Design and Application of Fault-Tolerant On-Board Computer System with High Reliability

Yukun Chen(✉), Dezhi Zhang, Gang Rong, Xu Wang, and Feng Qiu

China Academy of Launch Vehicle Technology, Beijing 100076, China

Abstract. On-board computer system has a significant role in spacecraft electronic system, and its reliability is especially essential to achieve final mission. In order to still work normally when on-board computer has failure, system architecture, switch method and estimation rule were introduced. On the basis of preserving the state signal between main computer and switch circuit, the state signal between backup computer and switch circuit, and the additional state signal between main computer and backup computer was adopted, then presented a modified independence switch method. By using modified independence switch method, independence switch function still worked normally when independence switch module had failure. Comparator was implemented by adopting software vote and software switch approach, and it could eliminate hardware comparator's key failure. Results indicated that the redundant technology could effectively improve the reliability of space on-board computer system. The scheme has engineering application value for design and application of space on-board computer system with high reliability.

Keywords: Dual Redundancy · Fault-tolerance · On-board Reliability

1 Introduction

With the development of aerospace technique, the spacecraft reliability and security must meet the needs of task. On-board computer system under space atmosphere is influenced by plasma, energetic charged particles, earth magnetic field, solar electromagnetic radiation, meteoroid, and so on, which will degrade performance. On-board computer system in space orbit has the feature of unmaintainability except for space station [1]. Aircraft mission may fail when On-board computer system has failure. Fault tolerance technology has become a urgent topic for on-board computer system to increase reliability.

2 The Dual Redundant Hardware Architecture and Switching Strategy

Backup fault tolerance architecture is common means for fault tolerance system architecture. It has four types, includes cold standby, warm standby, hot standby and duplex mode [2]. Redundancy will increase additional costs. According to performance and reliability, on-board computer system adopts multiple scheme based on flight sequence.

Q. Liang et al. (Eds.): CSPS 2022, LNEE 872, pp. 297–304, 2023.
https://doi.org/10.1007/978-981-99-2653-4_37

2.1 The Fault Tolerance Architecture of Dual Cold Standby

When aircraft is under station control or stable self-control, the scheme of one hot standby and one cold standby is appropriate to insure working life and decrease power consumption [3]. The typical fault tolerance architecture of dual cold standby includes two same sets of processor and multiple I/O, as depicted in Fig. 1. Fault tolerance module manages the switch between dual on-board computer. When host has failure, control right is transferred from host to backup. When backup also has failure while host don't recover, control right is transferred from backup to emergency module.

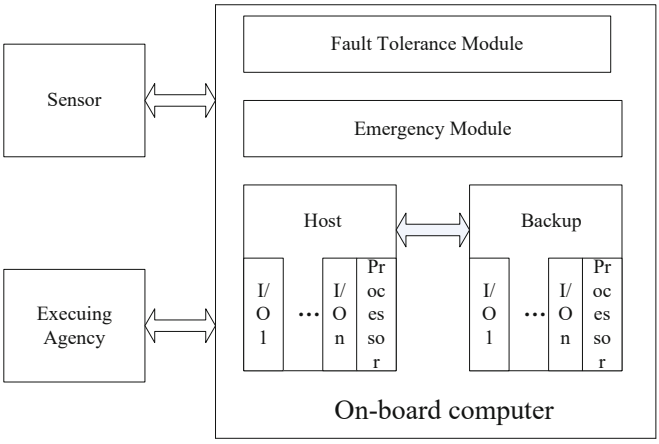

Fig. 1. The typical fault tolerance architecture of dual cold standby

Three factor should be taken into account, one is failure test, two is switch from host to backup, and finally is state recovery. Failure test is indispensable base for fault tolerance architecture of dual cold standby [4]. Failure test includes many methods, such as system self-test, program repeating, choosing two from three data sector, and watchdog technology. Majority fault can be discovered through system self-test, and the key point is that system self-test must work normally.

2.2 The Fault Tolerance Architecture of Dual Hot Standby

To insure aircraft wok normally and deal with fault quickly, on-board computer adopts the architecture of dual hot standby in initial attitude setting phase. When host has failure, control right is transferred from host to backup by commands or autonomous discrimination [5].

Host and backup both have power supply module separately. Control right can be achieved only by either host or backup at the same time. In the hot standby mode, both host and backup can accept system input signal. Processing results of the computer that has control right are chosen as system output through switching circuit. When command centre discovers a computer has severe failure and cannot work, the power supply can be shut down through remote control or autonomous switching circuit. Fault isolation

circuit deletes the computer that has failure. Closing failure computer cannot influence the other computer. Figure 2 shows the typical fault tolerance architecture of dual hot standby.

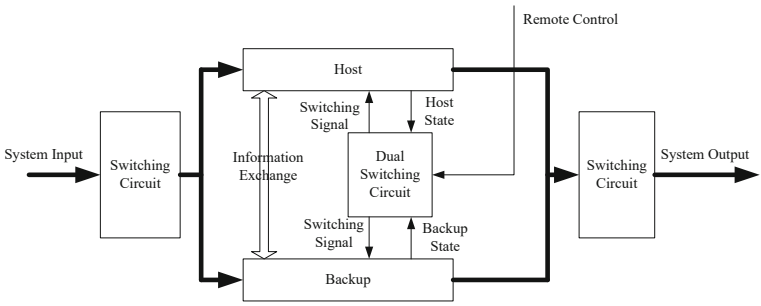

Fig. 2. The typical fault tolerance architecture of dual hot standby

Dual switching circuit is monitored by host and backup. It has timing monitor and corresponding logic circuit, designed by watchdog mechanism [6]. Dual switching circuit has two triggers. Host and backup reset corresponding trigger, but timing signal inside the dual switching circuit set two triggers. If reset signal don't appear before timing signal coming, switching signal will be generated automatically, then the computer working normally will be on duty. If host and backup are both working normally, switching signal is not generated, and host will be on duty. If host and backup are both out of work, host will be on duty, then at least there is still a guarding computer to avoid switching frequently between host and backup.

2.3 The Switching Implementation Mode Between Dual Computer

When aircraft is in the orbit, control right can be switched between dual on-board computer through remote control and switching autonomously [7]. 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.

2.4 The Modified Autonomous Switching Strategy Between Dual Computer

To avoid logic estimation failure between normal computer and faulty computer when autonomous switching module has hardware malfunction. The typical fault tolerance

architecture of dual hot standby is optimized. On the base of host state signal and backup state signal, the working state signal was presented. Autonomous switching could still be achieved if autonomous switching module has hardware failure. It can improve system redundancy. The principle was depicted as follows: host sent regularly its normal state signal to backup under regular condition, but backup could not receive normal state signal when host had failure. Backup could estimate that whether host worked normally through dual computer communication port. If backup worked normally and found failure on host, it would transmit on duty pulse to get control right. System architecture would be reconfigurable. Autonomous switching could be achieved when autonomous switching module inside dual computer switching circuit had failure, and it could tolerance a fault on autonomous switching module. Figure 3 illustrates the modified fault tolerance architecture of dual hot standby.

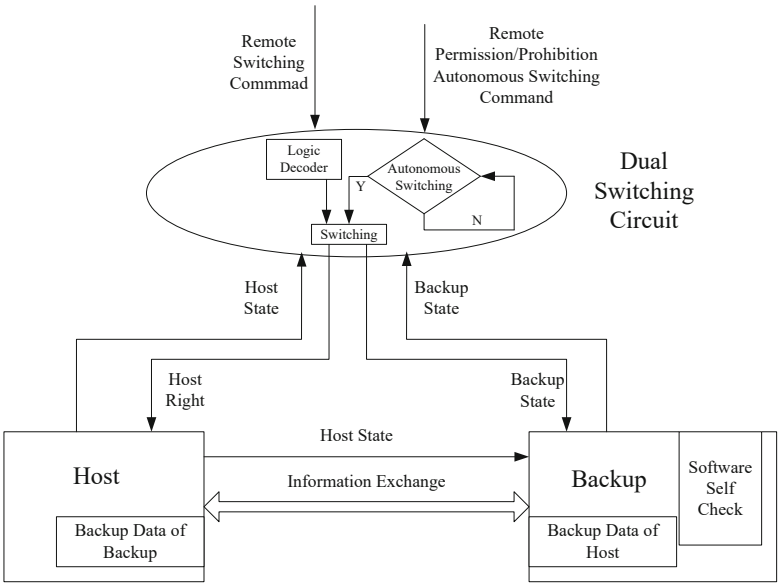

Fig. 3. The modified fault tolerance architecture of dual hot standby

There were separate cache in host and backup computer for exchanging data each other. Host sent its data to cache of backup, while backup sent its data to cache of host. Host and backup had the same component. Figure 4 shows the principle block diagram for dual computer communication.

Figure 5 displays the data flow diagram for dual computer communication. If M represents host, then N represents backup. Whereas if M represents backup, then N represents host.

3 The Design of Comparator in Dual Duplex Mode Architecture

When taking into account influence on system availability caused by success ratio and time of failure judgement, duplex system has greater availability than hot standby and

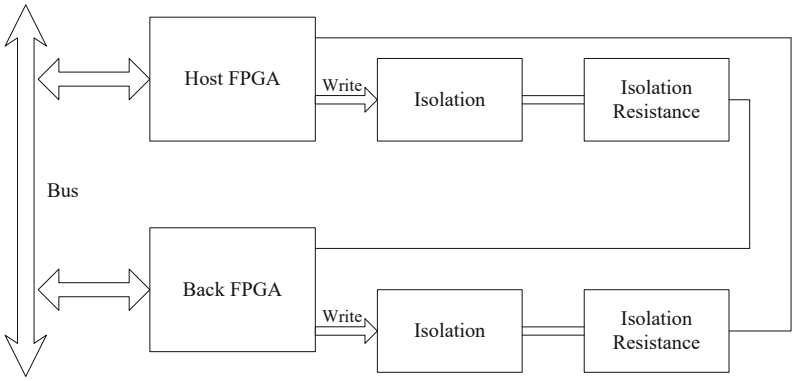

Fig. 4. The principle block diagram for dual computer communication

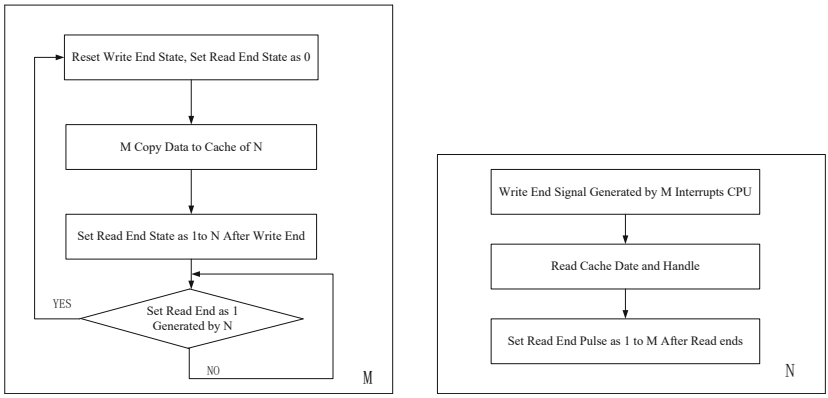

Fig. 5. The data flow diagram for dual computer communication

warm standby system under certain conditions. Besides duplex system has no switch problem, it is suitable to run under real time condition for crucial task, but it increases power consumption and has additional comparison circuit [8]. Dual duplex mode will output the comparison result of host and backup, so comparator is the crucial component for redundant system of dual duplex mode.

3.1 Hardware Design

Comparator is achieved by hardware in common redundant system of dual duplex mode. Hardware comparison module consists of comparison circuit and detection circuit executing agency [9]. Comparator adopts logic circuit for low redundancy level, and adopts independent processor system for high redundancy level. Figure 6 illustrates architecture for single comparator. If comparator has failure, it cannot generate detection signal or indicate faulty output, so the reliability of comparator becomes the new key single point for redundant system. To solve comparator's single point of failure, the problem can be relieved by increasing comparator's redundancy. Figure 7 depicts the architecture

for dual comparators. However when detection and switching circuit for multiple comparators should be introduced, hardware will become further complex. More and more redundancy will decrease the whole system reliability.

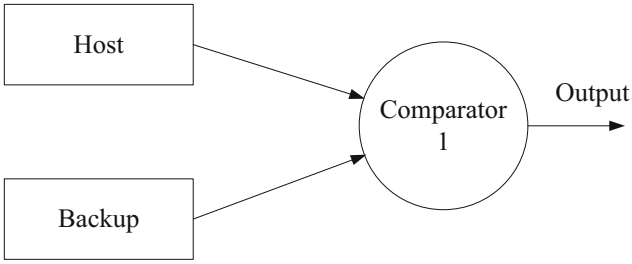

Fig. 6. The architecture for single comparator

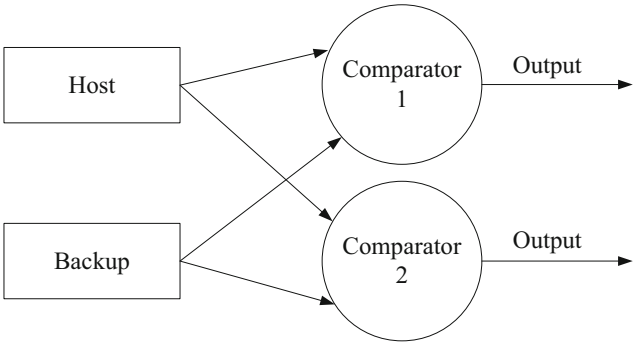

Fig. 7. The architecture for dual comparators

3.2 Software Design

To avoid comparator's disadvantage and increase reliability for real time and embedded on-board computer system, the design for solving comparator's reliability was presented. Based on the scheme of software voting and software switching, hardware unit for comparator was abandoned and comparator was implemented as software. The design was analyzed and detected as a part of system resource, which could solve the reliability problem caused by alone comparator detection, therefore the system could be optimized. From principle analysis, it was available that comparator belonged to system resource. First, comparator had less process load and simpler category, and software reliability could be guaranteed after testing, so it had low probability of leading to failure in system. On the other hand, hardware lifetime is limited according to reliability theory. Software reliability is almost invariable once put into use, so reliability of comparator can be guaranteed. Figure 8 illustrates the determination flow diagram of software for comparator.

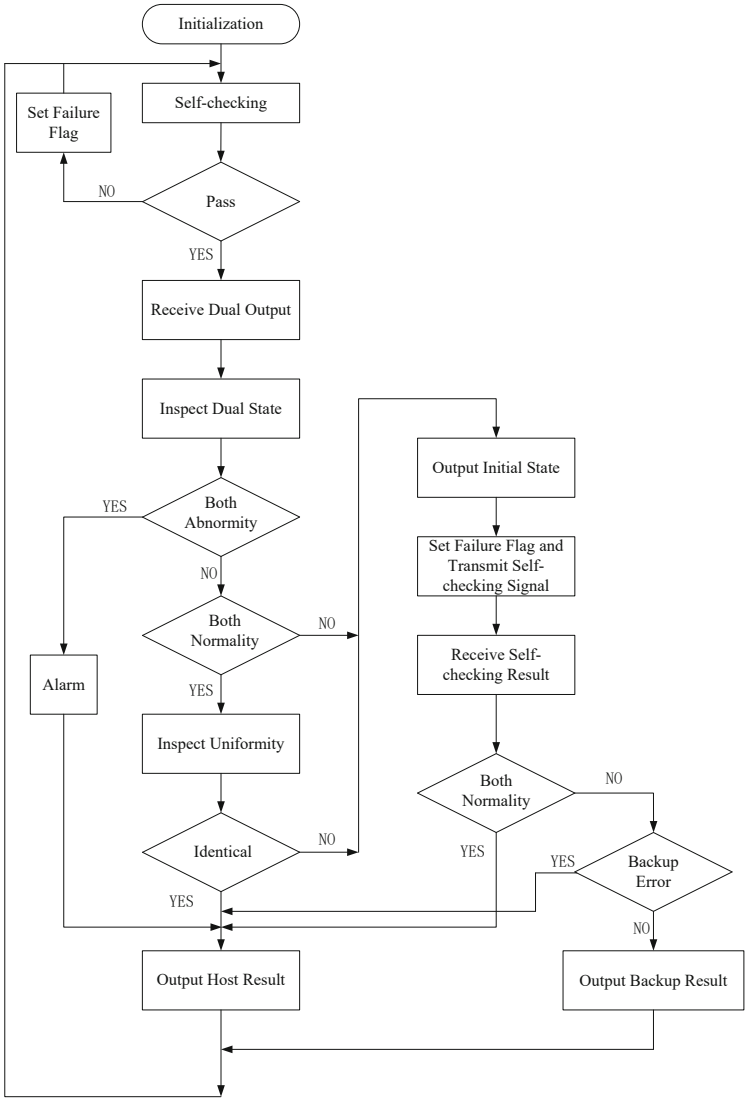

Fig. 8. The determination flow diagram of software for comparator

4 Conclusions

The reliability and security of on-board computer is the crucial topic for aircraft. The paper introduced architecture of fault-tolerant on-board computer system with redundancy function, and analyzed the dual switching strategy and determination criterion, finally presented a modified autonomous switching strategy and software suitable for comparator. Practice indicates that the redundant design improvement can effectively

enhance the performance 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.

References

1. Yang, M., Hua, G., Feng, Y.: Fault Tolerance Techniques for Spacecraft Control Computer. National Defense Industry Press, Beijing (2014)
2. Sun, X., Chen, Z., Gu, Y.: Research on fault-tolerant flight control computer system based on dynamic reconfiguration. J. Syst. Simul. **30**(10), 3957–3963 (2018)
3. Yu, Y., Wang, H.: Deep Learning-based Reentry Predictor-corrector Fault-tolerant Guidance for Hypersonic Vehicles. ACTA ARMAMENTARII **41**(4), 659–665 (2020)
4. Jiang, B., Zhang, K., Yang, H.: Fault-tolerant control of satellite attitude control systems. Acta Aeronautical et Astronautica Sinica **42**(11), 524662 (2021)
5. Wang, Y., Wen, X.: Research status and progress of fault diagnosis technology for spacecraft. Aero Weaponry **23**(5), 71–76 (2016)
6. Xu, A., Xia, D., Zheng, J.: The study of fault tolerance technical in civil aircrafts slat flap control computer. Microelectron. Comput. **32**(6), 36–40 (2015)
7. Xiao, A., Hu, M.: Reliability analysis of the computer with quad-modular redundancy byzantine fault tolerant. Aerosp. Control Appl. **40**(3), 41–46 (2014)
8. Lv, Y.: A fault-tolerant method for space computer memory with low-cost and high-reliability. Aerosp. Control Appl. **46**(3), 66–70 (2020)
9. Wang, Z., Cheng, S.F., Ma, X.B.: Design and implementation of highly reliable fault-tolerant computer with integrated multi-task. Aeronaut. Comput. Tech. **50**(4), 111–112 (2020)