M out of N Safety Computing System Based on General-Purpose Computers

Xingya Dai[1, a], Xinya Sun[2, b], Wei Dong[2, c], Xiang Yan[3,d], Yindong Ji[2,e]

[1] Department of Automation, Tsinghua University, Beijing 100084, China

[2]Tsinghua National Laboratory for Information Science and Technology, Beijing 100084, China

[3]Beijing National Railway Research & Design Institute of Signal & Communication Ltd., Beijing 100070, China

[a]daixy13@mails.tsinghua.edu.cn, [b]xinyasun@tsinghua.edu.cn , [c]weidong@mail.tsinghua.edu.cn

[d]yx@crscd.com.cn, [e]jyd@mail.tsinghua.edu.cn

Keywords: M out of N; Redundant System; Safety; Reliability;

Abstract. This paper designs an M out of N Safety Computing System based on general-purpose computers. The system consists of some computational nodes and a comparator. For the synchronization among the computational nodes, task synchronization was applied. The comparator designed based on the FPGA is implemented in the system. Test results shows that the safety and reliability of the M out of N Safety Computing System can meet the requirements of SIL4.

Introduction

With the development of the high-speed railway in China, the speed of the train is increasing, the safe problem came to the front of the people. The Train Control System plays an important role in the safe operation of the train. As the core of the Train Control System, it is necessary to design a high safe and reliable Safety Computing System. Currently existing systems are designed based on special-purpose computers, like hot standby system[1], 2 out of 3 system[2], and double 2 out of 2 system[3]. Not only they cost a lot, but also they are difficult to maintain. What's more, the existing systems which are lacking in data processing ability fail to meet the requirement of the high-speed railway, because they are limited by the clock synchronization of computational nodes. This paper, aiming at the shortcomings of the existing Safety Computing Systems, designs and implements an M out of N Safety Computing System based on general-purpose computers, by using task synchronization.

The Architecture of the M out of N Safety Computing System

The M out of N Safety Computing System consists of some computational nodes and a comparator. Its overall structure is shown in Fig.1. The resource pool of the computational nodes is mainly responsible for providing the computational nodes, and the computational nodes handle the data on the basis of the data processing logic. The comparator is mainly responsible for data distribution, computational nodes scheduling, and output decision.

The Resource Pool of Computational Nodes. The resource pool of computational nodes integrate server resources using virtualization technology for the use of the upper virtual machine on the basis of multiple servers, and the servers transfer data through the outside world by Ethernet. As each server contains more than one virtual machine and each virtual machine corresponds to a computational node in the M out of N Safety Computing System, this article uses the bridge network model to solve the problem of computational node virtual LAN network address assignment, for the purpose of ensuring each computational node independently establish connection with the comparator. The bridge network model is to bridge the virtual network adapter and the physical adapter by the VMnet0 virtual switch of the VMWare Workstation, so as to put the virtual network adapter and the physical adapter at the same position in the network topology, which is to say the virtual network adapter and the physical adapter have the same gateway. Through the use of the bridge network model, each computational node acts as

one independent computer with a separate IP address, meanwhile, each computational node and server stay on the same gateway, which is convenient for the supervision and management of the comparator.

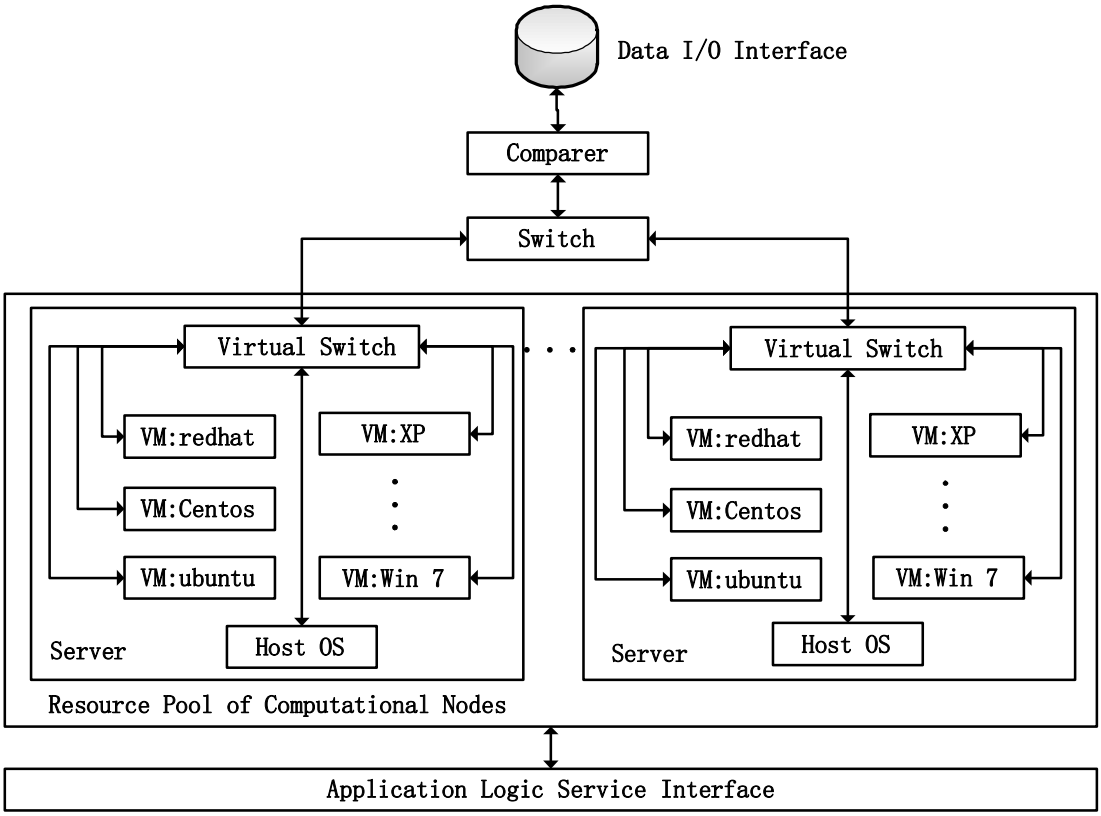

Fig.1 The Structure of M out of N Safety Computing System

The Comparator. The comparator output the calculation results decision, so its failure will seriously affect the safety and reliability of the M out of N Safety Computing System. To decrease the probability of the failure and improve the safety and reliability of the M out of N Safety Computing System, this article designs the comparator based on the XILINX SPARTAN-6 series XC6SLX16-2 csg324 FPGA chip, and builds a system on the basis of The MicroBlaze IPCore in the chip in order to implement the key functions of the comparator. The underlying hardware structure of the comparator is shown in Fig.2.

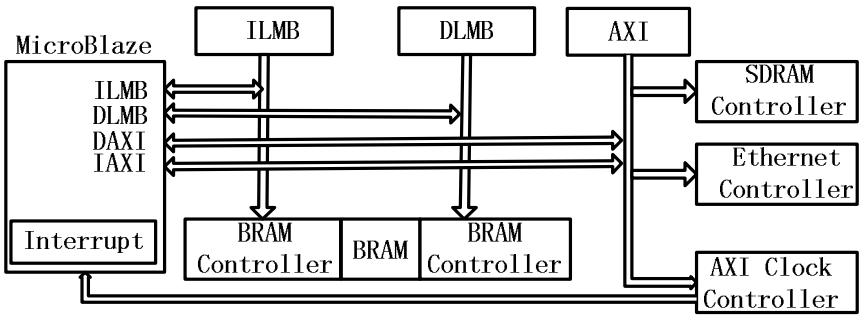

Fig.2 the Underlying Hardware of the Comparator

MicroBlaze IPCore connects BRAM (Block RAM) through LMB (Local Memory Bus). The ILMB is used to transfer instruction and DLMB is used to transfer data. It would decrease the efficiency of LMB if overload. So this paper extend memory through external DDR, realize reading and writing by connecting AXI bus and SDRAM controller. It would be helpful to reduce the LMB bus load and promote the running efficiency of the comparator for large program to run on the DDR. And MicroBlaze connects with the Ethernet controller using the AXI bus in order to ensure the data interaction between the comparator and the outside.

The Main Function of the M out of N Safety Computing Platform

The main function of the M out of N Safe Computing System including computational nodes synchronization function, the calculation results decision function and data processing logic setting function. The article will elaborate the above function.

The Computational Nodes Synchronization Function. It is required that the input and output always remain the same when making the M out of N decision from the computing results for the system. So the synchronization of computational nodes is the foundation of making decision. Recently, clock synchronization, fixed cycle synchronization and task synchronization is widely used. Based on the requirement of the performance of the M out of N Safety Computing System, this paper synchronize the computational nodes through task synchronization, and the detail of the strategy is described as below. Assume that the serial numbers for the participating computational nodes are 1 to N. After the connection is established successfully, the comparator distributed data to the non-fault computational nodes. When firstly receiving the signal of the successful reception of the data, the comparator will begin to time. The computational node, which not returning the signal of successfully receiving the data within the prescribed time, would be seen as a failure and be interrupted, and its final decision output would be empty. After distributing the data, the comparator would send synchronous signal and the computational nodes will started to run. From the time that the comparator firstly receiving the output to the prescribed delay time, the computational node, which not returning the result would be thought as a failure and be interrupted, and its final decision output would be empty. It is in this way that ensuring the task of computing nodes would start and end at the same time so that achieving the result of task synchronization.

The Calculation Results Decision Function. The M out of N Safety Computing System makes a decision based on the results that come back from the computational nodes. If the number of the same results is equal or bigger than M, then output the result. Otherwise output the fault signal. The specific process of the decision is shown in Fig.3.

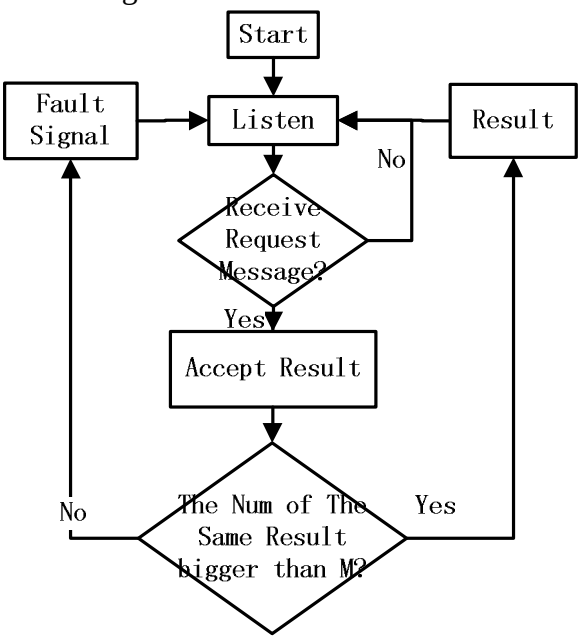

Fig.3 the Detail Process of Decision

The process of decision is shown in Fig.3. This paper uses Moore's Voting Algorithm[4] to achieve the results of the comparison and decision. The specific process of the Algorithm is shown in Fig.4.

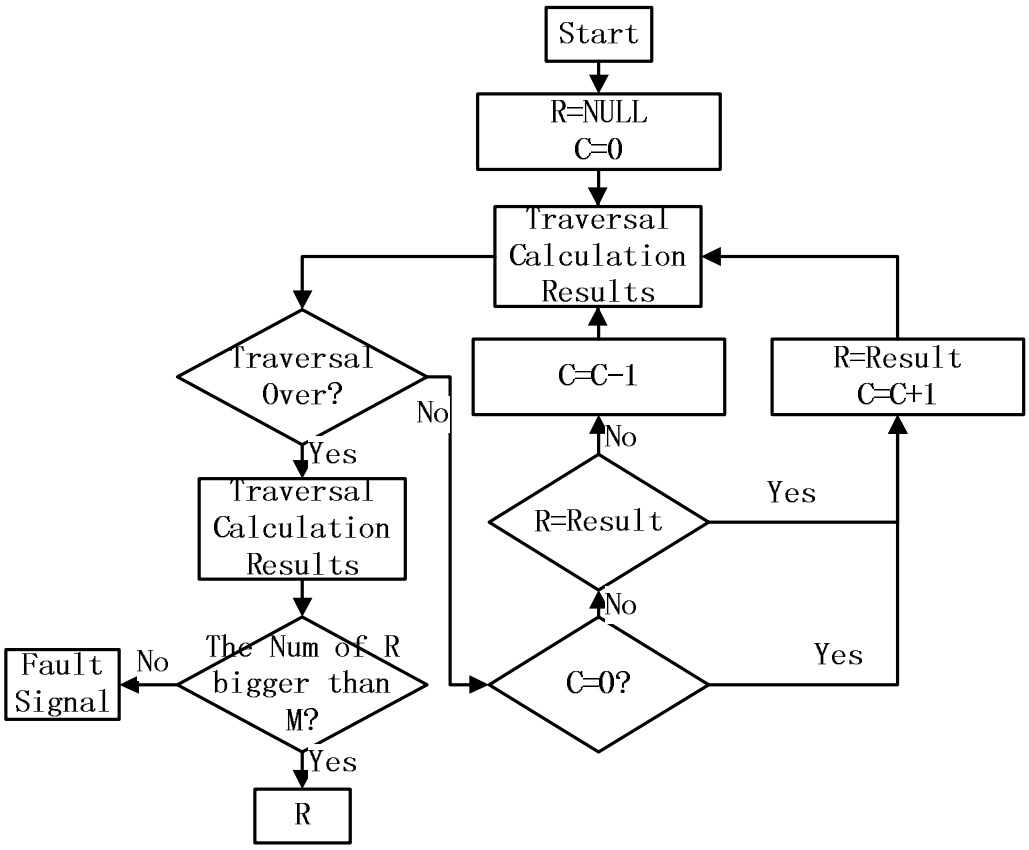

Fig.4 the Detail Process of The Moore's Voting Algorithm

Firstly, setting the output R to null and its frequency of occurrence C is 0. Secondly, scanning the whole results queue in turn. If not arriving at the end of the queue, determining whether C is 0. If C is 0 resetting R to the current result and C=C+1, otherwise, we need to determine whether the current result equals R. If the current result equals R then C=C+1, or C=C-1. Thirdly, scanning the results queue to see the frequency of occurrence of R. If it is equal or greater than M then the output is R or as a failure. It is easy to see that the strategy of Moore's Voting would get the final decision output after scanning the results queue twice, so the time complexity of algorithm is O(n) and the space complexity is O(1).

The Data Processing Logic Setting Function.

The M out N Safety Computing System provides user the corresponding service unit for the convenience of user to formulate different data processing logic for each task. Users can derive the corresponding task processing subclasses according to the provided service interface base class, and realize the data processing logic function according to the corresponding task processing logic. The main functions and relating parameters of the service interface base class using in this article are shown in Table.1:

Table.1 the Service Interface Base Class

Name of function	Parameter of function	result
double[] data_process(double[] data)	data: data to be processed	data processing results

As is shown in Table.1, the user only need to implement the data processing logic based on the base class. Then the computational nodes could do the task on the basis of the data processing logic which was implemented by the user. Fig.5 shows the process of the data processing.

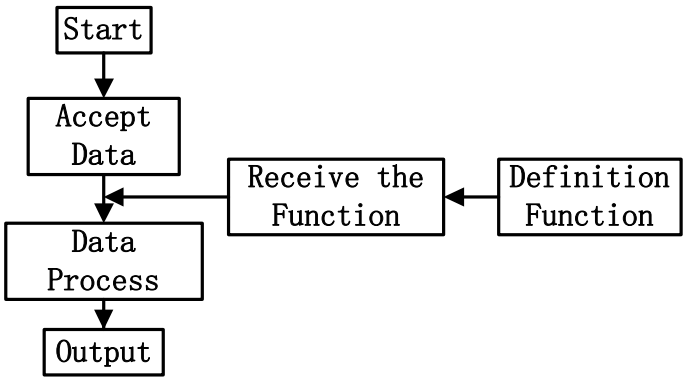

Fig.5 the process of data processing

As is shown in Fig.5, the computational nodes use the data processing function according to the name of the data processing class. It is convenient for user to derive the corresponding task processing subclasses according to the provided service interface base class, and implement the data processing logic function according to the corresponding task processing logic.

Analyzing The Safety Integrity of The M out of N Safety Computing System

We have analyzed the safety integrity of the M out of N Safety Computing System based on the Markov Process in the paper which has been accept by the ITNEC 2016. It proves that the safety and reliability of the M out of N Safety Computing System is able to meet the requirement of the SIL4 (Safety Integrity Level 4). The results of the simulation test are shown in Fig.6 and Fig.7.

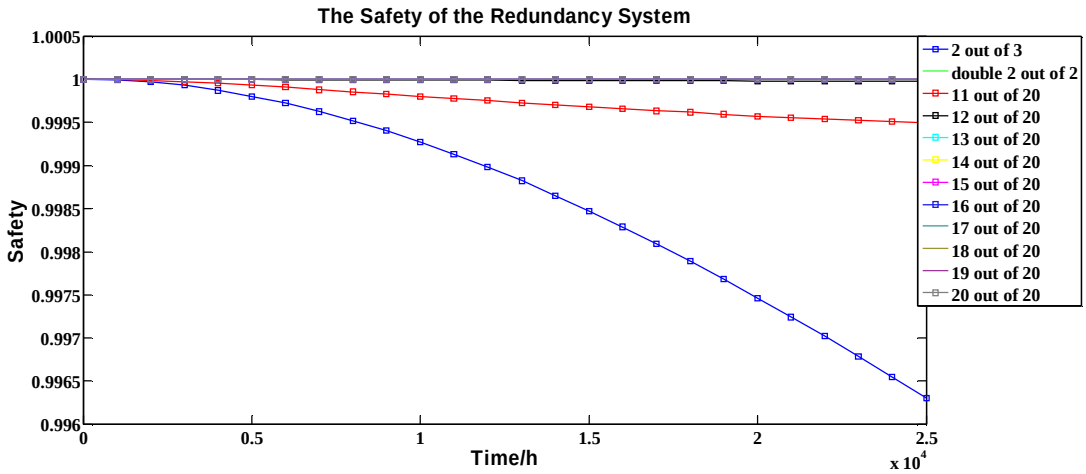

Fig.6 the Safety of the Redundancy System

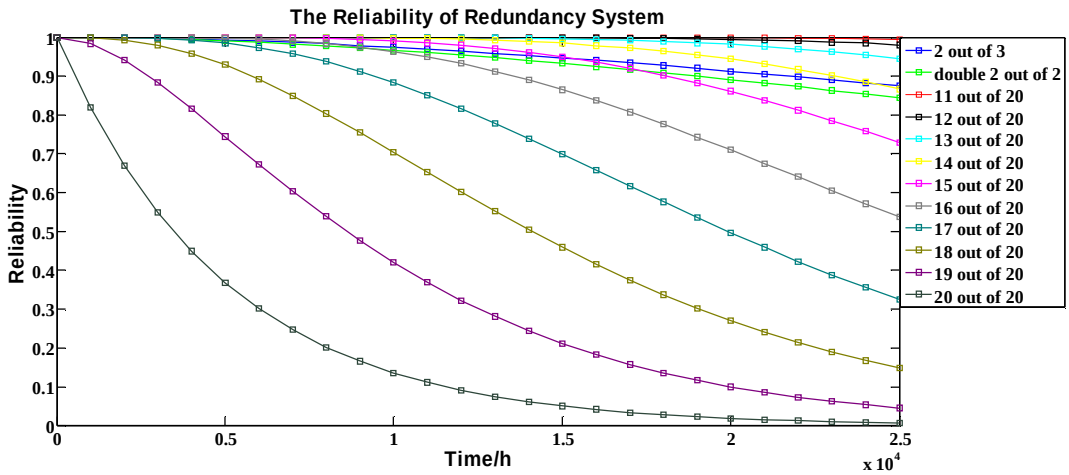

Fig.7 the Reliability of the Redundancy System

Fig.6 shows that when the M is bigger than 11 (the red line), the safety of the M out of N Safety Computing System is higher than the 2 out of 3 system. It also shows that the bigger the M is, the safer the M out of N Safety Computing System will be.

Fig.7 shows that with the increase of the M, the reliability of the M out of N Safety Computing System will decrease. When the M is less than 14, the reliability of the M out of N Safety Computing System will be higher than the reliability of the double 2 out of 2 system.

The results shows that if we select the appropriate proportion of the M and N, the safety and reliability of the M out of N Safety Computing System will be higher than the existing systems whose safety and reliability can meet the requirement of SIL4. So the safety and reliability of the M out of N Safety Computing System can meet the requirement of SIL4. In other words, the safety and reliability can meet relative requirement of the high-speed railway.

Conclusion

This paper designs and implements an M out of N Safety Computing System based on the general-purpose computers. The safety and reliability of the M out of N Safety Computing System is higher than the safety and reliability of the existing system. Meanwhile, compared with the existing systems, the M out of N Safety Computing System has a lot of advantages, such as low cost and high performance. So the M out of N Safety Computing System has broad application prospects in high-speed railway and other fields.

Acknowledgements

This work was supported by the Natural Science Foundation of China under Grants 61374123, 61490701, 61104019 and the Tsinghua University Initiative Scientific Research Program.

References

[1] Lu Y, Wang Q, Zhang B H, et al. Research on Fault-tolerant Technology for Computer System [J]. Computer Engineering, 2010, 13: 084.

[2] Huang T, Chen X X, Huang H. Safety Computer System Based on 2 out of 3 Redundant Structure [J]. Computer Engineering, 2011, 18: 087.

[3] Yi-li L. Double 2-vote-2 Computer-Based Interlocking System[J]. Computer Engineering, 2004, 30: 482-484.

[4] Boyer R S, Moore J S. MJRTY—a fast majority vote algorithm[M]. Springer Netherlands, 1991.

[5] European Committee for Electrotechnical Standardization. European standard EN50126 railway applications: The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS). 1999.

[6] European Committee for Electrotechnical Standardization. European standard EN50128 railway applications: Software for railway control and protection systems. 2001.

[7] European Committee for Electrotechnical Standardization. European standard EN50159-2 railway applications: Communication, signaling and processing systems (Safety related communication in closed transmission systems). 2001.

[8] European Committee for Electrotechnical Standardization. European standard EN50129 railway applications: safety related electronic systems for signaling. 2003.