UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Faculty of Information and Communication Technology

THREAT ANALYSIS FOR CYBER PHYSICAL SYSTEM

Mohammed Nasser Ahmed Al-Mhiqani

Master of Computer Science (Internetworking Technology)

2015

THREAT ANALYSIS FOR CYBER PHYSICAL SYSTEM

MOHAMMED NASSER AHMED AL-MHIQANI

A dissertation submitted
in fulfillment of requirements for the degree of Master of Computer Science
(Internetworking Technology)

Faculty of Information and Communication Technology

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2015

DECLARATION

I declare that this dissertation entitle “Threat Analysis for Cyber Physical System” is the result of my own research except as cited in the references. The dissertation has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature : ....

Name : Mohammed Nasser Ahmed Al-Mhiqani

Date : 23th June 2015

APPROVAL

I hereby declare that I have read this dissertation and in my opinion this dissertation is sufficient in terms of scope and quality for the award of Master of Computer Science (Internetworking Technology).

Signature : …………………………………………

Supervisor Name : Prof. Dr. Rabiah Binti Ahmad

Date : 23th June 2015

DEDICATION

To my beloved parents, that always giving me moral support that act as power of my inspiration. To all my friends, your support and encouragement helps me pass through and to solve problems in this project. To my supervisor, Prof. Dr. Rabiah Ahmad, your guidance is highly appreciated and I learn a lot from you during this project.

ABSTRACT

Cyber physical systems are the systems that have an interaction between the computers and the real-world; it has been widely used in many different areas and played a major role in our daily lives, Smart Grid, healthcare, aircrafts, and emergency management are the most areas where CPS applied. However the cyber physical systems currently one of the important hackers' target that have a lot of incidents because of the high impacts of these systems, many works have been conducted in CPS but still there are a lack of theories and tools that organizations and researchers can use to understand the natural of the new threats and the impacts that each threat can cause to the physical systems, in this project we will investigate the current threats on CPSs, develop matrices to calculate these threats, and conduct analysis on the collected data using quantitative approach.

ABSTRAK

Sistem fizikal siber adalah sistem yang mempunyai interaksi antara komputer dan dunia nyata ini ; ia telah digunakan secara meluas di kawasan-kawasan yang berbeza dan memainkan peranan yang penting dalam kehidupan seharian kita , Grid Pintar , penjagaan kesihatan, pesawat , dan pengurusan kecemasan adalah kawasan yang paling banyak CPS digunakan. Walau bagaimanapun sistem fizikal siber kini menjadi satu sasaran penggodam yang mempunyai banyak insiden kerana impak yang tinggi sistem ini, banyak kerja-kerja telah dijalankan di CPS tetapi masih terdapat kekurangan teori dan alat-alat yang organisasi dan penyelidik boleh gunakan untuk memahami semula jadi ancaman baru dan kesan yang sama boleh menyebabkan ancaman kepada sistem fizikal, dalam projek ini kita akan menyiasat ancaman semasa pada CPSS , membangunkan matriks untuk mengira ancaman ini , dan menjalankan analisis ke atas data yang dikumpul menggunakan kuantitatif pendekatan.

ACKNOWLEDGMENT

I grateful to Allah SWT almighty and oneness with overflow and His grace I have completed this dissertation.

I would like to thank everyone who had contributed to the successful completion of this dissertation.

I would like to take this opportunity to express my sincere acknowledgement to my supervisor Prof. Dr. Rabiah Ahmad from the Faculty of Information & Communication Technology Universiti Teknikal Malaysia Melaka (UTeM) for her essential supervision, support and encouragement towards the completion of this dissertation.

I would also like to thank Universiti Teknikal Malaysia Melaka, all my lecturers at UTeM, and special thanks to Dr. Zurina Saaya and Mrs. Zaheera Zainal Abidin. Furthermore, I want to thank my friends who have helped and motivated me throughout.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS

ARINC	-	Aeronautical Radio, Incorporated
BCIT	-	British Columbia Institute of Technology (BCIT)
CC	-	Cyber Crime
CE	-	Cyber Espionage
CIA	-	Central Intelligence Agency (CIA)
CMP	-	Cellular Multi Processing
CPS	-	Cyber Physical System
CW	-	Cyber warfare
DDoS	-	Distributed Denial of Service
DoS	-	Denial of Service
EM	-	Emergency management
EMIS	-	Emergency Management Information Systems
GIS	-	Geographical Information Systems
Gov	-	Government
H	-	Hacktivism
HAN	-	Home area network
HCI	-	Human and computer interaction
ICD	-	Implantable Cardioverter Deibrillators
INEC	-	Independent National Electoral Commission
MIPT	-	Memorial Institute for the Prevention of Terrorism
MRI	-	Magnetic Resonance Imaging
OIC	-	Organization of the Islamic Conference
SEA	-	Syrian Electronic Army
WSN	-	Wireless Sensor Networks

CHAPTER 1

INTRODUCTION

1.1 Introduction

Cyber-physical system is the system that has an interaction between the computers and the real-world; it has been widely used in many different areas in our lives nowadays. Majority of modern computing devices are ubiquitous embedded systems used to manage physical processes and monitor: airplanes, cars, automotive systems f highway, management of the air traffic, etc (Ezio Bartocci, Oliver Hoeftberger, 2014). In the past, embedded systems research tended to focus on the optimization problems of design for these computational devices. Recently, the main focus has shifted toward the synergy of complex between the physical environment and the elements of computational with which they interact. The term (CPS) Cyber-Physical Systems were coined to refer to the interactions. In CPS, communication devices and embedded computation, along with sensors and actuators of the physical substratum, are federated in heterogeneous, open, and systems-of-systems(Ezio Bartocci, Oliver Hoeftberger, 2014). Terrorists, criminals or activists, are mostly looking for a new and innovative techniques and targets for their goals to be accomplished, so cyber physical systems currently one of the important hackers' target that have a lot of incidents because of the high impacts of these systems(Applegate, 2013). This chapter will cover the background of cyber physical systems, it also explains the research problems, research objectives, and the significant and contribution of this project.

1.2 Background

The developments of computer and network technologies have brought great convenience to human’s lives in recent years. With the rise of the computer data processing capabilities and the rapid development of data communications technology, demand for a variety of computing systems and engineering equipment is not limited to the expansion of the function. Integration of information systems and physical equipment, rational allocation of system resources as well as the performance of system performance optimization, these factors have also been taken into consideration(Zhang et al., 2013). Guide by this demand, cyber-physical systems (CPS) emerged, attaching great importance to governments, academia and industry.

Cyber physical systems security has become a matter of national, societal importance and economic. Current days attacks on the nation’s systems of computer do not simply disrupt a single enterprise system or damage an isolated machine (Walker, 2012). Instead, infrastructures are targeted by modern attacks that are integral to the national defense, economy, and daily life. Computer networks currently have joined water, food, transportation, and energy as critical resource for the function of the nationals’ economy.

When some of the keys cyber infrastructures systems are attacked, the same consequences exist for a terrorist attack and a natural disaster.

1.3 Research Problem

For security to be effective it should be well organized to react in quick way and effectively communicate to overcome the problems across the enterprise. New physical security attacks, malware, insider threats and different security challenges threaten to derail new innovative government methods(Dan Lohrmann, 2012).

The widely used of cyber physical systems in our lives nowadays bring some risks and ways for the cybercriminal to use it in their attacks against the governments, organizations, or individuals. These applications of CPSs are becoming increasingly the cyber-attacks targets.

Currently there are a lack of tools and theories that researchers and organizations can use to understand the types of the new threats and the impacts that each threat can cause to the physical systems.

1.4 Research Questions

Based on the problem statement this study answers the primary question as well as the secondary question.

1.4.1 Primary question:

RQ1. What are the current physical security threats and what are their ultimate effects on human lives?

In order to answer this primary question, it is divided into two secondary questions; by answering these two secondary questions the answer of the primary question (RQ1) can obtained:

RQ1-A. What are the current threats that affect the Cyber physical systems?

RQ1-B. What is the impact of these threats on the human lives?

RQ2. How can we compute and analyze the cyber physical systems incidents?

In order to answer this primary question, it is also divided into two secondary questions:

RQ2-A. How can we compute the impacts and track cyber physical systems incidents?

RQ2-B.How can we understand the current status and natural of these threats?

Table 1.1: Summary of research Questions

	RQ	**RESEARCH QUESTIONS**
RQ	**RQ1-A**	What are the current threats that affect the Cyber physical systems?
	RQ1-B	What is the impact of these threats on the human lives?
	RQ2-A	How can we compute the impacts and track cyber physical systems incidents?
	RQ2-B	How can we understand the current status and natural of these threats?

1.5 Research Objectives

The research objectives section is comprised of three objectives (i.e., RO1, RO2, and RO3) in order to answer the previously defined research questions. The overall research objectives are:

- To investigate the current physical security threats on cyber physical systems for the last 5 years.
- To propose matrices for calculating the cyber physical systems incidents.
- To analyze these attacks in order to help the researchers to clearly understand the nature of these attacks and how they may be carried out.

Table 1.2: Summary of Research Objectives

	RQ	RO	Research Objectives
RP	RQ1-A RQ1-B	RO1	To identify the current physical security threats on cyber physical systems for the last 5 years.
	RQ2-A	RQ2	To propose matrices for calculating the Cyber physical systems incidents.
	RQ2-B	RO3	To analyze these attacks in order to help the researchers to clearly understand the nature of these attacks and how they may be carried out.

1.6 Research Scope

This research study will primarily focus on the cyber physical incidents that have been occurred in the last 5 years in the Organization of the Islamic Conference (OIC) countries member; some of the cases that happen around the world may be discuss in order to make more understanding of the threats and the methods of these threats.

1.7 Research Significance

This research can offers significant contribution towards researchers in the field of cyber physical security.

This research provides researchers with matrices for studying the threats and will enable them to rapidly identify and correlate key threats involving CPS systems and that, in turn, this will lead to an increased overall awareness of these incidents.

Table 1.3: Summary of Research Contribution

	R.Q	R.O	RC	RESEARCH CONTRIBUTIONS
P	R.Q1-A R.Q1-B	R.O1	R.C1	Will provide wide survey on all the cyber physical systems incidents cases from many different trusted sources, like security agencies, security centers, journals, conferences, projects, books, reports, news websites, and etc.
	R.Q2-A R.Q2-B	R.O2 R.O3	R.C2	Will provide incidents matrices that ease the understanding of these threats, and analysis of the cyber physical incidents that will be collected in RC1.

Overall structure of this research

This section provides a brief description of what are the contents of each chapter. This research contains six chapters: introduction, literature review, research methodology, threat verification, results and discussion, and conclusion and future work.

Chapter (1): Introduction

Chapter (1) is an introductory of the whole research which provides the readers with a general idea of what the research is about. This chapter includes a background overview on CPS as a general, the research problem, the research questions, the research objectives, and the significance of the research project and its contribution.

Chapter (2): Literature Review

Chapter (2) is the literature review which presents the concept of Cyber physical Systems (CPS) and how is these systems ease the human lives. Besides, this chapter presents most important cyber physical systems that are used nowadays.

This chapter also highlights the current security challenges in cyber physical systems. Finally, this chapter highlights related works that has been done by others and identify the differences between this research and theirs.

Chapter (3): Research Methodology

Chapter (3) presents the research methodology that is followed throughout the process of conducting this research. As a research methodology, quantitative approach is used for combing through researchers' literature that has been published or other trusted news websites. This chapter illustrates the four phases of the research design: defining the research problems and objectives, reading and exploring for the literature review, collecting data about cyber physical incidents, and conduct analysis on the collected data in phase 3.

Chapter (4): Threat Verification

Chapter (4) presents the actual threat verification of the research method in order to get the needed results. Cyber physical incidents matrices, and the modified taxonomy will be discussed in this chapter and the result statistics will be analyzed in chapter (5).

Chapter (5): Results and Discussion

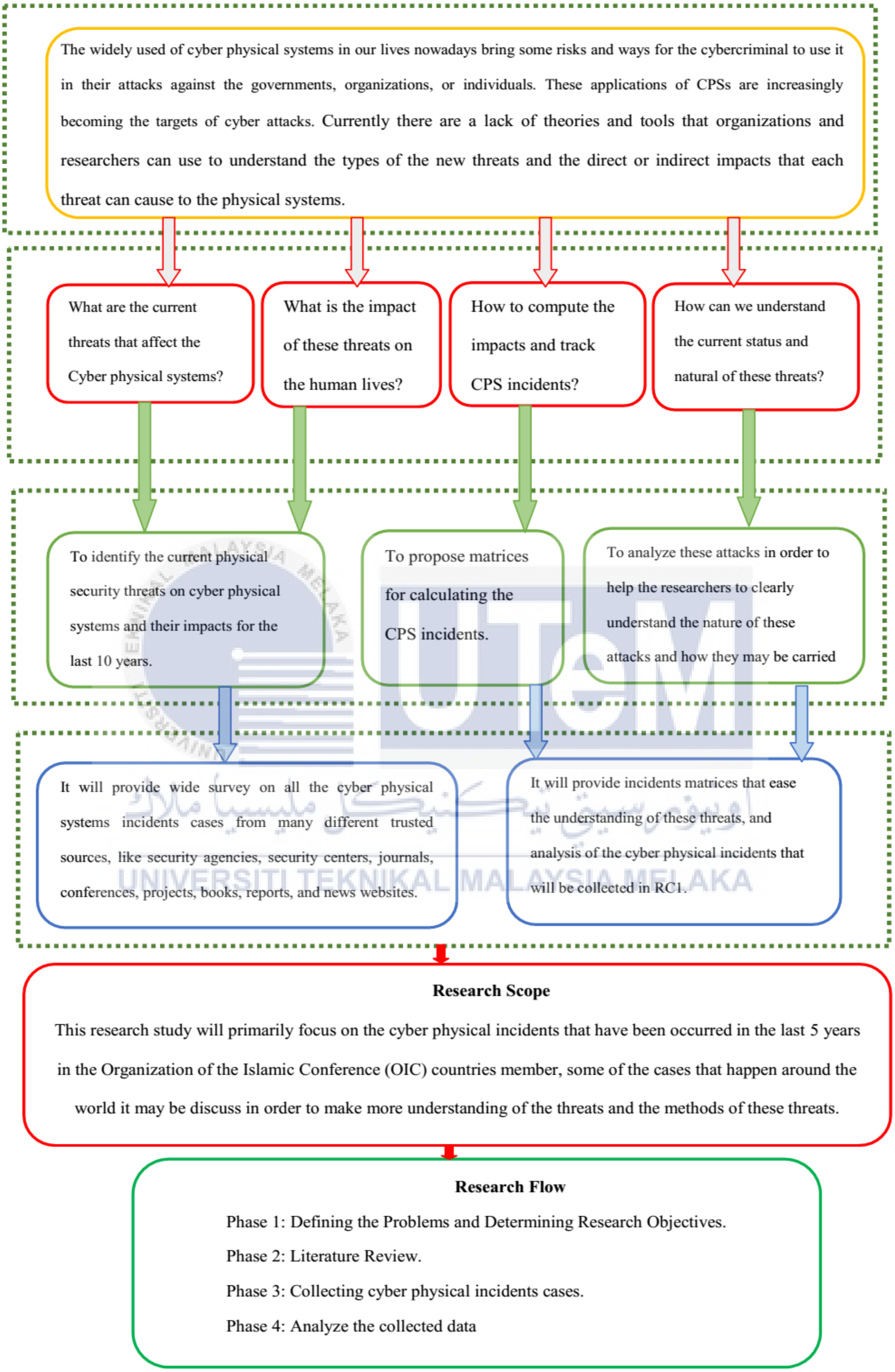
Chapter (5) presents the statistics or result obtained from the collected data of the different incidents, the matrices and modified taxonomy that has been presented in chapter (4) will be used for the analysis.

Chapter (6): Conclusion and Future Work

Chapter (6) concludes the research with a brief summary, research limitation, and future work. Besides, it gives a brief discussion on to what extent the results answer the research questions and reflect the objectives of the research.

1.8 Summary

As a conclusion this chapter provides a brief description of the contents of this research report. It is clearly defined the research problem, research questions, research objectives, research scope, and research significant and contribution. In addition, it provides summary of each chapter of this project. The figure 1.1 shows summary for the chapter contents.



The widely used of cyber physical systems in our lives nowadays bring some risks and ways for the cybercriminal to use it in their attacks against the governments, organizations, or individuals. These applications of CPSs are increasingly becoming the targets of cyber attacks. Currently there are a lack of theories and tools that organizations and researchers can use to understand the types of the new threats and the direct or indirect impacts that each threat can cause to the physical systems.

What are the current threats that affect the Cyber physical systems?

What is the impact of these threats on the human lives?

How to compute the impacts and track CPS incidents?

How can we understand the current status and natural of these threats?

To identify the current physical security threats on cyber physical systems and their impacts for the last 10 years.

To propose matrices for calculating the CPS incidents.

To analyze these attacks in order to help the researchers to clearly understand the nature of these attacks and how they may be carried

It will provide wide survey on all the cyber physical systems incidents cases from many different trusted sources, like security agencies, security centers, journals, conferences, projects, books, reports, and news websites.

It will provide incidents matrices that ease the understanding of these threats, and analysis of the cyber physical incidents that will be collected in RC1.

Research Scope

This research study will primarily focus on the cyber physical incidents that have been occurred in the last 5 years in the Organization of the Islamic Conference (OIC) countries member, some of the cases that happen around the world it may be discuss in order to make more understanding of the threats and the methods of these threats.

Research Flow

Phase 1: Defining the Problems and Determining Research Objectives.

Phase 2: Literature Review.

Phase 3: Collecting cyber physical incidents cases.

Phase 4: Analyze the collected data

Figure 1.1: Summary of Chapter 1

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

The aim of the literature review is to provide the readers with the general overview of Cyber physical systems. Recently, the CPS has become a popular used in many industries and public services. When CPS fail or malfunction, the operation of corresponding systems within the real world will reduce physical safety or trigger loss of life, cause enormous damage of economic, and thwart the businesses vital missions, states, cities and nation(Alliance, 2013). The first part of this chapter provides a brief description of cyber physical systems usage and security challenges in some of the important fields where CPS applied.

Finally, this chapter highlights related works that have been done by others to analyze and collect data about cyber physical incidents, and study that data in order to clearly understand the current status of the threats on CPS. Figure 2.1 shows the plan of the literature review.