Energy International Research Journal
ISSN: 2997-5158 |
Volume 11 Issue 3, July-September, 2023
Journal Homepage: https://ethanpub.online/Journals/index.php/E9
Official Journal of Ethan Publication

FORTIFYING THE LAB: A COMPREHENSIVE GUIDE TO DESIGNING AND IMPLEMENTING SECURE IOT SYSTEMS

Dr. Sophia Garcia and Professor Liam Jones
Department of Electrical and Computer Engineering, University of New South Wales, Sydney, Australia

Abstract:
The Internet of Things is to connect all the objects to interact with each other to form an interconnected network. The Internet of Things uses information technology to promote the comprehensive upgrade of human life and production services. In a broad sense, the interworking technology covers the physical field and the information field, which can promote the development of the space of things in the direction of systematization, intelligence and networking. The Internet of Things provides a new technical guarantee for laboratory safety management. In this paper, a variety of sensors, a variety of transmission networks and protocols are applied to achieve a laboratory security system based on the Internet of Things, which provides a new idea for laboratory security management and ensures that the laboratory can serve teaching and scientific research to the maximum extent. The core work of this paper is to design the laboratory security system architecture based on the Internet of Things, and realize the laboratory security monitoring and control system.

Keywords: internet of things; laboratory security system; design and implementation; ZigBee technology; RFID technology.

1. Introduction

The Internet of Things refers to the information sensing equipment, according to the agreed protocol, any object connected to the network, the object through the information communication media information exchange and communication, in order to achieve intelligent identification, positioning, tracking and supervision and other functions. The Internet of Things extends the network concept of communication and information exchange in the actual information world to the physical world, which includes the activities of property and things or property and people. The Internet of Things is closely connected with the Internet and sensor network [1]. Sensor network is short for wireless sensor network. The sensor network is a large number of sensors randomly designed by the nodes of the data processing unit and the communication unit as well as the detection area. It uses the wireless network to implement information transmission, and the information interaction between things and things and between things and people is realized in the form of a self-organizing intelligent network information system [2]. The Internet of Things technology has been developing rapidly and gradually becoming mature, which provides a new technical guarantee for laboratory safety management. Develop a laboratory security system based on the Internet of Things to provide information and intelligent management means for laboratory security.

Energy International Research Journal
ISSN: 2997-5158 |
Volume 11 Issue 3, July-September, 2023
Journal Homepage: https://ethanpub.online/Journals/index.php/E9
Official Journal of Ethan Publication

2. ZigBee Technology

ZigBee is one of the most important wireless protocols in wireless communication and has been widely used in various Internet of Things communication fields. ZigBee is a short-range, low-complexity, low-power, low-cost bidirectional wireless communication technology, mainly used in the data transmission between various devices with close distance, low power consumption and low transmission rate. ZigBee is based on the IEEE802.15.4 standard. The IEEE802.15.4 standard only defines the physical layer protocol and the MAC layer protocol, and the ZigBee Alliance standardizes its network protocol layer and API on this basis, and also develops a security layer. After the improvement of IEEE802.15.4 by ZigBee Alliance, the ZigBee protocol stack is finally formed. The ZigBee protocol framework structure is shown in Figure 1. In the ZigBee protocol framework structure, the physical layer is the most basic part of the protocol stack, including the basic functions of physical signal reception and transmission processing, signal measurement, and transceiver state adjustment and parameter setting. The media access layer is responsible for how wireless channels are used, establishing and maintaining pans, processing and maintaining guaranteed GTS, and coordinating the proper use of communication resources across multiple devices. Network layer to achieve network establishment, routing and network address allocation, the internal is divided into network layer data entity and network layer management entity, including coordinator, router and terminal node three types of devices. The application layer includes application support sub-layer APS, application framework AF, and ZigBee device object ZDO, which together provide a unified interface for application developers [3,4].

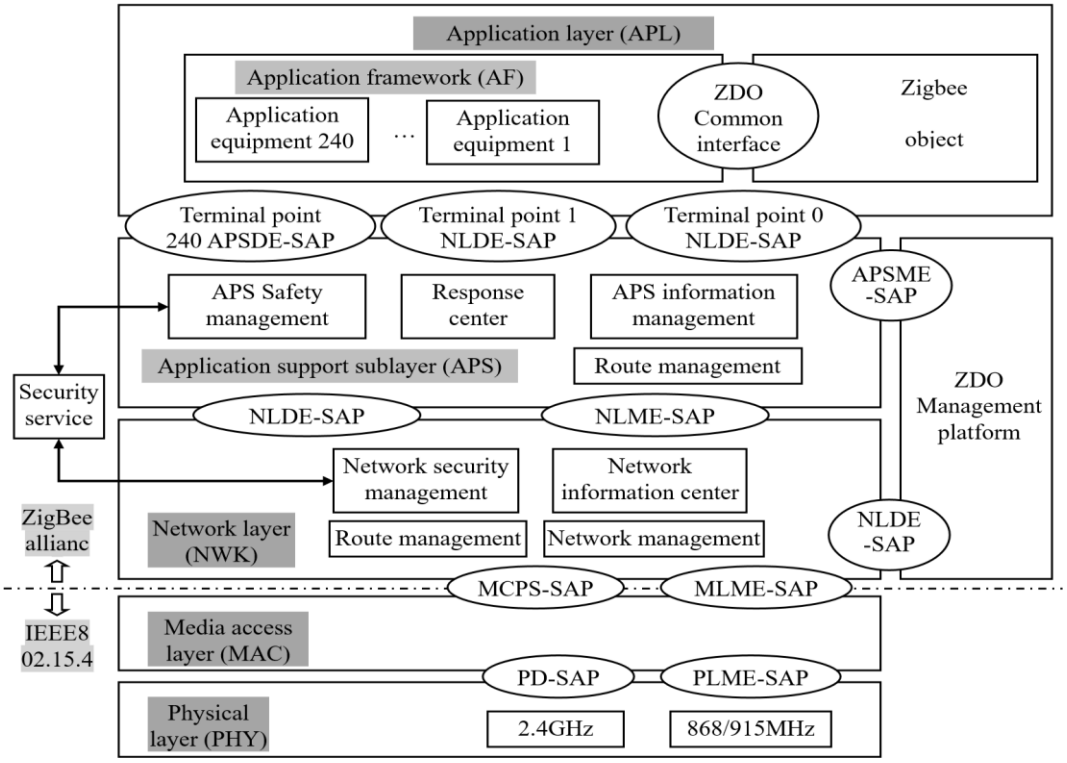

Figure 1: ZigBee protocol framework structure

There are three device roles in ZigBee networks, including coordinator, router and terminal. Among them, the ZigBee coordinator is the information collection point and core node of the entire network, responsible for the construction, maintenance and management of the network. The coordinator is usually ZigBee's gateway, responsible for the conversion to other protocols such as Wi-Fi, while having all the functions of a router. The router can send and receive data, and is responsible for searching and maintaining the path of data, so that the router or terminal device can join the network, usually as a coordinator and the terminal device relay node used. The terminal device can send and receive data, but cannot route data. The terminal device can be mounted only to the coordinator or router node. It is usually a low-power device, such as mounting various sensors, relays and switches.

ZigBee technology has the following main characteristics: First, low power consumption, ZigBee network node devices have a short working cycle, low power to send and receive information, and adopt sleep mode, low power consumption performance is significant. Second, short delay, communication delay and the delay of activation from sleep state are very short, the device search delay is 30ms, the sleep activation delay is 15ms, and the active device channel access delay is 15ms. Third, low cost, ZigBee protocol stack design is simple, the agreement is free of patent fees, coupled with the use of the frequency band does not need to pay, so the cost of ZigBee products is low. Fourth, the network capacity is large, a star structure ZigBee network can accommodate up to 255 devices, and the network composition is flexible. The mesh structure of ZigBee network can theoretically support 65535 nodes. Fifth, high reliability, ZigBee adopts collision avoidance strategy to avoid the competition and conflict of sending data. The MAC layer adopts the fully confirmed data transmission mode. Each sent packet must wait for the confirmation information of the receiver. If there is a problem in the transmission process, it can be resent. Sixth, high security, ZigBee provides data packet integrity check function based on cyclic redundancy check (CRC), supports authentication and authentication, adopts AES-128 encryption algorithm, each application can flexibly determine its security attributes.

3. RFID Technology

RFID is located in the perception layer of the Internet of Things architecture, which is the lowest level of the Internet of things and one of the mediums connecting with "everything". RFID consists of a transponder, a reader and an application software system. The transponder consists of an antenna, coupling components and chips, usually called the tag transponder, generally divided into passive, active and semi-active, each electronic tag has a unique electronic code to determine the target object. The reader consists of an antenna, a coupling element, a chip, and a device capable of reading and writing the tag information, and can be designed as a handheld RFID reader or a stationary reader. Application software system is application layer software, which mainly collects and further processes

Energy International Research Journal
ISSN: 2997-5158 |
Volume 11 Issue 3, July-September, 2023
Journal Homepage: https://ethanpub.online/Journals/index.php/E9
Official Journal of Ethan Publication

data for people to use [5]. The composition of RFID system is shown in Figure 2.

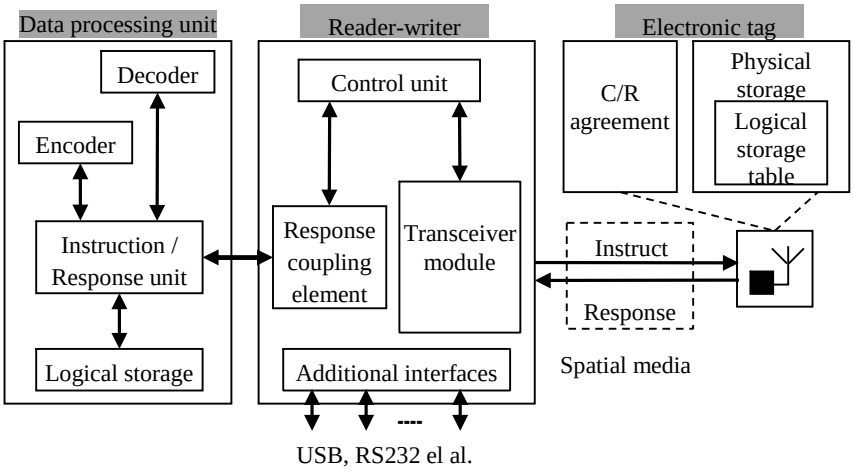

Figure 2: RFID system composition

The basic working principle of RFID system: The reader sends a radio frequency signal of a specific frequency through the transmitting antenna. When the electronic tag enters the effective working area, the induced current is generated, and the energy is activated, so that the electronic tag transmits its encoded information through the built-in antenna. The receiving antenna of the reader receives the modulated signal sent from the tag, and transmits it to the signal processing module of the reader through the modulator of the antenna. After demodulation and decoding, the effective information is transmitted to the background host system for related processing. The host system recognizes the identity of the tag according to the logical operation, makes corresponding processing and control for different Settings, and finally sends a signal to control the reader to complete different read and write operations.

The essence of the Internet of Things is perception, and the perception between objects is realized through radio frequency identification technology. Therefore, the application of radio frequency identification technology RFID is the core of the Internet of Things [6]. The advantages of RFID technology are obvious, the information in the electronic tag can be read and written repeatedly, the identification is strong, the reading speed is fast, the utilization efficiency is greatly improved, the information format in the electronic tag is unique, the labeled object has become unique, and the "thing" in the Internet of Things has become unique. Because of this, RFID technology is widely used in many areas of the Internet of Things such as item tracking, real-time monitoring, vehicle management, smart furniture, environmental monitoring and laboratory security to achieve the identification, control, interconnection and supervision of objects.

4. System Architecture

The laboratory security system based on the Internet of Things replaces the manual registration and management of laboratory personnel and equipment information in the past, realizes the information management of laboratory resources, facilitates the sharing of laboratory resources, and enables the management, analysis and statistics of equipment and personnel information. Real-time monitoring of

water and electricity in the laboratory, and analysis and statistics of the monitored data. Each room of the laboratory is monitored and video history playback is provided to prevent various safety accidents. To realize the access control function of the laboratory, only authorized laboratory personnel can enter the laboratory by swiping the card to increase the security of the laboratory. The architecture of laboratory security management system based on Internet of Things technology is shown in Figure 3 [7].

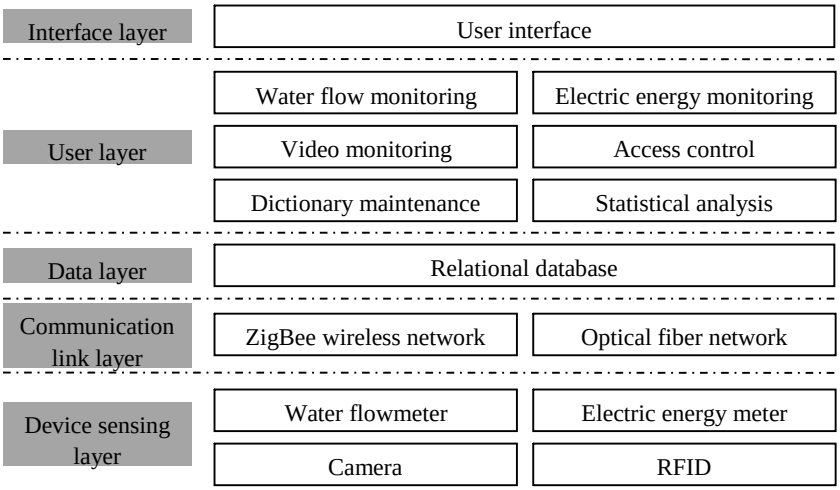

Figure 3: System architecture

The core functions of the system include four aspects [8]: First, water flow monitoring. The water flow meter is placed in the laboratory, and the distance transmission between the flow meter and the central control room is carried out through the application of optical fiber network, and the optical fiber big data is transmitted to the central server, and then the data is monitored and collected. Second, electric energy monitoring. Obtain the laboratory electricity situation, respond to and deal with sudden electricity accidents. A professional electrical energy detection box is set up in the laboratory, the current signal is sent by the transformer, and all the signals are uploaded to the power meter. Using ZigBee wireless transmission method to transmit data, through the optical fiber network and the system connection, the central server accurately read the energy meter data, so as to achieve real-time monitoring effect. Third, video surveillance. Monitor the dynamic situation of the laboratory, automatically identify the light camera in each room, connect the infrared camera with the client software, collect and transmit video data, and call up the monitoring screen or historical screen in real time. Fourth, access control management. Check the identity of people entering the laboratory, and only those who have access and meet the requirements can enter the laboratory. The access control system uses RFID radio frequency technology, which can accurately identify the target, and obtain information, and compare it with the information in the database. If the information is consistent, you can gain admission to the laboratory.

Energy International Research Journal
ISSN: 2997-5158 |
Volume 11 Issue 3, July-September, 2023
Journal Homepage: https://ethanpub.online/Journals/index.php/E9
Official Journal of Ethan Publication

Laboratory Safety Monitoring and Control System

Laboratory safety hazards mainly include five aspects [9]: First, fire hazards. The occurrence of fire accidents is universal and may occur in almost all laboratories. Second, explosive potential. Explosive accidents mostly occur in laboratories with flammable and explosive materials and pressure vessels. Third, potential toxicity. Almost all chemicals used in chemical laboratories have certain toxicity, and toxic accidents mostly occur in laboratories with chemical drugs, highly toxic substances and toxic gas emissions. Fourth, mechanical and electrical hazards. Mechanical and electrical injuries occur mostly in mechanical laboratories with high-speed rotation or impact motion, or electrical laboratories with live work and some laboratories with high temperature. The fifth is the potential theft. The hidden dangers of theft are mostly due to the poor anti-theft performance of the doors and Windows of the laboratory, or the responsibility of the relevant personnel is not in place. The laboratory defense system under the condition of Internet of Things covers all kinds of sensing and detection devices, as shown in Figure 4 [10].

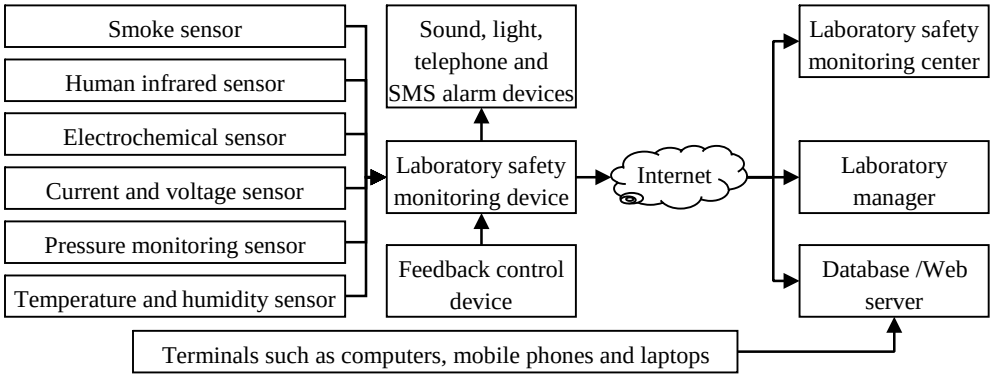

Figure 4: Architecture of laboratory safety monitoring and control system

Sensors are used to collect laboratory monitoring signals and abnormal state signals of instruments, equipment, fires and hazards to human health during experiments. Temperature sensor can feel the temperature and convert to the available output signal, temperature sensor is the core part of the temperature measurement instrument, according to the measurement method can be divided into contact and non-contact two categories. Ionic smoke sensor is a kind of advanced technology, stable and reliable sensor, which is widely used in various fire alarm systems, and its performance is far better than that of gas sensitive resistor fire alarm. The human body infrared sensor is used for life anti-theft alarm and visitor notification, etc. The principle is to convert the released charge into voltage output through the amplifier. Electrochemical sensors are mainly used to analyze the composition of gases, liquids or solids dissolved in liquids, the measurement of liquid pH, conductivity and REDOX potential and other parameters. The current and voltage sensor converts the high voltage into a certain value of low voltage for measurement and other uses, which can prevent the current or voltage from being too large to damage the instrument and equipment, and can greatly reduce the risk of electric shock for the experimenter. Pressure sensor A device or device that can sense pressure signals and convert pressure signals into usable output electrical signals according to certain rules.

Conclusions

The definition of the Internet of Things is to use RFID technology, laser scanners, global positioning devices and infrared sensors and many other sensor Settings, to connect everything with the network, communication and information exchange into the relevant protocol implementation, to achieve the intelligent goal of identification and management. A variety of sensors, a variety of transmission networks and protocols are applied to realize a laboratory security system based on the Internet of Things, which provides a new way of thinking for laboratory security management and ensures that the laboratory can maximize its service for teaching and scientific research.

Acknowledgements

This work is supported by guiding science and technology plan project of Dandong city in 2022 (Liaodong university united technology): Intelligent laboratory security management technology and system based on Internet of Things.

References

W. L. Zhuang. Design and research of Internet of things technology in laboratory security protection system [J]. Electronic Test, 2022, 36(09): 119-121+99.

J. Liu. Application of Internet of Things Technology in Laboratory Safety Monitoring[J]. Journal of Shaoxing University, 2019, 39(01): 110-114.

W. W. Han. Research on Wireless Network Application Based on ZigBee TechnologyJ]. Information Recording Materials, 2022, 23(10): 233-236.

B. L. Shi, G. Wang, H. X. Zhang, Y. J. Zhang. Strain Data Acquisition System Based on ZigBee Wireless Network [J]. Instrument Technique and Sensor, 2020, 57(01): 79-82.

X. Xu. RFID Technology in the Internet of Things[J]. Modern Industrial Economy and Informationization, 2023, 13(03): 119-121.

L. Li. Study on the Development and Application of Internet of Things Based on RFID Technique [J]. Shanxi Electronic Technology, 2016, 44(06): 38-39.

B. L. Shi, X. S. Zhang, X. L. Chen. Application of Internet of Things Technology in Laboratory Safety Management [J]. Research and Exploration in Laboratory, 2019, 38(03): 273-276.

Q. H. Lou. Application of Internet of Things technology in laboratory security management [J]. Computer Programming Skills & Maintenance, 2022, 29(01): 169-171.

G. X. Cui. Design of Laboratory Safety Management System Based on the Internet of Things [J]. Research and Exploration in Laboratory, 2015, 34(03): 287-290.

N. Qin. Research on university laboratory security system under Internet of Things environment [J]. Low Carbon World, 2015, 5(32): 153-154.