NFC based Inspection and Qualification Management (NIQM) System Preventing Counterfeit and Fraudulent Item

Chang Choong-koo*, Kim Young-joo
KEPCO International Nuclear Graduate School,1456-1, Shinam-ri, Seosang-myeon, Ulsan 689-882
**Corresponding author: ckchang@kings.ac.kr*

1. Introduction

Design, manufacturing, fabrication, transportation and installation of the devices and equipment for nuclear power plants shall be conducted under the thorough quality assurance program for the nuclear safety. However, from late in the 1980s, NRC began to issue a number of communications alerting licenses to issues involving counterfeit and fraudulent items. A number of incidents identified by the NRC in the 1980s and 1990s catalyzed the US nuclear industry to adopt standard precautions to guard against counterfeit items.[1,2]

The purpose of this paper is to develop the NFC (Near Field Communication) based Inspection and Qualification Management(NIQM) system preventing counterfeit and fraudulent items. NFC is one of the latest wireless communication technologies. As a short-range wireless connectivity technology, NFC offers safe-yet simple and intuitive-communication between electronic devices.

2. Recent Counterfeit and Fraudulent item Issues

Even though significant resources are at work addressing the issue of counterfeits from legal and enforcement perspectives, the number of counterfeiters is rapidly increasing. The rapid spread of manufacturing technology enables quick and easy creation of counterfeit products that are difficult to distinguish from the genuine product.[1,2]

2.1 Impacting U.S. NPP Between 2007 and 2009

The commercial nuclear power industryôs quality assurance and equipment reliability programs have been successful in preventing counterfeit and fraudulent items from being installed in safety-related applications. However, there are several known incidents of counterfeit and fraudulent items that have been discovered in non-safety related inventory and even installed in non-safety related applications. The impacts on U.S nuclear power plants between 2007 and 2009 are as follows[1];

- Counterfeit Ladish valves installed in non-safety related systems and stocked in several plants
- Incorrectly identified Flowserve valves
- Counterfeit electrolytic capacitors identified during receipt inspection
- Counterfeit integrated circuit installed in a portal monitor identified when the monitor failed calibration attempts
- Suspected counterfeit Square D breakers in stock at several plants
- Counterfeit Globe fire sprinklers with fraudulent Underwriters Laboratory, Incorporated (UL) label.

2.2 Examples of counterfeit and fraudulent items supplied to Nuclear Power Plants in Korea

All parts supplied for use in the reactors require quality and safety certificates from testing companies. Nevertheless, it turned out that 587 parts in 34 categories used for nuclear reactors including Hanwool(Uljin) 3, 4 and Hanbit(Younggwang) 3, 4, 5, 6 were supplied based on forged qualification documents. Further inspection after the parade of shutdowns found 694 more parts in 12 categories with fake warranties used in Hanbit 5 and 6 to put off their reactivation.[6]

The details of crime will be turned out after the prosecutorôs investigating is finished. In the meantime, the corruption cases can be classified into as followings according to the report of mass media ;

- Contract with an unlicensed contractor
- Pass the counterfeit item during acceptance test
- Supply fraudulent item to meet supply schedule
- Instigate fraudulent item because qualification process costs too much and requires too much time

3. NFC Technology for Real Time Two Way Communication

RFID(Radio Frequency Identification) technology includes many standards that operate at low frequency (LF), high frequency (HF), and ultrahigh frequencies (UHF). However, many standards are incompatible with each other within each of these frequency domains.

QR codes and RFID technologies have been widely explored to enable the connection between the virtual world of the internet and physical world we live in. QR codes can be printed at virtually no cost on existing packaging or the pages of a book, but might be considered too conspicuous and unattractive to marketers. In addition, QR code readers are sensitive to reader (usually a smartphone) orientation, and ambient lighting conditions and dirt, sometimes resulting in a

difficult capture experience.[3] In the other hand, RFID systems are often more expensive than barcode systems.

NFC is a subset of these standards operating in the HF band at 13.56 MHz under the ISO 14443, ISO 18092, and FeliCa standards, supporting a maximum data rate of 424 kbits per second (kbps) up to 10 cm. The NFC protocol not only supports communication between an active reader and a passive tag, but also allows for peer-to-peer communication between two active readers. Thus, an NFC-capable phone can both read a tag and receive and transmit data to another NFC-capable phone. Furthermore, tags can contain read/ write memory, and today there are tag products with 4 kbytes of Flash. [3,5]

An NFC-smart phone can thus write arbitrary data into a tag as long as it fits in the available memory. When reading such a tag, a mobile device will obtain both a tagôs unique identifier and if requested, the corresponding data contents. To support secure writing access, an unformatted tag is initially writable by everyone, but it allows a client to set a security key on internal blocks of data.

Table 1 Comparison between NFC and other Short Range Communication Technologies[5]

Description	NFC	Bluetooth	Zigbee	IrDa
Connection	P2P	P2P	Star, P2P	P2P
Chip Price	Low	Normal	Low	Low
RFID Compatibility	Possible	Impossible	Impossible	Impossible
Range	Up to 10cm	Up to 10m	10~20m	Up to 10m
Transmission Speed	106~848 kbps	~24Mbps	~250kbps	~4Mbps
Set-up time	<0.1s	~6s	-	~0.5s

4. NIQM System Preventing Counterfeit and Fraudulent Item

4.1 Construction of the NFC based Inspection and Qualification Management (NIQM) system

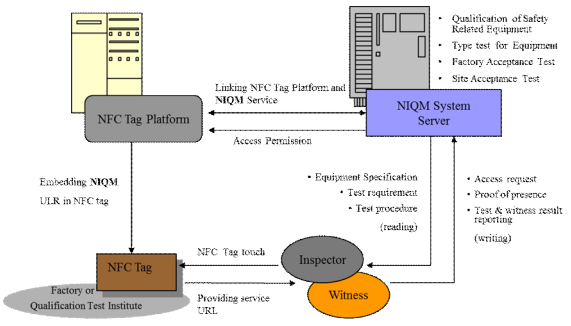

Fig.1 NFC based Equipment Inspection and Qualification Management System[4]

As shown in the Fig.1, to install NIQM server and NFC Tag platform. Then, build a mobile web for the operation of the NIQM system. Attach a NFC tag to each equipment or device to be tested or qualified and embed an URL. Each tag has unique identification (URL). For the exchange of information between NIQM system and legacy system, for example, procurement management system of plant information system, interface system is to be developed.

4.2 Operation of the NIQM System

The NIQM system can be used in line with qualification test, factory acceptance test(FAT), and site acceptance test. Inspector and witness touch the NFC tag attached at the equipment by NFC enabled mobile device such as smartphones. Then, equipment identification information is sent to the smartphone with the URL where the equipment specification and test procedure are stored. Inspector and witness can browse the technical specification, test procedure and acceptance criteria through the NFC enabled smart phone for the confirmation of the equipment to be tested. NIQM server controls access to the equipment data and qualification information for the secure operation of the system. Inspector and witness start the inspection and test with the signing on the test report. Inspector and witness can accomplish the proof of presence through the real time data communication with NIQM server. After finishing test, inspector writes the test results on the test report format preloaded in the NIQM server. Then, witness also signs on the test report. The test results are shared by manufacturer, test institute, third party witness and end user in real time base. Therefore, counterfeiting of the test report or certificate is impossible.

5. Conclusions

As described above, NFC technology can be applied to the inspection and qualification management system very effectively to prevent counterfeit and fraudulent items. In addition, NIQM system can use existing data and information through the interface with legacy system.

REFERENCES

[1] Plant Support Engineering : Counterfeit, Fraudulent, and Substandards Items : Mitigating the Increasing Risk, EPRI, Palo Alto, CA : 2009, 1019163

[2] Plant Support Engineering: Counterfeit and Fraudulent Items: A Self-Assessment Checklist. EPRI, Palo Alto, CA: 2010. 1021493.

[3] Roy Want, Near Field Communication, IEEE CS press, 1536-1268, July~September 2011

[4] Kyoung Jun Lee, Arum Park, Min Su Kang, Jungho Jun, NFC-based Smartwork Service Model Design, Journal of Intelligence Information System, 2013 June :19(2), pp.157~175

[5] Application of NFC technology for the public sector of the future government, IT& Future Strategy (8), National Information Society Agency, 2011.9.30, p.3

[6] Nuclear Energy Scandal to ' World Energy Congress Daegu 2013 ' Korea IT Times, Monday, August 12th, 2013