Design of a Reliable Three-mode Redundancy Computer System

Wenjun Zhou[a], Guoqing Xu[b*], Chaowen Lei[c], Kui Liu[d], Yuxuan Huang[e]

Shanghai Institute of Aerospace Electronics Technology, Shanghai University, Shanghai, China

E-mail: [a]1547283254@qq.com, [b*]juice5.xgq@gmail.com, [c]lcwrey@qq.com, [d]liukui_804@163.com, [e]georgehuangthu@gmail.com

Abstract. Computer system is the basis of aerospace space safety. This paper proposes a three-mode redundancy computer system, which performs real-time triple modular redundancy for work tasks to improve system reliability. The three-computer fault-tolerant system includes processor management software and voting software, and realizes the three-computer architecture through three sets of independent hardware environments. In order to meet the requirements of aerospace, this paper compares the three-computer fault-tolerant system with the traditional dual-computer system on the satellite, and designs the system from the aspects of system architecture analysis, voting process design, redundancy and reliability prediction.

Keywords: Computer fault-tolerant system; Three-mode redundancy; Synchronization; Voting.

1 Introduction

In the field of aerospace, computer systems are mostly used for the communication and control functions of aircraft, which have high reliable control requirements while transmitting large amounts of information [1]. At present, most on-board computer systems adopt dual-computer fault-tolerant architecture [2-4]. In the case of the failure of the host computer, the backup computer can be used to take [5,6] over the function. However, for the computer system with hard real-time and high reliability control requirements, there will be problems such as work interruption and control cycle change if the dual fault-tolerant architecture is used.

In order to solve the above problems, this paper proposes a three-mode redundancy computer system, which uses three sets of independent hardware to control the internal command of a single computer, so as to realize the triple computer mode. If there is a fault in one computer, it will be degraded to dual computer mode, and if there is a fault in dual computer mode, it will be degraded to single computer mode. Time synchronization, data synchronization and multilevel voting strategies are designed to ensure reliable and efficient fault-tolerant system environment.

© The Author(s) 2023
C. Chen et al. (eds.), *Proceedings of the 3rd International Conference on Digital Economy and Computer Application (DECA 2023)*, Atlantis Highlights in Computer Sciences 17,
https://doi.org/10.2991/978-94-6463-304-7_70

2 Design of three-computer fault-tolerant system

The typical on-board computer in the aerospace field uses a dual-computer backup system to meet the safety and reliability design requirements of satellites. As shown in Figure 1, a typical dual redundant computer includes external data interface, calculation control module, data output module and execution module, and the host [7] computer and the backup computer use completely independent software and hardware for redundant backup. In order to further realize the flexible configuration of dual computers, a dual computer monitoring channel [8] is set between the main computer and the backup computer to realize the mutual monitoring of the main computer and the backup computer under the dual computer architecture, so as to achieve the requirements of autonomous control switching.

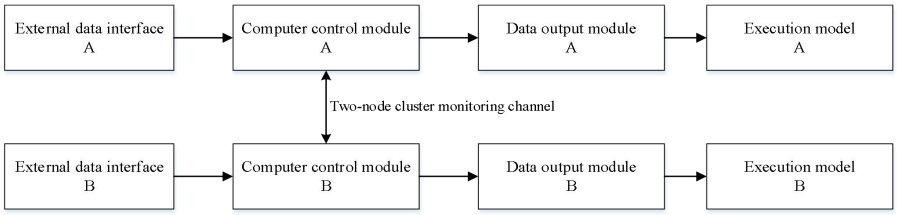

Fig. 1. Typical double redundant computer system architecture

Because the on-board control computer platform controls the satellite with high precision, three completely independent processor modules are designed for separate calculation control, and the voting module is used for instruction voting and data output. The double redundant system architecture is used in the execution module to be compatible with the cold condition of the main and backup of the traditional on-board computer. Each voting module makes independent judgment on the current working mode, and carries out computer instruction control according to the working mode.

The three-mode redundancy computer system is composed of processor module, voting module and execution module, and its system structure is shown in Figure 2.

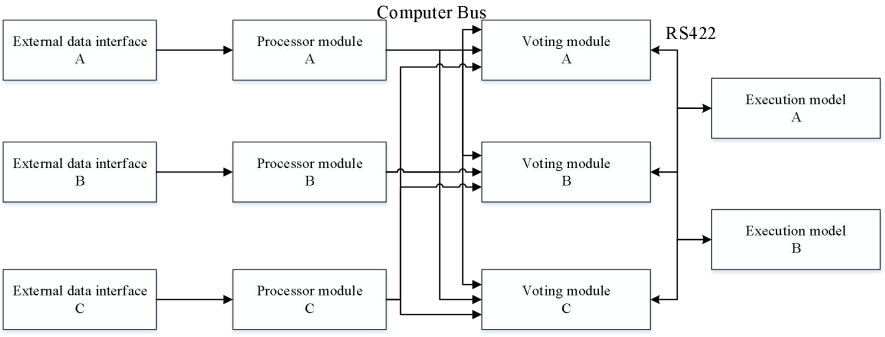

Fig. 2. Structure diagram of the three-machine system for the Promote Integrated Manager

It can be seen from the Fig.2 that each voting module can receive three identical data issued by processor A, processor B and processor C. For example, when CPUA writes vote A, it will write to the voting FPGA circuits B and C at the same time. The voting module votes on the current mode, and specifies the authority machine to send instructions to the execution module to achieve reliable control of the three computers. When an unrecoverable fault occurs in the manager, the corresponding voting module of the three machines can judge the fault machine independently, and prohibit the machine from sending downward instructions, and determine that the system working mode is degraded at this time.

In order to reduce the change of single machine fault mode, our system is designed as an asymmetric structure [9,10], as shown in Figure 3, so there are only three possible dual machine modes, namely "A main B standby", "A main C standby", "B main C standby". In this case, if any of the two machines fail, the hardware of the three machines can be judged to enter the fault degradation, and the system enters the single machine working mode.

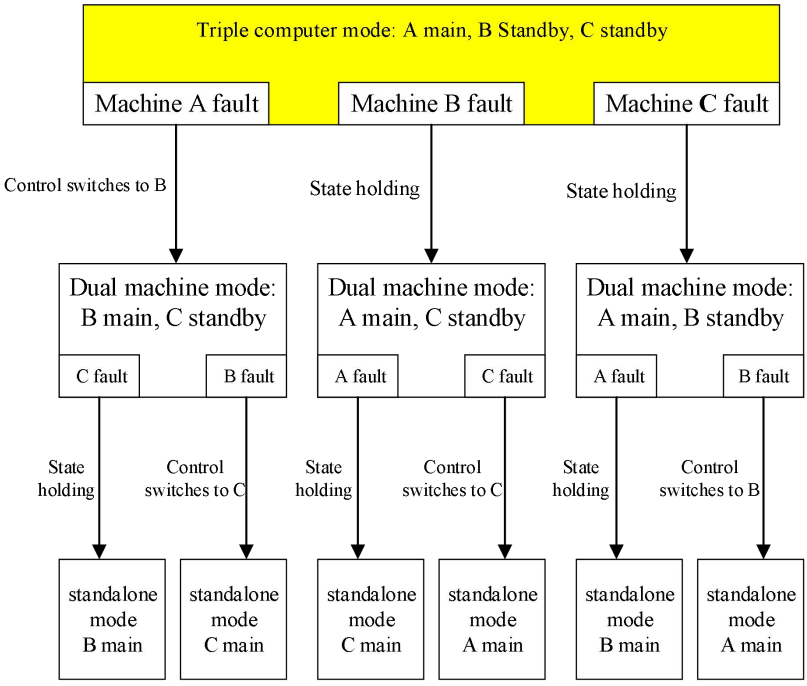

Fig. 3. Three-machine system operation mode

3 Three-machine system operation mode

3.1 Time synchronization of three machines

The synchronization mechanism is mainly used to eliminate the asynchronous degree caused by different clocks or delays among different CPUs in the triple modular redundancy system, so that the three CPUs in the system reach a relatively consistent state in the program execution state, cycle timing and time reference, so as to ensure the synchronization of input data and output data of the three CPUs. So that the voting module FPGA can carry out synchronous voting, ensure the consistency of the comparison data, and truly complete the function of triple modular redundancy.

As shown in Figure 4, each voting module generates a synchronization pulse and sends it to three processor modules at the same time. Each processor module uses its own time to monitor the quality of the synchronization pulse. By default, the synchronization pulse emitted by the voting module corresponding to the power machine is selected as the synchronization interrupt clock source. When the synchronization pulse has pulse width deviation, the synchronization pulse source switch is carried out.

The three CPUs use the same synchronization pulse to trigger the interrupt, so that the three CPUs work under the uniform synchronization pulse drive, so as to have the basis of synchronous operation.

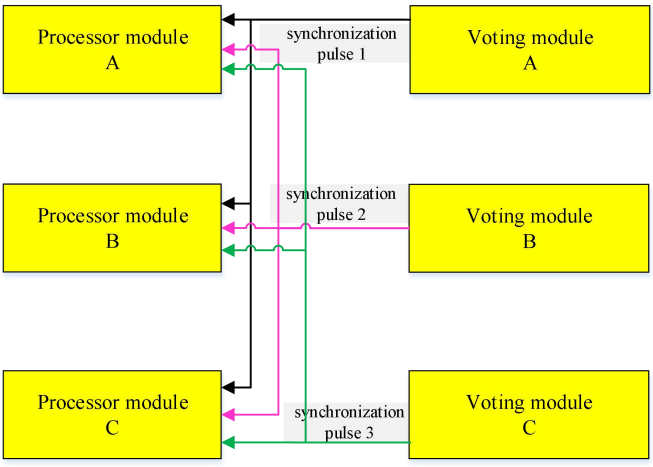

Fig. 4. Time synchronization method

3.2 Data synchronization of three machines

The three-mode redundancy computer system uses the architecture of triple modular redundancy, and the computing function of each computer is independent. The data synchronization of the three computers can realize the communication between the three independent processors.

The three computers communicate with each other to realize:

- The CPU business data of the three machines are exchanged, and the interaction results are used to unify the task states of the three machines.
- The interaction of CPU instruction status data of the three machines, and the interaction results are used to vote instructions and vote the current working status of the three machines;

The CPU realizes the data interaction of the three computers through the interactive RAM of the voting module. The CPU realizes the triple modular redundancy of data interaction by writing the interactive RAM of the three computers and reading the data of the corresponding interactive RAM of itself.

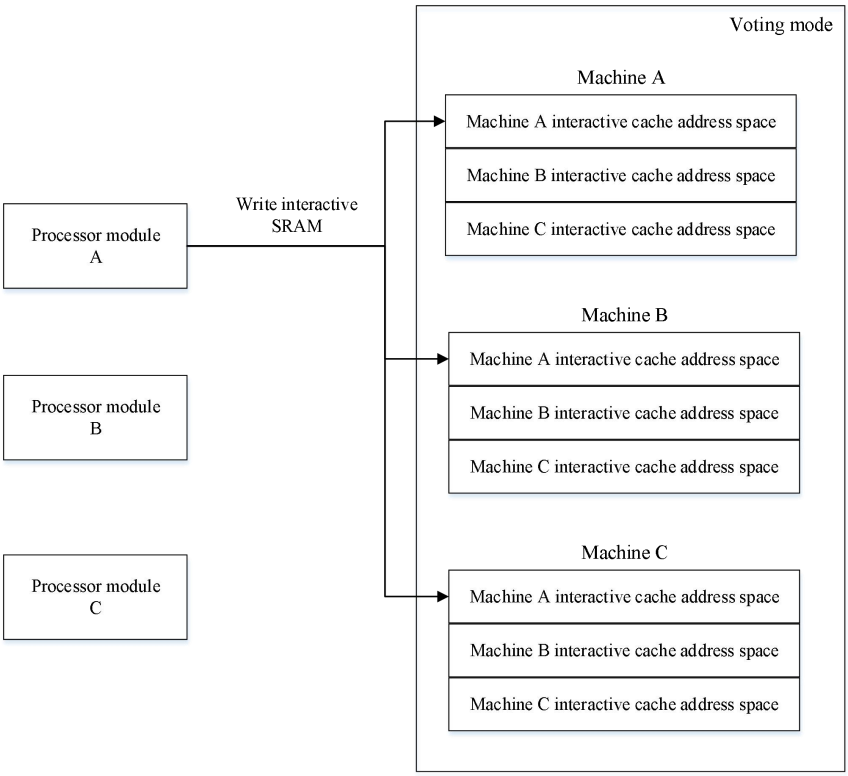

Fig. 5. Data synchronization method

4 Three-machine voting mechanism

The voting switching mechanism is the design core of the three-level fault-tolerant system. The fault detection and output control of the three-machine redundancy fault-tolerance are completed by the voting switching function. The voting process is divided into two levels:

The first level is when the CPU software is running. The CPUs of the three machines read the shared RAM of the corresponding voting module, and vote the interactive business data of the three CPUs. After voting, the data and status of the three machines are unified. The content of the first-level voting interaction mainly includes the CPU software self-test, the number of local watchdog reset, the local clock source and other information.

The second level is that after the CPU software completes the task calculation, the voting module votes on the instructions output by the three CPUs, and determines the current working mode of the three machines and the download instructions. After starting the voting, each voting module votes on the instructions from the three CPU machines. In order to obtain reliable instruction results, the instruction data are voted bit-by-bit in the form of high to low priority.

5 Simulation Verification

In order to verify the error correction ability of the three-machine system under fault conditions, this paper uses Vivado 2018.3 to simulate the propulsion integrated manager system, and injects fault modes for error correction test. As shown in Figure 6, clk_i is the 50MHz clock source selected by the three computers, and the three processors start the write voting module to enable wr_en at the same beat, and input their own data wr_dat to the voting module. After receiving the data from the three computers, the voting module performs three take two bit by bit voting, and the result is voter_tri_o.

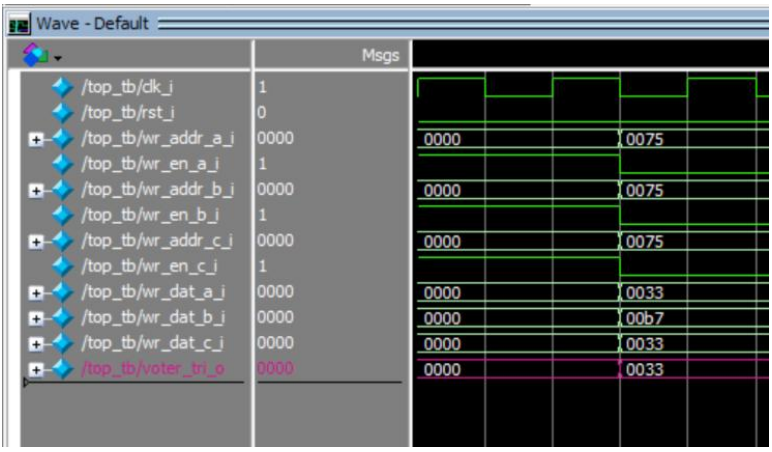

Fig. 6. Three - machine voting simulation test results

The above simulation test successfully realizes the time synchronization and data synchronization in the three-machine mode, and ensures the fault tolerance of the whole three-machine system through the three-machine voting mechanism when the failure of one machine occurs.

6 Conclusion

From the perspective of system design, this paper designs a three-machine fault-tolerant system with processor module and voting module as the core, which can realize time synchronization, data synchronization and reliable voting. The simulation test of the voting mechanism of the three machines in fault mode shows that the system can effectively realize reliable voting output under hard real-time requirements, and meet the requirements of safe and reliable control.

References

1. Chen, Junmei, Hao Chen, and Zongpeng Li. "A Double Serial Concatenated Code Using CRC-aided Error Correction for Highly Reliable Communication." Computer Networks (Amsterdam, Netherlands : 1999) 216 (2022): 109260. Web.
2. Samet, Refik. "Design and Implementation of Highly Reliable Dual-computer Systems." Computers & Security 28.7 (2009): 710-22. Web.
3. Liu, Li-jia, Dong Cao, and Yu-wei Wang. "Fault Tolerant Strategy for Master-Slave Dual Redundancy Flight Control Computer." Dianguang Yu Kongzhi = Electronics Optics & Control 7 (2017): 95. Web.
4. Jian Sun, Weifeng Gong, Xiaoshe Dong, Xingjun Zhang, and Yinfeng Wang. "High Availability Analysis and Evaluation of Heterogeneous Dual Computer Fault-tolerant System." 2014 IEEE 5th International Conference on Software Engineering and Service Science (2014): 460-64. Web.
5. "Supply Of Desk L Shape , Desk Straight Shape , High Back Chair , Medium Back Chair , Host Computer , Client Computer , Projector , Motorized Projector Screen , Online Ups With 30 Minutes Backup , Network Wire , Network Switch , Electricity Board , Main Bo." (2022): MENA Report, 2022. Web.
6. Yan Ma. [J]. "Design of Host and Backup Switching Board for Safety Computer Platform" Railway Signalling & Communication Engineering, 2020, 17(2):67-70. DOI:10.3969/j.issn.1673-4440.2020.02.012.
7. Li, Chao, Junzhi Zhang, Xiaohui Hou, Yuan Ji, Jinheng Han, Chengkun He, and Jiangmai Hao. "A Novel Double Redundant Brake-by-Wire System for High Automation Driving Safety: Design, Optimization and Experimental Validation." Actuators 10.11 (2021): 287. Web.
8. Wu, Li-Zhu, Yi-Hong Lu, Zi-Ye Zheng, and Jia-Hui Pan. "Online Real-time Sleep Staging System Based on Dual-channel EEG Signals." Jisuanji Xitong Yingyong = Computer Systems and Applications 1 (2023): 87. Web.
9. Chen, Jun, Zengxin Huang, and Dengfeng Kuang. "Optical Manipulation of Microspheres Using a Multi-axis Asymmetric Structure Beam." Zh ō ngguó J ī gu ā ng 48.24 (2021): 2413001. Web.
10. Cao, Jiazhen, Zhenmin Xu, Yao Chen, Shuangjun Li, Yue Jiang, Lele Bai, Han Yu, Hexing Li, and Zhenfeng Bian. "Tailoring the Asymmetric Structure of NH2 - UiO - 66 Metal - Organic Frameworks for Light - promoted Selective and Efficient Gold Extraction and Separation." Angewandte Chemie (International Ed.) 62.18 (2023): E202302202-N/a. Web.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.