Research on Triple-Module Redundancy Computer with Reconfigurable Capacity

Yukun Chen, Jiangkang Wang, Dezhi Zhang, Gang Rong, and Yanchen Zhao

Abstract On-board computer system is the crucial component in spacecraft electronic system, and redundancy techniques can provide high reliability for on-board computer running. To ensure computer still work normally under fault condition, system architecture, principle and key technology of traditional and degraded triple-module redundancy computer were introduced. Some methods were adopted in order to reliably detect fault computer, on-board computer will work degradedly only which could not be renovated. Fault computer read current computer's pointer and crucial data at the beginning of every course, and sent synchronization require to current computer at the end of the course, then presented a design scheme of reconfigurable triple-module redundancy space on-board computer and designed reconfigurable flow. The scheme can make the fault computer has the ability of recovery. Practice indicates that the reconfigurable scheme can effectively improve the reliability of space on-board computer system, and the paper has engineering application value for design and implementation of space on-board computer system with high reliability.

Keywords Redundancy · Reconfigurable · Triple-module

1 Introduction

The reliability and security of On-board computer plays an important role in spacecraft because it provides measures to control aerospace. On-board computer system in space orbit has the feature of unmaintainability except for space station. Aircraft mission may be result in fail when On-board computer system has failure. Fault tolerance technology has become a urgent topic for on-board computer system to increase reliability.

Y. Chen (✉) · J. Wang · D. Zhang · G. Rong
Beijing Institute of Astronautical Systems Engineering, Beijing 100076, China
e-mail: cyk99811@163.com

Y. Zhao
Xi'an Aerospace Propulsion Institute, Xi'an 710100, Shanxi, China

W. Wang et al. (eds.), *Communications, Signal Processing, and Systems*, Lecture Notes in Electrical Engineering 1032, https://doi.org/10.1007/978-981-99-7505-1_53

2 The Triple-Module Redundant Architecture and Strategy

The architecture of triple-module redundancy can adopt three on-board computers or more than three on-board computers, and consist of three on-board computers at least. Redundancy capacity can be enhanced through two out of three principle, and the two out of three system base on the principle of majority. The correct results can be achieved when only one compute has failure in the redundant architecture, as depicted in Fig. 1. Isolation and reconfiguration are not carried out when the system has failure [1]. The system will be disabled when more than one computer has failure.

Assume the reliability of each machine is R_M, the reliability of voter is R_V, and the reliability of system is

$$R = \left(3R_M^2 - 2R_M^3\right) \times R_V$$

The key of the architecture is how to get two out of three. Figure 2 shows the principle block diagram for two out of three algorithm.

Voter can be implemented by hardware or software methods. Hardware voter has the future of simplicity and rapidness. The voter failure will result in system output failure because voter is a single point [2]. The voter will become complex as output channels increase, then the reliability of voter will reduce. Software voting and hardware gating are introduced to solve the problem. The method increases mutual communication between systems to exchange voting message, besides the correct

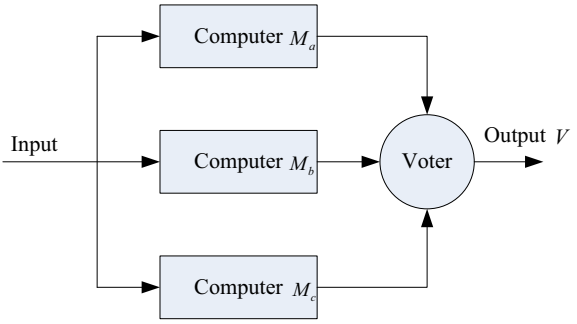

Fig. 1 The typical fault tolerance architecture of triple-module

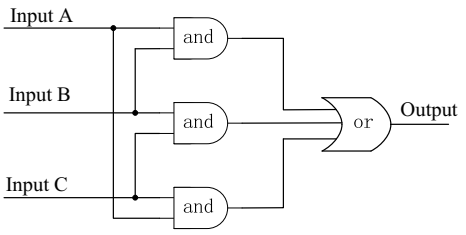

Fig. 2 The principle block diagram for two out of three algorithm

state voting strategy circuit is necessary [3]. Software voting increases time cost, and synchronization is also a indispensable problem.

3 The Triple-Module Redundant Architecture with Degraded Function

Triple-module redundant architecture is widely applied in control system. To increase system reliability and resource availability, the triple-module redundant architecture with degraded function can be presented according to system redundant strategy. Based on the design idea that triple-module computers voting when system work normally and one computer voting when system work abnormally, it can increase system reliability and enhance operating life [4]. The main feature is the architecture of triple-module, failure test and judgement is accomplished by arbitration and message exchange, and the normal computer result is the final output of whole system.

Triple-module redundant architecture with degraded function consists of three identical hardware computers running identical programme. Each computer has the same processor. The input of triple-modulecomputers is one to three, and the output is arbitration management control circuit consisted of hardware and software. Arbitration management control circuit allows that only one computer is output each time [5]. Figure 3 illustrates triple-module redundant architecture with degraded function.

Except for three identical redundant computers, the triple-module redundant architecture with degraded function has the following components and crucial technique:

(1) Communication among triple-module computers. Communication mode is full duplex by serial port.
(2) System synchronization. Synchronization has two levels, one is macroscopic period synchronization, the other is microscopic synchronization. Macroscopic synchronization is achieved by adopting unified clock frequency time circuit. The reliability of circuit has no relation with triple-module computers, and it also has redundant measures to ensure reliability. Microscopic synchronization is the synchronization in a period to ensure current computer is not influenced by the other two computers.
(3) State output. Each computer output its state message to arbitration management control circuit, then computer on duty can be present through logic judgement.
(4) Arbitration management control circuit. Basing on control instruction, arbitration management control circuit votes on duty signal through state signal. The on duty computer is system output by on duty signal.

Arbitration management control circuit releases one computer output through all state message or control instruction. Triple-module computers output state message through two out of three voting. One computer is choosing as output autonomously through triple-module computers state message, and other two computers is shut

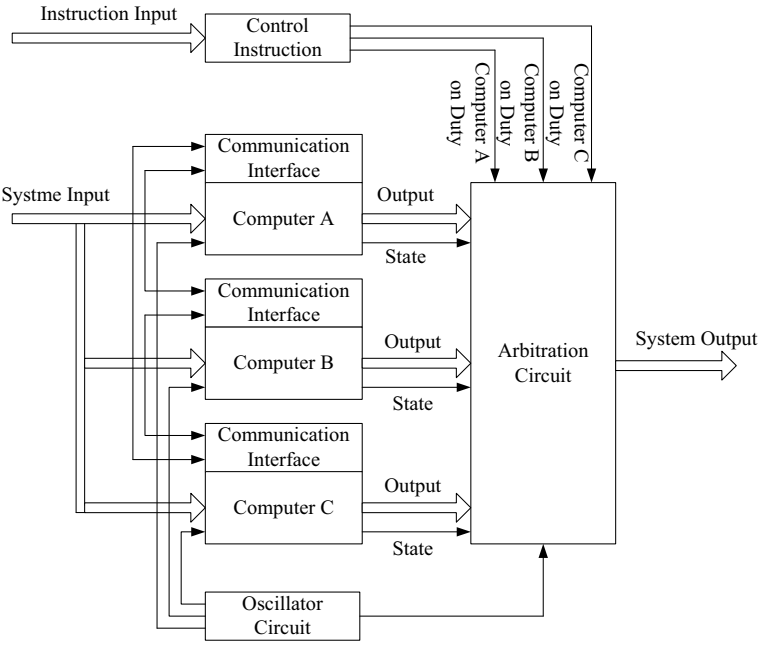

Fig. 3 The triple-module redundant architecture with degraded function

down [6]. Control instruction can also achieve the goal of releasing one computer output, at the same time the other two computers is shut down. Microprocessor on computer is responsible for data exchange among triple-module computers, and the physical link for data exchange is accomplished by serial port.

4 The Design of Triple-Module Redundancy Space On-Board Computer with Reconfigurable Capacity

Figure 3 displays that triple-module computers has the same and equal architecture, and any two computers between three computers has communication interface. To make full use of system resource, triple-module redundant architecture should not only degrade to one computer under definite conditions. System configuration can be achieved through adopting some strategy to recover fault computer. Static redundancy can be transferred to dynamic redundancy through measures of fault detection, fault location and fault recovery, then system resume to work normally and enhance system reliability and service life further.

4.1 The Fault Detection Mechanism

The symbol of triple-module computers is respectively A computer, B computer and C computer. The input signal and output signal of triple-module computers is independent, so the fault of one computer will not influence the other computers, and the on duty computer still can achieve all functions [7]. System has not single point failure from the view of interface and function. To reliably detect fault computer, single computer can still work normally under fault condition, and control right is acquired by self inspection, commutative inspection, other inspection.

(1) Self inspection. All output signal is marked through software. The computer will send abnormal feedback if it finds abnormal output.
(2) Commutative inspection. The voting FPGA of A computer monitors the real-time heartbeat signal of B computer's voting FPGA, C computer's voting FPGA and itself. The voting FPGA of B computer monitors the real-time heartbeat signal of A computer's voting FPGA, C computer's voting FPGA and itself. The voting FPGA of C computer monitors the real-time heartbeat signal of A computer's voting FPGA, B computer's voting FPGA and itself. State signal can be exchanged among three voting FPGA. Three CPU can acquire state signal and synchronization information of the other two CPU through respective interactive buffer, so commutative inspection can be achieved among three CPU.
(3) Other inspection. Three CPU send respectively data and state parameter to dual RAM of three voting FPGA, so that they can read triple-module computers data from corresponding voting FPGA to vote based on two out of three principle, then they dispatch vote results to three voting FPGA unit. Three voting FPGA feed back to three CPU after voting again based on two out of three principle, so that they can monitor respectively CPU's state.

If one voting FPGA cannot receive corresponding CPU data, it estimate the CPU has failure and send information to the other two CPU, and the other two CPU will degrade to dual hot standby mode. Three computer's CPU monitor power state signal of the two computer. If power has failure, triple-module computer estimate one computer has fault and transfer to dual computer mode.

4.2 The Reconfigurable Design of Fault Computer

If triple-module computer estimates one computer has software failure, the normal two computer will dominate output. At the same time it send reset signal to fault computer through reset pin on the internal bus, so that fault computer CPU can be reset [8]. The normal two computer degrade to dual hot standby mode, one computer is recognized to on duty. Triple-module computers are reconfigured based on the duty computer. If the fault computer cannot recover, the CPU will shut off all the output signal of the fault compute, and triple-module computer degrade to dual hot

standby mode. Figure 4 illustrates the reconfiguration flow diagram of triple-module redundancy mode.

As depicted in Fig. 4, if one computer's hardware fault happen many times in the process of triple-module computer voting based on two out of three principle, on duty computer will shut off power and restart power to resume fault computer, at the same time, on duty computer launches dual hot standby mode according to power-off state. After fault computer resumes, the method of implementing triple-module mode is as follows: at the beginning of each process on duty computer sends PC pointer and critical parameter to voting FPGA of fault computer, and after initialization fault computer begins to read data from on duty computer and

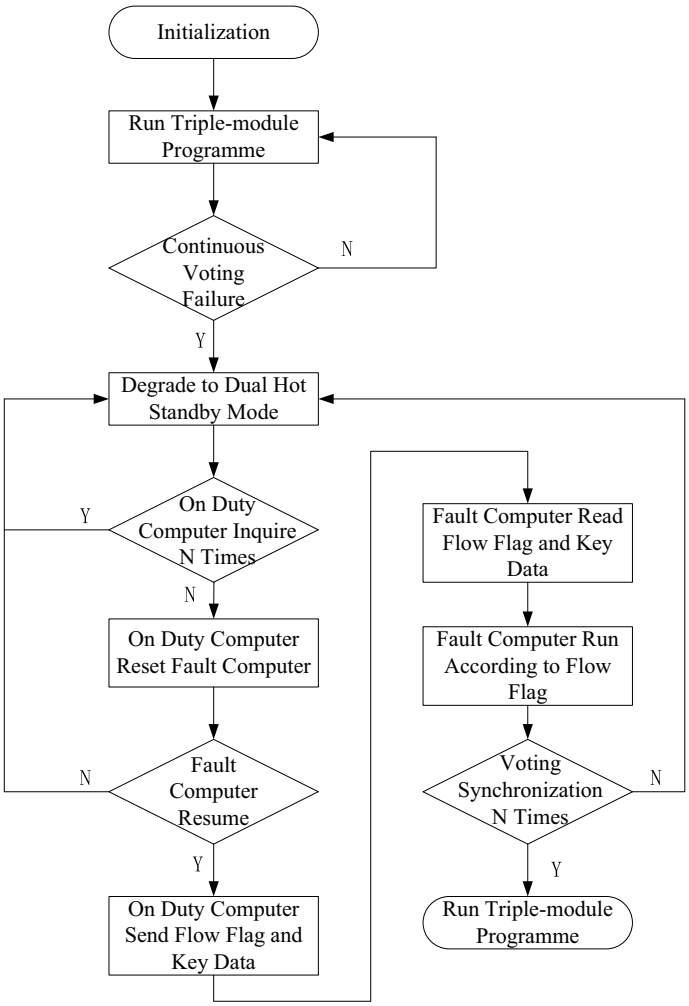

Fig. 4 The reconfiguration flow diagram of triple-module redundancy

immediately enters synchronization mode, at the same time fault computer sends operating data to voting FPGA of the other two computer. After reading on duty computer synchronization data, at the end of each process fault computer sends synchronization request to on duty computer through heartbeat monitor channel. After receiving synchronization request of fault computer, on duty computer reads data of triple-module computer and labels on data of fault computer, then it votes based on two out of three principle. If voting has the same result, on duty computer sends resumed triple-module synchronization signal through heartbeat signal, and it recovers triple-module computer mode.

When on duty computer has failure during dual hot standby, control right can be switched between dual on-board computer through remote control and switching autonomously [9]. When flight control centre estimates that current computer has failure according to telemetry data, control right can be switched between dual redundant computer by remote control command. When remote control mode takes into effect, autonomous switching is shut down, then output of the dual redundant is determined only by remote command. To shut down autonomous switching, permitting or forbidden time window of autonomous switching is set by remote command. Only when aircraft is in autonomous switching state, autonomous switching is permitted for on-board computer. In autonomous switching state, backup will take into effect when host has failure. Autonomous switching right is achieved by integral circuit to avoid accomplishing only by a piece of command. Switching command must be sent continuously many times, a certain level of integral circuit must be achieved to drive relay switching, and then backup computer will be on duty.

5 Conclusions

The reliability and security of on-board computer is the key component for aircraft. The paper displayed architecture of triple-module fault-tolerant computer system with degraded function, and introduced a design method of triple-module redundancy on-board computer with reconfigurable capacity, finally presented dynamic recovery flow diagram. Practice indicates that the triple-module computer with reconfigurable capacity can effectively enhance the reliability of space on-board computer system. The measure has engineering application value for design and implementation of space on-board computer system with high reliability under space harsh environment.

References

1. Yang M, Hua G, Feng Y (2014) Fault tolerance techniques for spacecraft control computer. National Defense Industry Press, Beijing
2. Duan Y, Wang J, Sun L (2022) Redundancy and fault-tolerant design of atmospheric data for UAV autonomous flight. J Proj Rocket Missiles Guid 42(6):75–78

3. Sun X, Chen Z, Gu Y (2018) Research on fault-tolerant flight control computer system based on dynamic reconfiguration. J Syst Simul 30(10):3957–3963
4. Wang Z, Wang M, An S (2022) Design and implementation of a fault-tolerant computer with 2×2 architecture. Ind Control Comput 25(5):44–45
5. Wang J, Wang S, Wang X (2018) Fault mode probability factor based fault-tolerant control for dissimilar redundant actuation system. Chin J Aeronaut 31(5):965–975
6. Zhang Z, Du J, Fan C (2021) The redundancy management in redundant fly control computer of launch vehicle. Flight Control Detect 4(3):48–56
7. Wang Z, Cheng S, Ma X (2020) Design and implementation of highly reliable fault-tolerant computer with integrated multi-task. Aeronaut Comput Techn 50(4):110–112
8. Lv Y (2020) A fault-tolerant method for space computer memory with low-cost and high-reliability. Aerosp Control Appl 46(3):66–70
9. Jiang B, Zhang K, Yang H (2021) Fault-tolerant control of satellite attitude control systems. Acta Aeronaut Astronaut Sin 42(11):524662