demonstrate the observers' corresponding components.

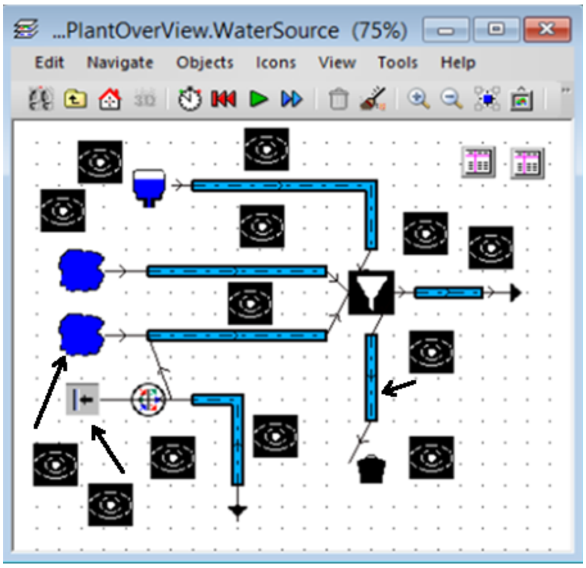


Figure 60 Water Source with Observers

One further example is displayed in Figure 61. The water tanks mechanism contains 10 observers for data extraction purposes.

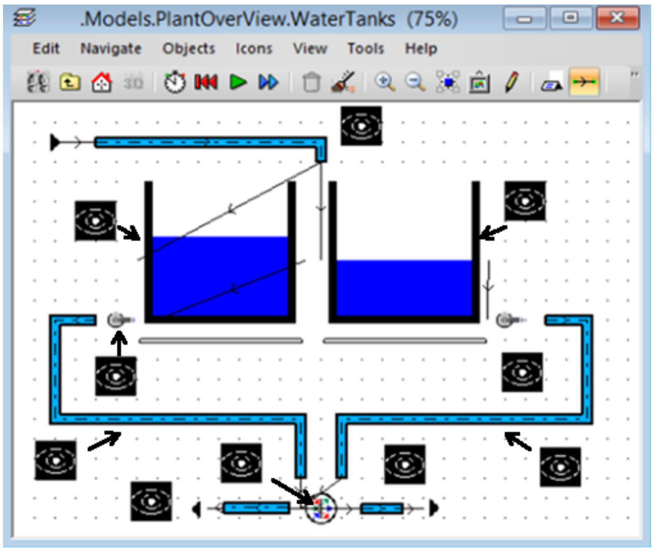


Figure 61 Water Tanks with Observers

Each component in the simulation has a corresponding observer, which extracts physical information about behaviour and constructs the data set required for the BOCISS evaluation. In order to have successful data classification, both normal behaviour data and attack data is needed and constructed in our simulation.

6.4.2 NORMAL DATA

The normal data set was constructed by running the simulation for a period of two simulated days with active sampling conducted at 4Hz (which is every 0.25 of a second). Therefore, the dataset generated consists of 732,000 records of data for each component.

Table 3 displays a sample of the data collected, where the value refers to the number of units of water being processed by the component at a given time. For example, between the times 15:04.3 and 15:07.4 the level of water in Pipe2 increases one unit then decreases. As the sampling was done every 0.25 of a second, Table 3 shows little change in the data due to the fact that it is a snap shot of data sampling taken at extremely close intervals.

Table 3 Normal Data Sample

Time	Pipe1	Pipe2	Water Tower Pipe	Pipe3	Pipe4	Waste	Pipe to Tank 1	Pipe to Tank 2	Water Store 1	Water Store 2	Pipe 5	Pipe 6	Pump 1	Pump 2
15:04.3	5	5	0	0	4	0	2	2	93	4	33	17	0	0
15:04.4	5	5	0	0	4	0	2	2	93	4	33	17	0	0
15:04.5	5	5	0	0	4	0	2	2	93	4	33	17	0	0
15:04.6	5	5	0	0	4	0	2	2	93	4	33	17	0	0
15:04.7	5	5	0	0	4	0	2	2	93	4	33	17	0	0
15:04.8	5	5	0	0	4	0	2	2	93	4	33	17	0	0
15:04.9	5	5	0	0	4	0	1	1	94	4	32	17	1	0
15:05.0	6	6	0	0	4	0	1	1	94	4	32	17	1	0
15:05.1	6	6	0	0	4	0	1	1	94	4	32	17	1	0
15:05.2	6	6	0	0	4	0	1	1	94	4	32	17	1	0
15:05.3	6	6	0	0	4	0	1	1	94	4	32	16	1	1
15:05.4	6	6	0	0	4	0	1	1	93	4	33	16	1	1
15:05.5	6	6	0	0	4	0	1	1	93	4	33	16	1	1
15:05.6	5	6	0	0	4	0	1	1	93	4	33	16	1	1
15:05.7	5	6	0	0	4	0	1	1	93	4	33	16	1	1
15:05.8	5	6	0	0	4	0	1	1	93	4	33	16	1	1
15:05.9	5	6	0	0	4	0	1	1	93	4	33	16	1	1
15:06.0	5	6	0	0	4	0	1	1	93	4	33	16	1	1
15:06.1	5	6	0	0	4	0	1	1	93	4	33	16	1	1
15:06.2	5	6	0	0	4	0	1	1	93	4	33	17	1	1
15:06.3	5	6	0	0	4	0	1	1	93	4	33	17	1	1
15:06.4	5	6	0	0	4	0	1	1	93	4	33	17	1	1
15:06.5	5	6	0	0	4	0	1	1	93	4	33	17	1	1
15:06.6	5	6	0	0	4	0	1	1	93	4	33	17	1	1
15:06.7	5	6	0	0	4	0	1	1	93	4	33	17	1	1
15:06.8	5	6	0	0	4	0	1	1	93	4	33	17	1	1
15:06.9	5	6	0	0	4	0	1	1	93	4	33	17	1	1
15:07.0	5	6	0	0	4	0	1	1	93	4	33	17	1	1
15:07.1	5	6	0	0	4	0	1	1	93	4	33	17	1	1
15:07.2	5	6	0	0	4	0	1	1	93	4	33	17	1	1
15:07.3	5	5	0	0	4	0	2	2	93	4	33	17	1	0
15:07.4	5	5	0	0	4	0	2	2	93	4	33	17	1	0

The data displayed in Table 3 refers only to the normal behaviour data, however, as previously discussed, two data sets were created for both attack and normal behaviour.

6.4.3 ABNORMAL DATA

Threat behaviour is constructed by causing targeted and random disruptions to the system by increasing the availability percentage in specific components. One such example would be the implementation of a failure to the steam pipes, which could be introduced to occur 50% of the time during runtime. The result would be, each steam pipe turning off and on during the simulation and causing a knock-on effect throughout the rest of the system. To construct our abnormal dataset, the availability percentage was increased in each of the components, whilst ensuring the system was able to continue functioning.

The difference between normal behaviour and attack behaviour can be seen both in Figure 62 and Figure 63. Two components were chosen as a representation of the differences in data between attack and normal system behaviour. Normal behaviour is represented by the triangles and attack behaviour represented by the squares. The x-axis numbers the 25 records of data and labels them from 1 to 25. The y-axis displays the mean value for the units of water in the component over an hour.

Figure 62 displays the data constructed for pipe 4. The result of the attack on the steam pipe has an effect, which can be clearly seen by the increase in the average value per hour.

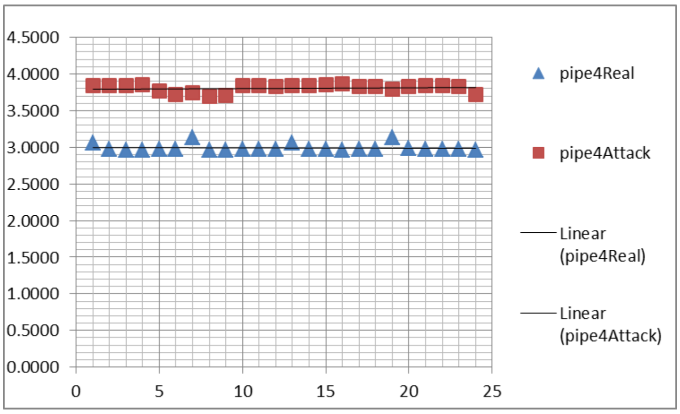


Figure 62 Pipe4 Data Normal and Attack Behaviour

Figure 63 displays the data constructed for pipe3. As before the triangles represent normal behaviour and the squares represent attack behaviour. The change in behaviour as a result of the attack can once again be seen but in the case of this component it is not as clear. The linear line for both normal and attack behaviour, however, shows a clear change once again in the average value.

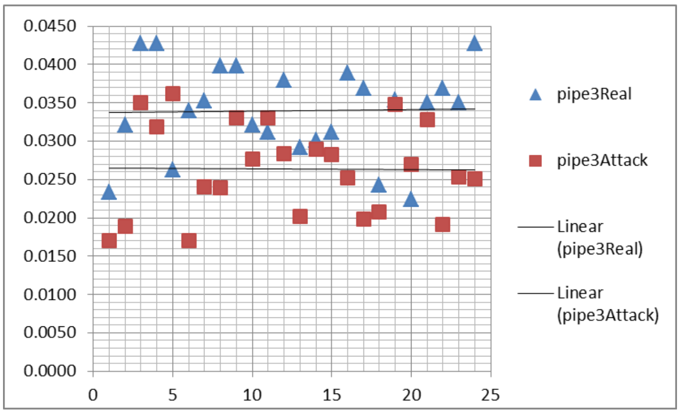


Figure 63 Pipe3 Data Normal and Attack Behaviour

Changes in behaviour as a result of an attack taking place can often be subtle and hard to identify. For that reason, data classification is essential. Identifying these variations in behaviour and subtle changes in patterns of activity to detect automatically threats to the system, and alert an operator, is the fundamental aim of our research.

6.5 Data Pre-Processing and Feature Extraction

In this section, the focus is on the data-preparation, feature extraction and classification stages of our system design as displayed in Figure 64. This entails the feature extraction process, the pre-processing of the dataset generated by our nuclear power plant simulation and the classification methodology.

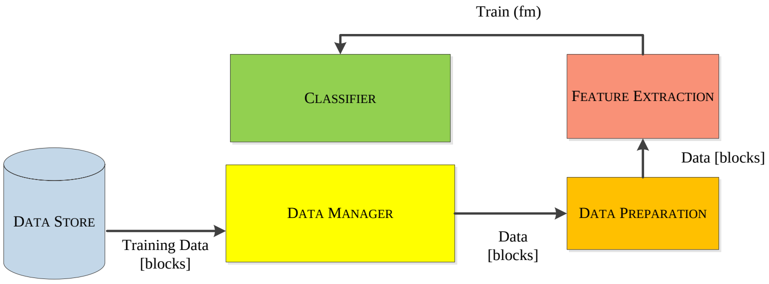


Figure 64 Methodology Process

A description of each of the data classifiers is provided to highlight how anomalous behaviour is detected in a dataset. In total, nine classifiers are applied to the dataset and the motives for their selection are also discussed later in this chapter.

6.5.1 Pre-Processing and Noise Reduction

As discussed in section 5.3.5, data requires pre-processing. One of the main issues with the dataset generated by the simulation is the level of noise in the data. In order to achieve the highest possible results in the classification process, noise needs to be reduced. This is achieved by editing or removing values from the dataset which are unwanted by the classifiers but constitute parts of the dataset which are of interest.

As a result of the behaviour of specific components in the system, there is a high level of zeros in our dataset. The zeros are a result of either components failing due to introduced errors, or units of liquid in the system passing through a component faster than the sampling rate. For example, in the steam pipes the pressure is high and the units pass through the pipes at a rate greater than the sampling frequency. Zeros, therefore, represent aspects such as pipes functioning normally. If the samples are consistently above zero for components such as the steam pipes, it would be the result of failures in the system. For that reason, the zero values are retained in our data set. Data pre-processing and feature extraction are essential stages, and affect the data classification results.

6.5.2 Feature Extraction

The features selected represent characteristics of system behaviour [184]. The process of feature selection effectively minimizes the dataset and presents a representation of the behaviour taking place in the data to the classifier. Primarily, we identify the goals of the feature selection process, which has three clear benefits including data comprehension, increased efficiency and prediction performance.

- Data Comprehension: Extracting features from a data set allows for a better comprehension of what the data is representing.
- Efficiency: Reducing the amount of data being classified allows for faster processing, reducing time of learning and reducing memory use.
- Prediction: The performance of the classifiers is also improved through effective feature selection. Factors such as noise reduction and the elimination of irrelevant data allows the classifiers to be efficiently trained.

Our overall evaluation process involves two feature sets: an initial smaller feature set and a main feature set. The methodologies for both feature sets are presented in this section.

6.5.3 Data Manipulation

The data manipulation process is the construction of feature vectors from significantly large normal and abnormal data sets. To construct a feature vector from a 15 minute block of data, for example, 3600 rows of data are processed. The aim is to create an array of feature vectors from the normal and abnormal datasets. This process would take place in the data pre-filtering, prior to the feature extraction stage in the system architecture.

6.5.4 Initial Feature Set

For the initial evaluation, 164 features are taken from the system dataset. The feature set is divided into two groups, comprised of 128 mechanism component features and 36 system component features. The mechanism components are discussed in section 6.3.4. The system components are comprised of pipes or cables, which link the mechanisms together as displayed in Figure 53 in section 6.3.5.

The features are constructed by taking the maximum, minimum, mean and median values every hour from the data which is sampled at 4hertz (4 times every second) for 24 hours simulation. Table 4 displays how the 164 features are formed. Each of the mechanism components provide a value produced by sampling the level of water, steam or energy passing through. This is also the case for the system components. The table displays the number of components, which are taken into account for each feature.

Table 4 Initial Feature Selection

Number of Mechanism Components					**Feature Construction**		
Type	Max Value	Min Value	Mean Value	Median Value	Sampling Rate	Feature Extraction	Simulation Time
Water Components	27	27	27	27	4Hz	Every Hour	1 Day
Steam Components	4	4	4	4	4Hz	Every Hour	1 Day
Energy Components	1	1	1	1	4Hz	Every Hour	1 Day
Number of System Components					**Feature Construction**		
Water Components	6	6	6	6	4Hz	Every Hour	1 Day

Steam Components	2	2	2	2	4Hz	Every Hour	1 Day
Energy Components	1	1	1	1	4Hz	Every Hour	1 Day

32 mechanism components provide 4 features each to form 128 features. The nine system components also provide 4 features each to produce 36 features. Using the features extracted from the two datasets for normal and attack behaviour, records of feature vectors are created. These initial records of data are used for testing the classifiers' ability to identify normal behaviour and, subsequently, recognise when normal behaviour is not occurring. In total, 12 feature vectors were used to train the classifiers consisting of 6 for normal behaviour and 6 for abnormal behaviour.

Minimum, maximum, mean and median values were selected to form our initial feature vector records because each provides an ideal representation of the system behaviour. For example, when observing the minimum and maximum levels of water in a pipe or water tank, the constraints of normal behaviour can be specified. If the levels recorded are lower or higher than the expected minimum or maximum values then the system is not behaving as it should. In the same way, observing the mean levels of water steam or energy allows us to identify the normal behaviour constraints of selected critical components.

6.5.5 Main Feature Set

The construction of the main feature set, involves additional features. This includes, the minimum, maximum, mean, mode and median values for 15 minute blocks of data. Additional features are considered in order to assess the classifiers' ability to evaluate large datasets. Table 5 displays the features and the blocks of time they are created in. Our main feature vector set is significantly larger than the initial feature set and consists of 220 features with 96 feature vectors for normal behaviour and 96 feature vectors for abnormal behaviour.

Table 5 Main Feature Selection

Number of Mechanism Components						**Feature Construction**		
Type	Max Value	Min Value	Mean Value	Median Value	Mode Value	Sampling Rate	Feature Creation	Simulation Time
Water Components	27	27	27	27	27	4Hz	15 minutes	1 Day

Steam Components	4	4	4	4	4	4Hz	15 minutes	1 Day
Energy Components	1	1	1	1	1	4Hz	15 minutes	1 Day
Number of System Components						**Feature Construction**		
Water Components	6	6	6	6	6	4Hz	15 minutes	1 Day
Steam Components	2	2	2	2	2	4Hz	15 minutes	1 Day
Energy Components	1	1	1	1	1	4Hz	15 minutes	1 Day

35 mechanism components provide 5 features each to form 175 features. The 9 system components also provide 5 features each to produce 45 features. These records of data are again used for training the classifiers and testing their ability to detect abnormal system behaviour. Table 6 displays the 220 features, which constitute the main feature set. Each component selected from our simulation is displayed in abbreviated format and represents the mean value, with median, mode, max and min number for each. The definition of each abbreviation can be found the appendix.

Table 6 Feature Set

W1WT	W5WS2	WDP1	Pump1	WTCP	PTR	NR	CP	T	OPTWS	OPTR
1med	5med	9med	13med	17med	21med	25med	29med	33med	37med	41med
1mode	5mode	9mode	13mode	17mode	21mode	25mode	29mode	33mode	37mode	41mode
1max	5max	9max	13max	17max	21max	25max	29max	33ax	37max	41max
1min	5min	9min	13min	17min	21min	25min	29min	33min	37min	41min
W2WT	W6WP2	TP	Pump2	TPTC	PTCT	SO	GSOP	G	OPTC	OSO
2med	6med	10med	14med	18med	22med	26med	30med	34med	38med	42med
2mode	6mode	10mode	14mode	18mode	22mode	26mode	30mode	34mode	38mode	42mode
2max	6max	10max	14max	18max	22max	26max	30max	34max	38max	42max
2min	6min	10min	14min	18min	22min	26min	30min	34min	38min	42min

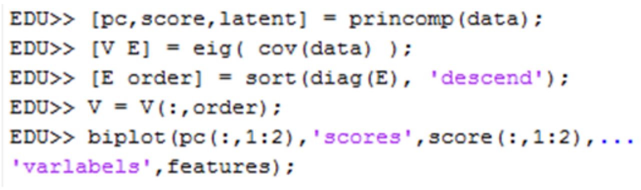
W3WS1	W8OP	WT1	T1P	MSTC	OTWT	RC	SP1	EL1	OWRP	OMSP
3med	7med	11med	15med	19med	23med	27med	31med	35med	39med	43med
3mode	7mode	11mode	15mode	19mode	23mode	27mode	31mode	35mode	39mode	43mode
3max	7max	11max	15max	19max	23max	27max	31max	35max	39max	43max
3min	7min	11min	15min	19min	23min	27min	31min	35min	39min	43min
W4WP1	W10WP	WT2	T2P	CT	PFT	C	SP2	OPTT	OPFR	OEC
4med	8med	12med	16med	20med	24med	28med	32med	36med	40med	44med
4mode	8mode	12mode	16mode	20mode	24mode	28mode	32mode	36mode	40mode	44mode
4max	8max	12max	16max	20max	24max	28max	32max	36max	37max	44max
4min	8min	12min	16min	20min	24min	28min	32min	36min	40min	44min

6.6 Data Refinement

To prevent overtraining the classifiers and to ensure the features selected are the most ideal when representing the dataset, dimensionality reduction is applied [185]. This is the process of reducing the number of unneeded variables, or in our case features.

6.6.1 Dimensionality Reduction

Dimensionality reduction is achieved using Principal Component Analysis (PCA), which is the extraction of the features, which best characterise the system behaviour [186]. In Matlab, PCA is achieved using the following code, which also generates a Biplot:



```
EDU>> [pc,score,latent] = princomp(data);
EDU>> [V E] = eig( cov(data) );
EDU>> [E order] = sort(diag(E), 'descend');
EDU>> V = V(:,order);
EDU>> biplot(pc(:,1:2),'scores',score(:,1:2),...
'varlabels',features);
```

Figure 65 PCA Code

Using a Scree Plot generated by the PCA analysis, the level of 'influence' each of the features has on the outcome of the classification results can be observed. The plot, displayed in Figure 66, displays the 220 features evaluated along the x-axis. Where the scree plot levels out, the features become less important to the classifier.

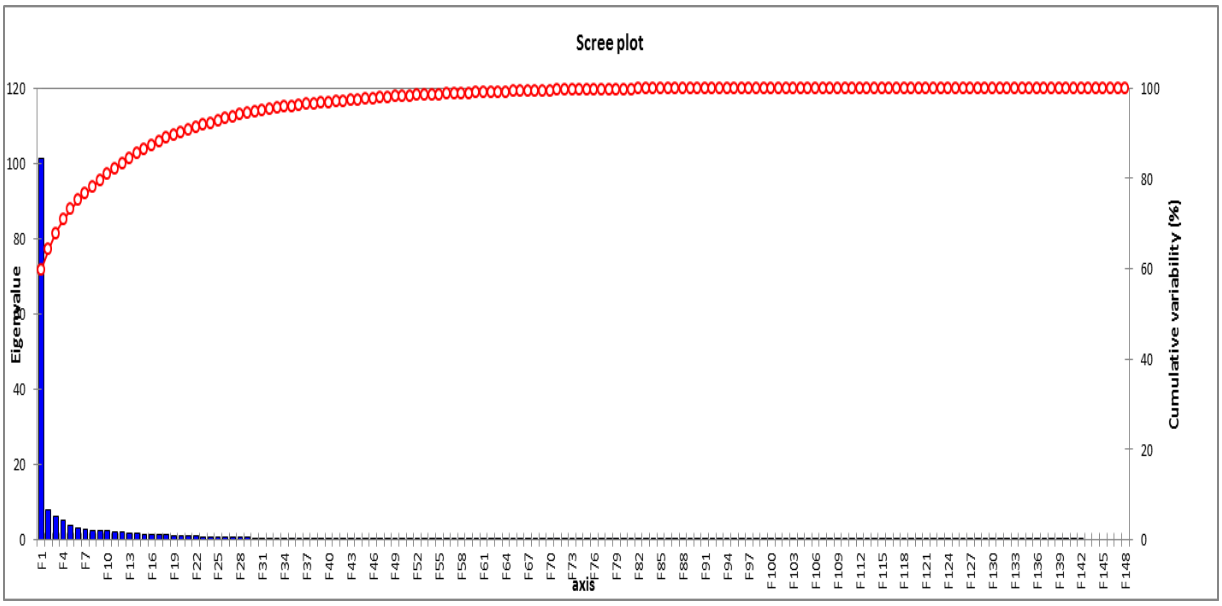


Figure 66 PCA Scree Plot

The scree plot displays that, of the 220 features extracted, approximately 30 are the most prominent in the dataset and effective for data classification. To coincide with the scree plot, the eigenvalues represent the impact the features have on the classifiers. Ideally, the first three eigenvalues should be high. A sample of the eigenvalue results are displayed in Table 7.

Table 7 Eigenvalue Table

	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12
Eigenvalue	101.377	7.796	6.121	5.137	3.859	3.304	2.632	2.483	2.470	2.299	2.145	2.052
Variability (%)	59.634	4.586	3.600	3.022	2.270	1.944	1.548	1.461	1.453	1.352	1.262	1.207
Cumulative %	59.634	64.219	67.820	70.841	73.112	75.055	76.603	78.064	79.517	80.870	82.132	83.338

In Table 7, the features are ranked in order of influence on the dataset and they contain the most information, which is relevant to our data classification process. We therefore, select the relevant features using a Biplot to identify which are prominent from the main grouping.

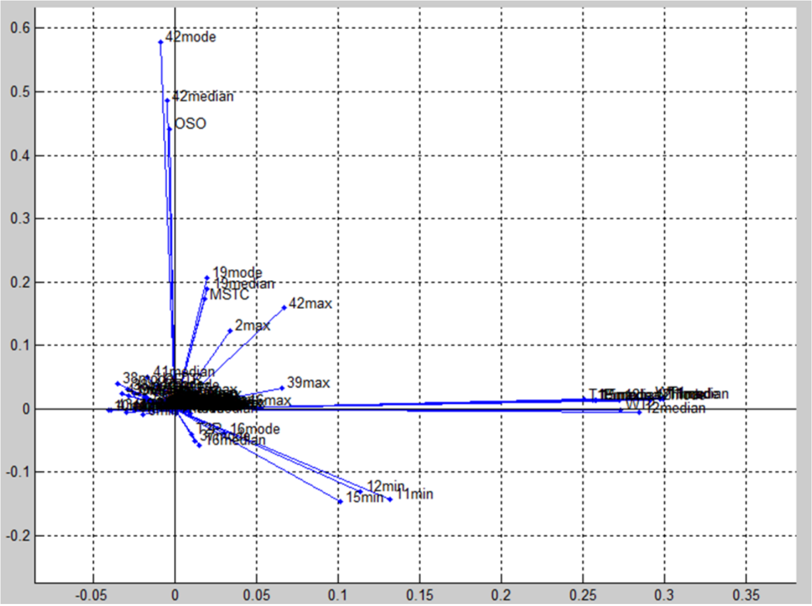


Figure 67 PCA Biplot

The Biplot is displayed in Figure 67 and shows the 30 features that are clearly identifiable from the main cluster. A 3D graph, displayed in Figure 68, shows how the vast majority of features are closely grouped in the centre with 30 separate from the main grouping.

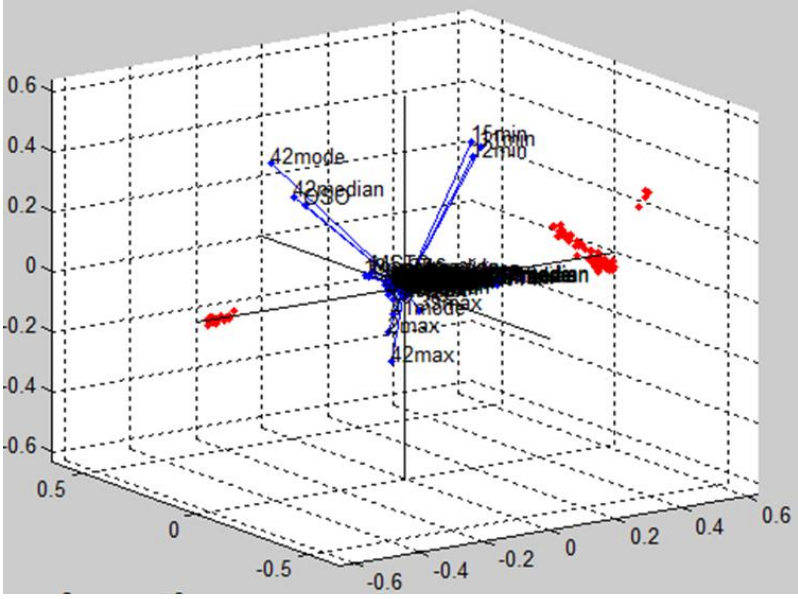


Figure 68 PCA Biplot 3D

Each of these features present an accurate picture of our simulation system behaviour and reducing the feature set to a smaller size prevents the classifiers from becoming over-trained.

6.6.1 FINAL FEATURE SET

Following the PCA analysis, our classification involves a set consisting of 30 features with 96 feature vectors. The 30 features displayed in Table 8, represent a significant reduction in the number initially generated for the main feature set.

Table 8 Final Feature Set

1	2max	11	12min	21	19median
2	WT1	12	T1P	22	19mode
3	11median	13	15median	23	37mode
4	11mode	14	15mode	24	38mode
5	11max	15	15max	25	39max
6	11min	16	15min	26	41median
7	WT2	17	T2P	27	OSO
8	12median	18	16median	28	42median
9	12mode	19	16mode	29	42mode
10	12max	20	MSTC	30	42max

In the following section, the data classifiers used for the evaluation process are presented, along with the evaluation techniques used to appraise their success.

6.7 CLASSIFICATION APPROACH

The evaluation process uses supervised learning. The approach involves specific data classification techniques including: Uncorrelated Normal Density based Classifier (UDC), Quadratic Discriminant Classifier (QDC), Linear Discriminant Classifier (LDC), Polynomial Classifier (PLOYC), k-Nearest Neighbour (KNNC), Decision Tree (TREEC), Parzen Classifier (PARZENC), Support Vector Classifier (SVC) and Naïve Bayes Classifier (NAIVEBC). A brief description of each of these techniques is provided in the following subsection.

6.7.1 SUPERVISED CLASSIFIERS

Linear Discriminant Classifier (LDC), is a technique which works by sorting or dividing data into groups based on characteristics to create a classification [187]. A discriminant function is obtained by monotonic transformation of posterior probabilities [188]. In other words, it performs an ordered transformation of unknown quantities, which are separated by a linear vector.

Quadratic Discriminant Classifier (QDC) works in a similar way to LDC by dividing the data into groups based on given characteristics. However, by using QDC the data is divided using a quadratic surface rather than a one-dimensional one. QDC makes no assumptions that covariance are alike. In other words, it assumes that the changing of two random variables will not be the same [189].

Uncorrelated Normal Density based Classifier (UDC) also operates comparably to the QDC classifier but computation of a quadratic classifier, between the classes in the dataset, is done by assuming normal densities with uncorrelated features. Quadratic Bayes takes decisions by assuming different normal distribution of data [190]. LDC, QDC and UDC are density based classifiers.

Polynomial Classifier (POLYC) is also a linear based classifier and it is used to sort data by evaluating the weighting, using a linear combination of features and considering the variables of the objects [188]. In detail, it functions by adding polynomial features (which are constant coefficients) into the data which supports the training of the classifier.

Decision Tree (TREEC) is a classifier which uses decision rules to divide the classes of data [188]. It operates by using criterion functions (the sum of squared errors), stopping rules (criteria for appropriate number of splits in a decision tree) or pruning techniques (the removal of unwanted tree sections). Using decision tree is a particularly ideal choice of classifier because it is well-known as one of the most effective supervised classification techniques [189].

Parzen Classifier (PARZENC) functions by including aspects of the training data when the classifier is built up. It is a non-linear classifier and it has the benefit that its parameters can be user supplied or optimised [189] [188].

k-Nearest Neighbour (KNNC) is similar to the Parzen Classifier in that it includes training data when building up the classifier. KNNC however, predicts values based on the ‘k-closest’ values from the training set. In other words data is classified by a majority decision by identifying ‘k-objects’ which are nearest to its neighbours [188].

Support Vector Classifier (SVC) functions by predicting two possible outputs from a given training feature. It uses quadratic programming for optimisation and its non-linearity is determined by the kernel, which maps data into a set. Naïve Bayes Classifier (NAIVEBC) functions by applying Bayes’ theorem to the dataset with independent suppositions. NAIVEBC is able to function with missing values and has the ability to learn incrementally [191].

Each of these classifiers where chosen because they have the ability to learn how to recognise abnormal values in a dataset. They also employ a supervised learning approach, which is a key part of the system design. In the following subsection, the classification evaluation techniques are presented. Each of the techniques provides an assessment of the classifiers' success or failure when classifying the data.

6.7.2 Classification Evaluation Techniques

Firstly, a Confusion Matrix determines the distribution of errors across all classes [192]. The estimate of the classifier is calculated as the trace of the matrix divided by the total number of entries. Additionally, a Confusion Matrix provides the point where miss-classification occurs [192]. In other words, it shows true positive (TP), false positive (FP), true negative (TN) and false negative (FN) values. Diagonal elements show the performance of the classifier, while off diagonal presents errors.

$$\begin{array}{c|c} \text{TP} & \text{FN} \\ \hline \text{FP} & \text{TN} \end{array} \qquad (2)$$

Using the confusion matrix the success rate of each classifier can be evaluated by dividing the number of True Positive and True Negative results by the total number of feature vectors, as displayed in the following formula:

$$\frac{TP + TN}{TP + FP + TN + FN} \qquad (3)$$

In addition to providing the success rate, the confusion matrix also provides the calculation of the sensitivity and specificity for each classification. Sensitivity is identification of positive results in a data set. In our work, this refers to accurately detected normal system behaviour and it is calculated using the formula:

$$\frac{TP}{TP + FN} \qquad (4)$$

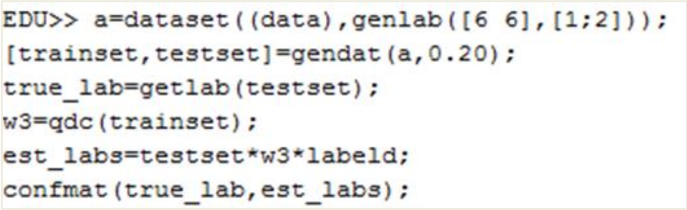
Whereas, Specificity is the identification of negative results and is calculated using the formula below. Again, in our work this refers to accurately detected normal and anomalous system behaviour.

$$\frac{TN}{TN + FP} \tag{5}$$

Using the confusion matrix, specificity and sensitivity results, we are able to evaluate ability of each of the data classifiers abilities to detect anomalous behaviour.

6.7.3 CLASSIFICATION METHOD

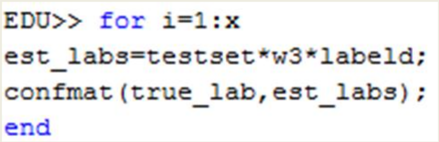
In this subsection, the classification methodology is presented. Using the array of features, Matlab is used to perform the classification analysis. Figure 69 displays an example of the code involved. In this example, the code is used for QDC analysis.



```
EDU>> a=dataset((data),genlab([6 6],[1;2]));
[trainset,testset]=gendat(a,0.20);
true_lab=getlab(testset);
w3=qdc(trainset);
est_labs=testset*w3*labeld;
confmat(true_lab,est_labs);
```

Figure 69 Matlab Code Sample

In order to conduct the experiments multiple times a simple for loop is added, as displayed in Figure 70. Using this code the classification experiments are conducted multiple times for the value of ‘x’. In our evaluation, x = 30. The reason the classification experiments are conducted 30 times is to account for errors and to give consistency [193]. Statisticians identify that experiments conducted 30 times provide an adequate realistic average [193].



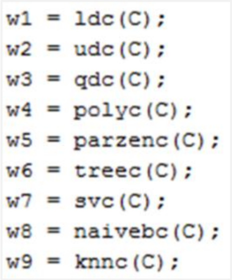
```
EDU>> for i=1:x
est_labs=testset*w3*labeld;
confmat(true_lab,est_labs);
end
```

Figure 70 Matlab For Loop

The result evaluation process is conducted using the above code which generates the confusion matrices and displays the success of each of the machine learning classifiers.

6.7.4 CLASSIFICATION VISUALISATION

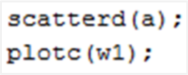
To visualise the classification results, discriminant functions and mapping scatter plots are employed. To achieve this, each of the classifiers are initially given a designation, as demonstrated in Figure 71, where ‘C’ refers to the training set.



```
w1 = ldc(C);
w2 = udc(C);
w3 = qdc(C);
w4 = polyc(C);
w5 = parzenc(C);
w6 = treec(C);
w7 = svc(C);
w8 = naivebc(C);
w9 = knnc(C);
```

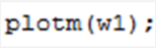
Figure 71 Matlab Plot Code Part 1

A ‘Plotc’ command plots the discriminant function in a scatter plot, whereas ‘Plotm’ plots the mapping, as displayed in Figure 72 and Figure 73.



```
scatterd(a);
plotc(w1);
```

Figure 72 Matlab Plot Code Part 2



```
plotm(w1);
```

Figure 73 Matlab Plot Code Part 3

Using both these plot commands, the results of the classification experiments are visualised and the grouping and vision of normal and abnormal data are displayed.

6.8 SUMMARY

Our development of a critical infrastructure simulation using the Siemens Tecnomatix Plant Simulator and SimTalk is presented in this chapter. The simulation detailed is the closest we can get to a real world system. A vast amount of technology used in infrastructures employ Siemens technology. The SimTalk code used is a representation of the ladder logic employed by PLC devices.

The simulation can be used to create substantial datasets. The behaviour of the system remains consistent during each simulation however, subtle changes in data patterns can be seen due to the random factors introduced into the system to provide realism. We intend to use the data set generated by this simulation to evaluate (BOCISS). The methodology for the evaluation process is presented in the following chapter.

The methodology presented in this chapter defines how the data is pre-processed prior to applying classification algorithms. Essential steps, such as noise reduction and dimensionality reduction ensure that the classifiers are able to achieve effective results. We presented the use of PCA to extract prominent features from the dataset and reduced the level of unwanted data prior to our classification process. In the following chapter, we present the evaluation of our classifiers and assess the effectiveness of our approach using the confusion matrices.

CHAPTER 7

EVALUATION

7.1 INTRODUCTION

In this chapter, we present the evaluation of BOCISS using the datasets constructed from our nuclear power plant simulation. The classification results and an assessment of their success is presented. The evaluation is conducted in two stages, as discussed in chapter 6. Firstly, we use a smaller feature set and data sample to evaluate the classifiers and provide an insight into each classifiers performance. The second part of the approach involves a larger dataset with an increase in the number of features used. A comparison between both and a discussion on the sets of results are also presented.

7.2 INITIAL CLASSIFICATION RESULTS

In the initial sample set, the aim is to present an initial evaluation of how abnormal behaviour can be identified in system behaviour. The features selected for input into the data classification algorithms are based on an evaluation of which extracted characteristics provide a true representation of our simulation’s behaviour. The features used, therefore, include aspects such as regular occurrences in system behaviour, and traits from individual components.

7.2.1 INITIAL DATASET SAMPLE

Table 9 presents a sample of the initial record set, which consists of an evenly divided dataset randomly divided using MATLAB into a 50% training set, with the rest of the 50% assigned to a test set.

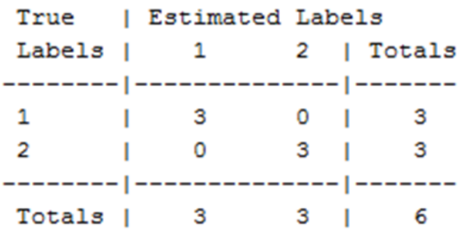
Table 9 Initial Data Set Sample

W2WTP	median	Max	min	**W3WS1**	median	Max	min	**W4WP1**	median	Max	min	**W5WS2**	median	Max	min	**W6WP2**	median	Max	min
0	0	0	0	1	1	1	1	11	11	11	11	0.2	0	1	0	10.2	10	11	10
0	0	0	0	1	1	1	1	10.6	11	11	10	0	0	0	0	10	10	10	10
0	0	0	0	1	1	1	1	11	11	11	11	0	0	0	0	10	10	10	10
0	0	0	0	1	1	1	1	10.2	10	11	10	0	0	0	0	10	10	10	10
0	0	0	0	1	1	1	1	10.8	11	11	10	0.2	0	1	0	10	10	10	10
0	0	0	0	1	1	1	1	10.8	11	11	10	0	0	0	0	9.4	9	10	9
0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	9.8	10	11	9
0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	10	10	10	10
0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	10.4	10	11	10
0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	10.2	10	11	10
14	14	14	14	1	1	1	1	11	11	11	11	1	1	1	1	10	10	10	10
14	14	14	14	1	1	1	1	11	11	11	11	1	1	1	1	10	10	10	10

The first six vectors, in blue, represent normal data, whereas, the red values represent abnormal data. A full dataset with all 164 features can be found the appendix. Using the above data sample, the performance of each classifier is evaluated to assess the classification accuracy. In the following subsection, an evaluation of the results is presented.

7.2.2 Initial Dataset Evaluation

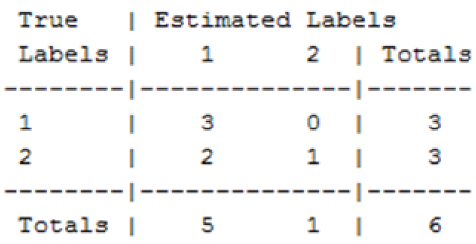
In order to obtain a more accurate assessment of which of the classifiers is most successful and consistent, the experiments were conducted 30 times. Figure 74 to Figure 76 present examples of three of the confusion matrices generated for KNNC, TREEC and QDC to provide and illustration of the evaluation process. Firstly, Figure 74 displays a confusion matrix showing 100 % data classification success for one of the 30 experimentations for the KNN-C classifier. KNN-C performed consistently throughout.



```
 True    | Estimated Labels
 Labels  |     1       2   | Totals
---------|---------------|-------
 1       |     3       0   |    3
 2       |     0       3   |    3
---------|---------------|-------
 Totals  |     3       3   |    6
```

Figure 74 Initial KNN-C Confusion Matrix

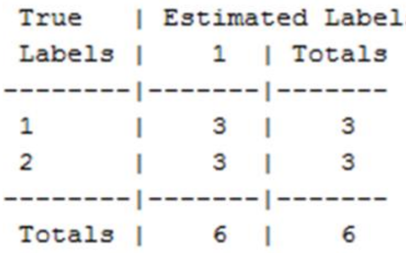
Figure 75 presents a confusion matrix for TREEC, which achieved a 66.67 % accurate classification with two errors in the False Positive column. TREEC achieved mixed results during the 30 classification experiments conducted.



```
 True    | Estimated Labels
 Labels  |     1       2  | Totals
---------|----------------|-------
 1       |     3       0  |     3
 2       |     2       1  |     3
---------|----------------|-------
 Totals  |     5       1  |     6
```

Figure 75 Initial TREEC Confusion Matrix

Figure 76 displays a confusion matrix for the QDC evaluation. The diagram displays a 50% classification success rate. In this particular sample, QDC was able to accurately classify 100 % of the normal behaviour, however all the abnormal data was misclassified.



```
 True    | Estimated Labels
 Labels  |     1   | Totals
---------|---------|-------
 1       |     3   |     3
 2       |     3   |     3
---------|---------|-------
 Totals  |     6   |     6
```

Figure 76 Initial QDC Confusion Matrix

An overall evaluation of the classification algorithms, is presented in Table 10 which displays the results of classification success, sensitivity and specificity with the mean value taken for 30 experiments.

Table 10 Average Classifier Performance for Initial Dataset

Classifier	Classification Success	Sensitivity	Specificity
LDC	62.78 %	1.0	0.21
UDC	88.90 %	1.0	0.82
QDC	50 %	1.0	0.0
POLYC	100 %	1.0	1.0
PARZENC	50 %	1.0	0.0
TREEC	90.01 %	1.0	0.80
SVC	100 %	1.0	1.0
NAIVEBC	100 %	1.0	1.0
KNNC	100 %	1.0	1.0

The results for sensitivities, which is the identification of normal behaviours, are high. The specificities, which is identification of abnormal behaviour, is mixed. Several of the classifiers are prone to generating false positive results, meaning abnormal behaviour values are grouped with normal behaviours.

It is clear from the results that the classifiers are able to identify normal behaviour with high success, as displayed by the sensitivity results. However, five of the classifiers group abnormal behaviours with the normal behaviour set, with QDC and Parzenc failing to identify a single abnormal behaviour. Four of the classifiers, POLYC, SVC, NAIVEBC and KNNC were able to successfully classify the data with 100% accuracy for each of the 30 classification experiments.

7.2.3 Initial Results Visualisation

In this subsection, a visualisation of the initial results is presented. Each diagram represents a sample of the outcomes and provides a visual demonstration of how the classifiers function. In each figure, the division of data into two groups for normal and abnormal behaviour is displayed, where blue ellipses group normal behaviours and red ellipses group abnormal. Each figure displays a scatter plot in either 2D or 3D. Each of the points represents a value from the features selected for visualisation. Two features were used in each visual representation to demonstrate how the classifiers function and to provide a graphical representation of the results obtained.

Firstly, Figure 77 shows the mapping of two classes on a scatter plot in a 2-D feature space for the Parzenc analysis. Feature 1, on the x-axis, refers to the one of the dominant features and Feature 2, on the y-axis, refers to one of the lesser dominant features from the final set of 30 selected during the dimensionality reduction process.

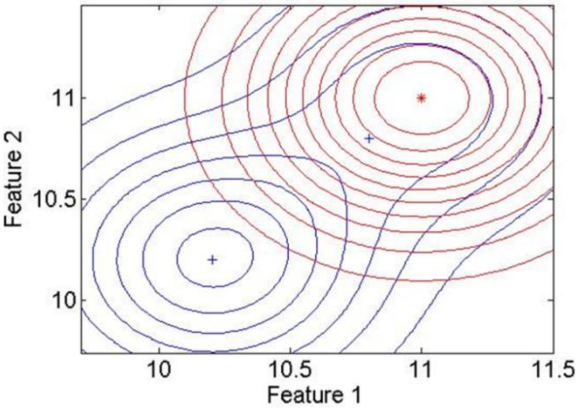


Figure 77 Parzenc Plot 2 Features

The process functions by creating a scatter plot of the values from both of the selected features then drawing the ellipses based on the division of the data. The ellipses, displayed, refer to likelihood contours, where the points inside the ellipse are most likely to belong to that grouping. The blue ellipses consist of data that comes from the normal behaviour dataset and the red ones referring to threat behaviour data. Threat behaviour can be identified as a result of one grouping clearly standing out from the other.

As the graph displays, Parzenc struggled to cluster the data into its correct grouping as the ellipses for normal behaviour values contour the red abnormal behaviour values. Figure 78, again shows the Parzenc results by mapping them in 3-D, where the ellipses are displayed as spikes or curves in three dimension. Ideally two clear spikes should be visible to demonstrate two distinct data groupings.

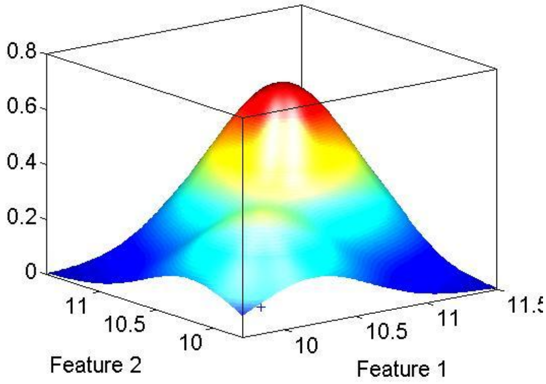


Figure 78 Parzenc Plot 2 Features 3D

Figure 79 displays the scatter plot for two of the classes from the Naivebc results, which achieved 100% success for classification. Similarly to Figure 77, the likelihood contours group the data into two distinct groups.

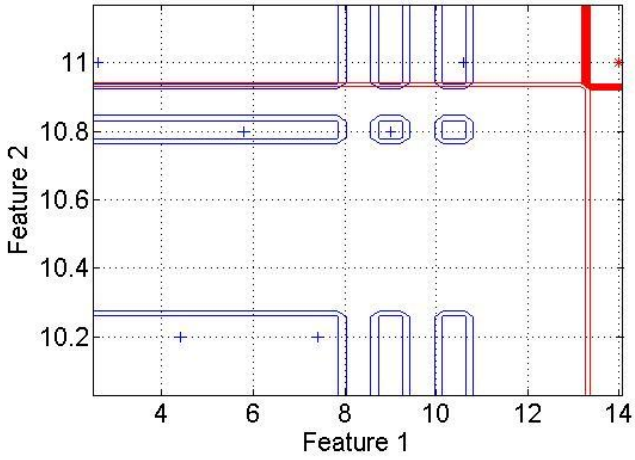


Figure 79 Naivebc Plot 2 Features

The plot displays how Naivebc is able to group the data more accurately, with the blue grouping referring to normal behaviour and red referring to abnormal behaviours.

7.2.4 Initial Summary of Results

The initial results of the classification conducted using a small dataset, support our findings that data classification can be used to detect abnormal behaviour in critical infrastructures. A comparison of the performance of the nine classifiers can be seen in Figure 80, which displays the mean average score for each.

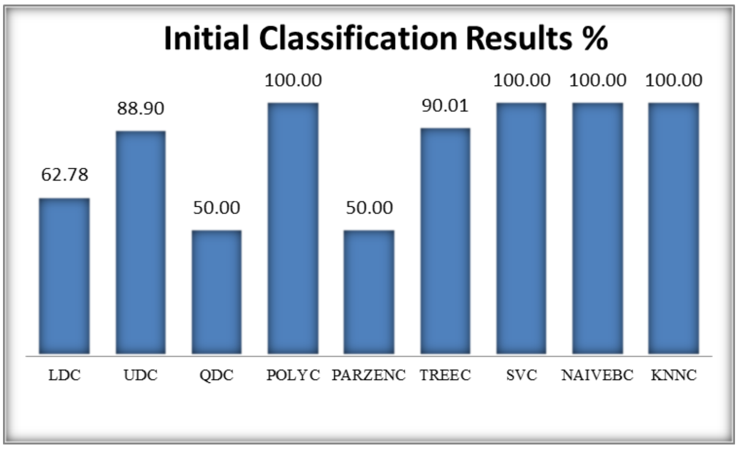


Figure 80 Initial Classification Results

Similarly, Figure 81 displays a comparison between the sensitivity and specificity results. Four classifiers produce a mean average of 100% success rate for both, while all classifiers identified 100% of normal behaviour. Clearly, the classifiers are able to identify normal behaviour easily, however, frequently group abnormal behaviour in the wrong cluster.

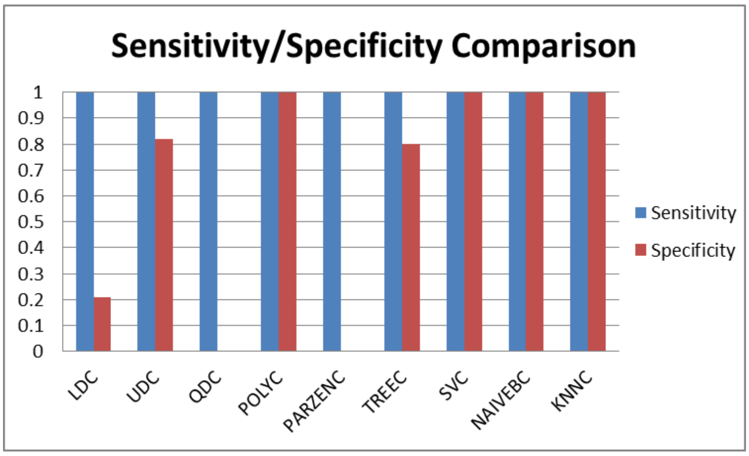


Figure 81 Initial Classification Sensitivity/Specificity

Whilst the results show that anomalous behaviour can be identified with some success using our chosen classifiers, our initial dataset impacted the results. The ability to classify abnormal behaviour, was hampered by the fact that our dataset was too small to allow the classifiers to train themselves to a substantial level. The results will be expanded upon in the following section.

We purposefully selected an abnormal dataset, which had a mixed of substantial deviations from the normal behaviour as well as similar values. The results show that half of the classifiers where able to achieve a high success rate and all the classifiers were able to identify 100% of normal behaviours.

7.3 Supervised Data Classification Results

Building on the results of the initial data set evaluation, additional features are taken into consideration when classifying the larger dataset. Using a more substantial dataset, in this section we present a more conclusive evaluation of the selected classifiers. The dataset used in this section, has a large number of more subtle anomalies in the behavioural data in contrast with the initial dataset.

7.3.1 Main Dataset Sample

Table 11 presents a sample of normal behaviour data from the set used. A larger sample of the data is displayed in the appendix. The main data set is evenly divided between 192 normal and abnormal feature vectors, which are comprised of 220 features.

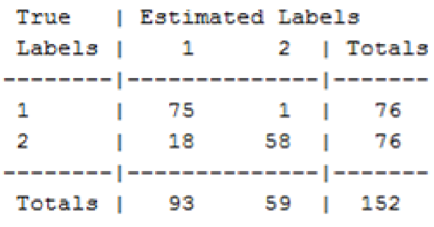
Table 11 Main Data Set Sample

WT1	11median	11mode	11max	WT2	12median	12mode	12max	12min	T1P	15median	15mode
0.49	0.00	0.00	1.00	1.62	1.00	1.00	6.00	0.00	13.80	14.00	14.00
0.47	0.00	0.00	1.00	1.00	1.00	0.00	8.00	0.00	14.00	14.00	14.00
0.49	0.00	0.00	1.00	8.33	9.00	10.00	13.00	4.00	13.80	14.00	14.00
0.48	0.00	0.00	1.00	5.44	4.00	3.00	12.00	1.00	13.99	14.00	14.00
0.48	0.00	0.00	1.00	2.09	2.00	1.00	7.00	0.00	13.77	14.00	14.00
0.50	0.00	0.00	1.00	0.62	1.00	1.00	2.00	0.00	13.96	14.00	14.00
0.51	1.00	1.00	1.00	9.50	12.00	1.00	19.00	0.00	13.95	14.00	14.00
0.50	0.00	0.00	1.00	3.73	3.00	1.00	11.00	0.00	14.00	14.00	14.00
0.51	1.00	1.00	1.00	2.18	1.00	1.00	9.00	0.00	13.78	14.00	14.00
0.49	0.00	0.00	1.00	4.37	4.00	1.00	11.00	0.00	13.99	14.00	14.00
0.47	0.00	0.00	1.00	1.82	1.00	1.00	6.00	0.00	14.00	14.00	14.00
0.46	0.00	0.00	1.00	2.41	2.00	1.00	7.00	0.00	13.81	14.00	14.00
0.52	1.00	1.00	2.00	3.53	2.00	1.00	11.00	0.00	13.81	14.00	14.00
0.48	0.00	0.00	2.00	9.09	9.00	10.00	13.00	4.00	13.83	14.00	14.00

As with the initial dataset, each classifiers' performance is calculated using a confusion matrix to evaluate, sensitivity, specificity classification success. In the following subsection, the results are presented.

7.3.2 CLASSIFICATION EVALUATION

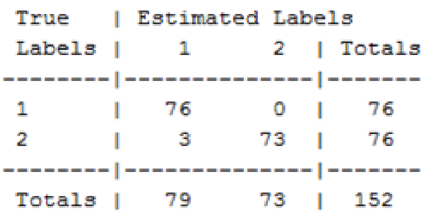
Figure 82 to Figure 84 presents an example of three of the confusion matrices generated for LDC, QDC and KNNC. As with the initial analysis, each of the classification experiments were conducted 30 times. Figure 82 displays 88.158% classification success for one of the 30 LDC evaluations, with 0.987 sensitivity and 0.763 specificity. In this particular experiment, 75 out of 76 normal behaviours were classified correctly and 58 out of 76 abnormal behaviours were accurately classified.



```
 True    | Estimated Labels
 Labels |     1       2   | Totals
--------|---------------|-------
 1       |    75       1   |    76
 2       |    18      58   |    76
--------|---------------|-------
 Totals |    93      59   |   152
```

Figure 82 LDC Evaluation Sample

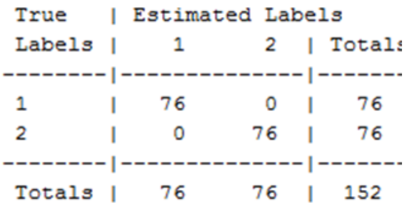
Figure 83 displays 98.026 % success for QDC classification with 1.00 for sensitivity and 0.961 for specificity. The sample experiment displays that all normal behaviours were accurately classified with only 3 incorrect abnormal values misclassified.



```
 True    | Estimated Labels
 Labels |     1       2   | Totals
--------|--------------|-------
 1       |   76       0   |    76
 2       |    3      73   |    76
--------|--------------|-------
 Totals |   79      73   |   152
```

Figure 83 QDC Evaluation Sample

Similarly to the initial evaluation, Figure 84 displays a confusion matrix showing 100 % data classification for one of the 30 KNN-C experiments. 1.00 for both sensitivity and specificity is also achieved.



```
 True    | Estimated Labels
 Labels |     1       2   | Totals
--------|--------------|-------
 1       |   76       0   |    76
 2       |    0      76   |    76
--------|--------------|-------
 Totals |   76      76   |   152
```

Figure 84 KNNC Evaluation Sample

A comparison of the classification success for each of the classifiers is presented in Table 12 below. Overall, the algorithms were able to accurately classify 98.14 % of the dataset on average between them.

Table 12 Classification Results

Classifier	Classification Success %	Sensitivity	Specificity
LDC	93.640	0.99957	0.874
UDC	99.759	1.000	0.995
QDC	89.868	1.000	0.798
POLYC	100	1.000	1.000
PARZENC	100	1.000	1.000
TREEC	100	1.000	1.000
SVC	100	1.000	1.000
NAIVEBC	100	1.000	1.000
KNNC	100	1.000	1.000

The results presented are a significant improvement on the initial evaluation. Six out of the nine classifiers were able to classify 100% of the data accurately. LDC, QDC and UDC have mixed results, however, each also displays a significant ability to accurately classify behaviour. As previously, the classifiers are able to identify normal behaviour with a high success with nearly all the errors occurring for the misclassification of abnormal behaviour. In the following subsection, we present a visualisation of the results, as well as, a discussion and a justification of the outcomes.

7.3.3 Main Results Visualisation

In this subsection, a visualisation of the supervised machine learning results is presented. As with the initial classification, the visualised results presented represent a sample of the classification outcomes. Figure 94 displays a scatter plot of two classes in a 2-D feature space for the LDC analysis. For the purposes of visualising the results, two of the features from the set are plotted once more.

The graph displays normal behaviour, represented by the blue cluster, and abnormal behaviour visible in the red cluster. The linear line generated by the LDC analysis displays the division between the two sets of data. Figure 94 displays one of the 30 experiments for LDC, which, on that occasion, obtained 100 % success.

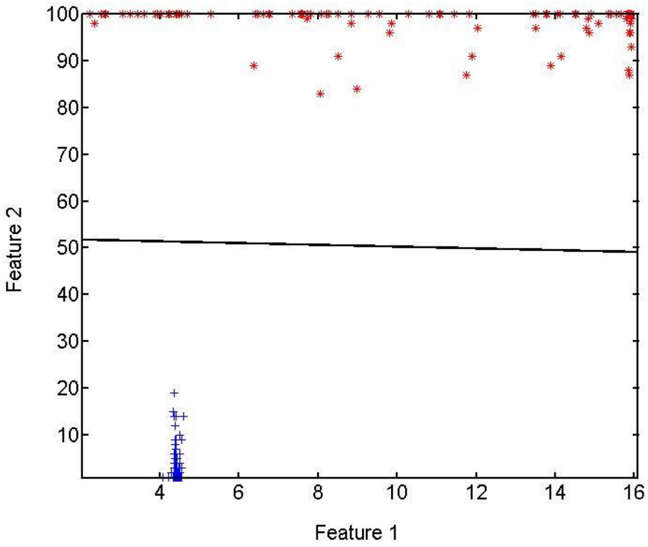


Figure 85 LDC Analysis Graph 100%

Figure 86 displays the same scatter plot, however, each of the classifiers' approach for dividing the data are visible. For this particular experiment, all the nine classifier are able to divide the data into two distinct clusters accurately. The diagram displays a clear visualisation of the methodology for each classifier when dividing the data.

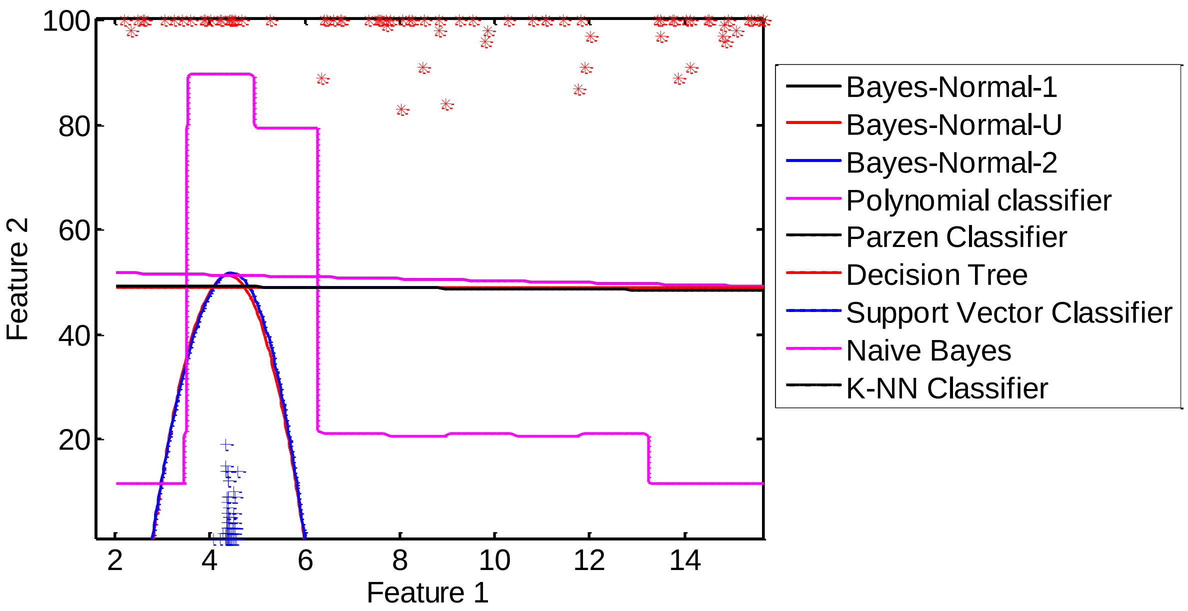


Figure 86 Main Results Plot

As in the initial evaluation, a visualisation of the Parzenc classification is displayed in Figure 87. However, in this case, Parzenc classification achieved higher results. As before, the blue ellipses consist of data that comes from the normal behaviour dataset and the red ones referring to threat behaviour data.

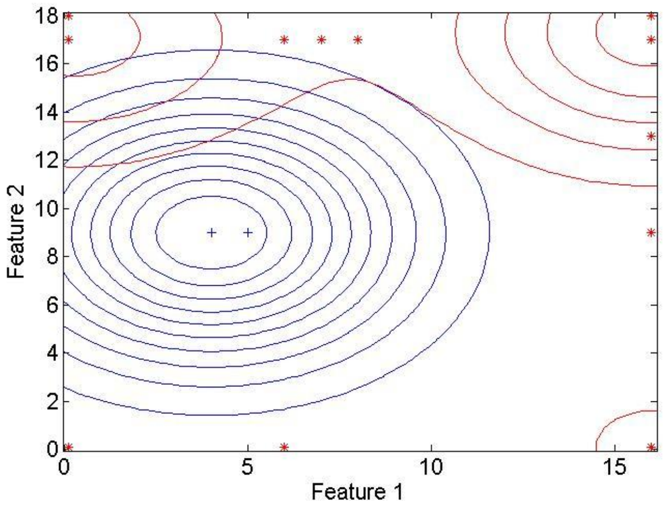


Figure 87 Parzenc Evaluation 2 Features

The ellipses for normal and abnormal behaviour values more accurately contour the correct data clusters than previously. This is again displayed in 3D, in Figure 88, where two distinct peaks created by the data groupings are visible.

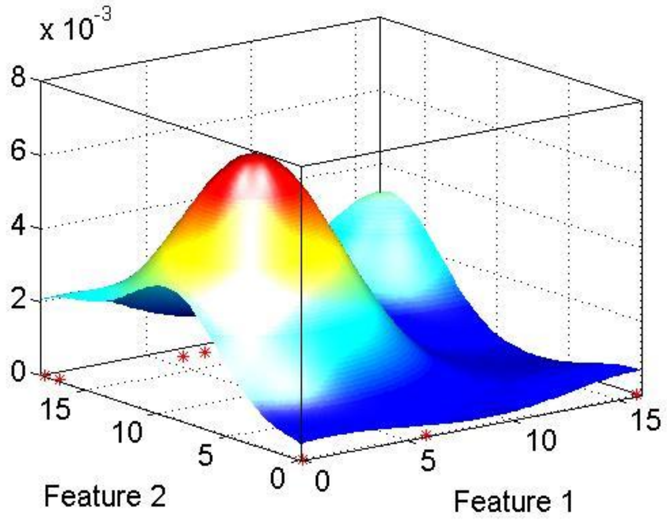


Figure 88 Parzenc Evaluation 2 Features 3D

In Figure 89, the visualisation of the likelihood ellipses for the LDC analysis is presented. As with the Parzenc diagram, data is grouped by likelihood ellipses. In this specific experiment, the LDC evaluation classified 96.71% of the data accurately meaning some of the data is misclassified and part of the wrong ellipse.

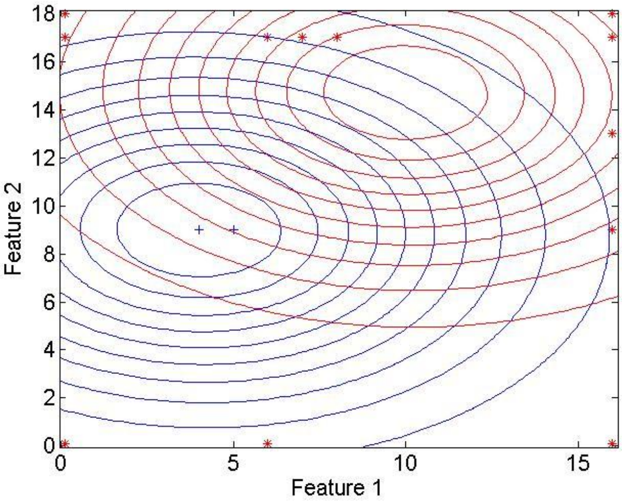


Figure 89 LDC Evaluation 2 Features

As with the initial evaluation, the results obtained support the findings that data classification can be used to detect abnormal behaviour in critical infrastructures. In light of this, in the following subsection, we present an assessment of the results obtained using the main dataset.

7.3.4 Assessment of Results

The comparison of the performance of each classifier is displayed in Figure 90, which shows the mean average score for 30 experiments.

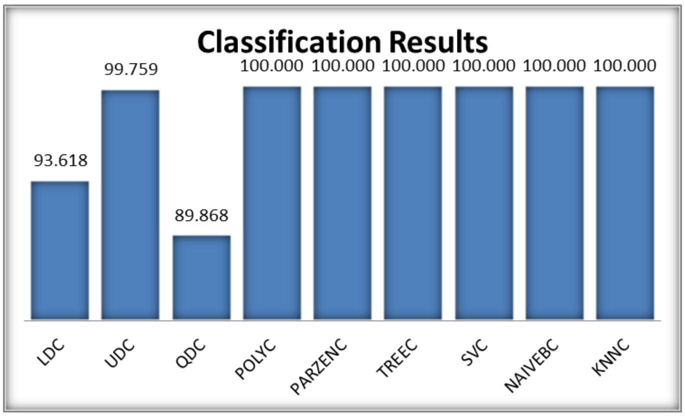


Figure 90 Classification Results

Similarly, Figure 91 displays a comparison between the sensitivity and specificity results. Seven of the classifiers produce a mean average 100% success rate for both while eight of the nine classifiers identified 100% of normal behaviour.

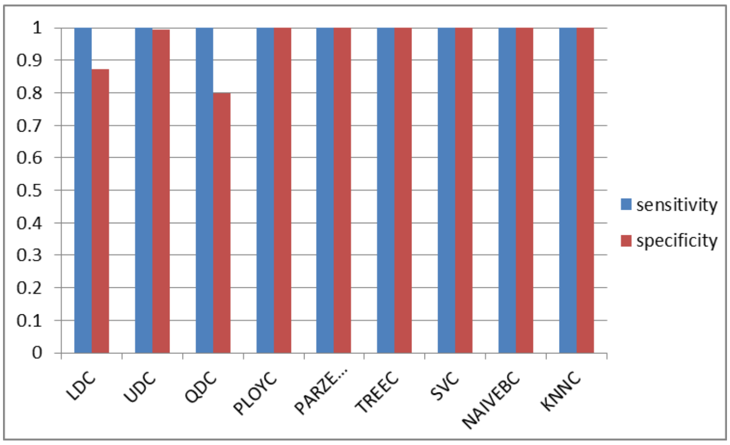


Figure 91 Sensitivity vs. Specificity Results

Once again, the classifiers are able to identify normal behaviour easily, with errors occurring for the classification of abnormal behaviour in the wrong cluster. However, the amount of misclassified data is relatively low. In the following subsection, a discussion on the results obtained in both of the evaluation stages is presented, along with a comparison of both.

7.4 DISCUSSION

The success of the classifiers is a result of various key stages including, noise reduction and principal component analysis prior to the classifiers being applied. In this section, we present a discussion and justification of the results obtained during the evaluation process.

7.4.1 RESULTS COMPARISON

One of the main observations is that the more data is added to the classifiers, the more accurate the results are. This is reflected in the comparison between the initial results and the main supervised machine learning results. Figure 92 displays the overall mean classification success of each of the classifiers combined. In total, in the initial evaluation, the classifiers were able to classify 82.41 % of the data accurately. This is lower than what would be ideal, for critical infrastructure security. In the case of critical infrastructures, it is important to achieve a high success rate. Subsequently, in the main evaluation, the classifiers were able to achieve a much higher mean rate of 98.138 % correctly classified data.

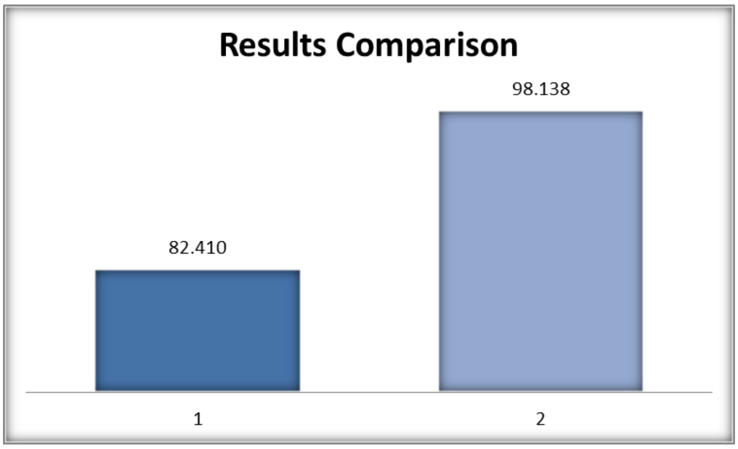


Figure 92 Best Results Comparison

Providing the classifiers with substantially more data, allows the algorithms to be trained to an effective level. Table 13 displays a detailed comparison between initial results and current results. Various key differences between the two evaluation processes include a notable improvement in the LDC, UDC, QDC Parzenc and Treec classification results.

Table 13 Classification Results Comparison

Initial Data Set				Main Data Set		
Classifier	Classification	Sensitivity	Specificity	Classification	Sensitivity	Specificity

LDC	62.78 %	1.000	0.21	93.618 %	0.99957	0.874
UDC	88.90 %	1.000	0.82	99.759 %	1.000	0.995
QDC	50 %	1.000	0.0	89.868 %	1.000	0.798
POLYC	100 %	1.000	1.0	100 %	1.000	1.000
PARZENC	50 %	1.000	0.0	100 %	1.000	1.000
TREEC	90.01 %	1.000	0.80	100 %	1.000	1.000
SVC	100 %	1.000	1.0	100 %	1.000	1.000
NAIVEBC	100 %	1.000	1.0	100 %	1.000	1.000
KNNC	100 %	1.000	1.0	100 %	1.000	1.000

Overall, the results display a remarkable improvement, in particular for LDC, QDC, UDC, Parzenc and Treec between the initial and main evaluation process.

7.4.2 Results Discussion

The improvement in the classification results is impacted by two key differences in the approach. Firstly, an advanced feature extraction process enhanced the outcomes. Collecting more features, which provided a more comprehensive representation of system behaviours, allowed the data to be filtered before being processed by the classifiers.

Secondly, having a larger dataset to train the classifiers produces results that are more accurate. As reflected by LDC, UDC and QDC in particular, which have been significantly improved upon.

Initially, LDC, QDC and UDC performed less effectively. However, both were able to classify a significant proportion of the data accurately. Figure 93 displays a comparison between their initial and main evaluation results for successfully classified data. The graph visually displays an improvement in the results for these three classifiers, which performed the least successfully out if the nine tested. The blue bars represent the initial evaluation, whereas the red bars signify the main evaluation results.

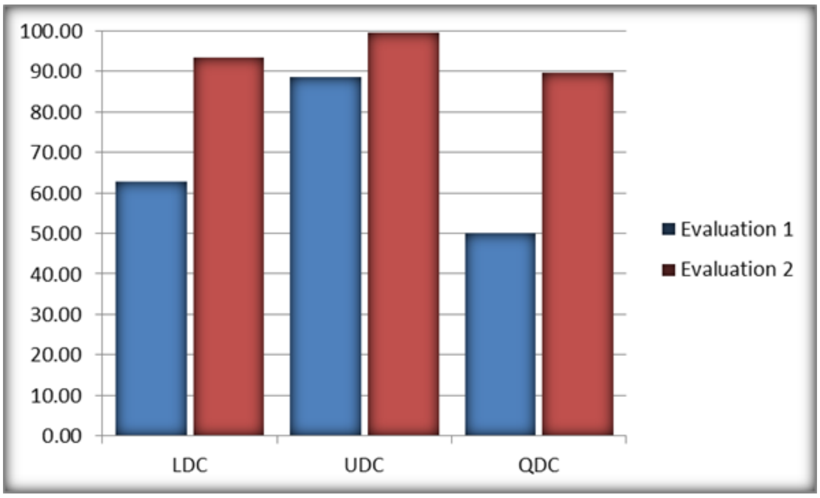


Figure 93 LDC, UDC and QDC Comparison

A comparison of all nine classifiers is displayed in Figure 94, which shows a radar chart of the sensitivity and specificity results for the initial evaluation for each of the classifiers. The data is presented in the form of a radar chart for visualisation purposes [55]. The results for each are plotted along separate axis starting at the centre and ending at the outside.

Radar charts are ideal for comparing aggregate values from multiple data series and present an effective visual representation of classification data. In this case, it is easy to identify changes between the first and second evaluation by looking at significant changes in the shape. In the first graph, the sensitivity is 1.0 for each of the nine classifiers; however the specificity is inconsistent.

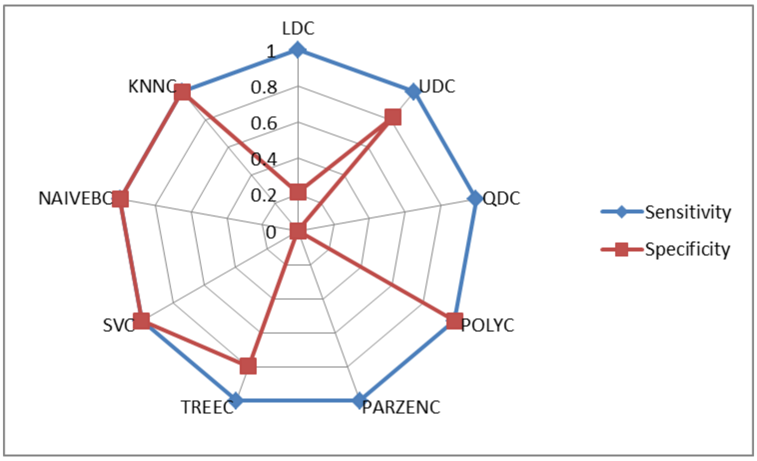


Figure 94 Initial Classification Results Radar Chart

Figure 95 displays the sensitivity and specificity for the main evaluation. By comparing the graphs, it is easily noticeable that the specificity results have improved. In the following subsection, a justification of the achieved results is presented.

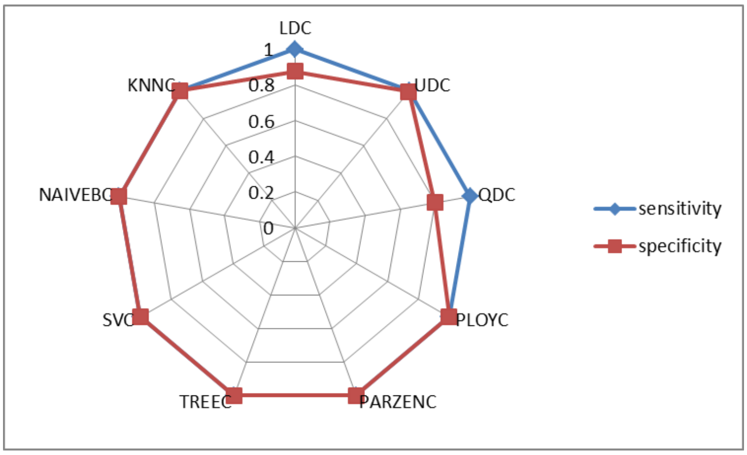


Figure 95 Main Classification Results Radar Chart

7.4.3 Results Justification

The evaluation presented in this chapter demonstrates how abnormal behaviour can be identified in a system using data classification techniques. The results achieved were high and successful. Our evaluation is affected by; firstly, the quality of data used which had an impact on the results. Despite creating a simulation which replicates a critical infrastructure, the quality of data produced is inferior to a real-world nuclear power plant. The dataset generated is intended to demonstrate the ability of the classifiers to classify data into its correct groupings and identify when any given system behaviour is not as it should be.

Secondly the high results were achieved through an efficient pre-processing of the data which removed noise and selected the most effective features for training the classifiers. It was also apparent that we ‘over attacked’ the system creating a mixture of large and more subtle anomalies in the data. The principal component analysis stage selected several of the features with large data anomalies for training the classifiers, in addition to the features with more subtle anomalies.

Finally, the advantage of using supervised machine learning had an impact on the results we achieved. As previously discussed, the approach involved giving the classification algorithms the ‘right answer’ to enable them to operate self-sufficiently. By using this method, we are able to train the classifiers using features which are known to be effective for achieving high results.

7.5 Summary

The evaluation presented in this chapter presents the effectiveness of BOCISS. The classification techniques used present a demonstration of how our system is able to support security by identifying anomalous behaviour caused by cyber-attacks taking place. In the following chapter, the thesis is concluded and a discussion on the contribution of our work is put forward along with an insight into the possible future directions of our research.

CHAPTER 8

CONCLUSIONS AND FUTURE DEVELOPMENTS

8.1 INTRODUCTION

Cyber-attacks are increasing at an alarming rate and critical infrastructure security must be continually developing to counter the growing threat. As threats evolve and become more adaptive, so should security measures become adaptive by adopting additional security techniques. The future lies with combating cyber-attacks in an innovative way combining both techniques where systems, such as BOCISS, are used along-side existing methods to provide well-structured defence in depth. In this chapter, a summary of the research completed in this thesis is presented. The main contribution of the work and its possible future directions are discussed in detail and a high-level comparison with the related research detailed in Section 4.4 is provided.

8.2 THESIS SUMMARY

Many examples of the threats facing critical infrastructures and the cost of failures are given in this thesis. Despite the clear need to develop effective protection methods, the task is a difficult one. Regardless of the fact that there is large investment into critical infrastructure security systems, clearly there are significant weaknesses. Creating multiple layers of security ensures that critical infrastructures are as protected as possible from potential security breaches.

In this section, we present an overview of the thesis and our research for supporting critical infrastructures against cyber-attacks using behavioural observation and data classification. A summary of each of the thesis chapters is provided.

8.2.1 OVERVIEWS

In chapter 1 of this thesis, we introduced the research area and presented the motivation behind the work being carried out. The aims and objectives of the research are discussed along with an overview of the solution and the novelty of the work. Secondly, in chapter 2 the background on critical infrastructures was presented. This chapter defined what critical infrastructures are, how they function, what weaknesses they tend to have and how they are protected against cyber-attack. In addition, related research into critical infrastructure protection was discussed.

Next, in chapter 3 we drew on examples of past and existing cyber-threats, digital breakdown, and critical infrastructure failures, which have taken place over the last decade, to explain the reason for this research being conducted. Subsequently, in chapter 4, we discussed related work including behaviour analysis and simulation research and detailed why their use is of great benefit for the development of future critical infrastructure securities.

In chapter 5 we presented out system design. This included an overview of the design specification and system architecture. The various modes of operation were put forward along with a description of each of the components and their interaction.

In chapter 6 we presented the development of a simulation of a nuclear power plant and its use for data construction. We also highlighted the methodology for the evaluation of BOCISS. This involved conducting an in depth look at data pre-processing, feature extraction and classification methodologies. In chapter 7 the evaluation was presented. This included an assessment of our approach, which uses behavioural observation for critical infrastructure security.

8.2.2 CONTRIBUTIONS TO KNOWLEDGE

The research presented in this thesis offers a significant contribution towards the advancement of critical infrastructure security. Adaptive security is becoming an increasingly important factor in critical infrastructure protection. Using our approach, which involves supervised data classification techniques to identify system threats, security is adaptive and can be customised to suit different critical infrastructure environments. This is due to the autonomous training process. BOCISS autonomously ‘learns’ the behavioural patterns of an infrastructure based on the data extracted. Using the learnt normal system behaviour, our approach is able to identify threats through the system by detecting unusual system behaviour. This is a novel approach to cyber-attack detection.

Support for security and defence in-depth is increased through the maintaining of the status quo of system behaviour. There is no requirement to have knowledge of existing cyber-threats to function. In addition, using a database of known behaviour patterns adds an extra dimension to security. The added database of known patterns of behaviour built up during the training mode allows known threat behaviours to identify specific attacks taking place.

By combining nine classifiers, BOCISS can provide the operator with the ability to perform various analyses of the system to gain a more accurate insight into whether the system is under attack. Extraction of data in windows prevents data overload from occurring. Extracting features from the data allows for decomposition and makes the approach scalable. Small amounts of data act as representations of a larger dataset. As features are abstractions from the system data, it is fair to say that they will offer an accurate representation of system behaviour, which will keep dataset sizes to a minimum.

BOCISS has no control over the data, and simply taps into sources of information. The result is that there is no slowing or the effect of a bottleneck of data activity inside the system. This is an aspect, which is a weakness of both IDS and UTM systems currently used.

8.3 Future Directions

As the system matures, it is possible to incorporate other features, which would enhance the cyber-attack detection methodology. In this section, several possible future research projects stemming from this thesis are discussed.

8.3.1 Additional Data Sources

By incorporating addition data sources, in its assessment of the on-going system activity, BOCISS would be able to provide feedback that is more effective to the operator. Figure 96 displays alternative sources of information, which could contribute to the approach our system takes. Combining data intake with external sources of information such as dangerous weather patterns [194], power consumption or terrorist threat levels [178], [195], our system would be able to provide increasingly accurate readings of system behaviour.

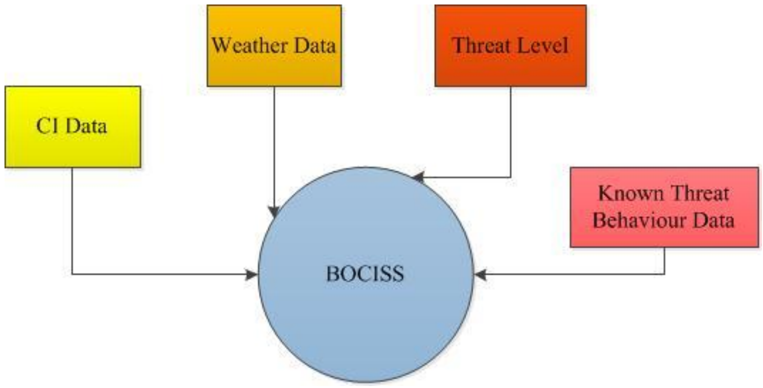


Figure 96 Future Work: BOCISS Data

As discussed in the thesis, weather patterns in particular have a tendency to affect critical infrastructures and produce alarms due to the disturbances caused to components. Increasing the sources of data input, particularly from components experiencing different weather patterns, would help reduce the level of false positive alerts.

8.3.3 Observer Network

Critical infrastructure security is referred to as having a hard outer shell with a soft gooey centre [83]. Figure 97 displays how different BOCISS observer units could be added into the various critical infrastructure layers.

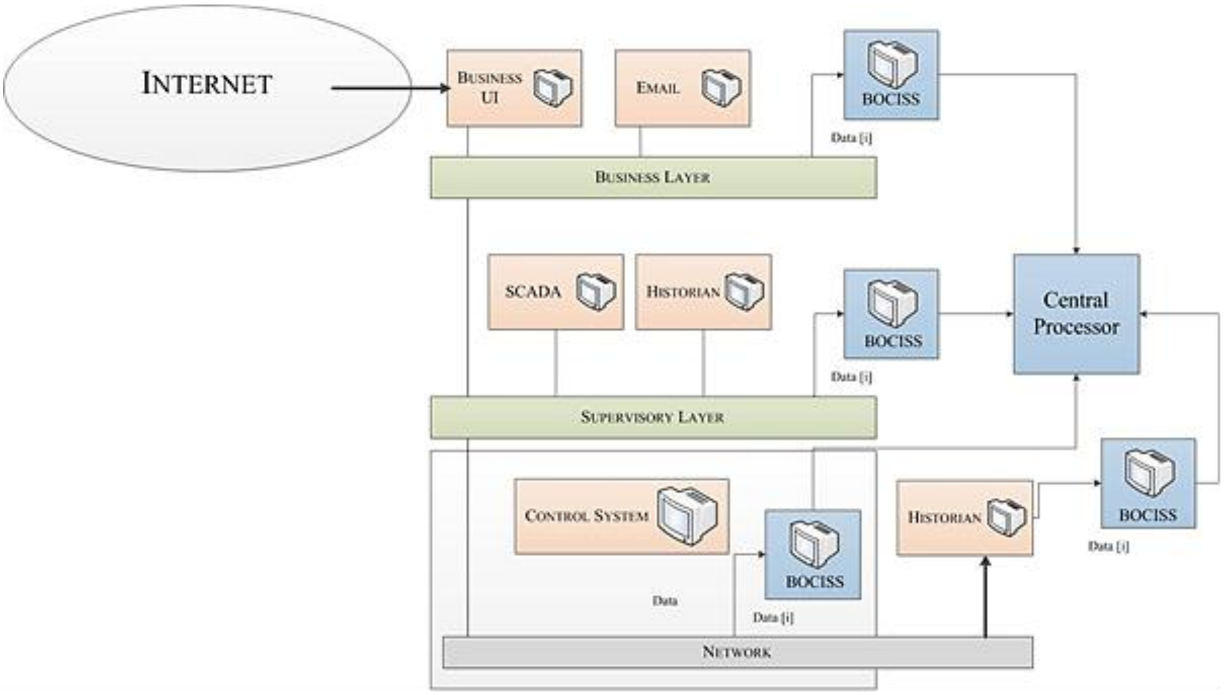


Figure 97 Future Work: BOCISS Network

Security has a tendency to focus on securing an outside layer and block intrusions with little security in place when a successful attack has taken place. Using our system, security can be implemented in depth by creating a network of observer devices. One observer per enclave and multiple observer units for different network groups could be linked together to provide a more multi-layered approach to security. This would improve the risk of the BOCISS itself being compromised by a cyber-attack.

8.3.4 Autonomous Feature Selection

As Figure 98 displays, future developments of BOCISS could include the enhanced selected of features through conducting an autonomous PCA and feature extraction process with the results presented to the operator for selection.

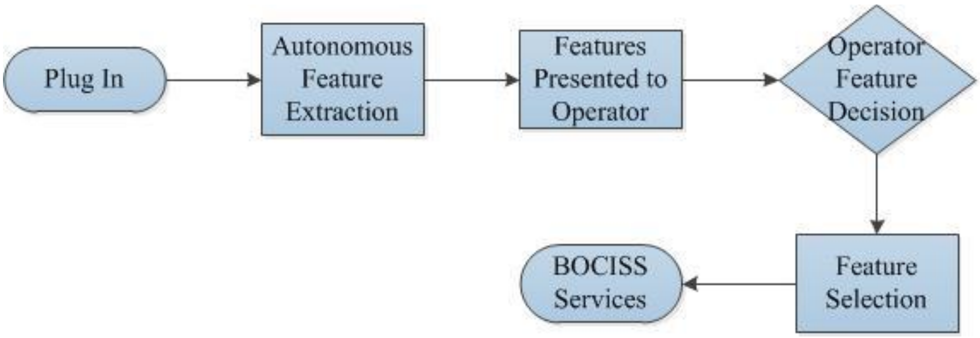

Plug In
Autonomous Feature Extraction
Features Presented to Operator
Operator Feature Decision
Feature Selection
BOCISS Services

Figure 98 Future Work: BOCISS Feature Selection

This approach would ensure the operator is presented with the features, which would be most ideal for achieving high data classification results.

8.5 Concluding Remarks

Critical infrastructures are growing in size and importance every year as the population grows and puts increasing demand on the unseen services provided. Protecting these infrastructures is clearly a key issue. Improved support, as well as helping with cost efficiency as billions are spent on cyber security, has benefits for the well-being of people and helps with the evolution and improvement of security. As threats increase it becomes clear that security may lie away from conventional computer security techniques and an original approach to critical infrastructure protection is required.

As threats evolve and become more adaptive, so should security measures used be able to adapt themselves by adopting new unconventional security techniques. The future lies with combating cyber-attack in an innovative way combining both techniques where behavioural observation is used along-side existing conventional security, working together to provide well-structured defence in depth.

The seriousness of critical infrastructure protection is clearly a key issue. Their vulnerability to the growing cyber-threat enforces this further. Defence in depth is a prominent factor, which must be taken into account when developing security. The aim of using our system is to provide functional support and enhance security. Through the development of a model of expected acceptable behaviour, by combining the network activity with the operational running of the infrastructure, threats can be identified.

Our research presents a way of improving critical infrastructure security by identifying threats, and unusual activity, through behavioural observation. Our technique, for critical infrastructure support, adds to the defence in depth that is currently in place. Using our approach, multi-level security is enhanced. Gathering more information about events taking place helps to deal with the unexpected, which is the aim of BOCISS. This research presents a new and adaptive solution to existing critical infrastructure security. Clearly, behaviour observation has a key role in security.

REFERENCES

[1] M. Merabti, M. Kennedy, and W. Hurst, “Critical infrastructure protection: A 21st century challenge,” in *2011 International Conference on Communications and Information Technology (ICCIT)*, 2011, pp. 1–6.

[2] I. Eusgeld and C. Nan, Creating a Simulation Environment for Critical Infrastructure Interdependencies Study, Proceedings of the Third IEEE International Conference on Industrial Engineering and Engineering Management, pp. 2104-2108, 2009.

[3] C. Wang, L. Fang, and Y. Dai, A Simulation Environment for SCADA Security Analysis and Assessment, Proceedings of the Second International Conference on Measuring Technology and Mechatronics Automation, pp. 342-347, 2010.

[4] S. J. League, Critical Infrastructure Protection- The Cyber/Information Dimension: Report on National Infrastructure Coordination Initiatives. Thirteenth Annual Computer Security Applications Conference, pp. 118-120, 1997.

[5] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies, IEEE Control Systems Magazine, Vol. 21 (6), pp 11-25, 2001.

[6] J. C. Knight, Safety Critical Systems: Challenges and Directions. Proceedings of the Twenty-Fourth International Conference on Software Engineering, pp 547-550, 2002.

[7] M. Shamir b. Hashim, Malaysia’s National Cyber Security Policy: The Country's Cyber Defence Initiatives. Proceedings of the Second Worldwide Cybersecurity Summit, pp 1-7, 2011.

[8] F. S. Yusufovna, F. A. Alisherovich, M. Choi, E. Cho, F. T. Abdurashidovich, and T. Kim, Research on Critical Infrastructures and Critical Information Infrastructures, Proceedings of the Third IEEE Symposium on Bio-inspired Learning and Intelligent Systems for Security, pp. 97-101, 2009

[9] N. K. Svendsen and S. D. Wolthusen, Analysis and Statistical Properties of Critical Infrastructure Interdependency Multiflow Models, Proceedings of the Third IEEE SMC Information Assurance and Security Workshop, pp. 247-254, 2007.

[10] C. M. Lawler and S. A. Szygenda, Components of Continuous IT Availability & Disaster Tolerant Computing, Proceedings of the IEEE Conference on Technologies for Homeland Security: Enhancing Critical Infrastructure Dependability, pp. 101–106, 2007.

[11] L. H. de Melo Leite, L. de Errico, and W. do Couto Boaventura, Criteria for the selection of communication infrastructure applied to power distribution automation, Proceedings of the IEEE PES Conference on Innovative Smart Grid Technologies (ISGT Latin America), pp. 1–8, 2013.

[12] M. Mafuta, M. Zennaro, A. Bagula, and G. Ault, Successful deployment of a Wireless Sensor Network for precision agriculture in Malawi, Proceedings of the Third IEEE International Conference on Networked Embedded Systems for Every Application (NESEA), pp. 1–7, 2012.

[13] S S. Amin, X. Litrico, S. S. Sastry, and A. M. Bayen, Stealthy deception attacks on water SCADA systems, Proceedings of the Thirteenth ACM international conference on Hybrid systems: computation and control - HSCC’10, p. 161, 2010.

[14] S. Simon, Autonomous Navigation in Rubber Plantations, Proceedings of the Second International Conference on Machine Learning and Computing, pp. 309–312, 2010.

[15] F. Cosmi, C. Fabro, P. Susmel, and G. Zoppello, Automation in dairy farms: a robotic milking system, Proceedings of the Eigth International Conference on Advanced Robotics. Proceedings. ICAR’97, pp. 33–37, 1997.

[16] A. Di Giorgio and F. Liberati, “A Bayesian Network-Based Approach to the Critical Infrastructure Interdependencies Analysis,” *IEEE Syst. J.*, vol. 6, no. 3, pp. 510–519, Sep. 2012.

[17] A. Di Giorgio and F. Liberati, A Bayesian Network-Based Approach to the Critical Infrastructure Interdependencies Analysis, IEEE Syst. J., vol. 6, no. 3, pp. 510–519, Sep. 2012.

[18] M. Langdon, Forecasting flood, Eng. Technol., vol. 4, no. 7, pp. 40–42.

[19] M. Sato, S.-W. Chen, and M. Satake, Polarimetric SAR Analysis of Tsunami Damage Following the March 11, 2011 East Japan Earthquake, Proc. IEEE, vol. 100, no. 10, pp. 2861–2875, Oct. 2012.

[20] M. Polycarpou, G. Ellinas, E. Kyriakides, and C. Panayiotou, Intelligent Health Monitoring of Critical Infrastructure Systems. Proceedings of the Third IEEE Conference on Complexity in Engineering (COMPENG), pp. 18-20, 2010.

[21] M. Rong, C. Han, and L. Liu, Critical Infrastructure Failure Interdependencies in the 2008 Chinese Winter Storm, Proceedings of the Second IEEE International Conference on Management and Service Science, pp. 1-4, 2010.

[22] C. Barrett, R. Beckman, K. Channakeshava, F. Huang, V. S. A. Kumar, A. Marathe, M. V. Marathe, and G. Pei, Cascading failures in multiple infrastructures: From transportation to communication network, in Proceedings of the Fifith International Conference on Critical Infrastructure (CRIS), pp. 1–8, 2010.

[23] L. Coyle, M. Hinchey, B. Nuseibeh, and J. L. Fiadeiro, Guest Editors' Introduction: Evolving Critical Systems, Computer (Long. Beach. Calif)., vol. 43, no. 5, pp. 28–33, May 2010.

[24] M. Brownfield, Y. Gupta, and N. Davis, Wireless sensor network denial of sleep attack, Proceedings from the Sixth Annual IEEE Systems, Man and Cybernetics (SMC) Information Assurance Workshop, pp. 356–364, 2005.

[25] C. Scarlat, C. Simion, and E. I. Scarlat, Managing new technology projects: Some considerations on risk assessment in the case of NPP critical infrastructures, Proceedings of the Second IEEE International Conference on Emergency Management and Management Sciences, pp. 911–915, 2011.

[26] M. Schlapfer, S. Dietz, and M. Kaegi, Stress induced degradation dynamics in complex networks, Proceedings of the First International Conference on Infrastructure Systems and Services: Building Networks for a Brighter Future (INFRA), pp. 1–5, 2008.

[27] G. O'Reilly, A. Jrad, R. Nagarajan, T. Brown, and S. Conrad, Critical Infrastructure Analysis of Telecom for Natural Disasters, in Networks. Proceedings of the Twelfth International Telecommunications Network Strategy and Planning Symposium, pp. 1–6, 2006.

[28] S. Braghin, I. N. Fovino, and A. Trombetta, Advanced trust negotiation in critical infrastructures, Proceedings of the First International Conference on Infrastructure Systems and Services: Building Networks for a Brighter Future (INFRA), pp. 1–6, 2008.

[29] S. Sridhar and G. Manimaran, Data Integrity Attacks and their Impacts on SCADA Control System, Proceedings of the Eighth IEEE PES General Meeting, pp. 1-6. 2010.

[30] J. Walker, B. J. Williams, and G. W. Skelton, Cyber Security for Emergency Management, Proceedings of the Fourth IEEE International Conference on Technologies for Homeland Security, pp. 476-480, 2010.

[31] A. Ghosh and G. McGraw, Lost Decade or Golden Era: Computer Security since 9/11, IEEE Secur. Priv. Mag., vol. 10, no. 1, pp. 6–10, Jan. 2012.

[32] E. J. Kartaltepe, Towards Blocking Outgoing Malicious Impostor Emails, Proceedings of the Second IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, pp. 657-661, 2006.

[33] R. Amin, J. Ryan, and J. van Dorp, Detecting Targeted Malicious Email Using Persistent Threat and Recipient Oriented Features, IEEE Secur. Priv. Mag., no. 99, pp. 1–1, 2011.

[34] S. Tang, The Detection of Trojan Horse Based on the Data Mining, Proceedings of the Sixth International Conference on Fuzzy Systems and Knowledge Discovery, pp. 311–314, 2009.

[35] D. Kushner, The real story of stuxnet, IEEE Spectr., vol. 50, no. 3, pp. 48–53, Mar. 2013.

[36] M. J. W. J.McIntyre, Protection of New Zealand in the age of Information Warfare, Proceedings of Protecting the infrastructure: the Third Australian Information Warfare and Security Conference, pp. 235-240, 2002.

[37] R. Langner, Stuxnet: Dissecting a Cyberwarfare Weapon, IEEE Secur. Priv. Mag., vol. 9, no. 3, pp. 49–51, May 2011.

[38] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, Inside the slammer worm, IEEE Secur. Priv. Mag., vol. 1, no. 4, pp. 33–39, Jul. 2003.

[39] Flamer: Highly Sophisticated and Discreet Threat Targets the Middle East | Symantec Connect Community. [Online]. Available: http://www.symantec.com/connect/blogs/flamer-highly-sophisticated-and-discreet-threat-targets-middle-east. [Accessed: 22-Jul-2013].

[40] S. Benson Edwin Raj and A. Annie Portia, Analysis on credit card fraud detection methods, Proceedings of the International Conference on Computer, Communication and Electrical Technology (ICCCET), pp. 152–156, 2011.

[41] Y. Zhang, F. You, and H. Liu, Behavior-Based Credit Card Fraud Detecting Model, Proceedings of the Fifth International Joint Conference on INC, IMS and IDC, pp. 855–858, 2009.

[42] S. Supakkul, T. Hill, L. Chung, T. T. Tun, and J. C. S. do Prado Leite, An NFR Pattern Approach to Dealing with NFRs, Proceedings of the Eighteenth IEEE International Requirements Engineering Conference, pp. 179-188, 2010.

[43] D. Voth and B. Alfonsi, In the News, IEEE Intell. Syst., vol. 21, no. 1, pp. 4–7, Jan. 2006.

[44] D. Prakash Geddam, V. Subramaniam, and P. Metharamitta, Distributed Power Plant Architecture in a Shared Infrastructure Network, Proceedings of the Thirty-Second IEEE Telecommunications Energy Conference (INTELEC), pp. 1-5, 2010.

[45] T. Bass, Intrusion detection systems and multisensor data fusion, Commun. ACM, vol. 43, no. 4, pp. 99–105, Apr. 2000.

[46] H. Pan, X. Yao, C. Qi, and H. Chen, A Category Theory Model for Learning and Memory of the Human Brain, Proceedings of the International Conference on Digital Manufacturing & Automation, pp. 11–14, 2010.

[47] E. O. Schweitzer, D. Whitehead, A. Risley, and R. Smith, How would we know?, Proceedings of he Sixty-Fourth Annual Conference for Protective Relay Engineers, pp. 310–321, 2011.

[48] W. Hurst, M. Merabti, and P. Fergus, Behavioural Analysis Techniques for Supporting Critical Infrastructure Security, *Inderscience Int. J. Crit. Infrastructures*, in press, 2013.

[49] W. Hurst, M. Merabti, and P. Fergus, Towards a Framework for Operational Support in Critical Infrastructures, Proceedings of the Twelfth Annual PostGraduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting, 2011.

[50] W. Hurst, M. Merabti, and P. Fergus, Behavioural Observation for Critical Infrastructure Security Support, Proceedings of the Seventh IEEE European Modelling Symposium (EMS2013), 2013.

[51] W. Hurst, M. Merabti, and P. Fergus, Operational Support for Critical Infrastructure Security, Proceedings of the Fourteenths IEEE International Conference on High Performance Computing and Communication & The Ninth International Conference on Embedded Software and Systems (HPCC-ICESS), pp. 1473–1478, 2012..

[52] L. Pla Beltran, M. Merabti, and W. Hurst, Using Behavioural Observation and Game Technology to Support Critical Infrastructure Security, *Inderscience Int. J. Syst. Syst.*, in press, 2013.

[53] W. Hurst, M. Merabti, and P. Fergus, Behavioural Analysis for Supporting Critical Infrastructure Security, Proceedings of the Fourteenth Annual Post Graduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting, 2013.

[54] W. Hurst, M. Merabti, and P. Fergus, Big Data Analysis Techniques for Cyber-Threat Detection in Critical Infrastructures, Proceedings of the Eight International Workshop on Telecommunication Networking Applications and Systems, 2014.

[55] W. Hurst, M. Merabti, and P. Fergus, Managing Critical Infrastructures through Behavioural Observation, Proceedings of the Third IEEE International Conference on Networked Embedded Systems for Every Application (NESEA), 2012, pp. 1–6.

[56] W. Hurst, M. Merabti, S. Iram, and P. Fergus, Protecting Critical Infrastructures Through Behavioural Observation, Inderscience Int. J. Crit. Infrastructures, 2013.

[57] J. Dehlinger, J. B. Dugan, M. Veeraraghavan, and M. McGinley, “Continuous open design of dependable systems for critical infrastructure,” in *2009 ICSE Workshop on Emerging Trends in Free/Libre/Open Source Software Research and Development*, 2009, pp. 48–53.

[58] DPSTelecom, Do You Know These Key SCADA Concepts? SCADA Tutorial: A Quick, Easy, Comprehensive Guide. pp. 1–12, 2011.

[59] D.-J. Kang, J.-J. Lee, S.-J. Kim, and J.-H. Park, Analysis on Cyber Threats to SCADA Systems. Proceedings of the IEEE Transmission and Distribution Conference and Exposition: Asia and Pacific, pp. 1-4, 2009.

[60] Z. Shuting and Y. Zhijia, A high performance architecture design of PLC dedicated processor, Proceedings of the Third International Conference on Advanced Computer Theory and Engineering(ICACTE), pp. V2–424–V2–428, 2010.

[61] K. W. Leucht and G. S. Semmel, Automated Translation of Safety Critical Application Software Specifications into PLC Ladder Logic, Proceedings of the IEEE Aerospace Conference, pp. 1–14, 2008

[62] O. Pavlovic and H.-D. Ehrich, Model Checking PLC Software Written in Function Block Diagram, Proceedings of the Third International Conference on Software Testing, Verification and Validation, pp. 439–448, 2010.

[63] M. Obermeier, D. Schutz, and B. Vogel-Heuser, Evaluation of a newly developed model-driven PLC programming approach for machine and plant automation, Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics (SMC), pp. 1552–1557, 2012.

[64] E. Estevez, M. Marcos, E. Irisarri, F. Lopez, I. Sarachaga, and A. Burgos, A novel approach to attain the true reusability of the code between different PLC programming tools, Proceedings of the IEEE International Workshop on Factory Communication Systems, pp. 315–322, 2008.

[65] B. E. Markwalter and S. K. Fitzpatrick, CEBus network layer description, IEEE Trans. Consum. Electron., vol. 35, no. 3, pp. 571–576, 1989.

[66] L. Loroch, P. Madrzycki, and M. Swiech, The Integrated Airbase Protection System, In Proceedings of the Third IEEE International Conference on Recent Advances in Space Technologies, pp. 119-122, 2007.

[67] T. Jankowski, G. Davis, J. Holmes, and G. Kemper, Increasing data historian efficiency, Proceedings of the Fifty-Third IEEE Cement Industry Technical Conference-IAS/PCA, pp. 1–14, 2011.

[68] M. van Doorn, Resilient Wireless Data Communication for Critical Infrastructure, Proceedings of the Fourth Power Systems Conference and Exposition, pp. 1-5, 2011.

[69] K. Claffy, S. O. Bradner, and S. D. Meinrath, The (un)Economic Internet?, IEEE Internet Comput., vol. 11, no. 3, pp. 53–58, May 2007.

[70] Z. Anwar, R. Shankesi, and R. H. Campbell, Automatic security assessment of critical cyber-infrastructures. IEEE, 2008, pp. 366–375.

[71] S. M. Rinaldi, Modeling and Simulating Critical Infrastructures and their Interdependencies, Proceedings of the Thirty-Seventh IEEE Annual Hawaii International Conference on System Sciences, pp. 8-pp, 2004.

[72] The Courier Times and Intelligencer: Made in the USA Series, Bringing manufacturing back to America, July 1 - 3. [Available at http://www.phillyburbs.com/news/local/courier_times_news/opinion/guest/made-in-the-usa-bringing-manufacturing-back-to-america/article_5afc2e05-6140-5b19-a1d3-47a1ca12511e.html] Acessed July, 2013.

[73] M. Hall-May and M. Surridge, Resilient Critical Infrastructure Management Using Service Oriented Architecture, Proceedings of the Fourth IEEE International Conference on Complex, Intelligent and Software Intensive Systems, pp. 1014-1021, 2010.

[74] M. Kaâniche, Resilience Assessment of Critical Infrastructures: From Accidental to Malicious Threats, Proceedings of the Fifth IEEE Latin-American Symposium on Dependable Computing Workshops, pp. 35-36, 2011.

[75] R. Anderson and S. Fuloria, Who Controls the off Switch?, Proceedings of the First IEEE International Conference on Smart Grid Communications, pp. 96–101 2010.

[76] L. H. de Melo Leite, L. de Errico, and W. do Couto Boaventura, Criteria for the selection of communication infrastructure applied to power distribution automation, Proceedings of the IEEE PES Conference on Innovative Smart Grid Technologies (ISGT Latin America), pp. 1–8, 2013.

[77] A. M. Hemeida, M. Z. El-Sadek, and S. A. Younies, Distributed Control System Approach for a Unified Power System. Proceedings of the Thirty-Ninth International Universities Power Engineering Conference, pp. 304-307, 2004.

[78] C. Esposito, D. Cotroneo, R. Barbosa, and N. Silva, Qualification and Selection of Off-the-Shelf Components for Safety Critical Systems: A Systematic Approach, Proceedings of the Fifth Latin-American Symposium on Dependable Computing Workshops, pp. 52–57, 2011.

[79] V. Urias, B. Van Leeuwen, and B. Richardson, Supervisory Command and Data Acquisition (SCADA) system cyber security analysis using a live, virtual, and constructive (LVC) testbed, Proceedings of the IEEE Military Communications Conference, (MILCOM), pp. 1–8, 2012.

[80] P. Naghshtabrizi and J. P. Hespanha, Analysis of distributed control systems with shared communication and computation resources, Proceedings of the American Control Conference, pp. 3384–3389, 2009.

[81] H.-C. Lapp, C. Gerber, and H.-M. Hanisch, Improving verification and reliability of distributed control systems design according to IEC 61499, Proceedings of the Fifteenth IEEE Conference on Emerging Technologies & Factory Automation (ETFA 2010), pp. 1–8, 2010.

[82] M. Siddique and A. Javeed, PC based SCADA implementation on circulatory fluidized bed combustioner, Proceedings of the Fourteenth International Multitopic Conference, pp. 250–254, 2011.

[83] E. Knapp and J. Broad, Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA and Other Industrial Control Systems, Syngress, Elsevier, 2011.

[84] I. N. Fovino, A. Carcano, T. D. L. Murel, A. Trombetta, and M. Masera, Modbus/DNP3 State-Based Intrusion Detection System, Proceedings of the Twenty-Fourth IEEE International Conference on Advanced Information Networking and Applications, pp. 729–736, 2010.

[85] I. N. Fovino, M. Masera, L. Guidi, and G. Carpi, An experimental platform for assessing SCADA vulnerabilities and countermeasures in power plants, Proceedings of the Third International Conference on Human System Interaction, 2010, pp. 679–686.

[86] European Commission Press Release, Digital Agenda: Cyber-Security Experts Test Defences in First Pan-European Simulation, June 12, 2010.

[87] M. Golling and B. Stelte, Requirements for a future EWS - Cyber Defence in the internet of the future, Proceedings of the Third International Conference on Cyber Conflict, pp. 1-16 2001.

[88] J. Li, J. Tong, and D. Mao, Influence of DC supply systems on unplanned reactor trips in nuclear power plants, vol. 6, no. 1. pp. 84–88, 2001.

[89] F. Walker, M. Mackay, and M. Merabti, Links to the Future: Communication Requirements and Challenges in the Smart Grid, IEEE Power Energy Mag., vol. 10, no. 1, pp. 24–32, 2012.

[90] T. M. Wilson, C. Stewart, V. Sword-Daniels, G. S. Leonard, D. M. Johnston, J. W. Cole, J. Wardman, G. Wilson, and S. T. Barnard, Volcanic ash impacts on critical infrastructure, Phys. Chem. Earth, Parts A/B/C, Jun. 2011.

[91] C. Barrett, R. Beckman, K. Channakeshava, F. Huang, V. Kumar, A. Marathe, and M. Marathe, Cascading Failures in Multiple Infrastructures: From Transportation to Communication Network, Proceedings of the IEEE International Conference on Critical Infrastructures, pp. 1–8, 2010.

[92] C. Davis and J. Tate, SCADA Cyber Security Testbed Development, Proceedings of the Thirty-Eighth IEEE North American Power Symposium, pp. 483 - 488, 2006.

[93] S. D. Wolthusen, GIS-based Command and Control Infrastructure for Critical Infrastructure Protection, Proceedings of the First IEEE International Workshop on Critical Infrastructure Protection (IWCIP'05), pp. 40–50, 2005.

[94] M. Chaturvedi, M. Gupta, and J. Bhattacharya, Cyber Security Infrastructure in India: A Study, CSI Publ. Emerg. Technol. E-Government, pp. 70–84, 2008.

[95] M. Harper, IT Application Downtime, Executive Visibility and Disaster Tolerant Computing. Proceedings of the International Conference on cybernetics and Information Technologies, Systems and Applications and International Conference on Information Systems Analysis and Synthesis, pp 165-170, 2005.

[96] H. Khurana, Moving beyond defense-in-depth to strategic resilience for critical control systems, Proceeings of the IEEE Power and Energy Society General Meeting, pp. 1–3, 2011.

[97] W. K. G. Seah, Z. A. Eu, and H.-P. Tan, Wireless sensor networks powered by ambient energy harvesting (WSN-HEAP) - Survey and challenges, Proceedings of the First International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology, pp. 1–5, 2009.

[98] D. R. Raymond, R. C. Marchany, M. I. Brownfield, and S. F. Midkiff, Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols, IEEE Trans. Veh. Technol., vol. 58, no. 1, pp. 367–380, Jan. 2009.

[99] J. Yick, B. Mukherjee, and D. Ghosal, Wireless sensor network survey, Comput. Networks, vol. 52, no. 12, pp. 2292–2330, Aug. 2008.

[100] L. Buttyan, D. Gessner, A. Hessler, and P. Langendoerfer, Application of Wireless Sensor Networks in Critical Infrastructure Protection: Challenges and Design Options [Security and Privacy in Emerging Wireless Networks], IEEE Wireless Communications Journal, 17(5), 44-49. 2010.

[101] A. Patchimpattapong, Development of Thailand's first nuclear power plant, Proceedings of the International Conference on Energy and Sustainable Development: Issues and Strategies (ESD 2010), pp. 1–3, 2010.

[102] Y. Xu, Z. Wang, W. Sun, S. Chen, Y. Wu, and B. Zhao, Unit commitment model considering nuclear power plant load following, Proceedings of the International Conference on Advanced Power System Automation and Protection, vol. 3, pp. 1828–1832, 2011.

[103] L. Yu-fan, Simple Analysis about the Environment Protection and Design of Nuclear Power Plant, Proceedings of the Third International Conference on Measuring Technology and Mechatronics Automation, vol. 3, pp. 233–235, 2011.

[104] Li Xiong, Dichen Liu, Bo Wang, Ping Wu, Jie Zhao, and Xi Shi, Dynamic characteristics analyse of pressurized water reactor Nuclear Power plant based on PSASP, Proceedings of the Fourth IEEE Conference on Industrial Electronics and Applications, pp. 3629–3634, 2009.

[105] S. D. Wolthusen, Modeling critical infrastructure requirements, in Proceedings from the Fifth Annual IEEE SMC Information Assurance Workshop, 2004, pp. 101–108, 2004.

[106] P. Katsumata, J. Hemenway, and W. Gavins, Cybersecurity risk management, Proceedings of the Military Communications Conference - MILCOM 2010, pp. 890–895, 2010.

[107] T. Dyhouse, A unified framework for it security - analysis - [IT security], Eng. Technol., vol. 4, no. 11, pp. 58–58, 2009.

[108] BBC News, UK ‘has cyber attack capability’, [Online Available: http://news.bbc.co.uk/1/hi/uk_politics/8118729.stm], Accessed August 2009..

[109] European Commission, Green Paper on a European Program for Critical Infrastructure Protection, Com(2005), vol. 576 Final, 2005.

[110] M. Abu Rajab, J. Zarfoss, F. Monrose, and A. Terzis, A multifaceted approach to understanding the botnet phenomenon, Proceedings of the Sixth Internation Conference on Internet measurement - ACM SIGCOMM - IMC’06, p. 41, 2006.

[111] C. W. Johnson and K. McLean, Tools for Local Critical Infrastructure Protection : Computational Support for Identifying Safety and Security Interdependencies between Local Critical Infrastructures, y, Proceedings of the Third IET International Conferenceon Systems Safety, pp. 1–6, 2008.

[112] H. Zhang, J. Ma, Y. Wang, and Q. Pei, An Active Defense Model and Framework of Insider Threats Detection and Sense, Proceedings of the Fifth International Conference on Information Assurance and Security, pp. 258–261, 2009.

[113] D. K. Hitchins, Secure systems - Defence in Depth, IEEE European Convention on Security and Detection, pp. 34-39, 1995.

[114] F. Rocha, T. Gross, and A. van Moorsel, Defense-in-Depth Against Malicious Insiders in the Cloud, Proceedings of the IEEE International Conference on Cloud Engineering (IC2E), pp. 88–97, 2013.

[115] B. Mukherjee, L. T. Heberlein, and K. N. Levitt, Network intrusion detection, IEEE Netw., vol. 8, no. 3, pp. 26–41, 1994..

[116] P. Nowak, B. Sakowicz, G. Anders, and A. Napieralski, Intrusion Detection and Internet Services Failure Reporting System, Proceedings of the Second IEEE International Conference on Dependability of Computer Systems, pp. 185-190, 2007.

[117] Y. Zhang, F. Deng, Z. Chen, Y. Xue, and C. Lin,. UTM-CM: A Practical Control Mechanism Solution for UTM System, Proceedings of the Second IEEE International Conference on Communications and Mobile Computing, pp. 86-90, 2010.

[118] G. and C. K. Vigna, Host-based Intrusion Detection. Handbook of Information Security. 2005, pp. 1–13..

[119] R. Sekar, T. Bowen, and M. Segal, On preventing intrusions by process behavior monitoring. In Proceedings of the Symposium on Operating Sytem Design and Implementaion (OSDI II), 1999.

[120] P. Li, Z. Wang, and X. Tan, Characteristic Analysis of Virus Spreading in Ad Hoc Networks, Proceedings of the International Conference on Computational Intelligence and Security Workshops (CISW 2007), pp. 538–541, 2007.

[121] F. Deng, A. Luo, Y. Zhang, Z. Chen, X. Peng, X. Jiang, and D. Peng, TNC-UTM: A Holistic Solution to Secure Enterprise Networks, Proceedings of the Ninth International Conference for Young Computer Scientists, pp. 2240-2245, 2008.

[122] H.-Y. Xue, MultiCore Systems Architecture Design and Implementation of UTM, Proceedings of the First IEEE International Symposium on Information Science and Engineering, pp. 441-445, 2008.

[123] Y. Qi, B. Yang, B. Xu, and J. Li, Towards System-level Optimization for High Performance Unified Threat Management. Proceedings of the IEEE International Conference on Networking and Services (ICNS '07), pp. 7–7, 2007.

[124] B. Snyder, Case Study: UTM's weakness: a single point of failure, Techworld [Available at http://howto.techworld.com/security/4037/case-study-utms-weakness-a-single-point-of-failure], March, 2008.

[125] C. Kreibich and J. Crowcroft, Honeycomb: creating intrusion detection signatures using honeypots, ACM SIGCOMM Computer Communications Review, vol. 34 issue:1, pp. 51-5, 2004.

[126] J. L. Rrushi, An exploration of defensive deception in industrial communication networks, Elsevier International Journal of Critical Infrastructure Protection, vol. 4, no. 2, pp. 66–75, Aug. 2011.

[127] T. I. Morris, L. M. Mayron, W. B. Smith, M. M. Knepper, R. Ita, and K. L. Fox, A perceptually-relevant model-based cyber threat prediction method for enterprise mission assurance, Proceeings of the IEEE

International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), pp. 60–65, 2011.

[128] S. Yang, J. Holsopple, and M. Sudit, Evaluating Threat Assessment for Multi-Stage Cyber Attacks, Proceeding of the IEEE Military Communications Conference - MILCOM, pp. 1–7, 2006.

[129] McAfee Foundstone Professional Services and McAfee Labs, Global Energy Cyberattacks:"Night Dragon", Santa Clara, CA, USA, url {www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf}, Feb 10 2011.

[130] M. Dogrul, A. Aslan, and E. Celik, Developing an international cooperation on cyber defense and deterrence against Cyber terrorism, Proceedings of the Third International Confefence on Cyber-Conflict - (ICCC), pp. 1–15, 2011.

[131] S. Pritchard, Securing the 2012 Olympics, Infosecurity, vol. 6, no. 6, pp. 12–15, Sep. 2009.

[132] European Commission, Digital Agenda: cyber-security experts test defences in first pan-European simulation, European Commission Press Release, 2010.

[133] ENISA, Cyber Europe 2010 Evaluation Report, European Network and Information Security Agency, [Online Available: www.enisa.europa.eu], Accessed April 2011.

[134] European Commission, Communication from the Commission to the European Parliament and the Council: The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, Com(2010), vol. 673 final, 2010.

[135] J. Wang, R. C.-W. Phan, J. N. Whitley, and D. J. Parish, *Augmented Attack Tree Modeling of Distributed Denial of Services and Tree Based Attack Detection Method*. IEEE, 2010, pp. 1009–1014.

[136] A. B. M. A. Al Islam and T. Sabrina, Detection of various denial of service and Distributed Denial of Service attacks using RNN ensemble, Proceedings of the Twelfth International Conference on Computers and Information Technology, pp. 603–608, 2009.

[137] M. H. Islam, K. Nadeem, and S. A. Khan, Optimal Placement of Detection Nodes against Distributed Denial of Service Attack, Proceedings of the International Conference on Advanced Computer Control, pp. 675–679, 2009.

[138] Y. Wang, H. Wang, Z. Li, and J. Huang, Man-in-the-middle attack on BB84 protocol and its defence, Proceedings of the Second IEEE International Conference on Computer Science and Information Technology, pp. 438–439, 2009.

[139] R. K. Guha, Z. Furqan, and S. Muhammad, Discovering Man-in-the-Middle Attacks in Authentication Protocols, Proceedings of the IEEE - IEEE Military Communications Conference - MILCOM, pp. 1–7, 2007.

[140] W. D. Yu, S. Nargundkar, and N. Tiruthani, A phishing vulnerability analysis of web based systems, Proceedings of the IEEE Symposium on Computers and Communications, pp. 326–331, 2008.

[141] Y. Joshi, D. Das, and S. Saha, Mitigating man in the middle attack over secure sockets layer, Proceedings of the IEEE International Conference on Internet Multimedia Services Architecture and Applications (IMSAA), pp. 1–5, 2009.

[142] M. Khonji, Y. Iraqi, and A. Jones, Mitigation of spear phishing attacks: A Content-based Authorship Identification framework, Proceedings of the International Conference for Internet Technology and Secured Transactions (ICITST), pp. 416–421, 2011.

[143] J. Wang, T. Herath, R. Chen, and A. Vishwanath, Research Article Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email, Prof. Commun. IEEE Trans., vol. 55, no. 4, pp. 345–362, 2012.

[144] M. Feily, A. Shahrestani, and S. Ramadass, A Survey of Botnet and Botnet Detection, Proceedings of the Third International Conference on Emerging Security Information, Systems and Technologies, pp. 268–273, 2009.

[145] N. Lambert and K. S. Lin, Use of Query tokenization to detect and prevent SQL injection attacks, Proceedings of the Third IEEE International Conference on in Computer Science and Information Technology (ICCSIT), pp. 438–440, 2010.

[146] K. Wei, M. Muthuprasanna, and S. Kothari, Preventing SQL injection attacks in stored procedures, Proceedings of the Australian Software Engineering Conference, 2006.

[147] N. Nicholson, SCADA Security in the light of Cyber-Warfare, Elsevier Comput. Secur. J., vol. 31, no. 4, pp. 418–436, 2012.

[148] S. D. J. McArthur, E. M. Davidson, J. A. Hossack, and J. R. McDonald, Automating power system fault diagnosis through multi-agent system technology, Proceedings of the Thirty-Seventh Annual Hawaii International Conference on System Sciences, pp. 8, 2004.

[149] M. B. A. Hamid and T. K. A. Rahman, Short Term Load Forecasting Using an Artificial Neural Network Trained by Artificial Immune System Learning Algorithm, Proceedings of the Twelfth International Conference on Computer Modelling and Simulation, pp. 408–413, 2010.

[150] K. Littlewood, Special Issue Papers: Forecasting and control of passenger bookings, J. Revenue Pricing Manag., vol. 4, no. 2, pp. 111–123, Apr. 2005.

[151] G. E. P. Box, G. M. Jenkins, and G. C. Reinsel, Time Series Analysis: Forecasting and Control (Google eBook). John Wiley & Sons, 2013, p. 746.

[152] B. Atlagic, M. Sagi, D. Milinkov, B. Bogovac, and S. Culaja, A Way towards Efficiency of SCADA Infrastructure, Proceeedings of the Nineteenth IEEE International Conference and Workshops on Engineering of Computer-Based Systems, pp. 74–81, 2012.

[153] T. Bass, Multisensor Data Fusion for Next Generation Distributed Intrusion Detection Systems, Proceedings of the IRIS National Symposium on Sensor and Data Fusion, 2002.

[154] S. Roschke, F. Cheng, and C. Meinel, A Flexible and Efficient Alert Correlation Platform for Distributed IDS, Proceedings of the Fourth IEEE International Conference on Network and System Security, pp. 24-31, 2010.

[155] L. Coppolino, S. D'Antonio, L. Romano, and G. Spagnuolo, An Intrusion Detection System for Critical Information Infrastructures using Wireless Sensor Network technologies, Proceedings of the Fifth IEEE International Conference on Critical Infrastructure (CRIS), pp. 1-8, 2010.

[156] E. Hooper, An Intelligent Detection and Response Strategy to False Positives and Network Attacks: Operation of Network Quarantine Channels and Feedback Methods to IDS, Proceedings of the Second IEEE International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, pp. 16-21, 2006..

[157] D. Prochazkova, Safety culture and critical infrastructure safety, Proceedings of the IEEE International Conference on Vehicular Electronics and Safety,pp. 263–268, 2011.

[158] A. T. Murray and T. H. Grubesic, Critical infrastructure protection: The vulnerability conundrum, Telemat. Informatics, vol. 29, no. 1, pp. 56–65, May 2011.

[159] A. Nusimow, Intelligent Video for Homeland Security Applications, Proceedings of the IEEE Conference on Technologies for Homeland Security, pp. 139–144, 2007.

[160] European Commission, Protecting Europe from large scale cyber attacks and disruptions: enhancing prepardness, security and resilience., COM(2009)149, vol. SEC(2009) , 2009.

[161] European Commission, Proposal for a Regulation of the European Parliament and of the Council Concerning the European Network and Infromation Secuirty Agency (ENISA), Com(2010)521 Final, no. Sec (2010) 1126, Sec (2010) 1127, 2010..

[162] ENISA, EISAS European Information Sharing and Alert System for Citizens and SMEs: A Roadmap for further development and deployment, 2011.

[163] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Infromation Infrastructure Protection ‘Achivements and next steps: towards global cyber-secu, 2011.

[164] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Infromation Infrastructure Protection. Protecting Europe from large scale cyber attacks and , vol. SEC(2009) , no. COM(2009) 149 final, 2009.

[165] McDonogh, Opinion of the European Economic and Socail Committee on the ‘Communication from the Commission to the European Parliament, the Counil, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Prot, Off. J. Eur. Union, vol. COM(2009), no. 149 final, 2010.

[166] S. Iram, D. Al-Jumeily, P. Fergus, M. Randles, and A. Hussain, Computational Data Analysis for Movement Signals Based on Statistical Pattern Recognition Techniques for Neurodegenerative Diseases, Proceedings of the Thirteenth Annual Post Graduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting, 2012..

[167] W. Hurst, M. Merabti, S. Iram, and P. Fergus, Protecting Critical Infrastructures Through Behavioural Observation, *Inderscience Int. J. Crit. Infrastructures*, in press, 2013.

[168] K. C. C. Chan, Mining fuzzy association rules in a bank-account database, IEEE Trans. Fuzzy Syst., vol. 11, no. 2, pp. 238–248, Apr. 2003.

[169] H. Ma and X. Li, Application of Data Mining in Preventing Credit Card Fraud, Proceedings of the International Conference on Management and Service Science, pp. 1–6, 2009.

[170] W. Fu, Application of the Genetic Algorithm in the process of the distributing credit card, Proceedingd of the IEEE International Conference on Computer Science and Automation Engineering, pp. 399–402, 2012.

[171] Y. Li and J. C. S. Lui, On detecting malicious behaviors in interactive networks: Algorithms and analysis, Proceedings of the Fourth International Conference on Communication Systems and Networks (COMSNETS), 2012, pp. 1–10, 2012.

[172] T. Bass, Service-oriented horizontal fusion in distributed coordination-based systems, Mil. Commun. Conf. 2004. MILCOM 2004. IEEE, pp. 615–621, 2004.

[173] P. Blauensteiner, M. Kampel, C. Musik, and S. Vogtenhuber, A socio-technical approach for event detection in security critical infrastructure, Proceedingds of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition - Workshops, pp. 23–30, 2010.

[174] E. B. Fernandez and M. M. Larrondo-Petrie, Designing Secure SCADA Systems Using Security Patterns, Proceedings of the Fourty-Third Hawaii International Conference on System Sciences, pp. 1–8, 2010.

[175] R. Ding, R. Zhao, and L. Han, An Automatic Computation and Data Decomposition Algorithm of Prioritized Dominant Array, Proceedings of the Thirteenth International Conference on Parallel and Distributed Computing, Applications and Technologies, pp. 305–308, 2012.

[176] X. Wu, Z. Guo, and H. Zhang, General method for empirical data decomposition filtering design, Proceedings of the Eleventh IEEE International Conference on Signal Processing, vol. 1, pp. 732–736, 2012.

[177] J. Hernantes, A. Lauge, L. Labaka, E. Rich, F. O. Sveen, J. M. Sarriegi, I. J. Martinez-Moyano, and J. J. Gonzalez, Collaborative Modeling of Awareness in Critical Infrastructure Protection, Proceedings of the Forty-Fourth IEEE Hawaii Internation Conference on Systems Science, pp. 1-10, 2011.

[178] S. Singh, J. Allanach, J. Areta, P. Willett, and K. Pattipati, Modeling threats, IEEE Potentials, vol. 23, no. 3, pp. 18–21, Aug. 2004.

[179] M. Raciti, J. Cucurull, and S. Nadjm-Tehrani, Anomaly Detection in Water Management Systems, Crit. Infrastruct. Prot., vol. 7130, no. 2012, pp. 98–119, 2012.

[180] C. Ko, G. Fink, and K. Levitt, Automated detection of vulnerabilities in privileged programs by execution monitoring, Proceedings of the Tenth Annual Computer Security Applications Conference, pp. 134–144, 1994.

[181] I. N. Fovino, A. Carcano, and M. Masera, A Secure and Survivable Architecture for SCADA Systems, Proceedings of the Second IEEE International Conference on Dependability, pp. 34–39, 2009.

[182] V. Chandola, A. Banerjee, and K. Vipin, Anomaly Detection: A Survey, ACM Computing Surveys, 2009.

[183] W. Hurst, M. Merabti, and P. Fergus, Behavioural Observation for Critical Infrastructure Support, in *13th Annual Post Graduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting*, 2012.

[184] Z. Xu;, I. King, M. R.-T. Lyu, and R. Jin, Discriminative Semi-Supervised Feature Selection Via Manifold Regularization, IEEE Trans. Neural Networks, vol. 21, no. 7, pp. 1033–1047, 2010.

[185] S. Deegalla and H. Boström, Improving Fusion of Dimensionality Reduction Methods for Nearest Neighbor Classification, Proceedings of the International Conference on Machine Learning and Applications, pp. 771–775, 2009.

[186] Principal Component Analysis l: Principal Component Analysis software | Principal Component Analysis Tutorial | Statistics package for Excel - XLSTAT. [Online]. Available: http://www.xlstat.com/en/learning-center/tutorials/running-a-principal-component-analysis-pca-with-xlstat.html

[187] E. Kuncheva, L, Combining Pattern Classifiers: Methods and Algorithms, IEEE Transactions Neural Networks, vol. 18, issue: 3, 2004..

[188] P. Fergus, P. Cheung, A. Hussain, D. Al-Jumeily, C. Dobbins, and S. Iram, Prediction of Preterm Deliveries from EHG Signals Using Machine Learning, PLoS One, vol. 8, no. 10, p. e77154, Oct. 2013.

[189] R. P. Duin, P. Juszczak, P. Paclik, P. Pakalska, D. De Ridder, D. M. . Tax, and S. Verzakov, A Matlab Toolbox for Pattern Recognition, Version 4. Delft Pattern Recognition Research, 2007.

[190] F. Lotte, Study of Electroencephalographic Signal Processing and Classification Techniques towards the use of Brain-Computer Interfaces in Virtual Reality Applications, 2009.

[191] S. B. Kotsiantis, Supervised Machine Learning: A Review of Classification Techniques. Informatica 31:249–268, 2007

[192] N. Marom, L. Rokach, and A. Shmilovici, Using the Confusion Matrix for Improving Ensemble Classifiers, Proceedings of the Twenty-Sixth IEEE Convention of Electrical and Electronics Engineers in Israel, pp. 000555–000559, 2010.

[193] N. J. Salkind, Statistics for people who (think they) hate statistics, Third Ediction, Sage Publications, 2008.

[194] A. L. V. Frauche, M. B. de Carvalho, and E. A. B. da Silva, 3D weather radar image compression using multiscale recurrent patterns, Proceedings of the Fifteenth IEEE International Conference on Image Processing, pp. 1049–1052, 2008.

[195] H. Auld and D. Maclver, Changing Weather Patterns, Uncertainty and Infrastructure Risks: Emerging Adaptation Requirements, Proceedings of the IEEE EIC Climate Change Conference, pp. 1–10, 2006.

APPENDIX A - DATA

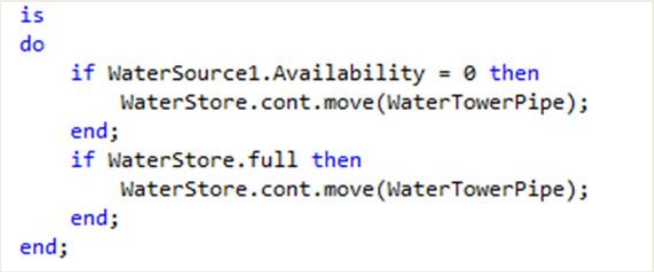
SIMULATION SETUP & CODE

To create a system where the components interact with each other, the programming language SimTalk is employed. The use of SimTalk implements a ‘Method’, which either reacts to events during runtime or alters the behaviour of a specific component. A Method is a function, which allows for simulation customisation by containing the SimTalk code.

Water Mechanisms:

In order to implement sensors in the water mechanisms we used Methods, which were coded using SimTalk to provide individual readings. SimTalk was also used to inform the Water Tower when it is required to provide water to the system.

The code to achieve this involves instructing the water tower to empty its contents based on the state of the water source. To prevent the water tower from overflowing it is instructed to empty its contents to the system upon reaching full capacity. The code to achieve this is illustrated below in Figure 99.

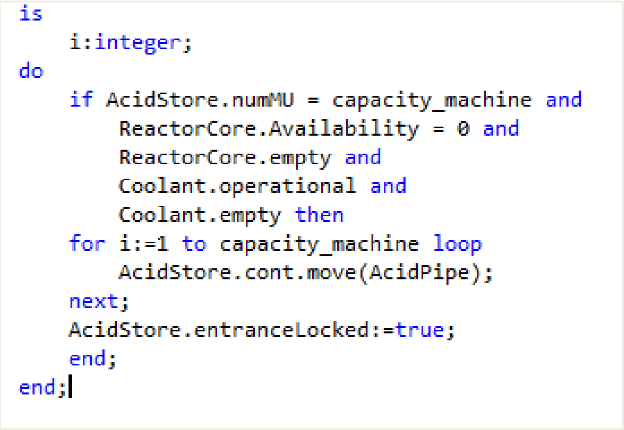


```
is
do
    if WaterSource1.Availability = 0 then
        WaterStore.cont.move(WaterTowerPipe);
    end;
    if WaterStore.full then
        WaterStore.cont.move(WaterTowerPipe);
    end;
end;
```

Figure 99 Water Source Code

Acid and Emergency Water tanks:

The acid tank control is illustrated in Figure 100.



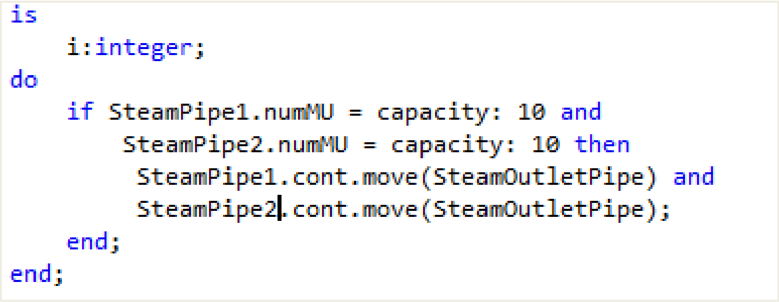
```
is
    i:integer;
do
    if AcidStore.numMU = capacity_machine and
        ReactorCore.Availability = 0 and
        ReactorCore.empty and
        Coolant.operational and
        Coolant.empty then
    for i:=1 to capacity_machine loop
        AcidStore.cont.move(AcidPipe);
    next;
    AcidStore.entranceLocked:=true;
    end;
end;
```

Figure 100 Simulation Emergency Tank Control Code

The code functions by locking the store if all the various conditions are met including: if the reactor core is functioning; if the core has coolant and if the coolant system is operational. If these conditions are not met, the code informs the store to unload its contents into the acid pipe and sends the liquid to the reactor. Using similar code with different variances, the water coolant tank is emptied if there is no presence of water in the reactor or the pipes leading to the reactor core. Again, if the conditions are met, the water is released into the reactor core.

Steam Pipe Overload:

If an overload of steam is detected, the steam is diverted to the steam outlet pipe and sent back to the condenser. This is achieved by implementing a method with the code:



```
is
    i:integer;
do
    if SteamPipe1.numMU = capacity: 10 and
        SteamPipe2.numMU = capacity: 10 then
         SteamPipe1.cont.move(SteamOutletPipe) and
         SteamPipe2.cont.move(SteamOutletPipe);
    end;
end;
```

Figure 101 Simulation Generator Code

The code informs the system to offload the steam to the steam outlet pipe if the capacity (10 units of steam) is reached.

Tecnomatix Simulator Data

A larger sample of data from the Tecnomatix Simulation is presented below.

Table 14 Large Data Sample

Point in Time	W1WT	W2WTP	W3WS1	W4WP1	W5WS2	W6WP2	W8OP	W10WP4	WDP1	TP
01:00:00	0	0	1	11	1	10	4	4	0	14
01:00:00.25	0	0	1	11	0	11	4	3	0	14
01:00:00.50	0	0	1	11	0	10	4	4	0	15
01:00:00.75	0	0	1	11	0	10	3	4	0	14
01:00:01.00	0	0	1	11	0	10	3	4	0	14
01:00:01.25	0	0	1	11	0	10	3	4	0	15
01:00:01.50	0	0	1	11	0	10	4	4	0	14
01:00:01.75	0	0	1	11	0	10	4	3	0	14
01:00:02.00	0	0	1	10	0	10	4	4	0	15
01:00:02.25	0	0	1	10	0	10	4	4	0	15
01:00:02.50	0	0	1	11	0	10	4	4	0	14
01:00:02.75	0	0	1	11	0	10	3	4	0	15
01:00:03.00	0	0	1	11	0	10	4	4	0	15
01:00:03.25	0	0	1	11	0	10	4	4	0	14
01:00:03.50	0	0	1	11	0	10	4	3	0	15
01:00:03.75	0	0	1	10	0	10	4	4	0	15
01:00:04.00	0	0	1	10	0	10	3	4	0	14
01:00:04.25	0	0	1	10	0	10	3	4	0	14
01:00:04.50	0	0	1	10	0	10	3	4	0	15
01:00:04.75	0	0	1	11	0	10	3	4	0	14
01:00:05.00	0	0	1	11	1	10	4	3	0	14
01:00:05.25	0	0	1	11	0	10	4	4	0	15
01:00:05.50	0	0	1	11	0	10	3	4	0	14
01:00:05.75	0	0	1	11	0	10	3	3	0	14
01:00:06.00	0	0	1	10	0	10	3	4	0	15
01:00:06.25	0	0	1	10	0	10	3	4	0	15
01:00:06.50	0	0	1	11	0	10	3	4	0	14
01:00:06.75	0	0	1	11	0	9	3	4	0	15
01:00:07.00	0	0	1	11	0	9	3	4	0	15
01:00:07.25	0	0	1	11	0	9	3	4	0	14
01:00:07.50	0	0	1	11	0	10	3	4	0	15
01:00:07.75	0	0	1	11	0	10	3	4	0	15
01:00:08.00	0	0	1	11	0	10	3	4	0	14
01:00:08.25	0	0	1	11	0	10	3	3	0	14
01:00:08.50	0	0	1	10	0	10	3	4	0	15
01:00:08.75	0	0	1	11	0	10	2	4	0	14
01:00:09.00	0	0	1	11	0	10	2	3	0	14
01:00:09.25	0	0	1	11	0	9	3	4	0	15
01:00:09.50	0	0	1	11	0	9	3	4	0	14
01:00:09.75	0	0	1	11	0	9	3	3	0	14
01:00:10.00	0	0	1	10	1	9	3	4	0	15

TECNOMATIX SIMULATOR OVERVIEW AND MECHANISM SCREEN SHOTS

The following figures display a visualisation of various mechanisms from the simulation in operation with the addition of TimeSequence units to capture the data.

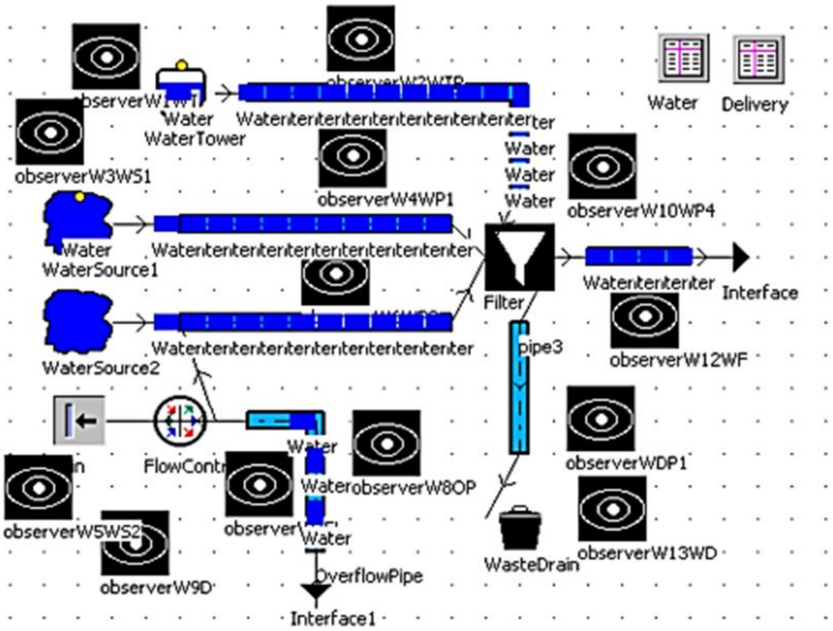


Figure 102 Appendix: Simulation Water Source Screen Shot

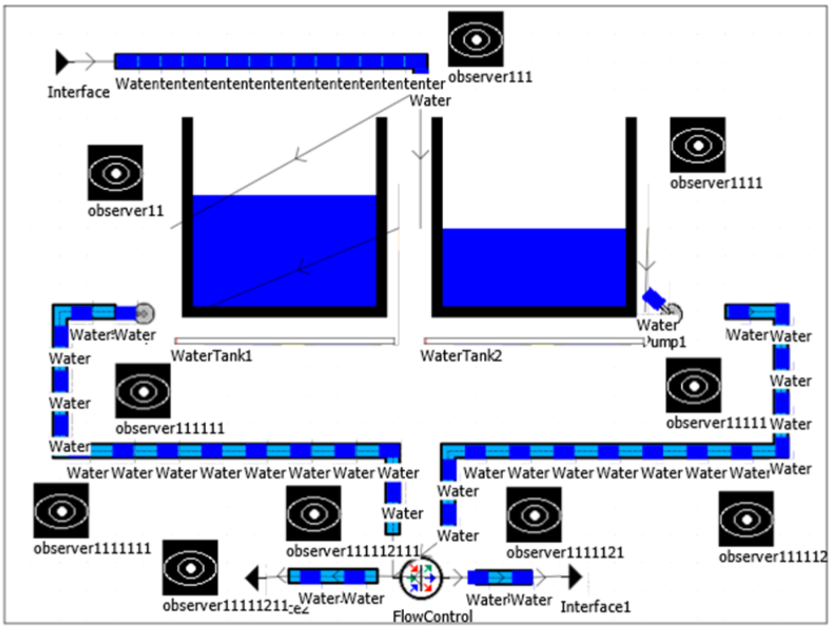


Figure 103 Appendix: Simulation Water Tanks Screen Shot

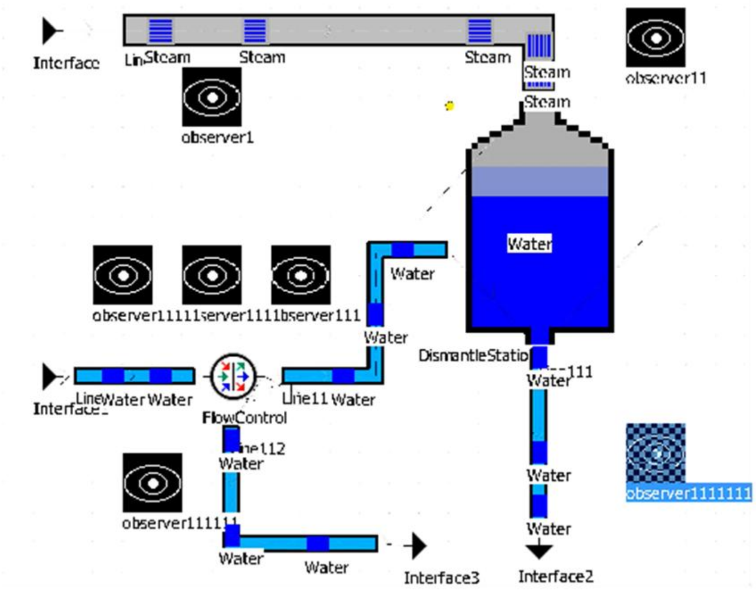


Figure 104 Appendix: Simulation Condenser Screen Shot

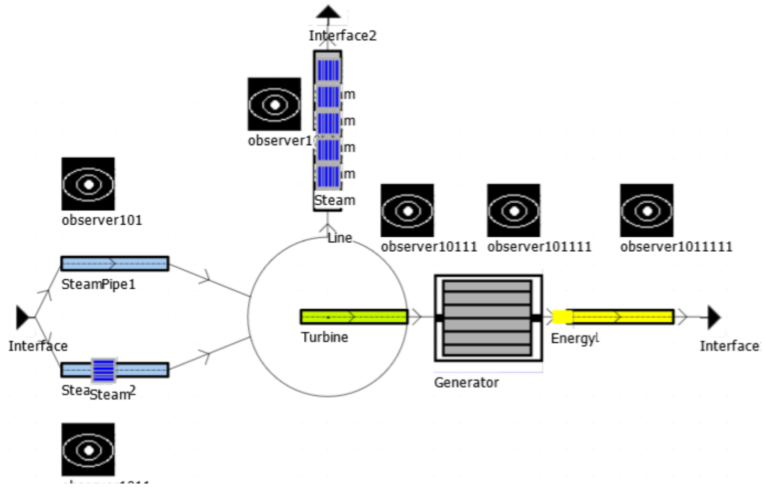


Figure 105 Appendix: Simulation Generator Screen Shot

APPENDIX B – FEATURE COMPONENTS

COMPONENTS & FEATURES

The following, Table 15, details an explanation of the abbreviations used to refer to the specific components.

Table 15 Feature Abbreviations

1. Water 1 Water Tower: W1WT	23. Outlet To Water Tower: OTWT
2. Water 2 Water Tower Pipe: W2WTP	24. Pipe From Tank: PFT
3. Water 3 Water Source 1: W3WS1	25. Nuclear Reactor: NR
4. Water 4 Water Pipe 1: W4WP1	26. Steam Outlet: SO
5. Water 5 Water Source 2: W5WS2	27. Reactor Core: RC
6. Water 6 Water Pipe 2: W6WP2	28. Coolant: C
7. Water 8 Overflow Pipe: W8OP	29. Coolant Pipe: CP
8. Water 10 Water Pipe 4: W10WP4	30. Generator Steam Outlet Pipe: GSOP
9. Water Drain Pipe 1: WDP1	31. Steam Pipe 1: SP1
10. Tank Pipe: TP	32. Steam Pipe 2: SP2
11. Water Tank 1: WT1	33. Turbine: T
12. Water Tank 2: WT2	34. Generator: G
13. Pump1	35. Electricity Line 1: EL1
14. Pump2	36. Overview Pipe To Tanks: OPTT
15. Tank 1 Pipe: T1P	37. Overview Pipe To Water Source: OPTWS
16. Tank 2 Pipe: T2P	38. Overview Pipe to Condenser: OPTC
17. Water To Condenser Pipe: WTCP	39. Overview Water Regained Pipe: OWRP
18. Tank Pipe to Coolant: TPTC	40. Overview Pipe From Reactor: OPFR
19. Main Steam To Condenser: MSTC	41. Overview Pipe To Reactor: OPTR
20. Condenser Tank: CT	42. Overview Steam Outlet: OSO
21. Pipe To Reactor: PTR	43. Overview Main Steam Pipe: OMSP
22. Pipe to Condenser Tank: PTCT	44. Overview Electricity Cable: OEC

Each component had a mean, median, mode max and min value taken from it. For example 12 mode would refer to WT2 and its mode value. 44 max would refer to OEC and its max value. As displayed in Table 16.

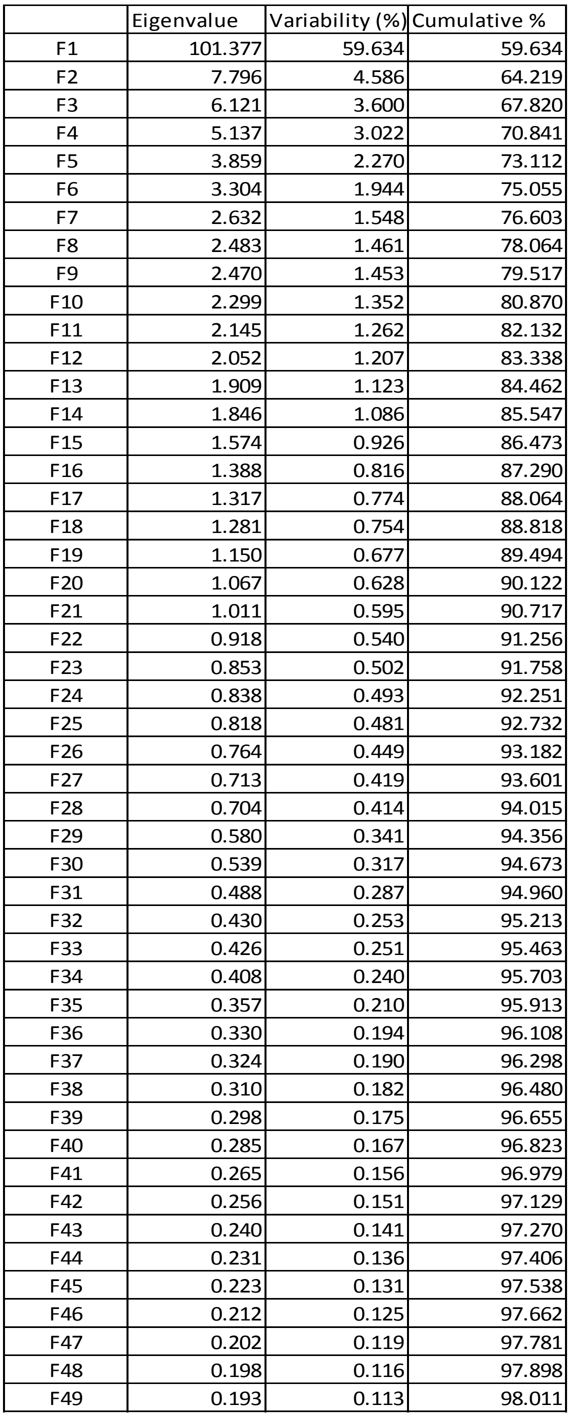
Table 16 Feature Numbers

W1WT	W5WS2	WDP1	Pump1	WTCP	PTR	NR	CP	T	OPTWS	OPTR
1med	5med	9med	13med	17med	21med	25med	29med	33med	37med	41med
1mode	5mode	9mode	13mode	17mode	21mode	25mode	29mode	33mode	37mode	41mode
1max	5max	9max	13max	17max	21max	25max	29max	33ax	37max	41max
1min	5min	9min	13min	17min	21min	25min	29min	33min	37min	41min
W2WTP	W6WP2	TP	Pump2	TPTC	PTCT	SO	GSOP	G	OPTC	OSO
2med	6med	10med	14med	18med	22med	26med	30med	34med	38med	42med
2mode	6mode	10mode	14mode	18mode	22mode	26mode	30mode	34mode	38mode	42mode
2max	6max	10max	14max	18max	22max	26max	30max	34max	38max	42max
2min	6min	10min	14min	18min	22min	26min	30min	34min	38min	42min
W3WS1	W8OP	WT1	T1P	MSTC	OTWT	RC	SP1	EL1	OWRP	OMSP
3med	7med	11med	15med	19med	23med	27med	31med	35med	39med	43med
3mode	7mode	11mode	15mode	19mode	23mode	27mode	31mode	35mode	39mode	43mode
3max	7max	11max	15max	19max	23max	27max	31max	35max	39max	43max
3min	7min	11min	15min	19min	23min	27min	31min	35min	39min	43min
W4WP1	W10WP4	WT2	T2P	CT	PFT	C	SP2	OPTT	OPFR	OEC
4med	8med	12med	16med	20med	24med	28med	32med	36med	40med	44med
4mode	8mode	12mode	16mode	20mode	24mode	28mode	32mode	36mode	40mode	44mode
4max	8max	12max	16max	20max	24max	28max	32max	36max	37max	44max
4min	8min	12min	16min	20min	24min	28min	32min	36min	40min	44min

EGENVALUES

The following, Table 17, contains a continuation of the list of the eigenvalues created up to the first 48 features.

Table 17 Eigenvalues



	Eigenvalue	Variability (%)	Cumulative %
F1	101.377	59.634	59.634
F2	7.796	4.586	64.219
F3	6.121	3.600	67.820
F4	5.137	3.022	70.841
F5	3.859	2.270	73.112
F6	3.304	1.944	75.055
F7	2.632	1.548	76.603
F8	2.483	1.461	78.064
F9	2.470	1.453	79.517
F10	2.299	1.352	80.870
F11	2.145	1.262	82.132
F12	2.052	1.207	83.338
F13	1.909	1.123	84.462
F14	1.846	1.086	85.547
F15	1.574	0.926	86.473
F16	1.388	0.816	87.290
F17	1.317	0.774	88.064
F18	1.281	0.754	88.818
F19	1.150	0.677	89.494
F20	1.067	0.628	90.122
F21	1.011	0.595	90.717
F22	0.918	0.540	91.256
F23	0.853	0.502	91.758
F24	0.838	0.493	92.251
F25	0.818	0.481	92.732
F26	0.764	0.449	93.182
F27	0.713	0.419	93.601
F28	0.704	0.414	94.015
F29	0.580	0.341	94.356
F30	0.539	0.317	94.673
F31	0.488	0.287	94.960
F32	0.430	0.253	95.213
F33	0.426	0.251	95.463
F34	0.408	0.240	95.703
F35	0.357	0.210	95.913
F36	0.330	0.194	96.108
F37	0.324	0.190	96.298
F38	0.310	0.182	96.480
F39	0.298	0.175	96.655
F40	0.285	0.167	96.823
F41	0.265	0.156	96.979
F42	0.256	0.151	97.129
F43	0.240	0.141	97.270
F44	0.231	0.136	97.406
F45	0.223	0.131	97.538
F46	0.212	0.125	97.662
F47	0.202	0.119	97.781
F48	0.198	0.116	97.898
F49	0.193	0.113	98.011