

การพัฒนาระบบความมั่นคงปลอดภัยแบบออนไลน์สำหรับ ต้นกำเนิดกัมมันตรังสี



นางสาวกานุสร พุຍะวง

จุฬาลงกรณ์มหาวิทยาลัย

CHULALONGKORN UNIVERSITY

บทคัดย่อและแฟ้มข้อมูลฉบับเต็มของวิทยานิพนธ์ตั้งแต่ปีการศึกษา 2554 ที่ให้บริการในคลังปัญญาจุฬาฯ (CUIR)

เป็นแฟ้มข้อมูลของนิสิตเจ้าของวิทยานิพนธ์ ที่ส่งผ่านทางบัณฑิตวิทยาลัย

The abstract and full text of theses from the academic year 2011 in Chulalongkorn University Intellectual Repository (CUIR)

are the thesis authors' files submitted through the University Graduate School.

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

สาขาวิชาเทคโนโลยีนิวเคลียร์ ภาควิชาวิศวกรรมนิวเคลียร์

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ปีการศึกษา 2558

ลิขสิทธิ์ของจุฬาลงกรณ์มหาวิทยาลัย

# DEVELOPMENT AN ONLINE RADIOACTIVE SOURCE SECURITY SYSTEM

Miss Phanousone Phouiyavong



A Thesis Submitted in Partial Fulfillment of the Requirements  
for the Degree of Master of Science Program in Nuclear Technology

Department of Nuclear Engineering

Faculty of Engineering

Chulalongkorn University

Academic Year 2015

Copyright of Chulalongkorn University

Thesis Title	DEVELOPMENT AN ONLINE RADIOACTIVE SOURCE SECURITY SYSTEM
By	Miss Phanousone Phouiyavong
Field of Study	Nuclear Technology
Thesis Advisor	Mr Decho Thong-aram
Thesis Co-Advisor	Assistant Professor Suvit Punnachaiya

---

Accepted by the Faculty of Engineering, Chulalongkorn University in  
Partial Fulfillment of the Requirements for the Master's Degree

..... Dean of the Faculty of Engineering  
(Professor Bundhit Eua-arporn, Ph.D.)

#### THESIS COMMITTEE

..... Chairman  
(Associate Professor Nares Chankow)

..... Thesis Advisor  
(Mr Decho Thong-aram)

..... Thesis Co-Advisor  
(Assistant Professor Suvit Punnachaiya)

..... Examiner  
(Associate Professor Somyot Srisatit)

..... External Examiner  
(Assistant Professor Attaporn Pattarasumunt)

ภาณุสร พุชยะวง : การพัฒนาระบบความมั่นคงปลอดภัยแบบออนไลน์สำหรับ ต้นกำเนิดกัมมันตรังสี (DEVELOPMENT AN ONLINE RADIOACTIVE SOURCE SECURITY SYSTEM) อ.ที่ปริกษาวิทยานิพนธ์หลัก: อาจารย์ เดโช ทองอร่าม, อ.ที่ปริกษาวิทยานิพนธ์ร่วม: สุวิทย์ ปุณณชัยยะ, 84 หน้า.

ได้พัฒนาระบบความมั่นคงปลอดภัยแบบออนไลน์สำหรับต้นกำเนิดกัมมันตรังสีเพื่อใช้สำหรับงานด้านการป้องกันการลักลอบนำต้นกำเนิดกัมมันตรังสีที่มีความแรงสูงไปใช้กระทำการในทางผิดกฎหมาย เนื่องจากต้นกำเนิดกัมมันตรังสีสามารถนำไปใช้สร้างอุปกรณ์แพร่กระจายสารกัมมันตรังสีได้ ในงานวิจัยนี้ได้ออกแบบระบบให้มีฟังก์ชันครอบคลุมพื้นฐานของระบบความมั่นคงปลอดภัยระดับ A ตามข้อเสนอแนะวิธีปฏิบัติของทบวงการประมาธระหว่างประเทศ เช่น การตรวจวัด ยับยั้ง ถ่วงเวลา ตอบโต้และจัดการด้านความมั่นคง โดยได้ปรับปรุงเครื่องสำรวจรังสีให้ทำงานเป็นอุปกรณ์เฝ้าระวังระดับรังสีแบบประหยัดขึ้นเพื่อประกอบเข้ากับระบบย่อยต่างๆ ได้แก่ ระบบกล้องโทรทัศน์วงจรปิด ระบบตรวจจับการเคลื่อนไหว ระบบควบคุมการเข้าออกและระบบติดตามผ่านดาวเทียม เพื่อที่จะเชื่อมต่อสัญญาณเตือนทุกส่วนผ่านระบบคอมพิวเตอร์ให้ทำงานตามลำดับขั้น โปรแกรมควบคุมการทำงานจากระบบได้รับการพัฒนาขึ้นให้ควบคุมการส่งสัญญาณเตือนจากระบบเฝ้าระวังแบบออนไลน์เข้าระบบเครือข่ายอินเทอร์เน็ตและโทรศัพท์เคลื่อนที่ ไปยังศูนย์รักษาความปลอดภัยรวมทั้งผู้รับผิดชอบ ผลทดสอบการทำงานจากระบบที่พัฒนาขึ้นแสดงให้เห็นว่ามีขั้นตอนการส่งสัญญาณเตือนผู้บุกรุกเข้าสู่ต้นกำเนิดกัมมันตรังสีในหลายลำดับขั้น สามารถนำไปใช้ในการป้องกันการเคลื่อนย้ายต้นกำเนิดกัมมันตรังสีโดยไม่ได้รับอนุญาตตามสถานประกอบการ เช่น โรงพยาบาล โรงงานอุตสาหกรรมและห้องปฏิบัติการรังสีสูงด้วยความเชื่อมั่นสูง

ภาควิชา วิศวกรรมนิวเคลียร์

สาขาวิชา เทคโนโลยีนิวเคลียร์

ปีการศึกษา 2558

ลายมือชื่อนิติต .....

ลายมือชื่อ อ.ที่ปริกษาหลัก .....

ลายมือชื่อ อ.ที่ปริกษาร่วม .....

# # 5670573721 : MAJOR NUCLEAR TECHNOLOGY

KEYWORDS: SOURCE SECURITY / RADIATION AREA MONITOR / ONLINE TRACKING SYSTEM / RADIOLOGICAL DISPERSAL DEVICE

PHANOUSONE PHOUYAVONG: DEVELOPMENT AN ONLINE RADIOACTIVE SOURCE SECURITY SYSTEM. ADVISOR: MR DECHO THONG-ARAM, CO-ADVISOR: ASST. PROF. SUVIT PUNNACHAIYA, 84 pp.

An online radioactive sources security System (ORSS) was developed for preventing high activity radioactive sources from committing a malicious act, since the radioactive source could be used to build a Radiological Disposal Device (RDD). The design features of an ORSS system in this research was covered the basic security functions such as detection, deterrence, delay, response, and security management according to the security level A of IAEA guideline. A detector was operate as an economical radiation monitor and integrated with the subsystem of compact CCTV unit, motion sensing unit, door access unit, and GPS tracking unit in order to link all alarm signals through a computerizing system in sequential actions. The system control software was also developed. The alarm signal could be sent via both internet and SMS mobile phone to the security center and responsible persons with online monitoring access. In functional tested results, it was revealed that the developed system could prevent unauthorized person from accessing the secured source in multiple alarm layers operation and could be used for protecting a high activity radioactive source removal without authorization at working place such as hospitals, industries and laboratories with high reliability security.

Department:	Nuclear Engineering	Student's Signature .....
Field of Study:	Nuclear Technology	Advisor's Signature .....
Academic Year:	2015	Co-Advisor's Signature .....

## ACKNOWLEDGEMENTS

First of all, I deeply gratitude to my thesis co-adviser, Assistant Professor Suvit Punnachaiya and my advisor Mr. Decho Thong-Aram, for his continuous consultation and advice academically, along with his support for my master student, for his patience, motivation, and immense knowledge. His guidance helped me in all the time of writing and research of this thesis.

I would also like to thank my thesis committee members, Associate Professor Nares Chankow, Associate Professor Somyot Srisatit and Assistant Professor Attaporn Pattarasumunt for their constructive criticisms and suggestion that really helped me to polish this work. Not forgetting those who have given assistance and contributed or indirectly to my work.

Also thank to the European Union and all of the professor in the Nuclear Engineering Department of Chulalongkorn University for the support and allowing us to perform this study, without which the present study could not have been completed. it is utmost gratitude that i thank you all.

## CONTENTS

	Page
THAI ABSTRACT .....	iv
ENGLISH ABSTRACT.....	v
ACKNOWLEDGEMENTS .....	vi
CONTENTS.....	vii
LIST OF TABLES .....	xi
LIST OF FIGURE.....	xii
CHAPTER 1 INTRODUCTION .....	1
1.1 Introduction .....	1
1.2 Objective.....	3
1.3 Scopes.....	3
1.4 Expected Benefits .....	3
1.5 Literature Review .....	3
CHAPTER 2 THEORY AND PRINCIPLE .....	6
2.1 Nuclear Security Fundamentals.....	6
2.1.1 Nuclear Safety and Nuclear Security Definition.....	6
2.1.2 Nuclear Terrorism .....	7
2.1.3 Responsibilities for Safety and Security .....	10
2.2 Radioactive Source Protection and Security .....	12
2.2.1 Code of Conduct on the Safety and Security .....	12
2.2.2 Security Levels and Security Objectives.....	13
2.2.3 Considerations for Assigning Security Levels .....	14
2.3 Radiation Source Security System .....	15
2.3.1 Security Functions .....	15
2.3.2 Design and Evaluation of Security Systems [11].....	16
2.3.3 Integration of Safety and Security Measures [11].....	17
2.4 Radiation Area Monitoring System.....	18
2.4.1 Type of Radiation Area Monitor .....	18
2.4.2 Structure of Radiation Area Monitor.....	18

	Page
2.5 Physical Protection System.....	19
2.5.1 Access Control .....	20
2.5.2 Intrusion Detection .....	20
2.5.3 CCTV Surveillance .....	21
2.5.4 Communication .....	21
2.5.5 Key Control Procedures .....	21
2.5.6 Locks, Hinges and Interlocks for Doors.....	21
2.5.7 Locked, Shielded Containers.....	22
2.5.8 Standby Power.....	22
<b>CHAPTER 3 DESIGN AND CONSTRUCTION OF A RADIOACTIVE SOURCE SECURITY SYSTEM (ORSS).....</b>	<b>23</b>
3.1 System Configuration Design.....	23
3.1.1 Criteria for System Design .....	23
3.1.2 System Structure Design .....	24
3.1.3 Inexpensive Sensor Devices Selection .....	26
3.2 Economical Radiation Area Monitor Development .....	31
3.2.1 Radiation Area Monitor Design .....	31
3.2.2 Gamma Alarm Setting.....	32
3.3 Online Radioactive Source Security Hardware Design.....	33
3.3.1 Microcontroller Based Alarm Control System.....	33
3.3.2 Microcomputer Based Central Alarm Monitoring System .....	35
3.4 System Control Program Design .....	39
3.4.1 Operating Step of System.....	39
3.4.2 Keypad Door Access Control system.....	41
3.5 Online Radioactive Source Security System Assembly .....	42
3.5.1 System Prototype Assembly.....	42
3.5.2 System under Test .....	44
<b>CHAPTER 4 EXPERIMENTAL RESULTS .....</b>	<b>46</b>
4.1 Physical Sensing Devices Control Testing .....	46



	Page
4.1.1 Instrument and Equipment .....	46
4.1.2 Keypad Door Access Control Device Testing .....	47
4.1.3 Door Switch Device Control Testing .....	48
4.1.4 IR Optical Switch Sensing Device Control Testing .....	49
4.1.5 PIR Motion Sensing Device Control Testing .....	51
4.1.6 Image Motion Sensing Device Control Testing .....	53
4.1.7 IP Camera Remote Control Testing .....	54
4.2 Radiation Area Monitoring Testing .....	57
4.2.1 Instrument and Equipment .....	57
4.2.2 Ratemeter Testing .....	57
4.2.3 Radiation Detection system .....	60
4.3 Online Communication Testing .....	62
4.3.1 Instrument and Equipment .....	62
4.3.2 Alarm link between alarm control and central alarm monitoring station Testing .....	62
4.3.3 Alarm Link to Mobile Phone Testing .....	65
4.3.4 Tracking Link to Mobile Phone Testing .....	66
4.4 System Integration Operation of ORSS Testing .....	67
4.4.1 Instrument and Equipment .....	68
4.4.2 Full System Operation Testing .....	68
4.4.3 Fault Alarm Testing .....	70
CHAPTER 5 CONCLUSIONS .....	72
5.1 Conclusion .....	72
5.2 Suggestion .....	73
REFERENCES .....	74
APPENDIXES .....	78
APPENDIX A .....	79
APPENDIX B .....	80
APPENDIX C .....	81

	Page
APPENDIX D.....	82
APPENDIX E.....	83
VITA.....	84



## LIST OF TABLES

Label	Title	Pages
4.1	The result of keypad door access control device testing	47
4.2	The result of door switch device control testing	49
4.3	The result of IR optical sensing device control testing	50
4.4	The result of sensitivity for PIR motion sensing device control testing	52
4.5	The result of sensitivity for image motion sensing control testing	54
4.6	Result of linearity test of ratemeter for 100 Hz and 100 kHz	58
4.7	Tested result of window alarm for area monitor testing	61
4.8	Data result from testing sensitivity alarm code sent to webserver	64
4.9	The tested result of alarm link to mobile phone simulation	65
4.10	The tested result of alarm link to mobile phone simulation	66
4.11	The test results of system operation with authorized password	68
4.12	The tested result of system operation with unauthorized password	69
4.13	The tested result for fault alarm testing	70

## LIST OF FIGURE

Label	Title	Pages
2.1	Radiation area monitoring system	19
2.2	Structure of radiation area monitoring system	19
3.1	Block diagram of online radioactive source security system	24
3.2	Keypad door access control system	26
3.3	First layer physical sensing devices	27
3.4	Diagram of first layer physical protection sensors connection	28
3.5	Motion sensor	28
3.6	Two IP cameras for monitoring	29
3.7	Diagram of second layer physical protection sensors connection	30
3.8	Location tracking using GPS tracker	30
3.9	Block diagram of a radiation area monitor	31
3.10	The scintillation detector module	32
3.11	Radiation alarm threshold setting	33
3.12	The Microcontroller kit for alarm control system development	34
3.13	Schematic diagram of microcontroller based alarm control system	35
3.14	Computer for monitoring system	36
3.15	Example of alarm display status of system	38
3.16	The SMS message on mobile phone	38
3.17	The GPS tracking information	39
3.18	Flow chart of the system control software	40
3.19	Door access system display	42
3.20	Top view of the developed ORSS	43
3.21	Front view of ORSS assembly	43
3.22	Rear view of ORSS assembly	44
3.23	Full function of system setup of ORSS	45

4.1	The connection diagram of keypad door access control device testing	47
4.2	The connection diagram of door switch control test	48
4.3	The connection diagram of IR optical switch control testing	50
4.4	The connection diagram of PIR motion device control testing	51
4.5	The connection diagram of image motion sensing control testing	53
4.6	Video recorded log file in microcomputer	55
4.7	Online remote viewing using web browsers	56
4.8	Online remote viewing using mobile phone	56
4.9	The block diagram for ratemeter circuit testing	58
4.10	The plot of linearity for ratemeter in range of 100Hz	59
4.11	The plot of linearity for ratemeter in range of 1kHz	59
4.12	The block diagram for radiation area monitoring testing	61
4.13	Block diagram for alarm link system testing	63
4.14	Data from event alarm code record in webserver at CMS	64
4.15	The SMS message on mobile phone	65
4.16	Location of source tracking on Google map	67

# CHAPTER 1

## INTRODUCTION

### 1.1 Introduction

The events of 11 September 2001 triggered a reconsideration of the risks and consequences of terrorist acts involving nuclear or other radioactive materials [1]. The dangers of radiological dispersal devices (RDDs) or so called dirty bomb were recognized. Nuclear security was started with the awareness that nuclear and other radioactive material, if coming into the wrong hands, could be used in nuclear explosive devices. It has given rise to countermeasures such as radiological material control and physical protection. The fear of radioactivity could create panic, with associated disarray in the society. The dispersed radioactivity would require decontamination which required a big amount of cost and time. Furthermore, a small quantity of the radiation doses could cause long term health effects and long lasting anxiety or psychological disturbances.

In response to a resolution by the IAEA General Conference in September 2002 [2], the IAEA has adopted an integrated approach to protection against nuclear terrorism. This approach coordinates IAEA activities concerned with the physical protection of nuclear material and other radioactive material, the security of radioactive sources, the security in the transport of nuclear and other radioactive material, emergency response and emergency preparedness measures in Member States. In 2006, the guidance for implementing security measures on radioactive sources was provided [2]. It also provides advice on implementing security related provisions in the code of conduct on the safety and security of radioactive sources for the prevention of, detection of, and response to malicious acts involving radioactive sources. It will also help towards preventing the loss of control of such sources. In order to ensure adequate security capability without imposing overly restrictive measures, the concept of security levels was set up. There are three security levels (A, B, and C);

- **Security level A:** Prevent unauthorized removal of a source

- **Security level B:** Minimize the likelihood of unauthorized removal of a source
- **Security level C:** Reduce the likelihood of unauthorized removal of a source.

Among all the security level, the security level A requires the highest degree of security while the other levels are progressively lower.

Nowadays, there is a growing concern that terrorist or criminal groups could gain access to radioactive sources and use the sources maliciously. Due to the dangerous radiation sources used in hospital and industry remain vulnerable to theft. Therefore, the radiation area monitor and associated security system become significant. In Thailand, the project to assist in developing and improving the security system was established for securing the radioactive materials used in medical treatment and industrial irradiation. The project was cooperated between the Office of Atoms for Peace (OAP) Thailand and Global Threat Reduction Initiative (GTRI), US Department of Energy (DOE). More than 10 units of the high activity source were under secured by the system installed and monitored at the central alarm office. The main focus of radioactive source security was about preventing loss of control of the source, either inadvertent or intentional and even malevolent, and thereby inducing a breach of radiation safety.

However, the turn key packages of the installation of the source security system are very costly because they include the engineering design and installation costs. In order to reduce the gap of radiological source securing, the explanation of system installation in proper security must be increased. Therefore, the economical source security system is required to be developed. In this research, the development of a low cost online radioactive source security in associated with inexpensive physical sensing devices was presented.

## 1.2 Objective

To develop an Online Radioactive Source Security System (ORSS) for preventing the radiation source from being lost or stolen.

## 1.3 Scopes

- a) An economical radiation monitor for integration with IP camera system, motion sensing system, GPS tracker, and door assessment system for monitoring the source will be design and construction.
- b) System control software will be developing for supporting of an online source security function.
- c) System online monitoring of alarm signal communication via internet and SMS mobile phone to the security center also developed.
- d) Test of the developed system on radiation source security simulation.

## 1.4 Expected Benefits

The developed system could be used for preventing a high level source removal without authorization at working place such as hospitals and laboratories, with cost effective. This development will gain up the knowledge of source security system for future development.

## 1.5 Literature Review

The research papers and documents related to the development of Radioactive Source Security System were published. The selected paper and documents are summaries as follows:

1. INTERNATIONAL ATOMIC ENERGY AGENCY, (2009), “Security of Radioactive Source, IAEA Nuclear Security Series No.11” which is the guideline for source security. This guideline provides advice on implementing security related provisions in the code of conduct on the safety and security of radioactive sources for the prevention of, detection of, and response to malicious acts involving radioactive



sources. It will also help towards preventing the loss of control of such sources. In order to ensure adequate security capability without imposing overly restrictive measures, the concept of security levels was set up. Three security levels (A, B, and C); **Security level A:** Prevent unauthorized removal of a source. **Security level B:** Minimize the likelihood of unauthorized removal of a source. **Security level C:** Reduce the likelihood of unauthorized removal of a source. The security level A requires the highest degree of security while the other levels are progressively lower [2].

2. Department of ECE Sri V, Engineering College, Tadepalligudem, AP, India, IJECT Vol.3, (2012), this paper research about “The Application of Stolen Radioactive Source Tracking System Based on GSM/GPS Technology”. The developed system could be used for securing the dangerous items like radioactive substances by continuously monitoring. If the secured source is moved from its location or stolen then the door will be automatically closed, monitor probe send an alarm to personal computer and the tracking system tracks the position of the source using GPS and a message also sent the respective mobile using GSM with the location information [3].

3. In 2012, Yosi K et. al. published a research about “Utilizing GPS and SMS for Tracking and Security Lock Application on Android Based Phone”. The case of phone lost has been a major problem these days. This case can happen because of the user own fault or because of intentional phone stolen. Seeing many of this missing case, the researcher tried to develop a system for tracking and securing a missing phone. The Android platform was selected because it was one of the best operating system for mobile phone right now and the user growth was very promising. This application would give an extra security when a phone gone missing, as we know we store a lot of sensitive data on our phone. The system work flow was very simple actually, system application would be on standby and monitor command that it received via SMS and it would work in the background so user won't be get any distraction from this application. Using these commands user could lock his phone, sound the phone alarm, delete his phone data, get his phone data, and get his phone last location. This application have some other feature too, like lock his phone when

someone change his phone card and sent the new number that attach in his phone to the owner. When system got any request about phone's last position then system will process that request to get phone's latitude and longitude via GPS, after that system would quietly sent its information to the owner [4].

4. Wasan W researched about “Development of GPS interfaced Gamma Monitoring System via Mobile Network” in 2012. The research aimed to develop a portable type radiation measuring system with GPS locators that communicate result via mobile network. This system was designed to support both integral and deferential counting and consists of low voltage power supply, pulse amplifier, single channel analyze, timer and ratemeter. The results indicated that the maximum counts for integral counting of the scale is 150 kcps and ratemeter was found to be 100kcps. The counting time could be set from 1 second to 99 minutes. The nonlinearity of LLD and  $\Delta E$  of the single channel analyzer in differential counting system was found to be 0.20% and 0.21% respectively. GPS receiver of system could achieve accuracies of approximately 10 meters. Energy spectrum of Cs-137 obtained by using 2” X 2” NaI(Tl) scintillator detector was very satisfactory with energy calibration linearity of 0.9996 [5].

5. A.O. Oke et. al. published a research, “Development of a microcontroller controlled security door system” in 2009. This paper presented that several security measures which have been employed to combat the menace of insecurity of lives and property. This research was done for preventing unauthorized entrance into buildings through entrance doors by using the conventional and electronic locks, discrete access code and biometric methods such as the finger prints, thumb prints, the iris and facial recognition. In this system, a prototype door security system was designed to allow a pillaged user to access a secure keyless door where the valid smart card authorization guarantees an entry. The model consists of hardware module and software which provides a functionality to allow the door to be controlled through the authentication of smart cards by the microcontroller unit [6].

## **CHAPTER 2**

### **THEORY AND PRINCIPLE**

#### **2.1 Nuclear Security Fundamentals**

The risk that the nuclear or other radioactive material can be used in malicious acts remains high and is regarded as a serious threat to international peace and security. The responsibility for nuclear security rests entirely with each State. Therefore, the appropriate and effective national nuclear security systems are vital in facilitating the peaceful use of nuclear energy and enhancing global efforts to combat nuclear terrorism.

The basic definition for nuclear security is the prevention of, detection of, and response to, criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities, or associated activities. The associated facility is referring to a facility (including associated buildings and equipment) in which nuclear material or other radioactive material is produced, processed, used, handled, stored or disposed of and for which an authorization is required.

##### **2.1.1 Nuclear Safety and Nuclear Security Definition**

According to the International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT) [7], the “radioactive material” means nuclear material and other radioactive substances which contain nuclides which undergo spontaneous disintegration (a process accompanied by emission of one or more types of ionizing radiation, such as alpha, beta, neutron particles and gamma rays) and which may, owing to their radiological or fissile properties, cause death, serious bodily injury or substantial damage to property or to the environment.

There are both natural and manmade radioactive materials. The natural occurring radioactive materials (NORM) are the radioactive materials that exist in the earth crust such as soil, water and rock. The long-lived radioisotopes like U-238, Th-

<sup>232</sup>Pb and <sup>40</sup>K are the common examples of NORM. The cosmic radiation that is emitted from outer space is also a source of natural radiation. Manmade radioactive materials are the artificial radioactive materials that are used in nuclear power plants, medical, industry, agriculture and scientific research. The common examples of manmade radioactive materials are <sup>137</sup>Cs, <sup>60</sup>Co, <sup>138</sup>Ir, <sup>241</sup>Am and <sup>239</sup>Pu.

Nuclear material is defined in the ICSANT and the Convention on the Physical Protection of Nuclear Material (CPPNM) [8] as plutonium, except that with isotopic concentration exceeding 80 percent in plutonium-238; uranium-233; uranium enriched in the isotope 235 or 233; uranium containing the mixture of isotopes as occurring in nature other than in the form of ore or ore residue; or any material containing one or more of the foregoing. Whereby “uranium enriched in the isotope 235 or 233” means uranium containing the isotope 235 or 233 or both in an amount such that the abundance ratio of the sum of these isotopes to the isotope 238 is greater than the ratio of the isotope 235 to the isotope 238 occurring in nature.

According to the definition of the International Atomic Energy Agency (IAEA), the “radioactive source” means radioactive material that is permanently sealed in a capsule or closely bonded, in a solid form and which is not exempt from regulatory control. It also means any radioactive material released if the radioactive source is leaking or broken, but does not mean material encapsulated for disposal, or nuclear material within the nuclear fuel cycles of research and power reactors. Meanwhile, the “orphan source” means a radioactive source which is not under regulatory control, either because it has never been under regulatory control, or because it has been abandoned, lost, misplaced, stolen or transferred without proper authorization.

### **2.1.2 Nuclear Terrorism**

The possibility of terrorist use of nuclear materials was recognized early in the development of nuclear energy. Terrorist attacks since September 11, 2001 have shown these concerns to be well-founded. Typically, the nuclear industry and public safety officials consider only one type of nuclear terrorism i.e. the use of a nuclear

explosive to create a catastrophic incident. However, other forms of nuclear terrorism also pose serious threats.

#### **2.1.2.1 The Definition of Nuclear Terrorism**

So far, there is no single internationally recognized definition for terrorism. Defining terrorism is a complex problem due to the political concerns. However, a specific definition of nuclear terrorism was found in ICSANT (Article 2, Section 1).

Any person commits an offence within the meaning of this Convention if that person unlawfully and intentionally;

- (a) Possesses radioactive material or makes or possesses a device:
  - with the intent to cause death or serious bodily injury
  - with the intent to cause substantial damage to property to the environment
- (b) Uses in any way radioactive material or a device, or uses or damages a nuclear facility in a manner which releases or risks the release of radioactive material:
  - With the intent to cause death or serious bodily injury
  - With the intent to cause substantial damage to property or to the environment
  - With the intent to compel a natural or legal an international organization or state to do or refrain from doing an act.

#### **2.1.2.2 Type of Nuclear Terrorism [7]**

The experts have identified four basic types of nuclear terrorism;

- (a) Acquisition and use of a military nuclear weapon:

The most devastating variant of nuclear terrorism involves a terrorist use of a military nuclear weapon. The same scenarios of Hiroshima and Nagasaki may happen if the terrorist uses the military nuclear weapons. The manufacture of a nuclear weapon by terrorists would be an almost insurmountable challenge. Theft or illicit purchase of a military nuclear weapon is slightly more likely but still a remote possibility.

(b) Theft or diversion of fissile material to construct an “improvised nuclear device” (IND):

This variant of nuclear terrorism involves the construction of an IND. IND can state for nuclear version of improvised explosive devices (IEDs) which often terrorists’ weapon of choice. The INDs differ from military nuclear weapons in yield, reliability, and safety, but these may not be concerned for terrorists. The acquisition of fissile material is the major barrier to IND use but the global stockpile of highly enriched uranium and separated plutonium is enough for constructing several ten-thousands of these devices.

(c) Attacks on nuclear reactors or other facilities to release radioactive material:

The terrorist attack on a nuclear reactor facility could create an incident comparable to or even worse than, the accidents at Chernobyl (1989) or Fukushima (2012). The facility operators usually very attentive to security concerns, but design basis threats may not reflect contemporary terrorist motivations or capabilities. The attack pathway could involve a deliberate breach of reactor containment or disabling the cooling system.

(d) Use of radioactive material for radiological attacks:

There are three possibilities for using radiological materials in a terrorist attack;

- Radiation emission device (RED) – places a radiological source in a location where it can expose a target population to harmful doses of radiation
- Radiological dispersal device (RDD or “dirty bomb”) – uses conventional explosives to disperse radioactive material over a wide area.
- Inhalation, ingestion or immersion (I3) attack – introduces radioactive material into the body via digestive or respiratory systems.

This type of nuclear terrorism has the least potential for physical destruction but could still cause widespread contamination and panic. Furthermore, the radioactive sources that widely used in many countries have remained vulnerability. The low-level radioactive source poses a low risk but should not be ignored as they presented in a very huge quantity.

### **2.1.3 Responsibilities for Safety and Security**

A legal and regulatory framework is the basis for which both safety and security are built on. This framework should define the responsibilities of the State, regulatory authority or authorities and the operating organizations.

#### **2.1.3.1 Responsibility of the State**

The International Nuclear Security Group (INSAG) [9] recommends that it is the responsibility of the state to set up an appropriate legislative regulatory framework to ensure control of nuclear power plants, as well as off the transport and use of nuclear material that present a radiological risk and thus require safety and security provisions. The state must designate a regulatory authority or authority in both the safety and security fields and provide the regulators with the authority, competence and the financial and human resources necessary to accomplish their tasks. More importantly, these regulators should be independent from the nuclear operators and other government entities which are responsible for promoting nuclear power or the use of radioactive material.

It is also the responsibility of the state to define rules for confidentiality and information protection in the security area and carry out checks to ensure the trustworthiness of personnel. They must also verify that the responsibilities in safety and security are well defined and are satisfied.

The operator has the principal responsibility for safety but it cannot alone ensure the protection of a site installation against terrorist threats. The state therefore plays a critical role in ensuring adequate protection. It is directly involved in the assessment of the risk and nature of a potential terrorist attack. It is the responsibility of the state to ensure that the security measures are suited to the various threat situations which may vary over time and to address this, the state typically defines a design basis threat that must be met by the operator, with guidance as to guide how to adjust the defensive capacity to account for the threat situation.

In addition, the State must be prepared to augment the defensive capability of the operator in the event of an attack and, if necessary, to execute an operation to seize back control over the plant. If the threat is a theft of material, the State must

participate in national and international programmes to prevent the theft, or to recover stolen material [9].

### **2.1.3.2 Responsibility of the Regulatory Authorities [9]**

According to the INSAG-24 report, it is the responsibility of the regulator (or regulators) to define the requirement to be satisfied by the operator for both safety and security. It also states that the regulator must also set up and implement a licensing and inspection and enforcement system. It is the regulator's responsibility to ensure that an adequate emergency response system is in place, including various off site elements that are not the responsibility of the operator. In both the safety and security fields, the regulator must also observe international commitment.

Many countries see advantages in having a single regulator responsible for both safety and security due to the closeness of both. This authority may in turn, be dependent on other government entities for assistance on security matters and might be dependent on intelligence information from a specialized agency. It may also turn to police entities for fighting capability to augment the operator's security forces. In the event that the security regulator is separate from the safety authority, it is essential to have a consultation and coordination mechanism between the two regulators to ensure that regulatory requirements are compatible and serve optimally to advance both safety and security [9].

### **2.1.3.3 Responsibility of Operators**

The preliminary responsibility for the safety and security of the nuclear power plant falls on the operating organization, although in the case of security, the operator's responsibility may be limited to defense against a design basis threat. This responsibility placed on the operating organization reflects the reality that operating staff are in the best position to identify the risks arising at the nuclear power plant and to ensure compliance with regulatory requirements. The INSAG recommends that the operators must [9]:



- Design, implement and maintain technical solution and other arrangements to satisfy regulatory requirement relates to both safety and security;
- Ensure first level control;
- Verify the skills and appropriate training of personnel;
- Inform the regulatory authorities of any event likely to affect the safety or security of the nuclear power plant and as appropriate, request support;
- Maintain coordination with State organizations that are involved in safety or security; and
- Implement a quality assurance system in both the safety and security fields.
- Operators should have a centralized information system and a centralized command Centre for directing operations during a safety or security event.

## **2.2 Radioactive Source Protection and Security**

### **2.2.1 Code of Conduct on the Safety and Security**

The IAEA decided to prepare the Code of Conduct on the Safety and Security of Radioactive Sources [10] to serve as guidance to States for the development and harmonization of policies, laws and regulations on the safety and security of radioactive sources.

The scope of the code applies to all radioactive sources that may pose a significant risk to health and the environment. In implementing the code, States should give highest priority to those radioactive sources which pose the most significant risk, i.e. the radioactive source belonging to Category 1 of the IAEA's "Categorization of Radiation Source"; however, in doing so, the State should also devote appropriate attention to the regulation of radioactive source other than those belonging to Category 1.

The code however does not apply to the control of nuclear materials as defined in the convention on the physical protection of nuclear materials and to radioactive sources within military or defense programs. However, such source should be managed in accordance with the principles of this code.

The objective of this code is to achieve and maintain a high level of safety and security of radioactive source through the development, harmonization and enforcement of nation policies, laws and regulation and through the fostering of international co-operation. In particular, this code addresses the establishment of an adequate system for the restoration of such control if has been lost.

This code depends on existing international standards relating to legal and governmental infrastructure for nuclear, radiation, waste and transport safety and to the control of radioactive source and is intended to complement existing international standards in these areas. In implementing this code, States should emphasize and reinforce to manufacturers, suppliers, users and those managing disused source about their responsibility for safety of radioactive sources [10].

The Code defines the role of the IAEA as that who should continue in collecting and disseminating information on laws, regulations and technical standards relating to the safe and secure management of radioactive sources, develop and establish relevant technical standards and provide for the application of these standards at the request of any State, inter alia by advising and assisting on all aspects of the safe and secure management of radioactive sources. In particular the IAEA should implement measures approved by its governing bodies, including pursuant to its Action Plan on Safety of Radiation Sources and the Security of Radioactive Materials [10]. The Code places the responsibility on the State to inform public and private organizations and persons involved in the management of radioactive sources, as appropriate, of the measures it has taken to implement this Code and should take steps to disseminate that information widely.

### **2.2.2 Security Levels and Security Objectives**

The provisions in the Code of Conduct relating to security of radioactive sources have been strengthened to provide measures to reduce the likelihood of malicious acts. A section in the IAEA Nuclear Security Series No. 11, [11] provides guidance to regulatory bodies on how to develop or enhance regulatory programs to address the security of radioactive sources. Safety and security measures should be

designed and implemented in an integrated manner so that they do not compromise each other. One step is to establish graded security level with corresponding goals and objectives.

In order to ensure adequate security capability without imposing overly restrictive measures, the concept to security levels should be used. Three security levels (A, B and C) have been developed to allow specification of security system performance in a graded manner. Security levels A requires the highest of security while the other levels are progressively lower.

Malicious acts can involve either unauthorized removal of a source or sabotage. While the security goals only address unauthorized removal, achievement of the goals will reduce the likelihood of a successful act of sabotage. Security systems that achieve the goals listed to an act of sabotage.

In order to meet the goals, it is necessary to achieve an adequate level of performance for each of the security function: deterrence, detection, delay, and response and security management. That level of performance is defined as a set of objective for each of the function. These objectives state the desired outcome from the combination object. Deterrence is a security function which is difficult to quantify. Consequently, it has not been assigned and associated set of security objectives and measures in this publication [11]. Security levels and associated security objectives are summarized in Appendix C.

### **2.2.3 Considerations for Assigning Security Levels**

The regulatory body could use categories to assign the security level applicable to a given source. The purpose of categorizing radioactive sources is to provide an internationally accepted basis for risk informed decision making, including measures to reduce the likelihood of malicious acts. The regulatory body, taking account of its national threat, may wish to enhance the security of sources in Category 4 and 5 sources in appropriate circumstances. This approach is summarized in Appendix D. The goal of security level A is to prevent the unauthorized removal of radioactive source. If an attempt at unauthorized access or unauthorized removal were

to occur, detection and assessment have to occur early enough to enable response personnel to respond with enough time and with sufficient resources to interrupt the adversary and prevent the source from being removed. In order to achieve this goal, the following measures are recommended as shown in Appendix E.

## **2.3 Radiation Source Security System**

### **2.3.1 Security Functions**

A security system for protecting radioactive source from an adversary intent on committing a malicious act should be designed to perform basic security functions such as: deterrence, detection, delay, and response and security management:

Deterrence occurs when a motivated adversary is dissuaded from undertaking the attempt to perform a malicious act. Deterrent measures must have the effect of convincing the adversary that the malicious act would be too difficult and the success of the act is too uncertain.

Detection is the discovery of an attempted or actual intrusion which could have the objective of unauthorized removal or sabotage of a radioactive source. It can be achieved by visual observation, video surveillance, electronic sensors, accountancy records, seals and other tamper indication devices, process monitoring systems and other means, adversary awareness of detection measures can also serve as a deterrent.

Delay on the other hand impedes an adversary's attempt to gain unauthorized access or to remove or sabotage a radioactive source, generally through barriers or other physical means. A measure of delay is the factor of time after detection that is required by an adversary to remove or sabotage the radioactive source. Adversary awareness of delay barriers can also serve as a deterrent.

Response involves the action undertaken following detection to prevent an adversary from succeeding or to mitigate potentially severe consequences. These actions typically performed by security or law enforcement personnel and other state agencies include interrupting and subduing an adversary while the attempted unauthorized removal or sabotage is in progress, preventing the adversary from using

the radioactive source to cause harmful consequences, recovering the radioactive source or otherwise reducing the severity of the consequences. The prospect of successful response can also serve as a deterrent [11].

Security management is the handling and ensuring of adequate resources such as personnel and funding for the security of source. It also includes developing procedures, policies, record and plans for the security of source and for a more effective security culture in general. This term also includes developing procedures for the proper handling of sensitive information and protecting it against unauthorized disclosure [11].

### **2.3.2 Design and Evaluation of Security Systems [11]**

A well designed security system should integrate measure to perform all five security functions so as to effectively secure the target from the threat, consistent with the following security concepts:

**Deterrence cannot measure:** the objective of deterrence is to dissuade an adversary from attempting a malicious act. As a result, the impact of deterrent measures cannot be quantified. Therefore, the design of a security system should not be wholly based on deterrence.

**Detection before delay:** the function of delay is to provide response personnel with sufficient time to deploy and interrupt or interdict the adversary's efforts to complete a malicious act. There, detection must precede delay. If an adversary is given the opportunity to overcome barriers and other obstacle prior to encountering intrusion sensor or other detection mean the adversary will have completed the most or difficult tasks before being detected and truss may well succeed in removing or sabotaging the radioactive source before the response personnel arrive. In this case, barriers do not serve as a delay but rather at most as deterrents.

**Detection requires assessment:** most means of detection provide an indirect indication off potential malicious action, such as attempted unauthorized access, removal or sabotage of a radioactive source. The only direct indication is by direct human observation. Therefore, when an alarm or direct indication is triggered, there is

always some uncertainty as to the cause. As a result, detection should always be complemented by assessment to determine the cause of the alarm. Alarm assessment requires human observation and judgment, though deployment of response personnel to investigate the cause of the alarm, though remote closed circuit television (CCTV) systems or similar means. Sometimes adversaries may attempt to exploit any delay between detection and assessment to mask their malicious intent. Therefore, immediate assessment is the goal of any security system.

**Delay greater than assessment plus response time:** A security system is successful if it detects and a correct assessment is made of an adversary attempting a malicious act in sufficient time for subsequent delay measures to permit response personnel to interrupt and stop the adversary prior to completion of the act or to initiate prompt actions to mitigate potentially high consequences. This relationship of the functions of detection, delay and response is known as timely detection.

**Balanced protection:** this is a concept of equivalent security functions (deterrence, detection, delay, response and security management) that provides adequate protection against all threats along all possible pathways. In other words, delay time through each pathway, detection measures associated with each detection element and the resulting response provide the necessary protection to prevent a successful act.

**Defense in depth:** A concept of several layers and methods of protection (structural, technical, personnel and organization) that have to be overcome or circumvented by an adversary in order to achieve their objective.

### **2.3.3 Integration of Safety and Security Measures [11]**

Safety measures and security measures have in common the aim of protecting human life and health and the environment. Safety measures and security measures should be designed and implemented in an integrated manner so that security measures do not compromise safety. In implementing the recommendations in this guide, the designers of security systems should consult with qualified safety experts to ensure

that security measures do not compromise the safety of individuals or the protection of the environment.

## **2.4 Radiation Area Monitoring System**

### **2.4.1 Type of Radiation Area Monitor**

Radiation area monitoring devices (as shown in Figure 2.1) are divided into two types, i.e., the portable area monitoring devices and the fixed area monitoring devices.

- a) A portable area monitoring devices, often known as survey meters or portable monitors, are used to measure external ionizing radiation dose rates or levels of radioactive contamination on surfaces.
- b) Fixed area monitoring devices, generally designed in two categories, i.e., external radiation monitor and airborne radioactive contaminants monitor.
  - External radiation monitor, a fixed area monitor for external ionizing radiation is used in a specific location to indicate variations in the radiation field and provide an alarm if the radiations dose rate, or the integrated radiation dose at that location exceeds a specified level.
  - Airborne radioactive contaminants monitor, a fixed area monitor for airborne radioactive contaminants is used in a specific location to measure the concentration of radionuclides in the air.

### **2.4.2 Structure of Radiation Area Monitor**

The basic structure of radiation area monitor (as shown in Figure 2.2) is composed of the gamma detector with integral counting system, analog ratemeter, alarm control system, and the alarm indicators like audible buzzer and LED. In modern radiation area monitor, the digital display and the programmable dose rate thresholds are included. The wireless, Ethernet and cellular communication and external power supply with battery backup are provided for optional devices.



(a) A portable area monitor



(b) A fixed area monitor

Figure 2.1 Radiation area monitoring system

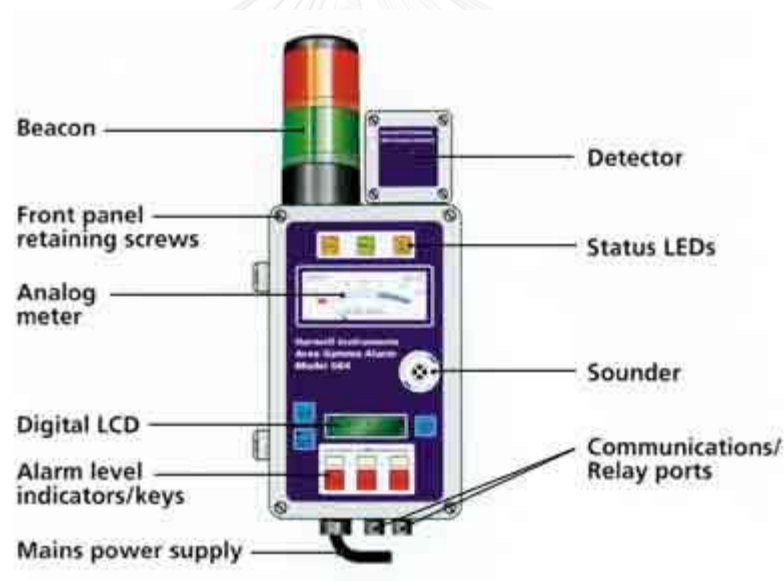


Figure 2.2 Structure of radiation area monitoring system

## 2.5 Physical Protection System

The source security system is a combination system of radiation security equipment and physical protection equipment. The following are the implementing on physical protection guide on Security of Radioactive Sources IAEA NSS No. 11.



### **2.5.1 Access Control**

Access controls can be exercised through entry checkpoints controlled by response personnel and the use of electronic readers or key control measures technology, in the form of automatic access control system (AACSS). The AACSSs are available in various forms, from simple pushbutton mechanical devices to more sophisticated readers that respond to proximity tokens or individual biometric characteristics. By integrating with a turnstile, an AACSS can also incorporate controls to inhibit practices such as pass back and tailgating. In most cases, the use of a card should be verified by a PIN keyed into the reader and in high security situations an AACSS entry point should be supervised by a guard positioned within view. The essential factor for prospective operators is to specify viable AACSS that is appropriate to the requirement and can be supported locally by a manufacturer or installer. It is also important to limit access to the AACSS management computers and software to prevent unauthorized interference with the system database. For the places where conventional lock and key is used as a means of control, the locks should be of quality and the key management procedures should be designed to prevent unauthorized access or compromise.

### **2.5.2 Intrusion Detection**

These systems are the useful means of monitoring the security of an unoccupied area. The technology can be extended to the outer area of an establishment use of a perimeter intrusion detection and assessment system. All intrusion detection systems should be supported by a response to investigate alarm events or conditions. Alarm can shoulder remotely at a security control point or locally through a high volume sounder. CCTV can be a useful aid in providing initial verification of events within an alarmed zone per area but should normally be backed up by a patrol making a visual check or investigation.

### **2.5.3 CCTV Surveillance**

CCTV is a useful and which security staff to monitor outer approaches and areas where radioactive source are stored. Cameras can be combined with an intrusion detection system (IDS) to provide event activated camera views. However, to be fully effective, the performance of CCTV cameras and monitors should be regularly assessed to ensure that they continue to display imagery of good quality. System should also be supported by a response so that alarm events and indications activated by technology can be investigated.

### **2.5.4 Communication**

Security personnel at all levels should be provided with effective and reliable forms of communication. This includes communication between patrols, fixed posts and the local reporting or control center. An effective communication should also be established to the external agencies responsible for providing rapid response to security events.

### **2.5.5 Key Control Procedures**

Keys which allow access to radioactive sources should be controlled and secured. These may be keys to cages, doors, storage containers or shielded units within which sources are used. Similar levels of control should be applied to duplicate and spare keys.

### **2.5.6 Locks, Hinges and Interlocks for Doors**

Locks used for the protection of radioactive sources should be of good quality and incorporating with the features that will offer some resistance to forcible attack. The same requirement applies to hinges on doors. Keys should be safeguarded in the manner outlined above under the procedural measures. Within premises, interlock

doors that meet safety requirements can serve the interests of security by controlling the movement of personnel and allowing staff to monitor access to the facility.

### **2.5.7 Locked, Shielded Containers**

Shielding and fixed units containing radioactive sources can provide protection, and can delay any attempt to interfere with the source. However, when staff members are not present, the area should be covered by an intruder detection alarm system to alert the response personnel or security response of the need to investigate the circumstances of any intrusion.

### **2.5.8 Standby Power**

Security control rooms and security systems should be able to cope with power dips or outright loss of a main electricity supply. This can be ensured through an uninterruptible power supply and a standby generator which automatically starts when a fluctuation in power levels is detected. Battery backup has only limited duration and should, therefore, be viewed as a short term source of standby power.

# **CHAPTER 3**

## **DESIGN AND CONSTRUCTION OF A RADIOACTIVE SOURCE SECURITY SYSTEM (ORSS)**

### **3.1 System Configuration Design**

In this research, the source security system was designed in according to the guidance of IAEA security level A and the guideline for Security of Radioactive Sources IAEA NSS No. 11, as mentioned in Chapter 2. The basic knowledge of nuclear security, nuclear radiation detection, physical protection system, electronic circuit and computer programming were integrated in the radioactive source security system development.

#### **3.1.1 Criteria for System Design**

The system must be provided a full function protection (delay, detect, response) of the radioactive source which categorized at A/D more than 10 [12], to prevent the removal of the radioactive source from the storage room by the unauthorized person. The design concept of the system included the instant active detection against any unauthorized person access to the source secured areas; with the multiple alarm sensing layers and also alarm signal communication to responsible personal. A source tracking system was also included to address the condition which the physical sensing system was blocked by the intruder. In the ORSS, the system structure could be divided into 2 major parts; a) a microcontroller based alarm control system, and b) a microcomputer based central alarm monitoring system in cooperation with mobile phone network communication. In the preliminary research stage, the various inexpensive sensors such as digital keypad door access control device, door switch, optical sensor, motion sensor, CCTV surveillance system and GPS tracker were studied in association with the Radiation Area Monitor (RAM). The window threshold alarm setting function (lower background and high gamma alarms) was employed in the RAM [14]. The appropriate sensing devices were selected and

employed in the microcontroller based alarm control system. The system integration of Online Radioactive Source Security (ORS) system, sending alarms signal via the wifi internet, was developed as illustrated in the block diagram as shown in Figure 3.1. The UPS back up also applied to the system for preventing the system error from power line failure.

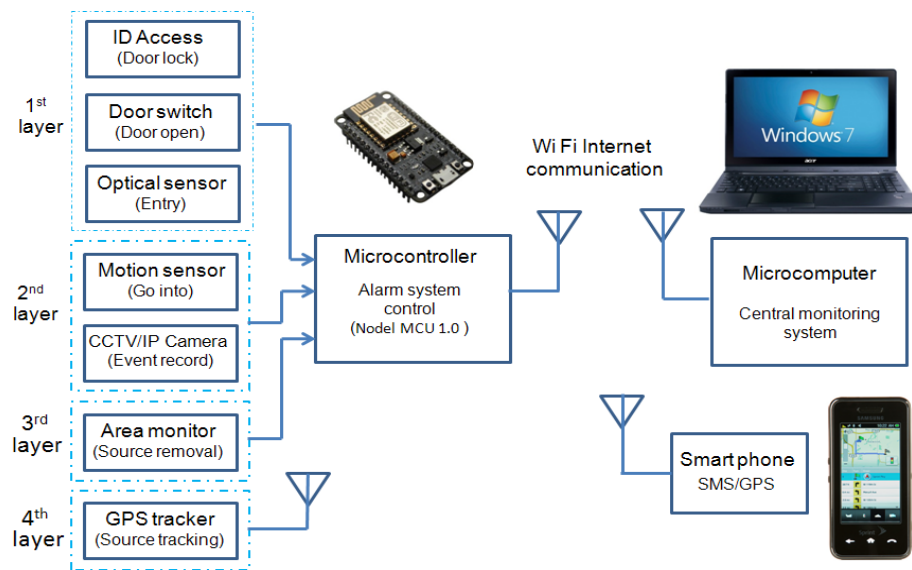


Figure 3.1 Block diagram of online radioactive source security system

### 3.1.2 System Structure Design

The development kit of ESP8266, NodeMCU, integrates GPIO, PWM, IIC, 1-wire and ADC all in one board with wifi module [13] was employed to develop a microcontroller based alarm control system. Four alarm sensing layers was arranged for supporting the source security function in action of delay, detect, and responses to prevent unauthorized person attempt to access to the secured source. Each alarm sensing layer consists of a set of physical sensing as follows:

*First layer:* Three physical sensors of digital keypad door access control device, door switch, and optical IR sensing device were installed for entering sequential checking. The door was locked by electromagnetic device. If unauthorized person

entered wrong code, the digital key coded ID access device would be locked for 10 minutes. This would be the action in delay entry step. In the case of the adversary break the door and go into the other sensors, the alarm signal would be generated.

*Second layer:* Two physical protection devices of motion sensor and 2 sets of IP camera were installed, one for entrance door independent viewing and another one for secured source viewing with image motion sensing. The IP camera could be used for both video record in web server and remote viewing online via web browser. The alarm events recorded could be searched by record index for video clips replay in case of investigation need. This would be the action in first step of detection when unauthorized person access to source storage.

*Third layer:* The radiation area monitor was installed for radiation alarm triggering when the radiation level was out of discrimination window. The gamma counted by scintillation detector was converted into voltage level and sent to Analog to Digital Converter (ADC) input which would then be used to compare the setting alarm levels. If the secured source moved pass through RAM, the high gamma alarm would be generated. In case of the source was moved out of storage room, the low background alarm would be generated. These alarms would trigger the system to send SMS message of GPS calling number every 5 minutes to mobile phone. This would be the action in second step of detection.

*Fourth layer:* The GPS tracker was hidden somewhere on a source shielding. When the responsible person called the GPS tracker, it would send the message of position of the source located to the respective mobile using GSM. The source location could be tracked by Google map. This would be active in response step, if the alarm system was jammed.

All alarm signals generated from each alarm sensing layer were set in active low condition, for detection the loss of signal if the sensor was removed or the cable was cut and would be interfaced to the microcontroller with system control software and online linked to the microcomputer at central monitoring system via the wifi internet. After the alarm system was activated, the entrance door would be automatically locked. The alarm signal output was also applied to activate the audio/visual warning devices at both source storage room and CMS for alerting security guard to respond

the alarm event. These alarm events would be displayed at Central Monitoring Station (CMS) and saved into the web server with information of date, time and video included. The event summary could be searched form the web server.

### 3.1.3 Inexpensive Sensor Devices Selection

In this system designed, the inexpensive sensor devices were provided from the local electronic markets and shops. The local available sensing devices such as: ID access key, door switch, optical sensor, motion sensor, IP camera and GPS trackers were employed in each section as follows:

- **Personal identify access or ID access**

The 4 x 4 keypad matrix was employed for keypad door access control system. The matrix bus was interfaced to microcontroller port for keypad access controller as shown in Figure 3.2. To control authorized person, the username ID and password could be set. The password and username could also be displayed on LCD.

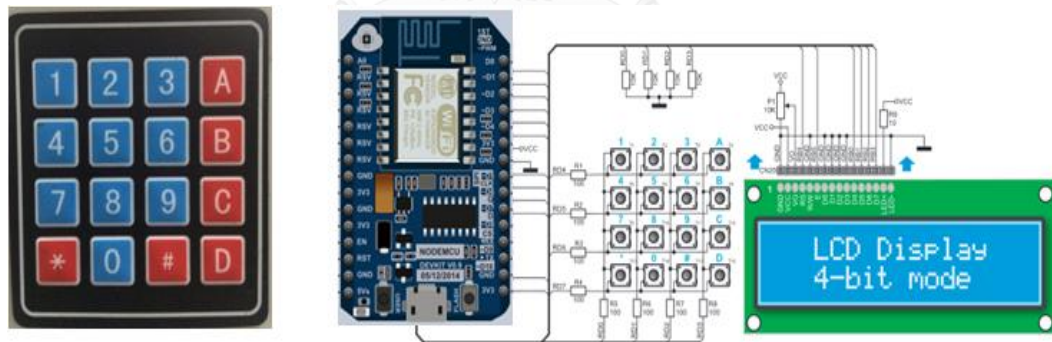


Figure 3.2 Keypad door access control system

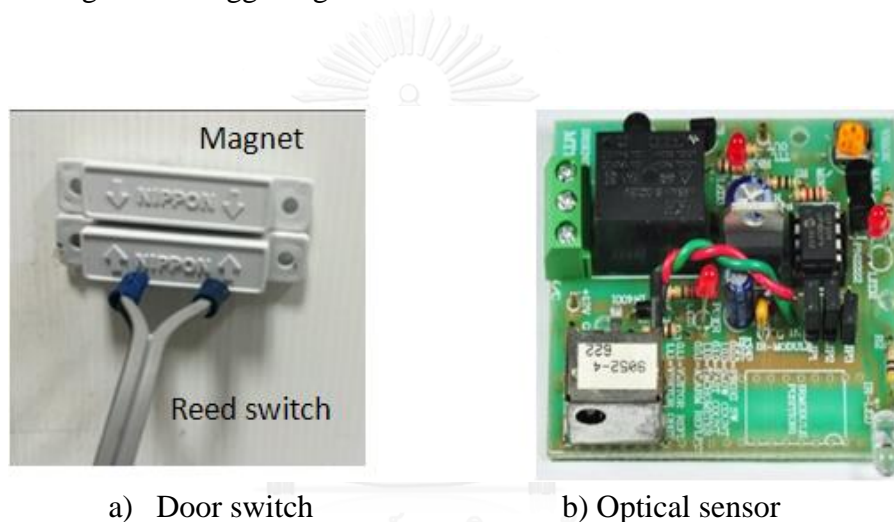
- **Door switch**

The inexpensive magnetic switch which composed of a pair of magnet and reed switch, commonly used in home security, as shown in Figure 3.3 (a), was selected for door sensing device. The contact status of door open and closed from magnetic switch was interfaced to the microcontroller. For the door open status, the

detecting signal assigned in manner of active low. If an authorized person enters the correct password the door would be automatic open and wait until door switch closed.

- **Optical sensor (IR sensor)**

A circuit module of infrared (IR) optical sensor, model MT150, was employ for a person pass through the entrance door. The module composed of IR receiver and IR-LED emitter with 5 V operating voltage, as shown in Figure 3.3 (b). The sensing operation could be configured as transmission or reflection interfaced to microcontroller port. When an unauthorized person passed through the door the IR sensor would generate trigger signal and sent alarm code information to CMS.



a) Door switch

b) Optical sensor

Figure 3.3 First layer physical sensing devices

The keypad door access system generated both the alarm signal with SMS information and the door lock signal to control the electromagnetic door lock while the door switch and optical sensor generated only the alarm signal with SMS information. Figure 3.4 shows the diagram of three physical protection sensors connection for first layer.



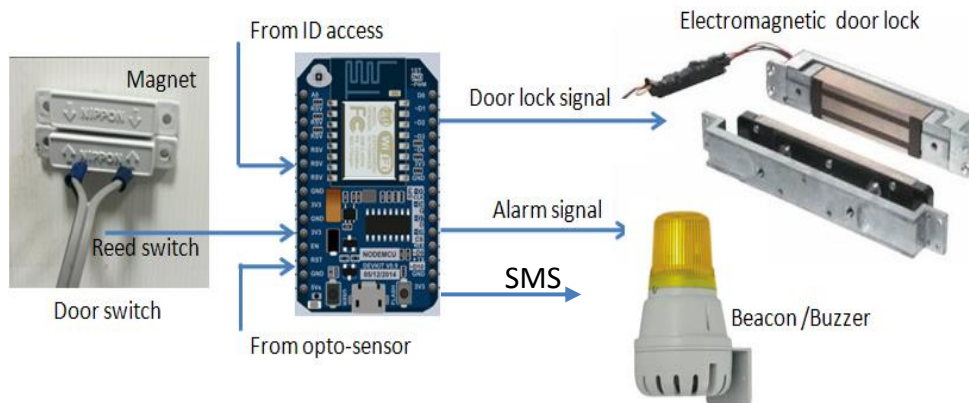


Figure 3.4 Diagram of first layer physical protection sensors connection

- **Motion sensor**

A compact module of pyroelectric infrared (PIR) motion sensor was employed to detect the presence movement of human body inside the room. The module composed of Fresnel lens and motion detection IC with 5 V operating voltage and the response time and sensitivity adjustment, as shown in Figure 3.5. When a human motion detected the trigger signal would activate the microcontroller and alarm signal was generated.



(a) Motion detection circuit board



(b) The PIR module with Fresnel lens

Figure 3.5 Motion sensor

- **CCTV/IP camera**

Two model of IP camera i.e., NEOCAM IP camera and VSTARCAM IP camera were selected for surveillance system, as shown in Figure 3.6. They were different in features; the NEOCAM IP camera capable for image motion sensing and remote monitoring via mobile phone while VSTARCAM IP camera was used only for video recording. The VSTARCAM IP camera was set for video recording in the source storage room and NEOCAM IP camera was interfaced to microcontroller for image motion sensing and supported for remote monitoring via mobile phone.



(a) NeoCAM IP camera (b) VSTARCAM IP camera

Figure 3.6 Two IP cameras for monitoring

Two physical protection devices of PIR motion sensor and image motion sensing mode from NEOCAM IP camera were employed for detection an unauthorized person access into the source storage area. The alarm signal would be generated with SMS information when the human motion detected in the surveillance area. Figure 3.7 shows the diagram of two physical protection sensors connection for second layer.

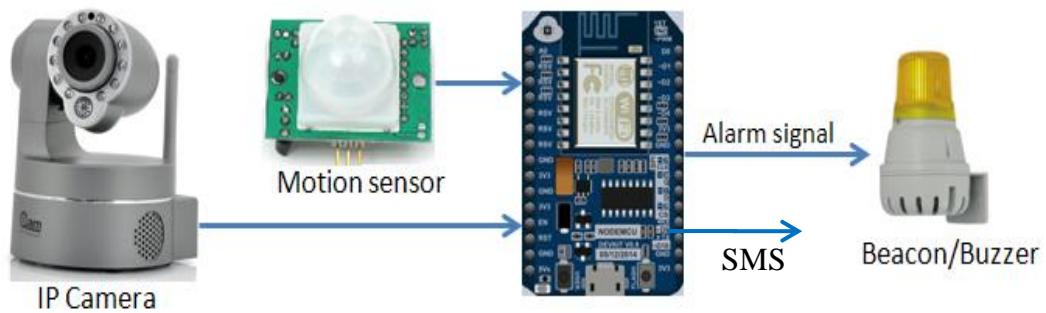


Figure 3.7 Diagram of second layer physical protection sensors connection

- **GPS tracker**

The GSM/GPRS tracker was applied for tracking the source location in case of the source security system jammed and the radioactive source was moved out of the security area. The local available compact GPS tracker with sensitivity of 159 dBm and operating frequency range of 850/900/1800/1900MHz was selected. Location tracking of radioactive source could be done by the responsible person called the GPS tracker. It would send the message of position of the source located back to the respective mobile using GSM. The source location could be tracked by Google map running by the application software on mobile phone or personal computer, as shown in Figure 3.8



Figure 3.8 Location tracking using GPS tracker

### 3.2 Economical Radiation Area Monitor Development

As mentioned in Chapter 2, the radioactive source security system was a combination of the physical protection system and radiation monitoring system. The inexpensive physical sensing devices were selected as mentioned above. For a radiation monitoring system, an economical radiation area monitor was developed as detailed in 3.2.

#### 3.2.1 Radiation Area Monitor Design

The fixed radiation area monitor (RAM) composed of two main parts i.e., gamma scintillation detector and integral counting system with analog ratemeter and voltage amplifier, as shown in Figure 3.9. This system was the source security in third layer of system.

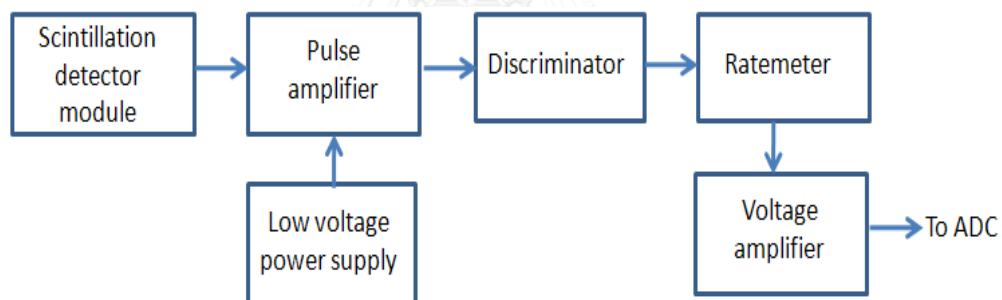


Figure 3.9 Block diagram of a radiation area monitor

The radiation area monitor was developed by using the detector assembly module and all the nuclear measuring circuit modules used were developed by the Center of Excellent for Nuclear Material Analysis and Testing (NucMAT) as following details:

- **Gamma Scintillation Detector**

The scintillation detector module composed of 1" x 1" NaI(Tl) scintillation crystal coupled with PMT (Photomultiplier tubes) module of Hamamatsu H10722 which a built in module of metal package PMT, adjustable high voltage circuit,

preamplifier and amplifier. The PMT module operated at +5V and -5V power supply. The detector assembled shows in Figure 3.10.

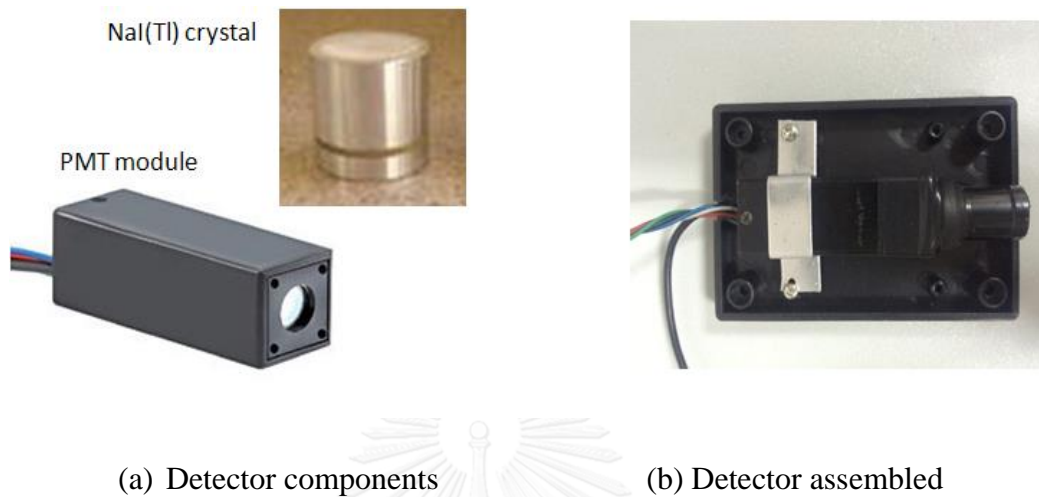


Figure 3.10 The scintillation detector module

- **Integral Counting System Assembly**

The developed circuit module of pulse amplifier, discriminator, ratemeter and voltage amplifier were assembled in the main system housing. The gamma counted signal from scintillation detector was amplified then discriminated the noise by discriminator before converted into voltage level by ratemeter. Since the signal output from ratemeter was 100 mV full scales, therefore, the voltage amplifier was applied for gained up the signal into 3 V for the built in ADC input range in the microcontroller.

### 3.2.2 Gamma Alarm Setting

The radioactive decay is a random process. In any measuring the count rate each, the frequency of occurrence gamma counting value follows some probability distribution such as normal distribution (Gaussian's). Due to these distributions, the discrimination between gamma background counts and sample counts must be distinguished correctly. The alarm threshold setting value can be expressed in terms

of sigma with coefficient N, or as the coefficient of the standard deviation of the background count rates [14], as shown in equation (1).

$$\text{Alarm threshold} = (N \times \sigma) + BG_{\text{avg}} \dots\dots\dots (1)$$

Where sigma ( $\sigma$ ) is the standard deviation of the average background (background count)<sup>1/2</sup> and N is the number entered. Figure 3.11 illustrated the concept of gamma alarm threshold setting. For high background level detection, N may set above 4 times of gamma sigma.

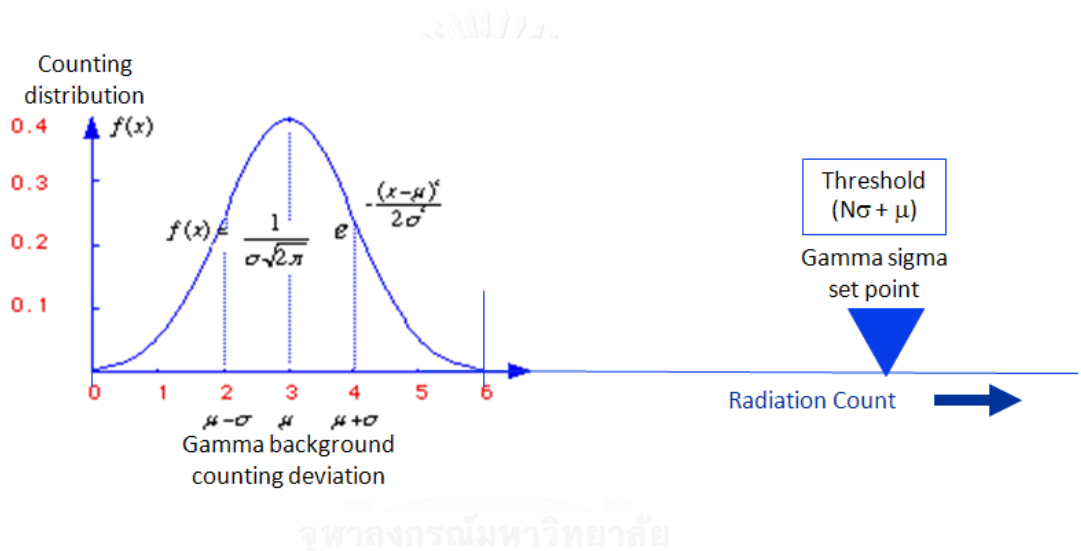


Figure 3.11 Radiation alarm threshold setting

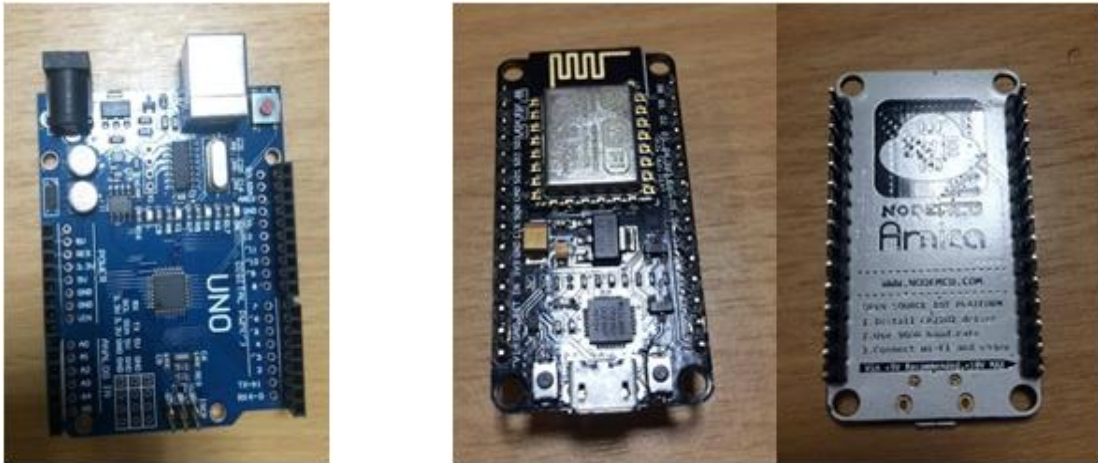
**3.3 Online Radioactive Source Security Hardware Design**

The online radioactive source security hardware design was done in according to the requirement of system structure design from 3.1. There were two main part of the system i.e., the microcontroller based alarm control system and the microcomputer based central alarm monitoring system.

**3.3.1 Microcontroller Based Alarm Control System**

Two microcontroller sets of NodeMCU 1.0 (ESP8266) kit and Arduino UNO board, as shown in Figure 3.12 (a) and (b) respectively, were employed to develop a microcontroller base alarm control system. Both microcontrollers have different in on

board function support and could be interfaced to each other with the signal level 5 V and 3.3 V.



(a) Arduino UNO Board

(b) NodeMCU ESP8266 with wifi Board

Figure 3.12 The Microcontroller kit for alarm control system development

The alarm control system would support the source security function in 4 layers of alarm sensing in action of delay, detect, response to prevent unauthorized person attempt to access to the secured source. All detecting output of physical protection sensor included the alarm signal generated output were interfaced to the microcontroller port. The design feature was explained as follows:

**Arduino UNO board:** the input/output port assigned for ID access control keypad decoding, door switch detection and interface to NodeMCU board. The input/output port also assigned for interfacing to LCD display board.

**NodeMCU development kit board:** the input port assigned for detection the sensing signal of optical sensor, motion sensor, image output sensor and RAM. The output port assigned to drive a beacon/buzzer, electromagnetic door lock device. The built in ADC also applied to support window alarm detection in association of RAM.

Schematic diagram of the microcontroller based alarm control system shows in Figure 3.13. The sensor signal would couple to the input port via opto-transistor

with a pull down resistor. When any of sensors was activated the microcontroller would generate alarm signal with alarm information code to web server at CMS and also sent alarm code to mobile phone.

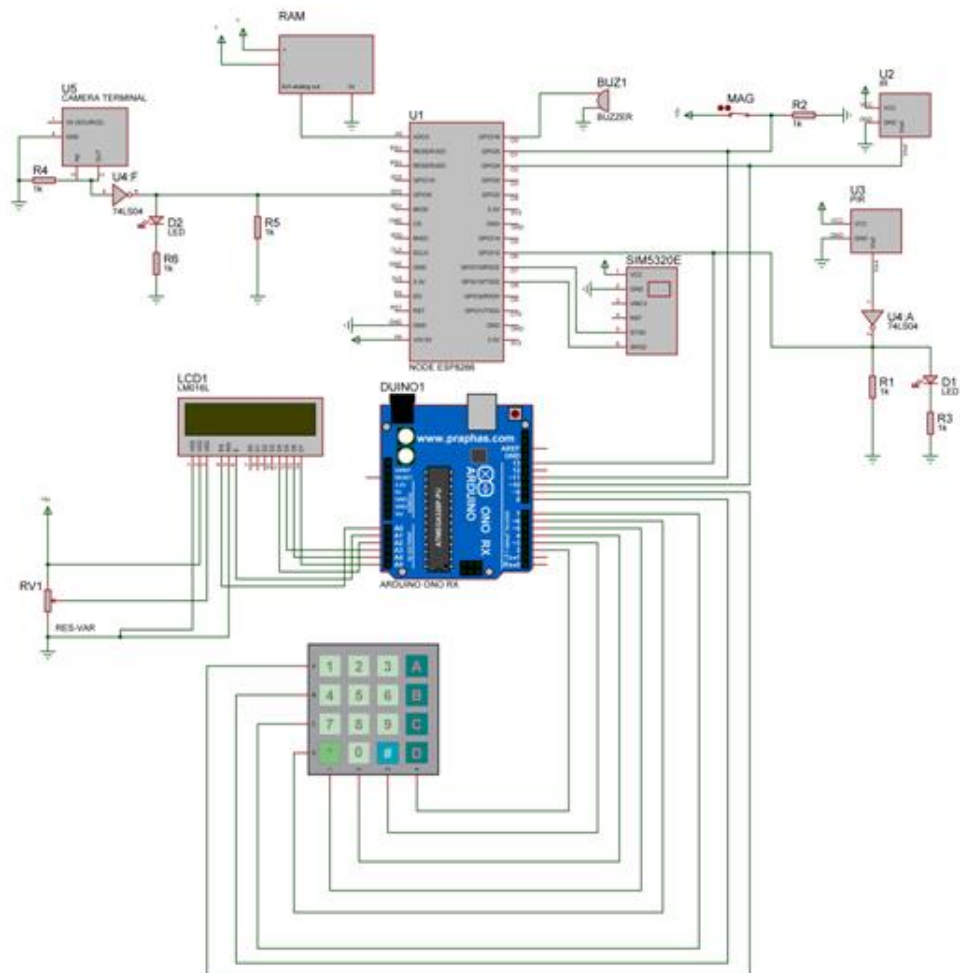


Figure 3.13 Schematic diagram of microcontroller based alarm control system

### 3.3.2 Microcomputer Based Central Alarm Monitoring System

A microcomputer with wifi connected was set up for central alarm monitoring system. The monitoring system was designed in operation of multi-window display, for viewing of real time video image from IP camera and alarm event status with information page, as shown in Figure 3.14. The alarm event with information and video image were recorded in web server. The video image could view by both of



multi-window display on computer screen and viewing online via mobile phone. However, video image could be recorded in both memory card and web server. The detail of communication link between the alarm control system and the central alarm monitoring system are explained in details.

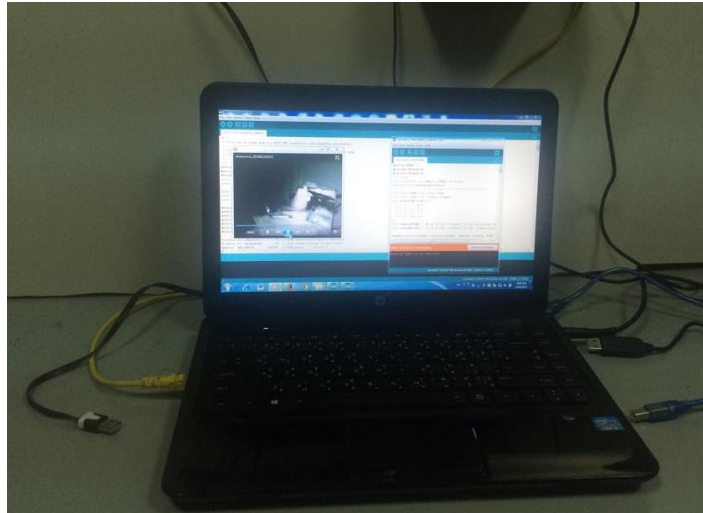


Figure 3.14 Computer for monitoring system

### 3.3.2.1 Alarm Link between Alarm Control and Central Alarm

#### Monitoring Stations

All alarm signals generated from each alarm in 4 layers would be interfaced to the microcontroller port and sent to the central monitoring system (CMS) via the wifi internet, the alarm signal output was also used to activate the audio/visual warning devices at both source storage room and CMS for security guard response. These alarm events would be displayed at CMS and saved into the web server with date, time, alarm information include video clip records in computer. The event summary could be searched form the web server.

For follow up the situation in source storage room, responsible person could view the surveillance area in online by browser or mobile phone, and could also be monitored by the microcomputer at CMS. All action of unauthorized person such as enter password, try to open the entrance door, movement inside room or move

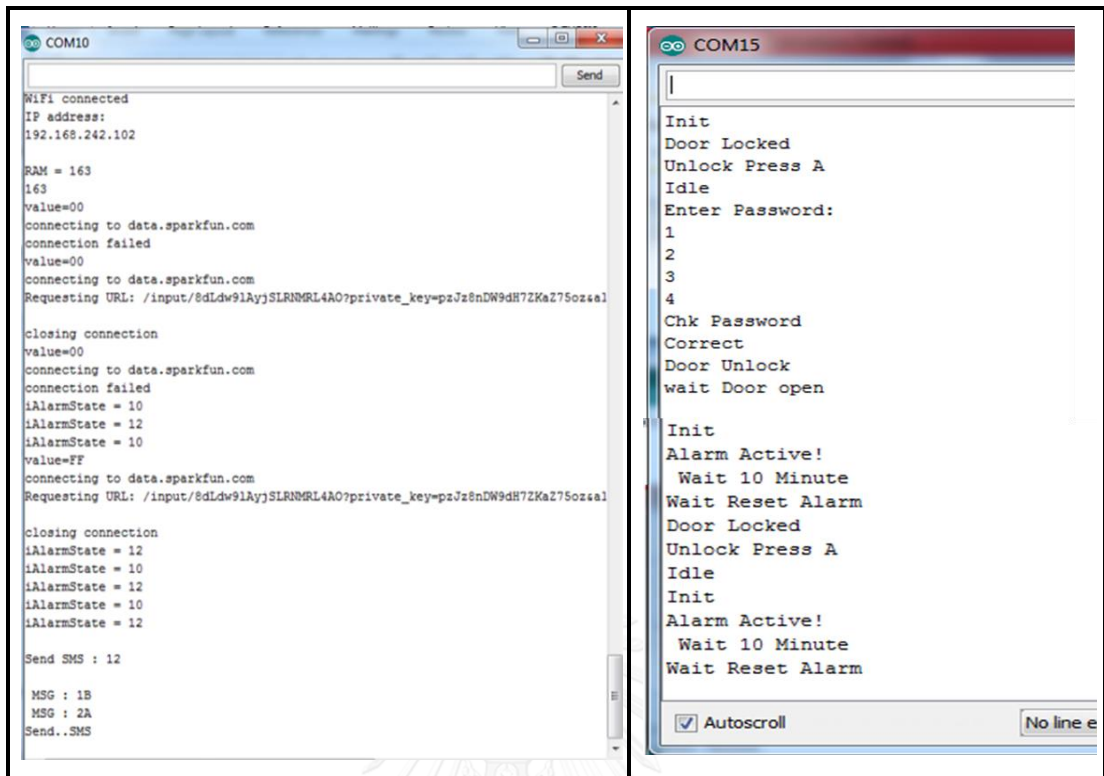
radioactive source, were displayed on screen, as shown in Figure 3.15. When the alarm signal generated it would be link to CMS and alert the security guard.

### **3.3.2.2 Alarm link to Mobile Phone**

The microcontroller would generate alarm message of each alarm layer sensor binding with the corresponded time of alarm event and link to the SMS (Short Message Service) sender. The responsible personal would alert via SMS on mobile phone and could be got the alarm information as shown in Figure 3.16.

### **3.3.2.3 Tracking Link to Mobile Phone Design**

The GPS tracker could be fixed on source shielding. In case of the security system failure and the secured source was moved out of security area, the responsible person could call the GPS tracker in order to tracking the location. The GPS tracker would send the message of position of the source location back to the respective mobile using GSM as shown in Figure 3.17 (a). The source location could be tracked by the Google Map application software on mobile phone or personal computer as shown in Figure 3.17 (b).



(a) Screen for displaying alarm status      (b) Screen for displaying ID access

Figure 3.15 Example of alarm display status of system

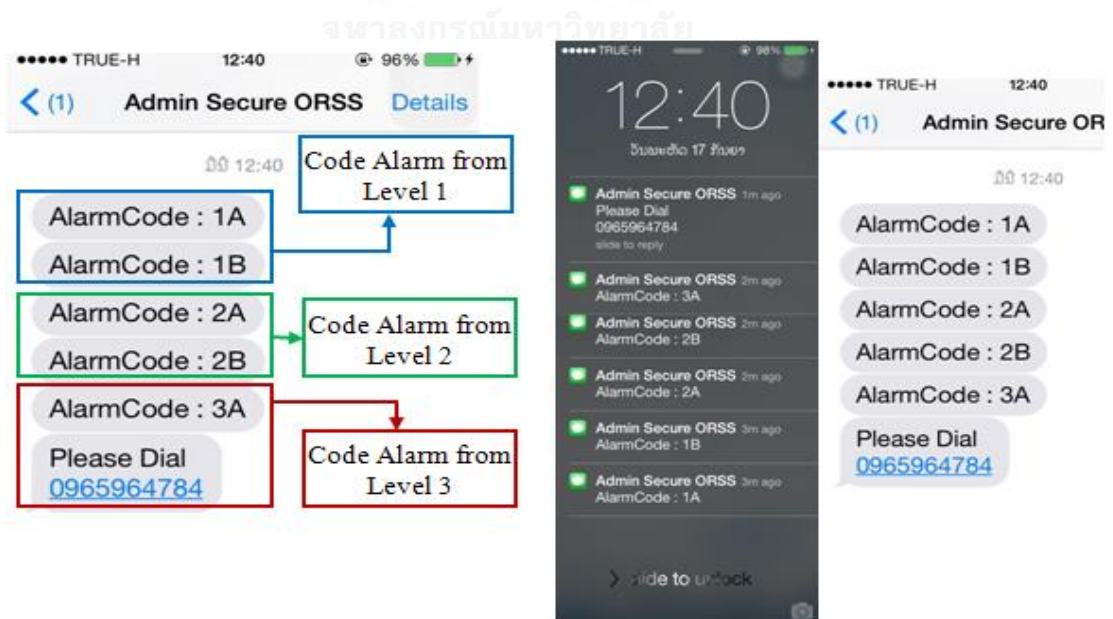
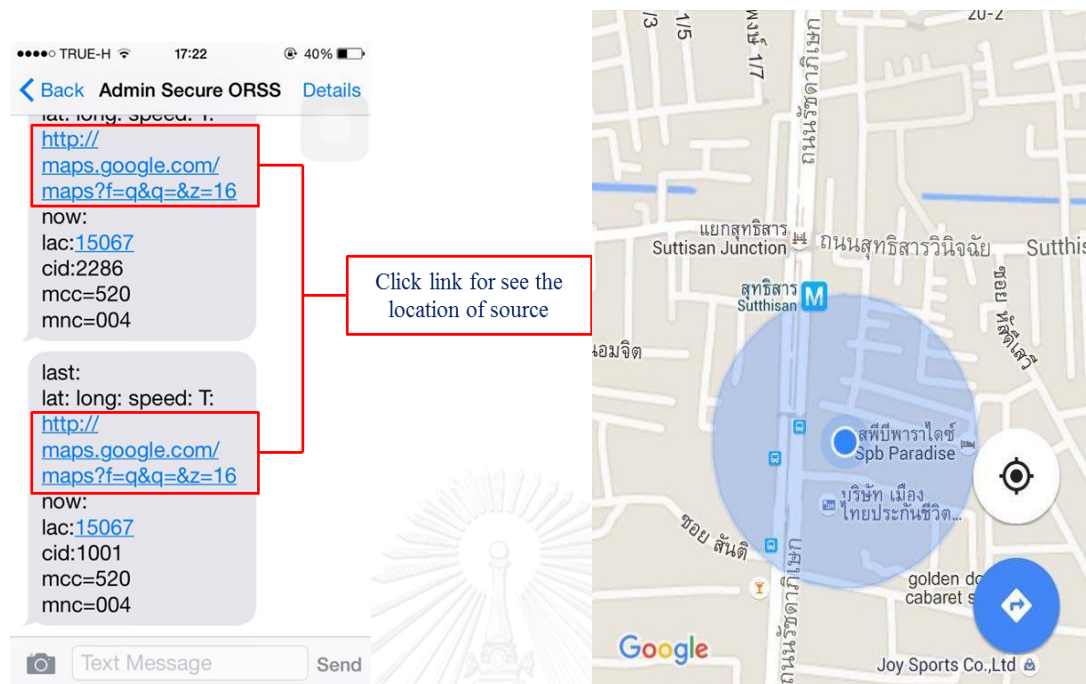


Figure 3.16 The SMS message on mobile phone



(a) Screen for display alarm status

(b) Screen for display ID access

Figure 3.17 The GPS tracking information

### 3.4 System Control Program Design

The Arduino software [15] was used in system control software development. A software structure was designed in association with hardware signal determination for properly working with the circuit operation of online radioactive source security system development. The flowchart of system control program was created as shown in Figure 3.18.

#### 3.4.1 Operating Step of System

In system start up, the system control program was designed for running an online system status checking and routine checking the sensor loop of each alarm layer. When alarm active signal was detected, the alarm event message and data were

organized. The system control software would automatically recheck the connection between the security system and CMS for preventing operation failure.

All alarm signals contained important information such as the sensor code, the date and time for displaying on the alarm event format, were sent via communication network such as wifi to the central monitoring station and SMS by the Global System for Mobile communication (GSM) to mobile phone. The alarm event report would be displayed on central monitoring system display screen and also displayed on mobile phone. The event summaries were recorded with event information in the web server. Alarm warning signal could be reset by acknowledgement of a responsible person.

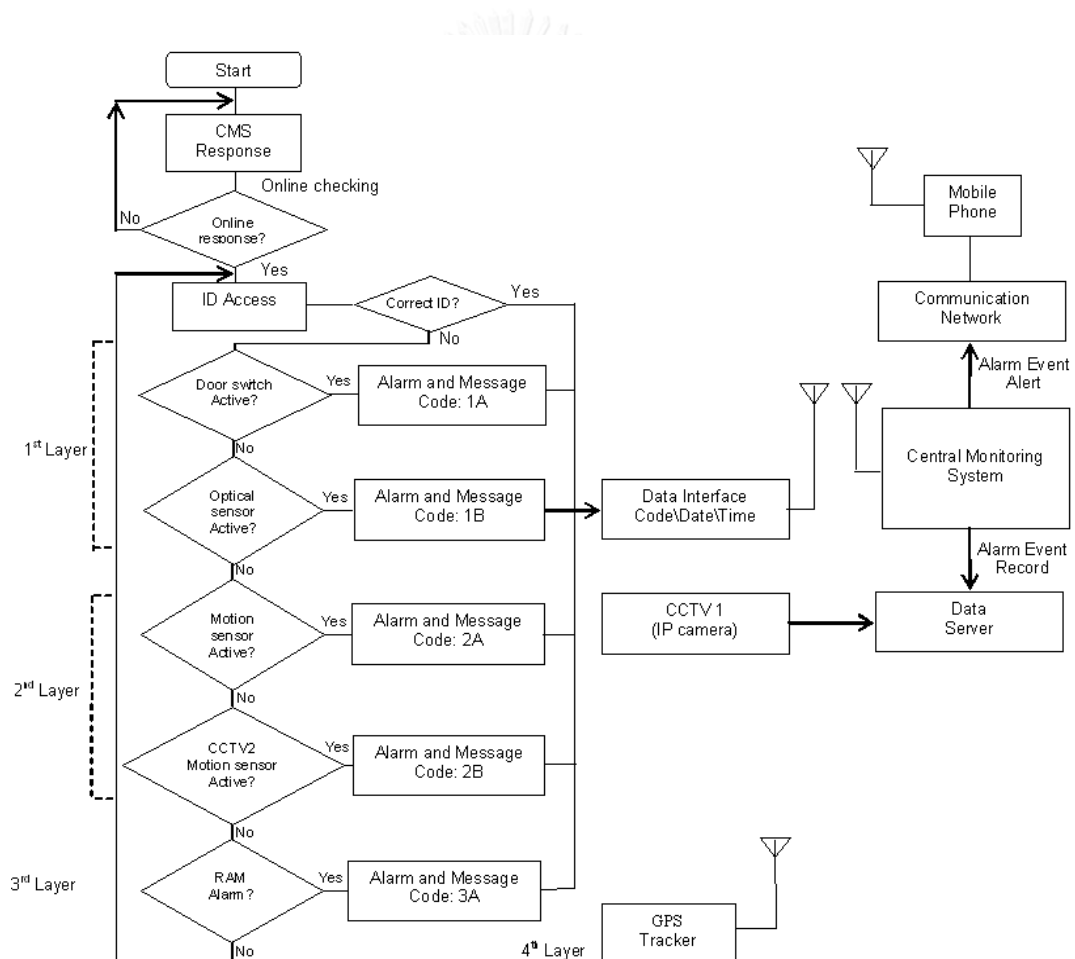


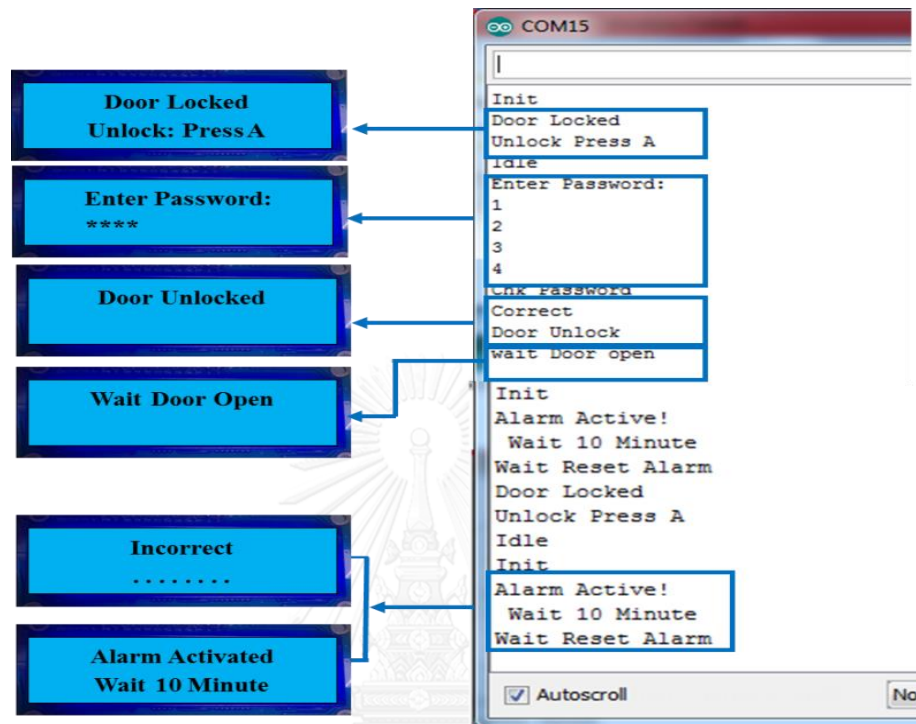
Figure 3.18 Flow chart of the system control software

In personal ID access, the system divided in 2 conditions, i.e., authorized personal entry and unauthorized personal entry. In case of authorized person input the ID code without error in 3 times confirmed, the alarm system would be set on inactive status. In case of unauthorized person attempted to access to secure area at working place and entered the wrong ID code 3 times, the system would trigger the alarm and sent the alarm code information to CMS. If an unauthorized person attempted to go inside by breaking the entrance door, the alarm system was still active. The first layer sensors included door switch and optical IR sensor would generate the alarm signal. If there was breaking in by the other way, the second layer sensors (motion sensor and IP camera 2 with image motion sensing) would be activated and alarm signal were generated and also the video signal from camera were recorded and sent online to web server. The third layer of detection, radiation area monitor, was activated if the intruder moved the source from secured location. The alarm signal regarding gamma level detection, high gamma alarm or low background alarm as window threshold alarm setting, was activated. In this case, alarm signal would trigger the system to alert the responsible person by sending out the SMS message of GPS calling number every 1 minute to mobile phone.

### **3.4.2 Keypad Door Access Control system**

The software was designed for keypad door access control system of 4 x 4 matrix keypad. Operating step for entering was determined. The number of password ID could be set. In case of authorized person input the ID code without error in 3 times confirmed, the alarm system would be set on inactive status. In case of unauthorized person attempted to access to secure area at working place and entered the wrong ID code more than 3 times, the system would trigger the alarm and sent the alarm code information to CMS. If enter correct password the electromagnetic door lock device would be open, status would show door unlock and wait for door open without alarm, then the system wait until door close. If over time limit the system would be locked and need to wait until 10 minute. But if enter wrong password more than 3 times the electromagnetic door lock device would not unlock and display show incorrect. Door access system display on LCD could also display in the same

information on CMS monitor as shown in Figure 3.19. The password ID could be added on by the responsible person or administrator person only for security control.



(a) Display on LCD at radiation room (b) display On computer at CMS Figure

Figure 3.19 Door access system display

### 3.5 Online Radioactive Source Security System Assembly

The circuit board of all physical sensors and the developed radiation area monitor module were assembled in main housing as compact unit. The integration system operation also setup for full function testing. Assembling details are listed as follows:

#### 3.5.1 System Prototype Assembly

The circuit board of microcontroller, keypad, LCD, radiation area monitor and low voltage power supply were installed in the prototype box with dimension of

(25cm x 22cm x 10cm). The top view of the circuit board fixing and cable wiring were shown in Figure 3.20. Keypad and display installed on front panel for performing testing and checking the data (as shown in Figure 3.21). Electrical connector terminal for all sensors was provided at rear panel, as shown in Figure 3.22.

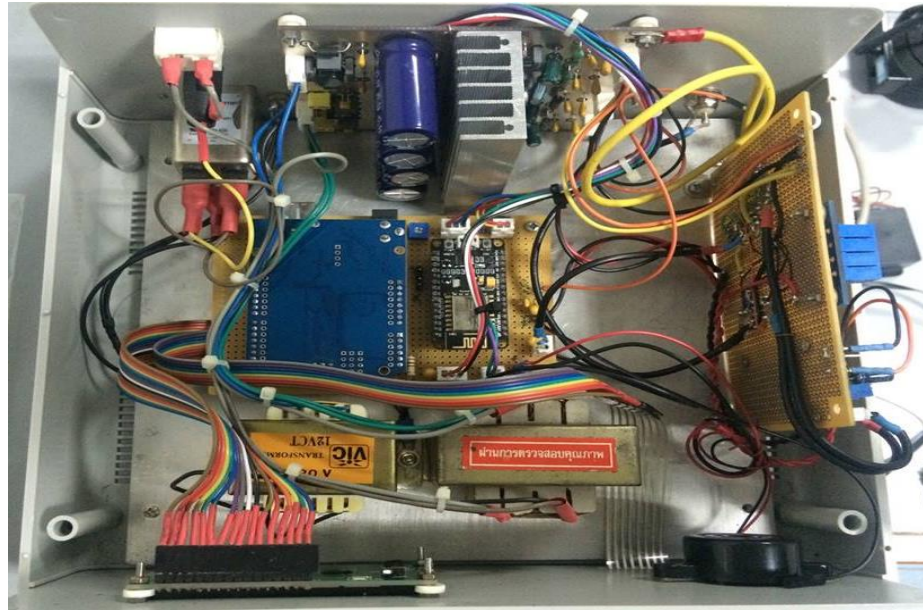


Figure 3.20 Top views of the developed ORSS

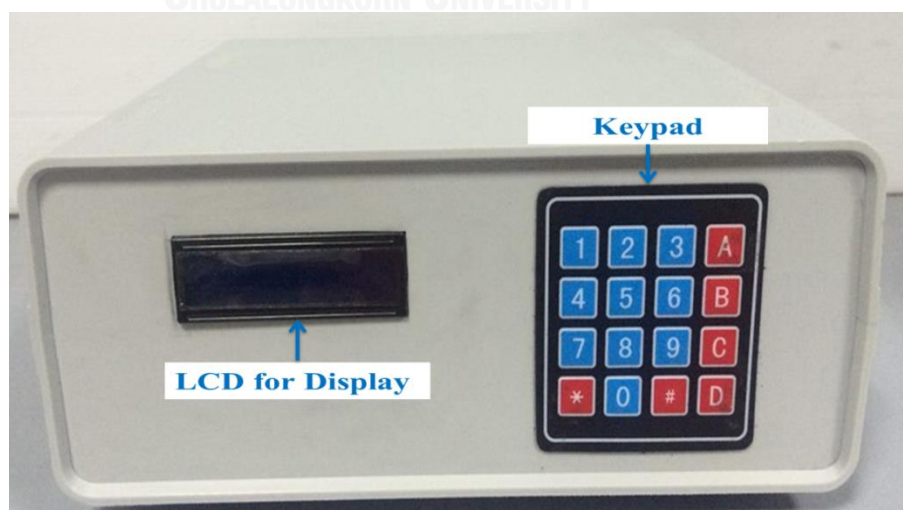


Figure 3.21 Front view of ORSS assembly



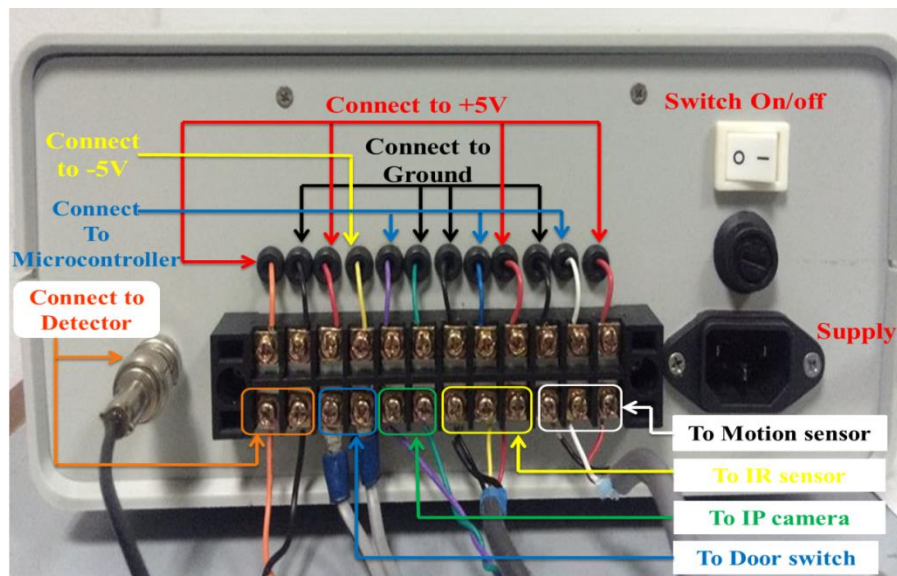


Figure 3.22 Rear view of ORSS assembly

### 3.5.2 System under Test

The ORSS system which assembled with physical protection sensors i.e., door switch, IR optical sensor, CCTV 1, CCTV 2 (image motion sensor) and developed radiation area monitor was setup for full testing. Four layers alarm sensing in action of delay, detect and response for prevention unauthorized person access to the secured radioactive source would be determined in Chapter 4. The system setup was illustrated in Figure 3.23.

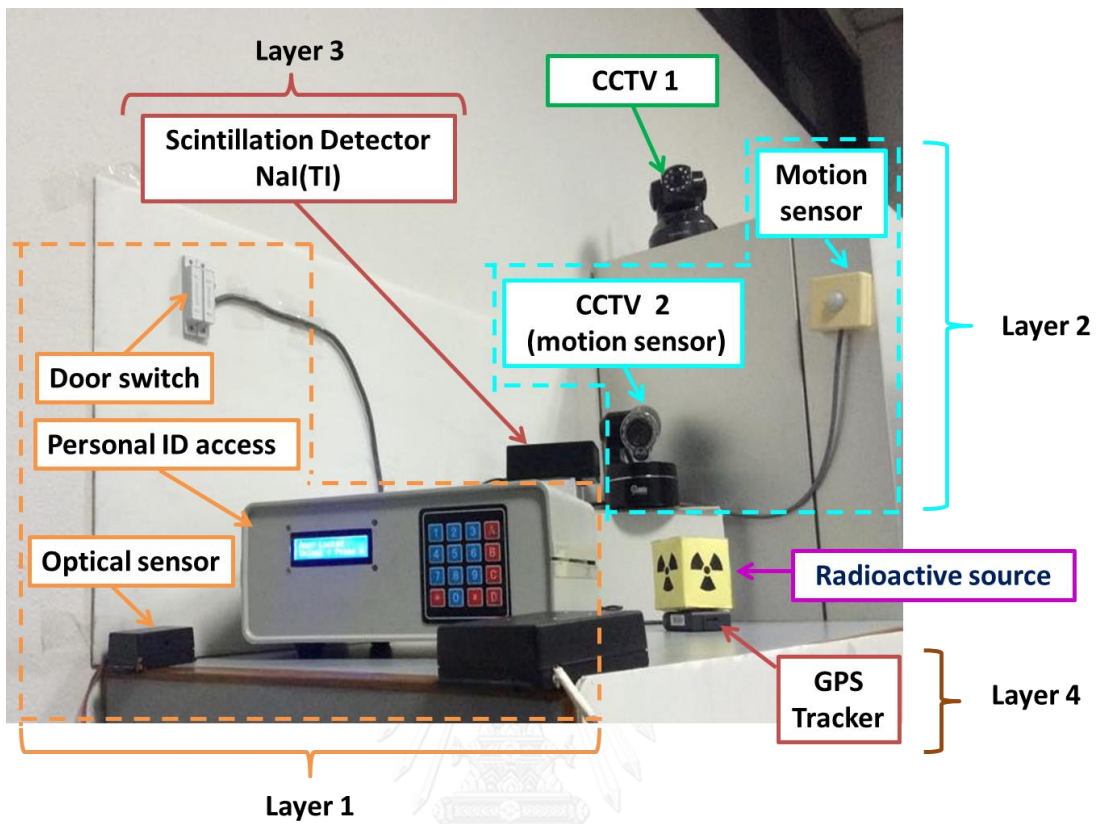


Figure 3.23 Full function of system setup of ORSS

## **CHAPTER 4**

### **EXPERIMENTAL RESULTS**

Capability and performance of the developed Online Radioactive Source Security (ORSS) system were tested. The system testing was divided into 4 main parts as follows:

1. Physical sensing devices control testing
2. Radiation area monitoring testing
3. Online communication testing
4. Full operation of ORSS system testing

#### **4.1 Physical Sensing Devices Control Testing**

This development aimed to use inexpensive physical protection sensors which were locally available. Some of inexpensive sensors devices such as IR optical sensor and PIR motion sensors were limited in full specification. Some parts developed in laboratory. Therefore, the reliability of all sensing devices in each protection layer was tested.

##### **4.1.1 Instrument and Equipment**

- Microcontroller board with developed interfacing hardware and control software
- Microcomputer with interfacing system
- Physical sensing devices
- Beacon/Buzzer alarm set
- Low voltage power supply of Hewlett Packard model 6284A

## 4.1.2 Keypad Door Access Control Device Testing

### 4.1.2.1 Methodology

- Connect the keypad of 4 x 4 matrixes to the microcontroller board with control software in associated with microcomputer and alarm devices, as shown in Figure 4.1.
- Enter the correct password and wrong password in repeating of 10 times. Observe the status of display and alarm action.
- The tested results showed in Table 4.1.

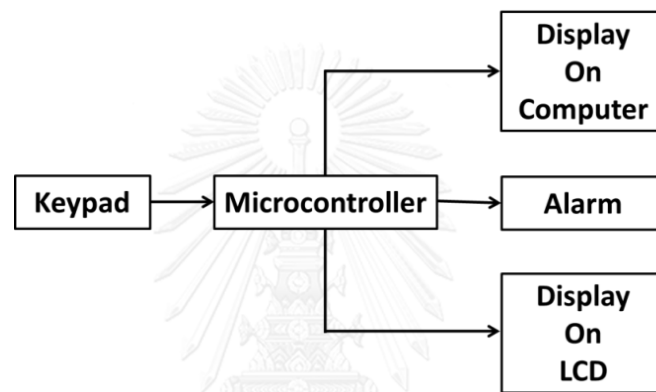


Figure 4.1 The connection diagram of keypad door access control device testing

Table 4.1 The result of keypad door access control device testing.

No.	Wrong password		Correct password		Wrong password in 3 times	
	LCD Display	Status	LCD Display	Status	LCD Display	Status
1	Please try again	Alarm	Door open	No alarm	Wait 10 minute	No alarm
2	Please try again	Alarm	Door open	No alarm	Wait 10 minute	No alarm
3	Please try again	Alarm	Door open	No alarm	Wait 10 minute	No alarm
4	Please try again	Alarm	Door open	No alarm	Wait 10 minute	No alarm
5	Please try again	Alarm	Door open	No alarm	Wait 10 minute	No alarm
6	Please try again	Alarm	Door open	No alarm	Wait 10 minute	No alarm
7	Please try again	Alarm	Door open	No alarm	Wait 10 minute	No alarm
8	Please try again	Alarm	Door open	No alarm	Wait 10 minute	No alarm
9	Please try again	Alarm	Door open	No alarm	Wait 10 minute	No alarm
10	Please try again	Alarm	Door open	No alarm	Wait 10 minute	No alarm

#### 4.1.2.2 Result and Discussion

Table 4.2 shows the tested result of entering wrong and correct password before open the door and also the wrong password for three times with the door closed. The results showed that the developed system was able to distinguish between authorized password and unauthorized password. In case of the adversary attempt to open the door without the correct password, the alarm could be triggered. If the system received the wrong password for three times, it could be disabled to key in password for 10 minutes. This could be delay the unauthorized person went into the security area.

#### 4.1.3 Door Switch Device Control Testing

##### 4.1.3.1 Methodology

- Connect the door switch to the microcontroller board with control software in associated with keypad door access control and alarm devices, as shown in Figure 4.2.
- Enter the correct password and wrong password with open/close the door switch in repeating of 10 times. Observe the status of alarm action.
- The tested results showed in Table 4.2.

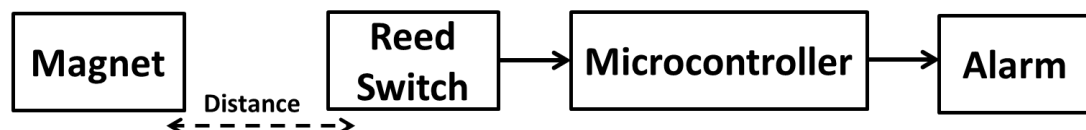


Figure 4.2 The connection diagram of door switch control testing

Table 4.2 The result of door switch device control testing.

No.	Wrong password		Correct password		Wrong password in 3 times	
	Door switch	Status	Door switch	Status	Door switch	Status
1	Open	Alarm	open	No alarm	open	Alarm
2	Open	Alarm	open	No alarm	open	Alarm
3	Open	Alarm	open	No alarm	open	Alarm
4	Open	Alarm	open	No alarm	open	Alarm
5	Open	Alarm	open	No alarm	open	Alarm
6	Open	Alarm	open	No alarm	open	Alarm
7	Open	Alarm	open	No alarm	open	Alarm
8	Open	Alarm	open	No alarm	open	Alarm
9	Open	Alarm	open	No alarm	open	Alarm
10	Open	Alarm	open	No alarm	open	Alarm

#### 4.1.3.2 Result and Discussion

Table 4.2 shows the tested result of door switch operation, when entering in wrong and correct password then open the door switch and also the wrong password for three times with the door switch open. If the door switch closed after the alarm triggered, the door could automatically locked. The results showed that the developed system work properly and could be functioned as the second alarm trigger for prevention of an unauthorized person went into the security area.

#### 4.1.4 IR Optical Switch Sensing Device Control Testing

##### 4.1.4.1 Methodology

- Connect the IR optical switch (model MT 510) to the microcontroller board with control software in associated with keypad door access control and alarm devices, as shown in Figure 4.3.
- The transmission sensing configuration was set. The sensing sensitivity was tested by varying the distance between IR source and receiver in range of 50 to 250 cm with an increasing distance of 50 cm.
- Pass through the sensor without access to the door switch system, in repeating of 10 times. Observe the status alarm action.

- The tested results showed in Table 4.3.

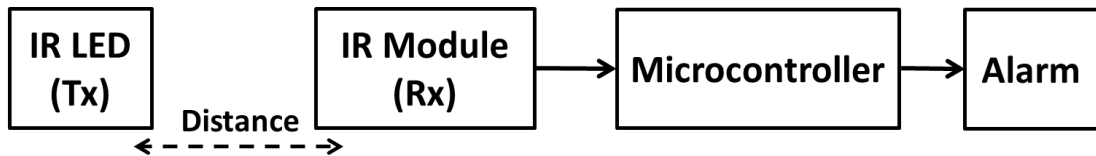


Figure 4.3 The connection diagram of IR optical switch control testing

Table 4.3 The result of IR optical sensing device control testing.

No.	Alarm action at distance between IR source and receiver				
	50 cm	100 cm	150 cm	200 cm	250 cm
1	Alarm	Alarm	Alarm	Alarm	Alarm
2	Alarm	Alarm	Alarm	Alarm	Alarm
3	Alarm	Alarm	Alarm	Alarm	Alarm
4	Alarm	Alarm	Alarm	Alarm	Alarm
5	Alarm	Alarm	Alarm	Alarm	Alarm
6	Alarm	Alarm	Alarm	Alarm	Alarm
7	Alarm	Alarm	Alarm	Alarm	Alarm
8	Alarm	Alarm	Alarm	Alarm	Alarm
9	Alarm	Alarm	Alarm	Alarm	Alarm
10	Alarm	Alarm	Alarm	Alarm	Alarm

#### 4.1.4.2 Result and Discussion

Table 4.3 shows the tested result of IR optical switch status; when a person passed through the path way by break the door or without open the door. The IR optical sensing device could trigger the alarm device at distance between IR source and receiver in range of 50 to 250 cm without error found. This sensitivity was good enough to be used in the ORSS system as a pass through sensor which could be placed at somewhere of path way. The results showed that the developed system work properly when setup the transmission distance between IR source and receiver up to

250 cm and could be function as the third alarm trigger for prevention of an unauthorized person went into the security area.

#### 4.1.5 PIR Motion Sensing Device Control Testing

##### 4.1.5.1 Methodology

- Connect the PIR motion sensor to the microcontroller board with control software in associated with keypad door access control and alarm devices, as shown in Figure 4.4.
- The PIR motion sensor with Fresnel lens was set. The sensitivity was tested by varying the sensing distance of human movement away from the sensor in range of 40 to 160 cm with increasing distance of 20 cm.
- Went into the security area without open the door switch in repeating of 10 times at each motion distance testing. Observe the status alarm action.
- The tested results showed in Table 4.4.

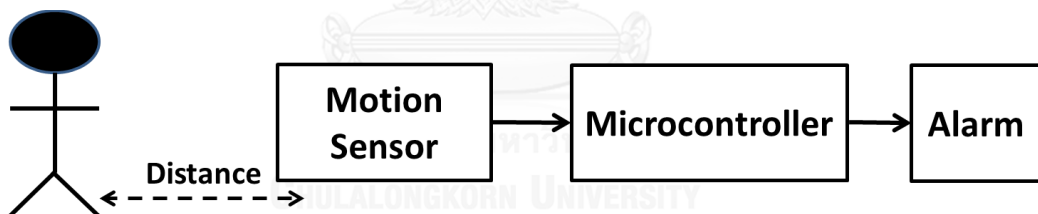


Figure 4.4 The connection diagram of PIR motion device control testing



Table 4.4 The result of sensitivity for PIR motion sensing device control testing.

No.	Motion distance at front view (cm)						Motion distance at side view (cm)			
	40	60	80	100	120	140	160	20	40	60
1	Alarm	Alarm	Alarm	Alarm	Alarm	Alarm	No alarm	Alarm	Alarm	No alarm
2	Alarm	Alarm	Alarm	Alarm	Alarm	Alarm	No alarm	Alarm	Alarm	No alarm
3	Alarm	Alarm	Alarm	Alarm	Alarm	Alarm	No alarm	Alarm	Alarm	No alarm
4	Alarm	Alarm	Alarm	Alarm	Alarm	Alarm	No alarm	Alarm	Alarm	No alarm
5	Alarm	Alarm	Alarm	Alarm	Alarm	Alarm	No alarm	Alarm	Alarm	No alarm
6	Alarm	Alarm	Alarm	Alarm	Alarm	Alarm	No alarm	Alarm	Alarm	No alarm
7	Alarm	Alarm	Alarm	Alarm	Alarm	Alarm	No alarm	Alarm	Alarm	No alarm
8	Alarm	Alarm	Alarm	Alarm	Alarm	Alarm	No alarm	Alarm	Alarm	No alarm
9	Alarm	Alarm	Alarm	Alarm	Alarm	Alarm	No alarm	Alarm	Alarm	No alarm
10	Alarm	Alarm	Alarm	Alarm	Alarm	Alarm	No alarm	Alarm	Alarm	No alarm

#### 4.1.5.2 Result and Discussion

Table 4.4 shows the tested result of PIR motion sensing device sensitivity, when a person went into radioactive source security area. This PIR motion sensing device could trigger the alarm device at maximum distance of 140 cm and 40 cm away from the sensor at front and side views, respectively. For improving sensitivity in covering large area, more set of PIR motion sensing device need to be installed. The results showed that the developed system using only one motion sensor could work properly when preventing small area. This could be function as the first alarm trigger in the second alarm layer for detection of an unauthorized person movement at source security area.

#### 4.1.6 Image Motion Sensing Device Control Testing

The IP camera with image motion sensing function was employed for surveillance of radioactive source at security area. When the image movement was found in viewing display, the motion sensing signal could trigger the alarm device. The IP camera could also be video record in computer or SD card. The device control testing would be conducted both alarm triggering and video recording.

##### 4.1.6.1 Methodology

- Connect the IP camera with image motion sensing function to the microcontroller board with control software in associated with keypad door access control and alarm devices as shown in Figure 4.5.
- The sensitivity was tested by setting the image motion sensing time at 1, 2 and 5 seconds in two conditions of room lights, switched on and off.
- Went into the security area without open the door in repeating of 10 times at each motion sensing time testing. Observe the status alarm action.
- The tested results showed in Table 4.5.

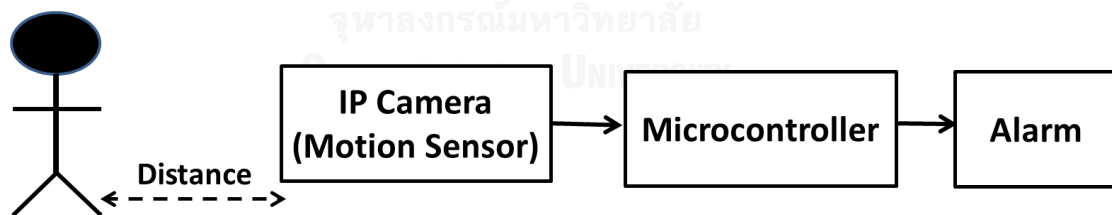


Figure 4.5 The connection diagram of image motion sensing control testing

Table 4.5 The result of sensitivity for image motion sensing control testing.

No.	Room lights turn on			Room lights turn off		
	Motion sensing time (seconds)			Motion sensing time (seconds)		
	5	2	1	5	2	1
1	Alarm	Alarm	Alarm	Alarm	Alarm	Alarm
2	Alarm	Alarm	Alarm	Alarm	Alarm	Alarm
3	Alarm	Alarm	Alarm	Alarm	Alarm	Alarm
4	Alarm	No Alarm	Alarm	Alarm	Alarm	Alarm
5	Alarm	Alarm	Alarm	Alarm	Alarm	No Alarm
6	Alarm	Alarm	Alarm	Alarm	Alarm	Alarm
7	Alarm	Alarm	Alarm	Alarm	Alarm	Alarm
8	Alarm	Alarm	No Alarm	Alarm	Alarm	Alarm
9	Alarm	Alarm	Alarm	Alarm	No alarm	Alarm
10	Alarm	Alarm	Alarm	Alarm	Alarm	Alarm

#### 4.1.6.2 Result and Discussion

Table 4.5 shows the tested result of image motion sensing function on a surveillance of IP camera, when a person went into radioactive source security area. The minimum sensing time setting was 1 seconds. Video image recording time could be set for every 1 second up to 99 second. Time required for image recording after motion detected depending on the time sharing in wifi network. This could be function as a second alarm trigger in the second alarm layer for detection of an unauthorized person movement at source security area.

#### 4.1.7 IP Camera Remote Control Testing

This IP camera (VSTAR CAM) was installed for independent surveillance at entrance door. The responsible person could online remote viewing via web browser or application on mobile phone. The video image could be records in computer at a recording time setting. The remote operation and video recording were tested by following procedure:

#### 4.1.7.1 Methodology

- Connect IP camera (VSTAR CAM) with remote control function to microcomputer via wifi network.
- The remote control access for online image viewing testing was conducted by web browser and mobile phone.
- The tested results showed in Figure 4.6, Figure 4.7 and Figure 4.8.














Name	Date	Type	Size	Length
 Anonymous_20150...	8/30/2015 5:37 PM	Video Clip	16,778 KB	00:01:00
 Anonymous_20150...	8/30/2015 5:38 PM	Video Clip	14,915 KB	00:01:00
 Anonymous_20150...	8/30/2015 5:39 PM	Video Clip	12,326 KB	00:01:00
 Anonymous_20150...	8/30/2015 5:41 PM	Video Clip	8,317 KB	00:01:00
 Anonymous_20150...	8/30/2015 5:44 PM	Video Clip	2,222 KB	00:00:15
 Anonymous_20150...	8/30/2015 9:42 PM	Video Clip	13,452 KB	00:01:00
 Anonymous_20150...	8/30/2015 9:43 PM	Video Clip	13,949 KB	00:00:59
 Anonymous_20150...	8/30/2015 9:46 PM	Video Clip	13,939 KB	00:01:01
 Anonymous_20150...	8/30/2015 10:49 PM	Video Clip	7,560 KB	00:00:37
 Anonymous_20150...	8/30/2015 11:15 PM	Video Clip	38 KB	00:00:00
 Anonymous_20150...	9/12/2015 8:52 PM	Video Clip	1,677 KB	00:00:07
 Anonymous_20150...	9/12/2015 8:54 PM	Video Clip	14,828 KB	00:00:59
 Anonymous_20151...	10/3/2015 4:02 PM	Video Clip	595 KB	00:00:02

Figure 4.6 Video recorded log file in microcomputer

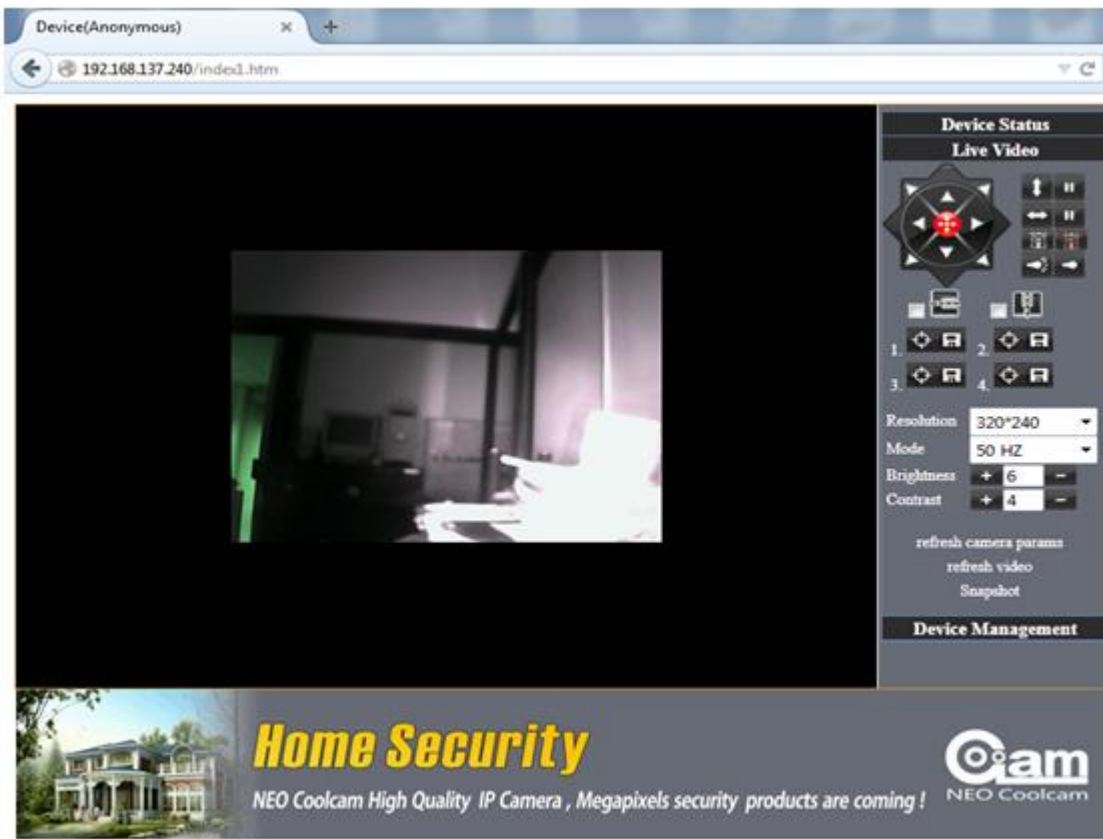


Figure 4.7 Online remote viewing by using web browsers

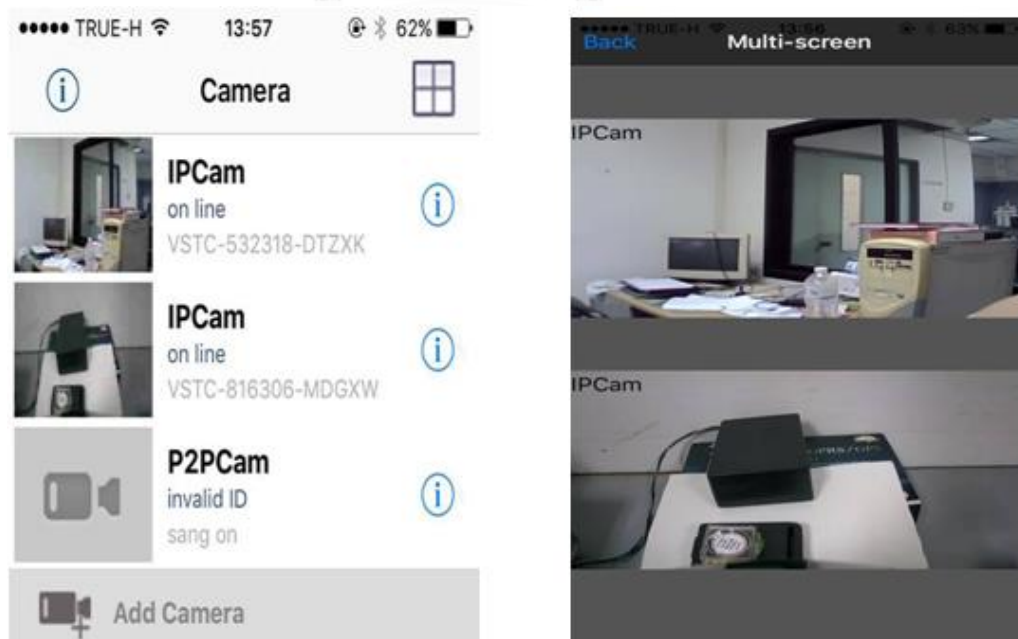


Figure 4.8 Online remote viewing by using mobile phone

#### **4.1.7.2 Result and Discussion**

The video clip could be recorded and could also be searched by the log file with information of file name, date and time, as shown in Figure 4.6. Online remote viewing could be done both by using web browser and by application on mobile phone, as shown in Figure 4.7 and 4.8, respectively. The viewing speed depends on the time sharing speed on wifi network.

### **4.2 Radiation Area Monitoring Testing**

The economical radiation area monitoring system with window type alarm threshold setting was developed for gamma detection. This system employed for supporting the third alarm layer. All system parts assembled and developed in laboratory. The reliability of system operation was tested as following:

#### **4.2.1 Instrument and Equipment**

- Microcontroller board with developed hardware and control software
- Microcomputer with interfacing system
- Developed radiation area monitoring system
- Beacon/Buzzer alarm set
- Radioactive source of Cs-137 with activity of 10  $\mu\text{Ci}$
- Low voltage power supply of Hewlett Packard model 6284A
- Function generator of GW Instek model GFG-3015
- Digital voltmeter of SANWA model PC5000

#### **4.2.2 Ratemeter Testing**

##### **4.2.2.1 Methodology**

- Connect the ratemeter to the microcontroller board with control software in associated with discriminator and voltage amplifier, as shown in Figure 4.9.
- Apply the TTL output signal from the function generator to ratemeter input.

- The linearity of two full scale of ratemeter were tested by varying the frequency in two ranges of 0 to 100 Hz and 0 to 1 kHz.
- The tested results showed in Table 4.6 and the graph plotting in Figure 4.10 and Figure 4.11.

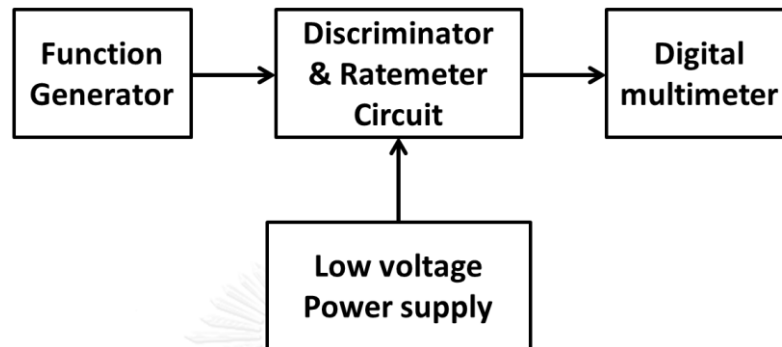


Figure 4.9 The block diagram for ratemeter circuit testing

Table 4.6 Result of linearity test of ratemeter for 100 Hz and 100 kHz

Frequency range (Hz)			
0 – 100		0 - 1000	
Input frequency (Hz)	Output voltage (V)	Input frequency (Hz)	Output voltage (V)
10	0.28	100	0.28
20	0.59	200	0.58
30	0.91	300	0.88
40	1.21	400	1.18
50	1.52	500	1.48
60	1.84	600	1.79
70	2.15	700	2.08
80	2.46	800	2.39
90	2.78	900	2.7
100	3.09	1000	3.02

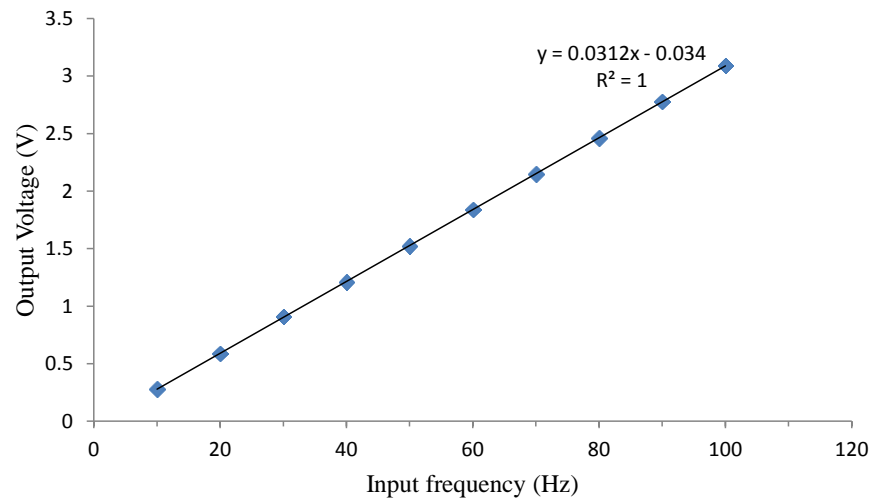


Figure 4.10 The plot of linearity for ratemeter in range of 100Hz

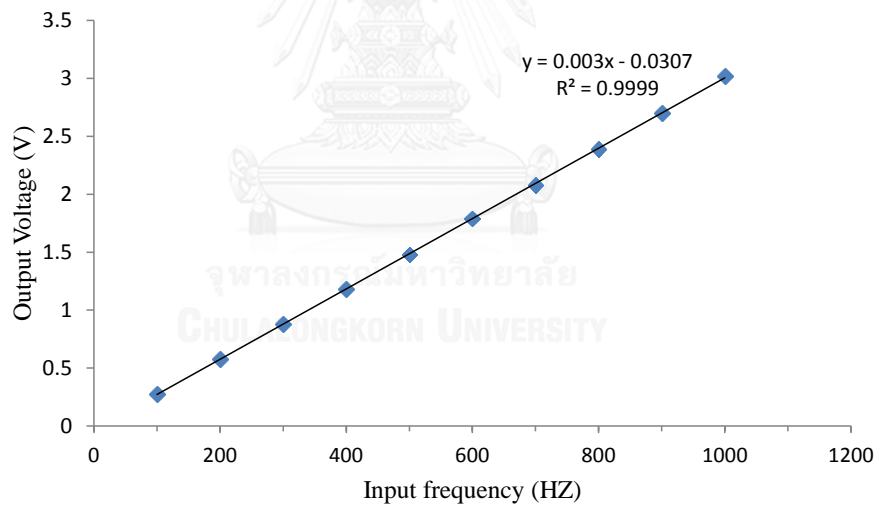


Figure 4.11 The plot of linearity for ratemeter in range of 1kHz

#### 4.2.2.2 Result and Discussion

The linearity tested results from the graph of Figure 4.10 and 4.11 showed that the frequency to voltage conversion of the ratemeter gave the output voltage in corresponding of both two frequency range of 100 Hz and 1 kHz at amplitude of 3V full scale with very good linearity.



### 4.2.3 Radiation Detection system

#### 4.2.3.1 Methodology

- Connect gamma detector with integral counting system in associated with microcontroller alarm system, as shown in Figure 4.12.
- Set distance between simulated radioactive source (10  $\mu\text{Ci}$  of Cs-137) and detector to be 3 cm.
- Input the upper and lower threshold value for high gamma and low gamma alarm setting as following:

$$\text{Upper threshold value} = + (N\sigma + \text{Background count with source})$$

$$\text{Lower threshold value} = - (N\sigma + \text{Background count with source})$$

In this experiment, upper threshold and lower threshold value were 242 counts and 424 counts, respectively. The values of the count were then converted to voltage value by using the calibration equation for the ratemeter of 1000 Hz range obtained in 4.2.2. The calculated voltage value for upper threshold and lower threshold were 0.726 V (digital value = 225) and 1.272 V (digital value = 394), respectively.

- Conducted the 2 Scenarios for simulation test of alarm window function:
  - Scenario 1, stimulate the case of adversary move the shielded radioactive source away from its original position.
  - Scenario 2, simulate the case of adversary move the shielded radioactive source, closed to the area monitor.
- Each scenario tested for 10 times.
- The tested result showed in Table 4.7.

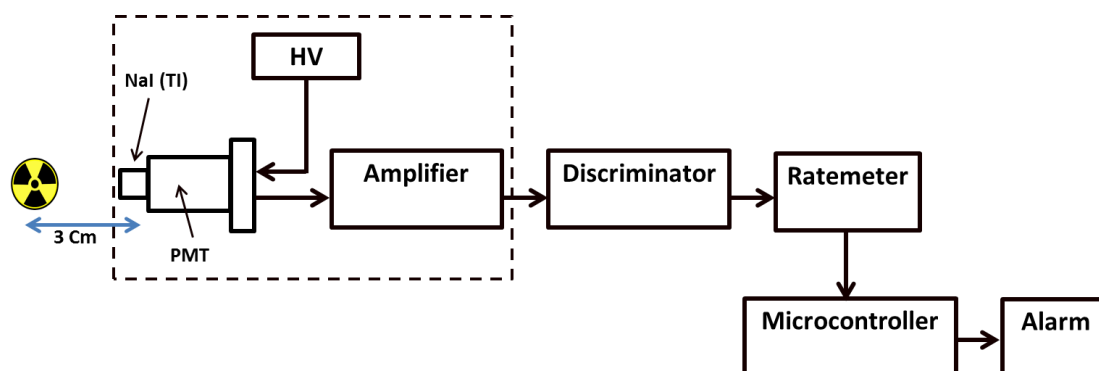


Figure 4.12 The block diagram for radiation area monitoring testing

Table 4.7 Tested result of window alarm for area monitor testing

No.	Source move pass through	Source move away
	High gamma alarm	Low gamma alarm
1	Yes	Yes
2	Yes	Yes
3	Yes	Yes
4	Yes	Yes
5	Yes	Yes
6	Yes	Yes
7	Yes	Yes
8	Yes	Yes
9	Yes	Yes
10	Yes	Yes

#### 4.2.3.2 Result and Discussion

The result of the Scenario 1 and Scenario 2 were shown in Table 4.7, left and right, respectively. In case of high gamma alarm, if the simulated source was moved from the original position closed the radiation area monitor, the gamma counting value higher than upper threshold setting, the system could trigger alarm system. In case of low gamma alarm, if the simulated source was moved away from original

position, the gamma counting value lower than lower threshold setting, the system could also trigger alarm system. The tested results showed that the third alarm layer detection of ORSS system could response in any case of the adversary trying to move the radioactive source from the control area or remove the source from shielding.

### **4.3 Online Communication Testing**

There were three alarm link via an online communication i.e., alarm link between alarm control station (ACS) and central alarm monitoring station (CMS), alarm link to mobile phone and tracking link to mobile phone. All online communications were tested as following:

#### **4.3.1 Instrument and Equipment**

- Microcontroller board with all sensors fixed and control software
- Microcomputer with interfacing system
- Developed radiation area monitoring system
- Beacon/Buzzer alarm set
- Mobile phone with application software
- GPS tracker
- Low voltage power supply model HEWLETT Packard 6284A

#### **4.3.2 Alarm link between alarm control and central alarm monitoring station Testing**

##### **4.3.2.1 Methodology**

- Set up the microcontroller based alarm control system and microcomputer based alarm monitoring system, as shown in Figure 4.13.
- All alarm sensing devices was simulated in each activated condition as the action of alarm layer 1, 2 and 3, sequentially.
- Check the alarm sending code by web browser which recorded web server at each alarm sensing device such as:

1A is the code from door switch, in alarm layer 1

1B is the code from door IR optical sensor, in alarm layer 1

2A is the code from PIR motion sensor, in alarm layer 2

2B is the code from IP camera (image motion sensor), in alarm layer 2

3A is the code from radiation area monitoring (RAM) system, in alarm layer 3

- The tested result showed in Table 4.8 and Figure 4.14.

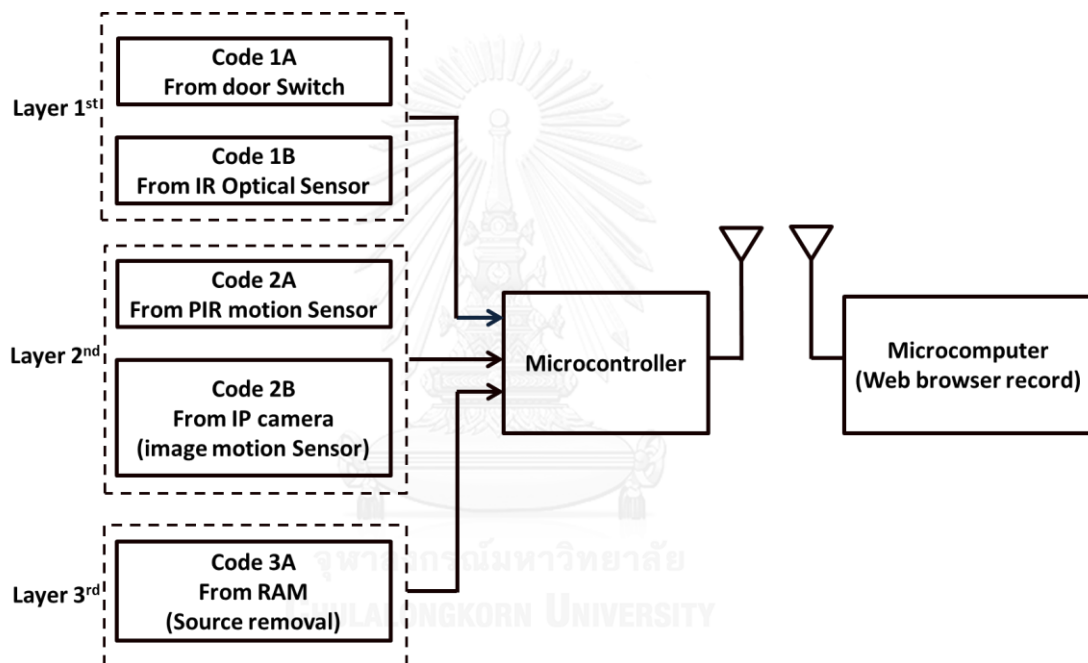


Figure 4.13 Block diagram for alarm link system testing

Nong 's Project This Stream is Log for AlarmCode

JSON CSV MySQL PostgreSQL Atom

alarmcode	timestamp
00	2015-09-17T12:40:55.089Z
00	2015-09-17T12:40:48.513Z
00	2015-09-17T12:40:37.741Z
FF	2015-09-17T12:40:32.782Z
FF	2015-09-17T12:40:33.662Z
2A	2015-09-17T12:40:27.158Z
FF	2015-09-17T12:40:11.093Z
2B	2015-09-17T12:40:03.682Z
00	2015-09-17T12:40:01.231Z

Ex: Code from Motion sensor

Date and Time

Ex: Code from CCTV (Motion sensor)

Figure 4.14 Data from event alarm code record in webserver at CMS

Table 4.8 Data result from testing sensitivity alarm code sent to web server

No.	Code 1A (Door switch)	Code 1 B (IR sensor)	Code 2A (motion sensor)	Code 2B (IP camera)	Code 1C ( RAM)
1	Recorded	Recorded	Recorded	Recorded	Recorded
2	Recorded	Recorded	Recorded	Recorded	Recorded
3	Recorded	Recorded	Recorded	Recorded	Recorded
4	Recorded	Recorded	Recorded	Recorded	Recorded
5	Recorded	Recorded	Recorded	Recorded	Recorded
6	Recorded	Recorded	Recorded	Recorded	Recorded
7	Recorded	Recorded	Recorded	Recorded	Recorded
8	Recorded	Recorded	Recorded	Recorded	Recorded
9	Recorded	Recorded	Recorded	Recorded	Recorded
10	Recorded	Recorded	Recorded	Recorded	Recorded

#### 4.3.2.2 Result and Discussion

Tested results in Figure 4.14 shows the alarm codes with date and time recorded in web server. The responsible person could search the alarm event in the summary file. The reliability tested of each sensor in 10 times found to be stable without error, as shown in Table 4.8.

### 4.3.3 Alarm Link to Mobile Phone Testing

#### 4.3.3.1 Methodology

- Set up the system as 4.3.2.1
- All alarm sensing devices was simulated in each activated condition as the action of alarm layer 1, 2 and 3, sequentially.
- Check the alarm sending code by SMS which recorded on mobile phone at each alarm sensing device such as:
- The tested result showed in Table 4.9 and Figure 4.15.



Figure 4.15 The SMS message on mobile phone

Table 4.9 The tested result of alarm link to mobile phone simulation

No.	Code 1 A (Door switch)	Code 1 B (IR sensor)	Code 2A (Motion sensor)	Code 2B (IP camera)	Code 1C (RAM)
1	sent	sent	sent	sent	sent
2	sent	sent	sent	sent	sent
3	sent	sent	sent	sent	sent
4	sent	sent	sent	sent	sent
5	sent	sent	sent	sent	sent

No.	Code 1 A (Door switch)	Code 1 B (IR sensor)	Code 2A (Motion sensor)	Code 2B (IP camera)	Code 1C (RAM)
6	sent	sent	sent	sent	sent
7	sent	sent	sent	sent	sent
8	sent	sent	sent	sent	sent
9	sent	sent	sent	sent	sent
10	sent	sent	sent	sent	sent

#### 4.3.3.2 Result and Discussion

When alarm sensor was activated the alarm code could both send to CMS via web browser and to mobile phone via SMS. Figure 4.15 shows the tested SMS message of alarm code on mobile phone. The reliability tested of each sensor in 10 times found to be stable without error, as shown in Table 4.9. The SMS could alert responsible person to manage the alarm event.

#### 4.3.4 Tracking Link to Mobile Phone Testing

##### 4.3.4.1 Methodology

- Test the response of GPS tracker in two conditions; placed alone and fixed on the radioactive source shielding.
- Use mobile phone call the GPS tracker, then GPS would send back the location message to mobile phone.
- Testing the response time of GPS tracker after called.
- Apply the Google map application to tracking the radioactive source location.

Table 4.10 The tested result of alarm link to mobile phone simulation

No.	Response time (Placed alone) (s)	Response time (Fixed on shielding) (s)
1	19.00	19.28
2	18.81	19.13
3	19.03	19.51
Average	18.94	19.31

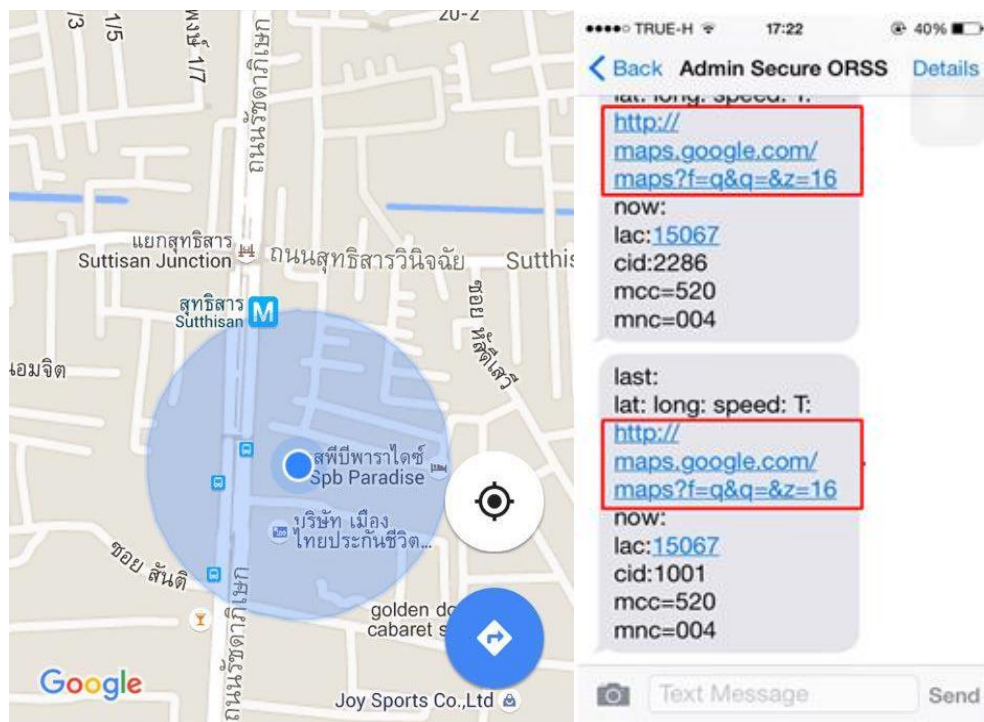


Figure 4.16 Location of source tracking on Google map

#### 4.3.4.2 Result and Discussion

From the tested result, it was found that there was no effect of signal loss of the communication signal, as shown in Table 4.10. The GPS tracker could be sent back the location every called time. The response time of GPS tracker was around 18-20 seconds. The sent back location could be loaded on Google map and tracked as shown in Figure 4.16.

#### 4.4 System Integration Operation of ORSS Testing

The developed ORSS system was test in full function of radioactive source security protection. The full system integration test was divided into three part i.e., system operation with authorized password, system operation with unauthorized password and fault alarm. The system operation with authorized password was test for verify that it should be no alarm trigger. In case of system operation with unauthorized password, it must be complete operation in four layer alarm protection. Fault alarm test in case of long term operation also be done.



#### 4.4.1 Instrument and Equipment

- Microcontroller board with all sensors fixed and control software
- Microcomputer with interfacing system
- Developed radiation area monitoring system
- Beacon/Buzzer alarm set
- Mobile phone with application software
- GPS tracker
- Radiation source (Cs-137)

#### 4.4.2 Full System Operation Testing

##### 4.4.2.1 Methodology

- Set up the system as 4.3.2.1.
- Enter the authorized password and went into the source security area for 5 times. The tested result showed in Table 4.11.
- Enter unauthorized password and test the function of all sensors for three times.
- The tested result showed in Table 4.12.

Table 4.11 The test results of system operation with authorized password

No.	Authorized password	Display		Alarm status
		Microcontroller LCD	CMS Monitor	
1	1234	****	1234	No
2	5678	****	5678	No
3	0123	****	0123	No
4	0789	****	0789	No
5	0000	****	0000	No

Table 4.12 The tested result of system operation with unauthorized password

Alarm layer	Sensors	Function	No.		
			1	2	3
Layer 1	Door switch	Alarm trigger	Yes	Yes	Yes
		SMS	Yes	Yes	Yes
		Data record	Yes	Yes	No
	IR sensor	Alarm trigger	Yes	Yes	Yes
		SMS	Yes	Yes	Yes
		Data record	Yes	Yes	No
Layer 2	Motion sensor	Alarm trigger	Yes	Yes	Yes
		SMS	Yes	Yes	Yes
		Data record	Yes	No	Yes
	IP camera (Motion sensor)	Alarm trigger	Yes	No	No
		SMS	Yes	No	No
		Data record	No	No	Yes
Layer 3	Radiation area monitor	Alarm trigger	Yes	Yes	Yes
		SMS	Yes	No	Yes
		Data record	Yes	Yes	No

#### 4.4.2.2 Result and Discussion

From the tested result, in case of system operation with authorized password tested it was found that the system work properly. But in case of system operation with unauthorized tested, some error in the image motion sensing function was found due to the sharing time of wifi network. However, most of alarm signal trigger of every sensor and SMS work properly. For data recording the reliability depends on the time sharing speed on wifi network, sometime a loss of recorded found.

### 4.4.3 Fault Alarm Testing

#### 4.4.3.1 Methodology

- Set up the system as 4.3.2.1.
- Under the power supply back up by UPS.
- Fix the location of the radioactive source under security, for keeping the radiation level in the alarm threshold window.
- Leave the system continue operation for 10 hours.
- Observe the fault alarm every 30 minutes.
- The tested result showed in Table 4.13.

Table 4.13 The tested result for fault alarm testing

Time	Alarm sensing system code				
	1A	1B	2A	2B	3A
10 min	No alarm	No alarm	No alarm	No alarm	No alarm
30 min	No alarm	No alarm	No alarm	No alarm	No alarm
1 h	No alarm	No alarm	No alarm	No alarm	No alarm
1 h 30 min	No alarm	No alarm	No alarm	No alarm	No alarm
2 h	No alarm	No alarm	No alarm	No alarm	No alarm
2 h 30 min	No alarm	No alarm	No alarm	No alarm	No alarm
3h	No alarm	No alarm	No alarm	No alarm	No alarm
3h 30mn	No alarm	No alarm	No alarm	No alarm	No alarm
4h	No alarm	No alarm	No alarm	No alarm	No alarm
4h 30mn	No alarm	No alarm	No alarm	No alarm	No alarm
5h	No alarm	No alarm	No alarm	No alarm	No alarm
5h 30mn	No alarm	No alarm	No alarm	No alarm	No alarm
6h	No alarm	No alarm	No alarm	No alarm	No alarm
6h 30mn	No alarm	No alarm	No alarm	No alarm	No alarm
7h	No alarm	No alarm	No alarm	No alarm	No alarm
7h 30mn	No alarm	No alarm	No alarm	No alarm	No alarm

Time	Alarm sensing system code				
	1A	1B	2A	2B	3A
8h	No alarm	No alarm	No alarm	No alarm	No alarm
8h 30mn	No alarm	No alarm	No alarm	No alarm	No alarm
9h	No alarm	No alarm	No alarm	No alarm	No alarm
9h 30mn	No alarm	No alarm	No alarm	No alarm	No alarm
10h	No alarm	No alarm	No alarm	No alarm	No alarm

#### 4.4.3.2 Result and Discussion

The tested result in Table 4.13 showed alarm status for long term operation. There was no alarm found in 10 hours tested period. False alarm might occur from the statistical count rate variation of the background.

## CHAPTER 5

### CONCLUSIONS

#### 5.1 Conclusion

The developed Online Radioactive Source Security (ORSS) system was designed in the active detection for against any unauthorized person access to the secure area, with multiple alarms of sensing layers for preventing the stolen source. Alarm signal communications to alert the responsible person was provided. The design feature conformed in full function protection (delay, detect, and response) according to the guidance security IAEA Level A. The developed system could be used for preventing the removal of the high level radioactive source without authorization person.

The NodeMCU microcontroller was employed for alarm control system in associated with inexpensive sensor devices such as digital keypad door access control device, door switch, IP camera system, motion sensing system, radiation area monitoring and GPS tracker. The system control software was developed for the support of security function. The microcomputer was used for online monitoring of alarm signal communication via wifi at central monitoring system (CMS). The alarm signal trigger could be sent the code alarm via message (SMS) to mobile phone of responsible person.

From the tested results, it was revealed that all sensors worked in detection function properly. Moreover, the system software could control the operation in multilayer alarms at the secure area or radiation room. Furthermore, the sequence of sensors was used with the data linking between NodeMCU microcontroller and microcomputer. The alarm signal could be sent via the internet network to security guard and responsible person for preventing the secured source removal.

The developed system was simple designed, and it was easy to use or maintenance. This development would gain up the knowledge of a source security system for future development. In conclusion, the developed system could be used for preventing a high level source removal without authorization at working place such as hospitals and laboratories.

## 5.2 Suggestion

In discussion of the tested results, the system improvement and beneficial of developed system were following suggest:

1. The redundant operation of network system should be determined in either case of limited speed or failure of internet network for preventing the loss of data recording and increasing of system stability.

2. The LAN option can be added for supporting in case of wifi failure. This could be improving by software improvement.

3. The designed system requires only the password to access the entrance. An ID card or user name combining with password is suggested to be included in door assessment for the purpose of personal recognition.

4. Approximately of 10 units of radioactive in medical used were not secured by the reason of very expensive system installation and maintenance very expensive. Therefore, the low cost system could be installed for source security and link alarm to the existing system of GRTI project.

5. For GPS tracker, it should be developed automatic sending the location to the responsible person without calling

## REFERENCES



- [1]. International Atomic Energy Agency. **Monitoring for Radioactive Material in International Mail Transported by Public Postal Operators.** Nuclear Security Series 3. Reference manual, Vienna: Publishing Section, IAEA, (2006).
- [2]. International Atomic Energy Agency. **Security of Radioactive Source.** IAEA Nuclear Security Series No.11, Vienna: Publishing Section, IAEA, (2009).
- [3]. International Atomic Energy Agency. **Dangerous quantities of radioactive material (EPR-D-Values).** Vienna, (2006).
- [4]. Yosi Kristian, Hendrawan Armanto and Michael Frans. **Utilizing of GPS and SMS for Tracking and Security Lock Application on Android Based Phone.** Signal and Information Processing Vol.3. No.4, (November 29, 2012).
- [5]. Wasan, W. **Development of a GPS interfaced gamma monitoring system via mobile network.** Master degree. Department of nuclear engineering. Chulalongkorn University, (2012).
- [6]. A.O. Oke, O.M. Olaniyi, O.T. Arulogun and O.M. Olaniyan. **Development of a microcontroller-controlled security door system.** Vol 10. No2, (2009).
- [7]. International Convention for The Suppression of Acts of Nuclear Terrorism. United Nations, (2005).
- [8]. International Atomic Energy Agency. **Convention on physical Protection of Nuclear Material (CPPNM) and Amendment thereto.** (1987).



[9]. International Atomic Energy Agency. **The interface between safety and security at nuclear power plants, INSAG-24.** International Nuclear Safety Group, Vienna, (2010).

[10]. International Atomic Energy Agency. **Code of conduct on the safety and security of Radioactive Sources,** (2000).

[11]. International Atomic Energy Agency. **Security of Radioactive Source,** IAEA Nuclear Security Series No.11, Vienna: Publishing Section, (2009).

[12] International Atomic Energy Agency. **Categorization of radioactive source, IAEA safety standard for protecting people and the environment,** Series No. RS-G-1.9, IAEA. Vienna, (2005)

[13] NodeMCU. Open-source, Interative, Programable, Low cost, Simple, Smart, wifi enabled. Retrieved 17 October 2015, available from:

[http://www.nodemcu.com/index\\_en.html#fr\\_54745c8bd775ef4b99000011](http://www.nodemcu.com/index_en.html#fr_54745c8bd775ef4b99000011)

[14]. Suvit.P. **Instrumentation Nuclear Technology.** Teaching material 2111601, faculty of engineering, Chulalongkorn University.

[15]. Simon.M. Programing arduino. McGraw-Hill Company. Library of congress cataloging-in-publication data. New york, (2012).

[16] Harvey. S. DACS Single Board Computer Workshop. Retrieved 13 November 2015, available from:

[https://dacs.org/downloads/SBCworkshop/Electronics\\_Project\\_parts.pdf](https://dacs.org/downloads/SBCworkshop/Electronics_Project_parts.pdf)

[17] Wikipedia. General-purpose input/output. Retrieved 15 November 2015, available from: [https://en.wikipedia.org/wiki/General-purpose\\_input/output](https://en.wikipedia.org/wiki/General-purpose_input/output)

[18] Harikumar, M. **Detection of Unauthorized Movement of Radioactive Sources in the Public domain for Regaining Control on Orphan Source.** International Conference on the Safety and Security of Radioactive Sources, IAEA, 27 June – 1 July, 2005.

[19] Ruixue, Li. **Indoor Wireless Localization System for radioactive Source Based on ZigBee.** International Conference on Computing, Control and industrial Engineering (CCIE), 5-6 June, 2010.

[20] Knoll, Glenn F. **Radiation Detection and Measurement.** 3<sup>rd</sup> edition. New York: McGraw-Hill Book Company, (1999).

[21] V.M Gandhi, D.Rajesh setty. **The application of stolen radioactive source tracking system based on GSM/GPS technology.** IJECT Vol.3, 4 Oct-Dec 2012.

[22] Fraden, J. **Handbook of Modern Sensors.** New York: Springer-Verlag, (2010).

## APPENDIXES







## APPENDIX C

### 3. Security Level and security objective (Categorized of Radioactive Source)

**TABLE 2. SECURITY LEVELS AND SECURITY OBJECTIVES**

Security functions	Security objectives		
	Security Level A Goal: Prevent unauthorized removal*	Security Level B Goal: Minimize likelihood of unauthorized removal*	Security Level C Goal: Reduce likelihood of unauthorized removal*
Detect	Provide immediate detection of any unauthorized access to the secured area/source location		
	Provide immediate detection of any attempted unauthorized removal of the source, including by an insider	Provide detection of any attempted unauthorized removal of the source	Provide detection of unauthorized removal of the source
	Provide immediate assessment of detection		
	Provide immediate communication to response personnel		
	Provide a means to detect loss of source through verification		
Delay	Provide delay after detection sufficient for response personnel to interrupt the unauthorized removal	Provide delay to minimize the likelihood of unauthorized removal	Provide delay to reduce the likelihood of unauthorized removal
Response	Provide immediate response to assessed alarm with sufficient resources to interrupt and prevent the unauthorized removal	Provide immediate initiation of response to interrupt the unauthorized removal	Implement appropriate action in the event of unauthorized removal of a source
Security management	Provide access controls to source location that effectively restrict access to authorized persons only		
	Ensure trustworthiness of authorized individuals		
	Identify and protect sensitive information		
	Provide a security plan		
	Ensure a capability to manage security events covered by security contingency plan (see the Definitions)		
Establish security event reporting system			

\* Achievement of these goals will also reduce the likelihood of a successful act of sabotage.

## APPENDIX D

### 4. Recommended default security levels for commonly used source (Categorized of Radioactive Source)

**TABLE 5. RECOMMENDED DEFAULT SECURITY LEVELS FOR COMMONLY USED SOURCES**

Category	Source	A/D	Security level
1	RTGs Irradiators Teletherapy sources Fixed multibeam teletherapy (gamma knife) sources	$A/D \geq 1000$	A
2	Industrial gamma radiography sources High/medium dose rate brachytherapy sources	$1000 > A/D \geq 10$	B
3	Fixed industrial gauges that incorporate high activity sources Well logging gauges	$10 > A/D \geq 1$	C
4	Low dose rate brachytherapy (except eye plaques and permanent implants) Industrial gauges that do not incorporate high activity sources Bone densitometers Static eliminators	$1 > A/D \geq 0.01$	Apply measures as described in the Basic Safety Standards [5]
5	Low dose rate brachytherapy eye plaques and permanent implant sources XRF devices Electron capture devices Mossbauer spectrometry sources Positron emission tomography (PET) check sources	$0.01 > A/D$ and $A > \text{exempt}$	

considerations when assigning security levels to radioactive sources. These factors represent variables that are specific to the source and the manner and location in which it is used — and these may affect the level of security that is appropriate for a given source or facility.

## APPENDIX E

### 5. Recommend Measure for security levels (Categorized of Radioactive Source)

**TABLE 6. RECOMMENDED MEASURES FOR SECURITY LEVEL A**  
(*goal: prevent unauthorized removal*)

Security function	Security objective	Security measures
Detect	Provide immediate detection of any unauthorized access to the secured area/source location.	Electronic intrusion detection system and/or continuous surveillance by operator personnel.
	Provide immediate detection of any attempted unauthorized removal of the source, including by an insider.	Electronic tamper detection equipment and/or continuous surveillance by operator personnel.
	Provide immediate assessment of detection.	Remote monitoring of CCTV or assessment by operator / response personnel.
	Provide immediate communication to response personnel.	Rapid, dependable, diverse means of communication such as phones, cell phones, pagers, radios.
	Provide a means to detect loss through verification.	Daily checking through physical checks, CCTV, tamper indicating devices, etc.
Delay	Provide delay after detection sufficient for response personnel to interrupt the unauthorized removal.	System of at least two layers of barriers (e.g. walls, cages) which together provide delay sufficient to enable response personnel to interdict
Response	Provide immediate response to assessed alarm with sufficient resources to interrupt and prevent the unauthorized removal.	Capability for immediate response with size, equipment, and training to interdict.
Security management	Provide access controls to source location that effectively restrict access to authorized persons only.	Identification and verification, for example, lock controlled by swipe card reader and personal identification number, or key and key control.
	Ensure trustworthiness of authorized individuals.	Background checks for all personnel authorized for unescorted access to the source location and for access to sensitive information.
	Identify and protect sensitive information.	Procedures to identify sensitive information and protect it from unauthorized disclosure
	Provide a security plan.	A security plan which conforms to regulatory requirements and provides for response to increased threat levels.
	Ensure a capability to manage security events covered by security contingency plans.	Procedures for responding to security-related scenarios.
	Establish security event reporting system.	Procedures for timely reporting of security events.



## VITA

Miss Phanousone Phouiyavong was born on 5 July 1988, in Vientiane Lao PDR. From 2004 to 2009, she went to study the Bachelor of Engineering in Electronic (Telecommunication) at National University of Laos. From 2009 to present, she has been working at Technology Computer and Electronic Institute (TCEI), Ministry of Science and Technology. From 2013 to 2015, she continued to study the Master of Science in Nuclear Technology with concentrate on Nuclear Security and Safeguards at Chulalongkorn University, Bangkok, Thailand.



