PHYSICAL SECURITY MEASURES FRAMEWORK FOR MARIB POWER PLANT

ANAS MUSTAFA MOHAMMED AL-AGHBARI

A project report submitted in partial fulfilment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computing
Universiti Teknologi Malaysia

JUNE 2013

This project report is dedicated to my parents for their endless support and encouragement. Also I dedicated my wife and my kids who supported me emotionally during my study.

ACKNOWLEDGEMENT

First and foremost, I would like to express heartfelt gratitude to Ministry of Defense in Yemen that sponsored me in my study and to my supervisor **Dr. Norafida Bint Ithnin** for her constant support during my study at UTM. She inspired me greatly to work in this project. Her willingness to motivate me contributed tremendously to our project. I have learned a lot from him and I am fortunate to have him as my mentor and supervisor

Besides, I would like to thank the authority of Universiti Teknologi Malaysia (UTM) for providing me with a good environment and facilities such as Computer laboratory to complete this project with software which I need during process.

ABSTRACT

Power plants infrastructure is very important infrastructure because electricity related with all aspect in our life. To be success infrastructure Power Plant must has good security protection from the attacks. Physical security is the most important because it is the first layer in security. In Yemen there are 18 power plants and generate around 1268.05MW of electricity 835.5MW Using steam and gas and 432.55 using Diesel. Marib Power Plant the largest station in Yemen Republic and cost $159.016000, it is include 341 MW and cover 27% from electricity in Yemen while 73% come from others 18 power plants. Moreover, Marib Power Plant supplies electricity to the capital city in Yemen Sana'a and other neighboring areas. However, Marib Power Plant faces many physical attacks, the high risky attacks was local armed tribesman, bombing and sabotage. According to the reports from ministry of electricity, the attacks that happen caused a lot of problems for the government (Social, political and economic). Therefore, this study aims to design physical security measures framework for Marib Power Plant to reduce the physical security attacks. The framework included many measures (Deterrence, Detection, Delay, Response and Army role). Validation of this framework conducted by two types: firstly, by conduct the interview with expert in Marib Power Plant, secondly, by the hypotheses testing between the components of the framework. The results from this study showed that, very important to reduce the attacks on Marib Power Plant.

ABSTRAK

Infrastruktur loji kuasa merupakan infrastruktur yang sangat penting kerana ia melibatkan tenaga elektrik sekaligus mengaitkan semua aspek dalam kehidupan kita. Untuk menjadi infrastruktur yang berjaya, Loji Kuasa mesti mempunyai perlindungan keselamatan yang baik dari serangan. Keselamatan fizikal adalah yang paling penting kerana ia adalah lapisan pertama keselamatan. Di Yaman terdapat 18 loji kuasa yang menjana sekitar 1268.05MW daripada 835.5MW elektrik menggunakan wap dan gas serta menggunakan 432.55 MW Diesel. Stesen Loji Kuasa Marib adalah yang terbesar di Republik Yaman dan kosnya adalah $ 159.016000 ini adalah termasuk 341 MW dan meliputi 27% daripada tenaga elektrik di Yaman, manakala 73% datang daripada 18 loji kuasa yang lain. Selain itu, Stesen Loji Kuasa Marib membekalkan elektrik ke ibu kota Sana'a di Yaman dan kawasan-kawasan jiranya. Walau bagaimanapun, Stesen Loji Kuasa Marib menghadapi serangan fizikal yang banyak, serangan berisiko tinggi adalah dari puak-puak tempatan yang bersenjata, pengeboman dan sabotaj. Menurut laporan daripada kementerian elektrisiti, serangan yang berlaku menyebabkan banyak masalah kepada kerajaan (sosial, politik dan ekonomi). Oleh itu, kajian ini bertujuan untuk mereka bentuk rangka keselamatan fizikal iaitu langkah-langkah untuk mengurangkan serangan keselamatan fizikal keatas Loji Kuasa Marib. Rangka kerja ini termasuk banyak langkah-langkah (Pencegahan, Pengesanan, Penangguhan, Tindak Balas dan Peranan Tentera). Pengesahan rangka kerja ini dijalankan dengan mengguakan dua kaedah: pertama, dengan mengadakan temu bual dengan pakar Loji Kuasa Marib, kedua, dengan ujian hipotesis antara komponen rangka kerja tersebut. Hasil daripada kajian ini menunjukkan bahawa, amat penting untuk mengurangkan serangan keatas Loji Kuasa Marib.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

RESEARCH INTRODUCTION

1.1 Introduction

Information security has become of great significance today because of the extensive dissemination of information. This, in addition to the expansion of computers and technology, has made attack on information easier to carry out. Therefore, security must develop in sophistication along with advanced technology. The threats may be logical or physical but as Weingart (2000) stated, a physical attack occurrence is easy as opposed to logical. Also, Norman (2007) said that there is no security without physical security.

So, focusing on physical security is very important because it is the first layer of defense. Also, physical security for buildings and infrastructure is very important to protect the information and assets from the threats and risks, because secured data and media in storage could be damaged or stolen if the building is not well-secured. So, secured entrance and access points can prevent potential threats and along with this is the consideration of environmental and terrorist attacks that will damage the building or infrastructure. So, physical security can help to maintain the building and infrastructure to detect the attacks before they occur and to responnd as soon as possible after their occurrence.

Power plants infrastructure is a very important infrastructure because electricity is related to all aspects of our lives. If there is any problem in electricity, lives may stop as all activities depend on it. The figure below shows the significance of electricity infrastructure and its impact on other infrastructures.

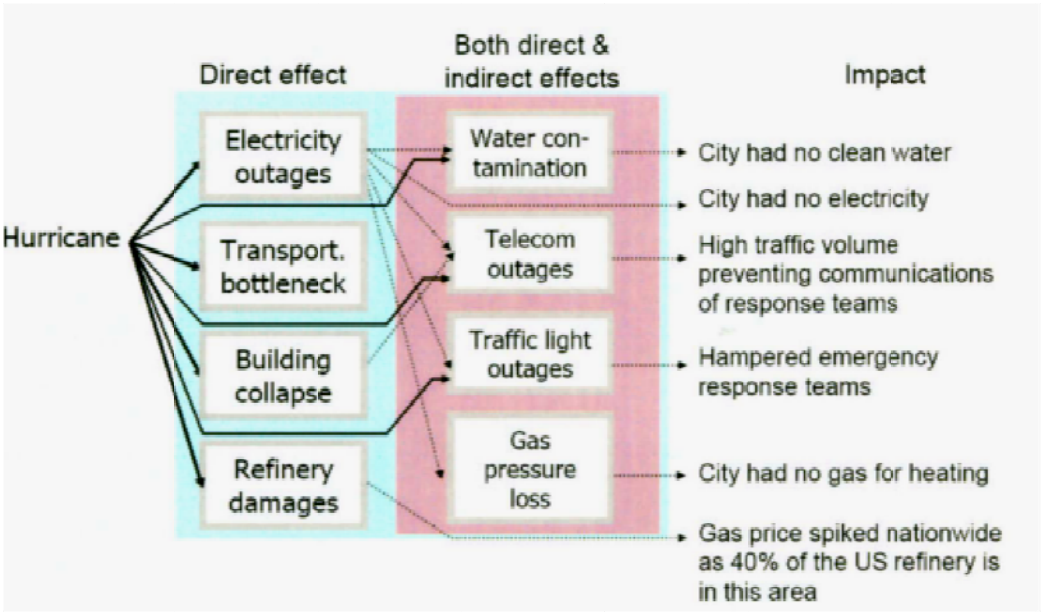

Figure1.1: Effects and Impacts of Electricity on other Infrastructures (Simpson, 2007)

The figure above shows that electricity is a very important infrastructure because it will affect all other infrastructures when it is shut down.

In Yemen, there are 18 power plants generating around 1268.05MW of electricity 835.5MW using steam and gas and 432.55 using Diesel. Electricity lines in Marib feed the Dhahban power station, the main source of electricity for Sanaa (Gaston and al-Dawsari, 2013). However the electricity infrastructure in Yemen has a big issue according to the reports from Ministry following the attacks that happened and this causes a lot of problems for the government (Social, political and economic). According to Redwan (2010), the continuous electricity shut down led to many problems in the Yemeni citizen's life, including:

- Business problems: the daily shut down lead to destroy many of the merchandise, especially in retail, and stopped many of the daily businesses
- Tourist Problems: lead to giving a bad picture of the infrastructure in Yemen and thus, decline in tourism and investments,
- Problems investments: many investors escape from Yemen as a result of poor infrastructure - some might say that most of the investment projects have their own sources of electricity
- Security problems: repetitive shut down of electricity at night leads to the risk of theft and burglary and increase of various crimes in the dark alleys of the streets.

So, all these bring a lot of problems to the government. In other words, the provision of good physical security will reduce the impact of threats and will introduce good protection. This project focuses on physical security for a major power plant in Yemen (Marib power plant).

1.2 Background of the Problem

Power plants are very important to provide electricity for in countries. Undoubtedly, electricity is one of the most vital elements without which human cannot proceed with the activities related to all aspects of life; for instance, in hospital, factories and interruption in internet.

Marib faced significant security issues even before 2011. In addition to having one of the highest levels of tribal conflict, because of the lack of government control, militant groups used Marib as a staging ground for attacks. AQAP was responsible for several high-profile attacks on electricity and oil resources in Marib in 2010, as well as frequent attacks on government officials and security forces (Gaston and al-Dawsari, 2013). Power plants in Yemen have been experiencing a big obstacle concerning the infrastructure and some facilities in the past few years as

its towers, facilities and power plants became the target of attacks, specifically in Marib province. This resulted in impacting the every aspect of Yemeni citizens' lives.

Marib gas station is the largest station in Yemen Republic which costs around $159.016000, provides 341 MW and provides 27% of electricity in Yemen - 73% are provided by 18 power plants. So any problems in this station causes interruptions in a lot of cities which means a huge area will be plunged in darkness. In addition, a lot of companies, factories and government organization will stop working. So that will cost the government huge spatial loss in all sides, especially in the economy.

The Yemeni news Agency reported that, Eng. Khalid Rashed said in a press conference in Sana'a that the total attacks that affected the power transmission lines Merib - Sana'a, reached 141attacks which costs over 33YR billion consisting of cost of spare parts, repairs and interrupted power (Fox, 2012).

The minister of electricity and power of Yemeni stated that the ministries agreed on Friday ***22 June 2012*** to stop work in Marib gas- operated power station and draw attention toward president Hadi and the government to bring complete protection for transmission lines.

Dr. Saleh Somai told Yemen Fox that "the ministry chose to stop Marib gas plant because of repeated attacks by vandals and will remain out of service until the army and security do their duties in protecting the lines. The electrical national grid would be destroyed completely if the repeated attacks on electric power transmission lines continued and we did nothing". Power plants in Yemen have been experiencing a big obstacle concerning the infrastructure and some facilities in the past few years as its towers, facilities and power plants became the target of attacks, specifically in Marib province. This resulted in impacting the every aspect of Yemeni citizens' lives (Fox 2012).

So, each building and infrastructure must have physical security, to detect and prevent attacks from happening. Also, all the staff inside the building should be

familiar with physical security, by providing them with courses and seminars (Longinow and Mniszewski, 1996), because physical security is the first phase in protecting devices and data (Caddy, 2005) and should not be ignored in any organization, either governmental or private. That is because successful attacks or physical access means getting access to the information easily (Vesperman, 2002).

In addition, physical security plays an important role in protecting all the assets responsible for the storage and data processing and operation systems (Stallings, 2009). Although there are many types of assets that are essential for continuity of organizational work, the most important one is the buildings because all of the components of the organization are inside the building. Securing the building strongly ensures weakness of the threats. The building threats include natural disasters, criminal and terrorist attacks, political issue and accidental events (Renfroe and Smith, 2011).

To implement a good protection for Power Plants, the facility managers should be involved in developing a good physical security plan. That is because their duties are planning and managing the building and infrastructure security, and thus, they are able to identify the real risks and take the appropriate reaction that reduces or eliminates such risks (Then and Loosemore, 2006; Lavy and Dixit, 2010).

1.3 Problem Statement

As reported by the Ministry of Electricity, more than 141 attacks were attempted on Marib power plants and the outcome of the attacks cost the government is over $153 Million in 2012-2013 (Fox, 2012) and there is no physical security for frequent attacks can be protect Marib Power Plant.

Therefore, the problem statement is concerned with the need to propose physical security measures framework to protect Marib Power Plant from the attacks.

1.4 Aim of the Study

The current study aims to reduce the attacks on Marib Power Plant by proposing physical security measures framework based on the previous studies on physical security measures and the collection of data from Marib Power Plant.

1.5 Research Questions

Due to the security risks faced by Marib power plants infrastructures and buildings in Yemen, this project attempts to answer the following questions:

i. What are the countermeasures used in physical security and what is the risk ranking in Marib Power Plant?
ii. What are the measures needed to be used in the framework to mitigate the risks?
iii. How can the proposed framework be evaluated?

1.6 Objectives of the Study

This study is conducted to achieve the following objectives:

i. To study and analyze previous studies on physical security measures to get suitable strong measures to be used, and to examine the risks in Marib Power Plant to come up with the risk ranking.
ii. To propose physical security measures framework in Marib Power Plants.
iii. To validate the proposed framework of Marib Power Plant.

1.7 Scopes of the Study

To able to achieve the project objectives that have been already mentioned in the earlier section, it is very crucial to determine the research focus boundaries that will guard and lead in achieving the research objectives which are stated in the following:

- The research focuses only on Marib power plants in Yemen.
- Data is collected from the top management by interviewing experts in Marib Power Plant and distributing the questionnaire to staff in Marib Power Plant.
- The questionnaire answers are analyzed in terms of the relationship between the security obstacles (deterrence, , detection, delay, response and defense) and physical security measures.
- The current study is also based on the observation that the electricity was shut down around 15 hours per day.

1.8 Significance of Study

This study contributes to reducing the attacks that happened in Marib Power Plant. Also, the study can be applied in other critical infrastructure in Yemen to protect it from the same attacks.

1.9 Thesis Organization

This project contains six chapters. Chapter one explains the problems and significance of this project and establishes the objectives that should be achieved from this project. Chapter two contains the literature review which discusses previous studies dedicated to this area. In addition, the overview of Marib power plant is also provided in Chapter two. Chapter three explains the research methodology that is followed in completing the project while chapter four contains the initial findings. Chapter five provides an overview of the results and chapter six contains recommendations.

REFERENCE

Aagedal, J. O., F. den Braber, et al. (2002). Model-based risk assessment to improve enterprise security. Enterprise Distributed Object Computing Conference, 2002. EDOC '02. Proceedings. Sixth International.

Alach, Z. J. (2007). Mapping the elements of physical security towards the creation of a holistic physical security model.

American, N. (2007). Security Guidelines for the Electricity Sector: Physical Security.

Andrews, M. H. a. A. (28-8-2012). "Nuclear Power Plant Security and Vulnerabilities." Congressional Research Service(CRS Report for Congress): 1-15.

AndyS.Krupa(2003).http://www.sans.org/reading_room/whitepapers/recovery/oversight-physical-security-contingency-planning_557

Bartlett, J., Kotrlik, J., and Higgins, C. (2001). Organizational research: Determining appropriate sample size in survey research. *Information Technology, Learning, and Performance Journal.*19(1): 43-50.

Challinger, D. (2008). Crisp Report From the Ground Up: Security for Tall Buildings. An_ASIS Foundation

Depoy, J., J. Phelan, et al. (2005). Risk assessment for physical and cyber attacks on critical infrastructures, IEEE.

Drevin, L., H. A. Kruger, et al. (2007). Value-focused assessment of ICT security awareness in an academic environment. Computers & Security 26(1): 36-43.

E.Long, l. (2005). "Security Solutions by Applied Research Associates, Inc. Conferences, Rail Tasit, EMI.

Fort Leavenworth, K. (2006). DCSINT Handbook No. 1.02, Critical Infrastructure Threats and Terrorism.

Fox, Y. (2012). Electricity minister: Mareb plant stopped due to vandal acts. newspaper.

Fox, Y. (2012). Yemen lost USD 154 mln due to power grids sabotage. News Paper- Yemen Fox.

Galisson, R. M. P. E. (2009). Evaluation of physical security in a Movie.

Garcia, M. L. (2007). Design and evaluation of physical protection systems, Butterworth-Heinemann.

Gaston, E. and N. al-Dawsari (2013). The Impact Of Transition On Local Justice And Security In Yemen.

Gouin, B. (2007). Chapter 10 - Security measures: Physical security. Strategic Security Management. Burlington, Butterworth-Heinemann: 183-215.

Gregory, P. (2009). CISSP guide to security essentials, Course Technology Ptr.

Headquarters, D. o. t. A. (2001). fm31930 physical security.

Homeland Security Presidential, (2003). Critical Infrastructure Identification, Prioritization, and Protection.http://www.dhs.gov/xabout/laws/gc 1214597989952.shtm#1

Johnson, E. C. (2006). Security awareness: switch to a better Programme.Network Security 2006(2): 15-18.

Kallhoff, J. (2007). Physical Security.

Lavy, S., J. A. Garcia, et al. (2010). Establishment of KPIs for facility performance measurement: review of literature. Facilities 28(9/10): 440-464.

Leedy, P. A., and Ormrod, J. E. (2001).Practical research: Planning and design (7th ed.). Columbus, OH: Merrill Prentice-Hall.

Matalucci, R. V. (2002). Risk Assessment Methodology For Dams (Ram-D Sm).

Maxim, P. (1999). Quantitative Research in the Social Sciences. New York: Oxford.

Mayer, R., Davis, J., and Schoorman, D. (1995). An Integration Model Of Organizational Trust. Academy Of Management.The Academy of Management Review. 20(3): 709-34.

MERONI, S. (2011). Vulnerability Assessment And Security Journal of

Physical Security 5.

Nuclear Energy Institute (2011) Safety and Securityhttp://www.nei.org/resourcesandstats /Documentlibrary/Safety-and-Security/factsheet/powerplantsecurity

Nuclear Services/Engineering Services (2012). "External Flooding Probabilistic Risk Assessment Analysis Identification of Plant Vulnerabilities."http://www.westinghousenuclear.com/Products_&_Services/docs/flysheets/NS-ES-0219.pdf

Norman, T. (2007). 7 - Physical Security Elements. Integrated Security Systems Design. Burlington, Butterworth-Heinemann**:** 139-178.

Onwubiko, C. and A. P. Lenaghan (2007). Managing security threats and vulnerabilities for small to medium enterprises, IEEE.

PA Energy Alliance (2009). U.S. nuclear power plants safe, secure. http://paenergyalliance.com/u-s-nuclear-power-plants-safe-secur

Paula D. Gordon (2012). The Japan Earthquake and Tsunami: Their Implications for the U.S. Journal of Physical Security **6**: 10-18.

Philpott, D. and S. Einstein (2006). The Integrated Physical Security Handbook, Homeland Defense Journal.

Platt, F. N. (2002). Physical Threats To The Information Infrastructure. FLY: 1401.

Redwan (2010). the millions that lose from the citizens .. electricity Yemen help on the inhibition of the Yemeni economy daily. News Paper- Alsaqer: http://www.yemen90.net/t9751-topic.

Services, N. S. E. (2012). "External Flooding Probabilistic Risk Assessment Analysis Identification of Plant Vulnerabilities."

Simpson, K. S. a. D. M. (2007). Critical Infrastructure Failure in a Natural Disaster:

Initial Notes comparing Kobe and Katrina." University of Louisnille.

Sinski, C. (2003). Structural Option Dr. Memari.

Stallings, W. (2009). Chapter 36 - Physical Security Essentials. Computer and Information Security Handbook. R. V. John. Boston, Morgan Kaufmann**:** 627-643.

Then, S. K. and M. Loosemore (2006). Terrorism prevention, preparedness, and response in built facilities. Facilities **24**(5/6): 157-176.

Times, Y. (2012). Marib Power Station shuts down, army attempts to catch saboteurs. Yemen Times.

The Royal Geographical Society (March 2011). Dr Bruce Malamud answers Questions On The Japanese Earthquake And Tsunami. http://www.rgs.org/Our Work/Schools/Geography +in+the+News/Ask+the+experts/Japanese+earthquake+ and+tsunami.htm.

Watson, J. and A. Scott (2009). New nuclear power in the UK: A strategy for energy security? Energy Policy **37**(12): 5094-5104.

Weingart, S. (2000). Physical security devices for computer subsystems: A survey of attacks and defenses, Springer.

Whitehead, D., C. Potter III, et al. (2007). "Nuclear Power Plant Security Assessment Technical Manual. SAND2007-5591, Sandia National Laboratories, Albuquerque, NM.

Wikipedia (2012). Physical security.

Wikipedia (2013). Ancient history of Yemen.

Yusta, J. M., G. J. Correa, et al. (2011). "Methodologies and applications for critical infrastructure protection: State-of-the-art." Energy Policy 39(10): 6100-6119.