Journal of Computers Vol. 28, No. 4, 2017, pp. 157-169
doi:10.3966/199115592017082804017

Serial Communication Card and Emergency Technology in Internet of Things

Lei Zhang[1], Lun Xie[1*], Liang Chen Jin[1], and WeiZe Li[1]

[1] School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing,100083, China
xielun@ustb.edu.cn

Received 25 October 2016; Revised 13 June 2017; Accepted 26 June 2017

Abstract. Accompanied with emergency technology and Internet of things(IoT for short) closely, emergency measure is coping burst with things related to unexpected happened events. Intelligent serial communication is applied more widely in the communication field, in these areas three standards are still being widely used. The article designed an intelligent serial communication card which integrated three kinds of serial communication standards—RS-232、RS-422 and RS-485 and two kinds of protocol——UART and HDLC. The main problem is that there is no customized serial card containing IoT technology and enough kinds and number in the ready-made market. IoT is information of things using intelligent sensor equipment, by means of several kinds of network transformation, arriving at emergency information center, realizing automation of information interactive and disposal. This paper's novelty lies in the technology for Emergency and Internet of things, combined with self-design communication card, this product has huge promotion value.

Keywords: emergency technology, intelligent FPGA, Internet of things, remote monitor and control, serial communication

1 Introduction

Emergency is the need to deal with the sudden incidents, which contains two meanings: the objective, the event is sudden; subjective, the need to deal with such incidents. The connection between the emergency and the Internet of things is reflected in the software application level. Currently at home and abroad the Internet of things is not a uniform and recognized standards and definitions, but essence from the network analysis, Internet of things is the development of modern information technology to a certain stage, the emergence of a polymer application and technology improvement. In the past, the number of serial ports was finite, and the type was incomplete, and there was no RFID, ZigBee, Bluetooth interface in the card. This card contains various sensing technology, modern network technology and artificial intelligence and automation technology of polymerization and application integration, so that people and wisdom of dialogue to create an intelligent world.

1.1 Intelligent Serial Communication Card Research Goal

The rapid development of emergency technology and intelligent serial communication card based on FPGA by the receiving host computer of each channel configuration information of each serial channel configuration, channels can achieve any combination of three kinds of serial communication standard besides two serial communication protocol. Various serial channels independent of each other, not interfere with each other, can support a variety of baud rate of serial communication, also can be customized, can meet the requirements of a variety of intelligent serial communication. Intelligent serial communication card intelligence lies in that through software setting can configure various serial

* Corresponding Author

communication channel parameter, FPGA receive configuration information after the information is written to the channel configuration registers, each channel at the beginning of self configuration information read, completed the configuration process. The design of serial communication card is mainly composed of FPGA hardware and emergency software.

1.2 Networking Emergency Technology Purposes

Networking emergency technology is using the advanced network communication technology, computer technology and integrated wiring technology, will be related to the various subsystems and the for integrated management, so that people have more to deal with emergencies, the loss of the accident is reduced to a minimum. Through a variety of Internet of things technology, to ensure that the emergency command and external information communicate smoothly, at the same time, give a variety of reasonable control for intelligent equipment.

2 Internet of Things Architecture (ITA)

The system structure of the Internet of things, a complete Internet of things system is usually divided into three levels: perception layer, network layer, application layer [1]. The bottom layer is the sensing layer for data acquisition, the middle layer is the network transmission layer for the data transmission, the upper layer is the practical application of the industry, also called the application service layer.

The system structure of the Internet of things module, as shown in Fig. 1.

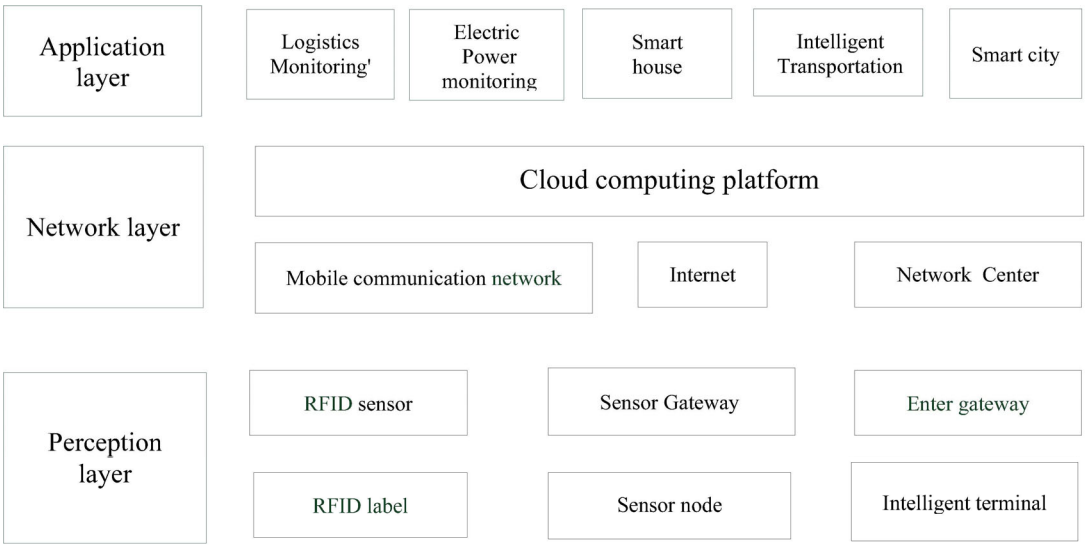


Fig. 1. The system structure of the Internet of things

2.1 Perception Layer

The perception layer is the skin and facial features of the Internet of things [2]. Perception layer consists of the sensor data acquisition equipment composition, the bottom in the Internet of things is the foundation of Internet of things, mainly realizes the data acquisition pretreatment, perception layer technology including sensor technology, RFID technology, two-dimensional code technology, ZigBee, Bluetooth Technology.

2.2 Network Transport Layer

The network transport layer is the nerve center of the Internet of things and the brain: data transmission and processing [3]. The network layer of the Internet of things is built on the basis of the mobile communication network and the Internet, which is connected with the mobile communication network and the Internet.

2.3 Application Service Layer

Application service layer is the Internet of things "social division of labor" - the combination of industry needs, to achieve a wide range of intelligent. The ultimate goal of the development of the Internet of things is to use the services provided by the application layer, namely, the Internet of things is ultimately to provide services for the human. Internet of things application layer is mainly through the analysis and processing of the perception of data, to provide users with a variety of services, is the Internet of things technology and industry depth integration of professional technology [4]. Specific applications can be divided into monitoring system, query system, control system, scanning system, and its representative examples such as logistics monitoring, remote meter reading, smart home, intelligent transportation, no parking fees, etc.

Fig. 1 shows a typical industrial control system network. Occasionally industrial control systems are connected via Ethernet to a corporate network used for day to day business operations. In the figure, the corporate network and the control system network are isolated by a security gateway. Isolation of the corporate and control system networks may be accomplished via use of virtual LANs, gateway devices which enforce various authorization schemes, or firewalls.

When Internet of things is used in industry, Industrial control system (ICS for short) is developing fast. Industrial control systems are distributed cyber-physical systems [5]. Remote terminal units are connected to sensors and actuators to interface directly with the controlled physical system. RTU store control parameters and execute algorithmic code (such as ladder logic or C programs) to directly control the physical process. Industrial control systems also support supervisory control and data acquisition. Industrial control systems include a master terminal unit (MTU) connected to the RTU via a communication link. This communication may use Ethernet or serial port technologies including RS-232 and RS-485. A common application layer protocol for MTU to RTU communication is MODBUS which includes MODBUS/TCP for Ethernet networks and MODBUS RTU or MODBUS ASCII for serial port networks [6]. The MTU polls the RTU periodically to read physical measurements from the controlled process. This information is displayed on a Human Machine Interface (HMI for short) to allow situational awareness and control. HMI allow control system operators to interact with the physical process. For example an operator may open a breaker to island an electric circuit, or open a valve to release pressure in a pipe or direct material flow. The MTU, RTU, communication link, HMI, and operator form a supervisory feedback control loop.

The diagram includes four networked devices HMI, MTU, Historian, and RTU. Often multiple kinds of communication links are used in an industrial control system. In the network, the security gateway connects to the HMI host and the historian via an Ethernet link. The HMI host is connected to the MTU via a RS-232 serial link. The MTU communicates with the RTU via an RS-232 or RS-485 serial link. The MTU to RTU link includes a proprietary radio link. Radio links are often used to connect device over distance without the need to install a wired link. The HMI to MTU and the MTU to RTU links use the MODBUS RTU or MODBUS ASCII protocol. The system diagramed in Fig. 1 matches control systems in the MSU SCADA Security Laboratory which includes multiple industrial control systems using commercial hardware and software and laboratory scale functional physical process from various critical industries [7]. There are many variations on the system shown in Fig. 1. Contemporary systems often replace the serial links with Ethernet links. Many types of wireless links, serial links and many application layer protocols are available.

3 Design of Serial Communication Card

Intelligent serial communication card based on FPGA by the receiving host computer of each channel configuration information of each serial channel configuration, each channel can achieve any combination of three kinds of serial communication standard and two serial communication protocol. Various serial channel independent of each other, do not interfere with each other, and support a variety of baud rate of serial communication, with great can be customized, can meet the requirements of a variety of intelligent serial communication [8]. Intelligent serial communication card intelligence lies in software setting can be completed on various serial communication channel parameter configuration, FPGA receive configuration information after the information is written to the channel configuration registers, each channel at the beginning of self configuration information read, completed the

configuration process. The design of serial communication card is mainly composed of FPGA hardware and software.

3.1 Software Composition

The intelligent serial communication of the software part is divided into three parts: programs in the FPGA chip, is mainly responsible for the complete configuration of various serial communication standards, communication protocol; serial data of various serial channel is detected, receiving, sending and processing [9]; complete the serial channel between the host computer and the data transmission. Second, control interface. This part mainly completes the user according to the demand of each serial channel such as communication standard, communication protocol and the corresponding parameter configuration. This part also completed the transfer effect of real-time display; the third is the underlying driver, the completion of a major part of the driving PCI bus, to host computer to realize real-time communication function [10]. Fig. 2 is hierarchy structure of the software.

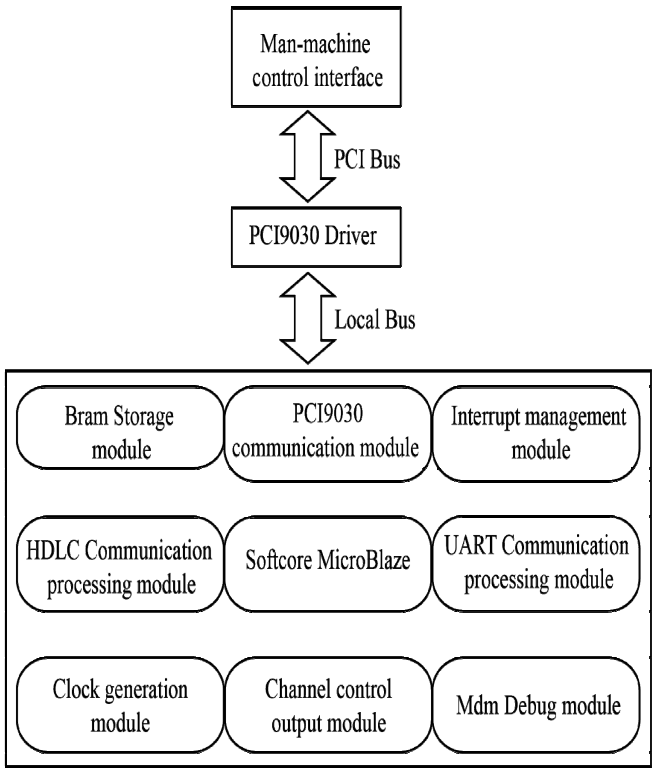


Fig. 2. Software structure level diagram

3.2 FPGA Chip Design

In chip design framework. In this paper, FPGA uses embedded solutions to design, the main components of the embedded system including the MicroBlaze soft processor core, the system bus, the peripheral Core IP clock generation module [11].

(1) MicroBlaze is FPGA in the design of the soft processor core, FPGA in the main program running on the inner core. The role of the soft core can be understood as a CPU core and its interior has the RISC architecture and a Harvard architecture 32-bit instructions and data bus, the 32 general-purpose registers R0 to R31 can configure a custom, can through access to the processor MicroBlaze status register (MSR) to understand at this time of the working state of the processor.

(2) Bram_block is the on-chip storage module, the size is 64K, set up in the SOPC system, which is equivalent to the meaning of CPU in Cache, the storage module stores the data and instructions for the MicroBlaze temporarily stored. It is different from other on-chip storage resources, IP can directly access.

(3) Debug Module Mdm is Microprocessor, due to the introduction of MicroBlaze debugging interface to support JTAG based software debugging tool (BDM), the debug interface and the MDM core, and MDM and FPGA JTAG Xilinx port connected [12].

Peripheral IP core can be directly realized all the functions required by the user and peripheral IP core respectively Myhdlc_0, XPS_EPC_PCI9050, S_channel_Ctrl, XPS_uart232, XPS_uartlite_0, XPS_INTC_0. This paper discusses its main function and realization in the behind.

(4) Mb_plb bus is Processer Local Bus (PLB), PLB bus contain the bus control unit, the watchdog counter, read/write data path, with a separate address space, the composition of the structure as shown in Fig. 3. Its main features include: the bus master device of lap PLB there is no limit to the number; support 128 bit, 64 bit and 32-bit the from device and the main equipment; arbitration time less than 3 cycles; the PLB bus to support sharing mode or the end to end configuration mode; PLB bus with a watchdog timer function.

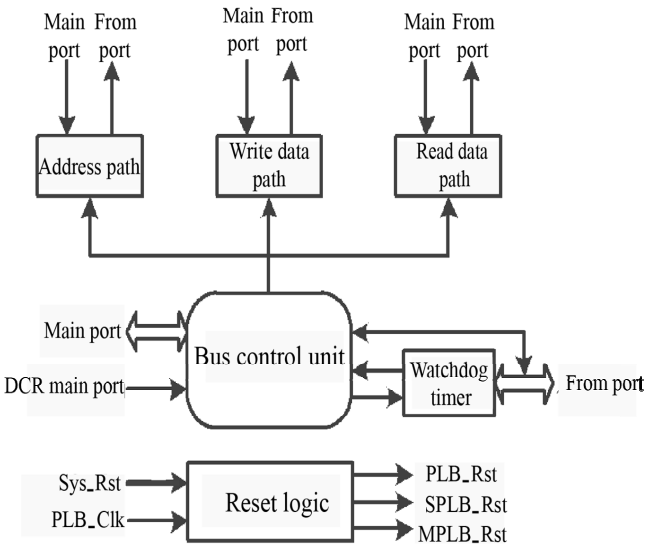


Fig. 3. PLB Schematic diagram of bus structure

(5) Lmb Bus is Local Memory Bus, the bus is responsible for the soft core and on-chip memory module Bram block read and write operations can be divided into responsible for instruction to read and write operation ilmb and data read and write operations dlmb bus, the bus will command to read and write, read and write data separately, in the same clock cycle can be completed at the same time read the instructions and data.

(6) Mdm Bus is special bus for online debugging. Mainly responsible for the debugging and testing functions in the core program.

FPGA with embedded system development model [14], on-chip program so as two parts: peripheral IP processing module and core software processing part of the program. Peripheral IP processing module is mainly responsible for basic communication protocol processing, the data storage, and PCI9050 between communication and the channel control; software processing part of the program is mainly on each channel stored data forwarding, and receiving host computer sent the number to send to the protocol processing module.

Peripheral IP hardware module. FPGA internal peripheral IP hardware module program is divided into four modules: UART asynchronous processing module, synchronous HDLC processing module, access control module and PCI9050 communication module, which UART asynchronous processing module is divided into two parts: RS-232 processing module and RS-422/485 processing module. The 9 pin RS-232 protocol using the simplified, need to complete the asynchronous communication mode alone, the use of Xilinx IDE 12.1 environment with RS-232 IP core, but in the end the data stored in the received FIFO, MicroBlaze left the memory interface [15]; HDLC synchronous processing module respectively and can be divided into sending and receiving two in part, HDLC communication mode, the receiving process is as follows, first, with 6 serial asynchronous communication channel selection and communication protocol through the PC control interface is set by the user, 6 serial data into the FPGA were processed by the synchronous processing module of each corresponding, and then stored in the receive buffer respectively (FIFO_Rx), carried out by the MicroBlaze to read and write PCI9050 in the transmission module waiting for PCI9050 to read, and finally sent to the host computer. The sending process is first by PC selected configuration protocol for each channel and way, and then will be 6 channels on the

transmission of information through PCI9050 written in field programmable gate array (FPGA) of each channel transmit buffer (FIFO TX). And then through the MicroBlaze sent to each channel sending module, then the protocol processing and sent to the connected device. Channel control module is in the first through the MicroBlaze read each channel configuration register information [16], the channel parameters are passed to a channel control module, access control module complete the configuration of each channel and open the serial channel. PCI9050 communication module is mainly through the xps_epc_PCI9050 to complete, its main function is to connect the PLB bus and Local Bus PCI9050 effectively, and achieve the data transmission between the two kinds of bus timely and reliable.

(1) UART communication processing module

UART processing module consists of six modules: send buffer and receive buffer, baud rate generator module, the logic control module, sending module and receiving module. The sending module and receiving module are the most important function modules of the whole logic circuit, they want to complete the protocol conversion and data sending and receiving. Baud rate generator module according to set the baud rate to produce corresponding crossover factor, then the system clock of corresponding frequency baud rate clock. The data cache module FIFO there are two main considerations: one is set up to solve the problem of FPGA PCI9050 and Local Bus cross clock domain communication problems, FPGA's internal clock and Local clock on the Bus is not consistent, data cannot be transmitted directly to a buffer zone to solve in different speed and remove the problem; the two is to solve the problem of competition to transfer 6 road serial channel, the 6 channels simultaneously, each independent of each other, and to the path of transmission is only 32 Local Bus, so each hand to set up FIFO data cache, on the other hand, waiting for the PCI9050 on each FIFO read because the storage speed, reading speed is much faster than the data, so it can guarantee the real-time communication between computer and channel 6. The logic control module is through the control information of the host computer to read, the corresponding agreement of the channel configuration control [17], but also for the entire process control.

(2) HDLC communication processing module

The HDLC protocol using ISO-13239-2002 version, the HDLC uses normal response mode (NRM) and normal response (NRM) mode is suitable for point to point and point to multi-point imbalance link structure, especially multi point link. In this way, the control of the whole link is in charge of the master station, the main work of the master station includes the initialization link, the control data flow, the recovery link, etc. From the station operation is simple, only in the case of the main station explicitly allowed, it can make response [18].

HDLC processing module is mainly divided into 5 small modules: data cache module, the clock generation module, CRC check code generation module, send module, receive module.

(3) PCI9050 communication module

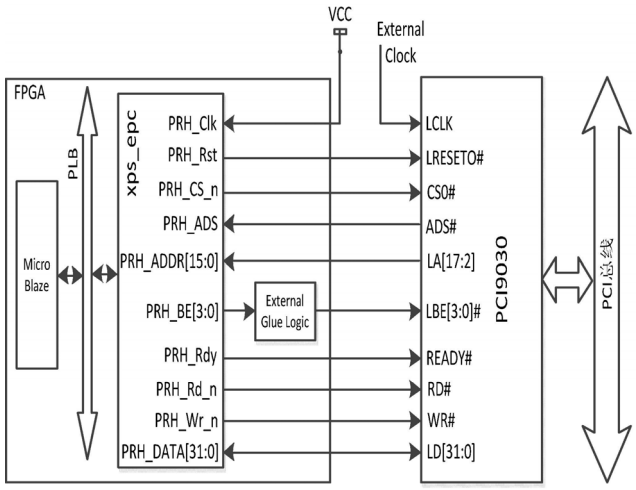


Fig. 4. Xps_epc Module and PCI9050 connection figure

The module is mainly responsible for the completion of the through pci9050 and PC communication, host computer through pci9050 complex PCI bus change for simple local bus, the pci9050 local bus and FPGA connected to the main signal line: 32 bidirectional data signal line LD [31:0], 16 address signal

lines LA [17:2], write enable signal line WR#, read enable signal line RD#, address lock control signal line ADS#, READY# signal line, as shown in Fig. 3. This part of the main circuit to achieve the communication between the PCI9050 chip and FPGA functions, including the control of read and write timing and decoding address, and so on.

(4) Channel control output module

Channel control module and the output of the main module from XPS GPIO complete the channel selection and light indicator, the module function is relatively simple, just read the information of each channel configuration registers, then pulled the corresponding pins can be. GPIO is a general input and output peripheral of PLB bus, each GPIO can be configured dynamically as input and output port. GPIO registers can be accessed in double - word, word and byte.

3.3 FPGA Software Programming Design

FPGA software program flow. The main program begins to read the configuration register information, complete its own configuration of the various channels, verify the configuration is completed, the completion of the system into the idle state.

In idle state, the system waits for the ADS# signal of PCI9050 and the interrupt signal of each channel. In this state, the IE (Interupt Enable) bit is set to 1 in the system MSR status register, and the system is able to query the PRH_ADS signal of the xps_epc module. Upon receipt of the road, a serial transmission channel interrupt signal IRQ n, the system enters data receiving status register the juxtaposition of MSR state ie bit is 0.

In the receiving state, the system will go through the serial channel has to deal with the data written to the receive FIFO buffer FIFO_Rxn. After the completion of the writing, pull system high XPS_EPC module of PRH ads signal, told PCI9050 data preparation is complete, read latency. After reading the data is completed, the system receives the PRH_Rdy signal indicates that the data read is completed, the next reading. FIFO_Rxn module in the empty signal, indicating that the data read all completed, the system set the MSR register IE to 1, enable interrupt and return to the idle state [19].

When the system to query the PRH_ADS into a high, that PCI9050 is about to send data, the system will enter the state of transmission. At this point the system will ie position 0, when PRH WR signal is pulled high, start sending data, pci9050 will data is written in a channel to transmit FIFO buffer FIFO_Txn. After the completion of the writing of, pulled READY# signal that send the completed, the next transmission. When the PRH_ADS signal is low, it indicates that the data is complete. Finally, the system will data transmission of the FIFO FIFO_Txn cache to the corresponding serial channel processing module to send, after the generation of the empty signal in the FIFO module FIFO_Txn that send data have been sent, the system set ie bit is 1, re enable interrupts and return to the idle state.

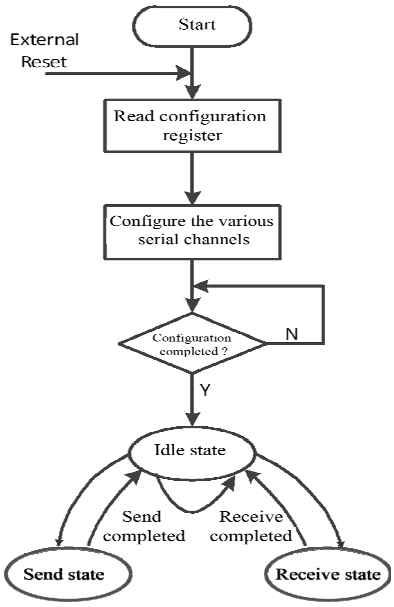
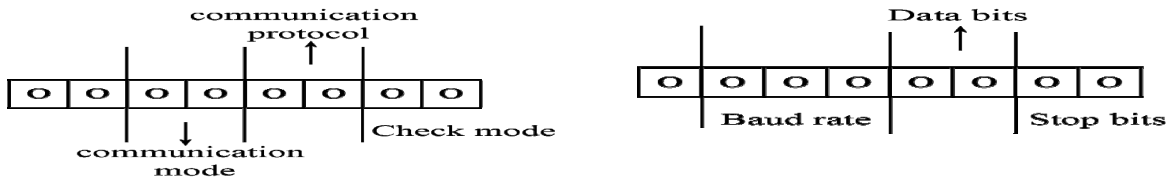


Fig. 5. State transition diagram of software main program

Each configuration register definition. Each channel serial configuration register is controlled by the configuration register and the baud rate, data bits, stop bits configuration register and the configuration register centralized control the configuration of the configuration of each channel RS-232/422/485 protocol and asynchronous transmission mode, transmission of data and the corresponding channel state information read to the simple control, the module can transport protocols for each channel and the way set in accord with external connected equipment communication requirements.



(a) Control configuration register

(b) The baud rate, data bits, stop bits configuration register

Fig. 6. Partial configuration register definition

FPGA built-in two configuration register, its role is stored record PC control interface input configuration information, second, for each two configuration register information read to complete the configuration of various by FPGA. Table 1 is the definition of the 1 parts of the register.

Table 1. Register partial flag definition

Num	Communication protocol	Communication mode	Check mode	Stop Bit	Data bits
00	RS232	HDLC	CRC check /Odd parity check	1bit	6 bits
01	RS422	UART	Parity check	2 bits	7 bits
10	RS485	Invalid	No verification	Invalid	8 bits
11	Invalid	Invalid	Invalid	Invalid	Invalid

PC control flow. PC control function of each serial port can be communication HDLC/UART, communication protocol (RS-232/422/485), parity and baud rate, stop bit, data bits, such as select and configure the corresponding, baud rate, stop bit, data bit settings when communication UART available. The communication mode of the HDLC, receiving the clock synchronization data receiving and sending can set the baud rate to select clock synchronization. After all channel configuration, click on the configure button, the channel configuration information is transmitted to FPGA MicroBlaze configuration is complete, after configuration is complete, the pop-up configuration complete the dialog box, click OK after that each channel configuration has been completed.

After configuration is complete, the PC will be required to messages sent through the PCI bus through PCI9050 will send the information into the corresponding channel to transmit into FIFO, waiting for the FPGA to read. When the channel is idle serial send; when receiving the FPGA will certain channel received the information into the channel of the receive FIFO in and send PRH ready signal waiting PCI9050 read, and then upload to the host computer.

4 Instant Messaging and Remote Monitoring

4.1 Instant Messaging System

The instant messaging has four protocols: instant messaging and attend the IMPP (Instant messaging and presence protocol), presence and instant information protocol prim (Presence and instant Messaging Protocol), for instant communication and attend extended balance process initiation protocol simple (session initiation protocol for instant messaging and Presence Leveraging Extensions) and extensible messaging and attend the XMPP (extensible messaging and presence protocol).

IMPP defines the necessary protocol and data format, which is used to construct a real time information system with the ability to receive and publish the space. An important draft of the organization's publication has two: one is for the site space and instant messaging model RFC2778; the other is for the instant messaging / space protocol requirements of the RFC2779. RFC2778 is a document of the nature of the draft, defines the principles of all presence and IM services. RFC2779 defines the minimum requirements for IMPP. In addition, the draft also defines a number of terms of the presence service, such as the operation of the command, the format of information, as well as presence server how to change the status of the presence notification to the customer. PRIM is currently almost no longer using. SIMPLE is so far the development of a more perfect. SIMPLE and XMPP two protocols, are in line with RFC2778 and RFC2779. SIMPLE plans to use SIP to send presence information. SIP is a protocol for terminal development in IETF.

4.2 Remote Monitoring

Remote monitoring function is one of the most complex functions of the system, which requires IM system, Http communication, UDP communication, image processing, and so on. So the test of remote monitoring system based on other functional test is carried out. The test is divided into two parts, one is the establishment of P2P communication, that is, NAT penetration; two is the image transmission, that is, the establishment of P2P connection data transmission work. NAT penetration test network environment is shown in Table 2.

Table 2. NAT test network environment

Equipment	network environment
P2P Center server	Location: fixed address of Supermarket Network IP: 115.25.48.198
Home gateway	Location: analog home network IP：192.168.13.10 Gateway: 192.168.13.1 Exit: 202.204.54.11
User terminal	Location: analog public Wi-Fi IP: 10.22.13.44 Gateway: 10.22.13.33

Based on the client's system clock, the time for initiating the P2P connection request is the start time, and the data of each step in the connection process is set up. In the network situation is relatively good, the user terminal with about 6S time and the family gateway to establish a P2P connection.

In P2P network, some of the data communication with the node initialization, the same can be used on the IM platform based on XML streaming. In the design of the full use of IM system TCP connection is reliable, advantages of news framework of unified, and of UDP network environment adaptation, control the advantages of flexible connection, using two kinds of communication mode to undertake in the nodes on the P2P connection establishment process in different tasks, collaboration to achieve efficient communication.

Communication node from the initial connection to the establishment of P2P communication, the use of instant messaging and data reported in collaboration with the steps shown in Fig. 7.

Cyber and physical. ICS attack methods can be divided into Physical Attack and Cyber Attack, and therefore may have a physical impact (Physical Effect) or Cyber Effect. Two kinds of attack methods and two kinds of influences are mapped into two dimensional matrix, and four kinds of classification are produced.

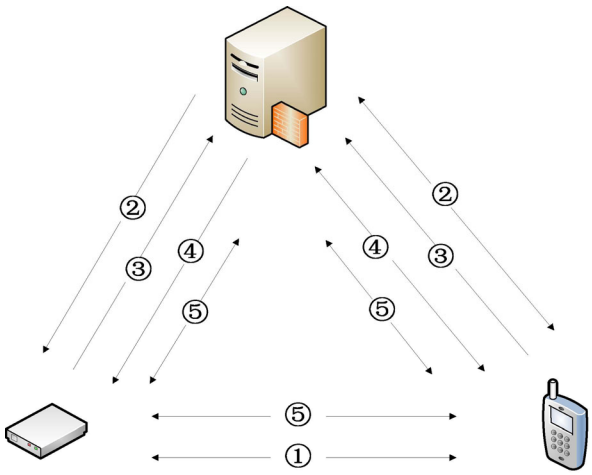


Fig. 7. Collaborative communication process

(1) Instant messaging

The User terminal through the IM system to the home gateway to send REQUIRE messages, request P2P connection. Home gateway to return RESPONSE messages that are available online.

(2) Instant messaging II

User terminal server sends the require message to P2P, the request distribution session ID, server create successful new P2P, terminal user transmits the ID, ID returns; and servers to gateway to send this message.

(3) Data report

The user terminal and the home gateway respectively send a UDP message containing the first step to the P2P server to the ID server, which is used as a heartbeat packet. The server receives the data report, analyzes the network address, according to the ID number to save in the corresponding conversation task.

(4) Instant messaging III

The user terminal sends a READY message to the P2P server and the session ID number, asking whether the network address of the two parties in the step of the step is registered. Server based on the ID number of inquiries, such as the two sides have received the registration of the network address, the two nodes return to the READY message.

(5) Data report II

The other communication node based on network address of the forth step received, UDP “hole” attempt. Attempt success marks set up P2P communication and connection process is completed, the two sides can negotiate their own follow-up point to point data transmission; otherwise the P2P server as a proxy, the exchange both follow-up data on the server side in transit. According to the step 2 distribution of session ID, in the server as a session tasks to deal with.

P2P server session, for the server to handle a pair of gateway and user terminal node to establish the basic task of the P2P connection unit. An example of a session that represents a P2P communication processing, the life cycle from the user terminal request connection to start, to the establishment of the P2P channel, or all data transmission over. The server side to handle the massive user node connection request, the design of the conversation task needs to be as simple as possible, efficient, easy to manage.

In the server program using Java language development conditions, this paper inherits the implementation of thread class Java in Thread to design the session task. Java language in the thread and the thread pool suitable for processing a large number of small scale parallel tasks [20].

The session task implements the caching, parsing and forwarding of the nodes of the two parties, the management of the network address of both parties and the control of the life cycle of the two parties. Its working flow chart is shown in Fig. 8.

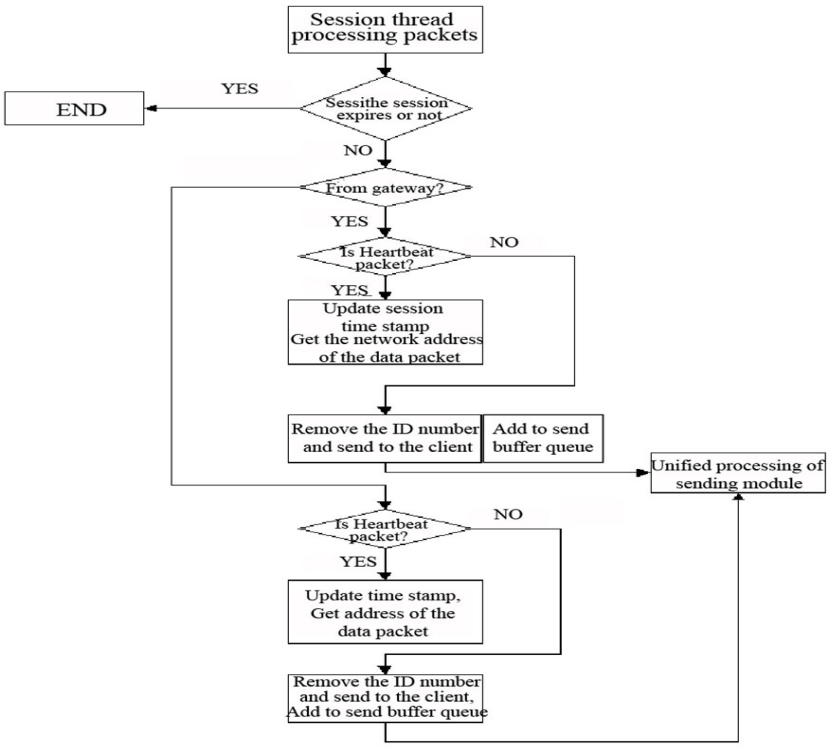


Fig. 8. Session task workflow

Test for image transmission, in order to maintain the consistency of the test, continue to use the above network conditions. A total of ten sets of new images of every 100 frames were tested, and the transmission efficiency was tested. Statistical results are obtained as shown in Table 3.

Table 3. P2P network image transmission efficiency

Num	Number of frames	Time consuming	The number of retransmission / retransmission packet number
1	100	36239	1/4、7~14、16、19
2	100	36317	1/1、5、7、9、11~13、15、17~19
3	100	104099	1/1~22
4	100	29203	1/2、13、15、17~19
5	100	24991	1/6、16
6	100	Not completed	1/2、3、5、8、11、13、16 Follow up client active disconnect
7	100	17332	1/2、9、21 1/0~21(The frame is missing all packets)
8	100	Not completed	1/3、6、9、11~13、15~17 Follow up client active disconnect
9	100	70761	1/2~21 1/0~21(The frame is missing all packets)
10	100	Not completed	1/3,、17、21 1/0~21 1/13、17、20 1/14、17、19、21 1/0~21(The frame is missing all packets) Follow up client active disconnect

In the above table statistics, in a test group of ten, 7 groups of smooth continuous transmission 100 frames, including the 6 groups for uninterrupted testing, namely maximum continuous transmission frames over 500. The other three tests in during packet loss retransmission times exceeds the upper limit, according to the debugging information that the client network obstruction, did not receive data gateway, so in the request retransmission times reaches the upper limit automatic disconnection after connection, is consistent with the objective to design.

In the completion of the 7 groups of tests, the 5 groups only once a packet loss occurs, the other group appears two times, that is, the image of a one-time transmission success rate in 98%~99%. In appear packet loss and retransmission, all one-time bulk transfer success; packet dropping number more than belonging to the image frame package possibility probability of about 50%, and the other 50% situation for sporadic packet loss. The average transmission time is 2.19 frames per second, which is about half the speed of the home network environment.

In the unfinished test group, after the loss of the packet, or a retransmission success, or due to fluctuations in the network conditions, there is a temporary obstruction, and can quickly recover. Therefore, by increasing the number of times to repeat the attempt to limit the number of times, you can reduce the client automatically disconnected.

5 Summary and Prospect

With the further technology development of those dimensions, all emergency events need to be monitored, forecast and forecast in advance. Close surveillance as much as possible, as far as possible. In advance of a possible occurrence prediction of unexpected events, in order to minimize the loss of people's lives and state property; to find and solve the disaster has occurred as fast as possible, so that timely rescue. Internet of things can provide this prediction, monitoring, detection and application, is closely integrated with the emergency. At the same time, intelligent series card can provide a quick solution for both emergency and Internet of Things.

Intelligent series card based on FPGA in software in the design process the method of embedded system, respectively, the foreign design IP module hardware and soft core CPU programming explained, to describe the process of PC to send receive data, and completed the communication module of FPGA and pci9050 the preparation and completion of the intelligent serial communication card in late stage testing.

In this paper, the overall operation of the various parts of the program is tested by the emergency & Internet of things technology. Combined with the current test results, the program runs stably, and the resource consumption is in the controllable range. The limitation of this research is that the depth of emergency technology is not enough, In the future, it will be more accurate, fast and intelligent by using computer software, at the same time, the speed of hardware transmission will be faster

Acknowledgement

This work is supported by the National Natural Science Foundation of China. (No. 61672093, No. 61432004), National Key Research and Development Program (No. 2016 YFB1001404).

References

[1] Q. Hong, Q. Zhou, Y. Wang, Research and hardware implementation of MD5 algorithm based on Hash function, Computer Engineering 39(3)(2013) 137-141.

[2] L. Zhang, L. Xie, W. Li, Z. Wang, A secure mechanism for networked control systems based on TrueTime, in: Proc. International Conference on Cyberspace Technology, IET, 2013

[3] Z. Pang, G. Liu, D. Zhou, Detection of deception attacks on the backward channel of networked control systems, in: Proc. Control Conference (CCC), 2012 31st Chinese, IEEE, 2012.

[4] Z. Deng, L. Xie, Y. Rong, W. Li, L. Jin, Data security transmission mechanism in industrial networked control systems against deception attack, International Journal of Security and Its Applications 10(4)(2016) 391-404.

[5] S. Yin, X. Li, H. Gao, O. Kaynak, Data-based techniques focused on modern industry: An overview, IEEE Trans. Ind. Electron. 62(1)(2015) 657-667.

[6] Y. Peng, C. Xiang, M. Zhang, D. Chen, H. Gao, F. Xie, Z. Dai, Industrial control system cybersecurity research, Tsinghua Univ (Sci & Tech), China 52(10)(2012) 1396-1408.

[7] G. Dondossola, J. Szanto, M. Masera, I.N. Fovino, Effects of intentional threats to power substation control systems, International Journal of Critical Infrastructures 4(1)2008 129-143.

[8] C.W. Ten, C.C. Liu, G. Manimaran, Vulnerability assessment of cybersecurity for SCADA systems, Power Systems, IEEE Transactions on 23(4)(2008) 1836-1846.

[9] Z.H. Pang, G.P. Liu, Design and implementation of secure networked predictive control systems under deception attacks, Control Systems Technology, IEEE Transactions on 20(5)(2012) 1334-1342.

[10] G. Hayes, K. El-Khatib, Securing modbus transactions using hash-based message authentication codes and stream transmission control protocol, in: Proc. Communications and Information Technology (ICCIT), 2013 Third International Conference on, IEEE, 2013.

[11] Z.H. Pang, G.P. Liu, D.H. Zhou, M.Y. Chen, Output tracking control for networked systems: a model-based prediction approach, IEEE Trans. Ind. Electron. 61(9)(2014) 4867-4877.

[12] L. Guoping, Secure networked control systems under data integrity attacks, in: Proc. Control Conference (CCC), 2010 29th Chinese, IEEE, 2010.

[13] R. Xu, L. Yang, S.-H. Yang, Architecture design of internet of things in logistics management for emergency response, in: Proc. 2013 IEEE International Conference on Green Computing and Communication and IEEE Internet of Things and IEEE Cyber, 2013.

[14] K.H. Yang, S.J. Niu, Data safe transmission mechanism based on integrated encryption algorithm, in: Proc. Computational Intelligence and Software Engineering, 2009. CiSE 2009. International Conference on, IEEE, 2009.

[15] G. Oliva, S. Panzieri, R. Setola, Agent-based input–output interdependency model, International Journal of Critical Infrastructure Protection 3(2)2010 76-82.

[16] C.W. Ten, G. Manimaran, C.C. Liu, Cybersecurity for critical infrastructures: attack and defense modeling, Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Trans. on 40(4)2010 853-865.

[17] W. Li, L. Xie, Z. Deng, Z. Wang, False sequential logic attack on SCADA system and its physical impact analysis, Computers & Security 58 (2016) 149-159.

[18] D.P. Cox, The Application of Autonomic Computing for the Protection of Industrial Control Systems, The University of Arizona, Arizona, 2011.

[19] W. Xu, Y. Tian, Xilinx practical tutorial FPGA development, Tsinghua University Press, Beijing, 2012.

[20] A. Kahate, Cryptography and Network Security, Tata McGraw-Hill Education, Noida, 2013.