1-1-2017

Development of an Intelligent Equipment Lock Management System with RFID Technology

Yeh-Cheng Chen
University of California

C. N. Chu
China University of Technology

H. M. Sun
National Tsing Hua University

Jyh-Haw Yeh
Boise State University

Ruey-Shun Chen
National Chiao Tung University

See next page for additional authors

Development of an Intelligent Equipment Lock Management System with RFID Technology

Yeh-Cheng Chen
Department of computer science,
University of California, Davis, CA, USA.
Email: ycch@ucdavis.edu

C. N. Chu
Department of Information Management,
China University of Technology, Taiwan.
Email: nung@cute.edu.tw

H. M. Sun
Institute of Information Systems and Applications,
National Tsing Hua University, Hsinchu, Taiwan
Email:hmsun@cs.nthu.edu.tw

Jyh-haw Yeh
Department of Computer Science,
Boise State University, Idaho, USA
Email: jhyeh@boisestate.edu

Ruey-Shun Chen*,
Institute of Information Management,
National Chiao Tung University, Hsinchu, Taiwan
*Email: chen1868@gmail.com

***Abstract*-The equipment lock has been an important tool for the power company to protect the electricity metering equipment. However, the conventional equipment lock has two potential problems: vandalism and counterfeiting. To fulfill the control and track the potential illegal behavior, the human labor and paper are required to proceed with related operations, resulting in the consumption of a large amount of human resources and maintenance costs.**

This study focused on the design of RFID technology applied to the traditional equipment lock, which, through the mobile and electronic technology, strengthens the management/operating convenience of the lock and provides the solutions for anti-counterfeiting and spoilage detection so that the national energy can be properly protected and fairly distributed.

Keywords: Radio Frequency Identification (RFID); Equipment Lock Management (ELM), Near Field Communication (NFC).

.

I. INTRODUCTION

The Taiwan Power Company (TPC) purchases about 4 million of equipment locks per year to protect electricity metering equipments such as the electricity meters. In order to manage these locks, the traditional method employs human labor to prepare reports for tracking and managing these equipment locks. Each traditional lock has its color and identification number so that the reader can identify the information about the device such as usage date and grade.

However, the traditional labor-intensive operation management requires more and more cost and resources; for example, during the process of human identification and manual transcription, the recognition and transcription errors may occur, resulting in extra cost. Moreover, the equipment lock is the main protection device for the electricity metering equipment, and although regulations and punishment measures are stipulated to deter vandalism and burglary, still some cheap people use various ways to circumvent the electricity metering mechanism, resulting in energy loss and social injustice. Once the equipment lock is spoiled, then those malicious can use a variety of direct or indirect methods to affect the measured data, and the readers must also be alert in the routine electricity metering process whether the lock is spoiled so as to reduce the possibility of energy being maliciously stolen. However, the conventional equipment lock is often maliciously spoiled or even counterfeited; therefore, the use of the scientific and systematic technology will help the operator identify spoilage in the first beginning on the spot and enhance the anti-counterfeiting functionality so as to reduce the burden for the inspectors and reduce the level of national energy stolen.

In order to solve the bottlenecks of manual operations shown above, to strengthen the management and efficiency of equipment lock, and to provide the detection of spoilage and anti-counterfeiting behavior, this study employs the radio frequency technology to embed an RFID chip into the lock and develop the supporting hardware and software facilities to achieve the following three main objectives:

- A more effective front-end mobile dispatching and meter reading operating system are established to reduce the labor cost and processing error rate.
- A centralized control system is provided to integrate the existing enterprise information platforms (including the CIS and NBS systems of the TPC) so that the managers can keep track of inventory and usage status of the equipment locks at any time.
- The RFID technology is employed to provide the mechanism for spoilage and counterfeiting detection so as to solve the resources abuse problem.

II. RELATIVE STUDY

A. Electronic Seal (RFID e-Seal)

The electronic seal is an RFID chip used by the port expert to embed into the metallic ring which is traditionally used to seal the container door, and this electronic seal is also a container tracking and spoilage detection tool [1].

To protect the safety of the goods and to detect the possible smuggling, foreign countries have adopted the RFID-based electronic seals to track the flow of containers and to accelerate the stocktaking [2][3][4]. To be able to detect if the seal is spoiled, many practices and related patents, including the antennas, signal contact, pressure sensing, and so on. In order to become the Asia-Pacific Regional Operation Center, Taiwan authorities has long been actively planning the automated expedited customs clearance system in which the RFID technology is used to accelerate the clearance of goods and inspect potential vandalism [5][6]. Therefore, when the container is stuck with an RFID electronic seal, the unique number is linked to the port system, in lieu of the traditional paper inspection. In addition, the detection device on the RFID can also be used to react to the vandalism events so as to favor the fight against smuggling. [7][8]

However, RFID can certainly be used to represent the identity of the object, but the counterfeit problem may cast negative effect on the RFID. If there is not a good anti-counterfeiting mechanism, the advantage of RFID representing the object identity is very likely used by malicious people to become the tools of crime. Therefore, the anti-counterfeiting technology and the associated verification mechanism must be taken into design consideration at the same time. Using PKI technology to protect the data against counterfeiting attack [9][10][11], has been gradually applied in the RFID-related areas. This study will also employ the digital signature protection mechanisms so that the information stored in the RFID has the non-repudiation property; that is, only the verified organization can generate the recognized RFID lock so as to eliminate counterfeiting.

B. NFC function (Near Field Communication, NFC)

The NFC is evolved from the integration of radio frequency identification and non-contact network communication technology, and its application is extended through the short-range wireless communication device to the mobile phones, wristwatches, digital cameras, portable game consoles, computers and other portable digital consumer electronic products, so that, after the authentication of ID information, both products can proceed with the exchange of data and services[12] on a specific billing basis. Future mobile phones or other portable devices can download and pay the bill in any public area providing the services. For example, PayPal, the world's largest electronic payment platform, released the NFC app software for the Android cell phone, in which users just keys in the monetary amount, with two phones back to back, enter the passwords, and then the transfer operation is done quite easy and convenient.

- The NFC characteristics [13][14] are shown below:
- It operates in the 13.56MHz frequency, and the sensing range is about 20 cm in distance.
- Three options for the data transfer rate: 106 Kbits/s, 212 Kbits/s, and 424 Kbits/s.
- Active and passive modes. The active mode requires a battery with ability to launch signals independently; the passive mode does not require a battery but without the ability to launch signals independently.
- Compatibility with contactless smart card technology such as Philips Mifare and Sony FeliCa.

III. CASE STUDY AND RESEARCH METHODS

A. Case Study

There will be a proprietary lock on the user's electricity meter provided by the case company to ensure the security of electricity metering equipment. The traditional equipment lock management processes, such as dispatching notice either orally or on paper, manual checking/accepting record of the equipment lock from the warehouse, outer appearance checking, and paper transcript for the reporting-back of dispatching order are mainly manual operation oriented, which will be effort consuming and time consuming; moreover, the paper operation is often error-prone, while the bottlenecks that the information cannot be processed immediately and effective analyzed will also be confronted.

Therefore, to effectively address the prevailing requests of the case company, this study links the radio frequency identification system installed on the object to the back-end information system through the interface and wireless network to proceed with the equipment patrol and information reporting-back in a systematic way, while also avoiding device vandalism or counterfeiting. The comparison between the traditional mode and RFID system architecture for the control process of equipment lock are shown in Figure 1.

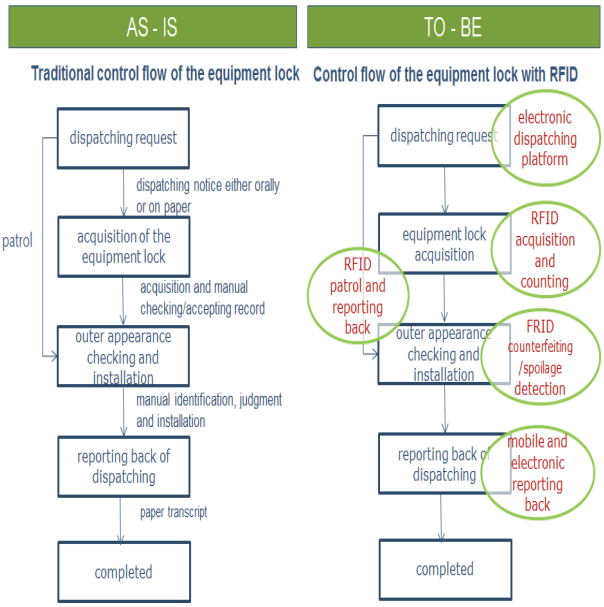

Figure 1. Traditional Mode and RFID System Architecture for the Control Process of the Equipment Lock

B. Research Methods

To improve the control process of the conventional equipment lock, there are four key points:

- Related design and research for the RFID chip embedding and the sharing of antenna and lock line: After the equipment lock is embedded with a RFID chip, it becomes an object with an independent number. This number becomes an important part of the ensuing subprojects and is used to track, record and collect data. The sharing design of antenna and lock line will be able to avoid the interference by the metal to the radio frequency device. In addition, it can be used to detect whether the lock vandalism occurs or not.
- After the lock is embedded with an RFID chip and

given a unique serial number, the "BSMI (Bureau of Standards, Metrology and Inspection) certification subsystem" will be set and embed an authentication code which is based on the cryptography principle and cannot be counterfeited to each legal equipment lock. This authentication code must have the PKI and RFID related function and construct a prototype for counterfeit detection.

- The equipment lock management system is established and integrated with the CIS and the NBS system of the Taiwan Power Company; the equipment lock control center is also established so as to help managers use the back-end management system to take full control of the flow and history records of each lock. The backend management system will have several information modules, including property management systems and database management systems.
- The mobile meter reading software is established to improve the processes and orders of relevant electronic workflow and integrate with the RFID equipment lock so as to accelerate the speed and accuracy of the meter reading operation.

This study will come out with an RFID equipment lock prototype owning the spoilage detection and anti-counterfeiting mechanism and integrate with the back-end management platform and front-end meter reading software of TPC's existing systems.

IV. SYSTEM ARCHITECTURE

For the equipment lock control flow of the TPC, the system architecture is divided into two modules. As shown in Figure 2, the first module supports the service requests from the front-end system, including the customization of RFID tags and special antenna, as well as the module design of mobile dispatching software so as to facilitate the RFID info reading and release of dispatching message; the second module supports the application requests from the back-end management platform, including integration among various types of network interfaces and implementation of back-end lock management system and data analysis modules so as to provide managers real-time information services.

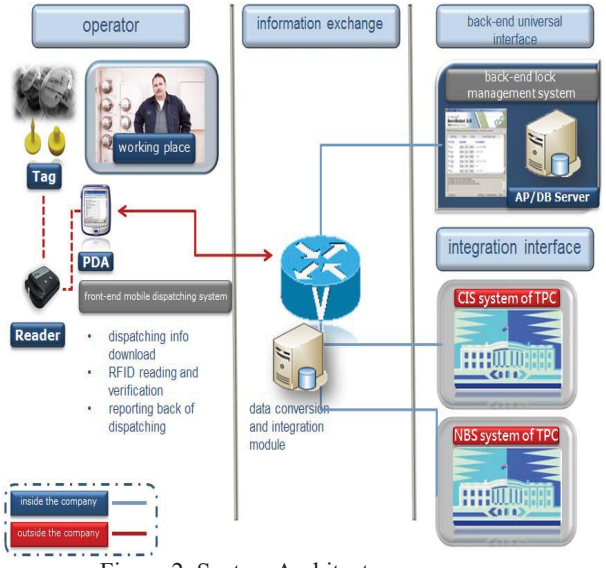

Figure 2. System Architecture

A. *Hardware R & D of the Equipment Lock*

In the case that the RFID container lock and RFID-embedded PCB architecture are used to design the RFID-based lock, and the PKI architecture is also used to establish the electronic digital signature and embed the RFID chip, it is shown in Figure 3; the major development steps are as follows:

- The equipment lock is embedded with an RFID chip in order to facilitate other subsystem to proceed with related function development.
- The function of the equipment lock is enhanced so it has the spoilage detecting ability.
- This lock is integrated with the software system so as to proceed with the Application Load Testing.

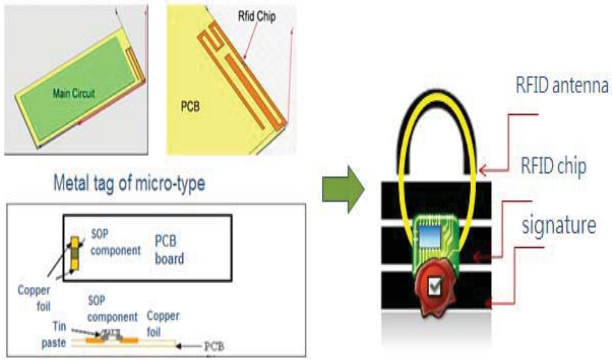

Figure 3. Hardware Development of the Equipment Lock

B. *Software Platform Design of the Equipment Lock*

In order to build a high performance and scalable lock management system, the lock software platform architecture in this study is as follows:

(1) The three-tier architecture is used to develop the back-end management platform for the equipment lock:

- The three-tier architecture is used in the Web system, which is made up of a database management system (ELM DB), a Web server system (ELM Management WEB system) and a client browser (browser), as shown in Figure 4.
- In the three-tier architecture, any component in any tier can be replaced at any time, thus reducing the coupling between various system components. For example, the ELM DB in this plan is MySQL, and it can be upgraded to Oracle or other large database systems in the future. The Web browser can be Google Chrome or IE, depending on the user's preference.

(2) A dual mechanism is employed to establish the front-end mobile dispatching system:

A dual-system mechanism is used on the handheld mobile device. In the case with a wireless network, the data is synchronized and the operation result is uploaded; in another case without a network, the offline dispatching operation is done with the help of the small internal database. In the design of handheld system, the use of dual structure can reduce the operating threshold for operators, thus bringing the following convenience:

- The traditional dock is not required to synchronize information. In the case of a wireless network, the dispatching information can be downloaded, or the result of dispatching operations can be uploaded.
- It is feasible to execute the dispatching operation in the case without a network. All dispatching

information can be synchronized through the wireless network in a particular area before operation personnel go out for work. When the dispatching contents are being executed on the client side, the small-sized database within the hand-held system can be used to proceed with the offline recording and data review. Omitting the GPRS or 3G requirements will increase the stability of the handheld system and also cut down on the cost.

- It has the on-line data synchronization module. The handheld system will detect the network connectivity and automatically synchronize the execution results.

(3) The Web Service mechanism is used to synchronize existing systems:

- The Web Service is used to collect the data that the CIS or NBS provide to the ELM DB. All information maintained by the RFID system is collected to the ELM the DB if necessary to write back and provides relevant web services for Taiwan Power Company to retrieve relevant system information on a regular basis.
- In the design of system integration, a separate table space is provided and given the limited DBA privileges. This will not only provide the independence of system integration, but also protect the security of both existing CIS and NBS systems.The purpose of the RMA system is to calculate the failure rate (FR) of equipment and spare parts. Data is then used as reference for future product design and production design of research establishments, quality assurance departments, and production departments. Generally, the standard failure, rate i.e. AFR (Annual Failure Rate) is determined at the time a contract is executed with the customer. AFR is computer as follows:

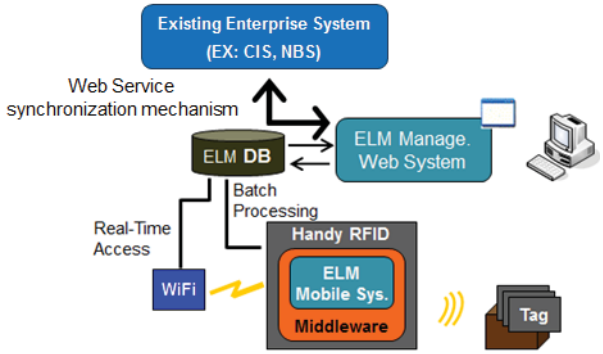

Figure 4. Management System Platform of the Equipment Lock

V. IMPLEMENTATION AND BENEFIT ASSESSMENT OF THE PROTOTYPE SYSTEM

A. System Development Environment

The default bandwidth for the RFID mechanism adopted in the system platform is 13.56MHz, and the specifications for main devices are as follows:

- The antenna of the handheld reading devices is "Linear with excellent polarization diversity", the communication interface is "Wi-Fi 802.11 b/g supporting the fixed and dynamic IP", and its operating system is "Microsoft Windows CE 6.0".
- The RFID data interface complies with the EPCglobal C1 G2 standard.
- The database for the back-end management platform is MySQL 5.5, the application server is JBoss 7, and the operating system is Sun Solaris 10.
- The program development tool is Eclipse 3.7. The report and back-end management interface development tool is BIRT.

B. Implementation of the Application System

As for the design of information flow and network connectivity, various kinds of mature network technology are employed to achieve the purpose of data transmission, and the architecture is shown in Figure 5. People in charge proceed with operations such as the custody of equipment lock and dispatching, and can at any time connect to the network to ensure that the commands are executed correctly via the authentication method. In addition, the platform also provides the top management with a consolidated information center where they can grasp the dispatching status at each time point and query the real-time inventory status of equipment lock.

In addition, the front-end operator may at any time synchronize the dispatching information in the factory or wireless network environment and report back the work contents. Not only can the front-end dispatching personnel save the paper work required for reporting back the work, but also the time required for transmitting information is shortened, while avoiding information transmission error due to erroneous manual operation.

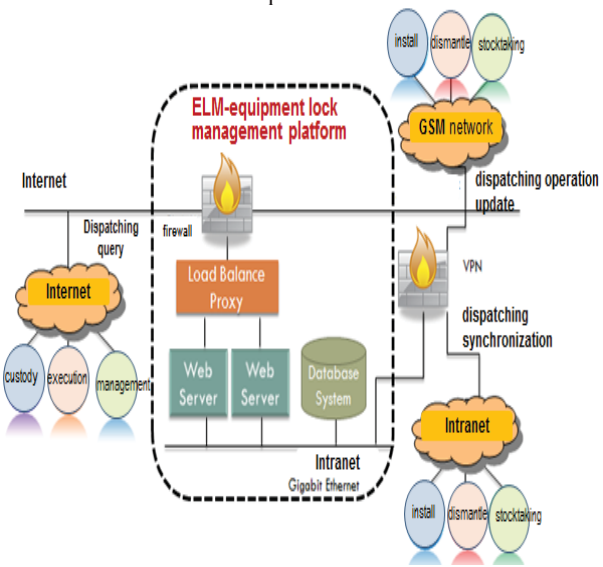

Figure 5. System Information and Network Architecture

The modularized component design for the Information system is shown in Figure 6.

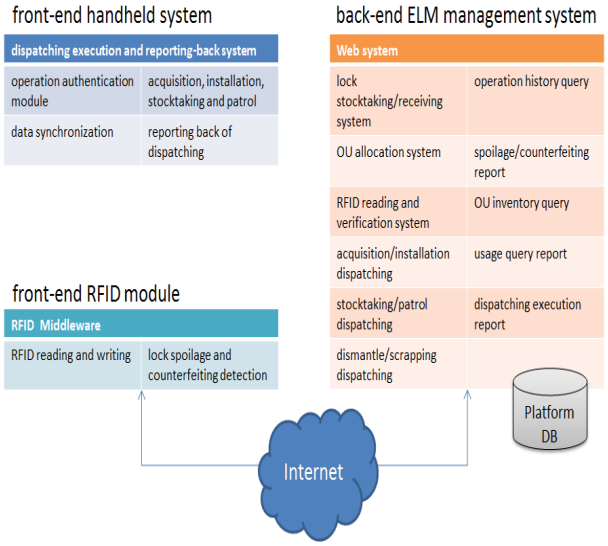

Figure 6. Component Architecture for the Information System

On the Web system, in addition to the standard login and privilege control system, those lock-related subsystems are shown in Figure 7, and the module numbers and function description are as follows:

ELM030100 lock OU inventory maintenance
ELM040100 lock receiving maintenance operation
ELM060100 lock acquisition operation
ELM070100 lock OU allocation operation
ELM080100 ock RFID reading and anti-counterfeiting verification function
ELM090100 lock RFID numbering and signature function

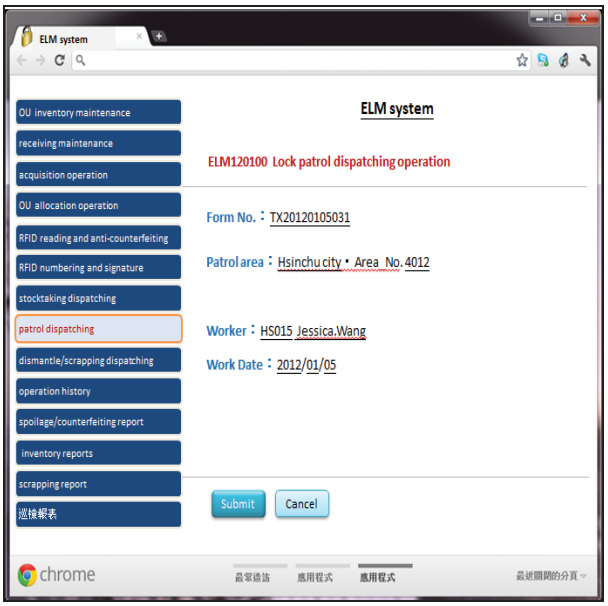

Figure 7. Back-end Management Platform of the Lock System - Lock Patrol Dispatching Operation

The front-end mobile modules of the lock system are shown in Figure 8, and the module numbers and function description are as follows:

ELM810100 operator login and logout
ELM820100 lock RFID numbering system
ELM830100 lock RFID spoilage detection module
ELM840100 lock RFID counterfeit detection module
ELM850100 lock acquisition registration
ELM860100 lock installation dispatching list and electronic workflow

Figure 8. Front-end Mobile Device Interface of the Lock System - RFID Spoilage Detection Module

C. Benefit Analysis

Focusing on the operation characteristics of patrol and stocktaking in the power company's working scene and the back-end information processing mode for the management, the customized lock RFID tags, RFID technology, mobile interface software, and an integrated application service platform are fulfilled to enhance information access efficiency for the operation people in the dispatching scene, while the instant RFID message feedback can enhance the information utilization of the back-end management; to quantify the benefit of this system, the information data in the third quarter of 2011 is used as sample range in which the RFID lock set up in the operating area A of the case company serves as the experimental group, amounting to 6,613 data records, and the traditional workflow in the operating area B of the case company serves as the control group for comparison purpose. It will be found that the RFID equipment lock cum integrated management platform will have a significant improvement in efficiency for its management processes, as shown in Figure 9. Among them, the stocktaking time for the equipment lock is reduced from 65 minutes for 100 locks to 17 minutes, thus the operation efficiency being increased by 74%; the access time for dispatching information is reduced from 93 minutes for the traditional mode to 22 minutes, thus the dispatching efficiency being increased by 76%; the anti-counterfeiting/spoilage detection of the equipment lock is significantly reduced from about one minute for the manual inspection to five seconds or less for the RFID device, thus the operation efficiency being increased by 92%; the reporting back timeliness of on-scene operation information is improved from daily "once per four hours" batch processing to the instant response for the data record within 60 seconds, thus significantly improving the timeliness of information update.

In addition, the comparison between the integration architecture of the RFID lock management platform and the traditional operation mode is shown in Table 1. Its management functions, such as dispatching management, stocktaking, anti-counterfeiting assurance, spoilage detection, on-site patrol, reporting back, and information analysis, can provide better operating efficiency and

information utilization for the case company.

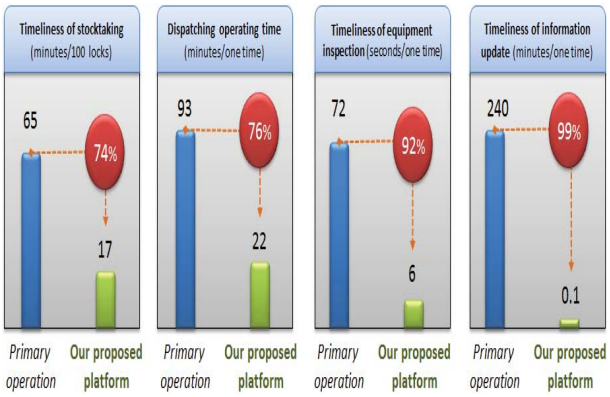

Figure 9. Efficiency Comparison between Two Modes

Table 1. Comparison of Business Processes Between Two Different Strategies

Items	Primary operation	Our proposed RFID platform
Dispatching management	Allocation by administrator	Automatic guide by electronic system
Inventory check	Handled by human and barcode	More efficiency; Retrieve with RFID
Anti-counterfeiting assurance	Control by human experience	Real-time system message response
Soil-age checking	Check by human operation	Detected by RFID mechanism
On-scene patrol	Passive mode	Mobile support with interactive mode
Reporting back	Off line	On line
Information analysis	Batch mode	Real-time display by the system

VI. CONCLUSION

Focusing on the operation requirements of on-scene usage and back-end management for the traditional equipment lock, the RFID technology and Web service software are fulfilled to provide a practical solution which will effectively improve the manual operating modes for dispatching and patrol. The customized FRID tag design constructs the lock sensing mechanism, and the front-end mobile interface provides the interactive information service so as to fulfill the on-scene dispatching convenience and real-time reporting back of information; the back-end integrated application platform provides the instant information contents and analysis service to support field activities; moreover, the characteristics of RFID are also employed to enhance the operational efficiency and reduce labor costs. The specific contributions are as follows:

- Being different from common lock vendors who use the RFID only for equipment identification, this study combines the RFID technology and Web Service mechanism to fulfill the overall requests for the front-end dispatching people and back-end managers, thus providing practical solutions in the equipment patrol and reporting back of data.
- The intelligent RFID tag design and the establishment of interactive management service platform will take real-time control of the usage status of the equipment lock, and the integration with the back-end systems will effectively improve the operating bottleneck for real-time information access.
- The integration of RFID data interface and mobile sensing devices will enhance the control of electricity meters and other metering devices for the power company and provide accurate and real-time information services. It will serve as the "last-mile" management tool for the electrical equipment and will be conducive to the subsequent research and development of the intelligent electric grids.

REFERENCES

[1] Yeh K.-C., Chen R.-S., & Chen C.-C., Intelligent service-integrated platform based on the RFID technology and software agent system, Expert Systems with Applications, 38(4), 3058-3068, 2011..

[2] Chin, L.-P., & Wu, C.-L. The Role of Electronic Container Seal (E-Seal) with RFID Technology in the Container Security Initiatives. 2004 International Conference on MEMS, NANO and Smart Systems (ICMENS'04), (pp. 116-120).2004.

[3] .Kwok, S., Ng, P., & Choy, K. Development of an RFID-based Intelligent e-Seal System for Container and Physical Asset Management. Annual Journal of IIE(HK), 28(1), pp. 70-81.2008.

[4] Zhang, J., & Zhang, C. (2007). Smart Container Security: the E-seal with RFID Technology. Modern Applied Science, 1(3), pp. 16-18. "Customer Relationship Management Forum", http://www.crm-forum.com

[5] Friedlos, D. (2009). GS1 Taiwan Pushes for EPCglobal E-seal Standard. RFID Journal.

[6] Chen, R. S., Tu A., Development of an agent-based system for manufacturing control and coordination with ontology and RFID technology. Expert System with Applications, 36(4), 7581-7593.2009..

[7] Le-Pong Chin, Ruey-Shun Chen, I-Hsin Chou and K.C. Yeh,,"Intelligent Radioactive Waste Management Platform for the Processes of Radioactive Waste Store Facility(RFID)", Nuclear Technology, Volume 182 / Number 3 / Pages 358-368, June. 2013..

[8] Yung-Shun Tsai, Ruey-Shun Chen*,Yeh-Cheng Chen, Chun-Ping Yeh,"An RFID-based manufacture process control and supply chain management in the semiconductor industry. Int. J. Information Technology and Management, Vol. 12, No1/2, 2013

[9] Batina, L., Guajardo, J., Kerins, T., Mentens, N., Tuyls, P., & Verbauwhede, I ,Public-Key Cryptography for RFID Tags. Proceedings of the Fifth IEEE International Conference on Pervasive Computing and Communications Workshops, (pp. 217-222).2007

[10] Juels, A.. Strengthening EPC Tags Against Cloning. Proceedings of the 4th ACM workshop on Wireless security, (pp. 67-76). Germany.2005.

[11] Ting, S., Ip, W., Lamand, W., & Ngai, E., A PKI-based Track and Trace Network for cross-boundary Container Security. IJCSI International Journal of Computer Science, 8(5), p. 1. ,2011

[12] Finkenzeller, K. RFID Handbook – Fundamentals and Applications in Contactless Smart Cards and Identification. John Wiley.2004..

[13] Lei, P., Claret-Tournier, F., Chatwin, C., & Young, R. Secure Mobile Track and Trace System for Anticounterfeiting. Proceedings of the IEEE International Conference on e-Technology, e-Commerce and e-Service, pp. 686-689.2005.

[14] Garfinkel, S., & Rosenberg, B., RFID Applications, Security, and Privacy. Canada: Addision-Wesley.2005