Research and Implementation of fault-tolerant computer interlocking system

Chen GuangWu[1] ,Fan DuoWang[2]
Key Laboratory of Opto-electronic Technology and
Intelligent Control，Ministry of Education
Lanzhou Jiaotong University，
Lanzhou, China
e-mail: cgwlz76@gmail.com

Yang JuHua[3]
School of traffic and transportation,
Lanzhou Jiaotong University，
Lanzhou, China
e-mail:yjh-lanzhou@sina.com

Abstract: A new signal control system for railway stations, fault-tolerant all- electronic computer interlocking control system, is proposed,in which the computer-based interlocking system layer is constituted through the implementation of electronic security unit replacing the Relay, and the all-electronic fault-tolerant controlling for whole system is fulfilled through two of three fault-tolerant computer system. Furthermore, the overall structure, function and fault-tolerant security designing of the system are discussed in detail. The system can meet the requirements of high reliability, availability and real-time controlling, it also can monitor the external equipments and their own equipments real-timely. The system has been put into operation and run stably and reliabl.

KeyWords: All-electronic ; Fault-tolerant computer ; Railway signal ; Computer-based Interlock.

I. INTRODUCTION

The computer interlocking control system is the key equipment of signal for railway station, which accomplish the realtime control system mainly by force of computer technology, at the same time it is also a key safety system with high reliability and high security and high realtime, security act an critical role in the system, takeing fault-tolerent tecnology is an important way to make sure system's security. Signal control system for railway station mianly passed through three stage of development which is mechanical interlocking ,6502 electrical centralized contol system and computer based interlocking. At present , most of the computer interlocking control system which are came into play using computer to relize interlocking

relations opertion, also using security relay to control and collect basic device status.Actully,it is a system with computer interlocking +relay execute,but do not relize all-electronic fault-tolerant computer interlocking control system absolutely. As the rapidly development of power electronic technology , fault-tolerant computer tecnology and signal technology, and the requirement of signal control system's reliability and usability constantly advanced, adopting fault-tolerant computer interlocking with high reliability intergrate with all-electronic intelligent executive module to relize all-electronic computer interlocking control system.

II. SYSTEM STRUCTURE

The figure 1 show the system structure of fault-tolerant all-electronic computer interlocking system. The system is made up of monitor of computer of dual modul hot spared redundant, maintenance of computer, fault-tolerant interlocking computer of 3-module redundancy,all-electronic implementation system with redundantly secure commuication channel,network communication system, and so on. The whole system can be divided into three layers:opertion and display layer, fault-tolerant interlocking logic layer, all-electronic unit layer. And the operation and display layer and fault-tolerant interlocking logic layer communicate through redundancy industry ethernet; fault-tolerant interlocking logic layer and all-electronic performance layer communicate with ringlike or star optical network; the all-eletronic execute layer adopt redudant CAN bus communication . From the security point of view, the whole system is divided into security and nonsecurity zone, the operation and display layer is security zone, but fault-tolerant interlocking logic layer and the all-electronic performance layer are non security zone.

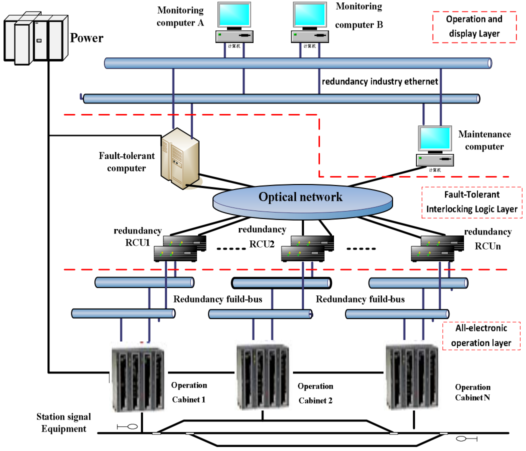


Figure 1. System Structure Diagram

III. OPERATION AND DISPLAY LAYER

Operation and display layer is made up of monitor of computer, maintenance of computer and communication network, which realize the whole system's operation, display, maintenance and communication with other systems of station.

978-1-4244-5392-4/10/$26.00 ©2010 IEEE

Monitor of computer(man-machine interface) is dual modul hot spared redundant and made up of industrial control computer A and B, communication with interlocking computer through two circuite industry ethernet. Two sets of monitor&control conputer work simultaneously, physically independent esch other,both have manul operation fuction(such as processing route). It send operation command to 3-module redundancy fault-tolerant interlocking computer in fault-tolerant interlocking logic layer through two circuite industry ethernet, as well as receive the executeive results of command and expression information of all signal devices in station from fault-tolerant interlocking computer, achieve all kinds of implementation tasks from people on duty, and display the results of implementation on the console or screen real-time.

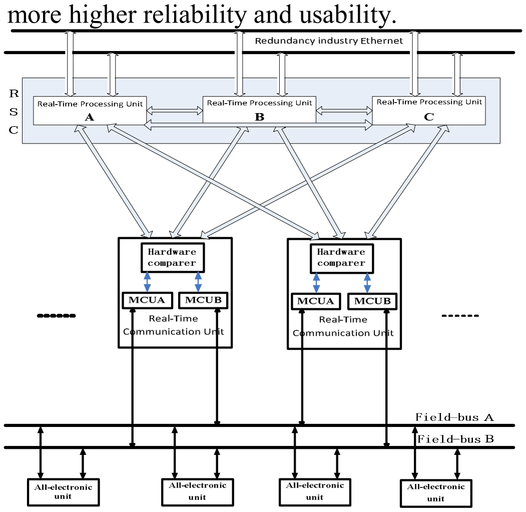
Maintenance of computer to display the state of station and to record and inquire equipment maintenance, and communicate with monitor of computer through two circuit industry ethernet. Aslo monitor operation command of monitor of computer, state of fault-tolerant computer command implement. Record operation command of people on duty, changed information of station and system error.And monitor communication state between the CAN bus and all-electronic implement units, collect state information of signal devices and implement units, to achieve the function of record storing, printing, reproducing and so on. Maintenance of computer have function of maintain computer of Electrical Affair Section andmicrocomputer monitor system,provide convenience for maintance of Electrical Affair. And offer interfacefor TDCS to relize connection with it.

IV. FAULT-TOLERANT INTERLOCKING LOGIC LAYER

Fault-tolerant interlocking logiclayer is responsible for accepting interlocking orders which are distributed by monitor computer, to run interlocking logicoperation according to local real-time status from the all-electronic performance layer , at the same time send the computation results to all-electronic performance layer and operation and display layer.

Fault-tolerant interlocking logic layer is the core of fault-tolerant all electronic computer interlocking control system, it is mainly composed of RPU(Real-Time Processing Unit,that is CPU mainboard),RSC(Real-Time Safety Computer, composed of three RPU). RCU(Real-Time Communication Unit).The problem which fault-tolerant tecnology due to settle is the usability of system, that is when fault appearing, we should let the computer system go on working, to make sure computers are incessantly used for clients. Fault-tolerant tecnology have already developed from most adopt reduntant functional unit or dual system to mainly adopt multiprocessor system using general processor, by integrating with VLSI tecnology ,can take a step forward reducing cost and improving reliability of system.

To implement fail-safe and fault-tolerant interlocking logic layer adoapting distributed configuration. Three operation units are distributed in this system, each operation unit accomplish task independently and take the output results sectionly to the RPU, to make sure the whole system not abnormally working which is caused by communication default, So that can distribute risks which are brought by centralazation contol, also can teamwork, make the system meet more higher reliability and usability.


Redundancy industry Ethernet
R
S
C
Real-Time Processing Unit A
Real-Time Processing Unit B
Real-Time Processing Unit C
Hardware comparer
MCUA
MCUB
Real-Time Communication Unit
Hardware comparer
MCUA
MCUB
Real-Time Communication Unit

Field–bus A
Field–bus B
All-electronic unit
All-electronic unit
All-electronic unit
All-electronic unit

Figure 2. Block diagram of synchronization and comparison

RSC is the core of the whole system, which is resiponsible for the control operation ,whether it is safe and reliable directly decide the safty and reliability of the whole system.RSC adopt 3-module redundancy configuration to implement fault-tolerant, that is to say three RPU which running the same interlocking programme are absolutely independently are absolutely independent.Operation orders of monitor computer are distributed to three RPU to take operation processing through industrial ethernet of redundant at the same time. To make sure the reliability of input information and synchronization of system operation, each RPU exchange information through high speed optical channel,make Collaborative but independently execute control command and make mathematical process by synchronization mechanism of each RPU. And send the output to the multi-mode hardware comparator in RCU through their star(or ringlike) optical communication network,each multi-mode hardware comparator in RCU compare three operation results, and output the right operate results to execute modules in station through two circuit CAN bus when there are two operate results consistent at least.At the same time multi-mode hardware comparator will feedback the comparated results to three RPU ,each RPU will proceed fault location and give the alarm according to the feedback results to make sure the system in working order. When all RPU in working order ,RSC working in the way of 3-module redundancy . If one RPU invalid, this system will degrad and working in the way of two modul hot spared redundant. The invalided RPU after repaired fast synchronize with other RPU by automatic tracing synchronization, reparticipate control operation, so that all sorts of system states can always keep consistent with each other.

To ensure the availability of communication between fault-tolerant special purpose computer system and field devices' performance unit, RCU adopt redundant mode, a set in host mode, another one in spared mode. RCU which is in the host communication mode sends the control command after comparison between multi-mode hardware comparator, and inputs the field apparatus's state collected by all-electronic performance unit to the RSC; RCU in spared communication mode is only for the output comparisons and bus monitor, not for sending command information. When the RCU in the host communication mode is failure, the RCU in spared communication mode was upgraded to host communication mode. In order to enhance system's reliability and extendibility, each RCU via two-circuit CAN field bus communicate with 32 performance units maximally. If the performance units are too many, the system's flexibility can be achieved by increasing the RCU. To improve the reliability of the system, each RPU exchange data among every RCU through their respective optical communication bus to realize the star optical network communications.

In the system all the communication between PRU and RCU use the optical channel, with the strong anti-interference ability, the strong anti-radar performance, and the high communication rate to ensure the system's high stability during running. The system has simple structure and strong scalability. On the condition that does not need to change operation and display layer, all-electronic performance layer and the redundant optical star network, the interlocking computer may take 2 out of 3 fault-tolerant computer systems, also may use double 2-vote-2 computer systems, and may realize the different pattern interlock system. To increase or decrease all-electronic performance system only according to the number of control devices can fit the various station scale size, and have regional interlock function.

In order to guarantee the reliability of logic operation layer, the CPU motherboard uses the hardware circuit board which designs specially, the processor uses 32-bit processor. Increase the automatic failure detection circuit, the synchronous comparison circuit, the optical communication interface circuit and so on in the CPU motherboard to enhance the fail-safe circuit characteristic. Because the multi-mode hardware comparator has the critical function to overall system's reliability and security, so adopt a million-gate large scale FPGA to design multi-mode hardware comparison controller chip. To guarantee that the communication links has the fail-safe performance, real-time communication unit RCU also use specifically designed communication circuit and communication security protocol. RSC take real-time embedded operating system VxWorks as RPU operating system,, develop the dedicated operating system closely with the CPU board hardware through cutting the operating system kernel, further strengthen the system's fault tolerance, reliability and real-time.

V. ALL-ELECTRONIC OPERATION LAYER

According to the type of station signal foundation equipment, all-electronic performance system make up of performance units such as the rail switch module, the signal module, the sector module, the telegraph code module, the scattered module and other interface module. The performance unit in accordance with the integrated design concept of "control, monitor, surveillance", realize "2-vote-2" logical control and closed loop detection, receive the interlocking operation result separately through the two-circuit redundancy CAN bus, carry on "and" logical control output, and real-time gathering device status feedback to the interlocking computer. The performance units transmit various state parameters to the maintenance monitoring machine through monitoring CAN bus, adopt the new power electronic devices as switching elements to replace the safety relay, achieve non-contact all-electronic control in the railway signaling system.

The all-electronic performance layer is responsible for the implementation of control commands which come from the fault-tolerant logic control layer, simultaneously transmit the field signal device's real-time condition to the fault-tolerant logic control layer. Both the intelligent gathering module and the intelligent driver module use the "2-vote-2" logical structure, with complete self-detected function, fault-tolerance function and dynamic-redundant function.

In the implementation of the unit, all controllers and monitors are designed for two sets. The interlocking operational data gives MCUA and MCUB separately through two- circuit CAN bus. Two MCU use "2-vote-2" and logical comparison to control output, take separate detection circuit monitoring real-time output and input signals respectively, carry on the synchronization and examination about order and condition through MCUA and MCUB synchronizing circuit. For general failure, double MCU after judgment and comparison can differentiate the failure nature, and make corresponding processing. If after comparison the processing results are inconsistent, might determine some group malfunctioned. If one of the MCU output port damages and occurs a fixed power, this can be found in MCU synchronous detection, so the failure will not cumulate. The two-circuit comparison may also avoid the influence of external interference on the module effectively.

In performance unit, after MCU dynamic control output the control command, the detection circuit uses the dynamic pulse feedback signal back to the MCU to carry on judgment processing to form the closed-loop control. When disconnection or short circuit the outputs are fixed DC level invalid signal, realize the false-true. If the state is unusual, cut off the driving power supply and the control output of dangerous side automatically while uploading alarm information.

VI. THE SYSTEM FAULT-TOLERANT DESIGN

In order to facilitate modular combination according to station scale, the system structure use the tree structure, realizes the fault isolation and the system's expansion. All the system' major subsystems adopt redundant mode or multi-mode type to improve system availability and enhance the system redundancy. The partial failure can be isolated and shield automatically to prevent the error output, and to guarantee system continuous and stable operation.

In the circuit board designing process with fault-tolerant computer's CPU motherboard and communication board, the electromagnetic interference and electrostatic protection are fully considered, makes isolation and protection well between power and ground. The hardware circuit designs the self-checking circuit for real-time detecting the state of the essential component, turnoff control output automatically on the exception condition. Maintains the system reliability through automatic withdrawal or re-start synchronization.

The multi-mold hardware comparator receives the control output form three sets of fault-tolerant computer's CPU system respectively through the three- circuit optical communication interface, undergo the hardware division, communicate with performance units by two-circuit CAN bus. The multi-mold hardware comparator designs into FPGA-based hardware controller chip without the software to vote output, so avoid the wrong output possibility causes as a result of the software flaw. The multi-mold hardware comparator takes redundant mode, when the main multi-mold hardware comparator in unusual state, switch to spared multi-mode hardware comparator automatically to compare the output. At present domestic and foreign 2 out of 3 fault-tolerant computers usually uses global comparator controller to realize 2 out of 3 output votes, exists the risks of overall system's paralysis due to its breakdown. The partition comparison and control can be achieved through dividing global hardware comparison controller into multi-channel redundant hardware comparison controller. Any section of them fault will only affect the partial execution control system's control output, but will not interfere with system's whole normal work.

Uses Vxworks operating system which have passed through the International security certification, cut out the function codes which is not used in operating system kernel, guarantee operating system kernel simple and stable, improve task dispatching capabilities, enhance the design about memory anti-leak, increase the function of driver code, only retain some interface driver codes in CPU motherboard design, form the special-purpose operating system, and realize the operating system and the CPU motherboard's close union.

Because of the synchronization need of status and data between the multiple independent operator units of fault-tolerant interlocking computing layer, the synchronization of intermediate state when running guarantees the running status consistent and the mechanism of failure recover and automatic isolation. When any arithmetical unit re-enter the system, realizes the active tracking synchronizing operation automatically; in running process, arithmetical unit in each operation cycle takes the logical comparison between intermediate state and comparison results. If discovered that this arithmetical unit data or the condition are inconsistent with other 2 set, requests for data synchronization initiative with other arithmetical unit via high-speed optical synchronous channel, maintains logical operation condition data's consistency and synchronization.

ACKNOWLEDGMENT

The all-electronic fault-tolerant computer interlocking control system uses the redundant structure, the failure isolation technology and the safety protection technology to guarantee the system hardware's safety and reliability. The fault-tolerant mechanism ensures the shield of single points of failure and the system's continuous safe operation. In the interlocking logic, the use of multiple technologies ensures the safety implement of interlock logic and the security and reliability of the software part in system. System has been already put into application in a number of stations, runs stably and reliably to guarantee the safe output of the entire control. In the course of future research, needs to carry on European standard EN5012X safety assessment and verification.

REFERENCES

[1] Hunger,M.Hellebrand,S.Verification and Analysis of Self-Checking Properties through ATPG[C]. On-Line Testing Symposium, 2008. IOLTS '08. July 2008:25-30.

[2] Wang Shuai,Ji Yindong,Dong Wei,YANG Shiyuan. Design and RAMS Analysis of a Fault-Tolerant Computer Control System [J]. TsingHua Science And Technology. 2007 .12(Z1) .

[3] Hai-feng Wang,Wei Li . Component-Based Safety Computer of Railway Signal Interlocking System. Computing, Communication, Control, and Management[C], 2008. CCCM '08. ISECS International Colloquium on Publication Date: 3-4 Aug. 2008.Volume 1:538-541.

[4] Ramaiah,P.S.Ben Swarup,M.Kumar,K.R.Conceptual Modeling for Safety Critical Computer Systems[C]. Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2008. SNPD '08. Ninth ACIS International Conference on.Aug.2008:814-819.

[5] Tetsuaki Nakamikawa,Yuuichirou Morita,.etal.:"High Performance Fault Tolerant Computer and its Fault Recovery", IEEE (PRFTS '97) (1997).

[6] Benso A,Di Cado S,Di Natale G,et a1.A watchdog processor to detect data and control flow errors[A].Proceedings of On-Line Testing Symposium[C].IEEE,2003,144-148.

[7] CENELEC:EN50128 Railways Applications:Communications, signaling and processing systems Software for railway control and protection systems[S].2001.

[8] CENELEC:EN50126Railway Applications:The Specificaton and Demonstration of Reliability,Availability,Maintain-ability and Safety (RAMS)[S]. 2002.