Science Discovery
2019; 7(1): 18-23
http://www.sciencepublishinggroup.com/j/sd
doi: 10.11648/j.sd.20190701.14
ISSN: 2331-0642 (Print); ISSN: 2331-0650 (Online)

Reliability Analysis of Safety Critical Computer System Considering Common Cause Failure

Zhao Deliang, Xu Hongze

School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing, China

Email address
16120283@bjtu.edu.cn (Zhao Deliang), hzxu@bjtu.edu.com (Xu Hongze)

To cite this article:
Zhao Deliang, Xu Hongze. Reliability Analysis of Safety Critical Computer System Considering Common Cause Failure. *Science Discovery*. Vol. 7, No. 1, 2019, pp. 18-23. doi: 10.11648/j.sd.20190701.14

Received: January 20, 2019; **Accepted**: February 27, 2019; **Published**: March 8, 2019

Abstract: The rail transit operation control system and nuclear reactor control system are extremely high for safety and reliability, especially the high speed maglev of more than 600 kilometers per hour. Therefore, the effect of common cause failure on the reliability of safety critical computer must be considered.The safety critical system is the key of the above-mentioned safety demanding system. In this paper, the structure and working principle of a safety critical computer with two-out-of-three and double two-out-of-two are analyzed.Considering the common cause failure and maintenance rate, by using Markov model, the reliability models of safety critical computer system with with two-out-of-three and double two-out-of-two are established. The simulation results show that the existence of common cause failure greatly reduces the reliability of the system. The maintenance rate can improve the reliability of the system. At the same time, considering the common cause failure and the maintenance rate, it is proved that the reliability of the two-out-of-three safety critical computer system is higher than double two-out-of-two safety critical computer system. Therefore, it provides theoretical support for the design of the subsequent differentiated security computer platform.

Keywords: Safety Critical Computer, 2oo3, 2x2oo2, Common Cause Failure, Reliability

考虑共因失效的安全计算机系统的可靠性分析

赵得亮，徐洪泽

北京交通大学电子信息工程学院，北京，中国

邮箱
16120283@bjtu.edu.cn（赵得亮），hzxu@bjtu.edu.cn（徐洪泽）

摘要：轨道交通运行控制及核反应堆控制等安全苛求系统对安全性及可靠性有极高的要求，尤其是600公里以上时速的高速磁浮对其可靠性提出了更高的要求，因此必须考虑共因失对安全计算机可靠性的影响。安全计算机系统是安全苛求系统的核心部件，本文首先分析了三取二以及二乘二取二的安全计算机的结构及工作原理，在考虑共因失效以及维修率的情况下，利用马尔可夫模型建立了考虑共因失效的三取二和二乘二取二安全计算机系统的可靠性模型，通过仿真分析证明了共因失效的存在大大降低了系统的可靠性，而维修率会提高系统的可靠性，同时在考虑共因失效以及维修率的情况下，证明了三取二安全计算机系统的可靠性是高于二乘二取二安全计算机系统，从而为后续差异化安全计算机平台的设计提供了理论支持。

关键词：安全计算机，三取二，二乘二取二，共因失效，可靠性

1．引言

在轨道交通运行控制、核反应堆控制、航空航天测控等安全苛求领域，安全计算机系统有着广泛的应用[1,2]。安全计算机[2]作为上述系统的核心部件，完成系统数据的安全采集，处理以及传输等，安全计算机可以确保系统发生故障时，系统能够导向安全状态。

可靠性作为衡量安全计算机系统的一个重要指标[3]，研究安全计算机系统的可靠性对保证安全苛求系统安全稳定运行有重要的意义。目前越来越多的学者对安全计算机系统的可靠性进行研究分析，但大都忽略了共因失效对系统可靠性的影响，文献[4]中在对系进行可靠性安全性建模时，没有考虑共因失效，只考虑了独立失效，导致计算的系统可靠性偏高，造成研究人员在设计、维修工作中对系统过于乐观，忽略一些影响安全行车的重要因素。

共因失效[5,6]是指系统中由于某种共同因素造成两个或者两个以上单元同时失效[7,8]。共因失效问题的存在会增加系统联合失效概率，从而降低冗余系统可靠度。文献[7]指出核工业的概率风险分析表明：共因失效是冗余系统失效和设备不可用的主要原因，由此可见高度重视共因失效的影响是十分重要的。

因此，本研究对目前主流的安全计算机系统的核心设备——三取二安全计算机和二乘二取二安全计算机在综合考虑共因失效和维修率的情况下建立马尔可夫模型，通过Matlab仿真，分析了共因失效、维修率对其可靠性的影响。为差异化安全计算机的设计提供理论支持。

2．安全计算机系统的系统的可靠性模型

2.1．马尔可夫过程

目前用于分析系统可靠性的方法有很多，如故障树分析法[9]，贝叶斯网络分析法[10]等，但由于分析的安全计算机系统主要由电子元件组成，寿命服从指数分布，而且考虑到共因失效，维修率等因素，马尔可夫模型更加方便和适合分析安全计算机的可靠性。

2.2．假设

在分析之前，本研究假设如下条件对于所分析的系统成立：

a) 系统及其组成单元只有故障与正常两种状态，不存在第三种状态；
b) 系统的所有输入在规定极限之内，即不考虑由于输入错误而引起系统故障的情况；
c) 不考虑软件可靠性，假设整个软件系统是完全可靠的；
d) 不考虑硬件表决的可靠性问题，假设硬件表决器是完全可靠的；
e) 每一系在独立失效下的寿命都服从指数分布。

2.3．考虑共因失效的三取二系统的可靠性模型

2.3.1．三取二安全计算机系统结构分析

三取二安全计算机系统结构[11, 12]如下图1所示，系统有三系组成。遵循少数服从多数的原则。工作时，三系会同时进行输入采集， 然后根据相同的输入独立进行数据处理，三系处理完成后同步输出，最终经过硬件表决产生一致性输出作为运算结果。当三系运算结果完全一致时，系统工作在2oo3状态，系统是可靠性的，当三系当中有一系出现故障而导致和其他两系不一致时，此时系统的输出将会和另外两系保持一致，同时三取二安全计算机具有自我诊断的功能，可以定位一系出现故障的问题，从而提醒维修人员进行维修，三系当中如果两系都出现故障，此时只有单机工作，但系统此时不输出而导向故障安全侧。

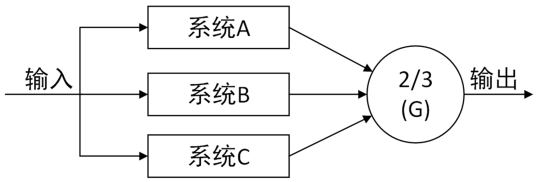

图1 三取二安全计算机系统结构图。

2.3.2．三取二系统的马尔可夫模型

由于传统的三取二系统的每一系是完全相同的，可进一步做如下假设：

a)三系完全相同，一阶失效率为 λ_1，二阶失效率为 λ_2 λ2，三阶失效率为 λ_3，每一系的维修率均是 μ；

b)三系完全一致，服从二项分布。

对状态的定义如下：

状态0表示：系统处于初始状态下，所有模块均正常，没有单元失效，系统工作在三取二模式下；

状态1表示：系统有且仅有一个模块发生故障，系统工作在二取二模式下；

状态2表示：系统有且仅有两个模块发生故障；

状态3表示：系统有三个模块发生故障。

则系统的马尔可夫状态转移如图2所示，

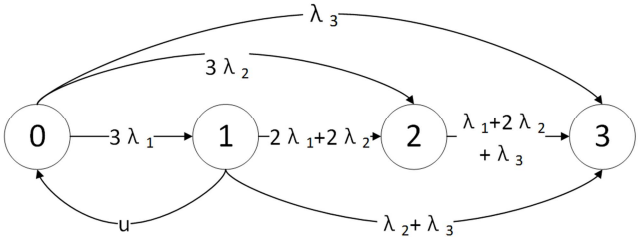

图2 三取二安全计算机系统状态转移图。

对状态转移的解释如下：

状态0->1系统发生独立失效；

状态0->2系统发生二阶失效；

状态0->3系统发生三阶失效；

状态1 ->0系统由单系故障经过维修恢复到三系正常；

状态1->2系统有一系发生独立失效，或者与坏了的一系构成二阶失效；

状态1->3系统出现二阶失效或者三阶失效；

状态2->3系统可能发生一阶，二阶或者三阶失效。

根据状态转移图列出系统的状态转移方程组，如下式

$$\begin{cases} p_{0'}(t) = -(3\lambda_1 + 3\lambda_2 + \lambda_3)p_0(t) + \mu p_1(t) \\ p_{1'}(t) = 3\lambda_1 p_0 - (2\lambda_1 + 3\lambda_2 + \lambda_3 + \mu)p_1(t) \\ p_{2'}(t) = 3\lambda_2 p_0(t) + 2(\lambda_1 + \lambda_2)p_1(t) - (\lambda_1 + 2\lambda_2 + \lambda_3)p_0(t) \\ p_{3'}(t) = \lambda_3 p_0(t) + (\lambda_2 + \lambda_3)p_1(t) + (\lambda_1 + 2\lambda_2 + \lambda_3)p_2(t) \end{cases} \quad (1)$$

其中状态0,1为系统的可靠性工作状态，状态2，3系统的不可靠性状态，则系统的可靠性计算公式为

$$R_t = p_0(t) + p_1(t) \quad (2)$$

2.4．考虑共因失效的二乘二取二系统的可靠性模型

2.4.1．二乘二取二安全计算机系统结构分析

二乘二安全计算机系统结构[13-15]如下图3所示，系统由两系组成，其中每一系都是一个二取二的结构，两系工作在双机热备的方式，其中一系为主系，另一系为备系，正常工作时，主系备系都上电工作，但是只有主系的输出是有效的，每一系都具备故障自检功能，每一系如果检测到自身故障就会发出控制信号，使切换单元切换到另外一系工作。二乘二取二系统具有二取二的高安全性和双机热备的高可靠性特点，同时由于一系可以单独运行，更加便于系统的调试和升级，因此广泛使用在国内的计算机联锁系统中[13]。

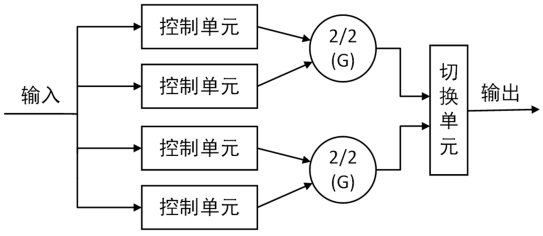

图3 二乘二取二安全计算机系统结构图。

2.4.2．二乘二取二系统的马尔可夫模型

根据对二乘二取二安全计算机系统的结构分析，其状态定义如下：

状态0表示：系统处于初始状态下，所有模块均正常，没有单元失效，此时系统工作在二乘二取二模式下；

状态1表示：系统有且仅有一个模块发生故障，此时系统工作在单系模式下；

状态2表示：系统有且仅有两个模块发生故障，且发生故障的两个模块都在一系， 此时系统工作在单系模式下；

状态3表示：系统有且仅有两个模块发生故障，且发生故障的两个模块一个在主系，另外一个在备系；

状态4表示：系统有且仅有三个模块发生故障；

状态5表示：系统所有模块都发生故障。

则系统的马尔可夫状态转移如图4所示，

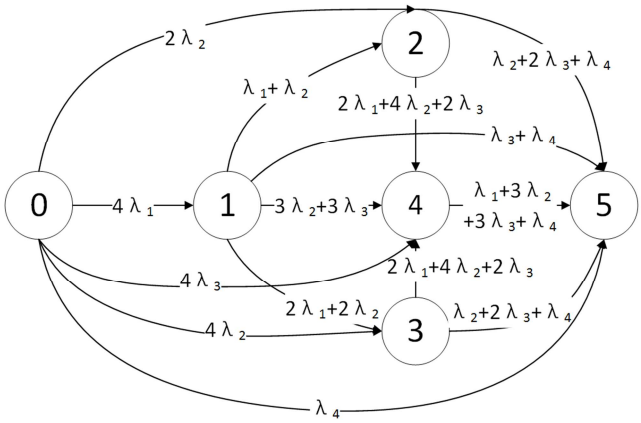

图4 二乘二取二安全计算机系统状态转移图。

由于二乘二取二状态转换概率计算过于复杂，下面给出各转移概率的具体计算：

状态0->1系统发生独立失效；

状态0->2系统发生二阶失效；

状态0->3系统发生二阶失效；

状态0->4系统发生三阶失效；

状态0->5系统发生四阶失效；

状态1->2所在系独立失效或所在系二阶失效；

状态1->3另外一系独立失效或另外一系和本系失效模块二阶失效；

状态1->4剩余三个发生二阶失效或剩余三个和已坏模块发生三阶失效；

状态1->5剩余三个三阶失效或剩余三个和已坏模块发生四阶失效；

状态2->4剩余二个一阶失效或剩余二个和已坏的两个模块发生二阶失效或剩余二个和已坏的两个模块发生三阶失效；

状态2->5剩余二个二阶失效或剩余二个和已坏的两个模块发生三阶失效或剩余二个和已坏的两个模块发生四阶失效；

状态3->4剩余二个一阶失效或剩余二个和已坏的两个模块发生二阶失效或剩余二个和已坏的两个模块发生三阶失效；

状态3->5剩余二个二阶失效或剩余二个和已坏的两个模块发生三阶失效或剩余二个和已坏的两个模块发生四阶失效；

状态4->5剩余一个一阶失效或剩余一个二阶失效或剩余一个三阶失效或剩余一个和已坏模块发生四阶失效。

根据状态转移图列出系统的状态转移方程组，如下式：

$$\begin{cases} p_{0'}(t) = -(4\lambda_1 + 6\lambda_2 + 4\lambda_3 + \lambda_4)p_0(t) + \mu p_1(t) + \mu p_2(t) \\ p_{1'}(t) = 4\lambda_1 p_0(t) - (3\lambda_1 + 7\lambda_2 + 4\lambda_3 + \lambda_4 + \mu)p_1(t) \\ p_{2'}(t) = 2\lambda_2 p_0(t) + (\lambda_1 + \lambda_2)p_1(t) - (2\lambda_1 + 5\lambda_2 + 4\lambda_3 + \lambda_4 + \mu)p_2(t) \\ p_{3'}(t) = 4\lambda_2 p_0(t) + (2\lambda_1 + 2\lambda_2)p_1(t) - (2\lambda_1 + 5\lambda_2 + 4\lambda_3 + \lambda_4)p_3(t) \\ p_{4'}(t) = 4\lambda_3 p_0(t) + (3\lambda_2 + 3\lambda_3)p_1(t) + (2\lambda_1 + 4\lambda_2 + 2\lambda_3 + \lambda_4)(p_2(t) + p_3(t)) - (\lambda_1 + 3\lambda_2 + 3\lambda_3 + \lambda_4)p_4(t) \\ p_{5'}(t) = \lambda_4 p_0(t) + (\lambda_3 + \lambda_4)p_1(t) + (2\lambda_1 + 5\lambda_2 + 4\lambda_3 + \lambda_4)p_2(t) + (\lambda_2 + 2\lambda_3 + \lambda_4)p_3(t) + (\lambda_2 + 3\lambda_2 + 3\lambda_3 + \lambda_4)p_4(t) \end{cases} \tag{3}$$

其中系统的状态0，1，2为系统的可靠运行状态，则系统的可靠性计算公式为

$$R_t = p_0(t) + p_1(t) + p_2(t) \tag{4}$$

3．仿真分析

3.1．系统的各阶失效率计算

为方便后续分析给出三取二系统各阶失效率的计算公式，二乘二取二系统计算方式类似，这里不再赘述。

针对于一个三取二系统的失效率，假设在时间t内系统出现了n_1次系统独立失效，n_2次二阶失效，n_3次三阶失效，根据文献[7]，那么系统的各阶失效率的计算公式为

$$\begin{cases} \lambda_1 = \dfrac{n_1}{t} / \dbinom{1}{3} \\ \lambda_2 = n_2 / t / \dbinom{2}{3} \\ \lambda_3 = n_3 / t / \dbinom{3}{3} \end{cases} \tag{5}$$

3.2．维修率对系统的可靠性的影响

不失一般性，假设系统的各阶失效率分别为$\lambda_1 = 10^{-5}$，$\lambda_2 = 2*10^{-6}$，$\lambda_3 = 10^{-6}$，$\lambda_4 = 0$维修率分别取0，0.001，0.003，0.006，0.01不同值时进行三取二安全计算机系统和二乘二取二安全计算机系统可靠性计算，其结果如下图5图6所示

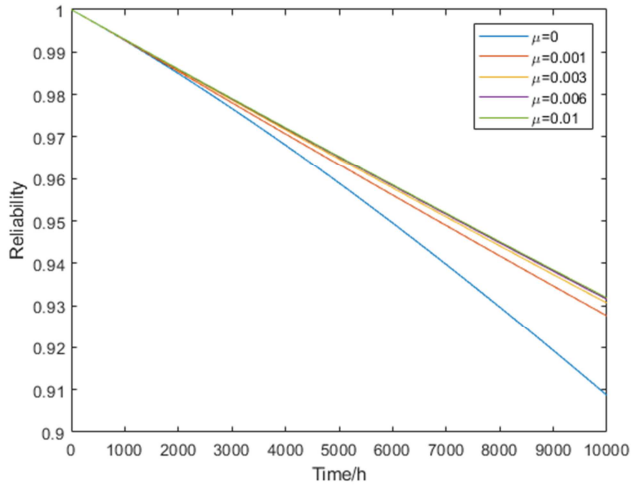

图5 三取二安全计算机系统维修率不同时系统的可靠性曲线。

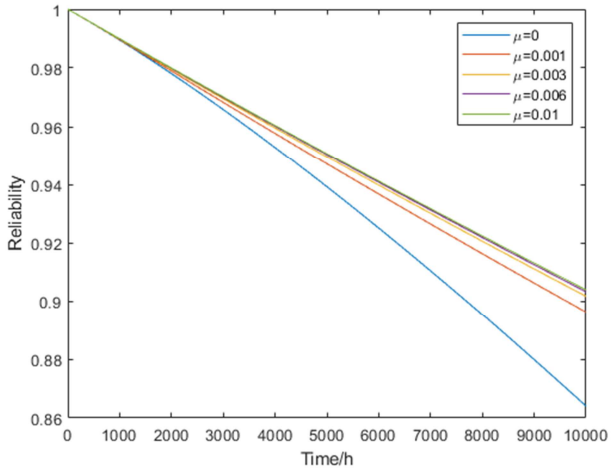

图6 二乘二取二安全计算机系统维修率不同时系统的可靠性曲线。

通过比较维修率μ取不同值时系统得可靠性曲线，可以发现，不论是三取二还是二乘二取二系统，相对于没有维修率的系统，有维修率系统的可靠性显著提高且可靠性受时间的影响减小、维修率越高系统的可靠性越高，但是当继续增加维修率时（如维修率大于0.06时），维修率对系统得可靠性影响将变得十分缓慢。

3.3．共因失效率对系统的可靠性的影响

假设系统在一定的时间(100000h)内失效的总次数保持不变，但出现各阶失效的次数不同，各阶的失效次数为如下表1中数据，并以此来计算系统的各阶失效率，同时取维修率$\mu = 0.01$，分别对三取二安全计算机系统和二乘二取二安全计算机系统可靠性计算，其结果如下图7图8所示：

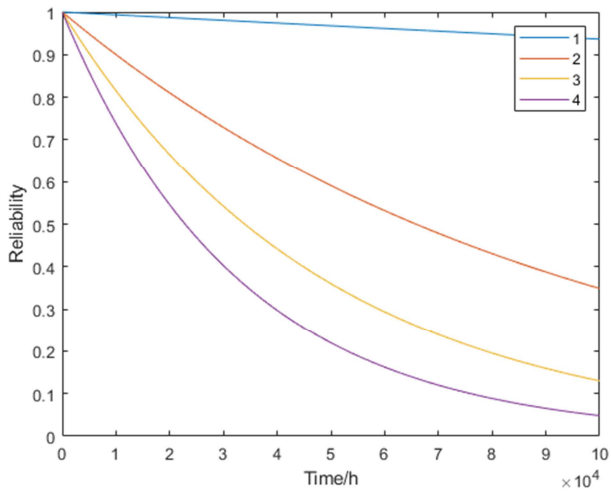

图7 三取二安全计算机系统共因失效率不同时系统的可靠性曲线。

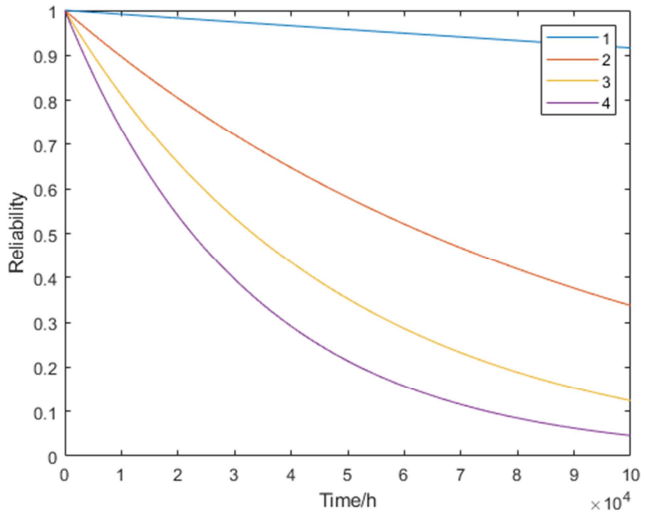

图8 二乘二取二安全计算机系统共因失效率不同时系统的可靠性曲线。

表1 各阶失效次数。

编号	一阶失效次数	二阶失效次数	三阶四阶失效次数
1	10	0	0
2	9	1	0
3	8	2	0
4	7	3	0

观察图7和图8，不难得出，不论是三取二系统还是二乘二取二系统，不考虑共因失效计算的可靠性是偏高的，共因失效率的增加都会导致系统的可靠性下降，而文献[7]指出共因失效是冗余系统失效和设备不可用的主要原因，因此在安全苛求领域分析系统可靠性时不能忽略共因失效对系统造成的影响。

3.4．三取二和二乘二取二系统的可靠性对比分析

取 $\mu = 0.001$，$\lambda_1 = 10^{-5}$，$\lambda_2 = 2*10^{-6}$，$\lambda_3 = 10^{-6}$，$\lambda_4 = 0$ 计算系统的可靠性得到如下曲线：

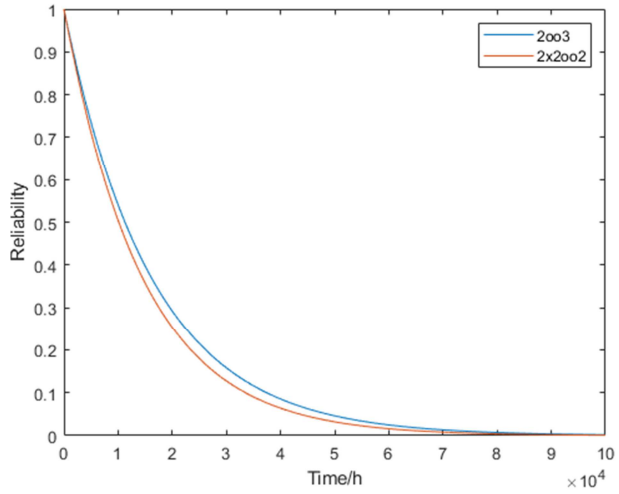

图9 三取二和二乘二安全计算机系统的可靠性曲线

虽然三取二和二乘二安全计算机系统的可靠性都是随着时间下降，但在各系参数相同以及维修率相同的情况下通过仿真结果可以看出三取二安全计算机系统的可靠性是一直高于二乘二取二的，因此研究三取二安全计算机对提高安全苛求系统具有重要的意义。

4．结论

本文利用马尔可夫过程首先建立了三取二安全计算机系统和二乘二安全计算机系统的可靠性模型，通过Matlab的ode45函数对其求解仿真通过分析得出以下结论：

不论是三取二安全计算机系统还是二乘二安全计算机系统，维修率都会提高系统的可靠性，但随着维修率的增加对系统的可靠性提升变得缓慢,随着系统的共因失效的概率增加，系统的可靠性都会大大降低；系统的差异化会导致共因失效率下降，可以提高系统的可靠性,在仅考虑共因失效和维修率的前提下，三取二安全计算机的可靠性要略高于二乘二取二安全计算机，这为后续差异化安全计算机的设计提供了理论支撑。

因此针对一些可靠性要求较高的场合，比如时速高达600公里的高速磁浮的运行控制系统，由于维修率对系统的可靠性提升不再明显，现有同构的安全计算机系统可能已经满足不了系统的要求。通过分析，降低共因失效可提高系统的可靠性，而采用差异化的安全计算机系统作为降低共因失效率的一种实现方式，可以进一步提高系统的可靠性，更加适合长大干线高速磁浮的运控系统。

致谢

本文为科技部项目《高速磁浮运行控制系统关键技术研究及装备研制》(2016YFFB200602-26)的阶段性成果之一。

参考文献

[1] 涂娟,朱骞,张璐.一种通用三取二安全计算机平台设计[J].信息化研究,2017,43(05):42-45.

[2] 马权,罗琦,宋小明,刘艳阳.数字化安全级DCS紧急停堆系统共因失效分析[J].核动力工程,2018,39(03):95-99.

[3] 员春欣, 江建慧.安全关键计算机系统[M].北京:中国铁道出版社, 2003, 154-156.

[4] 马小玲,张友鹏,杜求茂,郑伟.计算机联锁系统的可靠性和安全性比较[J].铁路计算机应用,2009,18(06):46-49.

[5] K. Mallikarjunudu, G. Venkatarami Reddy, Reliability analysis of Shared Load K Out of n: G System in the Presence of Non Lethal Common Cause Shock Failures,Journal of Computer and Mathematical Science, Volume 9, 2018, Pages 6-10.

[6] Jose E. Ramirez-Marquez, David W. Coit, Optimization of system reliability in the presence of common cause failures, Reliability Engineering & System Safety, Volume 92, 2007, Pages 1421-1434.

[7] 王学敏,谢里阳,周金宇.考虑共因失效的系统可靠性模型[J].机械工程学报,2005(01):24-28.

[8] 李春洋,陈循,易晓山,陶俊勇.基于马尔可夫过程的k/n(G)系统共因失效分析[J].系统工程与电子技术,2009,31(11):2789-2792.

[9] J.K. Vaurio, Common cause failure probabilities in standby safety system fault tree analysis with testing-scheme and timing dependencies Reliab Eng Syst Saf, 79, 2003, Pages 43-57.

[10] 张舟洋,李华,魏念龙.基于 贝叶斯网络的城市轨道交通CBTC系统SIL研究[J].铁道标准设计,2015,59(04):121-124.

[11] 陈州,倪明.三模冗余系统的可靠性与安全性分析[J].计算机工程,2012,38(14):239-241+245.

[12] 刘真.一种三取二安全计算机系统的设计与实现[J].铁路计算机应用,2016,25(11):49-52.

[13] 张永贤,邹力棒,吴文杰,廖肇聪.二乘二取二系统的一种新降级策略研究[J].华东交通大学学报,2017,34(05):99-105.

[14] 张佳楠,王海峰,蒋大明.计算机联锁系统二乘二取二容错结构分析[J].铁路计算机应用,2006(11):46-49.

[15] 黄鲁江,雷烨.基于Markov过程的二乘二取二计算机联锁系统的可靠性和安全性分析[J].铁路通信信号工程技术,2017,14(05):1-4+17.