Redundant Fault-tolerant Computer Structure Based On Dynamic Reconfiguration Bus

Wang Ying[1,2,a,*], Zhou Ji-qin[3,b], Zhang Wei-gong[2,3,c], Ding Li-hua[1,2,d]

[1]College of Information Engineering, Capital Normal University, Beijing, 100048, China

[2]Beijing Engineering Research Center of High Reliable Embedded System, Beijing, 100048, China

[3]Beijing Center for Mathematics and Information Interdisciplinary Sciences, Beijing, 100048, China

[a]wangyingstudio@163.com, [b]zhoujiqin@sina.com, [c]zwg771@139.com, [d]dinglihua@cnu.edu.cn

Keywords: Fault-tolerant computer; TMR; high speed serial bus; dynamic reconfiguration; UM-BUS

Abstract: Triple Modular Redundancy computer has been widely used in railway, aviation and other fields, and the structure of the standard parallel bus is adopted inside the computer, and the degradation is used in case of single machine fault. In this paper, Triple Modular Redundancy computer which is featured in internal dynamic fault-tolerant bus, standard extension and restorable degradation of the Triple Modular Redundancy computer is based on dynamic reconfigurable high speed serial bus.

Introduction

With the Triple Modular Redundancy computer widely used in the field of railway and aviation, its reliability is attached more and more importance. Usually the internal structure of TMR[1] is connected with the standard parallel bus like PCI Bus. This kind of bus is featured in rapid transmission speed, plug and play and etc., but the interface pins are relatively complex, which makes it difficult to connect within the computer units and to system-miniaturized design. Dynamic reconfigurable high speed serial bus(UM-BUS) is a new type of high speed serial and multi-lane concurrent bus which supports hot plug. Not only is data transmission rate improved by concurrent transmission with a couple of multiple serial lanes, but also dynamic reconfiguration of bus is implemented by lane health management and the mechanism of the data dynamic allocation. The UM-BUS has the characteristics of high data transmission rate and good fault-tolerance ability. Moreover, the bus interface pin is simple and small in size, which makes it convenient for the bus to extend and improve, and available for the high-reliability and miniaturized design requirements of embedded system.

Usually the process of degradation is adopted concerning the failure process in the TMR computer system. When it comes to single machine fault, the system is automatically degraded to the dual modular system or the single modular system. This system is mainly about holding the operation of the system by reducing redundancy and decreasing reliability, resulting in the fact that the reliability of keeping the system long-time running cannot be assured .

This paper proposes a kind of TMR structure fault-tolerant computer system (3+1 structure) based on dynamic reconfigurable bus. The TMR structure with the backup unit is adopted in this system, while the basic TMR structure consists of other three computer units. The backup unit used to cope with the single machine fault in the system in the form of cold backup, which keeps the system running in the basic TMR structure state. Interconnect structure based on UM-BUS[2] is adopted with the connection bus within the 3+1 structure and the expansion of the IO. High-speed transmission of the data transmission lane, the dynamic fault-tolerance of the bus, effectively improving the reliability of the system operation and avoiding permanent failure lead by the data transmission lane failure are implemented by the internal connection structure of the 3+1 structure with the UM-BUS. And the UM-BUS is used to help extend the IO function and the computer internal bus is extended towards the outside, implementing the access to the CPU external storage devices and data acquisition, which can reach the purpose of standard extension of the system bus.

UM-BUS

UM-BUS is a kind of dynamically reconfigurable multi-lane concurrent transferring high speed serial bus with which the efficient parallel transmission and the dynamically redundant fault-tolerance of the data transmission lane can be realized. The form of the nodes directly connected with each other is adopted in the bus topology and there can be 31 nodes at most. N lanes parallel transferring are supported in the UM-BUS and N-1 buses coming up with the breakdown can be fault-tolerant. The single lane rate of the bus is 200Mbps at most and it can be 6.4Gbps at most using the 32 lanes. The breakdowns can be isolated with the signals using the physical connection of the MLVDS. Farthermost transmission distance actually measured is up to 20 meters and the bus is a kind of fault-tolerant high speed serial bus. Topological structure diagram of the UM-BUS of the four lanes is shown in Fig. 1. The transmission rate is up to 800Mbps at most.

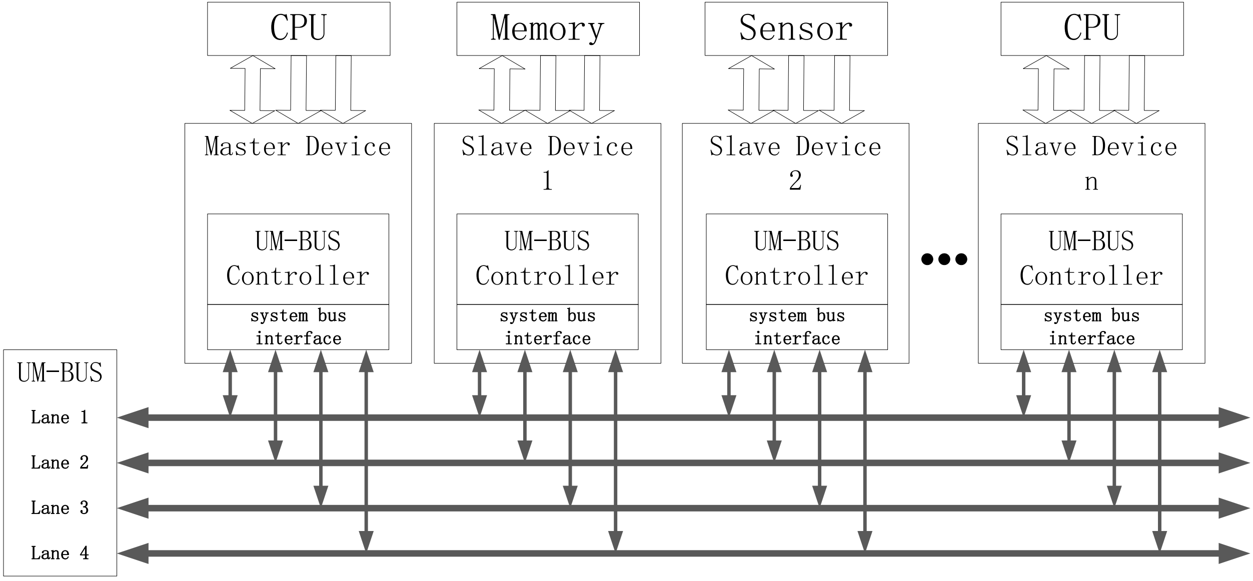

Fig. 1 The topology of UM-BUS with 4 lanes

The master-slave command response is adopted with the data communication of the UM-BUS[3] and the any communication process can only be launched by the master node and the slave node can only response to the command of the master node. This bus can support remote memory accessing and directly access the internal memory unit of the slave node. The bus defines the three kinds of the address space which is memory space, IO space and configuration space. Addressing spaces are respectively 256TB,1MB and 1KB. As is shown in Fig. 1, the UM-BUS controller of the master device is connected to the CPU through the data bus, address bus and control bus and the bus controller of the slave device is connected to the storage device, sensor device and CPU processor and other external devices, and the master devices and slave devices are connected through the UM-BUS. Hence, external devices can be connected to the local bus through the UM-BUS according to the CPU on master device through which it can access the external devices in the way of accessing the local storage units, which realizes the extension of the internal bus of the CPU and the standard extension of the bus.

N parallel lanes can be healthy-status tested by the UM-BUS bus controllers, which composes the table of information of the healthy states of the lanes. And the data waited to be transferred is distributed to all the healthy lanes averagely in bytes. When it comes up with the breakdown of the data lanes, the breakdown lane(s) will be isolated from the bus system by the bus controller and the data package can be redistributed to the other healthy lanes through the mechanism of the dynamic management, through which the dynamic grouping of the data and the dynamic redundancy of the transferring lanes can be realized. The least configuration of the UM-BUS structure can only depends on one bus controller, one bus driver and two groups of the MLVDS signal lane to realize the high speed serial data transmission of redundancy degree being one and transmission rate being 400Mbps. As is shown in Fig. 1, four transmission lanes are adopted in the UM-BUS, which makes it possible to dynamical fault-tolerance of the three data lanes breakdown. The number of the parallel lane can be set according to the actual requirements. 200Mbps can be increased after adding one group of MLVDS signal lane, which saves a lot of space for embedded system design, which is the effective solutions to the system miniaturization design. Moreover, redundancy degree of the bus can be increased after adding one group of MLVDS signal lane, which makes it possible to get the quite high reliability of the system at the least cost of the space. So it can be the fault-tolerant bus of the embedded system design.

Fault-tolerant Computer Structure Based On UM-BUS

Traditional Triple Modular Redundancy Computer Structure

Isomorphic equivalence is applied in triple modular redundancy structure[4], three computer units acquiring data, processing arithmetic operations and outputting results to the voting unit under the synchronous operation control. The three input operation results are compared by voting unit and the correct result is outputted by the principle of two out of three. Assuming that of the failure rate of each computer module is λ and the reliability is R_C, the reliability of triplication redundancy system R_T is expressed as：

$$R_T = 3R_C^2 - 2R_C^3 \tag{1}$$

And the mean time between failure(MTBF) of this system is expressed as:

$$MTBF = \frac{5}{6\lambda} \tag{2}$$

When there is a single machine fault, usually the normal computer will shut down the faulty computer, which makes the system continue to carry on under the dual modular system or single modular system. The single machine fault includes transient faults and permanent faults. The computer with transient faults usually can be controlled by system, and TMR structure can be recovered by system upgrade refactoring with the operations of restart - recognition - data recovery. Permanent faults are mainly about device failure and data transmission cable damage. The computers with permanent failures only can be degraded and then recovered by manual work, which not only has an impact on the reliability of the system but also is not advantageous to the quick recovery of reliability of the system. Above all, there exists two critical problems with the degraded system: 1)the reliability of the system is obviously below that of Triple Modular Redundancy computer system; 2) the degraded system is no longer with fault-tolerant performance.

3+1 Structure

In this paper, the designed fault-tolerant computer adopts 3+1 structure, which contains four identical CPU modules, one logic switching unit, and one voting unit. Among which, three modules compose the basic TMR structure[5], and one module is set up as the cold backup unit, which is used for the replacement of the basic TMR structure failure computer. The whole structure is shown in Fig. 3. The 3+1 structure takes the TMR structure as the core design, realizing the dynamic reconfiguration of TMR structure under the fault condition, and ensuring the reliability of the system.

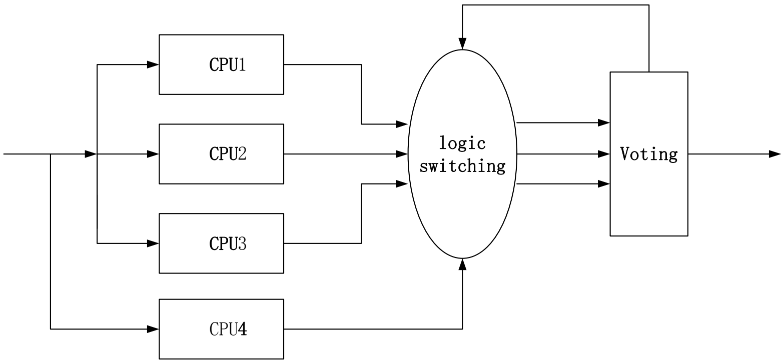

Fig. 2 3+1 structure

The advantage of fault-tolerant computer of the 3+1 structure is that it can tolerate two consecutive single machine fault. If the fault computer can be repaired and finish the self-checking, the system will working in the TMR structure for a long time. So it has obvious improve reliability compared with the traditional TMR structure. Assuming that the reliability of the backup computer is R_B and the reliability of every TMR structure is R. And also assuming that the switcher is fully reliable, so the system reliability is expressed as:

$$P_S = P_{T1}P_B + P_{T2}(1\text{-}P_B) \tag{3}$$

P_S —— The reliability of 3+1 structure
P_{T1} —— The needed reliability of the TMR structure when the backup computer is good
P_{T2} —— The needed reliability of the TMR structure when the backup computer is failure
P_B —— The reliability of backup computer

Therefore, the reliability of the normal operation system has two status: status1-The system reliability of the backup computer is normal operation and the TMR is working; status2-The system reliability of the backup computer is failure and the TMR is working. Based on the analysis given above, the system can tolerate two failure computers when the backup computer is normally working. Once the backup computer is failure, it must have two normal working computers at least in the TMR structure. So the reliability of the 3+1 structure is expressed as:

$$P_S = R\times[1-(1-R)^3]+(1-R)\times(3R^2-2R^3) \tag{4}$$

And the failure rate of every module in the system is λ and the 3+1 structure is approximately regarded as four computers parallelly working. So the MTBF of the system is expressed as:

$$MTBF = \frac{3}{4\lambda} - \frac{8}{3\lambda} + \frac{6}{2\lambda} = \frac{13}{12\lambda} \tag{5}$$

Assuming that the failure rate of single computer is 0.5%/(kh), reliability is 0.99. Compare the reliability of basic TMR structure and the 3+1 structure. As can be derived by calculating the reliability of the data shown in Table 1. It can be concluded: the reliability and MTBF are significantly higher than the basic TMR structure of fault-tolerant computer of 3+1 structure.

Table1 The reliability of two kind of TMR structure

[system structure]	[reliability]	[MTBF]
[basic TMR structure]	[0.999702]	[166666.7h]
[3+1 structure]	[0.999996]	[216666.7h]

The fault-tolerant computer application based on the UM-BUS

UM-BUS adopting plug and play is used as the data transmission lane among the three computers in the fault-tolerant computer based on the UM-BUS, and all the function modules in the system are connected with the three UM-BUS, which is shown in Fig. 3. The advantages are as follows: 1)the number of the backup computer is allowed to increase in the UM-BUS, and the fault-tolerant structure can be extended into the mode of 3+N according to the actual requirement. 2)dynamic redundancy of the N-1 the data transmission lanes of the fault-tolerant system can be realized, which can improve the reliability and fault-tolerance of the computer. 3)the external storage, sensor and etc. are designed independently and are linked into the fault-tolerant computer system by the bus controller, by which the dynamic change, increase and cut of the IO module can be realized.

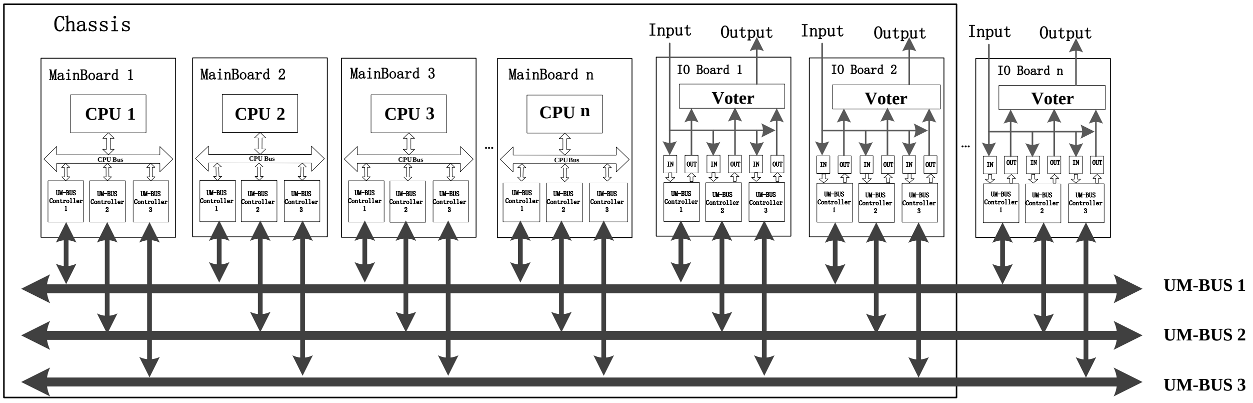

Fig. 3 The 3+1 structure based on UM-BUS

When it comes to the specific implement, each UM-BUS controllers is configured with every computer module and each UM-BUS controllers connected to a UM-BUS, and the UM-BUS controller is connected to CPU through the data bus and address bus of the CPU, and the other end is connected to MLVDS signal lane. Four groups of MLVDS signal lane are configured in each UM-BUS and the bus transfer rate is up to 800Mbps. The data can be dynamically redistributed to the healthy lanes by the bus controller when there is a breaking down on some lane(s). And three lanes breaking down can be tolerated on every bus at most, which can avoid invalidation problem resulted from lane breakdown during the data transmission.

In terms of master-slave distribution of the UM-BUS, each computer module is connected to the bus through the three bus controllers, and each bus must have one and only one master node at the same time, and the master node has to be the member of the TMR structure. With regard to the computer in TMR structure, the master node is used to send synchronous command and the data exchange command among the three computers in TMR structure and the distribute command to backup computer and another two controllers are set as slave node and are used to respond the command of the master node. As for the backup computer, the three bus controllers are all set as the slave nodes which can only be used to respond to the command of the master node of the bus.

Bus connection among the four computers are shown in Fig. 4-1. TMR structure is composed of CPU1, CPU2, CPU3 and CPU4 is the backup computer. When the CPU3 is breakdown, the CPU3 is logically replaced with CPU4. Chang the configuration of the three bus controllers in CPU4 from all slave to one master and two slaves. After being replaced, if CPU3 can be repaired, it is added to the system as the backup, and the three bus controllers are set as the three slave nodes. And the data exchange lane of the fault-tolerant system after the reconfiguration is shown in Fig. 4-2.

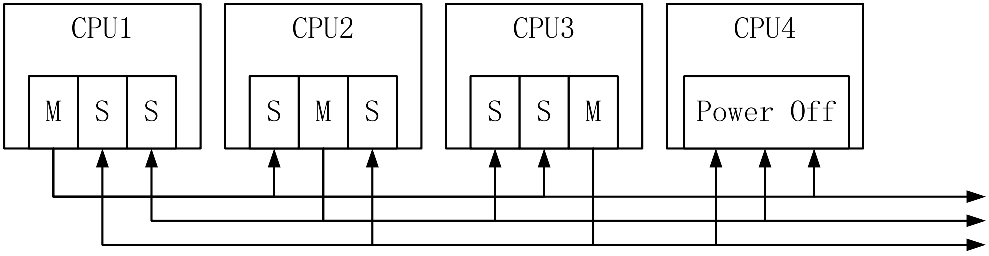

Fig. 4-1 Data exchange lanes

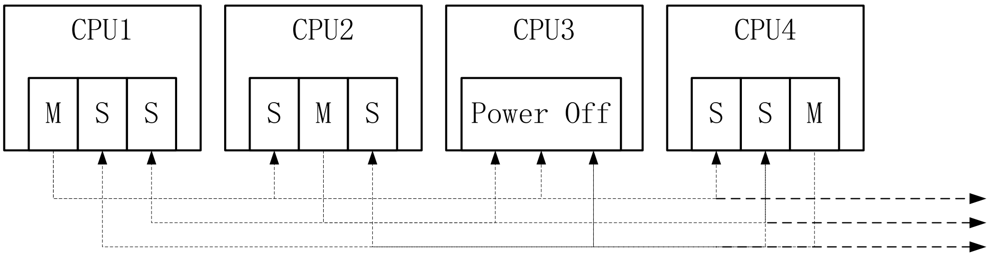

Fig. 4-2 Reconfiguration data exchange lanes

In the beginning, the basic TMR[6] structure(CPU1\2\3)is working normally while the backup computer(CPU4) is closed down. And the fault-tolerant computer is carrying on at the basic TMR structure. When the TMR[7] structure comes up with the single machine fault(like CPU1 breakdown), the breakdown computer can be identified by the logic switching unit and the power supply of the breakdown computer can be cut off, and then the system is degraded to the dual modular system (CPU2\3)for the moment. At the same time, the backup computer(CPU4)is powered up by the normal computers(CPU2\3), and the CPU4 successively executes the self test and synchronization. After the normal computers finished identify of the backup computer and the synchronization among the three computers and the data exchange, TMR structure is recovered into the CPU2\3\4. After the breakdown computer self-repaired or human-induced repaired, if it can implement the self test process, it can be added to the system as the backup computer and wait in the status of cold backup. Status switching among the four computers is shown in Fig. 5.

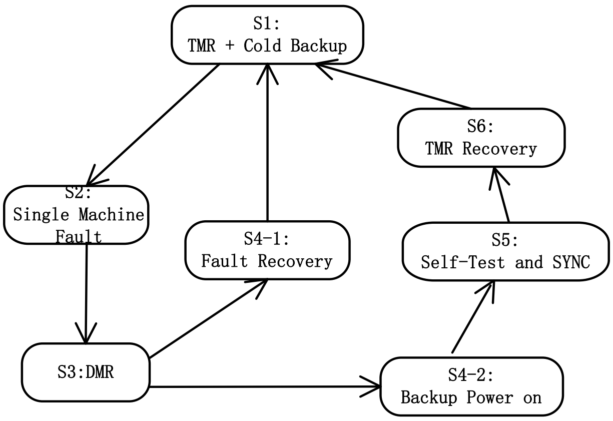

Fig. 5 Diagram of state switching among four computers

The CPU units and functional components are connected with the UM-BUS in the fault-tolerant computer system based on the UM-BUS, which not only can realize high speed data transmission, but also is able to realize the redundant fault-tolerance of the transmission lane and to enhance the reliability of the whole system. The sensor data acquisition, external-device control, memory read and write are all supported by the remote access of the UM-BUS. And external IO function unit is addressed through the bus protocol, and then is mapped to the storage space of the master node through the address translation, which is how the CPU accesses the IO devices.

Remote access of the UM-BUS makes a breakthrough that the traditional fault-tolerant system can only realize the design procedures of the module extension of the IO function inside the computer cases. According to the design of this paper, the IO board can be put inside the functional component that is needed to be measured and controlled at the remote, which makes the miniaturized design of the fault-tolerant system and the remote extension of the functional module possible. Three bus controllers are included in each IO board. And every controller which is used to response to the three master nodes in TMR structure is configured as the slave device. At most 28 IO node devices can be connected in the 3+1 structure according to the computation of node numbers which are supported by the UM-BUS. Hence, the UM-BUS is strongly featured in the IO extension and data storage operation.

Conclusions

This paper proposes a 3+1 structure fault-tolerant computer system based on UM-BUS, which focuses on the standard extension of the bus of the fault-tolerant computer system and the system reliability recovery problem after the single machine fault. With the dynamically reconfigurable UM-BUS, the system reliability is improved and especially the fault-tolerant computer with the core of TMR is more flexible in terms of function extension and remote access, which lays a good foundation for the design of the more reserve system based on the triple modular redundancy.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China (No.61170009, No.61472260, No.61402302); Beijing Natural Science Foundation of China (No.4132016, No.4143060); the Project of Construction of Innovative Teams and Teacher Career Development for Universities and Colleges Under Beijing Municipality(No.IDHT20150507); the Scientific Research Base Development Program of the Beijing Municipal Commission of Education.

References

[1] Lyons R E. The Use of Triple-modular Redundancy[J]. IBM Journal of Research and Development, 1965, 9(2): 200-209.

[2] Zhu Xiaoyan, Zhang Weigong, Wang Jianfen, Duan Qingya, and Liu Shurong, “The design of high reliable serial system BUS”. Proceedings of Computer Design and Applications, Qinhuangdao, Hebei, China, 25-27 June 2010; pp.V4-14-V4-17.

[3] Deng Zhe, Zhang Weigong, Zhu Xiaoyan. Design and Implementation of Data Transmission Management Method for Dynamic Reconfigurable Bus[J]. Computer Engineering. 2013, 39(1): 265-269. (in Chinese)

[4] Zhang Weigong, Zhang Yongxiang, Shang Yuanyuan, Guan Yong, Qiu Qinglin, Xin Mingrui. Reliability and security Analysis of Triple-module Redundancy System. Computer Engineering. 2012,38(14)

[5] Yao Rui, Wang Youren, Yu Shenglin, Chen Zewang. Design and Experiments of Enhanced Fault-Tolerant Triple-Module Redundancy Systems Capable of Online Self-Repairing. Acta Electronica Sinica. 2010,Vol.38, No.1:177-183 (in Chinese)

[6] Zhou Shuang-e, Zhou Zhonghong and Yuan Youguang. Research on Interrupt Synchronization Algorithm of Fault-tolerant Computer System[J]. Mini and Micro Computer System, Vol23(12),2002:1503~1505.

[7] C. M. Krishna and A. D. Singh, "Optimal configuration of redundant real-time systems in the face of correlated failure", IEEE Trans. Reliability, vol. 44, pp.587 -594 1995