Link Redundancy Research and Reliability Analysis Based on Dual CAN Architecture

Yangsong Feng, Hong Li

School of Electrical & Information Engineering, Changsha University of Science & Technology, Changsha, Hunan, 410004, China

email: ysf22@foxmail.com

*Corresponding author’s e-mail: hongli@csust.edu.cn

Abstract. Aiming at the problem that special vehicles still need to ensure the reliability of vehicle-mounted bus communication in the long-term complex and strong interference communication environment, a link layer redundancy scheme based on dual CAN channels is proposed. By adding redundant modules and improving the redundancy mechanism, dual CAN controllers can not only realize the undisturbed switching of data communication in hot redundancy mode, but also realize the function of error correction and retransmission in cold redundancy mode. Finally, a mathematical model of the reliability of dual CAN redundancy is established through the Markov state transfer chain, and this model is compared with other models for analysis and evaluation to verify that its reliability is significantly improved.

1. Introduction

The Controller Area Network bus \(^1\) (Controller Area Network, CAN) proposed by the German BOSCH company in the early 1980s is not only widely used in the automotive industry, but also in coal mines, machinery, textiles and other fields \(^2\). As the CAN bus environment is complex and diverse, the communication environment it faces is becoming increasingly complex and harsh. At the same time, the number of node devices connected on the CAN bus has gradually increased \(^5\). Therefore, improving the reliability of communication has become one of the research hotspots in the CAN bus field. Due to the particularity of its functions and the complexity of the working environment, special vehicles have higher requirements in terms of CAN bus safety.

At present, in many solutions to ensure the reliability of CAN bus communication system, there are two commonly used \(^6\): one is to improve the reliability of the components to improve the reliability of the system, but the reliability of the components is easily limited by the processing technology. At the same time, when the complexity of the system increases, the reliability of the system will decrease; the other method is redundancy. By adding additional components, it is guaranteed that after the working components fail, the additional spare components can be switched into the system to improve the reliability of the system. The redundancy related to CAN bus includes bus controller redundancy, bus driver redundancy, full system redundancy, and bus node redundancy \(^7\).\(10\).

Under normal circumstances, the hot redundancy fault handling mechanism in the CAN bus controller redundancy scheme is simple, which leaves hidden dangers in the reliability of communication. It is difficult to balance a series of deficiencies such as fault sensitivity and bus utilization in the design of cold redundancy using master nodes. This article proposes a link redundancy design based on dual CAN architecture, which can effectively solve such problems.
2. Materials and Methods

Redundancy mainly includes hot redundancy and cold redundancy. The backup components in the hot redundancy system are always in operation. Once the main equipment fails, the backup equipment can be switched into the system immediately, which can effectively guarantee the normal operation of the system in time, especially when the system cannot be shut down, the non-disturbed switching function of thermal redundancy is particularly important. The cold redundant backup components will only start to operate after the main equipment fails, so it takes time to start the equipment, or even manually. In occasions where system requirements are not high, cold redundancy has the advantage of energy saving compared to hot redundancy.

2.1. Thermal Redundancy Analysis of Common CAN Bus

There are two common CAN bus thermal redundancy mechanisms. 1) When both buses transmit data, the receiving end adopts the "first come first use" strategy. That is, if the bus data of any line arrives first, the CAN controller will adopt the data on this bus and discard the other bus. In this way, there will be some hidden dangers: the data that first arrives at the receiving end may be interfered with during transmission and cause errors, and the data that arrives later is accurate. In the above-mentioned redundancy mechanism, this communication fails. 2) The two CAN controllers are divided into main controller and standby controller. After the main controller normally receives the frame information, it sends a signal to the standby controller to keep it in the standby working state. When the communication link where the main controller is located fails to send a signal to the standby controller, the standby controller in the working state immediately takes over the main controller. In the above-mentioned redundancy mechanism, if the communication link from the main controller to the standby controller fails, a dual-master failure state will occur. Therefore, due to the ill-considered strategy of selecting a fault-free bus in the redundancy mechanism, a more efficient redundancy mechanism is required to ensure the reliability of CAN communication.

2.2. Analysis of Cold Redundancy of Common CAN Bus

In the cold redundancy mode of the ordinary CAN bus, a timer is set inside the control terminal CPU (Central Processing Unit) connected to the CAN controller. The CAN controller on the bus as the master node periodically broadcasts specific frame information to the bus, and the sending cycle should be less than the timer cycle. After receiving this frame information, the remaining CAN nodes reset their respective CPU timers. If the bus is faulty and the slave node cannot receive the frame information for resetting the timer, after the timer counts up, the switch signal is triggered to switch the standby CAN bus into the system, and the input of the original CAN bus will be shielded.

The disadvantage of ordinary CAN bus cold redundancy is that the counter cycle is too long, it will reduce the sensitivity to failure, and then affect the reliability of the system. If the cycle of the counter is too short, and the frame information of the counter reset is sent frequently, the utilization rate of the CAN bus will be reduced, and the communication efficiency of the CAN bus will be reduced. And because of the existence of the master node, additional redundancy for the master node is needed. Otherwise, when the master node fails and cannot periodically send the frame information for resetting the counter, the slave devices on the bus will switch to the backup bus by mistake.

2.3. The redundant structure design of dual CAN link

In response to the above-mentioned problems, this paper integrates CAN bus redundancy, interface redundancy and controller redundancy, and draws on the parallel voting redundancy structure in the IEC61508 functional safety protocol, and proposes the link architecture shown in Figure 3. Two independent CAN controllers are used, and each CAN controller is connected to a CAN bus. The voltage difference signal on the CAN bus is connected to the CAN controller and the redundant module after passing through the level conversion chip of the CAN interface. The data receiving storage module and the redundancy module inside the CAN controller are also connected to each other. In the non-redundant mode, the two CAN controllers are configured separately through the command, control bus, data, and
address bus to form two independent CAN channels. In the redundant mode, the diagnostic module not only records the fault conditions in the redundant state, but also shields the CAN controllers with data reception errors due to CAN bus failures through the selector, and selects the CAN controllers with correct data reception to access the system.

![Figure 1. Redundant block diagram of dual CAN architecture](image)

### 2.4. Reliability model establishment of dual CAN architecture
Normally, because the reliability of electronic equipment is distributed exponentially and it is assumed that two CAN controllers will not fail at the same time in a very short time. Combining the characteristics of special vehicles that are not easy to repair when they work in harsh environments, the Markov model based on non-repairable systems is established. The Markov models of the working state in hot redundancy and improved cold redundancy modes are shown in Figure 2 and Figure 3 respectively. In addition to the failure of dual CAN controllers due to successive failures of ordinary CAN bus thermal redundancy, there are also dual CAN controllers that become the main controller at the same time, which makes the sending and receiving of frame information in a disordered state. The state transition diagram is shown in Figure 4.

![Figure 2. Improved Markov Model of Hot Redundancy Mode](image)

![Figure 3. Improved Markov model of cold redundancy mode](image)
In Figures 2 to 4, $\lambda_1$ is the failure rate of the CAN1 controller, $\lambda_2$ is the failure rate of the CAN2 controller, $\lambda'_2$ is the failure rate of the standby CAN controller in the light-load working state, and $\lambda_3$ is the dual redundancy mode the failure rate of the dual-host failure state. According to the Markov model mentioned above, the improved mathematical model of cold redundancy is shown in equation (1). If $\lambda'_2$ in equation (1) is changed to $\lambda_2$, the mathematical expression of the hot redundancy mode can be obtained.

\[
\begin{align*}
\frac{dP_0(t)}{dt} &= -(\lambda_1 + \lambda'_2)P_0(t) \\
\frac{dP_1(t)}{dt} &= \lambda_1P_0(t) - \lambda_2P_1(t) \\
\frac{dP_2(t)}{dt} &= \lambda'_2P_0(t) - \lambda_1P_2(t) \\
\frac{dP_3(t)}{dt} &= \lambda_2P_1(t) + \lambda_1P_2(t)
\end{align*}
\]  

(1)

$P_0(t)$–$P_3(t)$ are the probability that the controller is in state S0–S3 at time t respectively. Let $P(t)=[P_0(t), P_1(t), P_2(t), P_3(t)]^T$, and the above differential equations are written in matrix form as

\[
\frac{dP(t)}{dt} = M_1P(t) 
\]  

(2)

\[
M_1 = \begin{bmatrix}
-\lambda_1 - \lambda'_2 & 0 & 0 & 0 \\
\lambda_1 & -\lambda_2 & 0 & 0 \\
\lambda'_2 & 0 & -\lambda_1 & 0 \\
0 & \lambda_2 & \lambda_1 & 0
\end{bmatrix}
\]  

(3)

Let $L_1=[1 \ 1 \ 1 \ 0]$, in the initial state, the function of each component is normal, set $P_i(0)=[1 \ 0 \ 0 \ 0]$ and the reliability is set as

\[
R_i(t) = L_1P_i(t) \big|_{P_i(0)=[1 \ 0 \ 0 \ 0]} 
\]  

(4)

In the same way, combined with the Markov model in Figure 4, the ordinary dual redundant state transition matrix is following $M_2$. 

Figure 4. Markov model of ordinary dual redundancy mode
\[
M_2 = \begin{bmatrix}
- (\lambda_1 + \lambda_2 + \lambda_3) & 0 & 0 & 0 & 0 \\
\lambda_1 & - \lambda_2 & 0 & 0 & 0 \\
\lambda_2 & 0 & - \lambda_1 & 0 & 0 \\
0 & \lambda_2 & \lambda_3 & 0 & 0 \\
\lambda_3 & 0 & 0 & 0 & 0
\end{bmatrix}
\]  

(5)

Let \( L_2 = [1 \ 1 \ 1 \ 0 \ 0] \) and \( P_2(0) = [1 \ 0 \ 0 \ 0 \ 0] \). The reliability of the ordinary dual redundant CAN controller is

\[
R_2(t) = L_2 P_2(t) |_{P_2(0)=[1 \ 0 \ 0 \ 0 \ 0]}
\]

(6)

3. Results & Discussion

Obviously, by adding redundant links, the reliability of the system can be greatly improved, which is detailed in the literature [13]. However, different redundancy mechanisms have differences in the improvement of system reliability. The following will explain through quantitative calculations. Compared with the ordinary dual redundancy mode, the CAN controller is reliable in the improved dual redundancy mode. The degree is significantly improved.

According to the data manual provided by the chip manufacturer and the functional safety protocol IEC61508, it can be known that \( \lambda_1 = \lambda_2 = 1.8 \times 10^{-6}, \lambda_3 = 2.5 \times 10^{-7} \). Substitute the parameters into the model before and after the improvement of the thermal redundancy mechanism, combined with Matlab Figure 5 shows the reliability distribution before and after the improvement of the redundancy mechanism in the thermal redundancy mode by calculation and simulation.

![Figure 5. Reliability distribution diagram in hot redundancy mode](image)

It can be seen from the figure that the improved redundancy reliability has been greatly improved. Taking the reliability of 0.98 as an example, the reliability life of the redundancy mechanism before and after the improvement is 52490h and 84800h respectively, and the improved reliability life is extended by 61.55%.

4. Conclusions

In summary, CAN bus is one of the most practical field buses. Adding redundant functional modules to the CAN bus network is beneficial to improve the reliability of data transmission. The redundancy
technology of the dual CAN architecture is developed on the basis of the traditional redundancy technology. The use of the improved redundancy technology of the dual CAN architecture in the CAN bus network can not only achieve information transmission efficiently, but also significantly extend the bus's mean time between failures. Therefore, the research on the CAN bus network using this technology has economic and practical value, and has a good research and development prospect.

References
[1] Jie Tan. Research and design of network bridge in CAN bus distributed measurement and control system[D]. Wuhan: Wuhan University of Technology, 2006.
[2] Tianhao Peng, Guo Chao. Design of remote monitoring system for coal shearer operating state parameters [J]. Coal Mine Machinery, 2020, 41(09): 1-4.
[3] Wangjie Tang, Huabiao Jin, Heming Li. Ship data acquisition and remote monitoring system based on CAN redundancy [J]. Ship Science and Technology, 2020, 42(3): 144-147
[4] Ting Zhao, Dong Xu, Lin Yang, Fei Wang, Xiaoping Tang. Research and application of loom network monitoring system based on CAN bus[J]. Cotton Textile Technology, 2016, 44(09): 44-47.
[5] Zhang L. Design of Electromagnetic Compatibility Performance of Multi-Node CAN-Bus System[J]. IOP Conference Series: Earth and Environmental Science, 2019, 295(3):032074 (5pp).
[6] Wang Zhenxi. Reliability, redundancy and fault tolerance technology [M]. Aviation Industry Press,1991:119-129.
[7] Qingsong Gao, Wei Zhao, Jun Sun, et al. Dual-redundant CAN bus interface design for satellite micro-vibration measurement system [J]. Automation Instrumentation, 2019, 40(09): 88-92
[8] Chunlai Yu, Hualong Xu, Genlong Liu, etc. Research on CAN Bus Redundancy Method[J].Measurement and Control Technology,2003,22(10):28-30
[9] Junmin Cao, Xiangqun Meng, Houjun Tang. Dual bus redundancy for a single CAN controllerNetwork realization[J].Microprocessor,2007,04:29-31
[10] Lin Zhao, Yan Gao, Rui Wei, et al. Reliability design of dual redundant bus communication[J]. Quality and Reliability, 2020(1): 25-28.
[11] Xiaosong Guo, Zhenye Wang, Chuanqiang Yu, etc. Fault-tolerant redundancy based on CAN busTechnical Research[J].Computer Measurement and Control,2009,17(1):60-63.
[12] IEC 61508,Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems[S]. Switzerland Geneva: International Electrotechnical Commission, 2010.
[13] Yiyong Tang, Chuande Wang. Research and reliability analysis of CAN bus redundancy system[J]. Journal of Zhongyuan Institute of Technology, 2010, 21(05): 73-75.