Journal of Zhejiang University-SCIENCE A (Applied Physics & Engineering)
ISSN 1673-565X (Print); ISSN 1862-1775 (Online)
www.zju.edu.cn/jzus; www.springerlink.com
E-mail: jzus@zju.edu.cn

Design and reliability, availability, maintainability, and safety analysis of a high availability quadruple vital computer system*

Ping TAN†1, Wei-ting HE1, Jia LIN†1, Hong-ming ZHAO2, Jian CHU1

(1*State Key Laboratory of Industrial Control Technology & Institute of Cyber-Systems and Control, Zhejiang University, Hangzhou 310027, China*)

(2*Zhejiang Insigma-Supcon Co., Ltd., Hangzhou 310013, China*)

†E-mail: ptan@iipc.zju.edu.cn; zeroplus_zju@zju.edu.cn

Received Sept. 23, 2011; Revision accepted Sept. 23, 2011; Crosschecked Sept. 26, 2011

Abstract: With the development of high-speed railways in China, more than 2000 high-speed trains will be put into use. Safety and efficiency of railway transportation is increasingly important. We have designed a high availability quadruple vital computer (HAQVC) system based on the analysis of the architecture of the traditional double 2-out-of-2 system and 2-out-of-3 system. The HAQVC system is a system with high availability and safety, with prominent characteristics such as fire-new internal architecture, high efficiency, reliable data interaction mechanism, and operation state change mechanism. The hardware of the vital CPU is based on ARM7 with the real-time embedded safe operation system (ES-OS). The Markov modeling method is designed to evaluate the reliability, availability, maintainability, and safety (RAMS) of the system. In this paper, we demonstrate that the HAQVC system is more reliable than the all voting triple modular redundancy (AVTMR) system and double 2-out-of-2 system. Thus, the design can be used for a specific application system, such as an airplane or high-speed railway system.

Key words: Fault tolerant, High availability quadruple vital computer (HAQVC), Reliability, availability, maintainability, and safety (RAMS)

doi:10.1631/jzus.A11GT003 **Document code:** A **CLC number:** U28

1 Introduction

A high-speed railway is an energy-saving, environmentally-friendly, and sustainable transport mode. It has the advantages of being safe, punctual, fast, and comfortable. High-speed railway trunk lines in China will be completed in 2012. With the construction of intercity railways, a high-speed railway network, covering large cities with a population of more than 500 000, will be gradually formed. There will then be more than 2000 high-speed trains put into operation. Safety and efficiency of railway transport is increasingly important. The train operation control system is the key signal system equipment to guarantee the safety of train operation and improve the transport efficiency. The system is composed of an on board automatic train protection (ATP) system and a ground control system. The on board train control system is the so-called ATP, including on board vital computer (VC), track circuit reader (TCR), balise transmission module (BTM), data recording unit (DRU), driver machine interface (DMI), train interface unit (TIU), and train and wayside communication unit (TWC), etc. ATP is the final safety executant to ensure safe operation of a high-speed train, satisfying the requirements of safety integrity level 4 (SIL4), with fault-oriented safe attributes.

Commonly, the existing domestic ATP system uses a double 2-out-of-2 VC platform. This computer platform is built on a hot-standby redundant

* Project (No. 2009BAG12A05) supported by the National Key Technology R&D Program of China

subsystem, which uses the 2-out-of-2 VCs (Qin *et al.*, 2010). When a failure is found in any module of the subsystem, it will be in the fail-safe state, and the double 2-out-of-2 system is transformed into 2-out-of-2 redundancy system (Dou *et al.*, 2007), whose hardware fault tolerance is 1. In the 2-out-of-3 VC platform, if a failure is found in a certain module, the system will be changed into the 2-out-of-2 redundancy system. If more than two modules failed, the system will be in the fail-safe state. The hardware fault tolerance of the 2-out-of-3 VC platform is also 1. There is no disparity between the double 2-out-of-2 VC platform and the 2-out-of-3 VC platform in the aspect of hardware fault tolerance (IEC 61508-6: 2000).

There are two approaches to improve the reliability and safety of the system to block the failure of a system. The first is fault avoidance, and the second is fault tolerance (Kim *et al.*, 2005). Because components may develop faults with time, a fault avoidance technique is very difficult to apply (Kim *et al.*, 2002). However, with the fault tolerance technique, the system has a redundancy, and a fault is allowed without termination of its normal operation.

There are several types of fault tolerance techniques, such as hardware redundancy, software redundancy, time redundancy, and information redundancy techniques (Kim *et al.*, 2005). In the high availability quadruple vital computer (HAQVC) system, we use a hardware redundancy technique, embedded software redundancy and safe-bus redundancy. Technologies used in safety systems mainly include voting structure, or parallel structure, or both structures. The typical voting system is comprised of *n* units. The *k*/*n* system is that if the numbers of active units are no less than *k* (*k* is between 1 and *n*), the system will not be inactive. We assume that the reliability of *n* units is *R*, and the reliability mathematical model is shown as

$$R_\text{s}=\sum_{i=k}^{n}\binom{n}{i}R^{i}(1-R)^{n-i}, \tag{1}$$

where $\binom{n}{i}=\frac{n!}{i!(n-i)!}$, and R_s is the system reliability. The parallel system is also comprised of *n* units, and each unit of the system is independent. When all of its units are inactive, the parallel system will be inactive. The reliability mathematical model is shown as

$$R_\text{s}=1-\prod_{i=1}^{n}F_i=1-\prod_{i=1}^{n}(1-R_i),\quad i=1,2,\ldots,n, \tag{2}$$

where F_i and R_i are the unreliability and reliability of unit *i*.

Using the voting and parallel structures, it not only has the voting structure's advantage of high safety, but also has the parallel structure's advantage of availability and maintainability. The reliability mathematics model of the system is shown as

$$R_\text{s}=1-\prod_{i=1}^{N}F_i=1-\prod_{i=1}^{N}\left[1-\sum_{j=k}^{n}\binom{n}{j}R^{j}(1-R)^{n-j}\right],\\ k\le n,\ i=1,2,\ldots,N. \tag{3}$$

As shown in Eqs. (1)–(3), we can obtain the reliability function of the 2-out-of-2 system, the 2-out-of-3 system, and the double 2-out-of-2 system, which can be formulated as follows:

$$\begin{cases} R_\text{2-out-of-2}=R^2, \\ R_\text{2-out-of-3}=3\times R^2-2\times R^3, \\ R_\text{double2-out-of-2}=2\times R^2-R^4. \end{cases} \tag{4}$$

However, the above analysis shows that there is no disparity between the double 2-out-of-2 system and the 2-out-of-3 system. In fact, the 2-out-of-3 system is of the highest reliability. In order to provide full play to the advantages of four modules architecture, and ensure the safety of the system, while improving the reliability and availability of the system, we designed a novel HAQVC system, based on the research on the framework and the mechanism of data interaction and redundant degeneration of the VC platform. At the same time, we draw the curves of reliability of the HAQVC system, the double 2-out-of-2 system, the 2-out-of-3 system, and the 2-out-of-2 system in the same figure as a contrast (Fig. 1). Obviously, the HAQVC system is of the highest reliability.

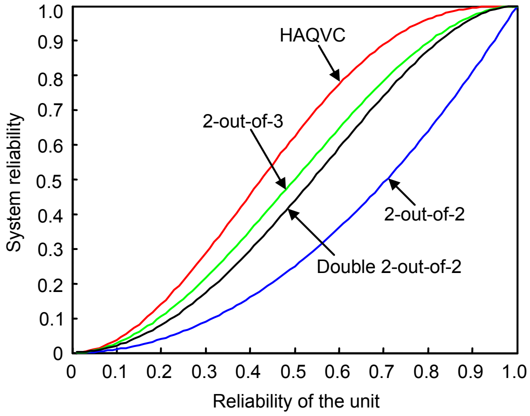


Fig. 1 Reliability of each system

2 System design

Compared with a general industrial control system, the on board ATP system is essentially a special safety control system with high-speed trains as its controlled object. The interface units and the function modules of the on board ATP system adopt the general modules except for the TIU, which mainly falls into two categories: multifunction vehicle bus (MVB) and relay interface. The function and scale of the system controller, types of input-output (IO) module, IO knot number, and types and number of communication module have been mostly determined. On the basis of meeting the requirements of the installation of rolling stock mechanical structure, electromagnetic compatibility, and convenient maintenance, a thorough study has been conducted for the key elements of the system, such as the requirements of safety, reliability, availability, maintainability, and real-timing and their restrictive relationships, so as to determine the scale of the control system, system architecture, network topology, hardware platform, and the mechanisms of communication scheduling and redundancy switching-over.

The VC module, input module, and output module of the HAQVC system are all of quadruple structure, linked by four redundancy safety buses (SBUS1, SBUS2, SBUS3, and SBUS4). The structure of the system is shown in Fig. 2. The system is double 2-out-of-2 when the four VC modules are operating correctly, in which one subsystem with 2-out-of-2 redundancy structure is composed of VC-A and VC-B, while the other subsystem is composed of VC-C and VC-D. We use four safety buses to achieve the interconnection, clock synchronization, and the communications scheduling between each subsystem. With the safety bus, the module can achieve the purpose of fault diagnosis, data synchronization, state information interaction, and safety data verification.

The traditional computer system of the double 2-out-of-2 includes two subsystems I and II, which are in a standby mode. Generally, only the master subsystem sends the results out, while the other subsystem is in the standby mode. Should the master subsystem break down, the slave subsystem will switch to the master subsystem and be run by the communication module. The way it works can significantly affect the availability and real time attributes of the system. If some data are lost because of the handover process, it will lead to an emergency brake. The HAQVC system works in a parallel operation mode. The subsystems I and II are in output states; thus, there is no disturbance caused by the shut-down process in the HAQVC system.

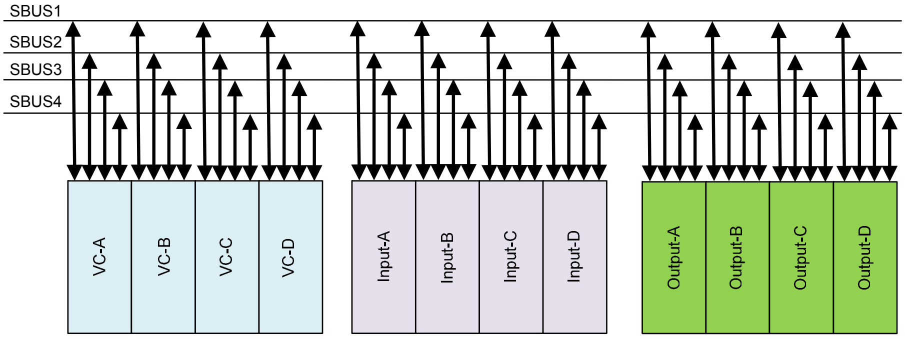


Fig. 2 Architecture of the high availability quadruple vital computer (HAQVC) system

In the traditional double 2-out-of-2 VC system, the system transforms into the 2-out-of-2 architecture when a failure is found in a certain module. Although there are two modules operating correctly, the system will be in the fail-safe state if subsystems I and II both have failures. However, if any module fails, the HAQVC system will degenerate to the 2-out-of-3 architecture. And if any two modules have faults, the system will transform into the 2-out-of-2 architecture. If more than three modules have faults, the HAQVC system will be in the fail-safe state. Table 1 lists the working state of the HAQVC system and the traditional double 2-out-of-2 system. States 2–5 mean the operating states of the system when only one module fails. The HAQVC system is operating with a 2-out-of-3 architecture and the hardware fault tolerance is 1. In the same condition, the traditional double 2-out-of-2 system is operating with a 2-out-of-2 architecture and the hardware fault tolerance is 1. States 7–10 indicate that two modules of subsystem I and II have faults. The HAQVC will be operating with 2-out-of-2 architecture while the double 2-out-of-2 system is in the fail-safe state. The HAQVC system has a distinct advantage over the traditional double 2-out-of-2 system.

In the system based on the HAQVC architecture, the key IO module and communication module use the similar architecture. And the interfaces of the ATP system, vehicle, and wayside equipment are more susceptible to the surge current and group impulse (Paul, 2006). In the application and engineering, we have found that the maintenance ratio of those interfaces is high. Therefore, using the HAQVC architecture can ensure the high availability and safety of the system, and enhance system reliability and maintainability.

3 Hardware and embedded safe operation system (ES-OS)

In fault-tolerant design techniques, there are passive hardware redundancy, active hardware redundancy, and hybrid hardware redundancy. The HAQVC system is passive hardware redundancy, which has a fault masking and detection. If the HAQVC system has no more than two faults, the fault is masked and has no effect on the system operation before repair. The HAQVC system is designed on ARM7.

The hardware fault diagnosis is one of the core contents of the hardware design of the safety-related system. According to the safety requirement of SIL4, the system hardware should be designed with high diagnostic coverage (DC). The DC should be more than 99% and 90% for the systems whose hardware

Table 1 Working state of the high availability quadruple vital computer (HAQVC) system and the double 2-out-of-2 vital computer[*]

Sequence No.	VC-A	VC-B	VC-C	VC-D	HAQVC	Double 2-out-of-2 vital computer
State 1	○	○	○	○	Double 2-out-of-2	Double 2-out-of-2
State 2	×	○	○	○	2-out-of-3	2-out-of-2
State 3	○	×	○	○	2-out-of-3	2-out-of-2
State 4	○	○	×	○	2-out-of-3	2-out-of-2
State 5	○	○	○	×	2-out-of-3	2-out-of-2
State 6	×	×	○	○	2-out-of-2	2-out-of-2
State 7	×	○	×	○	2-out-of-2	Fail-safe
State 8	×	○	○	×	2-out-of-2	Fail-safe
State 9	○	×	×	○	2-out-of-2	Fail-safe
State 10	○	×	○	×	2-out-of-2	Fail-safe
State 11	○	○	×	×	2-out-of-2	2-out-of-2
State 12	×	×	×	○	Fail-safe	Fail-safe
State 13	×	×	○	×	Fail-safe	Fail-safe
State 14	×	○	×	×	Fail-safe	Fail-safe
State 15	○	×	×	×	Fail-safe	Fail-safe
State 16	×	×	×	×	Fail-safe	Fail-safe

[*] ○: Normal; ×: Fault

fault tolerances are 1 and 2, respectively (IEC 61508-2:2000). The DC of the HAQVC system is over 99% by self-diagnosis of single module and the diagnosis between the modules. The vital CPU module will test the hardware equipment to ensure that the hardware is normal. The detecting items include instruction set, register, RAM, FLASH, the stack pointer, program sequence, crystal oscillator frequency, and power, etc. In terms of function, the detection module falls into four categories, power up detection sub-module, periodic check sub-module, the sub-module of interface of hardware detection circuit, and fault alarm sub-module. The system test and diagnostic flow is shown in Fig. 3.

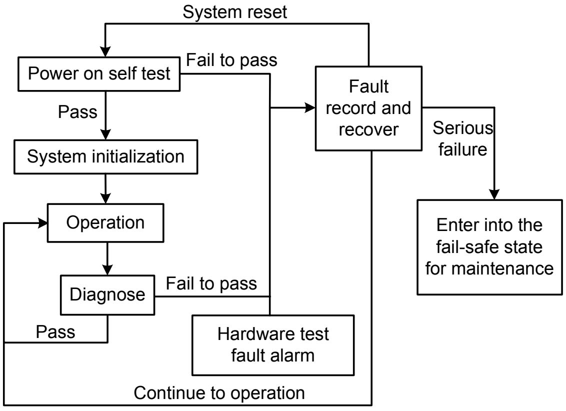


Fig. 3 System test and diagnostic flow

The power up detection sub-module will conduct a complete hardware detection of key hardware to ensure its normal operation when the system starts. The detecting objects include instruction set, register, RAM, and FLASH. The detection should not be complex, such that the power-on time of equipment is not too long. However, the detecting range must include the whole target objects.

In order to find hardware faults, the function of periodic check sub-module is to detect each part of hardware in real time during equipment operation. The detecting objects include instruction set, register, RAM, the stack pointer, and the chip.

The sub-module of interface of hardware detection circuit will receive the failure warning signal from the hardware detection circuit, such as the detection of the sequencing of programs using watchdog circuit, the crystal failure, the power management chip, and fault diagnosis of power.

The function of fault alarm sub-module is to record and report the failure detected by the hardware and provide corresponding measures.

The vital CPU hardware has been developed for nearly five years (Fig. 4). Besides the technical part of the development, an internal organization that corresponds to the European Committee for Electrotechnical Standardization (CENELEC) standards has to be built (EN 50126:1999; EN 50128:2001; EN 50129:2003). During the development period, the general and complex CENELEC process was stripped to an easier-to-handle specific process for generic developments. Thus, the development-process and the product itself fulfill the requirements of EN 50126:1999, EN 50128:2001, and EN 50129:2003.

Fig. 4 Picture of the hardware

According to the requirements of the safety system, a real-time embedded safe operation system (ES-OS) has been designed for the VC system. The ES-OS and application-program are non-volatile stored in compact flashcards. Power-on programs will be transferred to synchronous dynamic random access memory (SDRAM) and executed from there. Execution of the ES-OS begins with short self-tests and cyclic long-time-testing is proceeded by the ES-OS in background. The interface between the ES-OS and application via the application-interface (API) and application works with cyclic proceeded main-loops.

Hardware-abstraction-layer (HAL) communicates with hardware on chip and on board. HAL-functions include connector localization in rack, address-switch, on board/chip universal asynchronous receiver/transmitters (UARTs), test-signal reference, bus-arbitration, power-supervision, watchdog-supervision, pushing buttons, reset, light emitting diode (LED)-display, and so on.

The ES-OS functional modules communicate with HAL and API, serving as an interface between HAL and API. The functions of the ES-OS modules include general-control-module, communication between HAL and API, output of massages to display, scanning and control of pushing buttons, self-tests, exception-handling, system-functions, and so on.

API communicates with application, serving as an interface between ES-OS and application. Based on practical application, six kinds of API are designed in the ES-OS. EA-input-API announces the state of the inputs to the application. EA-output-API controls the outputs by the application layer and reading back the state of the outputs to the application layer. Man-machine-interface-API (MMI-API) displays messages and reacts of pushing buttons. External-communication-API (E-COM-API) sends and receives data via the buses and local area network (LAN), building and analyzing the safeguarded telegrams. Internal-communication-API (I-COM-API) communicates with the other channel. Error-handling-API (Errhler-API) announces errors to the application and exception-handling. System API is for special non-safe system functions such as timers.

4 Safety bus and deterministic communication schedule

The safety communication protocol has been adopted to develop the quadruple safety bus. By adding three bytes safe cyclic redundancy check (CRC) and extending a complete byte, a total of four bytes are transmitted to ensure the safety of the message. CRC adopts the Hamming distance *h* which equals 7 to ensure the safety of the 24-byte data. In this study, the bit false rate (BFR), which is usually set to the value of 10^{-9} in good transmission equipment, is 10^{-4}. The maximum transmission rate of the applied communication equipment is 500 frames/s. Each packet of the transmission frame format contains all the relevant safety performance. After the camouflage identification, the packets will be rejected and the message will be resent.

When the Hamming distance equals 7, 6-bit camouflage data can be identified. If 7-bit or more camouflage data emerges, there will be risks. Since the probability of over 7-bit camouflage data appearing is far lower than 7-bit camouflage data whose frame format is 216-bit, it can be neglected. Supposing that the number of bit is *n*, the binomial distribution would be: in a message frame format, the probability of the existence of *k*-bit camouflage data is

$$p(k)=\binom{n}{k}\times \mathrm{BFR}^{k}\times(1-\mathrm{BFR})^{n-k}. \tag{5}$$

Because BFR<<1, and $p(k)\approx\binom{n}{k}\times\mathrm{BFR}^{k}$. Based on BFR=$10^{-4}$, n=216, and k=7, the value of $p(7)$ can be obtained by $p(7)\approx\binom{216}{7}\times(10^{-4})^{7}=4\times10^{-16}$. In every 500 frames/s, the risk rate is shown as

$$\mathrm{HR}=4\times10^{-16}\times500\times3600\ \mathrm{h}^{-1}=7.2\times10^{-10}\ \mathrm{h}^{-1}. \tag{6}$$

In the double-channel system, the risk rate when the packet data of channels A and B are camouflaged simultaneously is 5.2×10^{-19} h^{-1}. Because of the low rate, it can be neglected during the actual calculation process, especially for the situation when only 20 addresses can be used for the system.

All the communications between modules and CPU rely on the safety communication bus. The HAQVC system adopts a fixed address coding technique. The first address of a set of modules (*n*) is a multiple of 4, *n*=4*k*. The other three address codes of the group module are 4*k*+1, 4*k*+2, and 4*k*+3, and the following codes 4(*k*+1), 4(*k*+1)+1, 4(*k*+1)+2, and 4(*k*+1)+3 are for the next set of modules. The CPU modules of HAQVC occupy four communication buses. For the ATP system, the relationship among communication links of the modules is fixed, and the content of communication will change over time and circle. Although the communication among different VC modules occupies the bus, it will not take the CPU resources of other modules, because the irrelevant information will be blocked in the link layer of the bus interface chip. At a certain time, some emergency concerning driving happens, such as the track circuit's code sequence mutates, active balise information and IO information on train safety status change. Even though the fixed communication slot has passed, the transmission of relevant messages will be through event-trigger communication, so that the vital CPU module can take safety measures in time and not need to wait until the next cycle (IEC/PAS 62409:2005). The specific scheduling diagram is shown in Fig. 5.

The vital CPU module of HAQVC provides interactive information exchange between diagnostic message and synchronic information through the safety bus in the second and third time slots. In addition, through the inter-communication, vital CPU module receives real-time working status and calculation results of other CPU modules, and thus guarantees the effectiveness and real time attribute of safety output function based on the voting structure, false diagnosis and screening function, rapid regression function, and failure-oriented safety function. The control data can be obtained in the fourth time slot.

The certainty of communication scheduling of the whole system is based on precision clock synchronization. The measurement accuracy is shown in Fig. 6. The system, which combines hardware and software synchronization, achieves the precise synchronization among modules and ensures the safety of clock synchronization. Master clock sends synchronization-related messages within the first communication slot. The system supports the access of absolute clock of global positioning system (GPS) to realize global synchronization, and provides a guarantee for accident and error recording.

The device modules of the HAQVC system are connected with system bus through isolating communication interface modules, so that the fault module can be cut off in case of failure, and thus ensure the system bus safety when modules are disconnected from it.

5 System modeling

The proposed HAQVC system structure is shown in Fig. 2. This system is comprised of four subsystems. As shown in Fig. 2, each CPU module receives voting data from four input modules and each output module receives voting data from four CPU modules. Thus, two CPU module, input module or output module failures have no influence on the system. To start the modeling, we have adopted the following assumptions.

1. The system starts in the perfect operation when all of the system's modules are operating correctly.

2. Only one failure will occur at a time.

3. The error probabilities are the same for the same module of the system, which show symmetry.

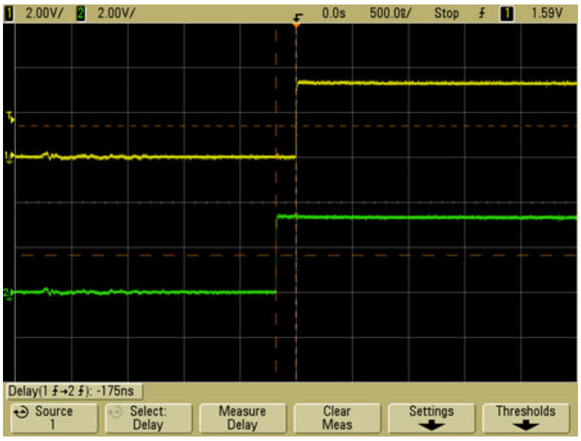


Fig. 6 Diagram of accuracy of clock synchronization
Green and yellow represent pulses generated by any two different modules. The synchronization accuracy is represented by the time difference of the two pulse rising edge

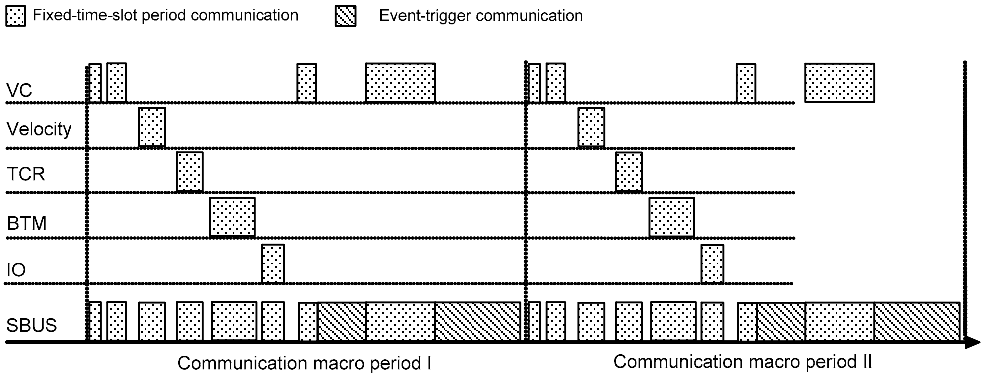

▨ Fixed-time-slot period communication
▧ Event-trigger communication
VC
Velocity
TCR
BTM
IO
SBUS
Communication macro period I
Communication macro period II

Fig. 5 Communication scheduling sequence

4. Errors affecting different components of the same unit are statistically independent.

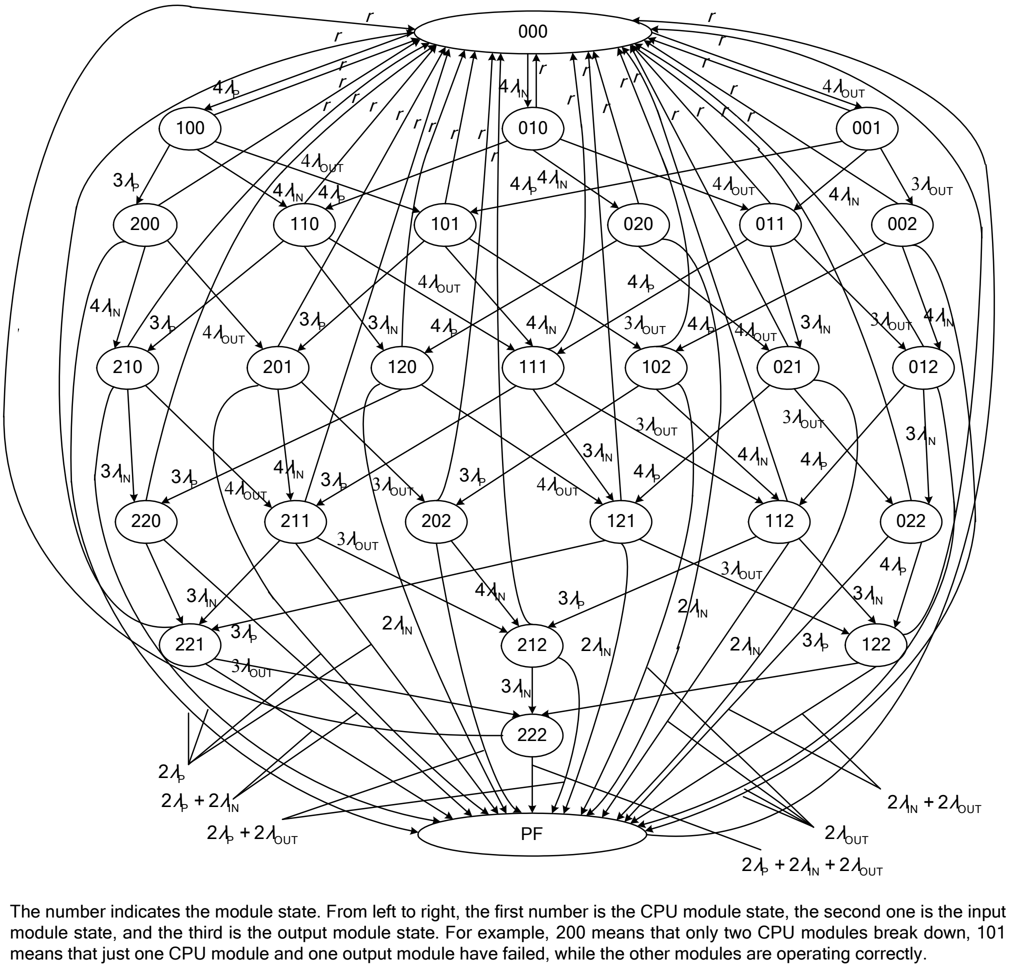
A Markov model of the HAQVC system is proposed in Fig. 7. The system is composed of 28 states. The PF state is a failure state and the rest state is operating. $\lambda_{\rm P}$, $\lambda_{\rm IN}$, and $\lambda_{\rm OUT}$ are the failure rates of the CPU module, the input module, and the output module, respectively, and r designates the system repair rate of the HAQVC system. For simplicity, we assume that the repair rate is a specific value for all states of the system. The discrete system equation is highly complex, and thus it is represented in a simple form as

$$\boldsymbol{P}=\begin{bmatrix} 1-\Sigma & S_{1,2} & \cdots & S_{1,27} & S_{1,28} \\ r & 1-\Sigma & \cdots & S_{2,27} & S_{2,28} \\ \vdots & \vdots & & \vdots & \vdots \\ r & S_{27,2} & \cdots & 1-\Sigma & S_{27,28} \\ r & S_{28,2} & \cdots & S_{28,27} & 1-\Sigma \end{bmatrix}, \qquad (7)$$

where $S_{i,j}$ is the state transition probability from state i to state j and Σ is the state transition probability sum of row of the matrix.

6 Evaluation

In order to be sure that this design is meaningful, we have carried out experiments to compare the performance of the HAQVC system, the all voting triple modular redundancy (AVTMR) system (Kim *et al.*, 2005), and the double 2-out-of-2 system (Wang *et al.*, 2007). Keeping the failure rate and the repair rate unchanged, we draw the curves of reliability, availability, maintainability, and safety (RAMS) parameters of the three systems in the same figure as contrast using Matlab.



The number indicates the module state. From left to right, the first number is the CPU module state, the second one is the input module state, and the third is the output module state. For example, 200 means that only two CPU modules break down, 101 means that just one CPU module and one output module have failed, while the other modules are operating correctly.

Fig. 7 Markov model of the high availability quadruple vital computer (HAQVC) system

6.1 Reliability

As is well known, reliability is the ability of a system to perform its required functions under stated conditions for a specified period of time. As shown in Fig. 8a, initially, the HAQVC system is of the highest reliability until about 730 000 h, and from 730 000 h, the double 2-out-of-2 system is the same with the HAQVC system. Anyway, the AVTMR system is not of good reliability among the three systems for a lengthy time.

6.2 Availability

Availability means the ability of a product to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval assuming that the required external resources are provided. Availability of the HAQVC system, the AVTMR system, and the double 2-out-of-2 system is shown in Fig. 8b. For simplicity, the repair rate of each system is assumed to be 0.003 for simulation. The availability of each system is close to that shown in Fig. 8b. The HAQVC system has the highest availability, and the double 2-out-of-2 system is better than the AVTMR system.

6.3 Maintainability

Maintainability is the probability that the failed system will be restored to an operational state within a specified period of time. As shown in Fig. 8c, the AVTMR and double 2-out-of-2 systems are of higher maintainability than HAQVC. Thus, this design can improve the availability of the system.

6.4 Safety

Safety is the probability of systems where there is no dangerous failure. That is, safety is a state in which there is no danger. We take each system as a repairable system and the repair rate is 0.003. As shown in Fig. 8d, the HAQVC system has the highest safety.

7 Conclusions

In this paper, based on the analysis of the architecture of the traditional double 2-out-of-2 system and the 2-out-of-3 system, we propose the HAQVC system, which is a novel fault-tolerant system with fire-new redundancy structure, and can significantly

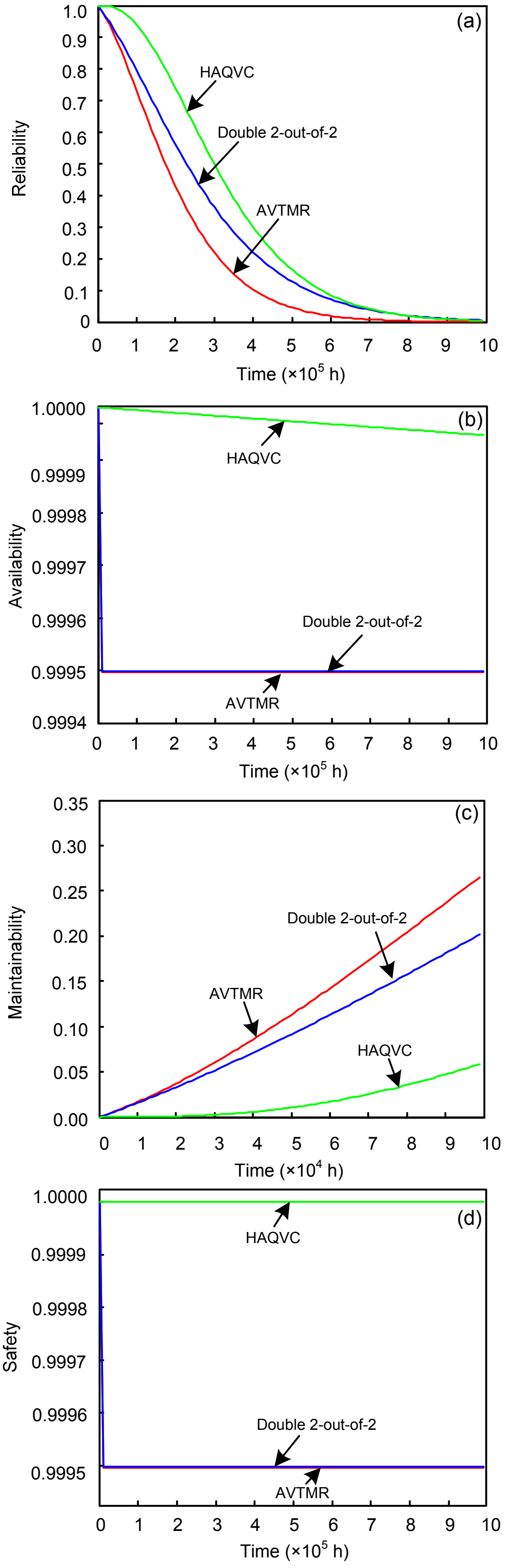


Fig. 8 Reliability (a), availability (b), maintainability (c), and safety (d) of each system

improve the reliability and safety. Its working process has been described and compared with the AVTMR system and the double 2-out-of-2 system in RAMS. Simulation results indicate that the HAQVC system has the best characteristic in RAMS and it is a better VC platform for a railway signal system.

References

Dou, F.S., Cao, Z., Luo, L., Long, Z.Q., 2007. Design and Realization of Safety Computer Systems Based on Double 2-Vote-2 Redundancy. Chinese Control Decision Conference, Wuxi, China, p.1059-1061, 1066 (in Chinese).

EN 50126:1999. Railway Applications—the Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS). European Committee for Electrotechnical Standardization.

EN 50128:2001. Railway Applications-Communication, Signaling and Processing Systems-Software for Railway Control and Protection Systems. European Committee for Electrotechnical Standardization.

EN 50129:2003. Railway Applications-Communication, Signaling and Processing Systems-Safety Related Electronic Systems for Signaling. European Committee for Electrotechnical Standardization.

IEC 61508-2:2000. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems—Part 2: Requirements for Electrical/Electronic/Programmable Electronic Safety-Related Systems. International Electrotechnical Commission.

IEC 61508-6:2000. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems—Part 6: Guidelines on the Application of IEC 61508-2 and IEC 61508-3. International Electrotechnical Commission.

IEC/PAS 62409:2005. Real-time Ethernet for Plant Automation (EPA). International Electro Technical Commission.

Kim, H., Jeon, H.J., Lee, K., Lee, H., 2002. The Design and Evaluation of All Voting Triple Modular Redundancy System. Annual Reliability and Maintainability Symposium, p.439-444. [doi:10.1109/RAMS.2002.981682]

Kim, H., Lee, H., Lee, K., 2005. The design and analysis of AVTMR (all voting triple modular redundancy) and dual-duplex system. *Reliability Engineering and System Safety*, **88**(3):291-300. [doi:10.1016/j.ress.2004.08.012]

Paul, C.R., 2006. Introduction to Electromagnetic Compatibility (2nd Ed.). John Wiley & Sons, Inc., Hoboken, NJ, USA. [doi:10.1002/0471758159.Fmatter]

Qin, Q.N., Wei, X.Y., Yu, R.R., Han, L., 2010. Simplified Design of Embedded Double 2-Vote-2 Computer System. 3rd International Symposium on Test Automation and Instrumentation, Xiamen, China, p.233-236.

Wang, S., Ji, Y.D., Dong, W., Yang, S.Y., 2007. Design and RAMS analysis of a fault-tolerant computer control system. *Tsinghua Science and Technology*, **12**(S1):116-121. [doi:10.1016/S1007-0214(07)70095-0]