THE IMPLEMENTATION OF INTEGRATED SECURITY SYSTEMS: CASE STUDY OF THE INDUSTRIAL SECTOR OF HARARE-ZIMBABWE

BY

DIMAX MUSONZA

submitted in accordance with the requirements for the degree of

MAGISTER TECHNOLOGIAE

in the subject

Security Management

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: DR OJ KOLE

FEBRUARY 2016

COPYRIGHT

DECLARATION FORM

Student number **33419515**

I, **DIMAX MUSONZA**, declare that this dissertation entitled: **THE IMPLEMENTATION OF INTEGRATED SECURITY SYSTEMS: CASE STUDY OF THE INDUSTRIAL SECTOR OF HARARE-ZIMBABWE** is my own work and that all the sources that I have quoted have been indicated and acknowledged by means of complete references.

_____ _____

SIGNATURE DATE

D. MUSONZA

ACKNOWLEDGEMENTS

Firstly and foremost I would like to thank God the Almighty for providing me with life as the primary requirement to complete this study. My gratitude goes to Him for giving me the wisdom, energy, patience, determination and resolve needed throughout the duration of the research process.

I rightly thank my family members for their encouragement, material, motivation and morale support which they provided under very difficult circumstances characterised by constrained resources. It is because of their invaluable support that I successfully managed to complete the programme.

Special thanks go to my courageous and supportive supervisor, Dr John Kole who guided me throughout the research process. I also want to thank Professor Minnaar for assisting with the preparation of the permission letters. I appreciate the assistance provided by Ms. Suwisa Muchengetwa with the statistical analysis of data. Mr Jack Chokwe is thanked for technical language edition of the report. Thanks to other UNISA staff for your continual assistance, technical advice, co-operation and encouragement. Without them this study would not have been effectively completed.

Thanks to friends and colleagues who provided me with the motivation, assistance and support. I really appreciate the morale and material contributions provided in hard times.

My gratitude goes to the organisations, staff and individuals who participated in the study. I thank them for allowing me into their facilities, participating in the interviews and assisting with the completion of my questionnaires. Their contribution made it possible and assisted in the completion of the study.

Lastly, I am grateful to all those who contributed in one way or the other for their assistance and support throughout the research process.

SUMMARY

Industrial sites in Harare contribute significantly to the economy of Zimbabwe. Harare is the capital city of Zimbabwe and therefore has significant manufacturing and commercial activity. The protection of industrial sites is very important because of the presence of valuable assets and operations. Therefore the main purpose of deploying security measures at industry premises is to create a safe and secure environment for the business functions. Security management is consequently an important element of an industrial organisation's continuity.

The implementation of integrated security systems was examined to some extent within this study. The size and nature of industrial facilities influenced this study to view integrated security systems as more effective than stand-alone security measures. The study sought to investigate the various aspects associated with the implementation. The purposes of the research included the following:

- Examine current practices, benefits, shortcomings in the implementation of integrated security systems;
- Critically evaluate the security management aspects required for the implementation of integrated security systems;
- Investigate successes and failures associated with integrated security systems and how implementation can be improved;
- Examine and identify factors necessary for a best practice approach to integrated security systems; and
- Determine a methodology for the effective implementation of integrated security systems.

Additionally the study briefly examined how security systems integration can assist in reducing the problem of connivance to theft at receiving and dispatch points at industrial facilities.

The report is divided into five chapters. Chapter 1 covers the research problem, Chapter 2 deals with the research methods while Chapter 3 has insightful information from literature review. Chapter 4 presents the data and how it was analysed. Lastly Chapter 5 has findings, recommendations and conclusions.

The study used the mixed-method approach. This approach includes both qualitative and quantitative research in order to gain a more in-depth understanding of the research problem. The

methods of data collection were site visits, interviews and questionnaires. The sample was drawn from a cross-section of sites within the industrial areas of Workington, Southerton, Willowvale, Graniteside, Msasa and few outside industries in the vicinity of Harare. A total of 11 sites were observed. The interviews consisted of 30 participants who were mainly security practitioners at management level as well as some non-security managers. In addition, a total of 102 respondents participated in this study by completing the questionnaire. The majority of the respondents were security practitioners who were the main focus of the study.

The findings support the various aspects of the implementation of integrated security systems. The conclusions emanating from the statistical analysis of the collected data included the following:

- The critical assets for protection at industrial facilities are infrastructure, products, revenue, people and other movable items or equipment;
- The main threat sources are from outsiders, crime syndicates and employees;
- Security systems suitable for integration are CCTV, electronic access control, alarms, personnel, policies and procedures backed by information communication technologies.
- Security should be functionally integrated with other departments which include Information Technology, Human Resources, Finance, Operations and Marketing;
- The preferred mode of linkage was established to be fibre optic on a local area or wide area network using intranet or internet;
- The key players in the integration were found to be security practitioners, top management, IT specialist, system suppliers, installers and operators;
- The implementation process consists of security policy, survey, system design, procurement, installation, training, operating, review and upgrade;
- Factors necessary for best practice include system purpose, availability of resources, top management commitment, skills, and feasibility to implement;
- The benefits are mainly improved effectiveness, easy of monitoring, improved outlook and record keeping;
- The most significant challenges are system breakdown, sabotage and power outage; and
- Connivance to theft can be mitigated by a combination of staff rotation, dedicated CCTV, spot checks, undercover surveillance and functional integration.

The dissertation covers extensively the implementation of integrated security systems in the industrial sector of Harare in Zimbabwe. However, there is much scope for further studies on this subject in particular on the costs and effectiveness of integrated security systems.

ACRONYMS

ASIS…….American Society for Industrial Security

CCTV……Closed Circuit Television

CPTED……Crime Prevention Through Environmental Design

EAC……..Electronic Access Control

ICT……Information Communication Technology

ISS……Integrated Security Systems

LAN…….Local Area Network

SCPM…….Situational Crime Prevention Methods

SSI……Security Systems Integration

UNISA……..University of South Africa

TABLE OF CONTENTS

Chapter 1: INTRODUCTION AND MOTIVATION FOR THE RESEARCH

Chapter 2: RESEARCH METHODOLOGY

Chapter 3: LITERATURE REVIEW

Chapter 4: FINDINGS: AN ANALYSIS INTERPRETATION AND PRESENTATION OF THE RESEARCH DATA

Chapter 5: CONCLUSIONS AND RECOMMENDATIONS

FIGURES

LIST OF TABLES

CHAPTER 1
INTRODUCTION AND MOTIVATION FOR THE RESEARCH

1.1 INTRODUCTION

Security management is a function found in almost all industrial facilities. Porter's value chain provides an exposition of the activities within an organisation (Louw & Venter 2009: 157). These activities are divided into operational and administrative functions (primary and support activities). Functional analysis of an organisation's value chain from a security management perspective can be used to identify risks and vulnerabilities within a specific function. An introspection of the functions highlights the need for the protection of the organisation throughout its entire functions such as operations, human resources, procurement, finance, and administration. Security can be placed as a support function in the value chain (*ibid*). The way the security framework is established varies in organisations. In some organisations it is a stand-alone function, department or section while in some it might be a sub-function within a main function such as human resources or risk. Several factors give rise to this and these include the organisation's business model; as well as management's desire to avoid or minimize risk within the organisation's environment.

The Harare industrial sector in Zimbabwe which was the area of focus of this study was subdivided into five areas, namely; Workington, Southerton, Willowvale, Graniteside and Msasa. The number of companies in this industrial area could be approximately 500. A snap survey carried out during sampling showed that there are similarities in security measures at most of the companies. These measures include perimeter security (fences and walls), access control, security guards, dogs, locks, lighting, CCTV and alarms among others. Van Jaarsveld (2011: 5-8) expounds on these security measures and emphasizes the need for such a multiplicity of security measures to be integrated. However, Van Jaarsveld does not provide the methods of integrating security systems. This study sought to explore how security systems can be integrated. According to Harare Police Crime Chart observed by the researcher, the average monthly crime rate stood at 6 681 reported cases during the year 2013 (Anon. 2013). The crimes of concern in the Harare industrial area were outlined as thefts,

burglary, robbery and fraud. Fraud is both a loss prevention and security issue but with a strong bias towards loss control because it can be mainly minimized by internal controls rather than physical security systems. Fikes (2009: 4) deals with fraud as white collar or organisational crime. While Fikes's *(ibid)* argument is confined to thefts and fraud by employees, the bottom line is that they can be committed by a syndicate involving both employees and outsiders.

The selection and implementation of security measures at an industrial facility is influenced by several factors. These include the nature of operations at the facility, the surroundings of the facility, general crime patterns and trends within the area as well as management's desire to avoid or minimise risk. Most security measures as observed by the researcher appeared to be stand-alone without any form of integration with other security measures. Olckers (2007: 74-78) explains the integration of gates and alarms with power supply systems. The integration proposed in this study goes further to link the gate access control, the intrusion alarm systems, CCTV and policies and procedures. For an industrial facility to be well protected there should be a comprehensive, well-co-ordinated security system with sub-systems across the entire organisation. These sub-systems should be linked by communication methods based on information technology solutions and/or policies and procedures, and organisational verbal and non-verbal communication. Document authorisation plays an important role in the movement of assets, products, materials, people and vehicular traffic into and out of the facility. Torres (2007: 4) advocates for a combination of loss prevention systems and security systems as the best practical approach to security systems integration. This study supports Torres's view which presupposes a holistic approach.

1.1.1 Organisation of security in Zimbabwe

The security industry in Zimbabwe was at the time of the research characterised by the following:

- The Ministry of Home Affairs which regulates and supervises security

companies under the Private Investigators and Security Guards Control Act, Chapter 27:10;

- The Zimbabwe Republic Police which is a national police service;
- Private security companies which can be categorised as small, medium and large. The rate of entry and exit is high mostly among small companies due to intense competition. This was obtained when the researcher held a discussion with the Controller of Security Companies at the Ministry of Home Affairs;
- Security Associations mainly the Security Association of Zimbabwe (SAZ) and Zimbabwe National Security Association (ZINSA). These associations are not regulated and security companies can choose to affiliate with any association;
- Security training institutions offering short courses, certificate and diploma courses. Most of the guard training is done by security companies. Other training institutions comprise of independent colleges;
- Security system providers offering a range of mostly electronic gadgets such as, CCTV, alarms, intercoms and EAC;
- Proprietary (in-house) security staff such as managers, officers and guards; and
- Security consultants/advisors but these were very few though some security companies could have consulting activities mostly for surveys, audits, inspections and investigations.

The composition of the above players was indicative of the importance of the security function at industrial facilities. The proliferation of crimes of concern in the Harare industrial area in the presence of existing security measures gave rise to choosing the topic of security systems integration as a possible solution to solving some of the security problems confronting organisations. The concept of integration is a contemporary global phenomenon which has also gained momentum in security management. However, in small industrial facilities, integrated security systems may not be a demanding requirement. The researcher did not come across any previous research in security systems integration in Zimbabwe. However, research literature was available from international sources but mostly in information security. This study focused on the integration of physical security systems through interface with information technology transmission systems, policies and procedures.

Typically, an integrated security system consists of a set of subsystems interconnected through IT routers and policies and procedures. The focus of the study was on the integration of access control, security personnel, intercoms, CCTV, alarms, security lighting, organisational functions, policies and procedures (Vellani 2007: 208). Non-security functions including safety of buildings such as fire and general lighting were not included in the study because the focus was to address crime-related problems through security measures in comparison to holistic integration advocated by Colombo (1999: 122). The identified challenge was on identifying which security systems to integrate in the context of the assets to be protected, the threats, existing security measures, vulnerabilities and cost of the integration (Colombo 1999:124). According to the SDM Security Magazine (1999), 48% of all access control systems are stand alone, less than one third are integrated while government has more than 50% integrated facilities. Information on levels of integration was not available in Zimbabwe and given the wide gap between the USA and Zimbabwe, levels of integration in Zimbabwe could be at the tail end. This research sought to establish levels of security systems integration in Zimbabwe.

1.2 BACKGROUND OF THE STUDY

As organisational threats increase, it will become more critical for organisations to explore possible measures of mitigating these threats. According to the Zimbabwe Republic Police (ZRP) National Service Plan (2007: 70-71), crimes of concern relative to the industrial sector are indicated as burglary (house breaking with intent to commit other crimes), theft, robbery and fraud. The same report distinguishes between crime trends and crime patterns. Crime trends refer to the occurrence of crime over a period of time which is useful in time series analysis. Crime pattern refers to the manner in which crime is committed in a specific area usually termed "*modus operandi"* and is important in identifying causes of crime (ZRP 2007: 71). The crimes of concern were on the increase in the Harare industrial area despite a proliferation of security service providers. According to a Staff Reporter of the Sunday Mail (2014), the police stated that crime in Harare increased by 7% from 92 314 cases in 2012 to 98 915 cases in 2013. Nleya (2013) of the Newsday gave a figure of 7 763 burglaries which were recorded in Harare during the year 2012 which was derived from police sources. These

burglaries included those that occurred in the Harare industrial area. The value of goods, products, materials, components and items stolen could run into hundreds of thousands if not millions of US dollars annually. According to the Confederation of Zimbabwe Industries (2012: 3), operating capacity in industrial companies was at 44.2% and that some companies had closed down due to viability problems. This had resulted in a surge in unemployment which was estimated at 70 – 80%. Unemployment in general contributes significantly to incidence of crime.

According to Anon. (2013), causes of crime in Harare included unemployment, poverty, and introduction of the US Dollar as local currency. The same report also indicates that robberies increased by 40% in 2012. Criminals bypass security measures such as perimeter walls, guards and alarm systems either through forced entry or connivance. Many people resort to property crimes due to unemployment and poverty. Those left in employment are mostly disgruntled because of poor remuneration systems and working conditions as a result of scaled down company operations. Such employees are prone to resort to theft and fraud due to a desire to steal which can be aided by the existence of weak security and loss control systems as per Cressey's Fraud Triangle (Fikes 2009: 19). The Triangle of Crime Causation (Rogers 2011: 25) has striking similarities with Cressey's fraud triangle. Instead of the somewhat confusing factor of rationalisation the crime, causation triangle opts for predisposing factors. However both models are applicable to the evaluation and implementation of integrated security systems. A combination of physical security systems and internal controls can help mitigate thefts of goods, assets, and materials from industrial facilities.

Much of Harare industrial area is situated close to high density areas from which labour force is derived. According to the researcher's experience as a police officer in Harare and informal discussions with Harare police, high density areas are considered as having high prevalence of crime. This may have a contagious effect to the neighbouring industrial areas; hence the need for effective security measures. Crime also increased in general due to technological advancement in transportation and information technology, particularly mobile phones and the internet. Police operations could be limited due to resource constraints

because of underperforming economic activity. Companies can be unable to deploy effective security measures because of increased costs of security especially guard services because revenue inflows are on the downside. This scenario may create a big opportunity for the prevalence of crime and propensity to steal among employees and criminal elements in society. In addition, employees could be prone to form crime syndicates with outsiders to facilitate undetected thefts, fraud and faked robberies in the face of weak security systems (Cappers 2008: 4-8). Cappers *(ibid)* established that the adoption of situational crime prevention methods would assist in crime prevention in the retail sector. There are similarities between crime prevention in the retail and industrial sectors, hence the relevance of Cappers' work. This research also sought among others to establish the *modus operandi* of crimes of concern in the industrial area. The study identified connivance between security guards, staff members and outsiders as a problem which most industrial companies had failed to solve. Cappers (2008: 60-61) discusses the disposal of stolen goods which can easily be disposed below market prices and adds that recoveries are very low especially on consumables.

Most of the industrial facilities had seemingly stand-alone security measures which were are dominated by security guards who may be vulnerable to connivance and robbery attacks. In some instances, guards may steal without any outside assistance. Some of the robberies may be stage-managed by the guards and their criminal associates. Pearson (2004: 193) emphasises the need for security measures to work in combination for better effectiveness. This combination can only be achieved through the integration of security systems. Security systems integration minimises the heavy dependence on the human factor ensuring that one measure checks or responds to the other timeously. Denial of service countermeasures can effectively be employed in an integrated security system. Some organisations may have not embraced the concept of ensuring that security exists throughout all the facets of the organisation. This can result in cases of fraud, embezzlement of funds and corruption being rampant much to the detriment of organisations without integrated security systems. Most organisations faced with changes in the environment do not initiate changes to their operating systems in order to counter the threats emanating from the environment (Torres, 2007: 2). Criminals exploit this lack of adaptation and organisational inertia. It was the study's assumption that most companies still used stand-alone security measures dominated by

fences, walls, gates, locks and guards. This lack of adaptation was also recently observed by Young and Leveson (2014: 31). While systems theory is an old revelation in management science, its implementation in the field of security management is still in progress. Most of the security systems in the Harare industrial area were assumed to be not capable of effectively performing the functions of prevention, discovery and rapid response because they were found to be not adequately integrated. Stand-alone security measures are costly because of their inability to effectively perform the above functions (Vellani 2007: 206).

While some organisations have a desire or are migrating to integrated security systems, there are potential problems of implementation. Some companies, and in particular security practitioners, may not be aware of the requirements for integrated security systems (Colombo 1999: 121). Most problems have to do with skills shortages in planning, design, installation, operationalization, training and upgrade. One observation was that the Rogers Security Risk Management Model and its adapted models have no skills component (Rogers, 2011: 17-19) but this is generally a key element in security management. This aspect could have been safely placed after the identification of control measures prior to implementation. Even TAG's Risk Assessment Process depicted in Figure 10.1 (Vellani 2007: 183) which has some similarities with the Rogers model also misses this important aspect. Further exploration and comparisons are covered in the chapter on literature review. The fear of cost may be a fear of the unknown. Some companies may not carry out a comprehensive return-on-security investment to justify the need for security systems integration (Williams, 2008: 6-9). This research sought also to establish if there were sufficient skills among Security and ICT practitioners to effectively integrate security systems.

1.3 STATEMENT OF THE PROBLEM

The identification and implementation of effective security measures is a challenge in the context of the evolving criminological and business environment. Most companies in the Harare industrial sector are confronted with security-related problems. The problem of security-related losses continues to trouble management with no immediate solutions. While literature on security systems integration is relatively abundant, the study established that

very little research has been conducted on it. Even though the costs of implementing integrated security systems may not be all that prohibitive, very little observable progress has been made in employing these systems. The study sought to investigate the reasons behind the failure by many companies to integrate security systems. One assumption held by the researcher was that there could be inadequate understanding of the platforms for integrated security systems in Zimbabwe in particular and in developing countries in general. While incidents of thefts, burglary and robbery on facilities are a known occurrence in the area of study, the existing security measures may not be well applied to repel or detect such attacks. Instances where security guards have been injured or killed in attacks at premises have been reported in press reports. Furthermore, crime syndicates along industry supply chains and within the company value chain make it difficult to prevent or detect security crime incidents. The study also sought to investigate how security systems integration could help in breaking crime syndicates. These syndicates involve many players some of whom might not be knowledgeable of other players in the chain. Williams (2008: 30-45) provides an exposition of supply chain security but his work failed to establish the impact of crime syndicates on supply chain security. The effectiveness of security measures needs thorough exploration before implementation. Consideration should be given to the overall security environment of the facility to be protected (Kole, 2010: 2). The other factor is that once implemented, it is difficult if not impossible to recover losses from an ineffective security system. In this case, the loss is dual in nature since it includes the crime loss, the cost of the ineffective security system and the additional cost of replacing the ineffective system.

Caution should be thrown to the wind because it should not be holistically assumed that the implementation of integrated security systems will lead to a complete elimination of all security problems. In the absence of an expert vulnerability assessment, the facility may continue to be exposed to unknown security threats. A regular review of the security system is necessary and in this regard the study sought to establish if existing security systems were being reviewed and upgraded (Rogers, 2011: 17). The researcher was of the view that the levels of integrated security systems in the Harare industrial area were very low and needed significant improvement and assistance through this research.

1.4 PURPOSE OF THE STUDY

The purpose of the research was to:

- identify the assets most vulnerable to security (crime) risks in the Harare industrial area;
- identify the security (crime) risks confronting the assets at the facilities;
- identify existing security measures and systems currently in place at the different locations in the area of study;
- investigate the extent to which security systems are integrated;
- examine the extent of the impact and effectiveness of integrated security systems in the industrial area;
- evaluate and examine the factors affecting the effective implementation of integrated security systems; and
- formulate recommendations for the effective implementation of integrated security systems.

1.5 RATIONALE OF THE STUDY

Crime patterns and trends evolve over time. Changes in criminological behaviour require evaluation and adaptation of appropriate security measures. Rogers (2011: 24-34) discusses factors causing crime which include opportunity, ability and desire to commit crime. Torres (2007: 12) asserts that security systems should provide added value to the organisation through a positive return on security investment. The role of security systems is to provide effective protection to the company's assets and operations to ensure business continuity. The study includes a number of issues in security management inclusive of: asset identification, threat appraisal, vulnerability assessment, security measures, benefits and an implementation process. In order to gain a deeper understanding of the concept, engagement of practitioners involved and review of relevant literature was necessary. Having insightful knowledge will help dispel fears on cost implications and complexities of integrated security systems. The research also assists in understanding problems and limitations associated with integrated security systems.

1.6 SIGNIFICANCE OF THE STUDY

Due to the persistence of security threats in the environment, the design and implementation of effective security systems should be a primary management function in organisations. This study provides valuable contributions to organisations implementing or contemplating to implement integrated security systems. The significance and importance of this study was based on establishing how value can be added by integrated security systems through efficiency and effectiveness. Industries and related organisations will have an additional platform on which to launch and evaluate security systems integration. The ability to reduce incidents of security risks through integrated security systems would benefit business organisations by reducing operating costs through reduced losses thus providing additional shareholder value. The research provides security practitioners with empirical data to support expenditures on security systems. The study provides impetus to the security management function in organisations particularly where security issues are of strategic concern. The changing security environment requires that security practitioners obtain additional knowledge from research work. There are different perspectives on levels of integration. Therefore the study sought to establish the best possible context of integration. Low probability, high-impact events require layers of security measures acting in a co-ordinated manner to continuously monitor, prevent and detect such eventualities at the earliest possible opportunity (Dave, 2007: 41).

1.7 AIM OF THE RESEARCH

The aim of this research was to examine the nature and extent of integrated security systems in the Harare industrial area. The research intended to examine and evaluate the security measures and systems that were currently in place. The security systems were examined in the context of prevailing crime risks. The researcher aimed to explore the ability of security systems to protect and prevent the facilities included in the study. The focus was to establish if the security systems have an impact on the incidence of industrial related crimes. The researcher sought to establish which security systems could be integrated in order to

effectively protect industrial facilities. The researcher aimed at identifying challenges and critical success factors in the implementation of integrated security systems. The research aimed at advancing an understanding of the impact or lack thereof of integrated security systems. Hopefully the study contributes towards the solving of the security problems in the industrial area.

1.8 RESEARCH OBJECTIVES

The objectives of the study were among others to:

- Determine the security risk assessment aspects for the Harare industrial sector in relation to the implementation of integrated security systems;
- Assess critically the extent of implementation of integrated security systems in the Harare industrial sector;
- Explore the main reasons for implementing integrated security systems in the Harare industrial sector;
- Recommend security measures for inclusion in an integrated security system in the Harare industrial sector;
- Advance the Information Communication Technology aspects suitable in the implementation of integrated security systems;
- Propose the key players to be included in the implementation of integrated security systems;
- Formulate a best practice process to be followed in the implementation of integrated security systems;
- Evaluate the factors necessary for the successful implementation of integrated security systems;
- Understand the effectiveness of integrated security systems in terms of the benefits of implementation;
- Examine the challenges associated with the implementation of integrated security systems; and
- Identify potential solutions for inclusion in the implementation of integrated security systems to solve the problem of connivance to theft in the Harare industrial sector.

1.9 RESEARCH QUESTIONS

The following are the research questions asked:

- What are the major security risks confronting organisations in the Harare industrial area?
- What is the extent of implementation of integrated security systems in the industrial sector of Harare?
- Why is it necessary to implement integrated security systems?
- Which security measures and systems need to be integrated?
- Are there any technological impediments to implementation of integrated security systems?
- Who are the key players in the implementation of integrated security systems?
- How is the implementation of integrated security systems carried out?
- What is required to implement integrated security systems?
- How effective are integrated security systems in the prevention and detection of security incidents?
- What are the problems associated with the implementation of integrated systems?
- How do security practitioners perceive the current state of security systems integration in relation to the problem of connivance to theft within the Harare industrial sector?

1.10 KEY THEORETICAL CONCEPTS

1.10.1 Closed Circuit Television (CCTV)

Olckers (2007: 64-65) describes a CCTV as a combination of a stand-alone camera transmitting captured images to a television monitor. The images are transmitted via cable to the television which is monitored by a staff member. Security can then react to suspicious activities observed on the CCTV system leading to prevention, detection and recovery.

1.10.2 Electronic Access Control (EAC) System

According to Vellani (2007: 96) it is an electrically powered security measure to control access to a facility. It is based on predetermined authority to allow or deny access to persons and vehicles. It can be composed of gates, doors, turnstiles, keypads, card readers or switches, security personnel and policies and procedures. An access control can be stand-alone or integrated with CCTV and intrusion alarm.

1.10.3 Integrated Security Systems (ISS)

It is a combination of security subsystems acting in unison and connected or not connected by an information technology protocol. For purposes of this study the system combines security personnel, CCTV, EAC, intrusion alarm, policies and procedures and other functions of the organisation. The system may include stand-alone security measures which may not be connected to the integrated security system but which are a totality of the facility security measures. Any more than two security measures acting in combination are considered as an ISS (Sewpersad 2010: 11).

Contos, Crowell, Colby and Dunkel (2007: 65) advance an ISS as referring to the integration of the security function with any other function such as human resources, finance or procurement more commonly through a common information internet protocol or through policies and procedures.

1.10.4 Security systems integration

This refers to the planning, design, installation and operationalization of an ISS. It is a process or project of linking together a number of security measures and systems into a co-ordinated unit. Integration can be by either IT protocols or policies and procedures. Typically this can be referred to as technological or procedural integration (Colombo 1999: 24).

1.11 ORGANISATION OF THE STUDY

This study is composed of five chapters titled as follows:

CHAPTER 1: **INTRODUCTION AND MOTIVATION FOR THE RESEARCH**

The chapter provides a background of the study and in particular gives an exposition of the problem. It sets the stage for subsequent chapters of the study.

CHAPTER 2: **RESEARCH DESIGN AND METHODOLOGY**

Details the research methodology and the design of the data gathering instruments.

CHAPTER 3: **LITERATURE REVIEW**

Provides detailed literature review on implementation of ISS and critical success factors.

CHAPTER 4: **FINDINGS: DATA COLLECTION AND ANALYSIS**

Outlines how the research was conducted and examines the results from the interviews, survey questionnaires and observations.

CHAPTER 5: **CONCLUSIONS AND RECOMMENDATIONS**

Documents the results of the research conducted, summarises the findings and provides recommendations.

REFERENCES

APPENDIX

1.12 CONCLUSION

This chapter provides a background for the study on ISS. As companies continue to experience security related losses the need for ISS becomes apparent. The chapter also provides a contextual framework of the study through statement of the problem, background of the study, purpose, rationale, significance, and aims of the research. In addition the chapter also describes some key theoretical concepts of ISS. Lastly the organisation of the study is outlined through a brief layout of the chapters. The next chapter discusses the research methodology used for the study. It provides an understanding of the research approach, design, sampling and data collection methods as well as the challenges faced during sampling and data collection.

CHAPTER 2

RESEARCH METHODOLOGY

2.1 INTRODUCTION

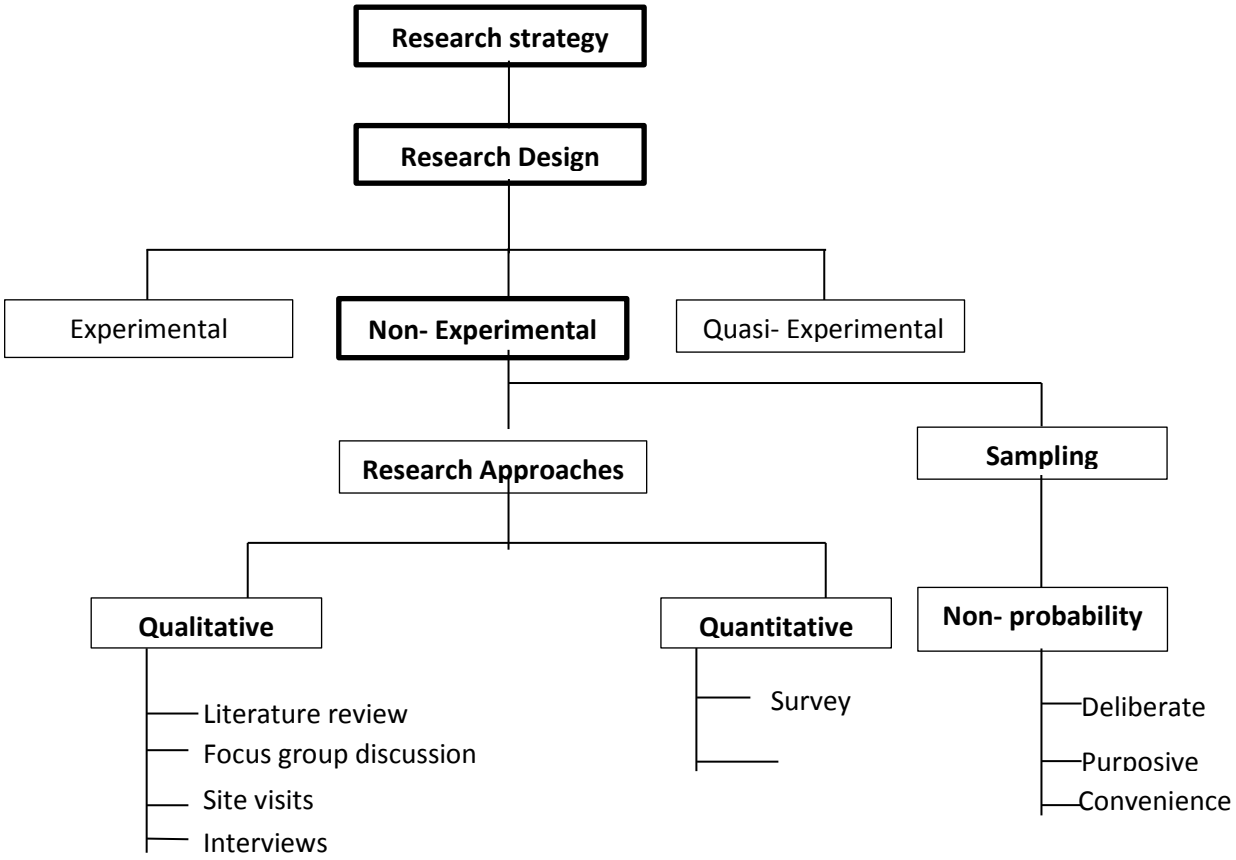
This chapter deals with the research design and methodology followed in the study. The research design, sampling procedures, data collection methods, data analysis and ethical considerations are covered in this chapter. It also explains the problems likely to be encountered in the study. The problem of implementing integrated security systems is multifaceted. Its major components are the security risks and security measures. The objective of the research was to, among others; examine the impact of integrated security systems on security risks in the Harare industrial sector. Because of the nature of the problem, the researcher used a mixed-method approach. The design consisted of qualitative and quantitative approaches. The qualitative approach was applied through observations at selected sites and interviews on managers. Interviews were also carried out on a few security system suppliers and installers. The quantitative aspect was done through a survey administered on security and non-security respondents. The questionnaire contained questions on a five-point Likert scale covering various aspects on SSI. The mixed-method approach was selected because of its integrative all-encompassing reliability in data gathering. The questionnaires were used as a means of validating the interviews and observations.

Research methods are concerned with sampling design, data gathering tools, data analysis, reliability and validity. The data collection methods for this study were literature review, site visits, interviews, and survey questionnaires. A focus group discussion was used to pre-test the research instruments. However, focus group discussions could not be used in the actual study due to cost and time constraints. Section 2.3 of this chapter explains the sampling procedures adopted. Due to operational constraints in the industrial area, the researcher was compelled to use non-random sampling techniques which include purposive, deliberate and convenience sampling. The section on validity and reliability explains how the accuracy of collected data was safeguarded. The researcher faced a number of problems and a separate section has been included to expand on these problems. The issue of ethical considerations was covered through permission from the University of South Africa (UNISA) according to the Research Policy. The next section covers the research design.

2.2 RESEARCH DESIGN

Research design refers to how data is collected, analysed and interpreted. The design provides the means by which these are carried out as explained by Biggam (2011: 127). It is the central part of the study in that it provides a practical link between conceptual understanding of the problem and outcomes of the study. Marczyk, DeMatteo and Festinger (2005: 139) developed a classification of research designs under experimental, quasi-experimental and non-experimental. This study adopted a non-experimental design which uses qualitative and quantitative approaches. Such type of a design can be referred to as a mixed method design as advocated by Cappers (2008: 71). The researcher chose to use a mixed method design to provide an adequate exploration of the research problem. The study was exploratory and descriptive because it sought to gain insightful knowledge about integrated security systems. Thematic areas were developed for the qualitative interview, survey questionnaire and observations. Most of the themes were developed using the McKinsey 7-S framework (Thompson & Martin, 2005: 139) and the Rogers Security Risk Management Model (Rogers, 2011: 17). Effective security systems can only be designed if vulnerability is adequately established. The researcher concluded that using one research approach without the inclusion of the other would not provide sufficient information for the study (Cappers 2008: 69). Therefore, a mixed method approach that aimed at addressing a variety of factors was used to obtain a complete view of the research problem. The mixed method approach was found desirable for this study in order to gain an in-depth understanding of the problem. Marczyk *et al*. (2005: 139) categorise research designs as experimental, non-experimental and quasi-experimental. The researcher provides an exposition of the research strategy followed in the study in the following diagram.

Figure 2.1: Framework of research design and approaches



In the above diagram, the experimental and quasi-experimental designs are included for purposes of completeness only and accordingly there are no sub-topics under them because the study was non - experimental. The diagram seeks to provide a schematic representation of the used non-experimental research design.

2.2.1 Qualitative design

The qualitative design is based on gaining an insider's view on how he or she understands a phenomenon (Sewpersad, 2010: 13). The insiders in respect of the study were the respondents at industrial sites where security systems are deployed. The qualitative approach is general in scope because it depends on the level of understanding of both the researcher and the respondent. Therefore, it is a subjective approach. The researcher should have sufficient knowledge of how the design is applied while the participants should have considerable knowledge and experience about the concept under investigation. Through education, experience and literature review, the researcher had sufficient background of the research problem. The researcher had a good background both in general management and security management in particular. The extent and level of the problem was pitched high enough to require intra-organisational skills to sufficiently address it. Background knowledge and experience made it possible for the researcher to collect information from a variety of sources using the qualitative approach. These sources included company owners, Chief Executive Officers, managers and officers from companies in the industrial area, security companies, system suppliers and other parties of interest to the study. Informal interviews were carried with other parties identified as directly or indirectly relevant to the study in order to broaden the scope of information.

The group of respondents for the qualitative interview selected by the researcher using deliberate and purposive sampling was assumed to possess the requisite skills, experiences and competencies necessary for the desired information. However, knowledge levels may have been different among participants depending on which aspects the respondent understood well. It was the researcher's assumption that some participants could find the interview challenging and demanding. Therefore, subjectivity could not be ruled out in the qualitative studies because the information obtained was dependent on the respondents' conceptual understanding of the aspect under consideration. Most participants performed well in aspects such as asset characterisation, risk categorisation and security measures. Some technical areas such as return-on-security investment, alignment of security policies and procedures proved difficult to some of the respondents. The researcher sought to establish the relationship between security risks and security systems through qualitative means. However, this was not a correlational study. While

the researcher used thirty structured interviews, in some instances these could overlap into in-depth interviews. Some of the interviews were in-depth due to high knowledge levels of the participants. This was the case with respondents who were receptive and showed much interest to the research problem. The qualitative design used in this study was not experimental or semi-experimental but was exploratory and descriptive in nature with the intention of gaining a deeper understanding of integrated security systems. The intention was to obtain insightful information from people involved in the daily settings of security systems from a practical point of view. Therefore, it can be safely understood that views were different depending on the site from which the information was obtained. The researcher observed that some sites had relatively integrated security systems while others had simple stand-alone security measures.

The qualitative approach for this study was non-experimental; it was a descriptive exploratory research design. In view of its subjective nature, the qualitative design needed to be backed up by the quantitative approach to enable triangulation. Qualitative research in this study was found to be suitable for discovering, orienting, finding out and gaining insight into the problem. Qualitative information was also obtained through literature review from books, research reports, journals and the internet. Observations were used as a qualitative research method because they depended on the subjective judgment of the researcher. In most cases, simple on-site orientations were carried out as outlined by Rogers (2011: 76) in order to gain an appreciation of existing security systems.

Time and permission constraints limited the number of sites visits carried out. However, the few of the site visits conducted were valuable to the study. Taking of site photographs was not possible due to the sensitivity of the information and ethical considerations. According to Tustin, Ligthelm, Martins and Van Wyk (2005: 265), observations are useful in that they provide the researcher with an independent and unbiased deduction of the natural setting. While the research was non-experimental, it had variables explored included security risks and security measures. The security measures in use depend on the perceived security risks and the ability of the company to employ desirable security measures. Some companies may not have the capacity to deploy appropriate security systems due to lack of skills and financial constraints. Nonetheless, the incidence of security risks can be dependent on the effectiveness of the security measures.

2.2.2 Quantitative design

The study was a descriptive case-study exploratory research for which the quantitative approach was also suitable. The quantitative method consisted of a survey questionnaire. Quantitative research was carried out after the qualitative data gathering. At most sites, the researcher used a top-down approach by first approaching top management. The researcher would then be accompanied on a site visit. Most of the observations were structured while a few were informal. Thereafter, interviews were conducted with management followed by survey questionnaires to functional officers. The majority of questions in the questionnaire were closed-ended on a five-point Likert scale thus enabling objectivity and statistical analysis. The first section of the questionnaire contained demographic items. The content in the questionnaire was operational in scope compared to the interview questions which sought to address managerial issues. The researcher was mindful of the respondents' education levels and ensured that the questions were developed in simple language. The constructs or themes of the questionnaires were mostly derived from the Rogers' Security Risk Management Model. Blaxter (2010: 65) advances that quantitative research covers a relatively large sample as compared to the qualitative design. The questionnaire covered a larger part of the sample than the interview thus contributing significantly to generalisability of the study.

The mixed-method approach was found to be particularly suitable to obtain information from a variety of sources. Integration entails bringing together a range of components to function as a co-ordinated unit for a specific purpose. Another component of quantitative research is crime statistics. However, this research did not obtain crime statistics. Statistics of crime incidents at companies were difficult to obtain because the information was considered to be highly confidential. It was not uncommon that some companies had no records of security incidents or losses. The reporting of crimes committed at a company, which are not public crimes, depends on company policy. It was established during the research that some crimes are not reported to the criminal justice system as they are disposed of through company disciplinary procedures and civil actions for loss recoveries. The value stolen was difficult to obtain from most industrial sites.

The use of mixed method approach allowed the researcher to compare information from different sources. Comparisons were made on observations, interviews and the survey. And with additional information from literature review, the study had considerably adequate information to rely on for validity and reliability.

2.3 POPULATION AND SAMPLING

According to Kothari (2004: 72), a population is the larger universe from which a sample is drawn and information is then gathered from the drawn sample. The same author (Kothari) goes on to include the need for a plan to collect a sample. The plan is called a sampling design. If the research covers the whole population it is referred to as a census instead of a sample. In most studies, it is difficult to gather information from the whole population; hence the need for sampling. The population in the Harare industrial sector was very large. It was estimated that the sector had more than 500 sites of which some are not industrial and therefore, fell outside the scope of the study. The study covered the five industrial areas of Workington, Southerton, Willowvale, Graniteside and Msasa in Harare. The population for this study was made up of industrial sites with relatively similar characteristics.

2.3.1 Target population

The target population consisted of industrial companies in Harare. The companies were either engaged in manufacturing, processing, storage, transportation or commercial. Some large groups of companies had locations in most of the five industrial areas. These are large corporates registered on the Zimbabwe Stock Exchange. Most companies included in the study were private limited companies. A few were companies in which the government is a major shareholder. Some sites were small or medium entities owned by individuals. Other sites were foreign international companies.

The target population was chosen for the study because the researcher perceived that integrated security systems play an important role in protecting industrial facilities and operations. Integrated security systems can also be used in other set-ups such as mines, hospitals, hotels and residents though on different approaches depending on the risks. The other factor that influenced

the choice of the target population was that the researcher resided in Harare. The population was in one locality and not geographical spread out over large distances and this was cost effective during the study. While industrial sites were the target population, for completeness of the study, the researcher included some security companies and selected system suppliers in Harare.

2.3.2 Units of analysis

The major units of analysis were identified as the sampled industrial sites. The security companies, security system suppliers and other stakeholders of interest formed additional units of analysis. Support services such as banks, service stations and retail outlets were not included as the sample units of analysis. Only one bank outside the industrial area was included. Twenty five (25) industrial units of analysis were sampled, that is, five from each of the five industrial areas, a security company from each industrial area. The individual units of analysis (sources of data) included company chief executive officers, security managers, functional managers, security and relevant functional officers, operations managers for security companies, and managers of system suppliers. These individual units of analysis were obtained through literature study and personal experiences of the researcher.

Permission letters were prepared for 35 units of analysis. The list was prepared from the sample and used for obtaining permission letters. The list did not include system suppliers or integrators as they were not known prior to fieldwork. One security company was included in each of the five industrial areas. However, the list was not conclusive as adjustments and additions were made before and during field work.

2.3.3 Sampling procedure

A sampling procedure is a selection method for coming up with units of analysis which will be used in the study. Kothari (2004: 58) deduces that sampling designs are usually classified into probability and non-probability approaches. The researcher adopted non-probability which is non-random and used an unrestricted sample. This type of sampling uses methods referred to by Kothari (2004: 58) as deliberate, purposive and judgmental sampling. The sampling method selected was found to be suitable for an exploratory and descriptive study. This type of selection

approach suited the researcher's situation since he conducted the study alone and the sampling techniques were less costly and flexible. In this study, site industrial units of analysis contained the majority sample and were sampled separately. Initially, the researcher used the telephone directory to compile a sample frame of industrial sites from which the sample would be chosen. Through such a deliberate method, the researcher came up with seventy (70), that is fourteen (14) from each industrial area to form the sample frame. After this, the researcher then physically went on the ground to select seven industrial sites from each area viewed as suitable for the study. The researcher did this through purposive selection of companies with the desired characteristics. The main reason was to select operating sites because some companies could have closed or scaled down operations due to the depressed economic environment prevailing in the country. In addition, the researcher wanted to select sites whose outlook showed that they were operational and with a visible security function in the form of security measures such as access control and security guards.

For the selection of security companies, the researcher used convenience sampling by selecting the most visible company with administrative offices in each of the five industrial areas. However, the researcher found no security company based in Msasa and opted for one nearest to that industrial area but not within any of the other areas. As for security system suppliers, the researcher used convenience and deliberate sampling to identify those applicable to systems integration in Harare.

Individual units of analysis were automatically derived from the site units of analysis. The researcher intended to conduct about 35 interviews and to have more than 100 questionnaires completed. The sample was considered to be representative enough for the study.

2.4 PILOT STUDY

A pilot study in the form of a focus group discussion was organised. The group comprised ten professionals. Six of them were security practitioners while four had an information technology (IT) background. The purpose of the discussion was to test the feasibility of applying the research questionnaire. The study was introduced to the group and this was followed by

completion of the draft questionnaires. Participants understood the purpose of the study. It was observed that it took almost 45 minutes to complete the questionnaire. Of concern was that it was too long and that some questions appeared to be duplicated. Furthermore, it was raised that the questions were highly pitched in view of the perceived low knowledge levels among the majority of security practitioners. Therefore, it was envisaged that some respondents would encounter difficulties in completing the questionnaire. Accordingly, this enabled the researcher to simplify the questionnaire to accommodate the concerns raised.

2.5 DATA COLLECTION METHODS

Data were collected after permission had been obtained from some of the sampled organisations. Information was collected using the mixed-method approaches mentioned in the design section. However, this section provides an elaborate exposition of the methods used for the collection of data. These methods were observations, interviews, and survey questionnaire in addition to the literature review. The main methods of primary data collection were observations, interviews and the survey. Literature review is a secondary data collection method for which a separate chapter is reserved and therefore detailed discussion of it in terms of content is covered in Chapter 3. The interview schedule and questionnaire were pre-tested by way of a focus group discussion. A few sites were selected to carry out pilot test of observations which were done informally. The focus group discussion was used to assess whether all the thematic areas pertaining to the study were covered by the data collection methods. The researcher used this platform to refine the data collection tools. The researcher then made some changes to the data collection methods based on the contributions of the focus group discussion members. Thereafter, the researcher did send the draft interview schedule and questionnaire to the supervisor for review and further refinement before fieldwork. Each of the data collection methods is expanded in the following subsections.

2.5.1 Literature review

The researcher used relevant literature to enhance knowledge on the research problem. The literature reviewed comprised of books, research reports, journals, newspaper articles and the internet. The researcher relied heavily on research reports as the main component of the

secondary data because they contain recent and practical information on the research problem. However, some useful information was obtained from reliable internet sources. Books contributed to conceptual understanding on the topic but most of them lacked the practical level of systems integration required by the study. Most of the integration material obtained from literature study covered access control, alarms, and CCTV and fire detection. The studied literature had very little reference to integration with policies and procedures or with other functions of an organisation. Literature on converged and embedded security systems which the researcher sought to include in the study was very limited. Be that as it may, the researcher got valuable information from literature review which was used in combination with primary data. The following were the advantages and disadvantages of collecting secondary data through literature review.

***i)* Advantages**

The following are some of the advantages gained through literature review conducted by the researcher in the context of the study:

- Provided the study with information on research and writings by other researchers;
- It gave the researcher a platform to evaluate the information in the context of the research problem;
- It provides readers of the research report with a broad understanding of the research problem; and
- It gave the researcher a foundation to broaden the scope of the research questions.

***ii)* Disadvantages**

The researcher experienced the following challenges during the process of carrying out the literature review:

- It was time consuming and tedious;

- The researcher had to be critically selective of volume of information available to guard against being taken off-track from the scope of the study ; and
- Some of the information might have been irrelevant to the study and there was a risk of including it in the research.

2.5.2 Information on crime trends

The researcher gathered general information informally during sampling, through the media, local police visits and informal discussions. This showed that industrial assets are highly attractive and vulnerable to such risks as theft, burglary, robbery, fraud, abuse and embezzlement just to mention a few. The researcher was especially keen to obtain information on crimes of concern. Information on crime trends and patterns enabled the researcher to have sufficient background for the data gathering activity.

2.5.3 Focus group discussion

The researcher organised one focus group discussion for the purpose of getting contributions to draft the questionnaire, preparing for site visits and interviews. The focus group discussion was held in Harare on the 16th February 2014. The group discussion involved 10 people composed of six security managers and four ICT officers from various companies all of which were not part of the units of analysis. The researcher initially introduced the group members to the research problem through the approved research proposal. The researcher timed the exercise of completing the questionnaire and noted that it took about an hour.

The researcher gave the participants a focus group discussion evaluation form to complete in order to obtain feedback. The members in their aggregated individual responses indicated that the meeting was worthy to attend and that it was well organised though it could have been better if the numbers were more. They indicated that such group discussions could cover topics to include; security risk management, corporate investigations, return-on-security investment and security policies and procedures among others.

2.5.4 Site visits

During site visits to conduct interviews, the researcher carried out formal and informal observations. These observations impressed upon the site participants and staff members that security is an important function. Some units of analysis took prompt corrective action to rectify observed security weaknesses while some promised to rectify the situation as recommended by the researcher. At units of analysis where authority was granted, the researcher carried out on-site orientations, surveys and semi-audits. Field notes were taken for comparison with interview and questionnaire responses. In some instances, the researcher had to conduct informal observations during the visits to the industrial areas. Observations were used to identify existing security systems and the levels of integration particularly at the access control points. The following are some of the advantages and disadvantages of this method experienced during the study.

i) Advantages of observations

As a general rule, observations are an essential activity in security management. The visits conducted by the researcher enriched the study in the following ways:

- The researcher had a practical view and experience of security systems at a particular site would then be compared with the interview and questionnaire responses;
- The researcher carried out informal interviews with security personnel manning the premises;
- The researcher was able to observe the strengths and weaknesses of some security systems; and
- In some situations, the researcher was able to carry out participant observation which provided in-depth experiences on the functional requirements of security systems.

ii) Disadvantages of observations

The observations provided significant exposure to the researcher but the following limitations were encountered:

- The observations were time consuming given the fact that the researcher conducted data gathering on his own without any form of assistance;
- The information obtained was very limited because certain aspects of functional integration were not observable; and
- At some sites, it was difficult to obtain permission for formal observations.

2.5.5 Interviews

The researcher conducted interviews with selected participants using an interview schedule. A proforma sheet was designed and used to transcribe responses during the interviews for record purposes and systematic analysis. In addition, the researcher took field notes as additional information to support the proforma sheets. The interview schedule is attached as Annexure C.
The following were the perceived advantages and disadvantages of the interview method for use in the study.

i) Advantages of interviews

There were several advantages gained by the researcher but the following were the important benefits derived from the interviews during fieldwork:

- It enabled the collection of in-depth information from respondents in positions of authority;
- The researcher was able to restructure questions as the interview progressed but without deviating from the themes;
- The researcher could adapt to the level of understanding of the interviewee;
- Additional information not included in the interview schedule but necessary for the enhancement of the study was collected; and

- The interviews provided a platform of networking and sharing information on current trends and future collaborative relationships.

ii) **Disadvantages of interviews**

The interviews presented the researcher with an interesting experience but there were a few notable problems. The following were the major constraints when organising and conducting the interviews.

- It was difficult to organise the interview in terms of availability of the interviewees because they were in management positions and had numerous work commitments; and
- Time constraints prohibited the completion of some interviews due to the unavailability of some interviewees and pressure on the researcher.

2.5.6 Survey Questionnaires

The researcher applied a survey questionnaire (attached as Annexure D). The questionnaire contained 11 thematic SSI questions contained in Sections B to F. Each question had sub-aspects under it as part of the question on a five-point Likert scale. Section 'A' covered demographic information. The questions were grouped in thematic clusters as follows.

- Demographic information;
- Company site information;
- Asset characterisation;
- Threat assessment;
- Integration scope;
- Functional integration;
- IT aspects;
- Key players in systems integration;
- Integration process;
- Critical success factors for systems integration;

- Benefits of security systems integration;
- Challenges of security systems integration; and
- Other factors.

The survey questionnaire did cover a reasonably large number of respondents. The questionnaires were hand delivered or e-mailed by the researcher. The completed questionnaires were then collected by the researcher or returned by e-mail. The researcher was cognisant of some of the advantages and disadvantages of the survey questionnaire related to the study and they are listed below.

***i)* Advantages of questionnaires**

The researcher used the questionnaire as one of the mixed methods for collecting data. The study experienced the following advantages in the survey:

- It was cost effective given that a reasonable number of respondents completed the questionnaire;
- The respondents were not influenced by the researcher in providing their responses;
- Respondents could provide well thought out answers to the questions; and
- The researcher obtained sufficient information for quantitative analysis.

***ii)* Disadvantages of questionnaires**

While the survey investigation contributed significantly to information gathering, there were certain constraints. The researcher experienced the following problems when gathering information through questionnaires:

- The researcher could not get additional information outside the scope of the questions. as compared to the interview;
- A large number of the questionnaires distributed were not returned;

- Physical distribution of the questionnaires was time consuming and costly; and
- The return of completed questionnaires took a long time than anticipated thus delaying the analysis of data and completion of the study.

2.6 DATA ANALYSIS

The collected data was analysed and interpreted in readable format for presentation in the research report. The purpose of data analysis was to make sense out of the collected data for deductions, recommendations and conclusions to be made. As mentioned earlier on, the mixed method approach of the research design consisted of qualitative and quantitative data. Therefore, the analysis followed a two-stage approach of qualitative and quantitative analysis. Qualitative analysis covered data collected through observations and interviews. Quantitative analysis covered information collected through questionnaires.

2.6.1 Qualitative data analysis

Qualitative data was collected from a smaller sample of the units of analysis mainly through observations and interviews. The information was recorded on proforma sheets and field notes during fieldwork. Names of respondents or sites observed were not indicated on the proforma sheets or field notes. The information was arranged according to the themes and patterns. The researcher organised the information in an orderly fashion and did some editing for identification of errors before analysis. During the editing process, the researcher ensured that there was no alteration from the original meaning of the responses. The information was then clustered into categories according to the themes. A code sheet was prepared in which the responses were coded according to themes. Qualitative analysis is by nature mainly descriptive. However, some of the responses were transformed into frequencies by counting the number of field notes. Therefore, the findings are presented in a descriptive and quantitative format. Simple arithmetic was used, for example, in counting sites where integrated security systems were observed by the researcher. Clustering was used to group similar observations and responses. Qualitative analysis was in addition used to establish the similarity of observations and views from respondents.

2.6.2 Quantitative data analysis

This form of analysis (quantitative) was used to analyse data obtained through survey questionnaires. The completed questionnaires were numerically numbered to establish the original meanings. A master code sheet was developed and all the responses allocated codes as following the sequence of the questionnaire. The codes were according to the themes in the questionnaire. Descriptive analysis was carried out through frequency distributions to categorise according to percentages and means. The information is presented in tables and figures. The researcher engaged a statistician for statistical processing using Statistical Package of Social Science (SPSS). The study used central theorem tests to measure the significance of data. These tests included means, standard deviation, variance analysis and Kolmogorov-Smirnov and Shapiro Wilk normality tests.

2.7 DATA TRIANGULATION

The sources of data for this study were literature review, observations, interviews and questionnaires. Zafar (2010: 47) asserts that there are several advantages of using different sources of information. The findings of this study are attributed to different but related sources of information. The combined use of literature study, observations, interviews and questionnaires provided corroboration of the findings (Zafar, 2010: 47). This study used several methods to analyse the data. These include qualitative descriptions, descriptive statistics, correlations, composite statistics, and normality tests among others. All these methods demonstrated some degree of serious research efforts. However, such combinations do not necessarily entail completeness of the study. Other areas of the study may not have received sufficient attention or may have been completely left out.

Data triangulation entailed combining the analysed data from qualitative analysis, quantitative analysis and the literature review. This type of analysis ensured triangulation by including information from different sources. This composite form of analysis was used to establish common patterns and trends in integrated security systems. Recommendations and conclusions were derived from this type of analysis. Triangulation of data combined common themes in

interviews, questionnaires and observations. The common themes included among others; asset characterisation, security risks, scope of integration, organisational issues, perceived benefits and challenges among others. This afforded the researcher a holistic picture of the findings of the study. This approach was useful because what could not be covered by one method was complemented by other methods.

2.8 VALIDITY AND RELIABILITY

For a research to be scientifically acceptable, it must be valid and reliable (De Vos, Strydom, Fouche & Delport 2005: 162-163). Validity and reliability can be accomplished by implementing an acceptable research design for the study. According to De Vos *et al.* (2005: 162), validity mainly pertains to the accuracy of the research instruments in measuring what they are supposed to measure. Reliability relates to the ability of the research design to be replicated and bring the same results (De Vos *et al*. 2005: 162-163). If a research design is repeated and brings different results, then it can be deemed unreliable. A study should satisfy both validity and reliability for it to be accepted**.** Multiple units of analysis were drawn from all areas of the Harare industrial sector to ensure adequate coverage. The researcher ensured that anonymity and confidentiality were maintained when collecting data. The same questions were asked throughout the interviews by utilising the interview schedule. The researcher ensured that the questions in the interviews and questionnaires were suitably understood by the respondents. The instruments contained questions of fact on existing security systems and opinion on integration of security systems. In instances where the responses were ambiguous, the researcher sought for clarification from respondents during interviews.

Corroboration was attained through the use of combined methods of data collection in the form of observations, interviews and questionnaires. The information obtained from interviews was compared with questionnaire responses as well as field notes taken by the researcher. Individuals used in the focus group discussion for pre-testing the instrument were excluded in the main study.

2.8.1 Validity

For a study to be valid, all outside interventions or influences (extraneous variables) must be excluded from the research design (Marczy, *et al*. 2005: 174). These unrelated influences may be erroneously included in sampling, interview and questionnaire design. In the context of interviews and questionnaires, these can be in the form of leading questions, double barrelled and ambiguous questions. In order to ensure internal validity, the researcher pilot tested the interview and questionnaires through a focus group discussion to remove any potential errors in the draft questions. During the sampling process, adequate safeguards against selection bias were made although this could not be totally avoided owing to the non-random sampling techniques used. The researcher selected industrial units of analysis so that they were evenly spread out in each of the five industrial areas. Security service companies selected were from different organisations of each industrial area included in the study. During the course of the study, the researcher ensured that no provide special treatment to any participants.

External validity refers to the extent to which the research results can be generalised to other situations similar to the area of study (Marczyk, et al. 2005: 190). In order to ensure external validity, the researcher should avoid any selection biases or undue loss of a large number of participants. If the final respondents are substantially reduced in number, the research may be externally invalid. In carrying out literature review, the researcher consulted recent sources of information to prevent the effects of maturation. Out-dated information may not be appropriate for contemporary security management issues. The themes in the questions were derived from the McKinsey 7-S framework and the Rogers Security Risk Management Model which are reputable models and were considered relevant to the study. The themes in the research instruments were arranged in a consistent fashion. In questions were the Likert scale was used, the responses were grouped according to the themes. The potential loss of units of analysis through refusal or drop outs was safeguarded by having extra units in the permission letters. It was foreseen that some units of analysis could refuse to participate in the study thus necessitating obtaining sufficient permission letters.

The collection of information was done by the researcher without any outside assistance. Use of untrained field workers could have impacted negatively on the validity of the study. Respondents who participated in the interview did not participate in the survey questionnaire and vice versa. The researcher engaged both the direct and indirect method of collecting information. Cross validation through literature review and observations was utilised. Participants used in the pre-tests were not part of the main study. Literature review was to some extent used for triangulation with information collected from other sources. Statistical tests were carried out using SPSS to determine relationships on collected data. Cappers (2008: 94) alludes that the mixed method approach of the research design enables triangulation of information from different sources through a combination of qualitative and quantitative approaches; hence the researcher found the approach to be suitable for the study.

2.8.2 Reliability

Reliability refers to the acceptance of the research for application in other areas outside the case study but with similar characteristics. The findings and recommendations on integrated security systems obtained from the study can be implemented in other set-ups where integrated security systems are used. The researcher ensured reliability by removing bias from sample selection and design of the research instruments. However, it is difficult to completely remove the element of bias in exploratory and descriptive studies. The researcher ensured that the research instruments are applied consistently throughout the study without any variations or major amendments as the study progressed. The margin of error should not be large enough to vitiate the validity and reliability of the study. The questions were categorised into themes and the data collection techniques were structured. The researcher did not intend to use unstructured in-depth interviews. Where unstructured interviews were used outside the scope of the sample, it was for purposes of obtaining general opinions on the problem as supportive information for future use by the researcher in his profession as a security practitioner. The use of both closed and open-ended questions enabled cross checking of responses.

Interviews, survey questionnaires and observations are widely accepted methods of collecting information in exploratory and descriptive case studies. The researcher was cautious of the

dangers of applying his own knowledge and experience in security management as this could have led to biased data collection. It is an unacceptable practice for a researcher to use his or her own opinions in conducting research particularly when presenting findings and recommendations as this will affect the reliability of the study. The researcher pre-tested the research instruments to enhance validity and reliability. This was done through a focus group discussion which provided a good platform for developing the research instruments. Marzyck *et al.* (2005: 170-172) also confirm the use of focus group discussions for the preparation of questionnaires. The draft questionnaire was reviewed before final adoption for field work.

2.9 PROBLEMS ENCOUNTERED

The researcher encountered the following problems during the study:

2.9.1 Sampling

According to the research proposal, the researcher intended to use a quantitative systematic random sampling method. However, when the researcher started sampling it was observed that random sampling was not practical in the circumstances. The researcher then changed to non-probability deliberate and convenience sampling. This type of sampling has an element of error in selection because it entails personal judgment by the researcher. In the circumstances, it is difficult to measure the margin of error by the researcher in selecting units of analysis. However, the researcher tried to ensure that the selected units of analysis were evenly spread out. Bryman (1988: 22) cautions that the researcher should be prepared to answer questions as to why a particular company was picked for the study and the researcher was prepared to sufficiently address this challenge. The sampled units of analysis had the requisite characteristics to participate in the study. Therefore, by adopting non-probability sampling, some units of analysis which could have been included in the study were deliberately left out. If the researcher had used probability sampling, some unsuitable units of analysis without the requisite characteristics could have been included. Use of random sampling could have been more costly and time consuming. Nonetheless, purposive sampling was deemed suitable for this explorative study.

2.9.2 Participant denial

According to Bryman (1988: 22), the researcher should be mindful of the fact that co-operation can be withdrawn. The researcher was confronted with the problem of some respondents at particular sites not being granted authority to participate in the study. This reduced the number of participants and if the magnitude had been too large, this could have affected the integrity of the study. In the event that this happened, the researcher resorted to reserve units of analysis for which authority would have been granted.

2.9.3 Response rate

The rate of response might have been affected by some of the following likely reasons:

- Some participants were unavailable for various reasons such as, illness, leave, absence and work commitments;
- Inability to complete the questionnaire effectively due to low levels of education. Some participants might not have been able to fully comprehend the content of the questionnaire particularly higher order questions; and
- Some participants might not have taken the study seriously and their responses were consequently poor.

In anticipation of response rate problems, Bryman (1988: 22) advises that response can be improved if the research is perceived as helpful by sampled organisations. Crime and loss awareness was high among the participants and the research was viewed positively.

2.9.4 Sensitivity of information

Company information is generally considered confidential in most organisations. Bryman (1988: 22) cautions that large scale organisations are mostly sensitive to individual research and to the publication of its findings. To safeguard against this, the researcher assured all organisations and participants of anonymity in all activities with the respondent participants. The researcher faced resistance at some sites in the provision of company data relating to security incidents. Electronic

recording equipment was not used during interviews as this might have caused some respondents to be suspicious and withhold necessary information.

2.9.5 Time and resource constraints

It was the researcher's intention to complete the study in the year earlier but this was not possible.. The researcher conducted the study on his own and was not funded. In addition the researcher had a heavy workload due to other personal commitments impacting severely on the smooth progression of the research. Accordingly the researcher resorted to working overnight in some instances on the research project. Coverage of all participants over a given period of time was hectic due to time and resource constraints on both the researcher and some of the participants.

2.10 ETHICAL CONSIDERATIONS

The researcher endeavoured in all respects to comply with the UNISA Code of Research Ethics during the study. In some instance written approval of authority was obtained through permission letters from organisations participating in the study. The interviewees were informed that their participation is voluntary. The top portion of the questionnaire had a clause informing respondents on an individual basis either to participate or not. It was the duty of the researcher to keep all the information obtained in confidence and to assure the participants of this aspect. The respondents were guaranteed of anonymity by the researcher**.**

2.11 CONCLUSION

This chapter covered research methods, which is the central part of the study that links the problem statement with findings and recommendations. It contains the critical stage of research design in which a non-experimental mixed-method approach was adopted. The reasons for this strategy were explained at length throughout this chapter. Population and sampling issues were discussed with emphasis placed on non-probability sampling approach for this exploratory study. The chapter then deliberated on data collection methods mainly composed of observations,

interviews and questionnaires. Data analysis approaches through descriptive and quantitative statistical analysis were explored. Issues of validity and reliability and how these can be safeguarded were discussed. This was followed by problems encountered. The last aspect before this conclusion was on ethical considerations. Having dwelt on research methods, the next chapter covers literature review.

CHAPTER 3

LITERATURE REVIEW

3.1 INTRODUCTION

This chapter deals with an insightful background on the implementation of integrated security systems (ISS) as well as to deliver an understanding of why the study was important and relevant in the field of security management. This review provides an extended examination of ISS, their place and value to industrial organisations in particular and other related situations. Brooks (2008: 12-23) states that security management is a multidisciplinary profession requiring a diverse range of knowledge across many areas. Because of increasing demands in today's environment, security management requires a multifunctional approach in problem solving. Brooks (*ibid*) advances several categories of the multidisciplinary context which include criminology, business, security and facilities management among others which are combined into a security framework. While Brooks (*ibid)* advocates for a security framework, this study's assertion is on security systems which are interdependent but co-ordinated to achieve specific protection objectives. Within business management, the security professional is expected to have understanding of human resources, procurement, operations, financial processes and information systems, among others. In today's business context, risks mainly reside in processes and systems rather than only in observable physical objects.

The purpose of the study was to provide a background and platform of understanding the implementation of ISS. In order to achieve this, the review initially looked at the following areas; integration theory, asset characterisation, security risk assessment and industrial security measures. The review also utilised two models in the form of the McKinsey 7-S Framework (Thompson & Martin 2005: 139) and Rogers Security Risk Management Model (Rogers 2011: 17) in the context of security systems integration (SSI). Another aspect covered was that of SSI in the contemporary business environment, and how security can be integrated with other company functions. After security risk assessment and using Rogers Security Risk Management Model as a guide, the review

looked at industrial security measures. Other aspects of relevancy to the study reviewed included, challenges, benefits and factors critical for the successful implementation of ISS. The mixed-method approach used in the chapter on research methodology was again applied to include the review of literature from a variety of sources. The sources consulted included books, research reports, journals, magazines and websites. This approach enabled a comparison of information from different backgrounds. The review revealed that SSI has evolved from guard and security system to a complex and relatively converged system that removes much of the decision making from the guard. Much of the human decision making in many security systems is counterchecked by the security sub-system components. The review explored various levels of integration but specifically focused on security systems and other organisation functions. Business leaders are now looking for greater return from their security investments and security practitioners should not base their activities on daily routines but should rather be continuously exploring opportunities for cost-effectiveness. Security management should now be viewed as a function that adds value to the operations of the organisation by safeguarding the company from security-related losses.

3.2 INTEGRATION THEORY

The concept of integration has evolved for some time and has recently gained much momentum in organisations and this has influenced security management to some extent. Integration is related to total quality management because of its holistic approach. Much of the theoretical literature on integration reviewed was mainly on SSI. Fay (2011: 411) articulates the three main parts of integration as people, processes and physical security. Integration entails that people, processes and physical security are interlinked. While Fay (*ibid*) provides a good descriptive model of integration, the review observed that the author left out the key component of information communication technology which links integrated systems. Business operations are driven by information in various formats which can be verbal communication, written communication or through information technology systems. Therefore, the review noted that information systems are a key driver of ISS. If this reasoning is sufficiently applied, the availability or non-availability

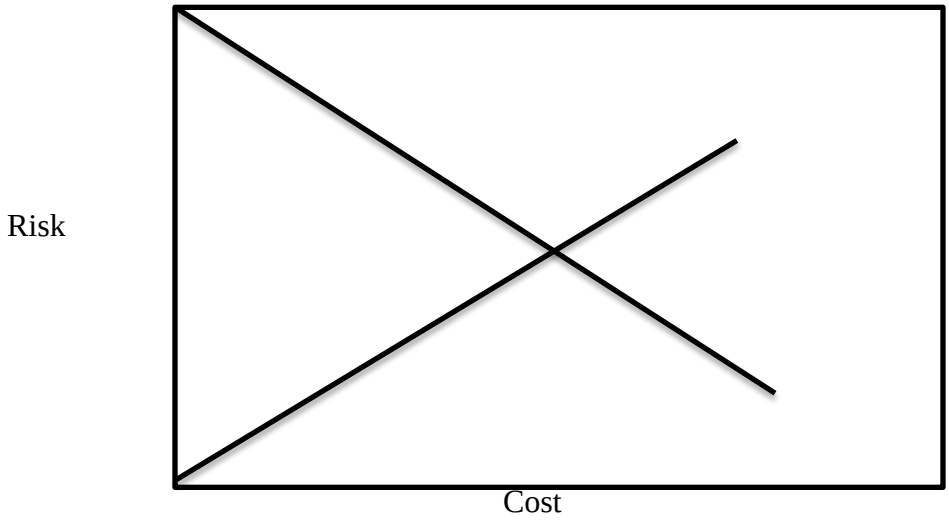
of information within the security system can impact on the effectiveness of the system. Timeous availability of information in a security system can lead to the prevention and detection of security incidents. This would be the case with the use of, for example, electronic article surveillance, CCTV and intrusion alarm systems. These systems are sources of information which can lead to an occurrence being responded to. This demonstrates that the effectiveness of security systems is dependent on the availability of reliable, dependable and accurate information.

Fay (2011: 412) further discloses that when the sub-systems work together, they are said to be in harmony with one another to achieve predetermined objectives. Accordingly, this study was in agreement with Fay's observations that stand-alone systems cannot achieve effective unity of purpose. Security systems which are purposefully integrated are more effective than stand-alone systems. An example of this would be a CCTV system integrated with an electronic access control system. However, the concept of integration should not be misconstrued as to mean that stand-alone security measures are not necessary. In fact, security sub-systems are derived from a combination of stand-alone security measures combined into a system. In some situations, stand-alone security measures may still be cost-effective. This would be a case like for example with a gate in a relatively crime free residential area. Stand-alone security measures act as support elements to an ISS and are therefore essential components of a security system.

Du Plooy (2012:3) made similar observations on integration by emphasising a comprehensive approach to risk management through consolidation of previously fragmented systems (often isolated in silos or separate compartments) in order to improve organisation effectiveness. Compartmentalisation can be attributed to the functional organisation structure which is predominant in most organisations. When security is viewed as an independent function, it may not be aware of what is happening in other functions of the organisation. In an integrated set-up, security activities are linked to other business functions. Armstrong (1992: 35) adopts a simplistic but comprehensive framework of human resources integration with other functions of the organisation, a framework which was found to be applicable to integrating security with other business

functions. The framework is depicted in Figure 3.3 later in this review in a security management integration context. Clifford (2004: 193) highlights the concept of dualism which ascribes to the fact that something is related or not related to security. The dualism mind-set may be predominant in some industrial organisations where security may be viewed as a backyard function and this may have negative implications to the organisation. Clifford (2004: 203) also holds the view that the integration theme is becoming more popular that Security Management (the industry's trade magazine) runs a regular section titled, "Focus on Integration". Clifford *(*2004*:* 105*)* elaborates that the seemingly independent aspects of a security system are not so independent but should work together to ensure a seamless ISS. However, caution should be applied because it can be difficult if not impossible to achieve an absolute security system which is impenetrable at an industrial facility. An absolutely seamless ISS could have the potential to constrain business operations through excessively costly security measures comprising personnel security, physical security, information security, interdepartmental dependencies and legal liability issues. In most business security system designs, the element of cost is essential because the security system will be funded from the operations which the system seeks to protect. In the Security Risk Management Model, Rogers (2011: 17) provides for cost implications through a return-on-security investment exercise. Rogers (2011: 76) demonstrates the cost implications of security measures in a diagrammatic representation which is shown in Figure 3.1 below.

Figure 3.1: Relationship between risk and security costs



The above diagram indicates that as risk drops due to security measures being implemented, there is a relative rise in security costs. The point of equilibrium in the diagram is where risk and cost levels meet. The major weakness of the above model is that in practice, it is difficult to arrive at such levels in quantitative terms. However, the model conveys the fact that it is important to accept that security measures are implemented at a cost relative to the risks which they seek to manage.

To conclude the theoretical foundations of SSI, Jackson (2003: 1) acknowledges that a system is a complex whole the functioning of which is dependent on its sub-systems and interactions between those sub-systems. In the scope of Jackson's assertion, it is important to understand the parts of a security system in order to understand the whole system. Jackson (*ibid*) further clarifies that sub-systems interact to ensure integration and co-ordination of the system through input from the environment, processing and output back to the environment. However, Jackson (2003: 6) cautions that a system should not be closed but opened for it to interact with the environment. According to Jackson (2003: 49), system analysis in the context of security management focuses on problem identification through security risk assessment. This is then followed by determination of possible solutions through recommendation of security measures. The cost implications of the security measures are evaluated by way of a return-on-investment exercise because

it is important to appreciate the benefits of the security system in the context of its costs. The risk consequences or limitations of the security system should be identified and appropriate safeguards put in place.

Jackson (*ibid*) discloses the attributes of a system which include that it should be multifunctional in order to co-ordinate various functions. The system design should specify requirements for implementation. In addition, it should be an effectively proposed solution which meets user requirements.

The above presupposes that security systems should be enterprise-wide cutting across all functional disciplines. It was also Jackson's (2003: 31) conviction that organisational problems are interdependent and require resolution through an integrated approach. This observation is highly applicable to most industrial organisations because one function of the company may be dependent on other functions to achieve its functional objectives which then contribute to ultimate organisational goals.

3.3 INDUSTRIAL ASSET CHARACTERISATION

The purpose of security at an industrial facility is to provide protection to the company's assets and operations. Rogers Security Risk Management Model (Rogers 2011. 17) provides for an activity referred to as on-site-orientation in which one of the tasks is to identify vulnerable assets. In the context of this study, it also includes the identification of vulnerable operations and processes. It was the study's assumption that security risks reside in assets, operations and processes. It was also the review's contention that Rogers (*ibid*) should have included operations and processes within the scope of assets unless the author was operating from general security management perspective which of course could have been the case anyway. The risk assessment process by Vellani (2007: 11) shows asset identification as the first step in the process. In comparison, Rogers Security Risk Management Model (2011: 17) misses this important point by relegating it to be within the on-site-orientation stage. It was the view of this study and also that of Vellani *(*2007:11) that the prime purpose of any security management function is to protect assets, operations and processes. From an industrial perspective, assets would include infrastructure which Vellani (2007: 12) rightly identifies as essential for an organisation

to perform its functions and operations. In addition, Vellani (2007: 15) holds the view that assets comprise of people, property, and information. However, it can be argued that operations and processes fall within the scope of critical assets as underlined by Vellani **(***ibid***)** who provides a link between assets and business operations.

As for asset classification, Vellani (*ibid*) provides that assets should be categorised using criteria such as; criticality of the asset to the organisation's operations and business continuity and the immediate impact of the asset if it was to be lost or damaged. The time and cost of replacing the asset to enable business resumption and the effect of the loss of the asset on other assets are other criteria for asset categorisation.

One logical method of identifying assets, operations and processes is by using applicable frameworks or models. A model which can be conveniently used at an industrial facility for this purpose is Porter's Value Chain as captured by Louw and Venter (2009: 157-159). The critical assets, operations and processes can be systematically profiled within each of the primary and support activities. A tabular example form of asset identification derived from the value chain is shown Table 3.1 below.

Table 3.1: Identification of assets using a value chain perspective	
Primary activities	**Assets**
Inbound Logistics	Raw materials and components
Operations	People, machinery, equipment
Outbound logistics	Products and services
Support activities	**Assets**
Information Technology	IT equipment, server rooms
Human Resources Management	People, processes
Procurement	Processes
Finance	Revenue and procedures
Administration	Movable and immovable assets

Another method of identifying assets and their criticality levels which is related to the value chain analysis is through functional analysis as advanced by Pearce and Robinson (2007: 156-159). In functional identification of assets, the security professional goes through each function and in conjunction with the asset owners in the respective departments, profiles the assets, operations and processes that need protection. Pearce and Robinson (*ibid*) outline the functions to include marketing, finance, operations, human resources, procurement, administration, and information management.

Interestingly, Vellani (2007: 15-17.) gives a view of assets as "targets" from a criminal (adversarial) point of view. Vellani *(ibid)* goes on to develop criteria for evaluating target values which includes the asset's potential for loss, damage or destruction and extent of disruption to operations and business continuity. Other criteria include impact on the organisation's reputation, and attention the asset would attract to the media and public upon its loss. In the event of loss or damage, other assets may cause fatalities and injuries with consequent impact on employee morale and productivity. The potential for recovering the asset in its original form for continued use should also be considered.

Vellani (2007: 20) recommends a four level scale for profiling assets as critical, high, medium and low. The Hanser Group (2010: B1-6) recommends a four criteria process for analysing critical assets which includes the number of workforce on site, service delivery provided by the asset, other assets dependent on the asset and the importance of the asset to company objectives. However, it can be argued that the number of workforce on site may not be relevant to the criticality of the asset because in today's environment with advances in technology, it is possible to find very few people at an industrial site but with critical assets. The review noted with enthusiasm the Hanser Group's (*ibid*) inclusion of operations and processes in asset characterisation. Generally, assets as disclosed by the Hanser Group (2010: 1-10) include; infrastructure, buildings, people, machinery, equipment, materials, products, semi-finished products, motor vehicles, revenue and information. These are some of the critical assets which ISS aim to protect.

In concluding this section, the review noted Torres (2007: 36) deliberation on a limited scope of integration but which nonetheless succinctly affirms the purpose of security on the protection of assets. Surprisingly, Torres (*ibid*) exhibits a serious shortfall of the security management function where mention is made that security is extremely limited in what it can contribute to an organisation other than protecting its facilities and property. It was the intention of this study to resolve such misconceptions which relegate the strategic importance of security in organisations. Nonetheless, Torres (*ibid*) work provided significant contributions to security management.

3.4 SECURITY RISK ASSESSMENT

The implementation of effective security measures is a product of a comprehensive security risk assessment activity. In regard to this, Landoll and Landoll (2006: 9-11) provide the view that security risk assessment is a review of the assets, threat environment in the context of existing security measures, the identification of vulnerabilities and the recommendation of additional controls to reduce losses to the organisation. The security function employs both a proactive and reactive approach to risk management. The proactive approach is the one desirable because it anticipates and safeguards the company from losses through security (crime) risks. This approach requires that the security risks confronting the assets be well understood in order to deploy appropriate security measures. Vellani (2007: 14) determines risk assessment as the process of identifying and prioritising risks in order to effectively implement countermeasures.

Rogers (2011: 12) considers risk analysis within the scope of risk assessment as to include a systematic approach to problem identification and solution determination. The study agreed with the above sentiments and concluded that security risk assessment comprises of threat assessment, risk analysis, security survey and vulnerability assessment. Each of these three aspects was reviewed separately and discussed below.

3.4.1 Threat assessment

A threat assessment is carried out after identification of the assets to be protected and in the context of existing security measures to identify sources of exposure to risks confronting the assets. Assets, risks and threats are interdependent aspects to be viewed holistically during the risk assessment process. The separation of assets, risks and threats is for discussion purposes only. According to Vellani (2007: 28), a threat is anything that can exploit a vulnerability causing loss or damage to the asset and those threats can be in the form of human actions or natural occurrences. The majority of threat sources from an industrial facility could be from human actions in the form of employees or outsiders. Human action may be intentional or negligent. Negligence can be attributed to lack of attention or inadequate competencies to carry out a specific activity. Threat should be linked to the asset and the risk. If the asset is for example revenue and the risk is fraud leading to loss of funds, the threat can be from employees, outsiders, supply chain elements or crime syndicates. According to the Hanser Group (2010: B2-15), threat characterisation assists in the identification of possible sources of threats. The Hanser Group (*ibid*) recommends a threat assessment process which can also be applicable to industrial facilities. The threat assessment process starts with identification of potential threat sources. These might be criminals, employees, industrial spies, crime syndicates or information hackers and hazards. The identification of threat sources requires background training and experience in aspects of criminology and security risk management for reasonable accuracy. The collection of threat information from previous incidents, police crime statistics, the media, intelligence sources and previous threat assessment surveys will enhance the activity. The identified threat sources are then categorised according to likelihood to attack the assets or processes. Imagination can be used to develop alternative threat sources and evaluation of their likelihood to occur. Vellani (2007: 28-29) recommends that threat assessment should be carried out as and when necessary or

at regular intervals such as quarterly or yearly. Threat assessment is important in industrial facilities because industrial assets are highly attractive to threat sources.

3.4.2 Risk analysis

Rogers (2011*:* 12) expands risk analysis to include crime risk analysis. In dealing with the aspect of risk analysis, Sennewald (2003: 193-196) arrives at the fact that the eventual goal of risk analysis is to strike a balance between the impact of risk and the cost of implementing security measures. Sennewald (*ibid*) goes on to provide the benefits of risk analysis, the most important being the determination of security measures. A closer analysis of the benefits provided by Sennewald seems not to relate to risk analysis but rather to security survey because it can be argued that security measures are determined by way of a security survey. The review agreed with the position of Vellani (2007: 12) in which security risk assessment is a process comprising of asset identification, threat assessment, evaluation of existing security measures and determining recommendations for improvement. The work of Rogers (2011: 112-113) identifies the objectives of risk analysis as to include the identification of vulnerable assets in the form of people, processes, products, information and capital. It also includes the identification of security risks confronting the organisation and reporting to management.

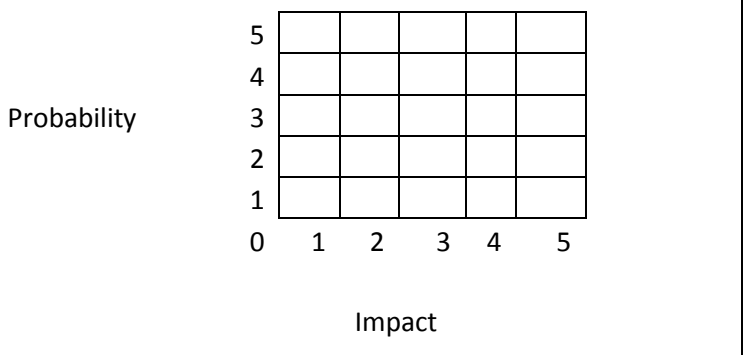
Risk analysis is therefore an informed but subjective determination of likelihood and consequence of a threat occurring event exploiting weaknesses within the security system.

Rogers (2011: 128) developed a risk analysis process that comprises of obtaining authority or permission to carry out the exercise and establishing a team to carry out the analysis which is then followed by asset identification and determining probability and impact. The risks are then prioritised and reported to the client for decision making.

The process articulated by Rogers (*ibid*) above could have been enhanced by carrying out an on-site-orientation by way of site observations, interviews and perusal of records soon after establishing the team. It is through such an activity that a practical risk analysis can be achieved. A desktop risk analysis may lead to determination of inappropriate security measures. In fact, Rogers (*ibid*) acknowledges the inclusion of the on-site-orientation as a component of risk analysis. One remarkable contribution of the risk analysis process advocated to by Rogers (*ibid*) is the composition of a multi-skilled committee to carry out the risk analysis exercise. The risk

analysis matrix provided by Rogers *(ibid)* which is widely used in risk management is shown in Figure 3.2 below.

Figure 3.2: Risk analysis matrix



The above matrix is a good tool for quantifying risks but its major perceived weakness is that the values are determined subjectively even though the use of a team may reduce subjectivity. Vellani (2007: 112) advocates that risk assessments can be both quantitative and qualitative and that risk can be classified as high, medium, and low. The quantification of risk into categories enables the security manager to determine what type of measures to employ to manage the identified risks. The profiling of risks should be well informed to enable implementation of effective measures. There are a number of security risks confronting industrial organisations as disclosed by Lombaard (2006: 6-7) and they include; burglary, theft and fraud, fire, robbery, industrial labour unrest and damage or loss of property including information. These risks if not properly managed in the context of an integrated security management programme can have a negative impact on industrial organisations.

3.4.3 Security survey

A security survey is an on-site activity carried out by a security professional to evaluate existing security measures and systems. Fennelly (2013: 41) discloses that a security survey is used to establish the present status of security measures, identify deficiencies and excesses and to make recommendations for improvement. The survey depends on the type of facility to be examined.

Surveys for different types of facilities such as residential, industrial, mining, hospitals and so on can be different in form and scope. In addition, Rogers (2011: 107) recommends a guideline of a security survey sheet based on the specific needs of the facility to be examined. Typically, a security survey involves a tour of the facility, making observations, interviewing staff members including security personnel, perusing policies, procedures and related documents. An in-depth survey in some instances may be preceded by a preliminary survey in the form of an on-site-orientation.

On the same issue, Broder and Tucker (2011: 49) hold the view that a survey is carried out to examine the company or facility's security management plan in particular its policies, procedures, operations and safeguards. According to Broder and Tucker (*ibid*), the survey should aim to establish protection measures for the company's assets against perceived security risks. The survey should also seek to develop access control procedures for various access points. The procedures will ensure secure movement of assets. In addition, Broder and Tucker (*ibid*) also place emphasis on the physical description of the facility and the security of its perimeter. Other areas for consideration include building security, security of the plant, tool room, dispatch, receiving areas, key control arrangements and procedures. Safety and emergency procedures including control of personnel and vehicles should also be evaluated. Particular attention should be given to critical points such as laboratories, server rooms and cash offices. In addition, the surveyor should analyse the loss control procedures in place for their effectiveness. The composition of the security personnel and its adequacy should be included in the survey.

3.4.4 Vulnerability assessment

There is very little difference between security survey and vulnerability because to some extent vulnerability is the remaining exposure in a security system observed during a survey or after recommendations have been implemented. According to Rogers (2011:13), vulnerability implies residual exposure to risk after the security management programme determined by the survey has been implemented. Therefore, vulnerability is a post-survey exposure analysis. As a result, security is not complete because weakness in security may continue to exist even after the survey and implementation of survey recommendations. In practice, some survey recommendations may not be implemented. In regard to the security survey's findings, management can opt to treat, terminate, tolerate or transfer the risk. Risk tolerance is an acceptance by management to

continue with operations regardless of the perceived remaining risks. Management may be of the view that further treatment of the risk will increase security costs relative to the risks. Vellani (2007: 86-107) contends that vulnerabilities refer to weaknesses or gaps in a security programme. According to Vellani (*ibid*), a vulnerability assessment can be carried out at any stage of the security management programme but more appropriately during the security survey.

There are different forms and types of vulnerabilities. Some vulnerability pertain to weaknesses in structural characteristics such as perimeter security, access points, and geographic location of the facility. Others could be technical vulnerabilities that may include network weakness, unavailability of intrusion alarm, electronic access control or CCTV and lack of mechanisms for the security of the assets. Operational vulnerabilities point to absence or weak security policies, procedures or internal controls.

The process of vulnerability assessment essentially entails the identification of assets in need of protection at the industrial facility in the context of the security programme. This is then followed by the evaluation of existing security to identify weaknesses and loopholes within the security system. Recommendations are then made to improve existing security. These may include additional security measures, security system upgrade, review of policies and procedures and manpower needs. However, as mentioned earlier on, vulnerability continues to exist even after implementation of the recommendations. It is the reduction of the level of vulnerability that is important to prevent further loss of assets.

The goals of vulnerability assessment include among others the protection of the facility and to ensure continuity of operations in a relatively safe and secure environment. A vulnerability assessment reveals opportunities that can be exploited by threat sources to attack the assets. It is an activity which is part of the security survey aimed at identifying weaknesses, gaps or loopholes in the security systems. Based on the outcomes of the vulnerability assessment, decisions can be made on how to improve the security systems.

A vulnerability assessment team can be composed of persons from various departments. The composition of the team depends on the nature of the perceived security problems. In some cases, it may include security, health and safety, audit and risk, operations or information

technology. The reason for a multifunctional team is to combine knowledge and awareness so that potential weaknesses are not overlooked during the assessment process.

There are various types of vulnerability assessments. The type of assessment to be employed depends on the security problems confronting the organisation. Usually, a vulnerability assessment is carried out following a security incident. Asset-based assessments focus on the critical assets and the threats that may exploit weaknesses in the protection of those assets. Scenario-based assessments develop various methods of possible attacks *(modus operandi*) that might be used by the threat sources. The scenario-based vulnerability assessment method follows certain steps which include speculation on a potential scenario to investigate, examination of the target-asset's characteristics followed by Identifying and evaluating potential types of threat sources and methods of attack. The vulnerability assessment team should anticipate the potential consequences of damage or loss of the asset. Techniques for scenario based vulnerability assessment include brainstorming, desktop scenario case studies and worst case scenario analysis. Another method for vulnerability assessment can be root-cause analysis process while some situations the assessment can be conducted using penetration tests. For a vulnerability assessment to be more informative, it is advisable to use mixed methods so as to develop an effective security system.

Generally, steps in the vulnerability assessment cover identification of critical site assets in need of protection, review and evaluation of historical site security incidents, and evaluation of existing security measures and systems. The vulnerability is then rated as very high, high, moderate or low depending on the outcomes. The vulnerability assessment process, though conceptually acceptable, may be difficult to implement in practice. A review of previous cases should not be confined to the site but should extend to other known cases which occurred within the surrounding areas.

Recommendations for additional security measures if applicable are then availed to management for decision making purposes in the form of a vulnerability assessment report. The vulnerability assessment report may take the form of a cover page and table of contents which guides the reader to location of aspects in the report. An executive summary for management perusal gives the objectives and dates of assessment, a summarised outlook of the report especially on findings and recommendations. A section on the scope of the assessment articulates the prime purpose or

security problems covered by the assessment. The facility or asset that was the focus of the assessment is described in brief. The composition of the assessment team is provided including its structure and contributions. The last sections may include summaries on threat assessment, findings and recommendations.

3.5 INDUSTRIAL SECURITY MEASURES

There are a variety of security measures that can be put in place at an industrial facility depending on the assets, threat sources and risks. The choice of prevention strategies depends on the assets to be protected and their attractiveness to threat sources. Lombaard (2006: 37) advocates for a protection in-depth at an industrial facility with layers of security measures and that security measures be integrated into the plans of the facility. The security measures applicable at industrial facilities were reviewed under the following categories.

3.5.1 Physical security measures

According to Lombaard (2006: 155-175), physical security measures normally follow a protection in-depth pattern comprising perimeter security which consists of fences, walls, perimeter lighting, intrusion alarms and guard patrol. Inner perimeter protection is made up of lighting, CCTV, intrusion alarms, guard patrols, dogs, and signage and so on. Perimeter security measures are designed to prevent and delay unauthorised entry through unauthorised points. If they are acting in combination, they are likely to have a higher deterrence, delay and detection effect than if they are stand-alone security measures. A security fence without lighting and back-up guard patrol is not likely to be effective in comparison to the one integrated with lighting, intrusion alarm and guard patrol. Perimeter security is the first line of defence at an industrial facility and should be presented in such a manner that the target becomes unattractive.

3.5.2 Access control

Access control facilitates movement of people, vehicles and goods in and out of the premises. An access control point acts in combination with perimeter security. Perimeter security directs people to the access control point by its outlook of roads, pathways, and signage. Security at the access control point can consist of vehicle and pedestrian gates, turnstiles, electronic access system, security personnel, signage, guard room, lighting, CCTV, policies and procedures and

security information logs. An access control point authenticates entry and exit into the facility. It is a screening point for people, vehicle and articles. An integrated access control point with the appropriate security measures and systems provides the desired agility to the security management programme. A stand-alone access point manned by a guard may not be effective at an industrial facility given the levels of movement into and out of the facility. An integrated access control point ensures accountability of access and egress to the facility.

3.5.3 Security of buildings

Building security at an industrial facility is equally important because it provides the protection of people, physical assets, operations, processes and information. Security measures mainly applicable to buildings include physical barriers, turnstiles, burglar protective measures, lighting, access control through gates and doors, policies and procedures, key control and locking devices, burglar alarms, CCTS, cameras, fire prevention and detection, safes and cabinets, security guards, staff members or undercover surveillance. In regard to this, Vellani (2007: 206) emphasises that the basic function of physical security is to prevent, detect and respond to a threat. Threat sources within buildings are minimised if they have been effectively deterred at the perimeter and access control point. Movement of people and assets within buildings is regulated by policies and procedures

3.5.4 Human security measures

At an industrial site there is likely to be an internal security function staffed with security personnel who are tasked with ensuring the security of the company. The organisation of the security function varies within companies. The importance of the security function is derived from the criticality of the assets and operations coupled with the attractiveness and exposure to threat sources. Some companies may have an internal security function without externally contracted security but others may have back up of contracted security to provide guarding and other ancillary services. The purpose of the security function is, among others, to design, implement, monitor security systems and ensure compliance to security policies and procedures. As part of the security system, the security function provides oversight on security of the premises in conjunction with other security measures. Security is also responsible for detecting, reporting and investigating of security breaches. Security assists staff members and the public on

issues of personal and company security. In order to be effective, the security personnel should be properly selected, trained, equipped and supervised towards predetermined objectives. Above all, security personnel must be highly disciplined, observant, and with good communication skills both verbally and in writing. In order to achieve integration, security activities should be aligned to company operations to ensure that all forms of crime risks are prevented and detected.

3.5.5 Procedural security

Procedural security consists of security policies and procedures covering a wide range of functions and activities as mentioned by Vellani (2007: 174). At an industrial site, policies and procedures may apply to access control, movement of people within the facility, movement of assets, work reporting procedures, internal controls and site security instructions. Procedural security ensures that everybody participates in the security management programme. Policies and procedures require compliance with the security systems. In comparison to other security measures, policies and procedures are the least costly and the most effective if properly implemented. Other security measures should be implemented in conjunction with policies and procedures. The conduct of people can be controlled through policies and procedures.

3.5.6 Loss control measures

In industrial operations, loss control is an issue of concern to management. Loss control targets the movement of goods, materials and revenue within the premises and along the company supply chain. Loss control measures that may be applicable to industrial sites include job descriptions, vetting of personnel, separation of functions, document authentication, electronic article surveillance, authorisation requirements and authority levels, inspections, document processing and transaction processing. The selection of loss control measures depends on the activities of the company. Loss control measures are meant to prevent and detect internal thefts, abuse, pilferage, stock shrinkage, frauds, syndicated crimes, corruption, corporate scandals and the like.

3.5.7 Technical security measures

Today’s security systems are dominated by advancements in technology. The integration of information technology and security is now unavoidable. Technological security measures and

systems include among others electronic access control, electronic article surveillance, electronic person identification, CCTV, intrusion, alarms, cameras, fire detectors, lighting systems, metal detectors, digital video surveillance, video motion detectors point-of-sale systems, internet protocol video systems and intelligent video systems. The list is not exhaustive and depends on the security management programme at the facility and the preference of the security practitioners on site (Vellani 2007; Caputo, 2010 ; Fennelly, 2013).

3.5.8 Crime prevention through environmental design (CPTED)

According to Vellani (2007: 98), CPTED is a security method to reduce opportunities for crime which include methods of manipulating natural settings. In relation to this, Cappers (2008: 56) highlights that CPTED seeks to reduce criminal behaviour through proper design and effective use of the environment. Security measures which may fall under CPTED include security of cash, visibility through lighting, limited access and egress points, employee security awareness, installation of CCTV cameras in strategic locations, deployment of security personnel and target hardening. CPTED is an important crime prevention method as it complements integrated security systems within the features of the facility. According to this concept of CPTED, security measures are incorporated into the set-up and activities within the facility. This method ensures that people are made conscious of security requirements within the facility without necessarily having to be under security supervision. It is a self-serving method of security systems integration.

3.5.9 Situational crime prevention methods (SCPM)

SCPM is the use of a variety of techniques to prevent and detect crime. According to Cappers (2008: 46), they require the involvement of management. SCPM at an industrial site are dependent on the nature and levels of operations of the facility at any given time. When operations are at a high level, security may be escalated and scaled down when operations are low. This would apply to seasonal manufacturing of products such as fireworks, fertilizers and ice crime just to mention a few. Cappers (*ibid*) disclose SCPM as including CCTV, electronic surveillance, and security personnel**.** In the context of the study, SCPM entails that security systems are deployed according to the demands of the company operations. It is a method of deploying security measures according to situational demands and may be cost-effective.

Integrated security systems take on various forms and SCPM contributes significantly in complementing integrated security systems. Security managers are able to justify security costs through deployment of SCPM.

3.5.10 Security awareness

General security awareness programmes at an industrial facility may contribute significantly in generating attentiveness among employees, visitors, customers and contractors about security requirements on the premises. Awareness efforts may take the form of employee induction orientation programmes, visitor checkpoint briefings, monitoring of compliance to security policies and procedures, case study examples, power point presentations, signage, company newsletters and e-mail reminders (Vellani, 2007: 174-176). People are an important component of a security system. Therefore, training and education enhance the understanding of the security system for effective implementation. A security system which is not well understood may present problems or be in conflict with other core functions of the organisation which it is meant to support. The value of a security system can be understood by the users who consist of staff members and outsiders who are supposed to understand its functionality. Users should be provided with information which only enables them to comply with the system. A security system can be compromised if users are aware of its intricate details. Confidential details should be the preserve of the owners of the security system which is usually the security management function.

3.6 APPLICABLE MANAGEMENT MODELS

There are several models in general management and risk management in particular. Security management is a subsidiary discipline of general management science. The review made reference to the McKinsey 7-S Framework (Thompson & Martin2005:139) and the Rogers Security Risk Management Model (Rogers 2011: 17) as elaborated in the following subsections.

3.6.1 The McKinsey 7-S framework

The McKinsey 7-S framework was developed by Peters and Waterman in 1982 (Thompson & Martin 2005: 139). The framework has seven elements which can be used in analysing organisations and strategies. The elements of the 7-S framework incorporated in security systems

integration are strategy, structure, systems, staff, skills, style and shared values. The study developed the following template using the McKinsey 7-S framework as a tool for analysing and developing security management systems.

Table 3.2: The McKinsey 7-S Framework Security Management perspective	
ELEMENT	**ISSUES**
Strategy	Alignment of the security management programme to the overall corporate strategy
Structure	Organisation of the security function and reporting systems
Systems	Integration of security systems in tandem with other systems and processes at the industrial facility
Staff	Security personnel deployments at the facility
Style	Top management risk appetite and posture on security management
Skills	Skills required for the implementation of integrated security systems
Shared values	Buy- in from all company staff on security issues at the site

The above table reveals that all the seven elements should be considered in the implementation of ISS. However, the most important ones according to this study were viewed as strategy, structure, systems and skills. The elements are interdependent and related to each other.

3.6.2 The Rogers Security Risk Management Model

The Rogers Security Risk Management Model was initially developed by Rogers in 2005 with later additions by Olckers (2007) and Kole (2010) as discussed by Rogers (2011: 17-19). The adapted Rogers Security Risk Management Model by Kole (2010) includes aspects of factors that cause crime, the existence of a security policy or mandate. In addition, there are activities of risk analysis, security survey and recommendations on security measures. Other aspects included in the model are service level agreements, return-on-investment and the submission of a security management report. This is then followed by implementation and evaluation of security measures. The last aspect of the model is the review and upgrade of security measures to

improve effectiveness. In relation to this study, the Rogers Security Risk Management Model provides a good background and guideline for the implementation of ISS.

3.7 SCOPE OF INTEGRATION

The decision to integrate security systems at an industrial facility involves top management. There are many issues to be considered in the implementation of ISS. According to Vellani (2007: 582), some of the aspects to be included at a single site include the fact that there should have been a security management problem that could have raised the issue of integration. It is important that the appropriate scope of integration be identified to resolve the problem. Security is such that if an inappropriate security measure is put in place, the problem will not be resolved. Implementation of integrated security systems involves other functions in the organisation and outsiders and therefore key internal and external players should be identified. Integration has cost implications which sometimes involve capital expenditure. Accordingly, it is important to evaluate the cost implications of the intended investment. An ISS may have some limitations. An assessment of challenges and benefits should be carried out before implementation. Consideration should be given to the factors critical for the successful implementation of the integration programme.

The common types of integration were explored but without going into the technical details. The review established the following as some of the components for inclusion in ISS at industrial facilities in the Harare industrial sector.

3.7.1. Perimeter security integration

Perimeter security at an industrial site can be a combination of fence, lighting, intrusion alarm, and video motion detectors, security personnel which can be monitored on or off site or both (Caputo, 2010: 294-300). Integrated perimeter security systems are perceived to provide an effective first line of defence to the facility. The system can deter, delay and detect security incidents and provide timely response when a breach has been detected. Caputo (2010: 295) provides a high level exposition of the technical issues relating to systems integration.

3.7.2 Integrated Access Control System

An integrated access control system may combine electronic access control, turnstiles, weighbridge policies and procedures, CCTV, a guard or control room, panic buttons and security personnel (Caputo, 2010: 294-300). According to Caputo (*ibid*), electronic access control is used to allow or deny access into a facility. Dave (2007: 58) conveys the effective functions of an electronic access control system as a powerful platform for controlling access to a facility. Most security management programmes pay particular attention to access control systems. An integrated access control system is meant to among others protect the facility from unauthorised entry and prevent assets from being stolen or abused. Potential intruders are deterred from entering the premises since the perimeter security will be combined with the access control point. In addition, an access control system provides visibility of security and orientation of persons entering the site. The safety of the facility is enhanced by prohibiting access of unwanted materials and equipment and persons.

3.7.3 Burglar alarm integrated security system

A burglar alarm system is meant to deter, delay and detect entry into buildings such as offices, warehouses, factories, operating system offices at an industrial facility. The system can be integrated by combining lighting, motion detectors, dome cameras, CCTV, security personnel and public address system. The system prevents and detects unauthorised entry to building locations for safety and security reasons. Swepersad (2010: 11) underlines how a security system is integrated through multiple security measures which can be connected to an on-site or off-site monitoring mechanism.

3.7.4 Integrated CCTV system

A CCTV system can be integrated with access control, alarms, guard monitoring and procedures. According to Cappers (2008: 49), CCTV is a powerful measure for deterring and detecting theft. Cappers (2008: 50) also points out that CCTV can be linked to an alarm system while Caputo (2010: 297-300) captures the integration of CCTV with access control.

3.7.5 Integration with Information Communication Technologies

Information communication technologies (ICTs) provide the link for integrated security systems to convey the information for use. Contos, *et al*. (2007: 95) point out that ICTs are a critical element of integrated security systems in organisations. Linking is provided by transmission modes which can be on a local area network (LAN) or wide area network (WAN) using an integrated services digital network (ISDN), asymmetric digital subscriber lines (ASDL) or wireless transmission. Monitoring can be in control rooms, desktop computers, laptops or mobile phones. The security systems such as access control, CCTV and alarms are linked to ICTs to complete the integration.

3.7.6 Integration with policies and procedures

Security policies and procedures provide for the effective implementation of integrated security systems. Policies and procedures outline how, what, why, when and who should carry out specific security related functions and activities. According to Rogers (2011: 43-47), the purpose of a security policy is to among others protect company assets, resolve conflict, delegate authority, limit authority, provide for responsibility and accountability. Security procedures are derived from the security policy and are operational in scope. Procedures outline specific duties and functions that must or must not be carried out by security personnel and staff members. Procedures can be separated into functions such as access control, asset movement, receipt and dispatch. Vellani (2007: 207) supports the same view that security countermeasures should be used in conjunction with personnel, policies and procedures. To emphasise the importance of policies and procedures, Vellani (2007: 173-181) elaborates by including security awareness programmes, security management plans and emergency management. Vellani (2007: 173) rightly pinpoints that security policies and procedures are often overlooked yet they are the most cost-effective. Policies and procedures may be written or unwritten but it is recommended that to ensure consistent compliance, they should be in written form. In addition, security personnel at a site can be provided with detailed site security instructions which are specific to their duties at

the site. Regular inspections and spot checks should be carried out to ensure compliance of security policies and procedures in conjunction with other security measures.

3.7.7 Functional integration

Most companies are organised along functional lines and are hierarchically structured. Interdepartmental co-ordination is through leadership and management efforts. Some functions may operate individually which may not contribute to effective achievement of company goals and objectives. Intra-company conflicts are not an uncommon occurrence at some organisations. While separation of functions and specialisation has many advantages, it may create challenging management issues leading to inefficiency. Armstrong (1992: 35) identified the need for intra-functional integration which this study advocates. Figure 3.3 below is a conceptual framework of integration of security and other organisation functions.

Table 3.3: Integration of security with other functions

Security elements	**Business functions for integration with security systems**				
	ICT	Human resources	Finance and Admin	Operations	Marketing & Distribution
EAC	X	X		X	
CCTV				X	X
Alarms			X		
Guards			X	X	X
Policies & procedure	X	X	X		X

The above conceptual framework if practically adopted ensures that security management activities are embedded in selected functional activities as indicated by the X markings. This enhances security management as it reflects a proactive approach to security-related problems. The framework supports the earlier observation that value chain and functional analysis may be suitable platforms for implementing ISS. Security controls are an additional method of ensuring

that security risk management is present in most functions of the company. Koleter (2010: 48) articulates types of controls applicable to integration which include complementary controls which are used in conjunction with other activities, detective controls designed to uncover undesirable conduct, and preventive controls meant to deter the occurrence of unintended eventualities. Directive controls provide guidance to help the company increase the probability of achieving desirable outcomes while corrective controls are meant to correct deviations from expectations. Security controls can be included in company standard operating procedures as a form of integration.

3.7.8 Methods of integrating security systems

The means by which security systems are integrated include physical security integration, procedural integration and technological integration. Physical integration is attained through a combination of security measures which means that the measures being integrated should be interconnected (Vellani, 2011: 206). Procedural integration is achieved by putting in place policies, procedures and internal controls to act as oversight mechanisms for integrated physical security systems. The most common form of security systems integration is through ICTs. Examples of reviewed technological components include alarm processing and transmission technology, electronic relay connections, two-way radio communication systems and electronic transmission options such as internet protocol (IP) or voice over internet protocol (VOIP). Other support elements are control panels which provide visibility to staff monitoring the system, access card technologies such as card readers and biometric identification, and software technologies which provide the platform for operating the integrated security system. Other common technologies used include intercom systems, fire detection and response systems, turnstiles, locking devices, motion sensors and electronic article surveillance depending on the situation.

3.8 PROJECT MANAGEMENT ASPECTS

There are various methods and approaches for implementing ISS. SSI requires a project management stakeholder approach. Such an approach ensures that there are various players involved in the implementation. The key players in the implementation of ISS can include

company's top management, security management professionals, information technology specialists and procurement. System designers (from the field of electronic engineering), system manufacturers, system suppliers, and system installers/maintainers are other players of the programme. Others of importance as well are system integrators, equipment vendors, and system operators or users. In some large programmes, there can be a need of a project manager.

According to Bill (2004: 82), the composition of a team can involve people from within and outside the organisation. The process or method to be followed in implementing ISS may differ from company to company. Rogers (2011: 13-19) recommends a project management approach with steps which include identification of security needs, setting up of project team or committee, specification of the security measures or systems, planning for the security project, and implementation of the project. On the other hand, Caputo (2010: 251) provides the five stages of project management as initiating the project, planning to execute the project, implementing the project, monitoring and control, and closing the project. In regard to this, Colombo (1999: 124) articulates the stages for implementing ISS as to include the design stage of the intended security system, programming through electronic elements, and installation of the chosen security system. This is then followed by monitoring the functioning of the installed system, full scale operation of the system, provision of administrative functions, maintenance and servicing of the system, changes and upgrades to the system if necessary. However, the project management approach is not specific to security management projects but it provides a guideline to formulating specific project plans.

Each company, depending on its commitments, may choose a convenient way of implementing ISS. Implementation may take long to complete depending on the urgency, availability of funding and the requisite skills. It is important that appropriate systems which are desirable and feasible in the circumstances be identified for implementation to avoid post-implementation disappointment such as system malfunction or failure to solve security problems.

3.9 CHALLENGES OF SECURITY SYSTEMS INTEGRATION

Implementing ISS is not without problems. Since it involves bringing together disparate components and functions, it is likely to arouse conflict. Some of the challenges as observed by Dave (2007: 93) include failure to fully understand the limitations of the existing security system design. An ISS based on an internet protocol without boundaries brings in potential risks of

information technology such as hacking, denial of service and viruses. There is also potential of a cultural change as ICT and security professionals combine their functions and responsibilities. Another challenge is that some ISS may utilise advanced information technology which some members in the company may find difficult to operate. This cultural shift may cause resistance to change. Identifying skilled project team members like the system designer and integrator can be a problem as such skills may not be readily available. The integration and interdependence of functional systems in the company can be difficult to co-ordinate. Another problem observed by Colombo (1999: 121) is the high level technical and programming skills required to integrate multiple sub-systems into one seamless control and automated response system. Implementing ISS can have cost implications particularly in design, installation and consultancy since high level skills may be required. An ISS once implemented can be difficult to change in the future when upgrade is needed as observed by Colombo (1999: 121). Another challenge can be that of choosing the correct integration platform for a security system. The continuous operation of an ISS may face constraints such as power outages, system breakdown, maintenance downtime and inability to operate complex ISS. Vellani (2007: 212) provides a list of system costs which may be prohibitive.

3.10 BENEFITS OF INTEGRATED SECURITY SYSTEMS

There are some benefits associated with implementation of ISS despite the challenges mentioned above. Among the benefits is the perception that centralised surveillance is less costly and more effective. ISS can be more effective than stand-alone security measures because they are not entirely dependent on human conduct, which is subjective and may be easily influenced and can therefore be unreliable. ISS information is readily available because it is timeously recorded and can be easily retrieved. Integration of security systems may improve morale of the security staff and the general outlook of the facility. With improved security, security-related losses are reduced and this may add to shareholder value. ISS are both proactive and reactive and moreover, they increase prevention, delay and detection in a security management programme.

3.11 CRITICAL SUCCESS FACTORS

The factors that may be critical for the successful implementation of ISS include top management support, organisation wide communication and buy-in. There should be clearly established objectives based on predetermined problems. Project team members should have diverse skills and experience in systems integration. Effective monitoring and control ensures that limitations of the system are identified and corrective measures taken. A change management programme may be essential to mitigate effects of potential resistance to the new system as people prefer to stick to previous systems. In addition, there should be an adequate budget to ensure availability of resources requirements are.

3.12 CONCLUSION

This chapter revealed discussions on the implementation of ISS through a review of literature from various sources. The sources included books, research reports, journals and internet sources. The purpose of the review was to gain an insightful understanding of the research problem. Aspects in the review included the theory of integration, characterisation or identification of critical assets in the context of an industrial site and security risk assessment. Security risk assessment covered identification of threat sources, risk analysis, security survey and vulnerability assessment. There was also a review of industrial security measures which included physical security measures, human security, policies and procedures, technological security measures, crime prevention through environmental design and situational crime prevention methods. The review utilised two management models in the form of the McKinsey 7-S Framework and the Rogers Security Risk Management Model on how these models could contribute to the implementation of ISS. The scope of integration was another aspect covered by the review which included types of integration methods. Lastly, the review covered potential challenges and benefits of ISS. The information obtained through the literature review assisted in the site visits, interviews and the survey. This information was compared and triangulated with information obtained from field work to come up with findings and recommendations.

CHAPTER 4

FINDINGS: AN ANALYSIS AND INTERPRETATION OF THE RESEARCH DATA

4.1 INTRODUCTION

This chapter provides a presentation, analysis and interpretation of the information collected during the study. The information was obtained using site visits, interviews and questionnaires. Therefore, the presentation follows the format of site visits, interviews and questionnaires. Comparisons of information are made in the process.

4.2 BIOGRAPHICAL INFORMATION

Biographical information follows:

4.2.1 Site visits

The mixture of sites visited provided the researcher with a wide view of the security measures deployed at the sites. Table 4.1 below indicates the distribution of sites visited.

Table 4.1: Distribution of sites visited in the industrial areas

Area	Sites visited	Percent	Site types
Workington	3	27.3	1 Industrial, 1 Security 1 Security systems supplier
Graniteside	3	27.3	1 Industrial, 2 Commercial
Willowvale	2	18.2	2 Industrial
Msasa	1	9.1	1 Industrial

Southerton	1	9.1	1 Industrial
Outside Industry	1	9.1	1 Commercial bank
Total	**11**	**100**	**As above**

From 11 (100%) sites that the researcher visited, 3 (27.3%) of the sites visited were from Workington; 3 (27.3%) of the sites visited were from Graniteside; 2 (18.2%) of the sites visited were from Willowvale; 1 (9.1%) of the sites visited were from Msasa; 1 (9.1%) of the sites visited were from Southerton; and 1 (9.1%) of the sites visited were from outside industry.

4.2.2 Interviews

A total of 30 respondents were interviewed using the interview guide. The table below shows the characteristics of the interviewees.

Table 4.2 Characteristics of respondents in the interview sample

VARIABLE	CATEGORY	f	%
Gender	Male	26	90
	Female	4	10
	Total	30	100%
Age	25 – 35	2	6.66
	36 – 45	6	20.0
	46 – 55	11	36.66
	56 years and older	11	36.66
	Total	30	100%

Position	CEO	1	3.34
	Manager	24	80.0
	Officer	5	16.66
	Total	30	100%
Qualifications	Certificate	5	16.66
	Diploma	7	23.34
	Degree	18	60.0
	Total	30	100%
Security experience	Yes	29	96.66
	No	1	3.34
	Total	30	100%
Years' experience	5 years or fewer	2	6.66
	6 to 10 years	9	30.0
	11 to 20 years	18	60.0
	No experience	1	3.34
	Total	30	100%
Location	Workington	6	20.0
	Southerton	5	16.66
	Willowvale	5	16.66
	Graniteside	5	16.66
	Msasa	4	13.34
	Outside industry	5	16.66

Total	30	100

From 30 (100%) participants, 26 (90%) of the participants were males while 4 (10%) were females. Security industry by its nature has always been dominated by males. Though women are underrepresented, they slowly make their way into the security industry.

In terms of the ages of the participants, 2(6.7%) were between the ages 25 35; 6 (20%) were between the ages 36 – 45; 11 (36.7%) were between the ages 46 – 55; and 11 (36.7%) were 56 years and older.

The participants occupied different positions as follows: Those occupying Chief Executive Officer positions were 1 (3.3%); those occupying Manager positions were 24 (80%); and those occupying Officer positions were 5 (16.7).

The qualifications of the participants were as follows: those with Certificate were 5 (16.7%); those with Diploma were 7 (23.3%); and those with Degree were 18 (60%).

From 30 (100%) participants, 29 (96.7%) had security experience and 1 (3.3) participants had no security experience.

In terms of the years of experience of the participants, 2 (6.7%) of the participants had 5 years or fewer years of experience; 9 (30%) had 6 to 10 years of experience; 18 (60%) of the participants had 11 to 20 years of experience; and 1 (3.3%) of the participants had no experience.

In terms of the location of the participants, 6 (20%) of the participants were from Workington; 5 (16.7%) of the participants were from Southerton; 5 (16.7%) were from Willowvale; 5 (16.7%) were from Graniteside; 4 (13.3%) were from Msasa; and 5 (16.7) were from outside the industry.

4.2.3 Survey questionnaires

Table 4.3 Characteristics of respondents in the survey sample

VARIABLE	CATEGORY	f	%
Gender	Male	92	90.2
	Female	10	9.8
	Total	102	100%
Age	20 – 25	7	6.9
	26 – 35	24	23.5
	36 – 45	31	30.4
	46 – 55	28	27.5
	56 years and older	12	11.8
	Total	102	100%
Position	Owner	4	3.9
	CEO	9	8.8
	Manager	43	42.2
	Officer	36	35.3
	Other	10	9.8
	Total	102	100%
Qualifications	Certificate	4	14.7
	Diploma	39	38.2
	Degree	40	39.2
	Post graduate degree	8	7.8

	Total	91	100%
Security experience	Yes	78	76.5
	No	24	23.5
	Total	102	100%
Years' experience	5 years or fewer	14	13.7
	6 to 10 years	27	26.5
	11 to 20 years	34	33.5
	Above 20 years	4	3.9
	No experience	23	22.5
	Total	102	100%
Location	Workington industrial area	11	10.8
	Southerton industrial area	21	31.4
	Willowvale industrial area	20	19.6
	Graniteside industrial area	12	11.8
	Msasa industrial area	16	15.7
	Outside industry in Harare	22	21.6
	Total	102	100%
Organisation type	Industrial	36	35.3
	Commercial	44	43.1
	Security Company	12	11.8
	Security system supply	8	7.8
	Other	2	2.0
	Total	102	100%

From 102 (100%) of the respondents, 92 (90.2%) of the respondents were males; and 10 (9.8%) were females.

In terms of the ages of the respondents, 7 (6.9%) of the respondents were between 20 – 25 years; 24 (23.5%) of the respondents were between 26 -35 years; 31 (30.4%) of the respondents were between 36 – 45 years; 28 (27.5%) of the respondents were between 46 – 55 years; and 12 (11.8%) of the respondents were 56 years and older.

The positions of the respondents were as follows: 4 (3.9%) were Owners; 9 (8.8%) were CEO; 43 (42.2%) of the respondents were Managers; 36 (35.3%) of the respondents were Officers; and 10 (9.8%) of the respondents fell under other categories.

In terms of the qualifications of the respondents the following can be observed: 4 (14.7%) of the respondents had Certificate; 39 (38.2%) of the respondents had Diploma; 40 (39.2%) of the respondents had Degree; and 8 (7.8%) of the respondents had Postgraduate degree.

The security experiences of the respondents were as follows: 78 (76.5%) of the respondents had security experience; and 20 (23.5%) of the respondents had no security experience.

In terms of the years of experience of the respondents, 14 (13.7%) were 5 years or fewer; 27 (26.5%) of the respondents were 6 – 10 years; 34 (33.5%) of the respondents were 11 – 20 years; 4 (3.9%) of the respondents were above 20 years of experience; and 23 (22.5%) of the respondents had no experience.

The location of the respondents differed as follows: 11 (10.8%) of the respondents were from Workington industrial area; 21 (31.4%) of the respondents were from Southern industrial area; 20 (19.6%) of the respondents were from Willowvale industrial area; 12 (11.8%) of the respondents were from Graniteside industrial area; 16 (15.7%) of the respondents were from Msasa industrial area; and 22 (21.6%) of the respondents were from Outside industry in Harare.

In terms of the organisation types, 36 (35.3%) of the respondents were from industrial side; 44 (43.1%) of the respondents were from Commercial side; 12 (11.8%) of the respondents were

from Security Companies; 8 (7.8%) of the respondents were from Security system supply; and 2 (2%) were from other categories.

4.2.4 Discussion

In terms of the site visits that were conducted, the study was confined to the Harare industrial areas of Workington, Willowvale, Southerton, Graniteside, and Msasa. Among the sites visited was one commercial bank outside the industrial area but within Harare. The commercial bank exhibited implementation of integrated security systems which proved insightful to the study.

As can be seen from the above table 4.3, most of the respondents 92 (90.2%) were male while 10 (9.8%) were female. A similar situation was also observed in the interviews where the majority was also male. This further reinforces the point that the security function is male dominated.
The statistics indicate that the majority of the respondents are in the 36-45 age group and very few in the 20-25 age categories. This resembles that the security function is preferably for mature people as also shown in the interviews.

In terms of positions held by the respondents, the statistics indicate that the majority of the respondents were either managers or officers. As regards the qualifications of the respondents, most of them were degree holders. These statistics point to the fact that the majority of the respondents were able to understand and respond meaningfully to the questionnaire. Research participants experience showed that 78 (76.5%) of the respondents had security related experience while 24 (23.5%) did not have some experience in security practice. The fact that the majority of them at 63.7% had more than 6 years' experience in security practice supports the view that a larger percentage of experienced respondents participated in the study.

Turning to location demographics for the respondents, the statistics indicate that the majority were from the five industrial areas while only 22 were from outside industry but within Harare. Some of those from outside industrial areas were from organisations which supply and install integrated security systems. The statistics show that respondents had sufficient background of security related issues in the area of study.

4.3 SECURITY SYSTEMS INTEGRATION

The different data gathering methods were followed to answer the following research questions as highlighted in Chapter 1. This subsection presents information from the site visits, interviews and questionnaires in terms of the research questions. Each research question is accompanied by a research objective. The presentation is in the form of discussions backed by descriptive statistics in some instances.

4.3.1 Security risks confronting organisations in Harare

The following question was asked in order to uncover the risks facing the organisations in Harare:

Research question 1: What are the major security risks confronting organisations in the Harare industrial area?
This question sought to answer the following research objective: Determine the security risk assessment aspects for the Harare industrial sector in relation to the implementation of integrated security systems.

This question was asked because there are different risks that organisations can be faced with, depending on the product or service that they render.

In order to fully address the research question, the study sought to include a security risk assessment process which included identification of assets, threat sources and the security risks so as to gain a broader understanding of the problem.

In addressing this research question, the site visits revealed that the assets were infrastructure, people, products, materials, revenue and movable assets. The researcher deduced potential threat sources as outsiders, employees and crime syndicates. The major security risks as perceived by the researcher during the site visits are theft, burglary and fire. During the on-site orientations as

provided by Rogers (2011: 86-97), staff that accompanied the researcher also alluded to the same security risks.

On the other hand, the interviews revealed that in relation to assets vulnerable to security risks the majority of interviewees (56.66%) indicated:

- infrastructure;
- products;
- materials; and
- revenue as critical for protection.

Most of the respondents (66.66%) viewed infrastructure as the most critical asset requiring security attention and Vellani (2007:13) also captures infrastructure as the fundamental assets of an organisation needed for it to sustain its operations. In terms of the threat sources, the majority of the interviewees (90%) indicated outsiders, employees and crime syndicates as the major threats to the assets. With regards to security risks, 90% said theft was the major security risk while 10% thought it was not. It was found out that 70% considered burglary as another major risk. On aggregate ranking, the majority of the participants perceived theft, burglary, fraud, robbery and fire as the main security risks confronting organisations in the Harare industrial sector. Of the 30 interviewees, 66.66% thought fraud was another security risk for consideration in security systems integration. Other risks which received considerable recognition were robbery and fire at 40% and 37% respectively. The study used qualitative risk rating as asserted to by the Microsoft Security Risk Management Guide (2006:57-58) and alluded to by Vellani (2007:112-113) in coming up with a security risk rating as per interview responses. The table below shows the risk ranking.

Table 4.4: Security risk ranking from interviews

Ranking	Security Risk	Risk Rating
1	Theft	High
2	Burglary	High

3	Fraud	High
4	Robbery	Medium
5	Fire	Medium

The above table shows that theft is the major security risk followed by burglary. Fire was included as both a security and safety risk while the others are purely security crime risks. The reason why theft is the major security risk may be attributed to the fact that it is the kind of risk that can be caused by the members of staff in the organisation, the people doing business with the organisation while visiting the organisation or external people who may not be properly controlled while in the premises. It is not surprising that burglary is the second major security risk because when people break into organisations they do so with intention to commit other crimes such as theft. Robbery and fire were pointed out to be the least security risks.

In terms of the security risks confronting organisations, the survey questionnaires investigated this in the context of assets, threat sources and security risks and gave the following results from Section B of the questionnaire which contained Questions 9, 10 and 11. The statistics in the table below were derived from Question 9 of the questionnaire on asset identification.

Table 4.5: Q9 Relationship of assets to implementation of ISS			
Q No	Asset type	Frequency	% in Agreement to some extent and above
Q9a	Infrastructure	92	90.2
Q9b	People	89	87.3
Q9c	Products & materials	100	100
Q9d	Revenue	98	96.1
Q9e	Movable assets	90	88.2
Composite percentage frequency of 60% and above			97.1

From the above table, the calculated composite frequency is 97.1% which shows that the respondents did agree from some extent to a very large extent that the assets contained in the table require protection in the Harare industrial sector.

Question 10 was related to the research question of security problems that confront organisations in the industrial sector**.** The table below shows statistics of those in agreement at 60% and above.

Table 4.6: Q10 Relationship of threat sources to implementation of IS			
Q No	Threat source	Frequency	% in Agreement to some extent and above
Q10a	Outsiders	96	94.1
Q10b	Employees	93	91.2
Q10c	Crime syndicates	93	91.2
Q10d	Power outage	88	86.3
Q10e	Negligence	55	53.9
Composite percentage frequency of 60% and above			93.1

In the above table, the major threat sources were identified as outsiders, employees and crime syndicates with more than 90%. The calculated composite frequency of those in agreement to some extent and above is 93.1%. Power outage and negligence have percentages below the composite frequency and are therefore considered not serious threat sources in relation to implementation of integrated security systems.

With regard to security risks, the statistics of those in agreement to some extent and above is shown in Table 4.7 below.

Table 4.7: Q11 Security risks to be considered in the implementation of ISS			
Q No	Security risk	Frequency	% in Agreement to some extent and above
Q11a	Theft	100	98
Q11b	Burglary	96	95.2
Q11c	Fraud	93	91.2
Q11d	Fire	93	91.2
Q11e	Robbery	88	86.3
Q11f	Corruption	69	67.6
Q11g	Violence related	31	30.4
Composite percentage frequency of 60% and above			85.3

According to the above statistics, the most highly rated security risks are theft, burglary, fraud, and fire whose percentages are above 90%. Corruption and violence-related crime have percentages below the calculated composite percentage of 85.3 and are therefore regarded as not impacted by implementation of integrated security systems.

The study concluded that the results from three different methods had similarities to some extent. In terms of assets, site visits and interviews indicated that infrastructure was the most critical while survey respondents were most concerned with products and materials due to theft consequences.

From the three methods, the major security risks were identified as theft, burglary, fraud, robbery and fire. Fraud was indicated in interviews and questionnaires as an indirect form of theft. In fact, the outcome of burglary, fraud and robbery is theft and they are considered as property

crimes. While interviews did not indicate corruption as a potential risk, questionnaires did to a certain extent raise it as a concern.

The research question was to a large extent successfully answered because the major security risks in relation to the assets and threat sources were highlighted. The research question and the results helped the research to develop further investigations into the implementation of integrated security systems. However, a deeper understanding could have been obtained with more site visits and interviews.

4.3.2 Implementation of integrated security systems

The following question was asked in order to uncover implementation of integrated security systems:

Research question 2: What is the extent of implementation of integrated security systems in the industrial sector of Harare?

This question also sought to answer the research objective: Assess critically the extent of implementation of integrated security systems in the Harare industrial sector.

In addressing this question, the site visits revealed that 55% did not have integrated security systems but had stand-alone security measures which were in close proximity. To fully address this question, the study sought to first identify the existing security measures. The most commonly observed security measure was physical security (91%) used in combination with security guards (82%). A common security application was found to be access control meant to limit access to persons and vehicles with a legitimate business purpose to enter the premises (Dave 2007: 58). Some sites (54.54%) had electronic access control.

CCTV was observed at six (55%) of the sites visited. With respect to alarms, it was established out that they were used in perimeter protection and burglar prevention at four (36.36%) of the premises. A major weakness at eight of the facilities was the absence of written security policies and procedures. While there were practices to be followed for physical access control, these were not in written form in about 73% of the sites.

Turning to existing scope of integration the visits revealed that it was in the form of close-proximity security systems which included access control, security personnel, CCTV, alarms and radio communication. Close-proximity security systems are not linked with information communication technology which is a key component of security systems integration. In general, the study noted that most sites 54.54% did not have integrated security systems, while some (27.27%) were partly integrated and only a few (18.18%) resembled some form of integration. At sites, 45.5% where some form of integration was observed it consisted of access control, CCTV, alarms and ICT backed by guards, radio communication and procedures.

The researcher also observed Crime Prevention Through Environmental Design (CPTED) during the site visits as complementary to security systems integration. This is because Cappers (2008: 56) determines that the theory of CPTED exhibits the deliberate design which is a useful approach in managing security at industrial facilities. The most commonly used measures of CPTED observed included pathways, entrance points, car parks, lighting, signage, wearing of uniforms by staff members. This was the case in about 63.63% of the sites that were visited. The researcher observed that the inclusion of CPTED measures with other security measures can further enhance the effectiveness of the security programme at industrial facilities by reducing predisposing and precipitating factors (Rogers, 2011:26). Most facilities exhibited the presence of CPTED but with potential for improvement. Observed weaknesses in CPTED at most facilities 81.81% included lack of care and maintenance with indications of tall grass, trees, poor lighting, dilapidated buildings and lack of signage. Therefore, the study contends that security at industrial facilities can be improved by inclusion of CPTED.

On the other hand, interviews revealed that the security measures in use were physical security (90%), guards (90%), electronic access control (63.33%), CCTV (46.66) and alarms (30%). The majority (60%) of the participants indicated that the systems were not integrated.

In terms of the questionnaires, there was no specific question which covered the extent of implementation of integrated security systems. Therefore, there were no results from the survey questionnaires connected to this research question.

By and large, the results from the observations and interviews indicated that the security systems in the Harare industrial sector were not really integrated but were mainly stand-alone security systems. This question was reasonably answered through the site visits and the interviews though much more information could have been obtained had the questionnaire covered this aspect. Furthermore, the researcher was not exposed to more site visits due to limitation in authorised permission letters.

4.3.3 Reasons for implementing integrated security systems

In order to uncover the reason for implementing the integrated security systems the following question was asked:

Research question 3: Why is it necessary to implement integrated security systems?

This question also sought to answer the research objective: Explore the main reasons for implementing integrated security systems in the Harare industrial sector.

In addressing this question, the research sought to establish the problems or weaknesses which might necessitate the implementation of integrated security systems.

The site visits revealed the following as vulnerable points which require integrated security systems at industrial facilities:

- Receiving, warehousing and dispatch points (63.63%);
- Plant and machinery where production or processing takes place (63.63%);
- Access control points comprising of entry and exit (8 of the sites);
- Sales offices with cash handling facilities (81.81%); and
- Office buildings which house various company functions (8 of the sites).

The security risks perceived to affect these points include unauthorised entry, burglary, theft, robbery, and fire among others.

On the other hand, the interviews revealed that the majority of the respondents (93.33%) were of the view that security incidents, particularly theft, were on the increase and difficult to detect hence the need for security systems integration. Another reason provided was that of increasing use of security technology as mentioned by 24 interviewees. A common perception among participants was that security risks are becoming more complex to be handled by stand-alone security measures. The majority of interviewees (86.66%) said that deployment of security guards was more costly and ineffective.

The questionnaires had no aspect on the reasons for the implementation of integrated security systems. However from the responses given by the respondents on the other aspects in the questionnaire it was deduced that the implementation of integrated security systems was much supported.

4.3.4 Scope of integrating security measures and systems

The researcher asked the following research question in order to uncover the scope of integrating security measures and systems.

Research question 4: Which security measures and systems need to be integrated?

This question also sought to answer the research objective: Recommend security measures for inclusion in an integrated security system in the Harare industrial sector.

This question was mainly investigated based on the desired integration scope. In addressing this question, the site visits (72.72%) revealed that the security systems with potential for integration were access control, intercom, CCTV, alarms, ICT, radio communication and fire systems.

On the other hand, the interviews revealed that participants at 43.33% preferred EAC, guards, alarms, CCTV, fire system, and procedures. Only 23.3% advocated for full integration which includes heat, ventilation and other functional management systems. The full responses reduced to statistical format are shown in Table 4.8 below:-

Table 4.8 Preferred security systems integration scope from interviews

Ranking	Integration Scope	Percent of Responses
1	EAC, guards, alarms, CCTV, fire system, policies and procedures.	43.3
2	Full integration which includes the above scope and functional integration	23.3
3	EAC, guards, alarms, CCTV, policies and procedures	20
4	EAC, guards, alarms, policies and procedures	13.3
Total		100

From the above table, it can be seen that the preference from a security management point of view was on type 1 scope of integration. This scope of integration is related to the security risks identified in Table 4.4 and 4.7 above. For example, policies and procedures include the prevention and detection of fraudulent activities over and above the management of other security risks identified.

The survey questionnaires gave the following frequencies of those in agreement to some extent (60%) and above in connection with the integration scope as shown in Table 4.9 below:-

Table 4.9 Q 12 Security measures for implementation in ISS as per survey			
Q No	Security measure		% in Agreement to some extent and above
Q12a	Physical security	96	95.1
Q12b	Security personnel	96	95.1
Q12c	EAC	101	99
Q12d	Alarms	102	100
Q12e	CCTV	100	98
Q12f	ICTs	101	100
Q12g	Policies procedures	101	99
Composite percentage frequency of 60% and above			100

As can be deduced from the above table, the calculated composite frequency percentage which is 100% indicate that most respondents agreed to a very large extent on the importance of security measures to be included the implementation of integrated security systems. However, physical security and security personnel are below the mean frequency of 100%.

In addition, the study included the aspect of functional integration with Security as complementary to security systems integration. In addressing this research question, the site visits (54.54%) revealed that functional integration was difficult to establish. However, notable indications of functional integration were observed at the receiving and dispatch points where there was presence of Security, Procurement, Distribution and procedural functions just to mention a few.

On the aspect of functional integration, the interviews revealed that about half of the interviewees at 56.66% were of the view that Security should be linked the IT, Human Resources and Finance functions while 10% submitted that integration was only possible between Security and IT functions. Only 26.66% believed that all company functions should be integrated while 6.6% were of the view that functional integration was not possible.

The survey questionnaires gave the following results from Question 13 as shown in Table 4.10 below:-

Table 4.10: Q 13 Organisation functions to be considered in the implementation of ISS			
Q No	Function		% in Agreement to some extent and above
Q13a	IT	98	96.1
Q13b	Human Resources	88	86.3
Q13c	Fin. And Admin	95	93.1
Q13d	Procurement	69	67.6
Q13e	Operations	91	89.2
Q13f	Marketing & Dist.	81	79.4
Q13g	Audit & Risk	79	77.5
Composite percentage frequency of 60% and above			98.0

Table 4.10 shows that IT, Finance and Admin, Operations and Human Resources have percentages above 80% but below the composite frequency of 98% indicating that respondents preferred to a large extent their integration with Security. Procurement, Marketing and Distribution and Audit and Risk have lower percentage values compared to the others but good enough for integration with Security. Interview and survey outcomes have similarities with regards to functional integration.

The integration scope derived from the three sources includes access control, CCTV, alarms, and ICT which includes intercoms. The three different sources supported each other in terms of integration scope. Administrative aspects of integration include personnel, policies, procedures and functional integration. What came out is that on the one side there is the actual technological

integration of security measures and technology and other hand, there if there is a need for administrative functions to implement the integrated systems.

It can be safely concluded that the aspects of integration were covered satisfactorily by the three methods.

4.3.5 Technological impediments

In order to find out if there are some technological impediments to implementation of integrated security systems the following question was asked:

Research question 5: Are there any technological impediments to implementation of integrated security systems?

This question also sought to answer the research objective: Advance the Information Communication Technology aspects suitable in the implementation of integrated security systems.

In addressing this research question, the study sought to identify the information communication technology aspects from which the impediments could be derived. The site visits 81.81% revealed that integrated security systems were mostly on local area network (LAN rather than wide area network (WAN). A few (18.19%) that were on WAN were provided by Security Companies which monitored them from dedicated monitoring sites. The technological problems observed included malfunctioning security gadgets of, disrupted internet connectivity for systems on WAN.

On the other hand, the interviews revealed that the preferred ICT aspects were twisted pair cabling for systems on LAN and fibre optic for WAN connected security systems bandwidth could be insufficient resulting in poor coverage. Participants (86.66) raised the concern of finding the right quality technology requirements. Interviews with security system suppliers (100%) revealed that the most preferred transmission modes are fibre optic, wireless, WAN, LAN and using an integrated services digital network (ISDN) or ADSL). However, some of these transmission modes were not accessible or when available were very costly. The choice of whether to adopt a WAN or LAN was said to depend on preference and financial capacity. The

study established from interviews with security system suppliers (100%) that WAN is more expensive than LAN because it operates over an internet protocol and has options for computer and off-site monitoring. It was also established that remote monitoring using internet protocols including voice over internet protocols (VOIP) but the services were costly to implement.

The study also found out that WAN is more exposed to internet risks and problems such as hacking, virus attacks and bandwidth limitations as confirmed by 100% of security system suppliers. Twisted pair cabling was said not to be effective in signal transmission due to poor quality output. Public telephone subscriber lines were being replaced by mobile phones and were therefore regarded as somewhat irrelevant. It was also pointed out that wireless transmission license was difficult to obtain because of legislative requirements. While mobile phones were ubiquitous, it was established that the cost to connect to integrated security systems was very high.

The survey questionnaires gave the following results as pointed out in Table 4.11 below in terms of ICT aspects which could be challenging in the implementation of integrated security systems.

Table 4.11: Q 14 ICT aspects for inclusion in the implementation of ISS			
Q No	IT aspect	Frequency	% in Agreement to some extent and above
Q14a	Twisted pair cable	52	51
Q14b	Fibre optic	99	97.1
Q14c	Wireless	98	96.1
Q14d	LAN	95	93.1
Q14e	WAN	95	93.1
Q14f	Extranet	91	89.2
Q14g	Public telephone	47	46.1
Q14h	ISDN	94	92.2
Q14i	ADSL	85	83.3
Composite percentage frequency of 60% and above			94.1

The most preferred transmission modes are fibre optic, wireless, WAN and LAN using an ISDN which have frequencies more than 90%. The calculated composite frequency is 94.1%. Twisted pair cabling and public telephone subscriber lines did not receive recognition as shown in lesser percentage frequencies. From the above table, it was deduced that twisted pair cabling and public telephone subscriber lines were not preferred in the implementation of integrated security systems.

Similarities of information from the three sources are in site visits and observations. Information from the survey questionnaire was about the preferred modes of transmission which did not specifically ask respondents to evaluate the potential impediments.

The research question was answered to some extent because the ICT aspects and related problems were evaluated. However, it was not fully answered because there are many aspects of technology under security systems integration. Hardware and software technological aspects were not covered in this study because the study focused on general implementation issues. However, the information obtained was sufficient enough for identifying the required ICT aspects in security systems integration.

4.3.6 Key players in implementing integrated security systems

The following question was asked in order to find out about key players in implementing ISS:

Research question 6: Who are the key players in the implementation of integrated security systems?

This question also sought to answer the research objective: Propose the key players to be included in the implementation of integrated security systems.

In addressing this research question, the site visits (45%) revealed that the key players were security practitioners, ICT practitioners, security system suppliers and security service providers. The site visits (45%) revealed that the critical ones were the security practitioners, top management, and information communication technology and security system suppliers.

On the other hand, the interviews revealed that the majority of participants at 90% indicated the key players in the integration process as; Security, IT, systems designer, installer and security service provider or a project team. Almost all the respondents were of the conviction that the Security Manager should be the lead person (champion) in the implementation of integrated security systems.

Turning to the survey questionnaires, the following results were achieved in terms of the key players in implementation of integrated security systems as outlined in Table 4.12 below:-

Table 4.12: Q 15 Key players in the implementation of ISS			
Q No	Player	Frequency	% in Agreement to some extent and above
Q15a	Security practitioner	100	98
Q15b	Top management	97	95.1
Q15c	System supplier	97	95.1
Q15d	System installer	100	98
Q15e	IT specialist	96	94.1
Q15f	System operator	99	97.1
Q15g	Security provider	89	87.3
Q15h	Project team	80	78.4
Composite percentage frequency of 60% and above			100

From the above table, the key players can be ranked as Security practitioner (98%), System installer (98), system operator (97.1), top management (95.1%), and system supplier (95.1%) IT specialist (94.1%) security service provider (87.3%) and project team (78/4%). All the key players with more than 80% are highly regarded in the implementation of ISS. The composite frequency to 100% indicates total agreement among the respondents.

There are some similarities from the three different methods although the survey has a bigger contribution. The observations provide a summary of the key players compared to the other two methods which are broader in scope.

The research question was considerably answered because the key players were established. However, members of the project team within an industrial set-up were not identified but are assumed to comprise the other key players who could be determined by scope of the project.

4.3.7 Carrying out implementation of ISS

The following question was asked in order to uncover how implementation of ISS is carried out:

Research question 7: How is the implementation of integrated security systems carried out?

This question also sought to answer the research objective: Formulate a best practice process to be followed in the implementation of integrated security systems.

In addressing this research question, the site visits did not include the implementation process because it was unobservable but assisted the researcher in developing a background of the perceived process to be investigated during interviews and questions. Such background information included security risk assessment and the integration scope. Therefore, this related knowledge showed that a process for implementing integrated security systems was necessary.

On the other hand, the interviews revealed that most participants (93.33%) had difficulties in outlining the stages of the process. However, the few (6.66%) who managed to give their views were in agreement that a process should be followed. Some of the suggested stages were security survey, proposal, budgeting, procurement, installation, testing, training, operationalization, review and upgrade. Among these, almost all respondents (100%) were convinced that security survey was to be the first step in the process. In terms of the application of return-on-investment (ROI) as part of an appraisal process for implementation the majority of interviewees (93.33%) had little knowledge about the aspect. The fact that the majority of participants had little knowledge on the integration process is a further indicator of lack of security systems integration in the Harare industrial sector. The study assumed that ROI is not used in practice as a decision making tool for security systems implementation in the majority of cases.

Turning to the survey questionnaire, it brought out the following results derived from Question 16 as outlined in Table 4.13 below:-

Table 4.13: Q 16 Process stages involved in the implementation of ISS			
Q No	Aspect	Frequency	% in Agreement to some extent and above
Q16a	Security policy	100	98
Q16b	Security survey	102	100
Q16c	System design	100	98
Q16d	Procurement	93	91.2
Q16e	SLA	98	96.1
Q16f	Installation	101	99
Q16g	Training	102	100
Q16h	Operating	102	100
Q16i	Review & upgrade	102	100
Composite percentage frequency of 60% and above			100

The above table shows that security survey, training, operating, review and upgrade have 100 % frequencies. Installation, security policy and system design have frequencies less than the calculated composite frequency of 100%. Heally and Walsh (1971: 11) substantiate the stages of security system integration as to include; risk assessment, identification of security measures, system design, procurement, installation, development of operating procedures, training, operating and maintenance, review and expansion**.**

A comparison of the three methods shows that questionnaires contained substantive feedback information on the process compared to the site visits and interviews. Some of the implementation stages mentioned in the interviews were substantiated in the questionnaire and supported by literature study in subsection 3.9 of Chapter 3. However, the aspect of return-of-investment appraisal was not prominent in all the methods.

It can be safely concluded that sufficient information was obtained to answer the research question in terms of the research process. Several stages on implementation were brought out particularly in the questionnaires. However, the term “how” may include certain aspects not related to the process and therefore not investigated.

4.3.8 Requirements for implementing integrated security systems

The following question was intended to find out the requirements for implementing integrated security system:

Research question 8: What is required to implement integrated security systems?

This question also sought to answer the research objective: Evaluate the factors necessary for the successful implementation of integrated security systems.

In addressing this research question, the site visits (100%) discovered that the factors necessary for the successful implementation of integrated security systems included top management support, availability of resources and skills. Both conceptual and technical skills were identified as necessary.
On the other hand, the interviews revealed that more than 80 % were of the view that the following were important:

- The perceived security risks for which the system should be implemented;
- The desire by management to commit itself to the implementation of ISS;
- The availability of resources to undertake the project;
- The supposed purpose of the system;
- The feasibility of successfully implementing the system; and
- The availability of the necessary skills to acquire, install and operate the system.

Another aspect mentioned by a few participants (10%) which the research thought is important was buy-in from staff members for them to embrace integrated security systems.

The following Table 4.14 depicts correlation of the critical success factors as obtained from the statistically transformed interview responses.

Table 4.14: Pearson's correlation coefficient matrix derived from interviews

	Management Commitment	**Resources**	**System Purpose**	**Feasibility**	**Skills to Implement**
Security Risk	.028	.274	.154	.755	.078
Management commitment		.849	.379	.721	.679
Resources			.154	.755	.414
System Purpose				.812	.679
Feasibility					.038
Skills to Implement					1

The above matrix indicates that all the factors are correlated. The above factors were viewed as the main determinants of implementing integrated security systems and that they should be considered holistically because they are interrelated. The majority of interviewees (55.56) indicated security risk, top management support and resource availability as the most critical.

The survey questionnaires gave the following results derived from Question 17 of the survey which covered the aspect of critical success factors in the implementation of ISS. The statistics for scores of 60% and above are shown in the Table 4.15 below:-

Table 4.15: Q 17 Critical success factors in the implementation of ISS			
Q No	Factor	Frequency	% in Agreement to some extent and above
Q17a	System purpose	101	99
Q17b	Feasibility	98	96.1
Q17c	Resources	100	100
Q17d	Skills	98	96.1
Q17e	Top mgt. support	97	95.1
Composite percentage frequency of 60% and above			98.0

It can be seen from the above table that resources have the highest percentage followed by system purpose, feasibility, skills and top management support. The common view on factors critical for the successful implementation of ISS from both interviews and questionnaire data is that system purpose, availability of resources, top management commitment and skills to implement are the most important.

Findings from the three sources corroborated each other. There are similarities in almost all the factors that came out. From the study's perspective, the research question was successfully answered because the critical factors were brought out from all the three different sources.

4.3.9 Effectiveness of integrated security systems

The following question was intended to uncover the effectiveness of the integrated security systems:

Research question 9: How effective are integrated security systems in the prevention and detection of security incidents?

This question also sought to answer the research objective: Understand the effectiveness of integrated security systems in terms of the benefits of implementation.

To further enhance the analysis, the study sought to establish the effectiveness of existing security systems which relates to the ability of security systems to prevent and respond to threat sources (Vellani, 2007: 184). However, the research did not have a component on the actual impact of integrated security systems but the perceived benefits were assumed to translate to effectiveness.

In addressing this research question, the site visits (63.63%) revealed that there are several benefits to be derived from the implementation of integrated security systems. Some of them observed included improved security outlook, reduced security personnel deployments, detection of security incidents and rapid response.

In relation to interviews participants who viewed the existing security measures as possibly effective were at 63.3% and 23.3% were of the view that they were ineffective while the remaining 13.3% were unsure. Some participants noted that effectiveness of security measures may be difficult to measure. One Chief Executive Officer cautioned that the non-occurrence of security incidents did not necessarily mean that the security function was effective because some incidents may be undetected. All the interviewees (100%) were of the conviction that integrated security systems are more effective in the prevention and detection of security related incidents in the Harare industrial sector. About 27% were of the opinion that integrated security systems are less costly than stand-alone security measures while 73% believed they were costly due to implementation costs. Only 30 % indicated that they could be easy to monitor while 70 % said that they could be difficult to monitor.

The survey questionnaires gave the results on perceived benefits from responses under Question 18. There was no actual measurement of existing integrated security systems but the respondents were asked to provide their views on such perceived impact factors translating to benefits. According to the statistics obtained for the perceived benefits, the calculated composite frequency is 99%. The statistics are displayed in Table 4.16 below.

Table 4.16: Q 18 Perceived benefits for the implantation of ISS

Q No	Benefit	Frequency	% in Agreement to some extent and above
Q18a	Effectiveness	101	99
Q18b	Ease of monitoring	99	97.1
Q18c	Reduced personnel	95	93.1
Q18d	Improved outlook	99	97.1
Q18e	Improved records	100	98
Composite percentage frequency of 60% and above			99

The above table shows that all aspects had more than 80% frequencies from respondents who agreed to some extent and above. Improved effectiveness was the most highly rated benefit which equalled the composite frequency of 99% indicating a very strong reason for implementing integrated security systems. Reduced security personnel have the lowest percentage frequency. In support of this, Hernandez and Mazzon (2006: 72-88) outline the five attributes of the innovation transmission aspects as system advantage in comparison to others, compatibility, ease of operation, benefits, and improved outlook among others.

On the other hand, Heally and Walsh (1971: 10) corroborate that the advantages of security systems integration are improved protection and reduced costs which support the views of the respondents.

The results from the three methods agreed that there were benefits to be obtained from the implementation of integrated security systems. In summary, integrated security systems were viewed as cost-effective. Therefore, the research question was to some extent successfully answered since the benefits were sufficiently advanced. However, the research question could have been further explored by linking the effectiveness with the security risks.

4.3.10 Problems associated with implementation of integrated security system

The following question was aimed at unpacking the problems that are associated with the implementation of integrated security systems:

Research question10: What are the problems associated with the implementation of integrated systems?

This question also sought to answer the research objective: Examine the challenges associated with the implementation of integrated security systems.

In addressing this research question, nine of the sites revealed that the potential challenges could be in skills to implement and availability of resources. During the visits, it was observed that there is a wide range of security system hardware to be identified as suitable for inclusion in an integrated security system. Another observed challenge was the after effects of the integrated system in terms of effectiveness. In relation to this, some of the observed problems included system breakdown, power outage and insufficient bandwidth. Additionally, some of the staff manning the integrated systems did not have adequate skills to fully utilise the systems. However, it was found out that security system problems are mainly encountered particularly in the early stages of implementation and were resolved by learning and correcting mistakes.

On the other hand, the interviews revealed that with regards to challenges the following were identified as some of the most common problems:

- The majority of interviewees at slightly above half (56.66%) indicated lack of skills as a challenge;
- 46.66 % attributed lack of top management support as a hindrance;
- Only 23.33 % indicated the problem of linking different systems on platforms of existing systems;
- Others indicated identification of a quality security system vendor (40%);
- Potential breakdowns or malfunction of the system (86.66%);
- Some systems could be disrupted by jamming or hacking (13.33%);
- False alarms could lead to wastage of rapid response resources (50%);
- Poor recording capability of some CCTV systems (33.33); and
- High costs of bandwidth and unreliable network connectivity (60%).

The survey questionnaires gave the following results as derived from responses from Question 16 with views of more than 60% and above as outlined in Table 4.17 below:-

Table 4.17: Q 19 Perceived challenges in the implementation of ISS			
Q No	Challenge	Frequency	% in Agreement to some extent and above
Q19a	System breakdown	91	89.2
Q19b	Difficult to operate	71	69.6
Q19c	Incompatibility	52	51
Q19d	Power outage	83	81.4
Q19e	Sabotage	80	78.4
Composite percentage frequency of 60% and above			84.3

The above table shows that most respondents were worried about system breakdown with a percentage frequency 89.2% which is above the composite frequency of 84.3%. Other challenges which featured prominently were power outage and sabotage. To mitigate on power outages, the research noted that most facilities had stand-by generators as substitute for conventional electricity. Incompatibility has a low percentage of 51 which indicates that it is not a deterrent from implementing integrated security systems. Interviews also made similar observations regarding challenges.

Similarities obtained from the three sources are potential breakdowns, incompatibility with existing systems, power outage and sabotage. In particular, the information obtained from interviews was similar to that of the questionnaires.

The research question was successfully answered and the research objective achieved to some extent. Some of the challenges to be expected in the implementation of integrated security systems were identified.

4.3.11 Current state of security systems in the Harare industrial area

The following question was asked in order to outline the current status of the security systems in the Harare industrial area:

Research question 11: How do security practitioners perceive the current state of security systems integration in relation to the problem of connivance to theft within the Harare industrial sector?

This question also sought to answer the research objective: Identify potential solutions for inclusion in the implementation of integrated security systems to solve the problem of connivance to theft in the Harare industrial sector.

The current state of security systems integration was linked to a later developed research objective involving connivance to theft in the Harare industrial sector. This problem was highlighted in the pilot study and in the early stages of the interviews as a serious problem which required attention by the researcher; hence its inclusion in the study.

In addressing this research question, the site visits (81.81%) revealed that most industrial sites had receiving and dispatch points which were vulnerable to plain theft or through connivance. The points were mostly manned by security guards who were perceived to be ineffective for the problem of connivance and worse still they were considered as potential participants in connivance. Site visits resolved that possible effective solutions could be combination of functional integration, tight procedures and CCTV monitoring.

On the other hand, the interviews revealed that most participants were concerned with theft through connivance in the Harare industrial sector and that the current state of security systems integration did not address the problem. On potential solutions, the majority at about 90% indicated CCTV with counting software to scare, monitor and assist in detection. With regard to connivance at receiving and dispatch points, most participants also suggested the following measures as potential solutions:

- Rotation of staff members manning the receiving and dispatch points received a contribution of 25 % from the responses;
- Dedicated CCTV at the points received 22% contribution;

- Functional integration of activities at the points also had 22%;
- Conducting of spot checks had 19%; and
- Placement of undercover surveillance personnel at the points had 12 % contribution.

The total contribution of the above factors from interview responses amounted to 100%.

The survey questionnaires gave the results on the views of the respondents on the problem of connivance to theft at receiving and dispatch points. Survey participants provided views as outlined in Table 4.18 below:-

Table 4.18: Q 20: Other factors measures in the implementation of ISS

Q No	Measure	Frequency	% in Agreement to some extent and above
Q20a	Staff rotation	102	100
Q20b	CCTV	102	100
Q20c	Undercover	102	100
Q20d	Spot checks	100	98
Q20e	Functional integration	101	99
Composite percentage frequency of 60% and above			100

According to the statistics in the above table staff rotation, dedicated CCTV and undercover surveillance are at 100%. This may suggest that the stated security measures could provide an effective solution to the problem if included in the implementation of integrated security systems.

The results from the three different sources were similar in providing potential solutions to the problem of connivance in the implementation of integrated security systems. However, the

solutions point to integrated deployment of stand-alone security measures and not particularly an integrated security system.

The question was to some extent successfully answered in that potential solutions to the problem of connivance were advanced. The study felt that there is more room to further explore the problem particularly as a single research study.

4.3.12 Composite means ranking of survey questionnaire aspects

Table 4.19 below shows the summary central theorem statistics from the responses of the survey questionnaire.

Table 4.19 Mean ranking of survey summary statistics				
Question Number	Mean	Median	Mode	Rank
Q 12: Integration scope of security systems	4.6415	4.7143	5.0	1
Q 17: Factors critical for success	4.3314	4.400	4.60	2
Q 16: Integration process	4.2168	4.222	4.22	3
Q 9: Asset characterisation	4.1471	4.20	3.80	4
Q 18 Benefits of implementing ISS	4.1314	4.1000	5.0	5
Q 15: Key players in the implementation of ISS	4.1042	4.0625	4.00	6
Q 20: Anti-connivance measures	4.0471	4.000	4.00	7
Q 13: Functional integration	3.9261	3.857`	3.86	8
Q 14: Information Communication Technology	3.7549	3.7778	3.67	9
Q 10: Threat sources	3.6824	3.60	4.090	10
Q 19: Challenges of implementing	3.600	3.600	3.40	11
Q 11: Security risks	3.5336	3.5714	3.57	12

The above table indicates that integration scope covered under Question 12 of the survey had the highest mean raking while security risks had the lowest. Security risks were largely affected by the inclusion of items 11f (corruption) and 11g (violence related incidence) which received low scores from the respondents. If these two items are removed, a higher mean score of 3.84 for Question 11 would have been achieved thus significantly affecting its ranking. This translates to the fact that corruption and violence related incidence were not seriously regarded by the respondents in the implementation of integrated security systems. Question 10 was also affected by items 10d and 10e comprising power outage and negligence as threat sources. If these items

had been deleted, a higher mean score of 4.66 would have been achieved thus upgrading its ranking to Number 1 which then shows that it is the first factor to be considered in the implementation of integrated security systems. Therefore, power outage and negligence were not reflected as serious threat sources to be considered in the implementation of integrated security systems In terms of the mode, integration scope and benefits both had a value of 5.0 which was the maximum and this shows that respondents had a keen interest in the study. Overall, all the aspects had mean values above 3.50 which translate to 70% on the 5-point Likert scale. The overall calculated grand mean of 4.0097 indicates a very good acceptance of the study.

4.3.13 Mean, standard deviation and variance analysis of survey statistics

Table 4.20 below shows statistics of means, standard deviation and variance of the 12 survey aspects. The statistics are presented to show central tendency in respect of levels of agreement and differences from the mean with a population of 102.

Table: 4.20 Means, standard deviation and variance of survey aspects			
Questionnaire aspect	Mean	Standard deviation	Variance
Q 9: Asset characterisation	4.15	.572	.327
Q 10: Threat sources	3.68	.572	.327
Q 11:Security risks	3.53	.525	.276
Q 12: Integration scope	4.64	.417	.174
Q 13: Functional integration	3.92	.581	.338
Q 14: Information Communication Technology	3.75	.511	.261
Q 15: Key players of integration	4.10	.496	.246
Q 16: Implementation process	4.22	.422	.178
Q 17: Critical success factors	4.33	.505	.255
Q 18: Benefits of integrated security systems	4.13	.625	.390
Q 19: Challenges of integrated security systems	3,60	.671	.450
Q 20: Other factors (Anti-connivance measures	4.05	.562	.316

The above table indicates that there was little variation in the mean values as most of them ranged from 3.0 to slightly above 4.0 indicating no major disagreements among the respondents. This is supported by the standard deviation values which were within a limited range of 0.4 to 0.6 as indicated in the above table. The highest standard deviation was in Question 19 of challenges while the lowest was on Question 12 of integration scope. In terms of variance, the largest was correspondingly on Question 19 of challenges while the lowest was favourable on

Question 12 of integration scope. The variance values ranged from 0.1 to above 0.3 which indicates that there were no major variations among the survey responses.

4.3.14 Normality tests of survey questionnaire items

Normality tests were conducted to establish the distribution of population parameters of the 102 survey respondents. Kolmogorov-Smirnov (K-S) and Shapiro-Wilk (S-W) tests were used and the statistics are indicated in Table 4.21 below:-

Table 4.21: Survey normality tests results				
Questionnaire aspect description	**Kolmogorov-Smirnov**		**Shapiro-Wilk**	
		Sig		**Sig**
Q 9: Asset characterisation	.110	.004	.952	.001
Q10: Threat sources	.119	.001	.946	.000
Q11: Security risks	.099	.016	.983	.224
Q 12: Integration scope	.195	.000	.819	.000
Q 13:Functional integration	.113	.003	.956	.002
Q14: ICT aspects	.103	.010	.976	.063
Q 15: Key players	.093	.029	.973	.037
Q 16: Integration process	.157	.000	.909	.000
Q 17: Critical success factors	.134	.000	.921	.000
Q 18 Benefits	.085	.070	.911	.000
Q 19 Challenges	.119	.001	.972	.029
Q 20 Other factors	.133	.000	.948	.001

The above table displays K-S and S-W tests of normality which indicate the distribution of the population statistics. From the table, it can be seen that all the K-S and S-W test values were more than 0.05 which indicates that the null hypothesis that data were normally distributed was not rejected. The test values represent normal distribution. The significance tests for both types of tests were positive with no values below 0.00 (<0.05) which results in the null hypothesis to be rejected.

4.4 CONCLUSION

This chapter made a presentation of the data for the study. It began with presentation of the data on qualitative aspects of observations and interviews. The second half presented results of quantitative research based on sample data from the questionnaires. In each part, a description of the sample was made followed by the data collection method and method of analysis. Factors which were evaluated in the study for security systems integration were risks, design, organisation and impact. Risk factors included assets, threat assessment and the actual risks confronting the organisations. Scope of integration, functional integration and IT integration comprised design factors. Organisation factors covered key players, integration process and success factors. Finally, impact factors involved the benefits and challenging perceived to be associated with integrated security systems. This arrangement enabled the researcher to have a deeper insight of information using the three methods of data collection.

The majority of observations and participants reflected a high level of agreement with the implementation of integrated security systems. However, participants could differ on the level of importance attached to each of the integration aspects. Under risks, the majority conclusion was that products and infrastructure needed protection from employees and outsiders to reduce the incidence of theft and burglary. In terms of design factors, the final model consisted of EAC, alarms CCTV and ICT aspects. The majority responses complemented this with physical security, guards and procedures. Many respondents in managerial and officer positions agreed that it was equally important for company functions to be linked with security. However, the research established that at the majority of sites there were no written policies and procedures while functional integration was not properly reflected. Considerable attention was also given to organisation factors. In this regard, the majority of respondents were of the view that IT, Security and Top Management were the key players in a process which involves security survey, system design, installation, training and operation. Key success factors were sighted as resources, top management commitment and skills. Participants also expressed their opinion on impact factors of benefits and challenges. Improved effectiveness was highlighted as the most outstanding benefit while system breakdown and sabotage came out as the most potential problems.

The analysis and findings broadly highlighted the direct and indirect relationships among the various aspects to be considered when implementing ISS. Chapter 5 presents a discussion of the results, findings, conclusions and recommendations for future studies.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

5.1 INTRODUCTION

This is the last chapter of the research study. The chapter comprises an introductory part which is this subsection. This is followed by findings of the study and contributions of the research. Later there are subsections on recommendations, then limitations and conclusion. The main purpose of the study was to investigate the implementation of integrated security systems in the Harare industrial area and thereby contribute to the search for knowledge on this topic. The problem which the research sought to address was the implementation of integrated security systems at industrial facilities. The study examined several contributing factors for the effective implementation of integrated security systems. The main factors of security systems integration were identified as risk, design, organisation and impact.

The study was based on establishing how security systems could be properly integrated. The significance and importance of this study was centred on providing added value to the implementation of integrated security systems. To accomplish this, the research used a mixed method approach which consisted of site observations, interviews, and survey questionnaires. The study found out that there is limited literature and research on the subject of security systems integration. Most of the literature reviewed included aspects on information technology security measures which do not include combination of physical security measures. This study intended to advance knowledge on combining security systems, ICTs and other organisational factors in resolving security problems at an industrial facility. This research was probably the first of its kind in Zimbabwe and, hopefully, it will help advance important aspects in the implementation of integrated security systems.

The following research questions were particularly central to the study:

- What are the major security risks confronting organisations in the Harare industrial area?
- What is the extent of implementation of integrated security systems in the industrial sector of Harare?
- Why is it necessary to implement integrated security systems?
- Which security measures and systems need to be integrated?
- Are there any technological impediments to implementation of integrated security systems?
- Who are the key players in the implementation of integrated security systems?
- How is the implementation of integrated security systems carried out?
- What is required to implement integrated security systems?
- How effective are integrated security systems in the prevention and detection of security incidents?
- What are the problems associated with the implementation of integrated systems?
- How do security practitioners perceive the current state of security systems integration in relation to the problem of connivance to theft within the Harare industrial sector?

The main themes of the study were derived from the above research questions.

5.2 INTERPRETATION OF FINDINGS

The summary of the findings was based on data analysis provided in Chapter 4. These findings are non-exhaustive but consist of the major outcomes of the study and are the following:-

- The main threat sources to industrial assets were sighted as employees and outsiders who contribute to the major security risks which were found to be theft, burglary, fraud, fire and robbery;
- Most of the sites (about 55%) did not have integrated security systems. The security measures in place mostly consisted of physical security, guards, CCTV, alarms, policies and procedures which are stand-alone. According to Vellani (2007: 206), security measures should be integrated in order to provide effective protection. Therefore, the

presence of stand-alone security measures at most industrial sites can compromise security;

- The reasons for integrating security systems at industrial facilities were found to be high vulnerability of receiving, warehousing, dispatch, plant and machinery, access control and cash office points which were likely to be affected by theft, burglary, fraud fire and robbery security risks. In view of advancements in security technology security systems, integration was found to be a suitable solution for protecting these vulnerable points;

- The three methods of data collection indicated the integration of access control, guards, alarms, CCTV, fire system, policies and procedures as an integrated security system. On functional integration, the study found out that the Security function should have close links with Information Communication Technology, Human Resources and Finance. Most industrial facilities (about 73%) did not have written security policies and procedures and Vellani (2007: 173) alludes that while policies and procedures are cost-effective, they are not mostly included in a security system;

- The suitable modes of transmission for an integrated security system were found to be fibre optic on local area networks (LAN) or wide area network (WAN) using Integrated Services Digital Networks (ISDN) or Asymmetric Digital Subscriber Lines (ADSL) and complemented by wireless transmission.

- The key players were indicated as Security practitioners, System suppliers/installers, system operators, top management, and Information Technology specialists, security service providers and/or project team members;

- The process of implementing integrated security systems was found to include security policy, security survey, system design, procurement, service level agreement (SLA), installation, training, operating, review and upgrade;

- The requirements for integrating security systems were found to be the need for the security system, availability of resources, top management commitment, skills to implement and feasibility to implement were critical to the effective implementation of ISS. In support of this, Larson (2009: 134) found out that executive management support is essential for the convergence of security systems. In addition, Vellani (2007: 175) also comments that upper management commitment ensures compliance to implementation of security measures;

- In terms of perceived effectiveness, all three methods indicated that integrated security systems were more effective, easy to monitor, provided a good outlook of security and ensured improved record keeping of the security function;

- The challenges of implementing integrated security systems were indicated to be possible lack of top management support, insufficient resources, system breakdown, and difficulties in operating due to skills shortages, sabotage, and incompatibility with existing systems, power outages and network connectivity; and

- The study also established that connivance to theft at receiving and dispatch points at industrial facilities may be reduced by the inclusion of dedicated CCTV, undercover surveillance, functional integration and spot checks.

5.3 CONTRIBUTIONS OF THE STUDY

The findings of this research provide several contributions to management, security, information technology, security service providers, security system suppliers and security training organisations. The contributions include the following.

5.3.1 Insightful to management

Upper management should draw insights from this study on its responsibility to ensure the implementation of integrated security systems. The study found out that top management is ultimately responsible and accountable for risk management even though it delegates this to some functions within the company structures. Authority to provide resources for security systems integration is granted by top management. If this approval is not granted, then there is no subsequent deployment of integrated security systems. The consequences of not deploying effective security measures will return back to management through losses due to thefts, burglary, fraud, fire and other security related problems as established by the study. This view was supported by the American Society for Industrial Security (ASIS) International Chief Security Officer Roundtable (CSORT) report (ASIS CSORT, 2010: 19) which discloses that programmes that integrate company activities should have strong support from executive management. The ASIS CSORT (2010: 5) rightly points out that establishing effective risk management should not be viewed as a costly luxury but a business case.

5.3.2 Lessons for security practitioners

Security practitioners may draw considerable lessons from this study based on the findings and recommendations. It was one of the study's findings that security practitioners play a critical advocating role in the implementation of integrated security systems. Top management can only be alerted and convinced by the security manager on the need to implement or upgrade security systems. Therefore, security practitioners should make serious efforts to gain insight into security systems integration not only from this study but from other sources as well. Security managers should have some knowhow in security technology because of the rapid changes in technology used in security in general. The ASIS CSORT (2010: 17) supports the view that information

technology aspects are important in the overall management of security risks in various organisation settings.

5.3.3 Coordination between IT and Security

Security practitioners should work closely with Information technology (IT) professionals to ensure effective deployment of integrated security systems. The convergence of information technology and physical security was alluded to by Larson (2009: 28-31) because security convergence has similarities with security systems integration. IT practitioners provide expert advice on technological aspects of systems integration, in particular the identification of quality security devices and the mode of data transmission. Transmission platforms and networks are important to security systems integration as they contain aspects of effectiveness and information security. A desirable security system should be both effective and secure. An insecure security system can be tempered with and therefore may in itself become a security weakness. The prime purpose of any security system is to deter, control, detect and in some instances, detain perpetrators at an industrial facility. Instant detection and rapid response are basic and powerful requirement of an integrated security system at an industrial site as asserted to by Vellani (2007: 206).

5.3.4 Informative to security systems and service suppliers

Suppliers of security services and systems can also benefit from this research. In the modern-day security environment, security measures should be deployed to complement each other. Stand-alone security measures may not be effective in view of the complexity of security threats confronting organisations. Suppliers of security services and systems should be able to advise clients on the suitability of security systems for integration in view of the security risks confronting the facility. Integrated security systems have potentially high initial capital outlay cost implications but the benefits are long-term if proper identification and deployment of combinations of security measures is made. Vellani (2007: 208) advises that it is important to employ more skill in identifying the requirements of an effective security system. In addition,

Vellani (2007: 209) demonstrates that security systems should be deployed in layers and that they be in sufficient combination to perform the desired security functions.

5.3.5 Contributions to training

Institutions and organisations that provide training in security and loss control management can take some aspects of this study into their training programmes. Security training organisations may consider some of the following for inclusion:-

- Security systems integration;
- Problem solving in the security management environment;
- Inductive and deductive reasoning for security practice; and
- Security practice root cause analysis.

According to Mouratidis and Giorgini (2007: 17-28), security system requirements are viewed as restrictions at a facility. These are some of the high-level skills which security managers at industrial facilities are supposed to acquire to ensure effective protection of the sites.

5.4 RECOMMENDATIONS

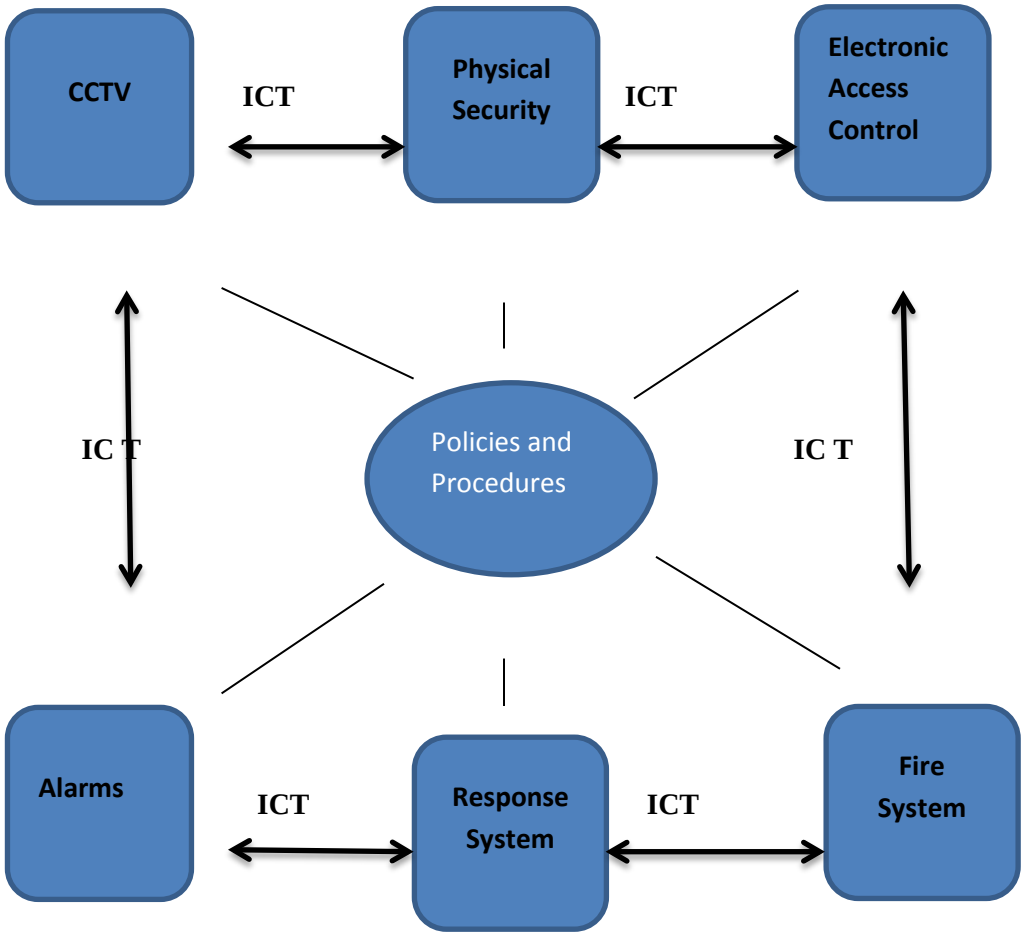
The recommendations are derived from the sources of the research which were literature studies, site visits, interviews and the survey. Common themes from the sources were combined to establish the recommendations. The recommendations are discussed in the following subsections.

5.4.1 Integration Scope

At an industrial facility, the task of identifying the appropriate security measures is not a simple one because security measures are obtained at a cost. Therefore, security measures are part of the cost structure of the facility's operations. More effort is required in arriving at a decision on

which type of security measures to deploy. In regard to this, Williams (2008: 314-315) discloses that institutional pressures from within the internal and external environment may cause organisations to adopt certain security measures without much consideration. Accordingly, companies may simply imitate what was implemented elsewhere. While some security measures may be regarded as the in thing, it is always necessary to carry out a proper evaluation before deploying the security system. According to Williams (2008: 317), organisations have much bigger task of securing their assets and operations because the threats have increased. While stand-alone security measures may in some cases be effective, this study recommends that, where applicable, the following design of security systems integration should be employed either in full or in part. The level of integration depends with the perceived risk incidence and the capacity of the organisation to implement the deployment. The study recommends the scope of integration as depicted in Figure 5.1 below.

Figure 5.1: Preferred scope of integration at an industrial facility



ICT: Information Communication Technology

(Source: Own source)

According to the above figure, the systems are linked by information communication technologies including networks. Clifford (2004: 193) agrees with this scope by mentioning physical security, information technology, personnel security and general security management which includes policies and procedures. On the same note, Fay (2011: 411-412) advocates for a similar integration structure made up of people, physical security and policies and procedures.

In the above diagram, security policies and procedures are at the centre because they are the ones which direct the operating of the other security measures. Each of the integration aspects will be briefly discussed below together with the appropriate recommendations.

Physical security characteristics

Physical security, which is part of Crime Prevention through Environmental Design (CPTED), is an integral part of any security system at an industrial plant. Physical security, in the context of this study, refers to in-built or static security measures which are non-electronic such as perimeter security, entrance points or windows. The design of physical security at a facility gives an impression and general outlook of safety and security, prevention and potential detection of violations.

However, industrial physical security measures are many to mention. The most common ones include perimeter security fences, walls, entrances, offices, plant and machinery, workshops, warehouses, locks, safes and lighting. Perimeter security can be integrated through fence, lighting, intrusion alarm, CCTV and guard monitoring. The study established that the purpose of physical security at an industrial site is to:-

- restrict entry and exit of people and vehicles;
- control the movement of people and vehicles within the facility;
- monitor the movement of assets;
- prevent unauthorised access to assets and operations; and
- confine the activities of the industrial facility within its precincts.

It was the study's finding that physical security measures should be regularly checked for damages and violations through weaknesses and that repair and maintenance of physical security should be part of an industrial security programme.

The study found out that the security function usually has security personnel under the security manager who is tasked with the design and implementation of the security programme. Security guards may be either internal or contracted. The study contends that it is important to ensure that

security staff at all levels are properly selected, trained and equipped in the context of the facility's security environment. Supervision, rotation and separation of functions are inherent requirements of a security programme depending on the prevailing situation. The security department should occasionally carry out security awareness programmes among company staff members highlighting security problems, implications and soliciting for potential solutions.

Access control

Access control is a very prominent and important security activity at an industrial site. In fact, all the other security measures are inherently part of access control. In relation to this, Vellani (2007: 196) deduces that the main purpose of access control is to allow or deny access depending on the circumstances as per security procedures. Laxity in access control may cause serious security problems at an industrial facility. Access control can take various forms such as entrances, gates, doors, turnstiles and electronic access control. At the main industrial entrance, a dual entrance of physical and electronic access may be desirable to cater for vehicle and pedestrian traffic respectively. An integrated access control system should include the following:-

- Physical access control;
- Electronic access control;
- Security personnel;
- Guard or control room;
- Lighting;
- CCTV;
- Alarms zoom;
- Radio communication;
- Intercom;
- Telephone and/or mobile phone; and
- Public address system;

Caputo (2010: 300) vividly captures the integration of CCTV surveillance and access control systems within the company's network infrastructure. Mouratidis and Giorgini (2007: 19) claim that access control as a security requirement is a restriction on the operations of the industrial facility. If that is the case, security practitioners should ensure that access control achieves the twin objective of enabling secure and continuous business operations.

Closed Circuit Television (CCTV)

Due to advancements in technology, CCTV has become a common part of most security systems (Vellani, 2007: 189). There are several forms of CCTV technology. However, the technical aspects of security systems were not part of this study. At the basic level, the functions of a CCTV involve capturing images and transmitting them to a monitor. The data are then stored in devices. CCTVs serve as deterrence and detection security measures and are useful as aids to investigations. The study recommends the following aspects to be taken into consideration in the deployment of CCTV systems;-

- The purpose of deploying the system;
- The quality of the camera in terms of its pan, tilt and zoom (PTZ) capabilities as well as lens types. Most security system suppliers recommended five megapixel cameras. Some cameras may have software capable of counting items as they pass through a receiving or dispatch point;
- Transmission options can be coax, fibre optic, unshielded twisted pair cabling or Internet Protocol (IP) and Vellani (2007: 191) supports these options. IP cameras which operate on WAN or LAN are preferable but less costly options can still be suitable. IP-based cameras which use the company's network infrastructure are desirable because they can be easily upgraded and can be interconnected to other security systems such as access control systems, desktop computers, laptops and smart phones (Caputo, 2010: 282-283);
- Consideration should also be given to the capacity of the controlling monitor. At large facilities a multiplexer or matrix switcher with capabilities of 2-16 and 32-64 cameras respectively are desirable;
- As for monitors, liquid crystal displays (LCDs) and computer monitors are preferable;

- Recording options can be time-lapse, event or digital recorders. There is now a shift from analogue to digital transmission and recording (Vellani, 2007: 195);
- Other advanced options include Internet Video CCTV systems and Intelligent Video motion detectors; and
- Administrative aspects in particular training of CCTV operators and potential public liability issues should be attended to. The risks of operating a CCTV system should be weighed against the benefits. In most cases, the benefits far outweigh the risks. The cost implications of deploying CCTV should be evaluated using return-on-investment recommendations where possible.

Alarm systems

Intrusion alarm systems are very useful in protecting the perimeter fences and restricted areas at an industrial facility. All round deployment of security guards at all points is not practically possible given the high costs involved. Therefore, the deployment of alarm systems can complement guards very effectively. An alarm system has the capabilities of sensing, processing, transmitting and reporting the presence of a security violation (Dave, 2007: 59). The purpose being to detect, deter and cause reaction to the security breach. Dave (*ibid*) discloses types of alarm sensors as point, beam, relay, capacitance and intelligent detection. The choice of sensors to be deployed depends on the type of threat source and the level of security at the facility. Industrial facilities may require maximum, medium or minimum security depending on the value of the assets and the threat sources (Fennelly, 2013: 42-43). Alarms are electronic security systems which after sensing then have to process, transmit and report the incident following which there will be reaction and evidence gathering (Dave, 2007: 58-63). Alarm systems can be integrated with CCTV, electronic access control, response systems and backed by policies and procedures. Given their purpose and cost-effectiveness, alarm systems can be considered to be an indispensable security component of an industrial security programme. However, there is always the possibility of responding to false alarms but there are some expert alarm systems which can mitigate or eliminate this problem depending on the environment.

Fire systems

Fire systems usually fall under the function of Safety and Environment at an industrial site. However, in some cases, Safety and Security are combined in one department or section. Where the security function is separate, there is still the responsibility of monitoring and reporting and reacting to a fire system. According to Vellani (2007:205), the purpose of a fire system is to detect the presence of fire or smoke and to cause subsequent response to fire incidents. Vellani (2007: 204-205) articulates various aspects of a fire alarm system which include types of detectors. Fire systems can be integrated with alarms, personnel, specialised fire response teams and any other emergency response units. Security personnel need to be regularly trained in basic fire drills since they may be the first to engage the fire at its early stages in the absence of other staff members at the facility.

Information communication technologies (ICTs)

Integrated security systems transmit data using ICTs. The choice of the data transmission technologies falls under Information Communication Technology specialists rather than security practitioners. However, security managers should demonstrate sound knowledge of information technology for them to properly understand integrated security systems.

The security subsystems can be connected by cables to the control centre. Transmission can be by copper wire (coaxial, twisted pair or multi-conductor), fibre optic or wireless transmission. Copper wire is recommended for single sites while fibre optic and wireless transmission is suitable for both single and multiple sites. Cable transmission is less costly than wireless transmission. Techniques of transmitting data are Integrated Services Digital Network (ISDN) and Asymmetric Digital Subscriber Lines (ADSL). ADSL is recommended because of its internet, video, high speed capabilities and compatibility with many computer types and applications.

The overall monitoring and control can be conducted on a single monitor in the control room over a local area network (LAN), wide area network (WAN) on intranet or Internet. A LAN is recommended for a single site while multiple sites and/or remote monitoring require WAN,

intranet or Internet. A graphical user interface (GUI) can be used to display the integrated data selectively and with convenience at the monitor.

Security policies and procedures

The study recommends that an industrial facility should have security policies and procedures as the central point of its security management programme. The security manager is tasked with the formulation and implementation of the security policies and procedures. On security policy, Rogers (2011: 39-47) advances its importance and mentions protection of assets, corporate responsibility, conflict management and accountability as some of the reasons for a security policy. There is no standard format for a security policy but Rogers (2011: 56-59) suggests that it may include philosophy, resources, procedures, duties, and responsibilities of staff members. The policy is a broad statement from top management that demonstrates its support for security management programmes.

Duties, responsibilities, functions, instructions and controls are part of security procedures. Security procedures are derived from the security policy. Rogers (2011: 50) insists that security procedures, instructions, standards and code of conduct are inexpensive and very effective security measures. Unfortunately, the study established that they were overlooked and absent at most industrial facilities. The study recommends that policies and procedures provide oversight of an ISS.

Functional integration

Another element of total security integration can include functional integration. Functional integration relates to the interdependencies of functions at the industrial site. The study strongly recommends the integration of Security, IT, Safety, Human Resources, Finance and Distribution departments at an industrial site in view of the risks confronting most industrial facilities. Harvey (1996: 158-159) asserts that the security function should be brought together with other business functions and points out that maximum benefits will not be derived if there is no security convergence with other functions at the workplace. The depth and breadth of security

convergence with other functions is largely dependent on the industrial site's business model, operations design and the risks confronting the organisation.

5.4.2 Levels of integration

Integration can be done at various levels depending on the preference of the organisation and the study recommends the following levels:-

- Level 1: access control, perimeter intrusion alarm, burglar alarm, CCTV, and intercom;
- Level 2: the above plus fire system; and
- Level 3: Level 2 plus lighting and temperature controls.

The choice of security technologies depends with the degree of vulnerability, desired level of security and capacity to implement. However, the study recommends Level 1 and a separate fire monitoring system. This reduces the risk of simultaneous failure. The fire system can be maintained separately by the Safety function but monitored by security at the control room. While the fire system can be independent from the security subsystems, all the subsystems including fire can be operated from the same control panel in the control room.

The study further recommends that the security systems should be provided by one supplier with the skills to design, install and maintain but the problem with a single supplier is that upgrading with products from other brand suppliers may be difficult. The study also established that it may be challenging to find a supplier with all the competencies. The separation of functions in design, supply, installation and maintenance is recommended for security reasons because if a single supplier is involved in all the activities the security system may be highly compromised.

5.4.3 Integration decision making matrix

The study developed the following integration matrix as a decision making tool for management at industrial sites. The information used in developing the platform was obtained from literature review, qualitative and quantitative data analysis. The matrix is shown in Figure 5.2 below.

Figure 5.2 Integrated security systems decision making matrix

	Effective	Partly effective	Not effective
Not integrated			**C**
Partly integrated		**B**	
Fully integrated	**A**		

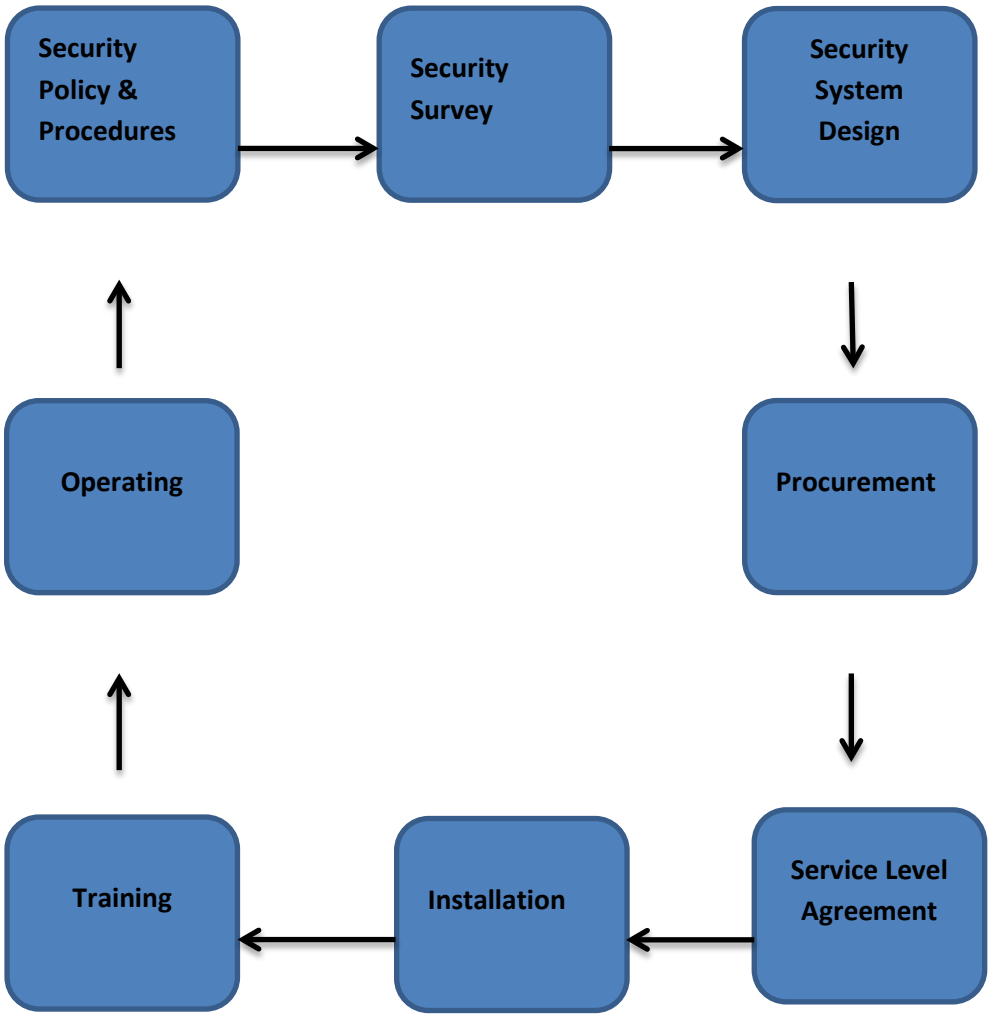
The above matrix has three integration options and three measurement points on the other side. The choice of integration depends with the security risks confronting the organisation and the company's capacity to deploy the preferred scope of integration. The A, B, C quadrants simply indicate the midpoint on the matrix. In some cases, a combination of stand-alone and integrated security systems may be ideal. Normally, this is what obtains on the ground in practice though the scope of integration may be heavily tilted towards not integrated or integrated. It is practically impossible to integrate all security measures at an industrial site. Full integration which includes heat, ventilation, air-conditioning (HVAC) though desirable may not be possible at most industrial points mainly due to various constraints although it provides optimum solutions at an industrial facility.

As for measurement it can be either effective, partly effective or deemed not effective. A security measure whether integrated or not should have some degree of effectiveness. However, it is very difficult to measure the effectiveness of security systems in quantitative terms alone. A combination of both qualitative and quantitative evaluation should be used to arrive at a reasonable conclusion. In addition, any security system proved to be ineffective by any standards should be replaced or upgraded. The element of cost-effectiveness was not part of the current study and therefore cost is not included in the matrix but is assumed to be a latent element present within the matrix.

5.4.4 Integration process

The recommended integration process which is shown in Figure 5.3 below has eight aspects which are security policy, security survey, security system design, procurement, service level agreement, installation, training, and operating. The process presupposes that there are already security measures and systems in place at an industrial site but that they are stand-alone or partly integrated. The process model may also be used for a new facility which commences with integrated security systems. The recommended model is just a guide. Individual organisations may decide to start at any point, put additional aspects, or not include certain aspects depending on their preferences. A brief description of the recommendations on each of the aspects follows.

Figure 5.3: Recommended model for security systems integration process



Security policy and procedures

The security policy provides a general guideline to the security management programme of the organisation. It shows the security risk posture of top management while security procedures the guidelines for implementation of the integrated system.

Security survey

Fennelly (2013: 41) advances a security survey as the best activity for establishing the protection needed at an industrial facility. In the scope of security systems integration, the security survey should take the form of a vulnerability assessment. This approach subsumes that the industrial facility is an on-going entity with existing security measures which need integration or upgrading. According to Vellani (2007: 86), vulnerabilities are weaknesses or gaps in the security system. The vulnerability assessment would indicate opportunities for integration or upgrading already integrated security systems. In support of this Young and Levison (2014: 35) also advocate for a vulnerability assessment arguing that it elevates security to an integrated system. Colombo (1999: 121) is of the same view that the survey involves a threat and vulnerability activity which is the basis for system design. The security survey may be carried out by the security manager, a team tasked to implement integrated security systems or an external security consultant/integrator. In the case of a project team, it may comprise Security, Information Communication Technology, Procurement and any other function deemed necessary. Only key functions should comprise the team because it should be lean. Other functions outside the team can be consulted for their input as and when necessary.

Security system design

The study recommends that the design be conducted by the project team. The designer should have expert skills in electronics and /or information technology. Dave (2007:37-42) asserts that security system design requires high-level skills which include development of pathways, specifications and product selection. In addition, Dave (2007: 40) conveys strong emphasis on product selection in the design stage and warns that wrong products will not meet the security requirements of the facility.

Procurement

Security systems integration involves capital expenditure (CAPEX) and therefore a financial implication. The procurement process includes budgeting and supplier selection. The budget may cover costs of equipment, consultancy, installation, training and any other related aspects. Suppliers should where possible be identified through a supplier selection and evaluation process. Monczka, Trent and Handfield (2005: 215-218) propose supplier evaluation criteria to include; capacity, skills, costs, quality and technological capability. Monczka *et al*. (2005: 106) advocate for cross-functional teams with regard to complex issues such as security systems integration. Cross-functional sourcing teams are ideal for medium to high level security systems integration involving CAPEX. Security system products should be evaluated using manufacturer's user guides and other complementary sources of information.

Service Level Agreement (SLA)

The SLA should be entered with the system supplier and installer. The SLA should cover aspects of guarantees, system breakdown, maintenance, upgrade, liability, and any other potential risks associated with the security system.

Installation

The installation stage involves the actual deployment of the security systems. The wiring which provides the connections between the subsystems and the monitor is the most delicate one. Caputo (2010: 281) stresses that the installation of the cables is very expensive since it involves connecting the devices into an integrated system. The project team should ensure that such expertise is proved and demonstrated. Any mistakes in installation will prove costly at the testing and operating stages and may render the system ineffective or absolutely redundant hence the need to engage skilled installers.

Training

The training programme should target operators, monitors and staff members at the facility. Training and awareness can be conducted by the security manager, consultant and dealer. Such training should involve dry runs for the system and trouble shooting. Training should also include supervision and be linked to the policies and procedures.

System operation

The system should be tested before full scale operation. The study developed the following site-monitoring matrix as a decision making tool for operating and monitoring integrated security systems.

Figure 5.4: Site monitoring matrix

	12 Hour	24 – Hour
On – Site		
Off – site		
Simultaneous		

The above monitoring matrix has six options. The choice of the integrated security system monitoring strategy depends on the security risks, the nature of the industrial site's operations and the company's capacity to meet the costs of operating and monitoring the systems. Most of the security systems are monitored on-site. Some security companies provide off-site monitoring services via internet and/or other wireless geographic information systems (GIS). The GIS systems include guard monitoring, alarm monitoring and vehicle tracking. Caputo (2010: 283) advises that where there is Internet Protocol network connectivity, the security system can be connected from anywhere including remote access monitoring by smart phone or computer through a secure virtual private network. The study found out that the following options may be suitable for most industrial sites:-

- On-site 24 hour monitoring; and
- Off-site 24 hour monitoring where necessary.

On and off-site 24 hour monitoring system would be ideal for sites considered to be high-level security sites such as power, fuel, water treatment sites and banks within the industrial area. Different monitoring combinations can be used especially when applying situational crime prevention methods where the crime rate has escalated or where there is perceived increase in threat levels.

Any faults and mistakes should be rectified during testing. In the early stages of operation follow up is required on training and awareness. Changes in the effectiveness of security systems at the facility should be noted by the security manager. If the earlier stages are done properly operating and monitoring should follow smoothly. Other underlying issues of changes in culture at the facility brought about by the introduction of the system should be noted. In the early stages resistance to change and conflicts may occur particularly between security and other functions. Buy-in is necessary for the system to achieve its mission and purpose. However minor complaints may be disregarded because they will fizzle out with time as people get used to the system.

Review and upgrade

In addition the security system should be regularly reviewed and upgraded. This can be occasioned by any of the following:-

- Regular scheduled review and upgrade;
- Following a security incident or spate of such incidents;
- System breakdown; and
- Technological advancements.

Whenever the system is being upgraded, incoming technology should be compatible with the current security system platform and in particular information communication technology aspects. Incompatibility may cause the whole system to be replaced at a very high cost. Organisations should deploy technologies which provide opportunities for upgrading with future products. Fibre optic technology offers such flexibility. Most computer based platforms offer opportunities for upgrading.

5.5 FUTURE RESEARCH

It is hoped that this study will generate more interest amongst security management scholars and practitioners to further investigate security systems integration. Other areas of security systems integration such as effectiveness and cost implications may need separate research work. Contemporary business environments are mostly information driven. This research confined its work to the security of tangible assets. However the platforms upon which these assets are managed are information driven through applicable software. It is within these software systems which cover functions such as human resources, procurement, finance and inventory management that losses can be experienced. The reasoning is that if these functional management platforms are penetrated, products, materials and revenues can be lost through theft or fraud without the knowledge of the security function. Therefore additional research may be required to establish how security systems mentioned in this study can be further integrated with these platforms in particular inventory management and transaction processing systems.

This study had its limitations one of them being that it was confined to the Harare industrial area. If the research had been limited to a case study of one large organisation, in-depth information could have been obtained. The fact that the study was spread over a large area means that disparate pieces of information were obtained which needed a lot of effort to meaningfully combine to make sense. Therefore it is believed that in-depth case studies will enable a deeper understanding of the impact of integrated security systems, the risks and costs involved. The current study can also be expanded to cover public sector institutions, specific commercial entities such as mines, and retail to get further information on the concept. By expanding to various other types of environments, more detailed information may be obtained for analysis and comparisons made with this study. There is also need to get contemporary information on integrated security systems because of rapid technological changes hence the need for future research.

During the interviews the study identified connivance to theft and fraud at receiving and dispatch points at industrial facilities as a challenge to security practitioners. While the current study collected some information on this aspect as part of the study it is believed that a separate study on this problem may be necessary. This will enable a wide and deep understanding of the problem and the development of potentially more effective solutions in view of the fact that security risks are continually evolving in complexity.

5.6 LIMITATIONS OF THE STUDY

This study had its limitations. The study was confined to the Harare industrial area and therefore its generalizability to other industrial or non-industrial entities may be limited. The response for the survey questionnaire was lower than expected. Non-response by potential respondents could be attributed to lack of knowledge about the research topic or simply lack of interest. Questionnaires delivered by e-mail may not have been accessed by some potential respondents. Low response from the survey was however complemented by one-on-one interviews and observations at the selected sites. The study could have been considered sensitive by some individuals hence the non-response in some cases. Most of the respondents were from firms without or with basic systems integration and therefore they may not have had sufficient experience in security systems integration and therefore the accuracy of the responses may be

treated with caution because some participants may not have been sufficiently knowledgeable about security systems integration. Other factors relevant to the study may not have been included in the data collection methods hence the study may not be considered conclusive. There is room for further research. It is hoped that this study will, despite these limitations avail knowledge and add value to security systems integration.

5.7 CONCLUSION

In conclusion this study examined the implementation of integrated security systems with reference to the Harare industrial environment. In this study the researcher investigated how security systems can be integrated at an industrial site. This study complements related literature in security systems integration or convergence. The challenge of maintaining the cost-effectiveness of stand-alone security systems can be offset by integrating them.

The study used a mixed-method approach comprising of qualitative and quantitative research methods. In the qualitative design, observations and interviews were conducted. The quantitative approach was composed of hand delivered and e-mailed questionnaires. In support of combined approaches Cappers (2008: 71-72) defends the use of the mixed-method research technique in that it is exploratory and contributes significantly to the body of knowledge about the research problem. By using the mixed-method technique the researcher took advantage of the strength and weaknesses of each research method with regards to the various aspects of security systems integration as alluded to by (Cappers 2008: 72). Zafar (2010: 48) concurs to the use of different methods of data collection in that the information can be combined to form a holistic outcome.

Though the research faced some problems and limitations, it does however set the stage for further research in the implementation of integrated security systems in general.

LIST OF REFERENCES

Anon. (1999). Five trends that shape integrated solutions. *SDM Magazine.* October 1999 Supplement. Available at: www.securitymagazine.com (accessed on: 17 February 2014).

Anon. (2013). *Zimbabwe 2013 Crime and Safety Report*. Available at: Https://www.osac.gov/pages/ContentReportDetails.aspx?cid=14191 (accessed on: 17 February 2014) (accessed on: 17 December 2014).

Anon. (2014). Harare crime rate shoots up. *Sunday Mail.* 19 January. Available at: https://www.sundaymail.co.zw (accessed on: 17 February 2014).

Armstrong, M. (1992). *Strategies for human resource management: A total business approach.* London: Kogan Page Limited.

ASIS International (2010). Enterprise security risk management: How great risks lead to great deeds. *A benchmarking survey and white paper* 1-32. Available at: www.asisonline.org (accessed on: 2 July 2013).

Bhandakar, P.L. (2009). *Methodology & techniques of social research*. Mumbai-India: Himalaya Publishing House.

Biggam, J. (2011). *Succeeding with your masters dissertation: A step-by-step handbook.* Berkshire Great Britain: Open University Press.

Bill, Z. (2004). The integrator relationship. *Security Magazine,* 41(I7): 20-24. Available at: http://O-search.proquest.com.oasis.unisa.ac.za/docview/36272677?accountid=14648 (accessed on: 15 March 2014).

Blaxter, L. (2010). *How to research.* Berkshire Great Britain: McGraw-Hill.

Broder, J. & Tucker, E. (2011). *Risk analysis and security survey.* Waltham (USA) Butterworth-Heinemman.

Brooks, D. (2008). Defining the science of private security through knowledge categorisation. *Acta Criminologica CRIMSA Conference Special Edition,* Special Edition (1)12-23.

Bryman, A. (1988). *Doing research in organisations.* London: Routledge.

Cappers, C. (2008). *Effectiveness of situational crime prevention strategies to deter organized retail theft.* Unpublished Phd Management Thesis. USA: University of Phoenix.

Caputo, C. (2010). *Digital video surveillance and security.* Burlington: Butterworth-Heinemann.

Clifford, M. (2004). *Identifying and exploring security essentials.* New Jersey: Pearson Education.

Colombo, B. (1999). A holistic approach to systems integration. *SDM Technology,* 121-124. Available at: http://O-web.a.ebscohost.com.oasis.unisa.ac.za (accessed on: 17 February 2014).

Contos, B.T. Crowell, W.P. Colby, D. & Dunkel, D. (2007). *Physical and logical security convergence: Powered by enterprise security management.* Norwell, MA: Syngress.

Confederation of Zimbabwe Industries (2012). Manufacturing survey. Available at: http://www.trademarksa.org/sites/default/files,publications/2012%20Report_The%20CZI%20Manufacturing%20Sector%20Survey.pdf (accessed on: 1 March 2014).

Dave, T. (2007). *Security convergence: Managing enterprise security risk.* United States of America: Butterworth-Heinemann.

De Vos, A.S., Strydom, H.,Fouche, C.B., and Delport, C.S.L. (2005). *Research at grassroots: For the social sciences and human service professions*. Pretoria: Van Schaik Publishers.

Du-Plooy, J. (2012). *Organisational resilience: A paradigm shift for managing security risks using a maturity model.* Unpublished M Tech Security Management Dissertation. Pretoria: University of South Africa

Fay, J. (2011). *Contemporary security management.* Amsterdam: Butterworth-Heinemann.

Fennelly, L. (2013). *Effective physical security.* Waltham (USA): Butterworth-Heinemann.

Fikes, E. (2009). *Dishonest associates in the workplace: The correlation between motivation and opportunity in retail among employee theft.* Unpublished MA Criminology and Criminal Justice Dissertation. Arlington (USA): University of Texas.

Hanser Group (2010). A reference security management plan for energy infrastructure. *Harnser Group for the European Commission,* 2010: A1-D23. Available at: www.hansergroup.com (accessed on: 15 March 2014).

Harvey, B. (1996). *Security: A management perspective.* New Jersey: Prentice Hall.

Heally, R.J. and Walsh, T.J. (1971). *Industrial security management: A cost-effective approach.* New Jersey: American Management Association.

Hernandez, J.M.C., and Mazzon, J.A. (2006). *Adoption of internet banking: proposition and implementation of an integrated methodology approach. IJBM* 25(2): 72- 88. Available at: www/emeraldinsight.com/0265-2323.htm (accessed on 27 December 2014).

Van Jaarsveld, L. (2011). *An investigation of safety and security measures at secondary schools in Tshwane, South Africa.* Unpublished M Tech. Security Management Dissertation. University of South Africa: Pretoria.

Jackson, M. (2003). *Systems thinking: Creative holism for managers.* West Sussex, England: John Wiley & Sons Ltd.

Kole, O. J. (2010). *An examination of security measures for the protection of petrol stations. An analysis of case studies in Gauteng.* Unpublished M Tech Security Management Dissertation. Pretoria: University of South Africa.

Koleter, J. (2010). *Rethink risk: How companies sabotage themselves and what they must do differently.* Available at: http://O-lib.mylibrary.com.oasis.unisa.ac.za/Open.aspx?id=264962 (accessed on: 15 March 2014).

Kothari, C. (2004). *Research methodology: Methods and techniques.* Delhi: New Age International.

Landoll, J. & Landoll, D. (2006). *The security risk assessment handbook: A complete guide for completing security risk assessments.* Florida: Auerbach Publications.

Larson, L. (2009). *Security convergence: Establishing baseline of best practice in industry.* Unpublished Phd Information Systems Management Thesis. Minnesota: Walden University.

Lombard , C. (2006.) *Industrial security. Study module for Security Practice II.* Pretoria: University of South Africa.

Louw, L. and Venter, P. (2009). *Strategic management: Winning in the Southern African Workplace.* Cape Town: Oxford University Press.

Marczyk, G. R., DeMatteo, & Festinger, R. (2005). *Essentials of research design and* methodology. New Jersey: Wiley Publishing.

Microsoft Corporation (2006). *The security risk management guide*. California: Microsoft Corporation.

Ministry of Home Affairs. Zimbabwe (2007). Private Investigators and Security Guards (Control) Act Chapter 27:10. *Supplement to Zimbabwe Government Gazette*. Harare. Government Printers 24 August.

Monczka, R., Trent, R., & Handfield, R. (2005). *Purchasing and supply chain management.* Ohio-USA: Thompson South Western.

Mouratidis, H. & Giorgini, P. (2007). *Integrating security and software engineering: Advances and future versions.* Available at: http://www.idea-group.com (accessed on: 4 July 2013).

Nleya, F. (2013). Crime wave worries police. *Newsday* 11 March 2013. Available at: https://www.newsday.co.zw/2013/03/11crime-wave-worries-police/ (accessed on: 17 February 2014).

Olckers, C. (2007). *An examination of the impact of residential security measures on the incidence of burglary in two selected northern suburbs of Johannesburg. A security risk management approach.* Unpublished M Tech Security Management Dissertation. Pretoria: University of South Africa.

Pearce, J. & Robinson, R. (2007). *Strategic management: Formulation, implementation & control.* New Delhi: McGraw-Hill.

Pearson, R. (2004). *Electronic security systems. A manager's guide to evaluating and selecting systems solutions.* Massachusetts: Butterworth-Heinemann.

Rogers, C. (2011). *Security practice 111: Study guide for Sep 3701.* Pretoria: University of South Africa.

Sanjeev, D. (2010). *Research methodology for business management studies.* Delhi, India: Global Media.

Sennewald, C. (2003). *Effective security management.* Burlington (USA) Butterworth-Heinemann.

Sewpersad, S. (2010). *An investigation of the bombing of automated teller machines (ATMs) with intent to steal cash contents. Case study from Gauteng.* Unpublished M Tech Security Management Dissertation. Pretoria. University of South Africa.

Thompson & Martin (2005). *Strategic management: Awareness and change.* China: C & C Offset Printing Co-Ltd.

Torres, H. (2007). *Creating added value through asset protection management.* Unpublished DLitt et Phil Thesis. USA: Capella University.

Tustin, D. H., Ligthelm, A. A., Martins, J. H., & H de J van Wyk. (2005). *Marketing research in practice*. Pretoria: University of South Africa.

Vellani, K. (2007). *Strategic security management: A risk assessment guide for decision makers.* United States of America: Butterworth-Heinemann.

Young, W. & Levison, N. (2014). *Inside risks: An integrated approach to safety and security based on systems theory.* Available at: http://0-web.a.ebscohost.com.oasis.unisa.ac.za (accessed on: 17 February 2014).

Williams, Z. (2008). *Supply chain security: An institutional approach to strategies and outcomes.* Unpublished DLitt et Phil Marketing Thesis. Mississippi: Mississippi State University.

Zafar, H. (2010). *Critical success factors for an effective security risk management programme in an organisation: An exploratory case study.* Unpublished Doctor of Philosophy in Business Administration Thesis. San Antonio (USA): University of Texas.

ZRP (2007). National Service Plan. *Zimbabwe Republic Police Headquarters.* December 2007.

ANNEXURES

ANNEXTURE A: PERMISSION LETTER

UNIVERSITY OF SOUTH AFRICA

SECURITY MANAGEMENT PROGRAMME
Muckleneuk Campus
DEPT. OF CRIMINOLOGY AND SECURITY SCIENCE
Preller St
SCHOOL OF CRIMINAL JUSTICE, COLLEGE OF LAW
Ridge, Pretoria
PROF. A. deV. Minnaar
Tel: (+27) (0) 12-4339530 Cell: 0838949485
Fax2email: 0865190625 e-mail: aminnaar@unisa.ac.za

Muckleneuk
P. O. Box 392
UNISA 0003
City of Tshwane
Gauteng, South Africa

Name of recipient **:** ……

Company **:** ……..

Address **:** ……..

Date **:** ……..

Dear Sir

RE: REQUEST FOR PERMISSION TO UNDERTAKE RESEARCH AT YOUR ORGANISATION/COMPANY

Mr. **DIMAX MUSONZA (Student Number: 33419515)** is currently a Masters student in the Department of Criminology and Security Science (Programme Security Management), School of Criminal Justice, College of Law at the University of South Africa(UNISA) and is busy with his research studies for a MTech in Security Management. The title of his Masters research project is: **THE IMPLEMENTATION OF INTEGRATED SECURITY SYSTEMS: CASE STUDY OF THE INDUSTRIAL SECTOR IN HARARE – ZIMBABWE.**

I would like to request permission for him to undertake fieldwork research at your company

DESCRIPTION OF THE PROJECT

Broadly the research project will examine aspects of efficiency, effectiveness and the need for integrated security systems for the protection the industrial sector.

PURPOSE OF THE RESEARCH

The purposes of the research study include the following;

- Examine current practices, benefits, shortcomings in the implementation of integrated security systems;
- Critically evaluate the security management skills required for the implementation of integrated security systems;
- Investigate successes and failures associated with integrated security systems and how implementation can be improved;
- Examine and identify factors necessary for a possible best practice approach in integrated security systems; and
- Determine a methodology for assessing the effectiveness of integrated security systems.

RESEARCH METHODS THAT WILL BE USED TO COLLECT INFORMATION

The research methods that will be used in this study will include the following:

- One-on-one interviews with selected CEOs, Security managers, IT managers and relevant heads of different functions in different organisations. The interviews are expected to be conducted at five selected industrial sites. The interviews will be semi-structured and with both closed-ended and open-ended questions. This will give room to explore other themes that may not be covered in the mailed structured survey questionnaire;
- Survey questionnaire will be designed and distributed to a sample of Security officers and IT officers.
- Site observations: Observing site procedures and daily workings of staff. At least five site observations will be carried out one in each industrial area. The site observations will be in the form of on-site-orientations to obtain insightful information on levels of security

systems integration. These will be carried out concurrently at the same site with the interviews.

RELEVANCE/BENEFITS AND VALUES TO THE ORGANISATION

This would be one of the first studies conducted in Zimbabwe and more specifically in Harare.

- The industrial sector would, hopefully, be guided by the findings;
- The research will highlight the current status of the effectiveness of the integrated security systems;
- Security weaknesses as a result of lack of integrated security systems will be identified;
- Financial loss suffered as a result of lack of integrated security systems will be highlighted; and
- For UNISA, it is planned that the research result could possibly be inputted into future study guides of the Programme Security Management in the Department of Criminology & Security Science.

Once permission is granted please inform Mr Musonza who would then be in touch with you or a representative of your company for the scheduling of any interviews or administering of the research questionnaire with relevant employees in the organisation.

Mr Musonza can be directly contacted at the following:

Cell: 263 774818092

Email: 33419515@mylife.unisa.ac.za or dimaxmusonza@yahoo.com

All the information that is received from the participants or respondents will be treated with the utmost confidentiality (i.e. respondents will remain anonymous and no reference will be made to their identity or of the organisation for which they work. Organisation and personal names will not be used in the research report. Participation in the research interviews will also be on a voluntary basis.

The final dissertation (research report) once accepted will be placed in the UNISA library and therefore in the public domain and can be accessed by interested parties. If any confirmation or other information is needed I can be personally contacted at the following telephone and cell numbers and e-mail address:

Thanking you

Regards

---------- (Prof)

A .deV. Minnaar

Programme Head: Security Management

Department of Criminology & Security Science

School of Criminal Justice, College of Law

University of South Africa

Mr. O. J. Kole

Senior Lecturer: Department of Criminology & Security Science

School of Criminal Justice, College of Law

University of South Africa

Email: koleoj@unisa.ac.za

Tel: +27-12 4339541 Cell: 0822534882

ANNEXTURE B: INFORMED CONSENT FORM

INFORMED CONSENT FORM

Agreement

I …… do hereby consent to:-

- Responding to questionnaires or being interviewed on the topic;

THE IMPLEMENTATION OF INTEGRATED SECURITY SYSTEMS: CASE STUDY OF THE INDUSTRIAL SECTOR IN HARARE – ZIMBABWE

Description of the Project

Broadly the research project will examine aspects of the efficiency, effectiveness and the need for integrated security systems for the protection of the industrial sector.

Purpose of the Research

The purpose of the research study includes the following:-

- Examine current practices, benefits, shortcomings in the implementation of integrated security systems;
- Critically evaluate the security management skills required for the implementation of integrated security systems;
- Investigate success and failures associated with integrated security systems and how implementation can be improved;
- Examine and identify factors necessary for a best practice approach to integrated security systems; and
- Determine a methodology for assessing the effectiveness of integrated security systems.

Relevance/Benefits and Value of the Research

- The industrial sector would hopefully be guided by the findings;
- The research will highlight the current status of the effectiveness of integrated security systems;
- Security weaknesses as a result of a lack of integrated security systems will be identified; and

- The research result could possibly be inputted into the future study guides of the Programme Security Management in the Department of Criminology & Security Practice.

I also consent to:-

- The responses being recorded in writing; and
- The use of the data derived from these responses by the researcher in a research report as he deems necessary.

I also understand that:

- I am free to end my involvement or cancel my consent to participate in the research at any time should I wish to;
- Participation is voluntary and there is no penalty or loss of benefit for non-participation.
- Information rendered up to the point of my termination of participation can, however still be used by the researcher;
- Anonymity is guaranteed by the researcher and data will under no circumstances be reported in such a way as to reveal my identity.
- I am free to determine that specific information that I reveal should not be recorded in writing;
- No reimbursement, gifts or services will be made by the researcher for information rendered or for any participation in this project.
- There is no compensation for responding nor is there any known risk or harm attributable to the research. In order to ensure that all information remains confidential I should not include my name on the questionnaire.
- By signing this agreement I undertake to give honest answers to reasonable questions and not to mislead the researcher; and
- Should there be need to get any form of help to facilitate the transmission of data, myself and the researcher will ensure that such data is transmitted timeously and safely.

I acknowledge that the researcher:

- Discussed the aims and objectives of this research project:
- Informed me about the contents of this agreement; and
- Explained the implications of my signing the agreement.

In co-signing this agreement the researcher undertakes to:

- Maintain confidentiality, anonymity and privacy regarding the identity of the subject and information rendered by myself, the respondent.
- Comply with the ethical principles set out in the UNISA Policy on Research Ethics.
- Communicate, where possible the availability and means of accessing the final research report once accepted by UNISA.

……

……..

Respondent Signature Researcher Signature

Date.....

Date……

I (the researcher)……. certify that I explained the contents of the above.

ANNEXURE C: INTERVIEW SCHEDULE

QUALITATIVE INTERVIEW SCHEDULE

RESEARCH TOPIC: THE IMPLEMENTATION OF INTEGRATED SECURITY SYSTEMS: CASE STUDY OF THE INDUSTRIAL SECTOR OF HARARE – ZIMBABWE.

Interview number:…….Date:…….Time:……..Place ……
……

Section A: Biographical data

Age: ……..

Race: …….

Gender: ……..

Marital status: ……

Position: ……...

Length of service: ……

Educational Qualifications: ……..

Section B: Contribution to the study

- What are the major security risks confronting organisations in the Harare industrial area?
- What is the extent of implementation of integrated security systems in the industrial sector of Harare?
- Why is it necessary to implement integrated security systems?
- Which security measures and systems need to be integrated?
- Are there any technological impediments to implementation of integrated security systems?
- Who are the key players in the implementation of integrated security systems?
- How is the implementation of integrated security systems carried out?
- What is required to implement integrated security systems?
- How effective are integrated security systems in the prevention and detection of security incidents?
- What are the problems associated with the implementation of integrated systems?

- How do security practitioners perceive the current state of security systems integration in relation to the problem of connivance to theft within the Harare industrial sector?

- Are there any other issues that could be included in the effective implementation of integrated security systems?

ANNEXURE D: SURVEY QUESTIONNAIRE

THE IMPLEMENTATION OF INTEGRATED SECURITY SYSTEMS: CASE STUDY OF THE INDUSTRIAL SECTOR IN HARARE- ZIMBABWE

Researcher: Dimax Musonza

The purpose of this study is to determine the context for the implementation of integrated security systems. The results of the study may be published but your name or organisation will not be used. You do not need to identify yourself or your organisation and similarly the researcher will uphold anonymity in that there will be no possibility of any respondent being identified or linked in any way to the research project.

Please indicate your response with an X or any applicable mark in the appropriate box. The questionnaire may take about 30 minutes of your time to complete.

SECTION A

GENERAL INFORMATION

The section is asking your background information.

Q1 Please indicate your gender

Male	1	
Female	2	

Q2 Please indicate your age category

20─25 years	1	
26─35 years	2	
36─45 years	3	
46─55 years	4	
56 years and older	5	

Q3 Indicate your current position in your organisation

Owner	1	

CEO	2	
Manager	3	
Officer	4	
Other (Specify)	5	

Q4 Please indicate your highest professional qualification

Certificate	1	
Diploma	2	
Degree	3	
Post graduate degree	4	

Q5 Please indicate if you have any related knowledge in security practice.

Yes	1	
No	2	

Q6. If Yes please indicate the number of years in security related practice.

5 years or fewer	1	
6 to 10 years	2	
11 to 20 years	3	
Above 20 years	4	

Q7 Please indicate the location of your organisation in Harare.

Workington industrial area	1	
Southerton industrial area	2	
Willowvale industrial area	3	
Graniteside industrial area	4	
Msasa industrial area	5	
Outside industry in Harare	6	
Other: specify	7	

Q8 Please indicate the type of industry your organisation belongs to.

Industrial	1	
Commercial	2	
Security company	3	
Security systems supply/installation	4	
Other: specify	5	

SECTIONS B TO E

THE CONTEXT AND FACTORS FOR IMPLEMENTING INTEGRATED SECURITY SYSTEMS IN THE INDUSTRIAL SECTOR

The implementation of integrated security systems is based on several factors some of which are provided in the sections B to E in this questionnaire. You are required to indicate the level of extent to which the factors impact on an aspect by ticking the corresponding number in the 5 point scale outlined below.

1	2	3	4	5
Not to an extent at all	To a little extent	To some extent	To a large extent	To a very large extent

Please mark with an X or any applicable mark on only one number for each statement.

SECTION B: SECURITY RISK ASSESSMENT

Q9. **To what extent is the implementation of integrated security systems in the industrial sector related to the protection of the following assets**?

Q9	**Asset**	Not to an extent at all	To a little extent	To some extent	To a large extent	To a very large extent
a)	Infrastructure	1	2	3	4	5

b)	People	1	2	3	4	5
c)	Products and materials	1	2	3	4	5
d)	Revenue	1	2	3	4	5
e)	Movable assets/equipment	1	2	3	4	5

Q10. To what extent are some of the following a threat source to which industrial assets may be exposed if security systems are not integrated?

Q10	**Threat source**	Not to an extent at all	To a little extent	To some extent	To a large extent	To a very large extent
a)	Outsiders	1	2	3	4	5
b)	Employees	1	2	3	4	5
c)	Crime syndicates	1	2	3	4	5
d)	Power outage	1	2	3	4	5
e)	Negligence	1	2	3	4	5

Q11. To what extent are the following factors some of the security risks which can be impacted by integrated security systems in the industrial area?

Q11	**Factors**	Not to an extent at all	To a little extent	To some extent	To a large extent	To a very large extent
a)	Theft	1	2	3	4	5
b)	Burglary	1	2	3	4	5

c)	Fraud	1	2	3	4	5
d)	Fire	1	2	3	4	5
e)	Robbery	1	2	3	4	5
f)	Corruption	1	2	3	4	5
g)	Violence related incidents	1	2	3	4	5

SECTION C: SECURITY SYSTEM DESIGN CONTEXT

Q12. To what extent can integrated security systems be implemented by a combination of the following factors?

Q12	**Factor**	Not to an extent at all	To a little extent	To some extent	To a large extent	To a very large extent
a)	Physical security	1	2	3	4	5
b)	Security personnel	1	2	3	4	5
c)	Electronic access control	1	2	3	4	5
d)	Alarms	1	2	3	4	5
e)	CCTV	1	2	3	4	5
f)	Information communication technologies	1	2	3	4	5
g)	Policies and procedures	1	2	3	4	5

Q13. . To what extent does the implementation of integrated security systems also require that the security function be integrated with the following company functions?

Q13	**Company function**	Not to an extent at all	To a little extent	To some extent	To a large extent	To a very large extent

a)	Information Technology	1	2	3	4	5
b)	Human Resources	1	2	3	4	5
c)	Finance and Administration	1	2	3	4	5
d)	Procurement	1	2	3	4	5
e)	Operations	1	2	3	4	5
f)	Marketing and Distribution	1	2	3	4	5
g)	Audit and Risk	1	2	3	4	5

Q14. . To what extent are the following information communication technology aspects relevant in the implementation of integrated security systems?

Q14	**Aspect**	Not to an extent at all	To a little extent	To some extent	To a large extent	To a very large extent
a)	Twisted pair transmission cabling	1	2	3	4	5
b)	Fibre optic transmission cabling	1	2	3	4	5
c)	Wireless transmission	1	2	3	4	5
d)	Local area network	1	2	3	4	5
e)	Wide area network	1	2	3	4	5
f)	Extranet or internet	1	2	3	4	5
g)	Public telephone transmission network	1	2	3	4	5
h)	Integrated services digital network	1	2	3	4	5
i)	Asymmetric digital subscriber lines	1	2	3	4	5

SECTION D: ORGANISATION FACTORS

Q15. To what extent could the following aspects be key players in the implementation of integrated security systems?

Q15	**Aspect**	Not to an extent at all	To a little extent	To some extent	To a large extent	To a very large extent
a)	Security practitioner	1	2	3	4	5
b)	Top management	1	2	3	4	5
c)	System manufacturer or supplier	1	2	3	4	5
d)	System installer	1	2	3	4	5
e)	IT specialist	1	2	3	4	5
f)	System operators	1	2	3	4	5
g)	Security service provider/ security company	1	2	3	4	5
h)	Project team					

Q16. To what extent does the process of implementing integrated security systems involve the following stages?

Q16	**Stage**	Not to an extent at all	To a little extent	To some extent	To a large extent	To a very large extent
a)	Security policy or mandate	1	2	3	4	5
b)	Security risk assessment and/or survey	1	2	3	4	5
c)	Security system design	1	2	3	4	5
d)	Budgeting, return-on-investment and procurement	1	2	3	4	5
e)	Service level agreement	1	2	3	4	5

f)	Installation and testing	1	2	3	4	5
g)	Training	1	2	3	4	5
h)	Operating and monitoring					
i)	Review and upgrade					

Q17. To what extent are some of the following factors critical for the successful implementation of integrated security systems?

Q17	**Aspects**	Not to an extent at all	To a little extent	To some extent	To a large extent	To a very large extent
a)	Purpose of the system	1	2	3	4	5
b)	Feasibility to implement	1	2	3	4	5
c)	Resources	1	2	3	4	5
d)	Skills to design, install, operate and maintain	1	2	3	4	5
e)	Top management commitment	1	2	3	4	5

SECTION E: IMPACT FACTORS

Q18. To what extent do the benefits of implementing integrated security systems include the following aspects?

Q18	**Aspect**	Not to an	To a little	To some	To a large	To a very
a)	Improved effectiveness	1	2	3	4	5
b)	Easy to monitor	1	2	3	4	5
c)	Reduced security personnel deployments	1	2	3	4	5

d)	Improved security outlook	1	2	3	4	5
e)	Improved record keeping	1	2	3	4	5

Q19. To what extent are the following aspects challenges of implementing integrated security systems?

Q19	**Aspect**	Not to an extent at all	To a little extent	To some extent	To a large extent	To a very large extent
a)	System breakdown	1	2	3	4	5
b)	Difficulties in operating	1	2	3	4	5
c)	Incompatibility with existing systems	1	2	3	4	5
d)	Power outages	1	2	3	4	5
e)	Sabotage by insiders or outsiders	1	2	3	4	5

SECTION F: OTHER ASPECTS

Q20. Connivance to crime is a major problem at receiving and dispatch points in the industrial area. To what extent would the under mentioned aspects assist in curbing connivance?

Q20	**Aspects**	Not to an extent at all	To a little extent	To some extent	To a large extent	To a very large extent
a)	Staff rotation at dispatch points	1	2	3	4	5
b)	Dedicated CCTV	1	2	3	4	5
c)	Undercover Surveillance	1	2	3	4	5

d)	Spot checks	1	2	3	4	5
e)	Functional integration	1	2	3	4	5

Thank you for your time and participation in this research survey

ANNEXURE E: EDITING CERTIFICATE

EDITING AND PROOFREADINGCERTIFICATE

7542 Galangal Street Lotus

Gardens Pretoria

0008

13 November 2015

TO WHOM IT MAY CONCERN

This letter serves to confirm that I have edited and proofread Mr D. Musonza's dissertation entitled: **"THE IMPLEMENTATION OF INTEGRATED SECURITY SYSTEMS: CASE STUDY OF THE INDUSTRIAL SECTOR OF HARARE- ZIMBABWE."**

I found the work easy and enjoyable to read. Much of my editing basically dealt with obstructionist technical aspects of language which could have otherwise compromised smooth reading as well as the sense of the information being conveyed. I hope that the work will be found to be of an acceptable standard. I am a member of Professional Editors Group and also a language editor at Bureau for Market Research at the University of South Africa.

Thank you.

Hereunder are my particulars:

Jack Chokwe (Mr)

Bureau for Market Research (Unisa)

Contact numbers: 072 214 5489 / 012 429 3327

jmb@executivemail.co.za

Professional EDITORS Group