Research on Mobile Online Microcomputer Anti-misoperation Locking System Based on NFC Technology

Mengqiang An, Xianglian Xu, Wei Lin, Lukai Mao, Chenhu Luo and Wei Zhou

School of Automation, Wuhan University of Technology, Wuhan, Hubei, China
Email: 1437181095@qq.com

Abstract. At present, the rapid development of the power grid industry, the scale of power grids is expanding, and the degree of automation is increasing in China. The requirements for switching operations, equipment inspections, and fault handling of electrical equipment are also becoming higher. Based on the Qt on Android smartphone platform and applying NFC (Near Field Communication) technology, a new generation of online microcomputer five anti-locking system is proposed in this paper. This design can solve the problem that the on-site operator can not communicate and exchange data in real time with the background when the traditional online microcomputer five-proof system is used for the switching operation. The mobile online microcomputer anti-misoperation locking system improves the informationization and intelligence of the traditional microcomputer five-proof system, and perfects the functions of its on-site use.

1. Introduction
The computer key is widely used in the anti-misoperation locking system. According to the operating rules, the operator first needs to preview the whole process of the switching operation on the anti-missing host and generate an operation ticket. If the rectification error occurs during the rehearsal, the operation ticket will not be generated. Pass and prompt the error content and suggest the steps to turn over. After the rehearsal is completed, the operation ticket is imported into the computer key through the adapter, and the operator can carry the computer key to the site to implement the actual switching operation. Every step of the switch operation must first complete the unlocking task via the computer key, and open the lock corresponding to the power equipment to continue the operation of the power equipment. If the lock to be opened by the computer key does not correspond to the equipment to be operated, the lock is forcibly blocked, and at the same time the computer key issues an alarm, thus avoiding the occurrence of the accident.

With the change of the operation and management mode of the power network, the error prevention system is widely applied to the power system and is in a state of constant updating. At present, the wireless base station is installed at the whole station at home and abroad, and the five-proof system based on the wireless network is established to improve the management of the power equipment by the five-proof system [1]. The communication and control functions of the computer and the logic judgment function of the microcontroller are used to realize the error prevention [2]. The online control system of the locking system adopts the development mode of the network control center, centralized control and unified management, and realizes the centralized five-proof system [3]. In the actual application process of the current microcomputer five-proof technology, all data must be uniformly controlled within the five-proof main station. The functions of operation preview, ticket library management and query, logic rule base setting, etc. should also be implemented in the main station [4].
The dependence of the station is strong, which is not conducive to the remote application of the five-defense technology, and is not conducive to the expansion of the five-proof system function on the mobile side.

Smartphones are now used in grid business and management, and have become a new form of power grid development and application [5]. The mobile phone client has also gradually developed into a new model of today's social development. This design applies a NFC-enabled smart phone instead of a traditional computer key, and develops a mobile client based on the Qt on Android platform, realizes the online mobile five-proof system function, and designs a passive The NFC lock implements the blocking function, which better solves the above problems.

2. Design of Online Microcomputer Anti-misoperation Locking System Based on NFC Technology

2.1. Logical Structure of Mobile Online Anti-misoperation Locking System Based on NFC Technology

Based on the original online anti-misoperation locking system, this design applies NFC technology, which makes the system application more flexible, and the switching operation is convenient and reliable, which makes the application of the anti-misoperation locking system more diversified. Figure 1 is a block diagram of online anti-misoperation locking system based on NFC technology.

![Figure 1. Structure diagram of online anti-misoperation locking system based on NFC technology](image)

In Fig. 1, based on the traditional online anti-misoperation locking system, the internal circuit of the lock is embedded in the NFC circuit to realize the NFC communication function between the lock and the mobile phone, so the NFC mobile phone can replace the traditional computer key. The operator uses an NFC mobile phone to obtain an operation ticket through the operation authority. Each time the unlocking task is completed, the NFC mobile phone must be close to the lock, communicate with the NFC circuit of the lock, and identify its code. If it is confirmed as the target lock, the mobile
client reports the recognition result to the five-defense system. After the five defense system determines that the logic is correct, an unlocking command is issued to the anti-misoperation controller to unlock the lock.

2.2. NFC Smart Lock Circuit Design

NFC is a short-range wireless communication technology that uses inductive coupling to transfer energy through a common magnetic field between two NFC devices [6]. The master device continuously provides an RF-field RF field, and when it is close to the slave device, an induced voltage is generated on the slave device coil to power the slave device [7]. Through load modulation technology, the slave device determines the data transmission rate and achieves matching with the master device.

The internal circuit block diagram of the NFC smart lock is shown in Figure 2. There are many types of smart locks, including mechanical padlocks, electrical locks, electromagnetic locks, etc., and the internal NFC communication part is designed for this kind of circuit.

The interior of the smart lock is mainly composed of an antenna coil, a MAX66242 passive IC and an SD5075 temperature sensor. The antenna coil constitutes a carrier for transmitting energy and information between the smart phone and the lock. Only the optimal RF circuit design is realized to maximize the transmission of RF energy, and the passive IC is more effective in extracting energy. The transmission efficiency of RF energy depends largely on the resonant mode and resonance accuracy of the NFC circuit.

\[ f = \frac{1}{2\pi\sqrt{LC}} \]  

(1)

\[ L = \frac{1}{4\pi^2 f^2 C} \]  

(2)

Where \( f \) is the resonant frequency, \( L \) is the coil inductance, and \( C \) is the resonant capacitor. The resonant capacitor and coil in the MAX66242 resonant circuit operate at 13.56MHz and the resonant capacitor is 21pF. According to Equation 2, the coil inductance is 6.56uH. Considering the effect of the lock metal on the resonant frequency, the coil inductance is increased to 6.78uH here, and the energy transmission efficiency is optimal.

The MAX66242 is a passive chip that communicates directly with external smartphones without the need for an external power supply or with a microprocessor. The MAX66242 integrates a SHA-256 encryption engine for two-way, secure authentication with mobile phones. The security of the communication is guaranteed. The internal ROM ID is a unique 64-bit serial number, which has been embedded in the production process to ensure the uniqueness of the lock recognition. In the
MAX66242, unused energy from the rectifier can be output to the peripheral circuitry through the \( V_{OUT} \) pin, powering the external SD5075 temperature sensor, and communicating with the sensor via the I2C interface for temperature information.

3. Based on Qt on Android Smartphone Client Design

Qt on Android platform is a software client platform for deploying Qt applications on Android mobile phones based on C/C++ programming language \[8\]. This design applies Qt Creator to develop the application interface of five defense systems and eight functional programs in the background, and realizes mobile phones through C/S architecture. Network data communication between the client and the five anti-servers. Figure 3 shows the software architecture of the five-proof system mobile client.

As shown in Fig. 3, the mobile client software architecture is divided into a data layer, a logic layer, and an application layer.

The database is the core of the data layer. It collects, extracts, sorts, transforms, and updates data at all times. Other information based on network link devices is obtained through the data layer. The entire system can be unified in data and information interaction.

The logic layer mainly implements the functions of functional requirements analysis and logic operations. According to the client's request, the function type is discriminated to retrieve the function to achieve the corresponding customer requirements.

The application layer integrates the eight major five-proof application functions, which is more comprehensive than the other two-layer functions, and is more powerful in implementation, and includes all the application capabilities required by the system.

Like other clients, users must have certain operational rights to visit and operate. Only those who have certain rights can successfully register the user and use some of the functions of the client within the scope of authority.

The client's ticket management and exercise ability is the strongest among the major functions and the most important among the five defense systems. The client strictly manages the preview, generation, query, call, and return of the operation ticket, and uses this as the basis for the actual
switching operation. Each operation ticket is strictly generated in accordance with the management of the five defense logic, making the switching operation safer and more reliable.

In order to complete the online real-time system function of the mobile terminal, the client also interacts with the database in real time, in order to obtain the current state of the primary device and the smart lock of the five-proof local area, and the client data can be updated, the purpose of which is to: 1. It is convenient for the operator to instantly call the background wiring diagram, view the current equipment status, and plan the current operation. 2. Determine the uniqueness of the current equipment operation, avoid multiple operating tickets simultaneously operating the same lock and power equipment, and the status of the lock and equipment. Causing uncertainty, causing “cutting conflicts”. 3. Based on the five defense logic, the legality of the current operation is judged in real time.

4. Unlock Process Design

![Unlock Process Diagram]

**Figure 4.** System unlock process

The process of unlocking and locking the microcomputer five-proof system is shown in Figure 4. Like other mobile client programs, the operator needs to enter his/her account and password in the user login interface to enter the operating system. After the login is successful, the mobile phone client communicates with the five anti-servers, synchronously monitors the current state data of the background power device and the smart lock, and updates the data in real time. After the client database update is completed, the power device connected to the power system primary wiring diagram in the client graphical interface will be transformed to the current actual state, and the client interface will intuitively reflect the operating state of the power system.

There are two ways to invoke the switch operation ticket. One is to call the operation ticket that has been generated and approved in the ticket library. The second is to use the analog preview function of the mobile phone client to generate the operation ticket on the spot. Regardless of whether the
operation ticket is generated on the unit error prevention host or completed on the mobile client, the operator has unique operation authority for the device to be operated, and regardless of the preview or on-site implementation, each step must be judged by the background logic rule base. The operation that meets the five anti-logic rules can be passed before the next operation can be performed. Operation that does not comply with the five defense logic can no longer continue the rehearsal, and with the prompt of the alarm, the operation ticket will not be generated eventually.

The operator calls the generated operation ticket on the spot with the NFC mobile phone, and performs the switching operation in strict accordance with the steps of unlocking, operating the device, confirming the device status, and blocking. The NFC unlocking mode is that the NFC front end of the application mobile phone identifies the ID of the internal NFC circuit of the lock, and the client judges whether the current smart lock is the lock to be operated by the ID, and the identification can pass the awake to prevent the host from issuing the command to control the unit controller to unlock the lock. During the operation of the equipment, there is often a situation where the equipment is not operated or the operation is not in place. The online five-proof system monitors the status of the equipment in real time. If this happens, the execution of the operation ticket will stay until the current. After the operation of the device is completed, the lock should be locked again to achieve the purpose of blocking the next task. The background system will also monitor the current state of the lock to prevent the lock from being in place.

5. Conclusion
Science and technology have driven the rapid progress of human society, and the power grid has gradually developed in the direction of “intelligent” and “unmanned”. These changes will inevitably put higher and higher requirements on the microcomputer anti-misoperation locking system. This project applies the smart phone client to the anti-missing lock function of the power grid, develops the mobile phone client on the Qt on Android platform, builds and perfects the eight functions of the mobile terminal five-proof system, and applies the NFC technology to unlock the mobile phone front end. The skill of the client and the mobile phone are skillfully combined to solve the problem that the data communication between the personnel and the background is difficult.

6. References
[1] Wu D Z. Design and Application for Five Anti-wireless System on Beijing Taiyanggong Power Plant [D]. North China Electric Power University, 2016.
[2] Wu E Z. Research on online anti-misoperation locking system [D]. North China Electric Power University, 2006.
[3] Wang Y J, Wang L, Tu S L. A design of computer key of anti-maloperation system based on networks [J]. Power System Protection and Control, 2009, 37(23): 96-99.
[4] Yang T, Niu H D. The advantages and disadvantages of the five anti program lock of the microcomputer based substation and the improvement measures [J]. China Science and Technology Expo, 2010, 35(3): 352-352.
[5] Flues H, et al. Artificial intelligence in power system operation [J]. Proceeding of the IEEE, 1987, 75(12): 1678-1685.
[6] Li W X, Wang J, Zhang H, et al. Research on wireless power transmission system based on magnetic resonance coupling [J]. Systems Engineering and Electronics, 2014, 36(4): 637-642.
[7] Lahtela A, Hassinen M, Jylha V. RFID and NFC in healthcare: Safely of hospitals medication care [C]. International Conference on Pervasive Computing Technologies for Healthcare, 2008. Pervasivehealth. IEEE, 2008: 241-244.
[8] Wang M S, Guo Y X, Wu W. Near-field and far-field shared structure for NFC and CNSS applications [J]. Iet Microwaves Antennas & Propagation, 2017, 11(15): 2116-2123.