การจัดประชุมเสนอผลงานวิจัยระดับบัณฑิตศึกษา มหาวิทยาลัยสุโขทัยธรรมาธิราช ครั้งที่ 5

The 5th STOU Graduate Research Conference

การพัฒนาระบบความปลอดภัยแบบออนไลน์สำหรับต้นกำเนิดกัมมันตรังสี

Development of an Online Radioactive Sources Security System

ภานุสร พุยยะวง (Phanousone Phouyavong)[1] เดโช ทองอร่าม (Decho Thong-Aram)[2]

สุวิทย์ ปุณณชัยยะ (Suvit Punnachaiya)[3]

Abstract

An online radioactive sources security (ORS) system 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 ORS 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 surveymeter was modified to 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.

Keywords: Source security, Radiation area monitor, Online tracking system, Radiological dispersal device

1 Graduate student, Nuclear Security and Safeguard program, Chulalongkorn University, p_phanousone@hotmail.com.

2 Lecturer, Department of Nuclear Engineering, Faculty of Engineering, Chulalongkorn University, decho.t@chula.ac.th.

3 Assistant professor, Department of Nuclear Engineering, Faculty of Engineering, Chulalongkorn University, suvit.p@chula.ac.th.

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, cost and time consuming, and even limited radiation doses could cause long term health effects and cause 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. 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.

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.

From the previous research, the system and feasibility studied on detection of unauthorized movement of radioactive sources in the public domain for regaining control on orphan sources was reported [1]. In 2010, the indoor wireless localization system for radioactive source monitoring system based on ZigBee network for improving the source security system was presented [2]. The utilizing of GPS and SMS for tracking and security lock application on Android based mobile phone was introduced [3]. Those researchers have aimed to individual study of the security function. Recently, the security equipment companies were introduced various package of source security systems for preventing the high activity source from being lost or stolen. However, the turn keys package of source security system installation very costly because they include 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 needs to be developed. In this paper, the development of a low cost online radioactive source security in associated with inexpensive physical sensing devices [6] was presented.

Research objectives and scopes

1. To study the feature of inexpensive sensing devices for physical protection including GPS tracker required in a source security system development.
2. To modify the surveymeter into radiation area monitor with a window threshold alarm setting.
3. To develop an online radioactive source security system by integration of physical protection and radiation area monitor.
4. To develop system control software for supporting of an online source security function with signal communication via internet and SMS mobile phone to the security center.
5. To test the full function of the developed system in according to the IAEA security level A.

Methodology

In this research, the source security system was designed in according to the guidance of IAEA security level A. The system must be provided a full function protection (delay, detect, response) to prevent unauthorized person from removing the radioactive source from storage. The design concept of instant active detection, against any unauthorized person access to the source secured area, with the multiple alarm sensing layers and also alarm signal communication to responsible personal were arranged. A source tracking system, if physical sensing system jam occurred, was also included. From mentioned above, the system structure could be divided into 2 major parts; a) A microcontroller based alarm system control, and b) A microcomputer based central alarm monitoring in cooperation of mobile phone. The security system included the inexpensive sensors such personal identifier access, door switch, optical sensor, motion sensor, CCTV surveillance system and GPS tracker. These sensors were studied in association with the modification of surveymeter onto Radiation Area Monitor (RAM) with window threshold alarm setting function (low background and high gamma alarms) [7]. The system integration of Online Radioactive Source Security (ORS) system, sending alarms signal via the Wi-Fi internet, was developed as illustrated in the block diagram of Figure 1. For preventing the system error from power line failure, the UPS back up was also applied to the system.

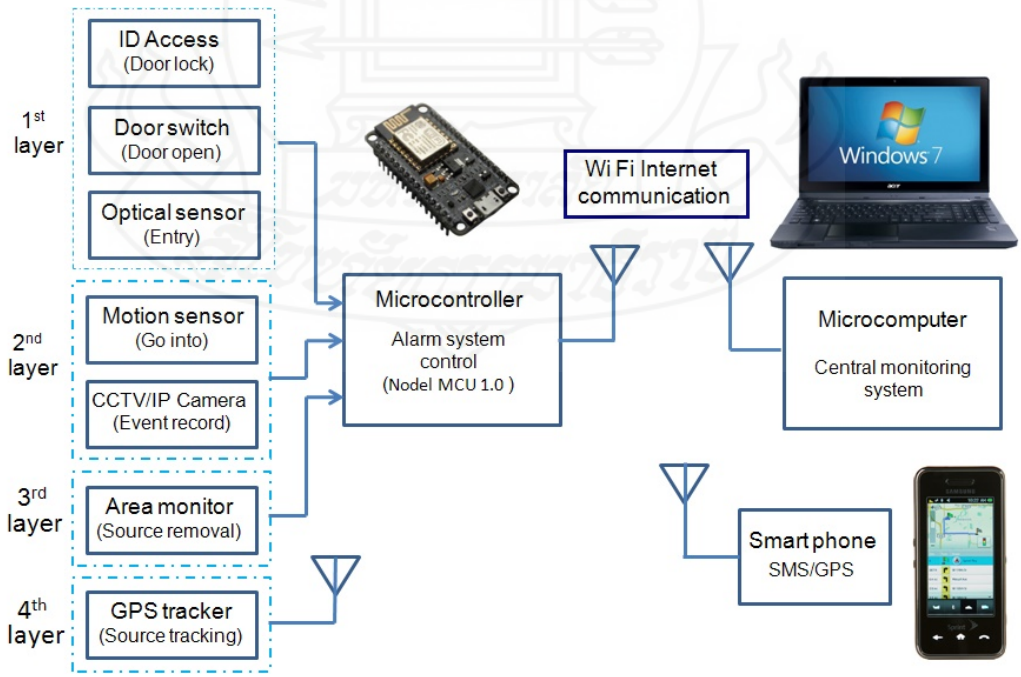


Figure 1 Block diagram of online radioactive source security system

A. System structure design

The development kit of ESP8266, NodeMCU, integrated GPIO, PWM, IIC, 1-wire and ADC all one board power with Wi-Fi module [8] was employed to develop a microcontroller based alarm system control for supporting the source security function in 4 layers of alarm sensing 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 key coded ID access device, door switch, and optical IR sensing device were installed for entering sequential operation checking. The door was locked by electromagnetic device. If unauthorized person entered the wrong code or breaking the door and go into the other sensors would generate alarm signal. This would be delayed in invading step.

Second layer: Two physical protection devices of motion sensor and 2 sets of IP camera were installed one for front door independent viewing and another one for secured source viewing with image motion sensing. The IP camera could be both video record in webserver and remote viewing online. The event recorded could be search by data for replay in investigation need. This would be active in the first step of detection when unauthorized person access to source storage.

Third layer: The modified radiation area monitor was installed for triggering when the radiation level was out of window. The gamma counted by scintillation detector was converted into voltage level and sent to ADC input and compared to setting alarm levels. If the secured source moved pass through RAM, the high gamma alarm would be generated, in the same way if the source was moved out of storage area, the low background alarm will 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 active in the second step of detection.

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

All alarm signals generated from each alarm layer would be interfaced to the microcontroller port and sent to the central monitoring system via the Wi-Fi internet, and the door would be automatically locked. 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 Central Monitoring Station (CMS) and saved into the webserver with date, time and video included. The event summary could be searched form the webserver.

B. System control software development

The Arduino software was used in system control software development. A software structure was designed in association with the signal polarity determination for properly working with the circuit operation of the online radioactive source security system. The flowchart of system control program was shown in Figure 2. In system start up, the system control program was designed for running in checking an online system status and repititive checking the sensor loop of each alarm layer. The system software would automatically recheck the connection between the security system and CMS for preventing failure operation.

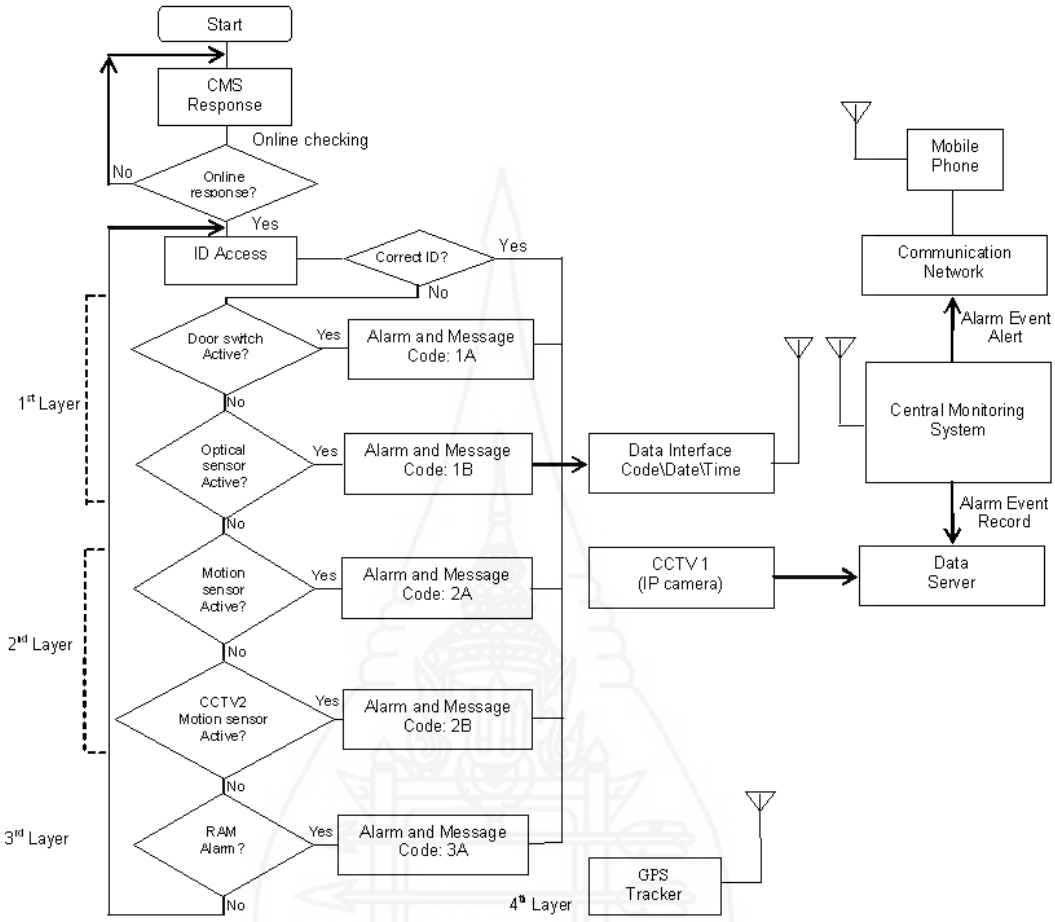


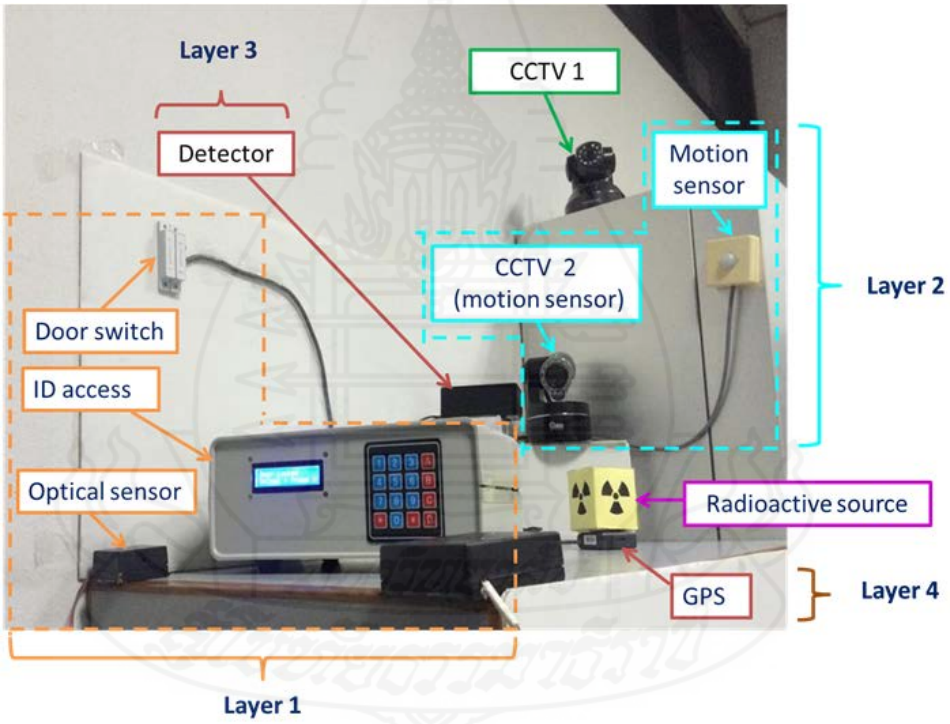
Figure 2 Flow chart of the control software

In personal ID access, the system was divided in 2 conditions, authorized personal and unauthorized personal entry. In case authorized person input the ID code without error in 3 times confirmed, the alarm system would be set on inactive status. In case 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 code information to CMS. If an unauthorized person attempted to go inside by breaking the 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 was generated, and also the video signal camera were recorded and sent online to the webserver. The third layer detection, radiation area monitor, was activated if intruder moved the source from secured location. The alarm signal regarding gamma level detection, high gamma alarm or low background alarm, 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 2 minutes to mobile phone. All alarm signals contained significant information, sensor code, date, and time for displaying on the alarm event format and being sent via communication network such as Wi-Fi 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 summary was recorded with event information in the webserver. For tracking radioactive source by GPS tracker, the position information could be received by calling the GPS tracker and running the application software on mobile phone or personal computer for tracking the location on Google map.

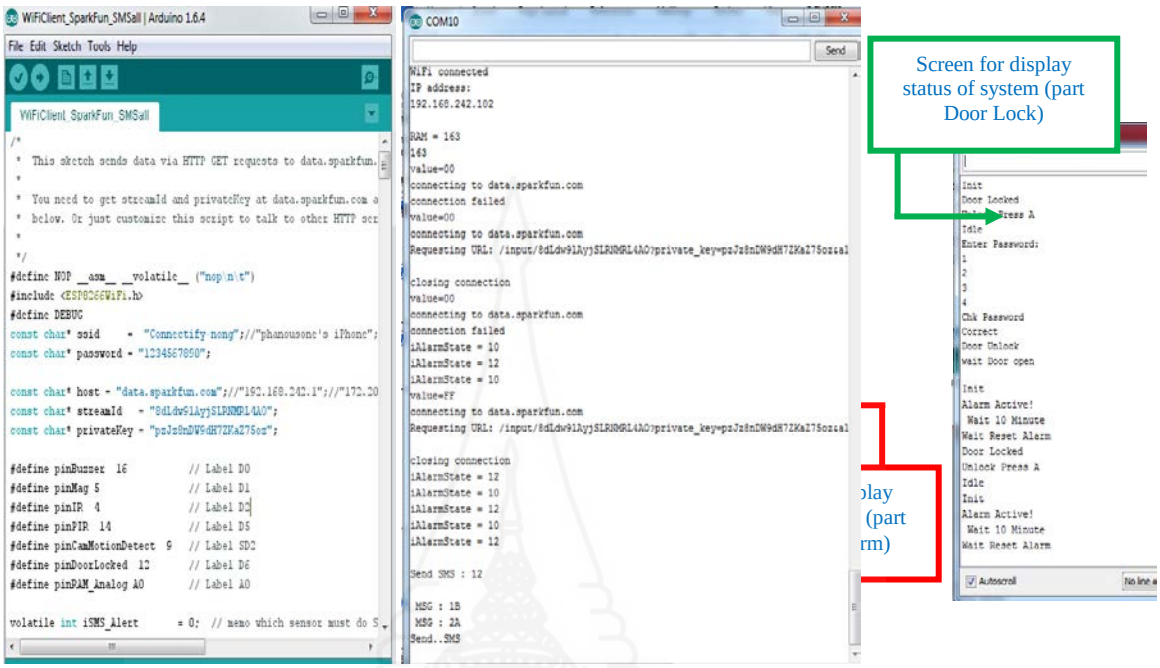
Results

The Figure 3.a showed the developed online source security system under tested in full function of security level A guideline such as delay, detect, and response in each alarm sensing layer. All sensors were connected to the microcontroller. The sensor was simulated like real situation for activating the alarm signal output to the online source security system under testing. The alarm event from each alarm sensing layer was display at CMS screen as shown in Figure 3.b.

The tested results showed that the developed system could be worked with the developed software effectively. The optical IR sensor could be set up in both sensing conditions of refection and transmission at entrance door. The motion sensing was tested by creating movement at various distances from the sensor. With the movement test, the result found that the system could detect the movement of human at maximum distance of 1.4 meters away from front side of sensor. The image motion sensing of IP camera could be applied for motion sensor alarm as well as video clip of alarm event recorder in viewing of source secured area. The tested results of the system secured source in multiple alarm layers in event summaries report and on mobile phone display were shown in Figure 4 and Figure 5, respectively. Figure 6 showed the status message display on microcontroller.



a) The developed system under tested



b) Multiwindow display on screen at CMS

Figure 3 Security system simulation test

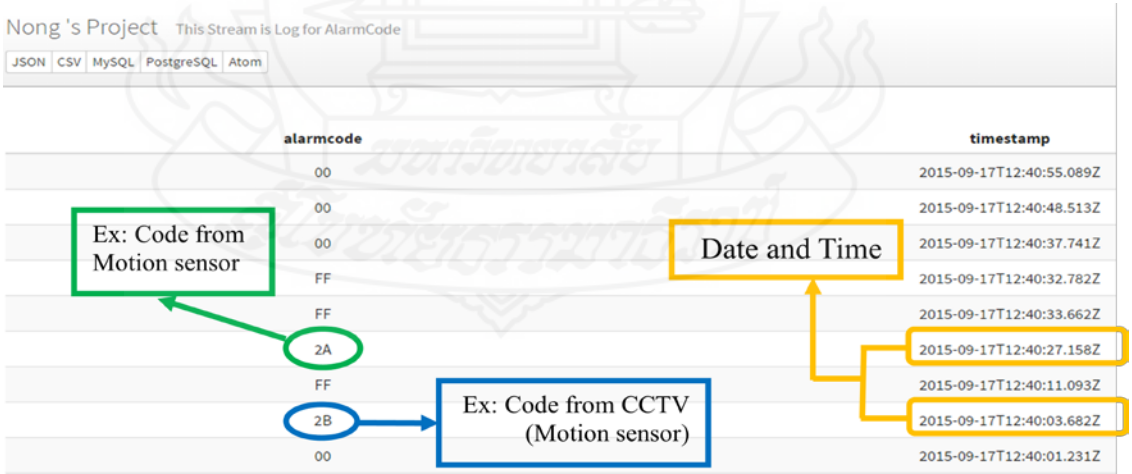


Figure 4 Event summaries from webserver

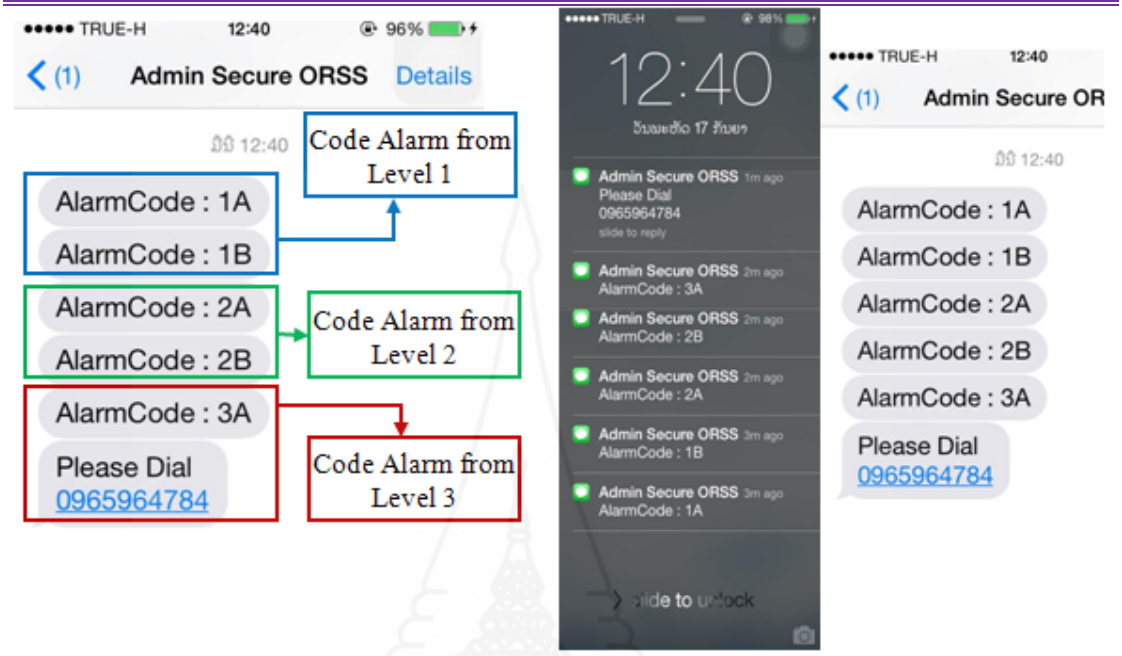


Figure 5 The SMS message on mobile phone

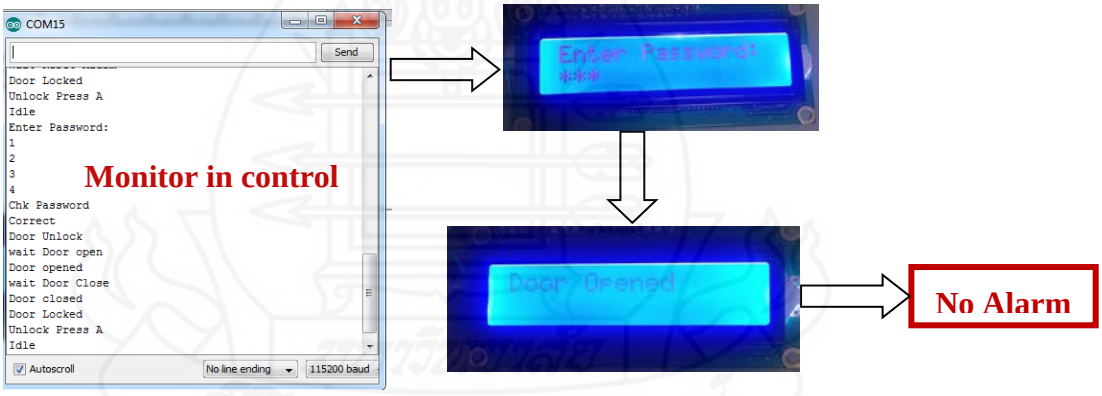


Figure 6 the status message display on microcontroller

Conclusions and discussions

In conclusion, the system development results showed that all inexpensive physical sensing devices applied for system operation are locally available. From the tested results, it was revealed that all sensors work in detection function properly and the system software could control the operation in multilayer alarm and sensing sequence with data linking between NodeMCU 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 design and ease of maintenance. This development would gain up the knowledge of a source security system for future development. 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.

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 Wi-Fi 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. Therefore, the low cost system could be installed for source security and link alarm to the existing system of GRTI project.

References

1. International Atomic Energy Agency. (2006). Monitoring for Radioactive Material in International Mail Transported by Public Postal Operators. Nuclear Security Series 3, Reference manual, Vienna: Publishing Section, IAEA.

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

3. Harikumar, M. (2005). 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.*

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

5. Yosi, K. (2012). 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*.

6. Fraden, J. (2010). Handbook of Modern Sensors. New York: Springer-Verlag.

7. Knoll, Glenn F. (1999). Radiation Detection and Measurement. Third Edition, New York: McGraw-Hill Book Company.

8. http://www.nodemcu.com/index_en.html, Retrieved, 2014