VULNERABILITY ASSESSMENT AND PERFORMANCE OF THE SUPERVISORY CONTROLLED AND DATA ACQUISITION SYSTEM AT KENYA ELECTRICITY GENERATING COMPANY LIMITED, KENYA

BY

GITONGA JAMES MURIITHI

A RESEARCH PROJECT REPORT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF MASTER OF BUSINESS ADMINISTRATION (MBA), SCHOOL OF BUSINESS, UNIVERSITY OF NAIROBI

2016

DECLARATION

I, the undersigned, declare that this my original work and has not been submitted to the University of Nairobi or any other institution for academic credit.

Sign……………………………………… Date…………………………

GITONGA JAMES MURIITHI
D61/64756/2013

DECLARATION BY SUPERVISOR

This research Project has been submitted with my approval as a University of Nairobi Supervisor.

Sign……………………………………… Date…………………………

DR KATE LITONDO
SCHOOL OF BUSINESS, UNIVERSITY OF NAIROBI.

ACKNOWLEDGMENT

First of all I would like to thank God for blessings and inspiration throughout the Research Project, the great opportunity and the grace he granted to me through my entire period of Research Project.

Special mention goes to university of Nairobi that offered an opportunity for the course. I highly do appreciate all my lecturers for providing me with the academic knowledge. My special appreciation goes to my supervisor Dr. Kate Litondo for the patience and professional guidance, encouragement and support throughout my project work. I am indebted to you for your patience in reading and reviewing the report. May God bless you.

During the preparation of this report and the entire Research Project period, a lot of guidance was administered and I would like to take this opportunity to thank the staff of Kenya Electricity Generating Company for their cooperation and support while conducting this research.

I would also wish to acknowledge the support I have received from my family. You are a source of strength. To Faith, Emmanuel and Lemuel may the Almighty bless you abundantly. To all my friends, thank you for being there for me and your support is highly appreciated.

To everyone who has helped me, may God shower you with His blessings.

DEDICATION

This Research project is dedicated to my wife Faith, my son Emmanuel and Lemuel for the mutual support and understanding while I was undertaking this course, And my parents Erastus and Elisheba for introducing me to God at my tender age and your constant reference to the holy book and upbringing that has brought me this far.May the Almighty God bless you all.

“My son keep your fathers command and forsake not your mothers teaching bind upon your heart always tie them about your neck. When you walk they will watch over you awake they will talk with you.”

Proverbs 6.20 –22
The Bible (R.S.V)

ABSTRACT

SCADA is an acronym of Supervisory Control and Data Acquisition System. This system is used in various industries for example utility companies, water,oil and Electricity utilities. Kenya Electricity Generating Company Limited, KenGen is the leading electric power generation company in Kenya, producing about 80 percent of electricity consumed in the country. The company utilizes various sources to generate electricity ranging from hydro, geothermal, thermal and wind. Vulnerability Assessment is a process that defines, identifies, and classifies the security holes in a computer, network, or communications infrastructure. Vulnerability analysis forecasts the effectiveness of proposed countermeasures and evaluates effectiveness after they are put into use. The study was carried out in five areas namely Eastern Hydro, Western Hydro, Kipevu, Olkaria and Central Operations where SCADA systems have been installed. The objectives of the study were to determine the extent to which the SCADA system is vulnerable, establish the challenges of performing a vulnerability assessment on the SCADA system and to determine the link between vulnerability assessment and performance of the SCADA system. The design of the Research was descriptive correlation survey. We had 50 successful respondents out of a sample size of 55.A structured questionnaire was used to collect data from Key SCADA users distributed in various KenGen areas who were selected using stratified random sampling technique. Collected data was analyzed using descriptive statistics by means of the statistical package for social sciences (SPSS). The data analysis was in form of frequency and percentages to determine the relationship of the variables. From the study 45% of the respondents were in the age bracket of between 30-39 years who have more IT Skills to detect vulnerability of the SCADA system. The study also found out training on SCADA system in KenGen was very low, KenGen implements adequate security policies for SCADA Systems but does not conduct adequate periodic audits on the SCADA security enforcement policy. The study recommends that the KenGen needs to be conducting adequate periodic audits on the security enforcement policy. Pearson correlation analysis was used to study the relationships between the variables. Independent t-tests (2-tailed) and ANOVA test were used to determine the level of significance. According to the results of the study, there is a strong relationship between Vulnerability assessment and Organizational performance. The study further recommends that employees be trained on the importance SCADA security and how it can affect the competitiveness of the KenGen. The limitations of the study were; the sampled respondents were drawn from some selected sections KenGen staff and the study was only focused KenGen that uses SCADA system. This study recommends further research on the contents and comprehensiveness of SCADA Vulnerability assessment and performance can be done to other related parastatals in Kenya using SCADA systems.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS AND ACRONYMS

CERT	Computer Emergency Response Team
CC	Coordination Center
DCS	Distributed Control Systems
DoS	Denial of Service
IED	Intelligent Electronic Devices
ISO	Independent Service Operators
IP	Internet Protocol
IS	Information Systems
IT	Information Technology
ICT	Information Communication Technology.
KENGEN	Kenya Electricity Generating Company
LAN	Local Area Network
MOE	Ministry Of Energy
MW	Mega Watts
OS	Operating System
PLC	Programmable Logic Controls
PC	Personal Computer
QoS	Quality of Service
RTU	Remote Terminal Units
SQL	Structured Query Language
SCADA	Supervisory Control and Data Acquisition
VPN	Virtual Private Network
VSAT	Very Small Aperture Terminal

CHAPTER ONE: INTRODUCTION

1.1 Background of the Study

Information Security fears against critical utility assets are common in the recent decades. As the outcome of the numerous Kenyan terrorist attacks ranging from United States Embassy, (1998).Since the attack to Garissa attack,(2015) there have been great care to the safety of critical Kenyan utilities. Unsecured computer structures can lead to distribution of Electricity distribution. Breakdown of whichever gadget involved in the critical utility can lead result in the failure of essential services and organizational delivery as stated by Chunlei et al. (2011).SCADA is an for Supervisory Control and Data Acquisition System, Ozdemir, (2006).

According to Ozdemir (2006), the word supervisory control and data acquisition (SCADA) was initially introduced in the 1960s at Bonneville Power Governance and was first printed in the PICA (Power Industry Computer Applications) Conference. Bailey stated that (2003) SCADA encompasses gathering of the information, transmitting it back to the dominant site, carrying out any essential analysis and control and before displaying that information to several operators' screens or display. The essential control actions are at that time conveyed back to the process.

Cilliers, (2002) mentioned that Cyber threats are from misuse of cyber system by users with unauthorized access. A possible cyber threat to Supervisory Control and Data Acquisition (SCADA) structures attack can be affected when an intruder attains access to the supervisory control access of a SCADA scheme and launches control activities that may cause major injuries of system. Increasing necessity upon communications over the

Internet and increasing demands for connectivity amongst corporate networks and SCADA systems have formed the risks and presented susceptibilities. According to Fernandez, (2005) uncertain network designs may be as due to inadequate funds or of absence of knowledge of the practitioners of the system.

ISO 27005 state that vulnerability is a weakness of an asset or assortment of assets that can be misused by one or several threats where an asset is of any kind which has value to the organization, its occupational operations and their endurance, as well as information resources that upkeep the organization's mission. Vulnerability is a fault which allows an invader to reduce a system's information guarantee, (Shou,Corey (1996).Inside the SCADA systems setting, most of the studies have been done in assessment of the vulnerabilities and threats organizations face, this theories include Hong et al,(2003) an Integrated Scheme Theory, Creery & Byres ,(2007) about Safety Life Cycle Model. Security Inspiration Workman et al (2008) theory, Institutional Theory by Bjork,(2004) as well as Information Safety Management Theory;Ericsson, (2010); Finne, (1998).This study will heavily embrace Integrated System Theory since of its measurement indicators and constituents fulfill the research goals and objectives.

The KenGen is the foremost electric power generation firm in Kenya, producing around 70 percent of electricity spent in the country. The company uses various sources to produce electricity starting from Hydro, Geothermal, Thermal and Wind. Hydro is the principal source, with connected capacity of 804.40MW, which is 80 % cent of the company’s connected capacity. In KenGen, SCADA was inducted in mid-2009.The SCADA was installed and ordered by IBERDROLA Ingenieriay Construction from Spain and staff from ICT of KenGen. The Dispatch Centre design hosts Plant Control System, SCADA, company Information and Telecommunication Infrastructure for Key Hydros: Masinga, Kamburu, Gitaru, Kindaruma, Kiambere and Turkwel. (MOE, 2016).

1.1.1 Vulnerability Assessment

Bailey,(2006) mentions that Vulnerability assessment is a system of identifying, quantifying, and prioritizing the vulnerabilities in a scheme. Examples of schemes for which vulnerability assessments are done include information technology schemes, energy supply schemes, transport and intercommunication schemes. In address to disaster management vulnerability means evaluating the threats from potential hazards that are in the utility. This can be in PEST (Political, Environmental, Social and Technology) areas.

Assessments are typically done according to the following procedure; the first step comprises cataloging of assets and abilities (resources) in a scheme. This is followed by allocating quantifiable value and their standing to the mentioned resources. Followed by identification of the vulnerabilities or possible threats to each resource is ended. Lastly Mitigation or elimination of the gravest vulnerabilities for the most valued resources is done as specified by Priya, (2011).Vulnerability study additional focusing on both consequences for the entity itself and on primary and secondary outcomes for the nearby environment. It also involves itself with the possibilities of decreasing such consequences and of improving the ability to manage future incidents as indicated by the American Department of Energy, (2002).

1.1.2 Supervisory Control and Data Acquisition (SCADA)

SCADA is an abbreviation for Supervisory Control and Data Acquisition System, stated by Ozdemir,(2006).Bailey (2003) stated that SCADA involves collection of data from the central site which is then computed and displayed on operator display. Clarke,(2003) admits that the major role of a supervisory system is to link human operative for control. Ozdemir, (2006), indicated that the SCADA system is made up of several subsystems. Data for processing is acquires by a supervisory scheme which processes the commands. Digital data are changed from sensor signals by Remote Terminal Units which links supervisory scheme to the digital data.

1.1.3 Kenya Electricity Generating Company Ltd (KenGen)

KenGen is the principal leading electric power generating company in Kenya, creating about 80 percent of electricity demand in the country. Modes of generation mix include Hydro, Geothermal, Thermal and Wind. Hydro is the principal source, with an installed capacity of 804.40MW, which is 80% of the company's connected capacity. In KenGen, SCADA was initiated in mid-2009.The SCADA was connected and commissioned by IBERDROLA Ingenieriay Construction from Spain and staff from ICT of KenGen. The Dispatch Centre design hosts company Control System, SCADA, company Information and Telecommunication Infrastructure for Key Hydros: Masinga, Kamburu, Gitaru, Kindaruma, Kiambere and Turkwel. A total of 15 producing units from six power plants are under the command of Dispatch Center where frequency, voltage, water management, generation and reports preparation are being supervised and centrally harmonized. The Dispatch Centre is hosted in Kamburu Power Station around 160Km from Nairobi.

1.2 Research Problem

According to Webnar, (2013) SCADA schemes are mainly responsible for serious operations and nationwide infrastructures when such are and abused, could severely ruin the operations of electricity, water as well as power suppliers. The result of an attack may well go far elsewhere a damage of data, it could also result to harm of physical assets and in given circumstances, the cause of death. From time immemorial cyber security tools, such as anti-virus software, have not being effective. Considering the case scenario of Flame virus that went unnoticed from 43 different anti-virus tools and took more than two years to notice (Vijayan, 2011). Attackers aim at energy sector "to steal intellectual property on new technology, such as wind or solar power generators or gas field assessment charts." But “the sector is also a main target for sabotage attacks, which will not create direct profit for the attacker. Such troublesome attacks do already occur and may lead to big financial losses. (Darlene, 2015).

Nelson, (2003) study revealed that the framework of the control center has progressively developed from locked monolithic assembly to exposed networked surroundings. In compatibility of principles this has equalized the price of system deployment between the vendors resulting to system upgradeability. Tighter integration as caused new susceptibilities due to information sharing of numerous power entities which is very difficult as result of cyber threats. Therefore increasing dependency on communications protocols via the Internet has complicated the problem. Manimaran, (2011) stated that safety interrelated modeling comprises of considered internal attacks and the upgrading on power scheme information architectures as well as communication interface. The SCADA examination bed growth is a productive means of pinpointing vulnerabilities of power utilities. Cyber security for the power grid is an upcoming research field as explored by CheeWooi (2009). Moreover, there has not been a method to measure the vulnerability of a cyber scheme by integrating the influence on the power scheme. According to Shaw, (2004) an interior risk can be in the method of intention sabotage which can lead to vulnerability.

The present setup in KenGen is that the SCADA system is held in the process LAN.Specific corporate operators in the corporate LAN link to the process LAN through specific ports which are acceptable to access process LAN.The process LAN is secured by a firewall. Karanja, (2012) says that an intruder can have an access to the SCADA system via the allowable computers in the corporate LAN.This might be owing to security (Generator, 2010).Invader can also gain access to the process LAN via the services like internet access in control systems. Ports are secured by physical firewall may be harmless but ports on software firewall could get an attack by corrupting the software. There is no water tight communication system, particularly on the use of VSAT Network. This system has been hired by a 3rd Party provider with KenGen with no full control over its safety. These remain susceptible and can be simply used by intruders to attack the system.

The evaluation of cyber susceptibilities in control schemes has been a common area of recent research. Research at Sandia National Laboratory, (2012) provided assistance on performing a cyber vulnerability valuation on an SCADA system. Haln, (2011) study on Assessment of Cyber security Valuation Tools on a SCADA environment explored whether the methodologies and tools normally used for traditional information technology (IT) schemes were adequate to meet the cyber safety assessment requirements in power system. Additional work has focused on concerns for performance penetrations tests on control schemes. This study differentiated itself from the previous research as it sought to address vulnerability of SCADA. To the Researcher's best knowledge no research had been done in Kenya regarding vulnerability assessment and performance of SCADA system specifically at Kenya Electricity Generating Company Ltd. This presented a gap in knowledge that this study was intended to fill.

This study attempted to enumerate effect of Vulnerability assessment and performance of SCADA at KenGen.

i) To what extent is KenGen SCADA System Vulnerable?

ii) What are the challenges of performing vulnerability assessment on the SCADA system?

iii) What is the relationship between vulnerability assessment and performance of the SCADA system?

1.3 Research Objective

The general Objective of the Study was to assess the Vulnerability of the SCADA system at KenGen:

a) Determine the extent to which the SCADA system is Vulnerable.

b) Establish the challenges of performing a vulnerability assessment on the SCADA system.

c) To determine the link between vulnerability assessment and performance of the SCADA system.

1.4 Value of the Study

Deviating from previous research that have generally focused on the connection between information safety and factors such as policy framework, resources and levels of literacy, this study endeavors to present a comprehensive viewpoint on Vulnerability assessment versus organizational performance. As such, this study would facilitate knowledge accumulation and conception concerning the organizational performance of SCADA system investment. Via this research KenGen's administration was able to measure the threats, vulnerabilities and challenges that would help to advance on its organizational performance. The conclusions of this study would also help KenGen management team make well-versed decision regarding safety of SCADA system. It would also be a valued platform for KenGen directors to understand SCADA Vulnerability as well as Performance of SCADA system. Other organizations in the electricity sub sector would also benefit as the circumstances under which KenGen functions are not that diverse and will therefore be able to apply the knowledge and findings of this study in their SCADA Systems. The study can also be of help to Researchers, academicians, and other students to advance further research on the topic.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

This chapter analyses SCADA system, SCADA architecture and its application. It also reviewed the Theoretical foundations, Vulnerability assessment, Challenges of SCADA systems. Lastly, the chapter presents Empirical studies on Vulnerability Assessment and Performance of SCADA and Conceptual Framework.

2.2 Theoretical Foundations

A theoretical framework offers a rationale for forecasts about the relationships between variables of a research study and has implications for each decision made in the research practice as mentioned by Mertens, (1999). This study was instituted on three theories.

2.2.1 Management System Theory

Management schemes theory studies the relationships among the organizations and the environment in which they are used. This focus imitates on organizations' ability to familiarize to changes in environmental circumstances according to Boulding, (1956); Kahn and Katz (1978). Founded on the organizational necessities and security approaches, Sherwood (1996) suggested information safety architecture SALSA (Sherwood Associated Limited Security Architecture) which comprises: business wants, major security approaches, security services, security machinery; and safety products and technologies. This theory enlightens the study since it highlights that an organization should create and maintain a known information security administration system to control and guard information assets. ISMS comprise six steps of describing the policy, describing the scope of ISMS, undertaking risk valuation and managing the risk and lastly selecting control aims. (BSI, 1999).Organizations must inspect the environments and safety standards to create an information security policy, describe the scope of information safety and assess the threat and control in order to create an information safety management scheme.

2.2.2 An Integrated Systems Theory

Igure et al., (2006) states that in determining the safety requirements of an organization, it is essential to assess how organizations method information sharing inside the organization. In order to safeguard the security requirements of a company are addressed, this study focused on gauging how the organizations' data security goals are attained based on the components used from Integrated System Theory.

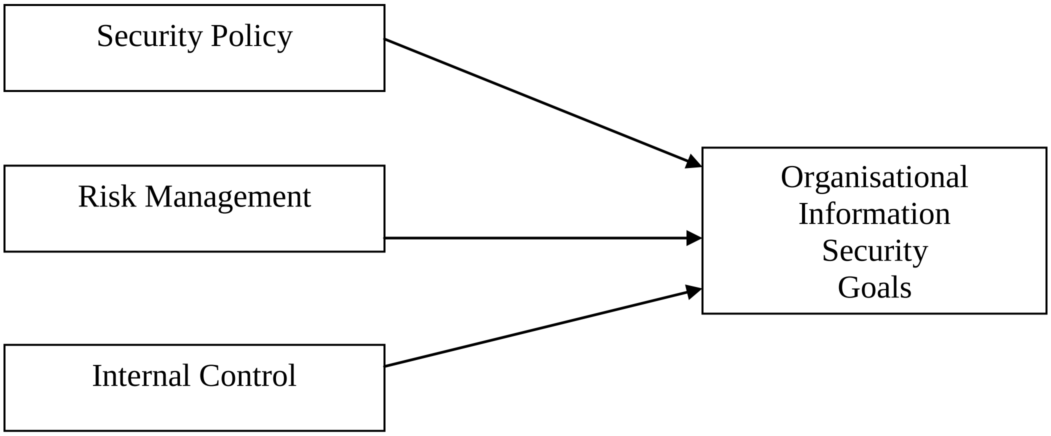


Figure 2.1 displays the Research Classical that was used according to (Hong, Chi, Chao, & Tang, 2003).

Implementing safety policies is indispensable in organizations, particularly organizations dealing with essential services. Safety procedure is precise guidelines of what not allowed system's safety as stated by Stouffer et al. (2011) and Bishop (2003); Safety strategies are significant for certifying agreement to safety practices in an organization. Susceptibilities in a SCADA scheme can happen as result of negligence of dangers, misconfigurations, lowly conservation on the bases of hardware, functioning schemes as well as applications. Danger valuation helps to recognize measure and rank dangers alongside standards for threat approval plus aims applicable to the organization, precisely to users of SCADA schemes. This results in risk valuation that can result in identified action essential to management of the information safety threat to the SCADA as stated by Ismail et al. (2014).

The third significant constituent of Integration System Theory (IST) is regulating and auditing theory this proposes that the performance of every organization depends on the setting of their security systems as stated by (Hong et al., 2003). Control can address avoidance. Detection and correlating actions in the system in order to avoid illegal and illegal access as stated by Ismail et al. (2014). Stouffer at al. (2011) outlined that with put controls like management, functioning and technical controls this guards the confidentiality, honesty and availability of the scheme and its related data.

The performance of every organization depends on the setting of their security systems as stated by (Hong et al., 2003).

2.2.3 Contingency Theory

Structuring and management of organizations is best done using the Contingency theory According to their research based on management of innovation, the environment level best stability should be in variance of the environment as stated by Stalker (1968), found out that organizational systems should vary based on the level of stability in the environment. Contingency approach is to identify and respond to situational variables so as to achieve organizational objectives as stated by (Drazin and VandeVen, 1985).

Contingency management interacts between a set of environmental variables to technological and managerial variables (Lee et al., 1982; Luthans, 1976).

Contingency theory was used in IS research to explain how organization and individuals have a relationship to generate effective systems. The contingency approach focused on two central findings in which the first finding was on how a firm can organize itself. Also other organizing methods are equally effective according to (Galbraith 1973).

Contingency theory is also the central point for situational variables as focuses on unlimited proposition. Feidler (1964) established that the success of contingency theory is in the prediction of a large percentage of the context. Contingency models relate primary variables to performance which includes both organizational performance and system performance. Otley (1980) stated that measurement of performance is done to permit an appropriate form of the contingency theory. This theory informs the study since contingency approach has been applied to information security management.

SCADA schemes incorporate Programmable Logic Controllers, Human Instrument Interfaces and the Local area system or the wide area system, according to Paritosh (2009). By application of SCADA system companies are controlled and observed either from nearby or remotely. SCADA schemes are used in plant upkeep to assist in recognizing the cause of a problem, correcting a looming fault and observing the status of the field devices including the plant itself. Some of these schemes can be constructed to send signals to email addresses of the plant maintenance personnel when a fault happens or when the parameters surpass the set restrictions. Plant performance can be monitored for a given period of time by use of the past archiving. These features also assist the plant maintenance crew in troubleshooting.

2.3. SCADA System Architecture

SCADA scheme architecture varies dependent on a client’s requirements. SCADA architecture includes connection of SCADA scheme to field devices. A SCADA scheme may be constructed in a Local Area System (LAN) or in a Wide Area System. Field devices comprise sensors (temperature, level, flow etc), relays and Intellectual Electronic Devices (IED) which are part of the scheme. Relays are used for on behalf of present status of apparatus, for example if a pump is operational or if it is stopped. IED are gadget such as protection relaying gadget, circuit breaker controllers etc. Pacific (2006), figure 2 portrays a typical Electronic Power SCADA scheme and connections to other systems such as those fitting to backup control centers, the corporate system, and field devices.

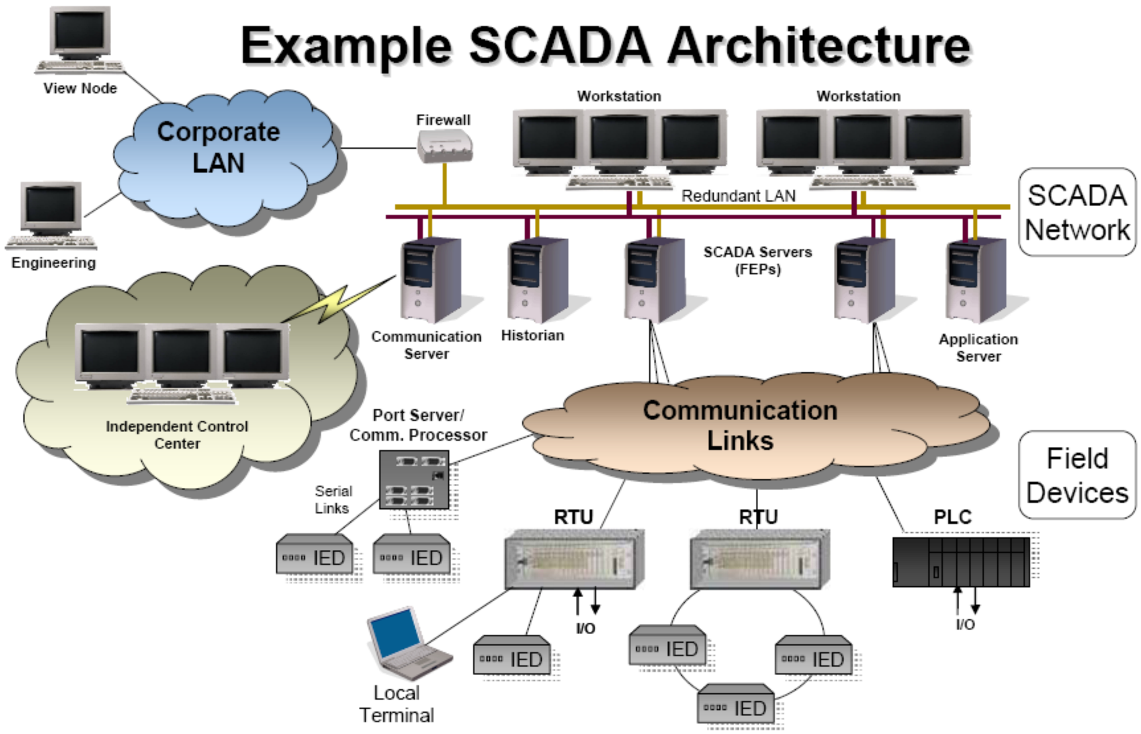


Figure 2.2: SCADA Architecture. Source: Pacific Northwest National Laboratory, U.S Department of Energy 2006.

2.3.1 Significance of SCADA System

Schemes controlling essential infrastructure for producing, transmitting, dispensing, storing, and using energy as well as for procedures in manufacturing are no longer inaccessible. The drive towards interacted industrial control schemes is due to numerous factors. Integration of geographically dispersed assets through central control improves agility in answering to supply and demand variations, reduces cost of processes and enables procedure efficiencies unattainable in the past as stated by Juniper, (2010). Juniper (2010), states that, Electricity utilities are essential to provide just in time generation data to Independent Service Operators (ISOs) and additional market entities.

2.3.2 Application of SCADA System

SCADA systems are widely used in large utilities. Newton-Evans, (2007) states that the power utility uses SCADA in most of their connections as exposed by Motorola, Inc (2007). SCADA schemes are used to monitor water control, Gas and oil distribution, ships and pipelines, as mentioned by Stouffer, (2006).

2.4 Vulnerability Assessment

According to Bailey (2003) Susceptibility Assessment is undertaken to test the safety posture of the information scheme both internally as well as externally .This comprises Vulnerability Definition and classification of system or systems resources done. The Following step is allocating of relative levels of prominence to the resources. This is followed by discovering and identifying potential dangers to each resource. Finally description and implementation of ways to decrease the consequences if an attack happens as mentioned by Ankita Gupta *et al*, (2013).Andersen, et al, (2004) examined if safety holes are found as a result of susceptibility analysis, a vulnerability discovery may be compulsory. If the vulnerability is not categorized as a high level danger, the merchant may be given a certain duration of time to fix the problem before the vulnerability is revealed publicly.

According to Turner, et al, (2003) the other phases of vulnerability analysis (categorizing potential threats) are occasionally done by a white hat by means of ethical hacking techniques. Using this technique to assess vulnerabilities, safety experts intentionally probe a network or system to learn its weaknesses. This process offers rules for the expansion of countermeasures to prevent honest attack. Limited List of SCADA Security valuation activities comprise analysis of the firewall, router, switch alignments, operating schemes configurations, SCADA security alignments and IP based field gadget configuration. According to Gupta, (2013), penetration testing is a technique of evaluating the safety of a system. Services are assessed to identify weakness, faults, vulnerabilities and the absence of covers. It also includes internal infiltration testing done locally inside the network and exterior penetration testing done by remote. Ethical hacking is recognizing weakness in computer schemes or computer networks and providing counter measures that guard the weaknesses.

Neil,(2006) states that ethical hackers stands to getting written consent from the owner of the computer scheme before hacking, guarding the privacy of the association being hacked, Transparently reportage all identified faintness in the computer system to the organization and lastly notifying hardware and software merchants of the identified faintness (Kirandeep,2013).Halderman, (2008) maintains that a password is a expedient and easy technique of authentication for users entering a computer scheme. The system merely requires the user to provide something he knows as a evidence that he is really who he claims to be. This is easily executed, but at the same time the password method is subject to a number of safety threats.

Passwords are frequently besieged by attackers in need of breaking into systems. It is serious that this first line of defense contrary to unauthorized access is operative by rigorously using good password management strategies. Different passwords ought to be used for different schemes with respect to the security necessities and the worth of information assets the need to be secured. Make use of other admission control mechanisms to enable password management and decrease the effort necessary by users in memorizing a huge number of passwords. This should be imposed with good security strategies and guidelines, reinforced by user awareness training and education on the finest practices in picking and management of passwords (Pogue, 2013).

2.4.1 Challenges of Vulnerability Assessment

One of the biggest trials of assigning risk to new susceptibilities is a lack of information. If an group does not have familiar knowledge of its own assets, system design, defense-in-depth policies, and processes, they will find it challenging to quickly and precisely assess the risk level of the susceptibility by Microsoft (2005) for the minor organization this data can be equally easy to collect and document. Corporations must budget for 'housekeeping' actions such as asset and change administration in order to make these actions effective. Classically, ICT safety risk has been seen as the duty of the IT or system staff, as those personalities has the best understanding of the mechanisms of the control infrastructure. Thirdly ICT ought to understand the relative importance of different sets of schemes, applications, data, and storing and communication appliances. To meet such necessities, organizations should achieve security risk assessments that makes use of the enterprise risk assessment tactic and include all participants to ensure that all phases of the ICT organization are addressed, comprising of hardware and software, servant awareness training as mentioned by Schimitting, (2010).

2.5 Empirical Studies on Vulnerability Assessment and Performance of SCADA

This study based on the research of effect of ISMS Warranty to a better organization Performance as stated by Cheol-Soon Park,et,al (2010).The study tried to establish that when an enterprise acquires ISMS certification this leads better public relations that results to better corporate image resulting to increase in Customers bases which further relates to increment in sales. By control of intrusions resulted in cost savings to due control of threats and risks. Further the study also established out that achievement of the information security enhanced the stability of information resources.

Also the study on the effects of information safety systems in relation to businesses performance had some challenges. Information Safety and Organizational Performance: An Empirical research of the Korean Securities Industry through Heekyung Kong, Insung Lee, Suhyun Jung, as well as Seung-Jun Yeon, (2014). This study suggested a model by which, in the security industry from, Korea, information safety activities bolster business stability, ultimately prominent to improved organizational performance. The study empirically confirmed that information safety activities contribute to operation stability, eventually fostering organizational performance. Rossetto et al, (2013) mentioned that by doing so, the validity and influence of information safety activities can be investigated, and corporations and organizations can invent a policy for information security investment and activities, therefore enhancing their commercial performance. Therefore, investment and actions related to IT service structure, information sharing, as well as information security were established not as hygiene issues but as motivational issues under Herzbeg's Two-Factor Theory.

From the findings of this study can be of use as data to support the impartiality and validity of the existing information safety investment, and they are appear as part of the method of describing information security investment not as cost but as operational investment, and of providing investment performance. A constraint of this study was that it was additional like an exploratory study for the analysis of genuine proof in the future. This was because the investment approach for IT services, information safety and information involvement was established founded on existing studies, and the possibility of the investment approach was measured using subjects which were had limited understanding of the information safety investment approach (Masqood, 2010)

2.6 Summary of Literature Review

This chapter reviewed literature on SCADA architecture, its use and importance. It was obvious that the SCADA has been useful in diverse industrial uses. Prominence of SCADA has been acknowledged in the various areas of its use. It also reviewed the Theoretical foundations, Susceptibility assessment, Challenges of SCADA systems. Lastly, the chapter offered Empirical studies on Vulnerability Valuation and Performance of SCADA and a conceptual background on which the complete study revolves. From the review automation schemes had contributed to the growing of operation and progressions of various industries.

2.7 Conceptual Framework

The conceptual framework enclosed three independent variables and three dependent variables, two moderating variables. This study was done to establish how the independent variable affected the dependent variable. Kumar (2005) defines independent variable as the cause invented to be responsible for partying about change(s) in a phenomenon or condition, dependent variables as the result of the change(s) brought about by the introduction of an independent variable. Baron (1986) sates that a mediator or moderator is a 3rd variable that brings about variations the association amongst an independent variable and result variable. The independent variable for the research was Vulnerability assessment of SCADA system. The dependent variable for the study was Performance of SCADA system. The moderating variables were Experience of

Operational staff as well as Staff Training. Moderating variable were treated as constant for the purposes of the study.

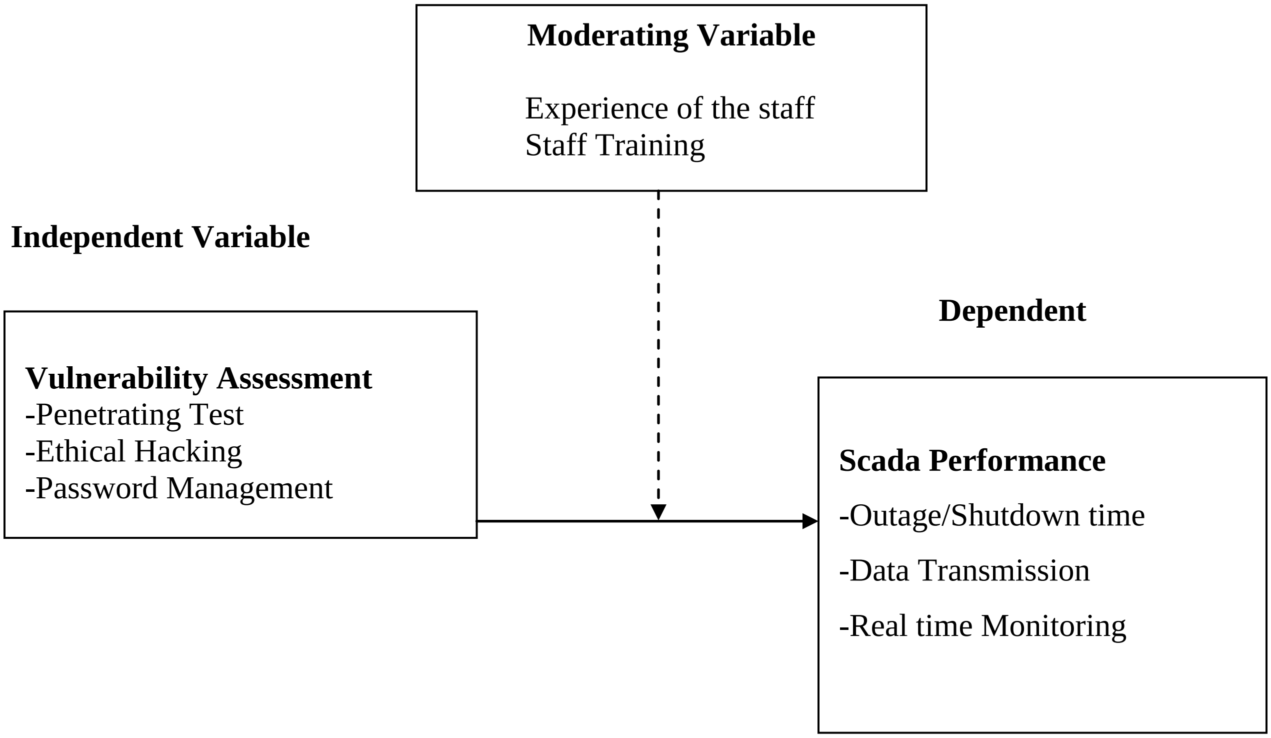


Figure 3.1: Conceptual Framework

(Author, 2016)

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

This chapter focuses on description of how the research was to be directed. It contained research design adopted by the study, target population of the study, sample scope, sampling formula, research instruments, validity of research tools, validity of research tools, collection of data collection measures as well as analysis of data systems.

3.2 Research Design

Crewell, (2009) defines; research designs are strategies and the actions for research that span the choices from abroad expectations to detailed procedures of data collection and investigation. According to Gay et al (2000), correlation research is research that involves collecting data in order to determine whether, and to what degree, a relationship exists between two or more quantifiable variables. This study focused on survey research in which the researcher selected a sample of respondents from the stated population and then administered a standardized questionnaire to them. According to Angus and Katona, (1953) survey research gives a capacity for wide application and broad coverage which hence makes the survey technique very useful. The goal was to provide the Researcher with in-depth evidence on what challenges, KenGen as an organization faces on vulnerability assessment and performance of the SCADA system. The case study was suitable research design as it carried out in-depth analysis of KenGen as a unit hence facilitated intensive study of the same.

3.3 Target population

According to Kantardzic, (2011), the whole of the observations with which were worried in statistical analysis, whether their number was limited or infinite, constituted what we call a population. Target population included KenGen ICT officers, Shift controllers and Technical Services. The ICT officers knowledgeable on the present status and threats, both internal and external. Shift controllers and Technical Services knowledgeable on restrictions of the system and possible areas of upgrading. Selected users conversant on difficulties faced by end users when using SCADA scheme.

The distribution of the targeted population was as given in Table 3.1 below.

AREA OF OPERATION	**No of Shift Controllers**	**No of ICT officers**	**No of Technical Services**
Eastern Hydros	**10**	**8**	**8**
Western Hydros	**10**	**8**	**8**
Geothermal	**10**	**8**	**8**
Thermal	**10**	**8**	**8**
Central Office, Operations	**6**	**4**	**6**
TOTAL	**120**		

Table 3.1: Target and Sample Population

3.4 Sample design

The complete population may not be easy to study therefore a sample has to be taken from the study population. Abayo & Oloko (2015) effectively used Yamane classical to obtain the sample size in their study; it is the classical this study embraced. According to the model,

$$n_s = \frac{N}{\left\{1 + N\left(e^2\right)\right\}}$$

Where $\mathbf{n_s}$ = Sample size; **N** = Population size;

e- Correctness level (at 0.90 confidence interval, e = 0.1)

Given N = 102, then;

$$\mathbf{n_s} = \frac{\mathbf{120}}{\mathbf{1 + 120(0.1^2)}}$$

= 55 Respondents

3.5 Research Instruments

The Researcher made use of questionnaire as a research tool. The questionnaire used planned questions that were modest and easy to understand. The unstructured inquiries were used to obtain in depth statistics from the respondents.

3.6 Data collection

The study depended on both on Primary and Secondary data in which secondary data previously existed in records.A structured questionnaire including of 3 sections was used to collect data for the study. The queries had variables which were measured in both interval and nominal scales. For interval measures, a 5-point Likert-scale (1 – “strongly agree” to 5 – “strongly disagree”) were used to measure respondents’ agreement with the concepts under investigation. Majority of the questions were close ended. After approval of the research proposal by the supervisor and the university panel, the Researcher got an approval from Human Resources Manager KenGen to conduct the research study. To ensure high response rate, the Researcher frequently did an email reminder to the respondents

3.7 Data Analysis

Analysis was done using descriptive statistics with choice of descriptive statistics being necessary for systematic summarizing of all the data to be collected. The Researcher used SPSS to aid in the analysis and for ease in the interpretation of the results. To determine the relationship between SCADA performance, Vulnerability assessment and experience of Staff, a simple regression model was used. The analyzed data was presented by use of frequency tables, percentages and charts including pie charts and bar graphs. The following regression model was used to determine Vulnerability Assessment and Performance of SCADA system at Kenya Electricity Generating Company.

$Y= a_0 +a_1 x_1+a_2 x_2+a_3x_3+e$ **…….. (Equation 1)**

Variable for:

y= SCADA Performance
x_1= Vulnerability Assessment.
x_2 = Experience of Staff in years.
x_3= Number of Staff Trained
a= Constant
e = Error

CHAPTER FOUR: ANALYSIS OF DATA, FINDINGS AND DISCUSSION

4.1 Introduction

The study was based on vulnerability assessment and performance of the supervisory controlled and data acquisition system at Kenya Electricity Generating Company limited, Kenya. Target population included KenGen ICT officers, Shift controllers and Technical Services. The ICT officers informed on the present status and threats, both internal and external. Shift controllers and Technical Services informed on limitations of the system and possible areas of improvement. Selected users informed on difficulties faced by end users when using SCADA system. The study sampled 55 respondents out of which 50 responded making response rate 90 percent.

4.2 The Demographic Information

The study enquired on the details of the respondents' background that included age of the respondent's gender, current position as well as highest academic qualification among others. This information aimed at testing the appropriateness of the respondent in answering the questions regarding the vulnerability assessment and performance of the supervisory controlled and data acquisition system at Kenya electricity generating company limited, Kenya.

4.2.1 Respondent Age Bracket

Researcher enquired on the age bracket of the respondents and the findings are presented on the Figure 4.1

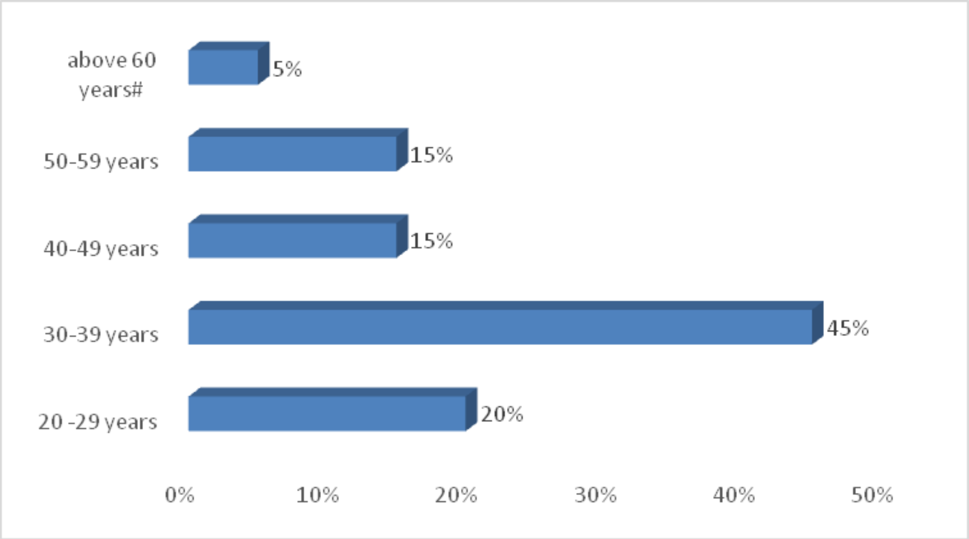


Figure 4.1 Respondent Age Bracket

From figure 4.1 45% of the respondents were of the age bracket of between 30-39 years,20% of were aged between 20-29 years, 15% of the respondent were in the age bracket of between 40-59 years while only 5% were aged above 60 years of age.

4.2.2 Respondents distribution by Gender

The study established the result of the respondent gender as presented in Figure 4.1

Table 4.1 Respondents Gender Distribution

Gender	frequency	Percentage

Male	40	80
Female	10	20
Total	**50**	**100**

From the study findings 80% of the respondents involved in this study were male while female respondents were 20% .The findings depicts that majority of the study participants in assessment of the Vulnerability of the SCADA system at KenGen were male.

4.2.3 Highest Education Qualification

The Researcher sought to find out the highest education qualification for the respondents. The findings are presented on the table.

Table 4.2 Highest Education Qualification

Education qualification	**Frequency**	**Percent**
High school or equivalent	1	2.0
Certificate	5	10.0
Diploma/higher diploma or equivalent	21	42.0
Degree	21	42.0
Masters	2	4.0
Total	**50**	**100.0**

From the study, majority of who responded had attained diploma/higher diploma or equivalent and degree academic qualification, these were represented by 42%, 10% had attained certificate education level, 4% had attained master’s degree academic qualification while only 2% high school or equivalent academic qualification. The finding shows that the study participants had attained adequate academic qualification in understanding the Vulnerability of the SCADA system at KenGen.

4.2.4 Respondents distribution by KenGen Business Area.

The Researcher enquired on the respondent's KenGen business area, the findings are presented on the Table 4.3

Table 4.3 Respondents distribution by KenGen Business Area

KenGen business area	Frequency	Percent
Eastern Hydros	13	26.0
Western Hydros	14	28.0
Central office operations	2	4.0
Kipevu	10	20.0
Total	**50**	**100.0**

According to the findings presented on the table 4.3 28% of the respondents were from western Hydros, 26% of the respondents were from Eastern Hydros, 20% of the respondents were from Kipevu while only 4% of the respondents came from central office operations.

4.2.5 Length of Service in KenGen

The study enquired on the length of service at KenGen, the findings are presented on the table 4.4

Table 4.4 Length of Service in KenGen

	Frequency	Percent
Less than 5 years	17	34.0
6-9 years	11	22.0
10-15 years	12	24.0
Above 16 years	10	20.0
Total	**50**	**100.0**

According to the findings presented on table 4.4 34% of the respondents had been in service for less than 5 years, 24% had been in service for period of between 10-15 years, 22% of the staff had been in service for a period of 6 to 9 years while only 20% had served for above 16 years. The findings shows that majority of respondents had adequate experience at KenGen company.

4.2.5 Period of time in use of SCADA System

The study enquired on the period of time the respondents had used the SCADA systems, the findings are presented on the figure 4.2.

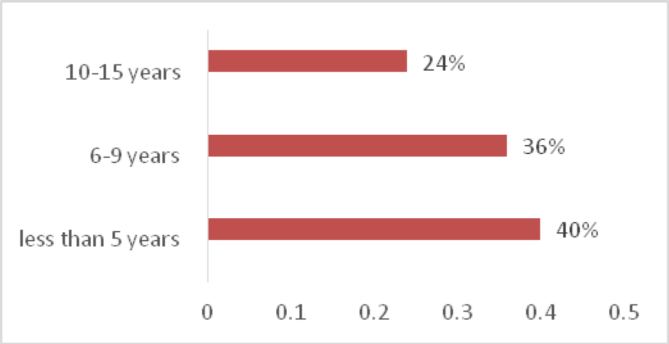


Figure 4.2 Period of time in use of SCADA System

According to the study findings 40% of the respondents had used SCADA System in the KenGen Company for the less than 5 years, 36% of the respondents has used SCADA System for a period of 6-9 years, while only 24% had used the SCADA System for a period of between 10-15 years. The findings demonstrate that KenGen staff involved in this study had used SCADA System for a long period of time.

4.3 Respondents Familiarity with Real Time Monitoring of SCADA

Respondents were requested to indicate their familiarity with real time monitoring of SCADA systems. The findings are presented on the figure 4.3

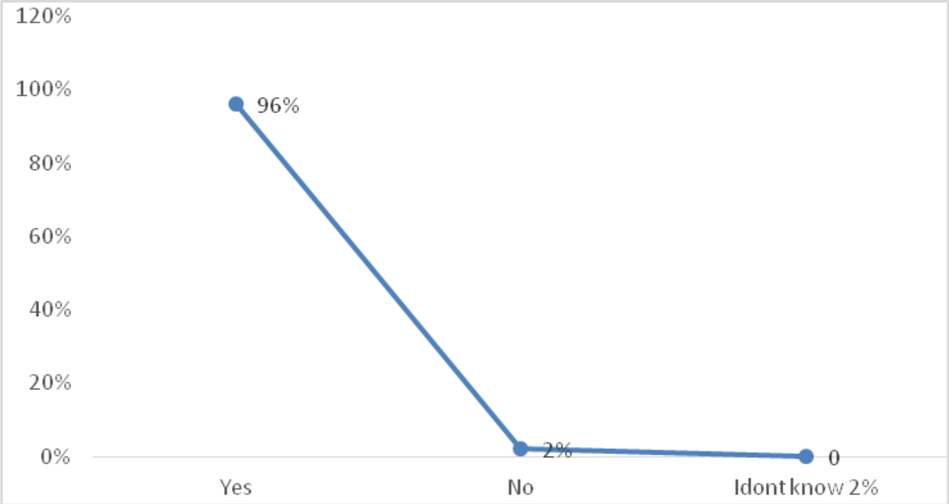


Figure 4.3 Respondents Familiarity with Real Time Monitoring of SCADA

Majority of who responded represented by 96% who were familiar with real time monitoring of SCADA systems, only 2% of the respondents indicated that they were not familiar with real time monitoring of SCADA systems, another 2% did not understand real time monitoring of SCADA systems. The findings reveal that KenGen staffs were very conversant with real time monitoring of SCADA systems in the plant.

4.3.1 Respondents Accessibility to Plant Information link from their Work Station

The study enquired on the respondent's accessibility to plant information link from their work station, the findings are presented on Figure 4.4

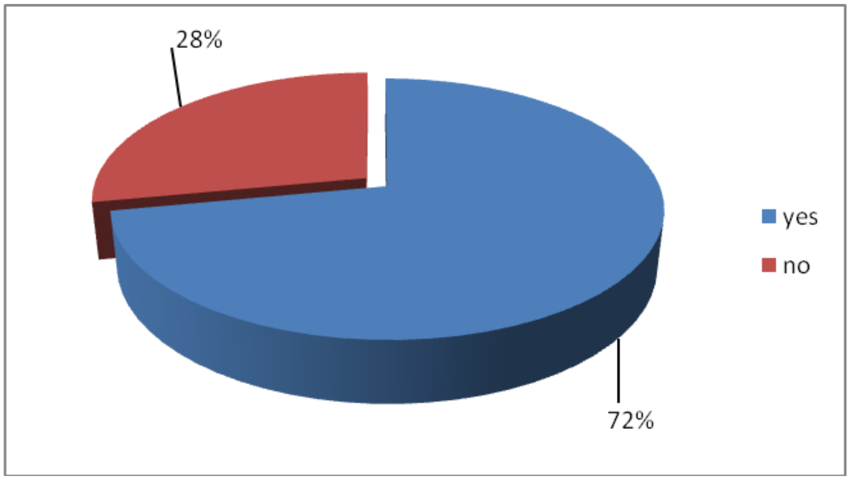


Figure 4.4 Respondents Accessibility to Plant Information link from their work station

From the finding of the study majority of the staff were represented by 72% presented on Table 4.4 indicated that they were accessible to plant information link from their work station, while only 28% of the respondents were not accessible to plant information link from their work station. The findings depicts that staff at the KenGen were accessible to plant information link from their work station.

4.3.3 Monitoring of Plant Parameters using SCADA

The Researcher enquired how often the respondents monitored Plant parameters using SCADA, the presentation of the findings are done as shown.

Table 4.5 Monitoring Plant Parameters using SCADA

Responses	Frequency	Percent
Never	3	6.0
Daily	34	68.0
After every 3 days	6	12.0
Weekly	5	10.0
Monthly	2	4.0
Total	**50**	**100.0**

From the study findings presented on the table 4.5, 68% of the respondents stated that monitoring of plant parameters using SCADA on daily basis, 12% indicated that they do the monitoring of plant parameters using SCADA after every 3 days, 10% indicated that they monitor on weekly bases,6% of the respondents never of plant parameters using SCADA, 2% of the responses did the monitoring on monthly bases. The findings depicts that monitoring of plant parameters using SCADA was being carried out on daily bases by KenGen plant officials.

4.3.4 Rate the Quantity of the Monitored Plant Parameters in SCADA

The Researcher enquired on the rate of quantity of monitored plant parameters in SCADA as per table 4.6

Table. 4.6 Rate the Quantity of the Monitored Plant Parameters in SCADA

Responses	Frequency	Percent
Inadequate	2	4.0
Moderate	10	20.0
Sufficient	38	76.0
Total	**50**	**100.0**

According to the study findings 76% of the respondents stated that the rate of the Quantity of the Monitored Plant Parameters in SCADA was sufficient, 20% of the response indicated that the quantity was moderate while only 4% were for opinion that the rate of the quantity of the Monitored Plant Parameters in SCADA was inadequate. The study reveals that the rate of the Quantity of the Monitored Plant parameters in SCADA was sufficient.

4.3.5 Rate of representation of data in the HMI (Human Machine Interface)

The study enquired on the rate of representation of data in the HMI (Human Machine Interface) and the findings are presented on figure 4.5

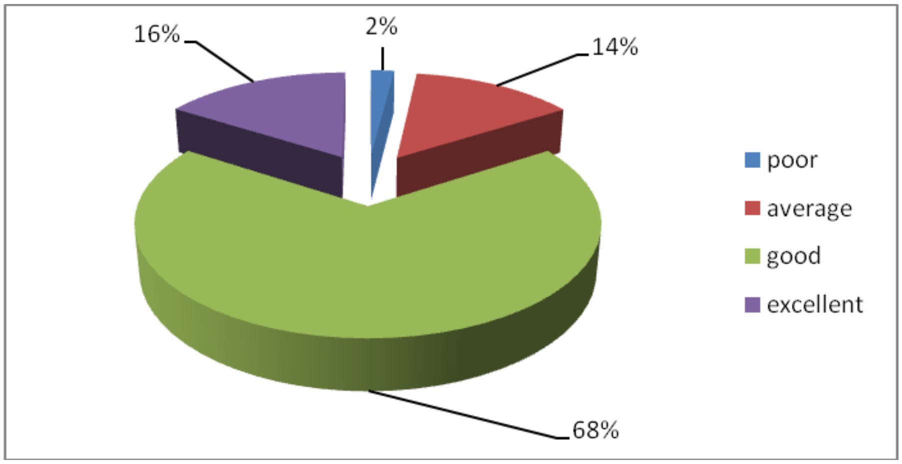


Figure 4.5 Rate of representation of data in the HMI (Human Machine Interface)

According to the study findings on figure 4.5, 68% of the respondents stated that rate of representation of data in the HMI (Human Machine Interface) was good, 16% of the response were for the opinion that the rate of representation of data in the HMI (Human Machine Interface) was excellent,14% of the respondents indicated that the rate of representation of data in the HMI was average while 2% of responses said that the rate of representation of data in the HMI (Human Machine Interface) was poor. The study concludes that the rate of representation of data in the HMI (Human Machine Interface) at the KenGen plants was good.

4.3.6 Rate Accuracy of the Parameters Monitored

The study enquired on the How the respondents rated accuracy of the parameters monitored, the response are presented on the table 4.7

Table 4.7 Rate Accuracy of the Parameters Monitored

Responses	Frequency	Percent
Poor	1	2.0
Average	2	4.0
Good	39	78.0
Excellent	8	16.0
Total	**50**	**100.0**

According to the study findings presented on table 4.7, 78% of the respondents indicated that the rate of accuracy of the Parameters Monitored was good, 16% indicated that the rate of accuracy of the parameters monitored was excellent, 4% said that the rate of accuracy of the parameters monitored was average while only 2% were for the opinion that the rate of accuracy of the Parameters Monitored was poor. The study findings depicts that the rate of accuracy of the Parameters Monitored was good in KenGen plant.

4.3.7 Monitoring of Real Time Plant parameters

The Researcher wanted to establish the purpose monitoring of real time plant parameters, the findings are presented on the table 4.8.

Table. 4.8 Real Time Monitoring of Plant Parameter

Responses	Frequency	Percent
Not aware	2	4.0
Plant maintenance	23	46.0
Troubleshooting	25	50.0
Total	**50**	**100.0**

From the study findings presented on table 4.8: 50 percent of who responded indicated that the purpose monitoring of real time plant parameters was for troubleshooting purposes, 46 percent said the purposes monitoring on real time of plant parameters was for plant maintenance while 4 percent of the respondents were not aware. The study reveals that the purpose of monitoring on real time of plant parameters was for troubleshooting purposes.

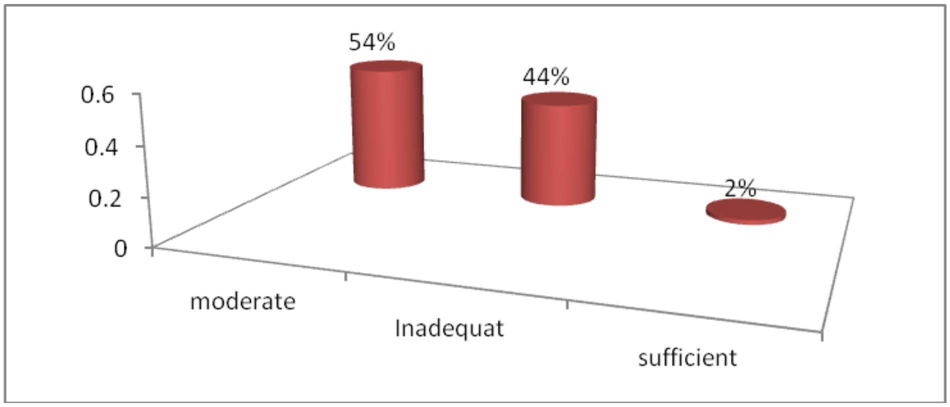


Figure 4.6 The rate of the historical archive of the parameter trends

According to the study findings presented on the figure 4.6: most of the respondents represented by 54% stated that the rate of historical archive of the parameter trends was moderate, 44% of the respondents said that the rate of the of historical archive of the parameter trends was sufficient, while 2% indicated that the rate the of historical archive of the parameter trends was inadequate. The study reveals that the rate of the historical archive of the parameter trends at KenGen plant was moderate.

4.4.1 Training on SCADA

The Researcher sought to find out whether the respondents had been trained on SCADA systems. The findings are presented on the table 4.9

Table 4.9 Training on SCADA

Responses	Frequency	Percent
Yes	29	58.0
No	21	42.0
Total	**50**	**100.0**

According to the study findings presented on table 4.9: 58 percent indicated that respondents had training on SCADA systems, 42 percent indicated that they had been trained on SCADA systems. The study reveals that they had been trained on SCADA systems and therefore they were able to understand vulnerability assessment and performance of SCADA System at KenGen plant.

4.4.2 SCADA System Training Level

The further sought to establish the training level in the SCADA systems, the responses are presented on the table 4.10

Table 4.10 SCADA System Training Level

Responses	Frequency	Percent
Basic User	26	52.0
As maintenance personnel	5	10.0
Non Applicable	19	38.0
Total	**50**	**100.0**

As per findings of table 4.10, 52 percent of the respondents indicated that they had attained basic user level of training, 38 percent mentioned that they were not trained at all while only 10 percent of the responses indicated that they had training as maintenance personnel. The study reveals that the level of training on SCADA system was very low and thus KenGen management ought to increase the SCADA training levels to improve vulnerability assessment and performance of SCADA System in the plant.

4.4.3 If you have not been trained, how have learnt using SCADA system

The study enquired how the respondents had learnt on how to use SCADA system if were not trained on how to use SCADA systems. The findings are presented on table 4.11

Table 4.11 if you have not been trained, how have you learnt how to use SCADA system

Responses	Frequency	Percent
From others	38	76.0
Training	12	24.0
Total	**50**	**100.0**

From the findings on table 4.11: majority indicated that respondents had learned on how to use SCADA from others, this represented 76% of the responses, only 24% had training on how to use SCADA systems. The findings reveal that the respondents had no formal training on the SCADA systems. The KenGen plant needs to invest more on their labour force to promote knowledge on the use of SCADA systems.

4.5.1 Whether you have Factory Default Password

The Researcher enquired on whether the respondents had factory default password, the findings are presented on table 4.12.

Table 4.12 Whether You Have Factory Default Password

Responses	Frequency	Percent
Yes	26	52.0
No	24	48.0
Total	**50**	**100.0**

The study findings presented, 52 percent of the responses indicated that KenGen plant has factory default password, 48 percent indicated that they do not have factory default password. The study finding reveals that the KenGen plant has factory default password.

4.5.2 How often do you change your SCADA Password

The Researcher sought to establish how often the KenGen plant changes their SCADA password. The findings are presented on Table 4.13

Table 4.13 How often do you change your SCADA Password

Responses	Frequency	Percent
Never	27	54.0
Rarely	19	38.0
Always	4	8.0
Total	**50**	**100.0**

From the findings presented, majority of those who responded 54 percent indicated that KenGen plant does not change their SCADA password, 38 percent of the respondents indicated that KenGen plant changes their SCADA password rarely, but 8 percent indicated that KenGen changes their SCADA password always.

4.5.3 Whether You Have Guest accounts for SCADA System

Study enquired on whether KenGen has got the guest accounts for SCADA system, the findings are presented on Table 4.14

Table 4.14 Whether You Have Guest accounts for SCADA System

Responses	Frequency	Percent
Yes	9	18.0
No	31	62.0
I don't know	10	20.0
Total	**50**	**100.0**

Majority of those who responded indicated that KenGen power plant does not have guest account for SCADA systems, this accounted for 62 percent of the responses,20 percent of the respondents did not know whether KenGen power plant do have guest account for SCADA system, 18 percent of the respondents indicated that KenGen do have guest accounts for SCADA systems.

4.5.4 Whether you have a Biometric System for Authentication

The research sought to establish whether KenGen have the biometric system for authentication, the Table 4.15 presents findings

Table 4.15 whether you have a Biometric System for Authentication

Responses	Frequency	Percent
Yes	7	14.0
No	40	80.0
Not applicable	3	6.0
Total	**50**	**100.0**

As from the study, KenGen plant does not have biometric system for authentication, this was represented by 80 percent, 14 percent of the respondents admitted that KenGen have got the biometric system for authentication while only 6 percent indicated that biometric system for authentication was not applicable to KenGen plants.

4.5.5 Integrity Checkers

The study enquired on whether KenGen has integrity checkers to monitor alternative of system files, the table 4.16 presents the findings

Table 4.16 Whether KenGen has Integrity Checkers to Monitor Alternatives of System Files

Responses	Frequency	Percent
Yes	13	26.0
No	37	74.0
Total	**50**	**100.0**

From the study findings majority of the respondents 74 percent indicated that KenGen plant does not have integrity checkers to monitor alternatives of system files while only 26 percent said that KenGen plant has got integrity checkers to monitor alternatives of system files. The findings depicts that KenGen plant does not have integrity checkers to monitor alternatives of system files.

4.6.1 Vulnerability Assessment

Policy and Procedure: The responses were rated on five point Likert scale where **SD** –1 Strongly Disagree; **D**-2 Disagree; **NS**-3 Not Sure **A-** 4 Agree; **SA-** 5 Strongly Agree,. The mean and the standard deviation were generated and presented as shown in the Table 4.17

Table 4.17 Policy and Procedure

Policy and Procedure	Mean	Std. deviation
KenGen implements adequate security policies for SCADA Systems.	4.06	0.210
KenGen implements adequate security training and awareness policies.	2.10	0.645
KenGen has adequate guidelines in SCADA systems hardware/equipment maintenance	3.48	1.034
KenGen has adequate policies for portable devices	4.46	0.102
KenGen conducts adequate periodic audits on the security enforcement policy	2.05	1.022
KenGen has an appointed person in charge to manage security policies and procedures.	3.08	1.035

From Table 4.17 ,those who responded agreed that KenGen has adequate policies for portable devices as represented by mean of 4.460, further respondents agreed that KenGen implements adequate security policies for SCADA Systems, KenGen has adequate guidelines in SCADA systems hardware/equipment maintenance this was represented by mean of 3.48 and 4.06 respectively. Respondents were not sure on whether KenGen had a person appointed to manage and be in charge of procedure and policies as indicated via a mean of 3.08.however respondents disagreed on the statement that KenGen conducts adequate periodic audits on the security enforcement policy and that KenGen conducts adequate periodic audits on the security enforcement policy as presented by mean of 2.05 and 2.10 respectively.

4.6.2 Software Vulnerabilities

Software Vulnerabilities: The responses were rated on five point Likert scale where **SD** –1 Strongly Disagree; **D**-2 Disagree; **NS**-3 Not Sure **A**- 4 Agree; **SA**- 5 Strongly Agree,. The mean and standard deviation were generated and presented as shown in the Table 4.18

Table 4.18 Software Vulnerabilities

Software Vulnerabilities	**Mean**	**Std. deviation**
KenGen periodically updates software.	4.20	0.042
The protocols (i.e. Modbus, Profibus, etc.) used in KenGen are secured	4.00	0.048
There are controls implemented to access unauthorized applications in the system.	4.56	0.045

Adequate level of access controls on configuration and programming software are implemented.	3.09	0.562
KenGen keeps track and ensure that all logs are maintained.	3.25	0.548

As per Table 4.18, respondents agreed strongly that there are controls implemented to access unauthorized applications in the system presented by average of 4.56,the agreement by respondents was that KenGen periodically updates software and that the protocols (i.e. Modbus, Profibus, etc. used in KenGen as shown by mean of 4.20 and 4.00 respectively. Respondent were further not sure on the statement that Adequate level of access controls on configuration and programming software are implemented and that KenGen keeps track and ensure that all logs are maintained as shown by mean 3.0 consecutively.

4.6.3 Hardware Vulnerabilities

Hardware Vulnerabilities: The responses were rated on five point Likert scale where **SD** –1 strongly Disagree; **D**-2 Disagree; **NS**-3 Not Sure **A-** 4 Agree; **SA-** 5 Strongly Agree, The mean and the standard deviation were generated and presented as shown in the Table 4.19

Table 4.19 Hardware Vulnerabilities

Hardware vulnerabilities	**Mean**	**Std. deviation**
KenGen physically secure network related equipment’s	3.000	0.095
KenGen physically secure network ports	3.312	0.089

KenGen has a backup plan for network’s hardware in case of loss of power	4.431	0.0460

According to the study findings presented in Table 4.19, respondents agreed that KenGen has a backup plan for network’s hardware in case of loss of power as shown by mean 4.431, however respondents were sure on the statement KenGen physically secure network ports and that KenGen physically secure network related equipment’s as shown by mean score 3.3 and 3.0 respectively.

4.6.3 Technical Controls

Table 4.20 Technical Controls

Technical controls	**Mean**	**Std. deviation**
KenGen verifies users, process in the SCADA system	4.360	0.340
KenGen has controls that grants access to SCADA system’s hardware and software	4.000	0.251
KenGen conducts independent reviews and examinations the SCADA system controls	4.944	0.236
KenGen implements a mechanism to protect system and data transmission components within the environment	3.401	1.003

As per the study findings presented in Table 4.19, respondents agreed that KenGen has a backup plan for network’s hardware in case of loss of power as shown by mean 4.431, however respondents were sure on the statement KenGen physically secure network ports and that KenGen physically secure network related equipment's as shown by mean score 3.3 and 3.0 respectively.

4.6.4 Configuration Vulnerabilities

Table 4.21 Configuration Vulnerabilities

Configuration Vulnerabilities	**Mean**	**Std. deviation**
How Data is are stored in external drives protected.	4.067	1.834
KenGen's operating systems requires passwords to access.	4.970	1.951
The operating system password is strong, not shared and has administration privileges	4.000	1.908

From the study findings in table 4..21 the respondents agreed strongly KenGen's operating systems requires passwords to access as evidenced by the mean of 5.00, Data stored in external drives and protected and that the operating system password is strong, with administration rights shown by mean 4.067 and 4.000 respectively.

4.7.0 Correlation Analysis

The data presented before on vulnerability assessment, experience of staff in years, and numbers of staff trained were done by use of per factor single variables which was obtained by the mean of each factor. The study used a 95% confidence level interval for Pearson's correlations analysis As per table below shows the correlation matrix for the factors of vulnerability assessment, experience of staff in years, and numbers of staff trained and SCADA Performance. Positive SCADA Performance relationship and vulnerability assessment, experience of staff in years, and numbers of staff trained of magnitude 0.894, 0.493, and 0.661 respectively. There was correlation among the factors and the SCADA Performance. Vulnerability assessment has the greatest value and experience of staff in years resulting to low value of correlation.

Other factors that were examined with p-value (p<0.05) at 95% confidence level. Relationship values of SCADA performance and vulnerability assessment, experience of staff in years, and numbers of staff trained values were 0.018, 0.031, and 0.024 respectively. This indicated that vulnerability assessment was the most significant factor, followed by experience of staff in years while numbers of staff trained was the least significant.

Table 4.22 Correlation Matrix

	SCADA performance	Vulnerability assessment	Experience of staff in years	Numbers of staff trained
SCADA performance (r) (p) Sig. (2 tailed)	1.000			
vulnerability assessment (r) (p) (2 tailed)	0.894 0.018	1.000		
experience of staff in years	0.493	0.316	1.000	

(r)	0.0321	0.047		
(p) Sig. (2 tailed)				
numbers of staff trained (r)	0.661	0.163	0.216	1.000
(p) Sig. (2 tailed)	0.024	0.019	0.047	

4.7.1 Regression Analysis

Multiple regression was conducted by the testing the relationship between independent variables of the at SCADA performance KenGen. Coefficient of determination showed how changes of the dependent variable changed the independent variables of SCADA performance at KenGen) which is elaborated all the three independent variables (vulnerability assessment, experience of staff in years, and numbers of staff trained).

4.7.2 Model Summary

The three independent variables that were studied showed only 84.5% of SCADA performance at KenGen represented by the R^2. This translated to other factors not studied in this research contributed 15.5% of the SCADA performance at KenGen. Therefore further research can be done on other factors (15.5%) that affect SCADA performance at KenGen in Kenya.

Table 4.23 Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.919	0.845	0.789	0.6273

Source: Research, 2016

4.7.4 ANOVA Results

The significance rate is 0.0179 which is lesser than 0.05.This means that vulnerability assessment, experience of staff in years, and numbers of staff trained has a small relationship in forecasting how SCADA affect performance at KenGen in Kenya. The F critical at 5% level of significance was 3.23. Since F calculated is greater than the F critical (value = 9.475), this shows that the general model was significant.

Table 4.24 ANOVA

Model	**Sum of Squares**	**df**	**Mean Square**	**F**	**Sig.**
Regression	2.534	6	1.267	9.475	.0179[a]
Residual	9.307	44	2.327		
Total	**3.465**	**50**			

4.7.5 Coefficient of Determination

SCADA performance relationship was determined by use of multiple regression analysis at KenGen in Kenya using the three variables. The predictor model, using the standardized beta coefficients shown in table 4.25, is as follows below is the SPSS generated equation with organisation performance being the dependant variable.

Y = $\beta_0 + \beta_1X_1 + \beta_2X_2 + \beta_3X_3 + \varepsilon$) becomes

$Y= 1.147+ 0.752X_1+ 0.487X_2+ 0.545X_3$

From the regression calculation factoring vulnerability assessment, experience of staff in years, and numbers of staff trained) constant at zero, SCADA performances at KenGen was 1.147. It was evident that all additional independent variables at nil, any raise in vulnerability assessment resulted to 0.752 increment in SCADA performances at KenGen. Also any increase in Experience of staff in years resulted in 0.487 increase in SCADA performances at KenGen, a unit increase in numbers of staff trained translated to an increase of 0.545 in SCADA performances at KenGen.

This concludes that vulnerability assessment contribute most to the SCADA performances at KenGen followed by experience of staff in years. With 5% level of significance and 95% level of confidence, vulnerability assessment had a 0.0192 level of significance, experience of staff in years showed a 0.0269 level of significance, numbers of staff trained showed a 0.0251 level of significance, therefore the most significant SCADA performances factor was vulnerability assessment which constituted; Penetrating test, Ethical hacking and Password Management.

Table 4.25 Determination of Coefficient

		Standardized Coefficients			
Model		**Beta**	**Std. Error**	**t**	**Sig.**
1	Constant	1.147	1.2235	1.615	0.367
2	Vulnerability Assessment	0.752	0.1032	4.223	.0192
3	Experience of staff in years	0.487	0.3425	3.724	.0269
4	Numbers of staff trained	0.545	0.2178	3.936	.0251

4.8 Discussion of the Findings

The study revealed that Vulnerability Assessment and Performance of SCADA in KenGen is essential to assess how organizations method information sharing inside the organization. In order to safeguard the security requirements of a company are addressed, this study focused on gauging how the organizations’ data security goals are attained based on the components used from Integrated System Theory as stated by Igure et al., (2006) in determining the safety requirements of an organization.

The study also indicated that SCADA system availed a mechanism to prevent compromised or unauthorized access to company information thereby protecting company vulnerability. Implementing safety policies is indispensable in organizations, particularly organizations dealing with essential services. Safety procedure is precise guidelines of what not allowed system's safety as stated by Stouffer et al. (2011) and Bishop (2003).Susceptibilities in a SCADA scheme could happen as result of negligence of dangers, misconfigurations, lowly conservation on the bases of hardware, functioning schemes as well as applications. Danger valuation helps to recognize measure and rank dangers alongside standards for threat approval plus aims applicable to the organization, precisely to users of SCADA schemes. This results in risk valuation that can result in identified action essential to management of the information safety threat to the SCADA as stated by Ismail et al. (2014).

Another significant constituent of Integration System Theory (IST) is regulating and auditing theory this proposes that the performance of every organization depends on the setting of their security systems as stated by (Hong et al., 2003). Control can address avoidance. Stouffer at al. (2011) outlined that with put controls like management, functioning and technical controls this guards the confidentiality, honesty and availability of the scheme and its related data. The performance of every organization depends on the setting of their security systems as stated by (Hong et al., 2003). Management system theory informed the study since contingency approach has been applied to password management; integrity checkers and Ethical hacking. By application of SCADA system

KenGen has controlled and assisted in recognizing the cause of a problem, correcting a looming fault and observing the status of the field devices including the plant itself. This theory enlightens the study since it highlighted that an organization should create and maintain a known information security administration system to control and guard information assets. ISMS comprise six steps of describing the policy, describing the scope of ISMS, undertaking risk valuation and managing the risk and lastly selecting control aims. (BSI, 1999).

Finally from the Empirical research of the Korean Securities Industry through Heekyung Kong, Insung Lee, Suhyun Jung, as well as Seung-Jun Yeon, (2014). This study suggested a model by which investment and actions related to IT service structure, information sharing, as well as information security was established. From the findings of this study KenGen is using data to support the impartiality and validity of the existing information security investment.

CHAPTER FIVE: SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This chapter presents the summary of findings, discussion, conclusion drawn from the findings and recommendations made. The conclusions and recommendations drawn focus on the purpose of the study.

5.2 Summary of Findings

This study sought to investigate Vulnerability assessment influences organizational performance at Kenya Electricity Generating Company. The exploration was guided by the following objectives determine the extent to which the SCADA system is vulnerable, establish the challenges of performing a vulnerability assessment on the SCADA system and to determine the link between vulnerability assessment and performance of the SCADA system.The study used regression analysis to find the association between factoring vulnerability assessment, experience of staff in years, and numbers of staff trained and SCADA performances at KenGen. The study found out that majority of the users was aware about Vulnerability Assessment and that they were playing a significant role in protecting the SCADA system.

The study findings depicts that the rate of accuracy of the Parameters Monitored was good in KenGen plant. 50 percent of the respondents indicated that the purpose monitoring of real time plant parameters was for troubleshooting purposes, Majority of the respondents represented by 54% indicated that the rate of historical archive of the parameter trends was moderate. Study found out that vulnerability assessment contribute most to the SCADA performances at KenGen followed by experience of staff in years. vulnerability assessment had a 0.0192 level of significance, experience of staff in years showed a 0.0269 level of significance, numbers of staff trained showed a 0.0251 level of significance, therefore the most significant SCADA performances factor was vulnerability assessment which constituted; Penetrating test, Ethical hacking and Password Management.

Focusing on SCADA Training the study findings, 58 percent of the respondents indicated that they had not been trained on SCADA systems. In address to SCADA Password management the study findings, 52 percent indicated that KenGen plant has factory default password, majority of the respondents 54 percent indicated that KenGen plant does not change their SCADA password.

Finally for Vulnerability Assessment, KenGen has adequate policies for portable devices and KenGen implements adequate security policies for SCADA Systems, adequate guidelines in SCADA systems hardware/equipment maintenance. Respondents disagreed on the statement that KenGen conducts adequate periodic audits on the security enforcement policy.

5.3 Conclusion

The study made the following conclusions, majority of the study participants in assessment of the Vulnerability of the SCADA system at KenGen were male. The study participants had attained adequate academic qualification in understanding the Vulnerability of the SCADA system at KenGen. Staff involved in this study had used SCADA System for a long period of time, and that they were very conversant with real time monitoring of SCADA systems in the plant. They were also accessible to plant information link from their work station. Monitoring of plant parameters using SCADA was being carried out on daily bases by KenGen plant staff.

The rate of representation of data in the HMI (Human Machine Interface) at the KenGen plant was good. The staff had been trained on SCADA systems and therefore they were able to understand vulnerability assessment and performance of SCADA System at KenGen plant .The rate of the historical archive of the parameter trends at KenGen plant was moderate. The training on SCADA system was very low and thus KenGen management ought to increase the SCADA training levels to improve vulnerability assessment and performance of SCADA System in their plant. Respondents had no formal training on the SCADA systems.

The KenGen plants need to invest more on their labour force to promote knowledge on the use of SCADA systems. KenGen has adequate policies for portable devices. Further respondents agreed that KenGen implements adequate security policies for SCADA Systems; KenGen has adequate guidelines in SCADA systems hardware/equipment maintenance. KenGen does not conduct adequate periodic audits on the security enforcement policy. The most significant SCADA performances factor was vulnerability assessment which constituted; (Penetrating test, Ethical hacking and Password Management.

5.4 Recommendation for Practice and Policy

The training on SCADA system was found to be very low, thus KenGen management ought to facilitate training for all SCADA users. This will increase the awareness on vulnerability and performance of SCADA System.

There is need to introduce a password management policy on SCADA System to enhance security. The study established that most of the passwords are factory default thus increase vulnerability of SCADA system.

Study found out that KenGen does not conduct adequate SCADA systems periodic audits on the security enforcement policy. Thus the study recommends that the management of KenGen should be conducting adequate SCADA systems periodic audits on the security enforcement policy.

5.4 Limitations of the Study

The following were the limitations of the study the sample of the respondents were drawn from some selected sections KenGen staff , the effects found were mainly reflective of the situations in particular sections. Hence the findings may not have been representative of all staff in KenGen power plants the study also limited itself to vulnerability assessment and performance of the supervisory controlled and data acquisition system at Kenya Electricity Generating Company limited, Kenya since there many factors that could influence vulnerability assessment and performance of the supervisory controlled and data acquisition system.

The study had a number of limitations. Respondents were at first fearful about giving out information since they were unsure where the information was to be used. Financial constrain was another factor that affected my research, since one had to keep on calling the users to remind them and also moving from one area to another in order to collect the questionnaire. Thirdly the research only factored KenGen as company which is among the users of SCADA system. A wider research to other users could have given more detailed findings.

5.6 Suggestion for Further Research

Since this study was on the vulnerability assessment and performance of the supervisory controlled and data acquisition system study suggests that similar study can be done to other related parastatals in Kenya using SCADA system in purposes of comparison and allowing the generation of the findings on the vulnerability assessment and performance of the Supervisory Controlled and Data Acquisition systems.

REFERENCES

Bruce Li, P.Eng, (2007). "*SCADA application in water and waste water industry*" Declan IWS, pp 81-83.

Creery and E Byres,(2007) "Industrial Cyber-security for power system and SCADA networks", *IEEE Industry Application*, vol. 13, no. 4, pp. 49-55.

Chandia R, J Gonzalez, T Kilpatrick, M Papa and S Shenoi,(2011) "Security Strategies for Scada Networks", *Proceeding of the First Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection*.

Davis CM, J E Tate, H Okhravi, C Grier, T J Overbye and D Nicol, (2006) "SCADA Cyber Security Testbed Development", *Proceedings of the Power Symposium*, pp. 483-488.

Holm H, T. Sommestad, and M. Ekstedt, (2012) *Vulnerability assessment of SCADA systems*.

Industry Applications Magazine, (2003).McClanahan, *SCADA and IP: is network convergence really here"*

Johansson E, T. Sommestad, and M. Ekstedt,(2008) "Security Isssues For SCADA Systems within Power Distribution," in *Proceedings of Nordic Distribution and Asset Management Conference (NORDAC)*.

Mander, F Nabhani, L Wang and R Cheung, (2007) "Data Object Based Security for DNP3 Over TCP/IP for Increased Utility Commercial Aspects Security", *Proceedings of the Power Engineering Society General Meeting*, pp. 1-8

McClanahan, *SCADA and IP: is network convergence really here*? Industry Applications Magazine, 2003.

Medida S, Sreekumar, N, Prasad, K.V, *SCADA-EMS, (1998)"on the Internet, Energy Management and Power Delivery*, Pages: 656-660 vol.2.

Miklovic, D.T. (1992) *Real time control networks for batch and process industries.*

Majdalawieh,F, F, F Parisi-Presicce and D Wijesekera,(2009) "Distributed Network Protocol Security (DNPSec) security framework", *Proceedings of the 21st Annual Computer Security Applications Conference*.

Nai Fovino, A Carcano and M Masera,(2009) "A secure and Survivable Architecture for SCADA Systems", *Proceedings of the Second International Conference on Dependability*

Nai Fovino, A Carcano, M Masera, (2003), “proceedings *of the 24th IEEE Int. Conference on Advanced Information Networking and Applications*

Nai Fovino, A Carcano, M Masera and A Trombetta,(2008) "Scada Malware, a proof of concept", *Proceedings of the 3rd International Workshop on Critical Information Infrastructures Security*, pp. 211-222.

Power Engineering Society Winter Meeting,(2000). *Intranet-based SCADA (supervisory control and data acquisition system) for power system,*

Rune GUST A VSSON, (2000) "*Sustainable virtual utilities based on Microgrids*", School of Engineering, Blekinge Institute of Technology Ronneby, SE-372 25, Sweden

Sommestad, G. Ericsson, and J. Nordlander,(2009) “SCADA *System Cyber Security* .

T Mander, F Nabhani, L Wang and R Cheung, "Data Object Based Security for DNP3 Over TCP/IP for Increased Utility Commercial Aspects Security", *Proceedings of the Power Engineering Society General Meeting*, pp. 1-8

Sommestad, G. Ericsson, and J. Nordlander, (2009) “SCADA *System Cyber Security*.

Walski, Thomas M., et. al (2003) *Advanced Water Distribution Modeling and Managemen*

APPENDICES

Appendix I

Letter of Transmittal

Gitonga James Muriithi

D61/64756/2013

Dear Respondent,

Re: Academic Research

I am Gitonga James Muriithi, a student at the University of Nairobi. I am conducting a research on "**Vulnerability Assessment and Performance of SCADA in KenGen, Kenya"**. The research is in partial fulfillment of the requirements for the award of Masters of Business Administration of the University of Nairobi.

You have been randomly selected to participate in this research as a respondent, and this participation is entirely on voluntary basis. Please provide responses to every question in the questionnaire.

I assure you that your responses will be treated with outmost confidentiality and will not be used for any other purposes other than the intended research work. Please take your moment and answer the following questions.

For any Clarifications please contact me on E-mail jgitonga@KenGen.co.ke or jamtos@gmail.com or Cell Phone: 0723-263253

I thank you for your support and cooperation.

Appendix II

Research Questionnaire for Vulnerability Assessment and Performance of SCADA System.

Instructions

Please answer the questions to the best of your knowledge.

Write your responses in the space provided.

Please put a tick (✓) where appropriate.

Section A: Demographic Information

1. What is your Age group?

20-29 Years: ( ) 30-39 Years: ( ) 40-49 Years ( ) 50-59 Years ( ): Above 60 Years ( )

2. What is your gender?

Female: ( ) Male: ( )

3. What is the highest level of education you have attained?

High school or Equivalent: ( )

Certificate: ( )

Diploma/ Higher diploma or equivalent: ( )

Degree: ( )

Masters: ( )

Doctorate: ( )

4. In Which KenGen Business Area are you based? Choose one

Olkaria ( )

Eastern Hydros ( )

Western Hydros ( )

Central Office Operations ( )

Kipevu ( )

5. Length of Service in KenGen

Less than 5 Years ( ): 6-9 Years ( ) 10 -15 Years: Above 16 Years ( )

6. How long have used SCADA System?

Less than 5 Years ( ): 6-9 Years ( ) 10 -15 Years ( ): Above 16 Years ( )

Section B: SCADA Performance

1. Are you familiar with real time monitoring of SCADA?

Yes: ( )   No: ( )   I don't Know ( )

2. Do you have an access to Plant Information link from your work station?

Yes: ( )   No: ( )

3. How often do you monitor Plant parameters using SCADA?

Never: ( )   Daily: ( )   After every 3 days: ( )   Weekly: ( )   Monthly: ( )

4. How do you rate the quantity of the monitored plant parameters in SCADA?

Inadequate: ( )   Moderate: ( )   Sufficient: ( )

5. How do you rate representation of data in the HMI (Human Machine Interface)?

Poor: ( )   Average: ( )   Good: ( )   Excellent: ( )

6. How do you rate accuracy of the parameters monitored?

Poor: ( )   Average: ( )   Good: ( )   Excellent: ( )

7. What is the purpose of real time monitoring of plant parameters?

Not aware: ( )   Plant maintenance: ( )   Troubleshooting: ( )

8. How do you rate the historical archive of the parameter trends?

Inadequate: ( )   Moderate: ( )   Sufficient: ( )

Section C: Training on SCADA system

1. Have you been trained on SCADA?

   Yes: ( )   No: ( )

2. What was the level of the training?

   Basic User: ( )   As maintenance personnel: ( )   Programmer: ( )

3. Has the training helped in learning how to use SCADA system?

   Yes: ( )   No: ( )

4. If you have not been trained, how have you learnt how to use SCADA system?

   …………………………………………………………………………………………

   …………………………………………………………………………………………

   …………………………………………………………………………………………

5. How do you rate the training?

   Inadequate: ( ) Moderate: ( ) Sufficient: ( )

(v) SCADA Password Management

1. Do you still have Factory Default Password?

   Yes: ( ) No: ( ) Not Applicable: ( )

2. How often do you change your SCADA Password?

   Never ( ): Rarely ( ); Always ( )

3. Do you have a Guest accounts for SCADA System?

   Yes: ( ) No: ( ) I don't Know ( )

4. Do you have a biometric system for authentication?

   Yes: ( ) No: ( ) Not Applicable: ( )

5. Do you have Integrity Checkers to monitor alternatives of system files?

   Yes: ( ) No: ( )

6. What is the age of the SCADA Password?

   Weekly: ( ) Fortnight: ( ) Monthly: ( ) More than a Month: ( )

<u>Section D: Vulnerability Assessment</u>

Kindly tick where applicable

Key: **SD** – Strongly Disagree; **D**-Disagree; **A**-Agree; **SA**-Strongly Agree, **NS**- Not Sure

(i) Policy and Procedure

No		**SD**	**D**	**A**	**SA**	**NS**
i	KenGen implements adequate security policies for SCADA Systems.					
ii	KenGen implements adequate security training and awareness policies.					
iii	KenGen has adequate guidelines in SCADA systems hardware/equipment maintenance					
iv	KenGen has adequate policies for portable devices					
v	KenGen conducts adequate periodic audits on the security enforcement policy					
vi	Who Manages KenGen Security policies and procedures.					

(ii) Software Vulnerabilities

No		SD	D	A	SA	NS
i	KenGen periodically updates software.					
ii	The protocols (i.e. Modbus, Profibus, etc.) used in KenGen are secured					
iii	There are controls implemented to access unauthorized applications in the system.					
iv	Adequate level of access controls on configuration and programming software are implemented.					
v	KenGen keeps track and ensure that all logs are maintained.					

(iii)Hardware Vulnerabilities

No		SD	D	A	SA	NS
i	KenGen physically secure network related equipment's.					
ii	KenGen physically secure network ports.					
iii	KenGen has a backup plan for network's hardware in case of loss of power.					

(iv) Technical Controls

No		SD	D	A	SA	NS
i	How does KenGen controls and verify users in the SCADA system.					
ii	What KenGen Control for SCADA system's hardware and software are in place?					
iii	Does KenGen conduct examinations to enhance system controls?					
iv	KenGen implements a mechanism to protect system and data transmission components within the environment.					

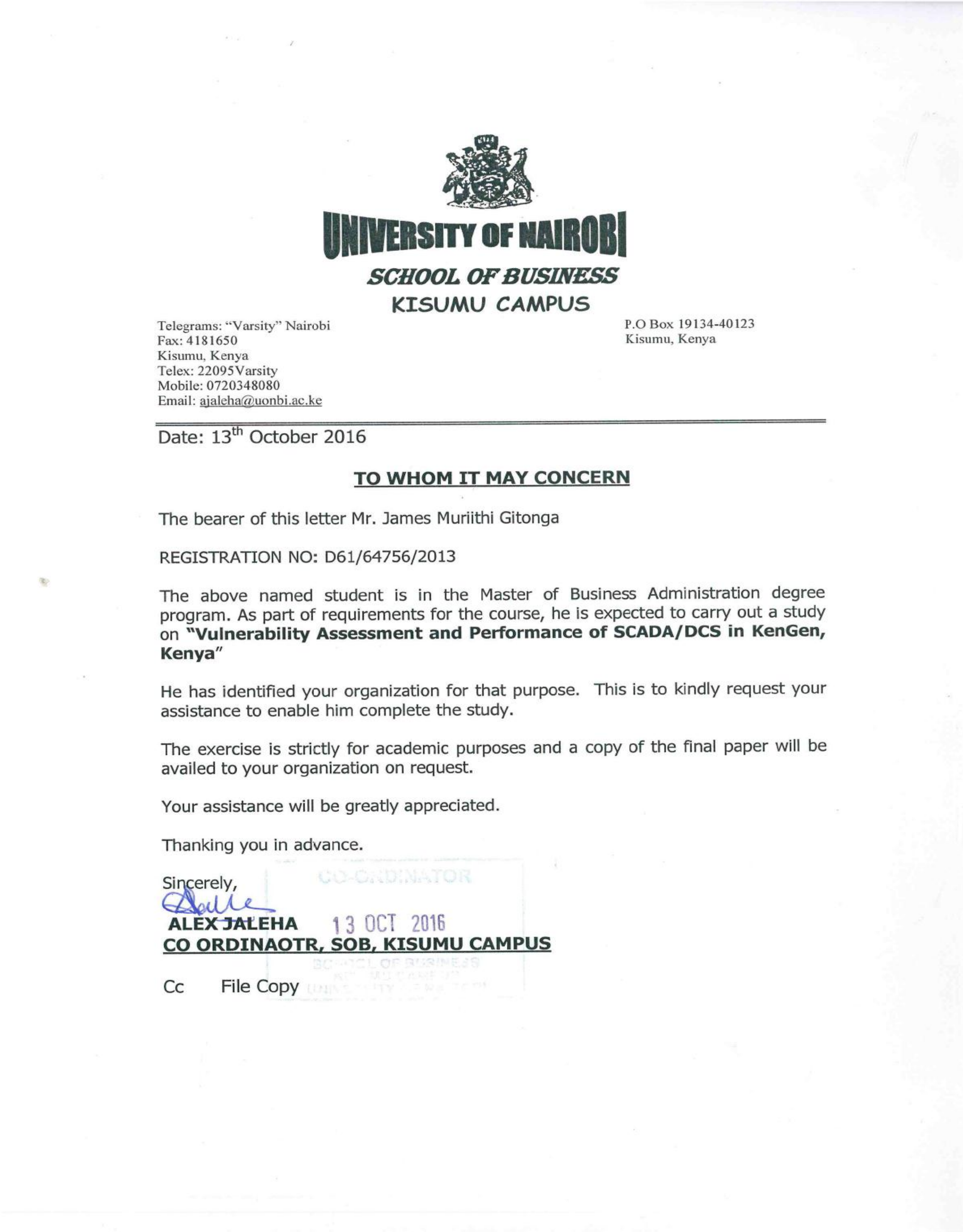
(v) Configuration Vulnerabilities

No		SD	D	A	SA	NS
i	How the protection of Data is are stored in External drives.					
ii	KenGen’s operating systems requires passwords to access.					
iii	How is the strength of Operating system password?					

Appreciation for Your Contribution

You have come to the end of the end of the questionnaire. I highly appreciate for taking your moment to fill this questionnaire. Thank you for the valuable support.

Appendix III



UNIVERSITY OF NAIROBI
SCHOOL OF BUSINESS
KISUMU CAMPUS

Telegrams: "Varsity" Nairobi
Fax: 4181650
Kisumu, Kenya
Telex: 22095Varsity
Mobile: 0720348080
Email: ajaleha@uonbi.ac.ke

P.O Box 19134-40123
Kisumu, Kenya

Date: 13th October 2016

TO WHOM IT MAY CONCERN

The bearer of this letter Mr. James Muriithi Gitonga

REGISTRATION NO: D61/64756/2013

The above named student is in the Master of Business Administration degree program. As part of requirements for the course, he is expected to carry out a study on **"Vulnerability Assessment and Performance of SCADA/DCS in KenGen, Kenya**"

He has identified your organization for that purpose. This is to kindly request your assistance to enable him complete the study.

The exercise is strictly for academic purposes and a copy of the final paper will be availed to your organization on request.

Your assistance will be greatly appreciated.

Thanking you in advance.

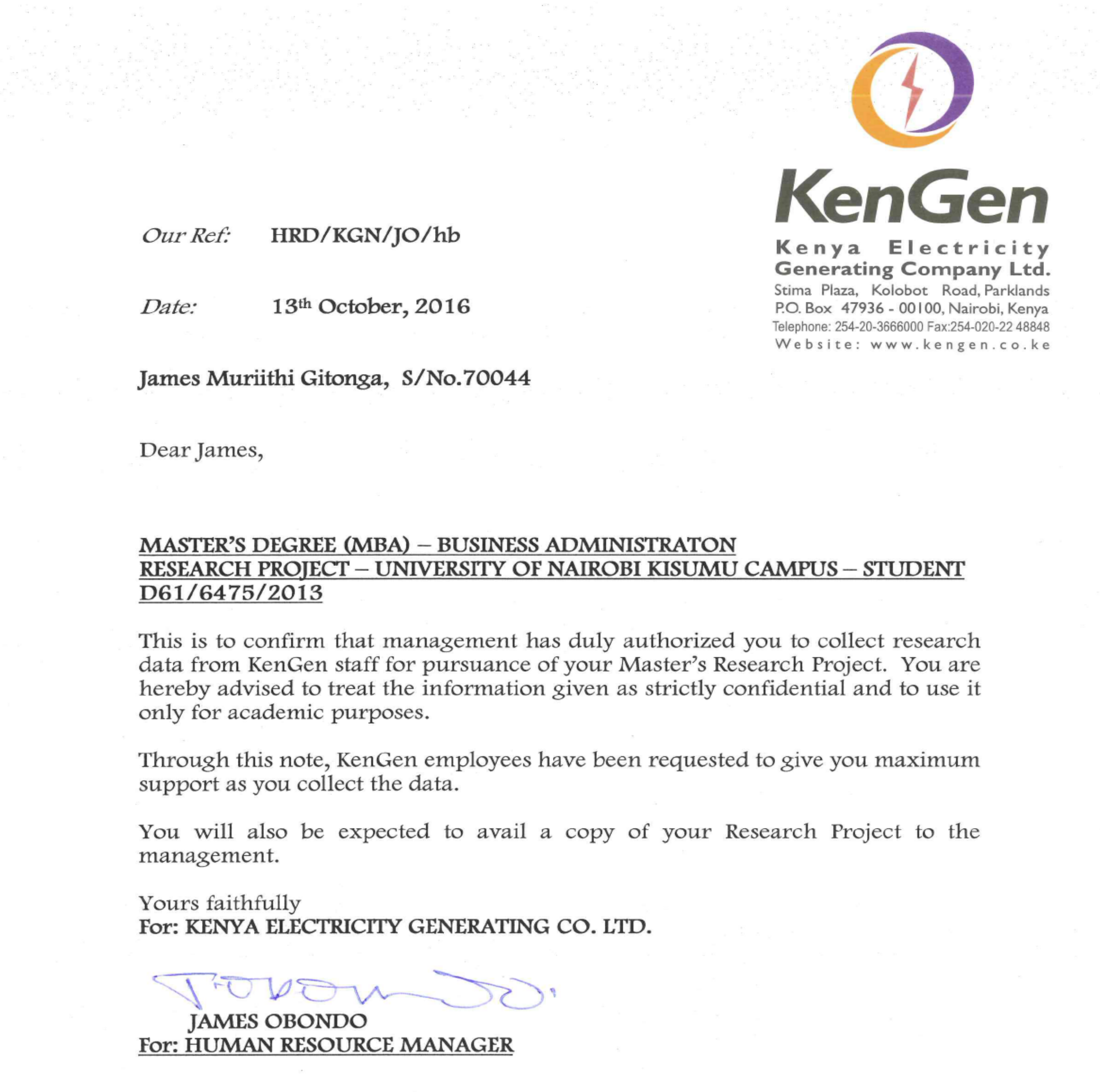
Sincerely,

ALEX JALEHA
CO ORDINAOTR, SOB, KISUMU CAMPUS

CO-ORDINATOR
13 OCT 2016
SCHOOL OF BUSINESS
KISUMU CAMPUS
UNIVERSITY OF NAIROBI

Cc File Copy

Appendix IV



KenGen
Kenya Electricity
Generating Company Ltd.
Stima Plaza, Kolobot Road, Parklands
P.O. Box 47936 - 00100, Nairobi, Kenya
Telephone: 254-20-3666000 Fax:254-020-22 48848
Website: www.kengen.co.ke

Our Ref: HRD/KGN/JO/hb

Date: 13th October, 2016

James Muriithi Gitonga, S/No.70044

Dear James,

MASTER'S DEGREE (MBA) – BUSINESS ADMINISTRATON RESEARCH PROJECT – UNIVERSITY OF NAIROBI KISUMU CAMPUS – STUDENT D61/6475/2013

This is to confirm that management has duly authorized you to collect research data from KenGen staff for pursuance of your Master's Research Project. You are hereby advised to treat the information given as strictly confidential and to use it only for academic purposes.

Through this note, KenGen employees have been requested to give you maximum support as you collect the data.

You will also be expected to avail a copy of your Research Project to the management.

Yours faithfully
For: KENYA ELECTRICITY GENERATING CO. LTD.

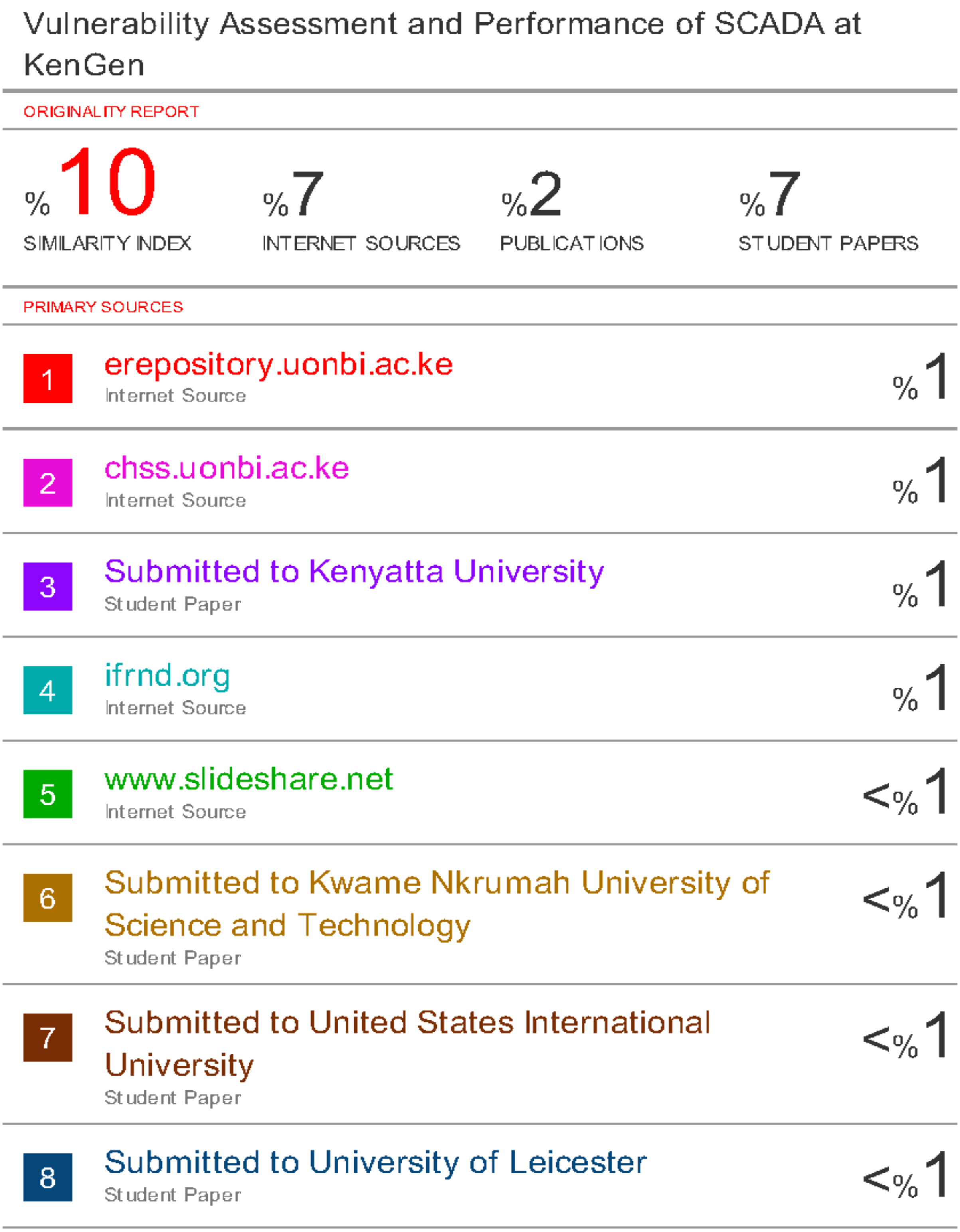
JAMES OBONDO
For: HUMAN RESOURCE MANAGER

Appendix V

SCHEDULE PLAN

Phase	**Task**	**Number of Days**															
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	**Data collection**	X	X	X	X												
2	**Data analysis**					X	X	X									
3	**Result writing**								X	X	X						
4	**Report writing**											X	X	X			
5	**Compiling**														X	X	X

APPENDIX VI



Vulnerability Assessment and Performance of SCADA at KenGen

ORIGINALITY REPORT

%10	%7	%2	%7
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	erepository.uonbi.ac.ke Internet Source	%1
2	chss.uonbi.ac.ke Internet Source	%1
3	Submitted to Kenyatta University Student Paper	%1
4	ifrnd.org Internet Source	%1
5	www.slideshare.net Internet Source	<%1
6	Submitted to Kwame Nkrumah University of Science and Technology Student Paper	<%1
7	Submitted to United States International University Student Paper	<%1
8	Submitted to University of Leicester Student Paper	<%1

9	Diaz, D. Sabin, and R. De Keyser. "WinCC® application via OPC communication to MatLab® for integrated systems", ETFA2011, 2011. Publication	<%1
10	www.puc.edu Internet Source	<%1
11	Submitted to Africa Nazarene University Student Paper	<%1
12	Submitted to Laureate Higher Education Group Student Paper	<%1
13	Submitted to American Public University System Student Paper	<%1
14	Submitted to University of Nairobi Student Paper	<%1
15	wudpeckerresearchjournals.org Internet Source	<%1
16	www.computerworld.com Internet Source	<%1
17	Ten, Chee-Wooi, Chen-Ching Liu, and Govindarasu Manimaran. "Vulnerability Assessment of Cybersecurity for SCADA Systems", IEEE Transactions on Power Systems, 2008.	<%1