An Innovative Structure of Information Security Equipment for Remote Control

Jian Zhao [1, a], Yang Chen [2,b]

1Zhengzhou Institute of Information Science and technology, china

2 Sias International College of Zhengzhou University, china

a zhaojian_zz@126.com, b cy_yzhy@126.com

Keywords: Remote Control; System Structure; Trust Management; Automatic Destroy

Abstract: Oriented at the actual application demands of the remote control with the information security equipment, this paper proposed an information security equipment structure supporting remote control, the workflow and the functional structure of the equipment module are introduced. The structure is compatible with the early equipment effectively, and has characteristics of credible to ensure the safe operation of the equipment. The structure adopts module design, each functional module can be configured flexibly according to application requirements. At the same time, the equipment support destroying the sensitive information automatically in an emergency case, which can effectively improve the level of safety management of equipment.

I Introduction

With the continuous development of the information technology, information security issues have become more and more serious. In order to protect the security of all kinds of information system, a variety of security protective equipment is widely used. However, the security and controllability of these equipment themselves play an important role. Now, some of the equipment can't be effective remote controlled because of the original structure design. To solve the problem fundamentally, it's necessary to research and design a new equipment structure, which should has the following characteristics:

1. Compatibility: Ensure the new designed equipment can be effectively compatible with the early equipment, so that the updating of the equipment can be taking smoothly and the influence of the equipment replacement is reduced.

2. Credibility: The new structure must have the credible feature, so that the reliability of the equipment in the operation process and the security of the equipment operation can be ensured, and reduce the risk of attacks.

3. Flexibility: The new structure requires a modular structure frame, which can be configured effectively according to the different application requirements.

4. Security: The new structure not only need to ensure the security of the equipment for its sensitive information, to ensure that the sensitive information can be automatically destroyed in critical situations, and also to ensure the security of the control module, so that it does not become the bottleneck of the system security.

Remote control are widely used in various industries. [1] proposed a PSM power remote control communication system, the dissertation [2] designed a wireless remote control system, and the thesis [3-7] gives a series of remote control system based on network, the research on these systems with remote control function has a very good reference value to our new information security equipment structure design.

II Equipment structure for remote control

The structural diagram of the equipment for remote control is shown in Figure 1.

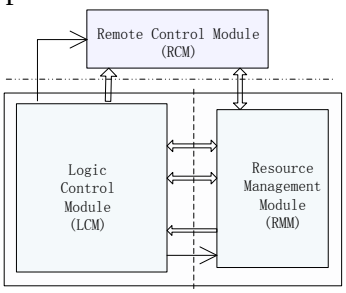

Figure.1 Equipment Structure for Remote Control

The new designed equipment structure mainly consists of three parts (the dotted line separated): Remote Control Module (RCM) to, Resource Management Module (RMM) and Logic Control Module (LCM) as follows:

1. RCM is mainly worked for acquiring the environmental information, and wireless data transceiver and other functions. The module receives instructions from the control terminal and uploads data through the ZigBee wireless sensor network or GSM mobile communication network. The module can also provide equipment security parameters according to their own information in the environment and other peripheral equipment information to the RMM.

2. RMM can evaluate the security of the equipment according to the information which RCM sends to it, such as the equipment status, environmental parameters and equipment operation situation. Give the alarm information and implement the destruction of sensitive resources once the equipment is in danger or critical condition.

3. LCM is mainly to complete some normal functions such as the system condition monitoring, code integrity check, user access authentication, and also should detect credibility of the equipment, in order to ensure the system is credible and reliable.

III The design of each module and functional description

1. RCM

RCM structure is shown in Figure 2. The whole module is composed of a sensor unit, a battery and a charge management unit, MCU, GSM module and the ZigBee radio frequency module and for connecting two buses of remote control interface and equipment monitoring unit.

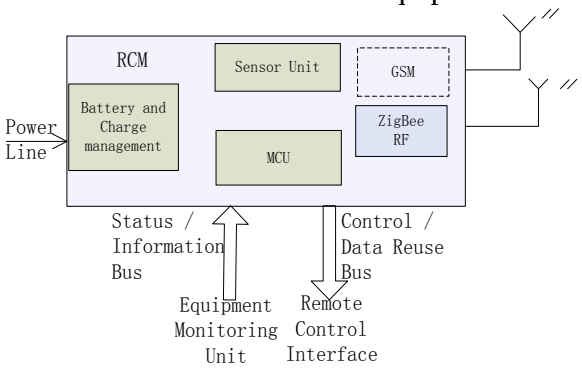

Figure.2 Remote Control Module

The sensor unit is mainly used to perceive the environment, collect the status of the equipment, and then send the information to the RMM for security assessment. GSM module and the ZigBee radio frequency module is mainly used to complete the wireless signal transceiver, the GSM module is optional, It's used only when the communication distance beyond the ZigBee network coverage. The RCM can use the battery when the equipment is out of the power supply. The power

supply cord can be used to charge the battery when the equipment is supplied.

2. RMM

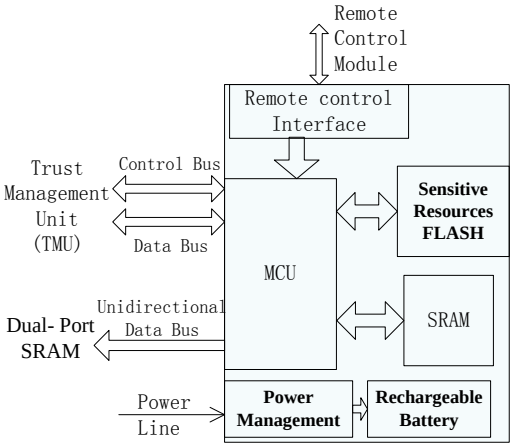

Figure.3 Resource Management Module

As shown in Figure 3, the RMM is mainly composed of the microprocessor, the sensitive resources FLASH, the SRAM and the power management, the rechargeable battery and the related data communication interface. Sensitive resource flash is used to store equipment related sensitive resources (password, algorithm and parameters). The MCU can realize the en/decryption and hash algorithm, in order to complete the data communication verification and other functions, ensure the equipment running reliable, and the confidentiality/integrity of the received information. The MCU complete the security assessment by the environment and status information from the other modules, and the microprocessor writes the sensitive resources to the dual port SRAM in LCM when it's in credible conditions, to provide data resources for normal operations. The information whether the LCM is reliable from the trust management unit(TMU), the password update operations are also completed by the TM; Microprocessor can erase the sensitive resources in the flash when necessary to ensure the security of the equipment. The rechargeable battery and power supply management unit provide energy support for the module, and the SRAM provides running space for the program of the microprocessor.

3. LCM

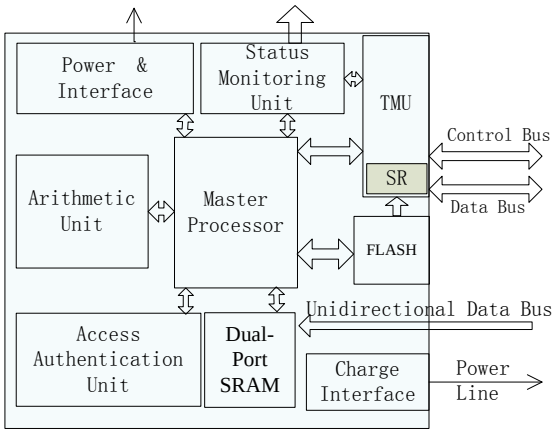

Figure.4 Logic Control Module

The LCM is composed of the following parts, as shown in Figure 4:

- The equipment master processor is mainly responsible for the normal business operations, management, execution related instruction and coordinate system resources.
- The arithmetic unit, equivalent to the coprocessor of the master processor, is mainly used to complete the operation of the algorithm, The unit can be a dedicated algorithm chip or a reconfigurable chip, and the specific parameters of the reconstruction algorithm need to be provided by the RMM, to ensure the algorithm's security.
- The access authentication unit, is designed to ensure the safety of the equipment through

authentication, at the same time, related operating instructions can be transmitted to the main control microprocessor through the module, according to the different users and their permissions, such as password updates, operation of the remote control module choose. The unit is the interface between the user and the equipment.

- The dual port SRAM provide operation space for the control microprocessor, sensitive resources from RMM are loaded when startup , in order to carry out the relevant operation.
- Power and interface unit and a charging interface are the power supply components, power support for RMM and RCM can be provided through the charging interface.
- The FLASH is used to store the running codes of the master processor, not only the master processor can read the codes, trust management unit can also read the codes in FLASH to verify.
- The status monitoring unit is mainly used to monitor the status of the system, such as the environment temperature, system power supply, the system running state, the user permissions and so on, the unit mainly uses some sensors and communication signal line to complete the information collection.
- The trust management unit(TMU), which is the most characteristic part in LCM, the unit complete the verification the operation reliability and trustworthiness of the LCM, collecting information about the state of the system and report the information and verification results to the RMM.

IV. Design of equipment workflow

The operation flow of the new designed equipment is shown in Figure 5. The equipment must have the following conditions before use:

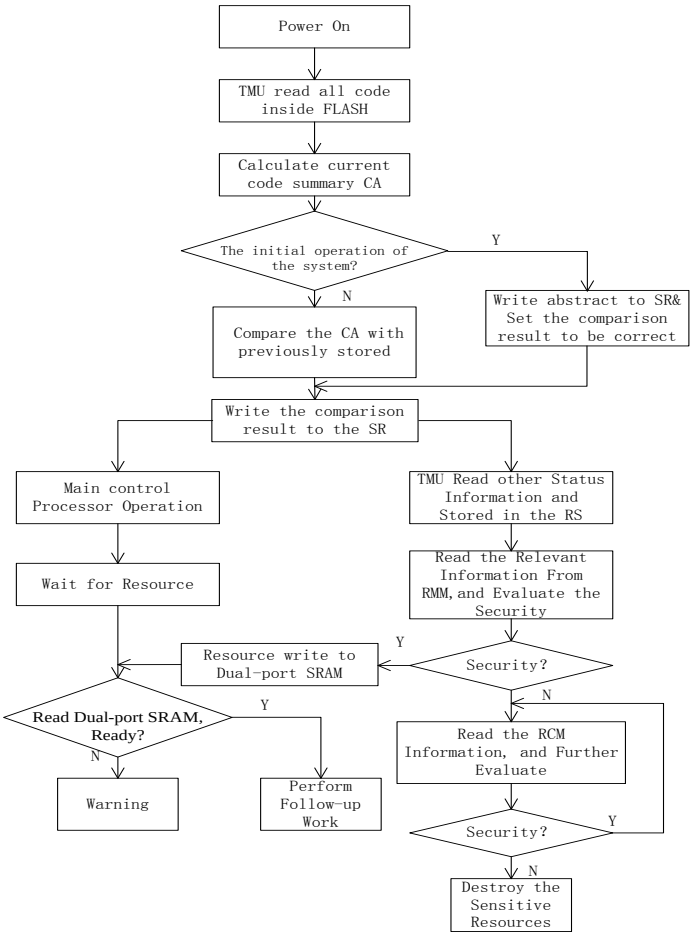

Figure. 5 Equipment Workflow

- The equipment manager must write the following information to the SR of the TMU: 1. the TMU initial key(TIK) of the algorithm for encryption and communicate with the equipment management center; 2. the user ID for evaluating user permissions.
- The RMM has been set the security parameter threshold to judge the security of the equipment.

From the workflow we can be seen that it's needed to assess the current equipment status and the security of the working process, alarm information will be proposed to the user if it's not safe enough, it's the users' responsibility to solve the related problems, and will destroy the sensitive resources automatically in critical situations.

V. Conclusions

The structure of the new designed information security equipment is divided into three modules, each module maintains limited communication and has the following advantages:

- Resource access authentication: Before the RMM provides sensitive resources to LCM, the security certification of the LCM should be carried out, to ensure that the status and operating of the LCM are normal, all these further ensured the reliable use of resources. At the same time, because of the design of data interface, the transmission of sensitive resources is unidirectional.
- Structure flexibility: The interface of the RCM and the equipment are simply designed so that it can realize the hot plug of the modules, and integration and functional cutting is every easy. At the same time, the working status of the RCM can be set up flexibly by authenticated users to ensure the flexibility of the module.
- Reliability of the resources destruction: In addition to a common power supply interface the RMM is also equipped with a rechargeable battery, which can provide protection for the RMM. Thus, the destruction of the sensitive resources in the emergency can be realized even when the equipment is dropped.

Reference

[1]ZHANG Meng,YAO Lie-ying,WANG Ying-qiao: A remote communication system based on CAN bus technology for PSM high-voltage power supplies[J], Nuclear Fusion and Plasma Physics,2015.1

[2] Chen Bo, GaoXiue,Sui Guangzhou:Research and realization on wireless remote control system[J], Chinese Journal of Scientific Instrument, 2006, 27(Z2)

[3]WANG Yi-le, SONG Shu-zhong, ZHU Jin-hong, DAI Le-yi: Research of remote monitoring system based on network[J], Chinese Journal of Power Sources ,2013, 37 (12)

[4]XIONG Rui-ping, YIN Guo-fu: Internet-based teleoperation system for networked manufacturing[J], Computer Intergrated Manufacturing Systems, 2006 12(11)

[5]TANG Yang, XIE Chong: Wireless remote control and monitoring system for well control equipment design[J], Manufacturing Automation 2013,(18)

[6]WANG Dewen, ZHU Yongli, DI Jian, ZHAI Xueming: A Method for Electric Power Equipment Remote Control Based on IEC 61850[J], Automation of Electric Power Systems, 2009,33(5)

[7]ZHENG Juan-yi: Research on Home WSN Based on ZigBee Technology and Remote Control[J],Video Engineering, 2010,34(4)