

Research on Precise Synchronization System for Triple Modular Redundancy (TMR) Computer

Wang Meng, Yue Su-ge, Zhao Yuan-fu, Lan li-dong, and Lu Zhen-lin

Beijing Microelectronics Technology Institute, Beijing, 100076, China

Abstract: *The article presents a sound synchronization system which is composed by three synchronization modules: time-base synchronization module, period synchronization module and state synchronization module. By the principle of drag and wait, the period synchronization precision can reach 10ns. State synchronization precision and synchronization efficiency have also been greatly improved because of the fast hardware voting mechanism on FPGA and the close cooperation between hardware and software. Comprehensive fault detection mechanism also ensures the security of the TMR computer and makes the system more reliable.*

Keywords: *TMR, Reliability, Synchronization Control, Fault detection.*

1. Introduction

TMR computer, via a vote of 2 out of 3, can put out the right results in the case of a single computer module breaks down, so it can ensure the reliability of the system[1]. Because of its high reliability, there is a strong application demand in the field such as aerospace, aviation, railway and so on [2]. Synchronization technology is one of the core technologies of the TMR fault-tolerant computer. Only when synchronous, the three modules of TMR computer can get the same input signal and transfer the data to the voter at the same time, finally give the correct outputs. However, ensuring synchronization of the three modules is actually difficult because of the clock drift, input delay and so on. The situation becomes more critical as the system operating frequency increases. Synchronization precision and synchronization efficiency have become the key factors that limit the performance of TMR computer [3]. Besides, in order to enhance the TMR system reliability, sound fault-detection mechanism must be built to monitor the system failure.

2. Related Work

Many researches have been done on the synchronization of the TMR computer. The patent [4] implements synchronization of the TMR-DSP output data using a clock adjustment module which can record the periodic pulse signals and adjust the frequency and hold time of the input clock. Although it can make the clocks of each module synchronize precisely, it cannot achieve the synchronization of the executing state and the realization is complex. In the patent [5], discrete components are used to vote for the periodic clock from each processor, and give a unified interrupt, then each module responses the interrupt to achieve period synchronization. The design is simple, but the task of software is complicated which will definitely increase the synchronization time and reduce synchronization efficiency. In addition, lack of effective fault-detection mechanism will make the system difficult to detect fault and then recover from failure. The article [1] implements precise synchronization, making the synchronization precision below 30ns through dual state machine. However, it firstly use the traditional task synchronization to achieve rough synchronization, which will also reduce synchronization efficiency, and the low bandwidth will make it worse.

This article presents a new technology to implement precise synchronization. The technology sets up a sound system which is composed by three synchronization modules: time-base synchronization module, period

the difference is that period_fault signal will be given and the indication signals (p_a_fault/p_b_fault/p_c_fault) will judge out the error module. The delay unit consisted of several latches is simple and can make the delay time more accurate.

Period reload register can also be written by SPARC V8 processor through the bus. Different reload number will be written for different applications. A_fault/b_fault/c_fault signals from the fault detection module are used to monitor the failure of three modules, which makes the system more reliable.

3.3. State Synchronization Module

State synchronization ensures the three modules to work at the same pace. Processors transfer the computer data to state synchronization module and get the vote results. Data vote and fault detection are accomplished by hardware, so the process of vote can accelerate. Because of the close cooperation between hardware and software, the vote efficiency highly increases. The functional block diagram is shown in figure 3.

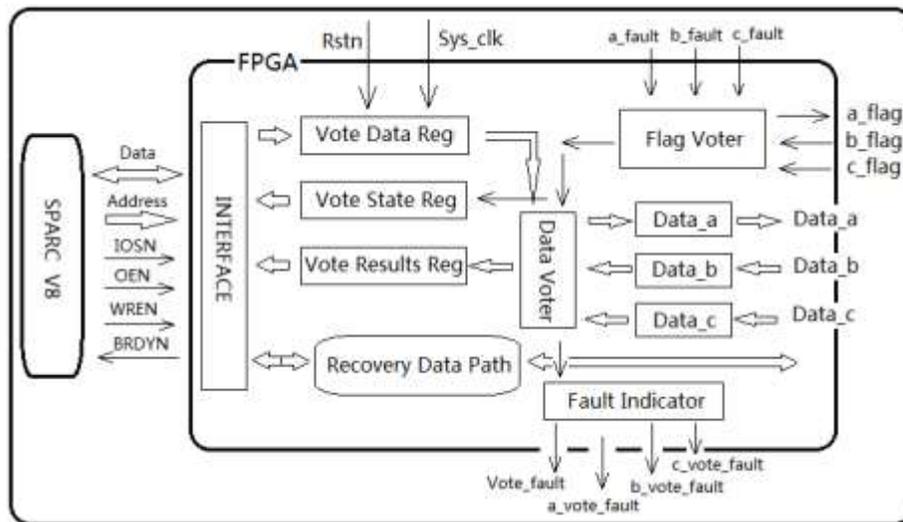


Fig. 3: Functional block diagram of state synchronization module

At the vote point, data from processor are transferred into vote data register and data_a register, and vote data-arrival signal a_flag turns active immediately. Vote data are transferred to each other through separate 16-bit-buses, so the bandwidth is high. If three data-arrival signals (a_flag/b_flag/c_flag) all arrive, data voter starts to work. Thanks to the hardware and high bandwidth, the process of vote is fast. Vote state and vote results will be read in next two read-cycles of processor. When the asynchronous degree is not too much, the time of state synchronization will only consist of one write-period and two read-periods of processor and the precision can be controlled less than one read-period.

If the data from one processor is different from the other two when voting, fault indicators are given to show that error occurs and one processor is in failure. When one module is in failure, 2 out of 3 data vote will be meaningless and state synchronization module will not be written and read. If the third data arrival signal does not arrive over two read-periods, processor will mark this and feedback the error to the fault detection unit.

4. Simulation Results

Synchronization module is implemented in FPGA BQV300 designed by Beijing Microelectronics Technology Institute. The system frequency is 100MHz. Synthesis tool is XST and simulation tool is Isim. The language is Verilog HDL. Simulation results are shown as follows. The output will be same when detecting the same inputs for the three computer modules, so we just show the simulation results of one computer module. Ensuring that the input clock frequency of three computer modules is same, the asynchronous degree of output will be less than one clock.

4.1. Time-base Synchronization Simulation

Figure 4 shows the time-base synchronization simulation results. From the waveform, we can find that no matter which two us-count signals arrive, the us_out signal puts out and the reload signal is active. Three modules are all the same.

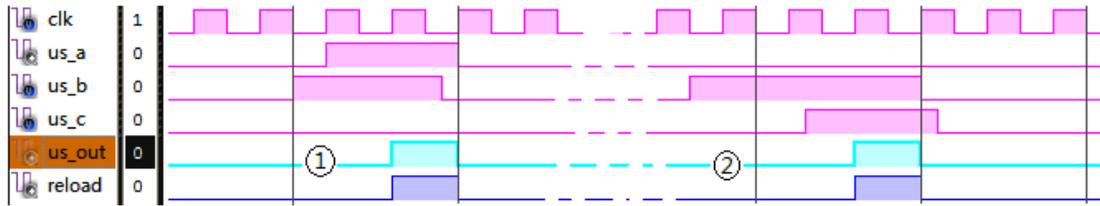


Fig. 4: Time-base synchronization simulation results

4.2. Period Synchronization Simulation

Figure 5 shows the period synchronization simulation results. There are three situations.

- 1) There is no module in failure and period count signals arrive within the setting time. Period_out is active correctly. Three modules are all the same.
- 2) Module A is in failure and the other two modules arrive. For module A, period_a is inactive and period_out is not given. Because module A is in failure, the period synchronization module should not give the interrupt signal, although two period count signals arrive. The other two modules are shown in situation 3).
- 3) Two period-count signals arrive and the third one does not arrive within the setting time (Supposed that module B is in failure). As shown, for the normal modules, period_out is given correctly after the setting time. Fault signals are given to indicate the error.

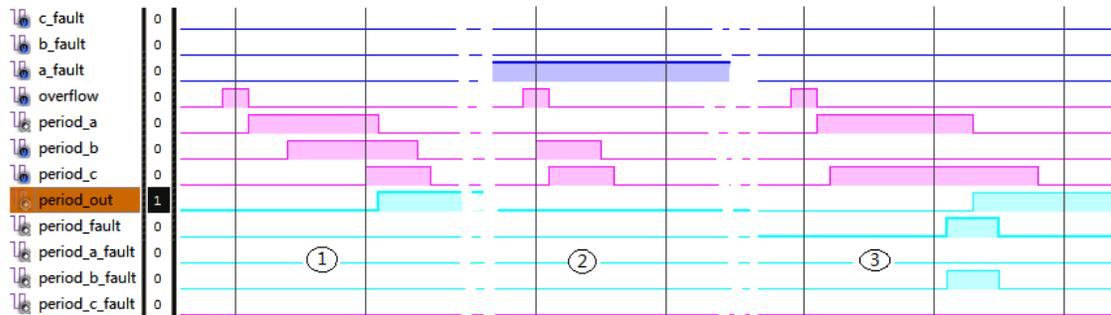


Fig. 5: Period synchronization simulation results

4.3. State Synchronization Module

Figure 6 shows the state synchronization simulation results. There are also three situations.

- 1) Data arrival signals all arrive and vote data are same. In this situation, vote results will be given at the rising edge of the third system clock after all three data arrival signals arrive. Vote results (25128) are same to the three vote data and can be read correctly in the second read-period. No fault signal is given.
- 2) One vote data (360) is different from the other two (25128), the results obey the principle of 2 out 3 and the fault signal is given. The module will report that which module is in failure.
- 3) The third data-arrival-signal does not arrive in two read-periods. The late module will be judged out by reading the STATE_REG and the outcome will be feedback to the fault detection unit.

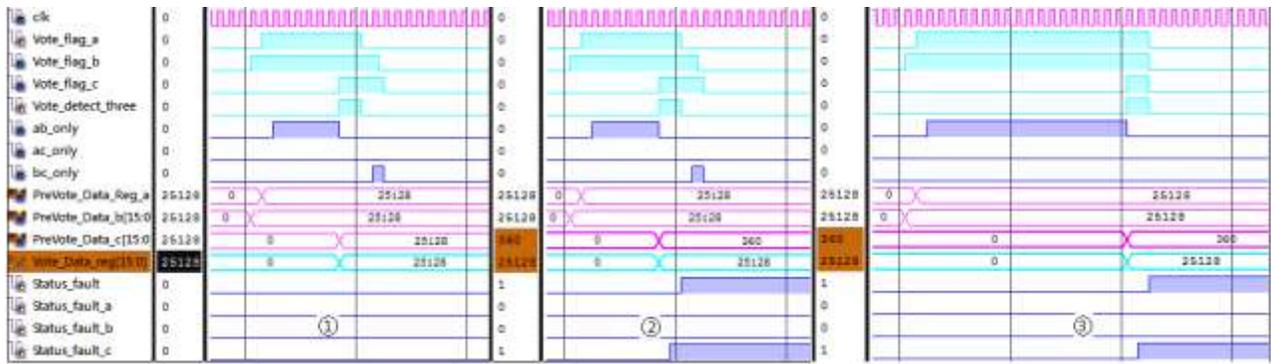


Fig. 6: State synchronization simulation results

5. Summary

The article presents a sound synchronization system achieving the synchronization of TMR computer. The system can not only implement the precise synchronization and improve the synchronization efficiency, but also can rebuild itself soon after detecting the fault. The period synchronization precision can be about 10ns. State synchronization precision can be about 50ns and the time consumption will be less than 150ns. Workload of software will become much less in cooperation with the synchronization system. The improved synchronization precision and efficiency will make the TMR computer more reliable.

6. References

- [1] Zhang Wei-gong, Zhang Yong-xiang, Shang Yuan-yuan, "Research on Precise Synchronization for TMR Fault-Tolerant Embedded Computer," in *Proc. International Conference on Multimedia Information Networking and Security*, 2009, pp. 322-325.
<http://dx.doi.org/10.1109/MINES.2009.98>
- [2] Yang Meng-fei, Guo Shu-ling, Sun Zeng-qi, "On-Board Computer Techniques for Spacecraft Control," *Aerospace Control*, vol. 23, pp. 69-73, Apr 2005.
- [3] Song Zheng-yu, "The synchronization Control Technology in Launch Vehicle Redundant Design," *Manned Spaceflight*, vol. 19, pp. 11-16, Mar 2013.
- [4] Tong Jie-wen, Wang Hui-quan, Jin Zhong-he, "On-Board TMR System Based on clock synchronization technology," C.N. Patent 103389914 A, Nov 13, 2013.
- [5] Feng Yan-jun, Li Ren-xin, Qiao Lei, "A Periodic Synchronization Mechanism for TMR Fault-Tolerant Computer," C.N. Patent 102053883 B, Aug 22, 2010.