高速铁路智能 CTC 自律机系统的可靠性与安全性评估

陈 峰[1,2] 袁志明[1,2] 闫 璐[1] 许 伟[1] 苗义烽[1] 高博文[1]

摘 要 自律机系统是智能调度集中控制 (Centralized traffic control, CTC) 系统的核心, 其安全性和可靠性都至关重要. 首先分析了双机热备自律机系统和二乘二取二自律机系统的结构及工作原理; 然后综合考虑自律机分机的故障检出率和故障发生率等因素, 采用 Markov 模型, 构建了两个系统的安全度和可靠度模型. MATLAB 仿真结果表明, 双机热备自律机系统的可靠性高于二乘二取二自律机系统的, 但双机热备自律机系统的安全度远低于二乘二取二自律机系统的, 因此二乘二取二自律机系统更能保障 CTC 系统的安全.

关键词 铁路运输, 高速铁路, 智能调度集中控制, 自律机系统, 可靠性, 安全性

引用格式 陈峰, 袁志明, 闫璐, 许伟, 苗义烽, 高博文. 高速铁路智能 CTC 自律机系统的可靠性与安全性评估. 自动化学报, 2020, **46**(3): 463−470

DOI 10.16383/j.aas.c190195

Reliability and Safety Evaluation of Autonomous Computer System of Intelligent CTC in High Speed Railway

CHEN Feng[1,2] YUAN Zhi-Ming[1,2] YAN Lu[1] XU Wei[1] MIAO Yi-Feng[1] GAO Bo-Wen[1]

Abstract Autonomous computer system is the core of the intelligent centralized traffic control (CTC) system, and its safety and reliability are very important. Firstly, the structure and working principle of the dual computer hot standby autonomous system and the double 2-vote-2 autonomous system are analyzed; Then, the factors such as error detection rate and failure rate are considered. Next, combined with the Markov model, the safety and reliability model of two systems are established. MATLAB simulation results show that the reliability of the dual computer hot standby autonomous system is higher than that of the double 2-vote-2 autonomous system, but the safety of the dual computer hot standby autonomous system is much lower than that of the double 2-vote-2 autonomous system, so the double 2-vote-2 autonomous system can guarantee the security of CTC system more.

Key words Railway transportation, high-speed railway, intelligent centralized traffic control (CTC), autonomous computer system, reliability, safety

Citation Chen Feng, Yuan Zhi-Ming, Yan Lu, Xu Wei, Miao Yi-Feng, Gao Bo-Wen. Reliability and safety evaluation of autonomous computer system of intelligent CTC in high speed railway. *Acta Automatica Sinica*, 2020, **46**(3): 463−470

高速铁路智能调度集中控制 (Centralized traffic control, CTC) 系统是结合我国 “智能高速铁路” 的发展需求, 采用云计算、物联网、大数据和人工智能等先进技术, 通过信息的全面感知、安全传输、融合处理和科学决策, 构建的具有模式标准化、局站调控一体化、监视综合化、决策智能化、控制自主化的先进智能行车调度系统. 智能调度集中控制系统 (智能 CTC) 由包括铁路总公司、铁路局、车站的三层 CTC 子系统构成, 其中车站子系统为整个高速铁路网络的基本功能节点, 不仅具有调度中心与高速列车之间的指令传输功能, 还有车站调车作业的执行功能.

车站自律机系统是智能 CTC 的核心设备, 主要完成列车跟踪、自动排路、分散自律逻辑检查、外部系统接口以及控制指令输出等功能. 调度集中系统与计算机联锁系统的通讯, 是通过车站自律机与操作表示机进行交叉互联实现的. 车站自律机系统将调度中心的调整计划和直接操作指令, 以及车站

收稿日期 2019-03-20 录用日期 2019-12-08
Manuscript received March 20, 2019; accepted December 8, 2019
国家自然基金项目高铁联合基金 (U1834211), 中国国家铁路集团有限公司科技研究开发计划课题 (J2019G015, N2019G020), 中国铁道科学研究院集团有限公司科研课题 (2019YJ066, 2019YJ071) 资助
Supported by National Natural Science Foundation of China (U1834211), Science and Technology Project of China National Railway Group Corporation Limited (J2019G015, N2019G020), and Science and Technology Project of China Academy of Railway Sciences Corporation Limited (2019YJ066, 2019YJ071)
本文责任编委 董海荣
Recommended by Associate Editor DONG Hai-Rong
1. 中国铁道科学研究院集团有限公司通信信号研究所, 北京 100081 2. 国家铁路智能运输系统工程技术研究中心, 北京 100081
1. Signal and Communication Research Institute, China Academy of Railway Sciences Corporation Limited, Beijing 100081
2. National Research Center of Railway Intelligence Transportation System Engineering Technology, Beijing 100081

值班员的直接操作指令, 经检测无冲突后适时发给车站联锁机系统执行, 因此具有生成进路操作命令和将指令变为命令的功能. 目前, 为了保证控制指令的唯一性, 当自律机系统进行进路选排、进路触发等工作时, 被控对象同一时刻只能接收到一台自律机的指令, 这也是自律机系统双机热备的主要工作方式[1]. 所以为了保证系统的可靠性, 必须保证自律机和实现自律机之间切换的倒机装置可靠性.

双机热备是指同时执行两台设备, 设备之间相互备份, 共同保证重要服务执行的方式. 当某台设备发生故障时, 由第二台设备自动接替前者继续任务, 保证了缺乏人工干预情况下, 系统能继续执行任务[2]. 因为在可靠性和安全性上优势, 双机热备已经在农业、交通运输业、工业等领域得到广泛应用[3−9]. 例如在铁路方面, 王江江等[10] 结合故障比较机制和同步机制, 为铁路信号设备的双机热备切换提供指导; 闫剑平等[11] 通过 Markov 模型, 对铁路信号常用双机热备结构进行安全性和可靠性进行分析; 胡爱锋等[12] 综合分析以往道岔驱动系统的应用情况, 认为今后控制系统将会朝着硬件热备冗余控制系统的方向发展; 王秀娟[13] 根据倒机优先级和原则, 制定调度集中系统中双机热备的实施方案; 孙蕾等[14] 和刘芳等[15] 考虑到实际情况, 对双机热备计算机联锁控制系统的安全性和可靠性进行了分析; 文俊等[16] 对铁路信号中在线诊断、故障模式和共因失效等多个因素进行了综合分析, 提出了两种不同的双机热备结构的同构 Markov 模型; 李军丽等[17] 针对双机热备和二乘二取二的计算机联锁系统, 构建了危险失效概率和安全失效概率的动态故障树模型; Kumar 等[18] 针对具有双环拓扑的局域网, 提出了一种可用于分布式铁路信号系统的容错节点转换器; Kim 等[19] 基于 MC68000 研发的一种二乘二取二系统, 可直接用于飞机、高速铁路等嵌入式控制系统.

从国内外研究可以发现, 铁路方面的双机热备系统结构及其功能的研究主要集中在通信信号和计算机联锁控制系统领域, 对于车站自律机系统的研究则较少, 尤其对自律机系统的结构及其安全性和可靠性的研究, 目前还处于探索阶段. 为了比较不同系统结构对车站自律机系统功能的影响, 本文将通过 Markov 过程对 CTC 车站自律机系统结构的安全性和可靠性进行分析, 以期为未来的车站自律机系统设计提供参考.

1 自律机系统的结构及工作原理

双机热备自律机系统与外部装置连接协同工作是通过双机冗余的方式进行的, 是由一个切换单元和两台完全相同的自律机组成. 一般情况下, 两台自律机执行完全相同的任务、处理相同的数据, 其中一台自律机会被切换单元指定为主机. 为了保证系统运行正常, 当被选定的主机发生故障时, 切换单元会向另一台自律机发出切换信号, 将其切换成主机. 双机热备自律机系统的结构如图 1所示, 其中每台自律机都由驱动、主机和采集控制系统组成, 能对自身系统进行诊断, 完成故障检测.

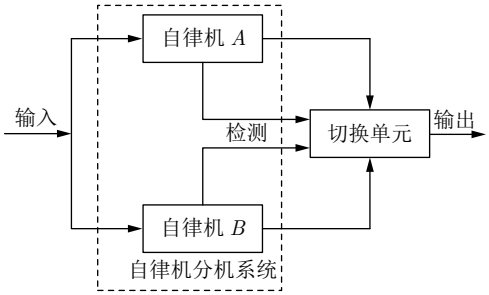


图 1 双机热备自律机系统结构图

Fig. 1 The structure of double hot standby autonomous computer system

新一代自律机系统采用二乘二取二结构, 具体如图 2 所示, 二乘是指两个比较子系统, 二取二是指每个比较子系统上均有两个处理器单元, 并且两个处理器单元执行完全相同的任务, 一旦两个处理器单元的运算结果存在差异, 系统就会出现 “错误” 的警告提示, 拒绝输出指令信息. 与双机热备系统相比, 二乘二取二系统较为显著的特征是多了两个比较器, 有助于提高系统安全性, 但是同时增加了系统的软硬件成本, 因此, 二乘二取二系统的比较器大多采用成品或半成品模式[20−21].

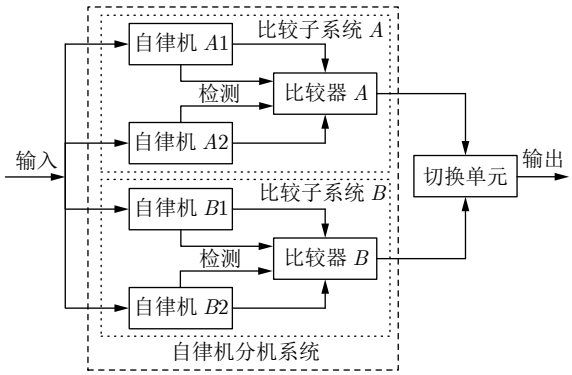


图 2 二乘二取二自律机系结构图

Fig. 2 The structure of double 2-vote-2 autonomous computer system

切换单元由一组安全互斥继电器和两个独立的切换板组成, 主要用于切换两台自律机 (或两个比较子系统) 的通信与热备及其接口设备的通道. 其

中安全互斥继电器由来自两个不同机笼的输出信号驱动, 确保两台自律机状态的相互排斥, 并最终实现单机状态下的故障切换.

2　铁路系统的 RAMS 管理

对于铁路交通车辆系统而言, RAMS (Reliability, availability, maintainability, safety) 代表了系统的可靠性、可用性、可维修性和安全性[22]. 是目前国内外铁路行业最为常用的质量管理评价标准, 涉及到系统全寿命周期的各个阶段[23]. 在 RAMS 的四个要素中, R 关注的是系统故障及故障发生的可能性, 重点评价故障对系统功能的影响, 常用可靠度来衡量; A 关注的是故障预防及故障修复的能力, 常用维修时间来衡量; M 关注的是系统处于可用状态的能力, 常用可用时间与总时间的比值来衡量; S 关注的是危险及危险发生的可能性, 常用安全度来衡量.

铁路交通车辆系统在运行时, RAMS 的四个要素往往相互关联, 其中 R 和 S 作为系统运转过程中所表现出来的两种故障状态, 将对系统性能产生不同的影响. 图 3 为铁路系统故障产生及其影响的示意图, 由于受到系统内部及外界环境的干扰, 系统会出现部分功能下降或丧失的故障状态, 进而影响系统的可靠性, 但是并不是所有的故障都会带来危险, 也就是通常所示的具有危害性的事件或者事故, 因此, 只有某些特定的故障才会影响系统的安全性.

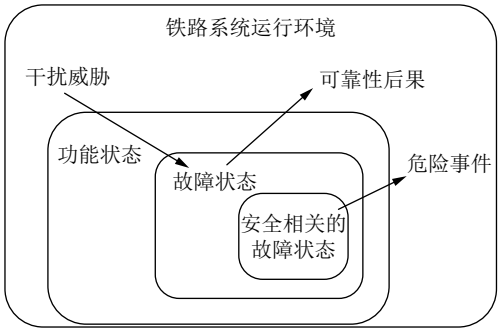


图 3　铁路系统故障的产生及其影响

Fig. 3　Faults of railway system and their influences

3　自律机系统的 R 和 S 建模

3.1　条件假设

由于双机热备系统实现了故障的隔离, 使得单台自律机系统的失效并不会带来人员伤亡或财产损失等危害, 进而影响系统安全性, 但是增加了故障发生的概率, 进而影响系统的可靠性. 因此, 只有对自律机系统的故障模式进行研究, 并建立相应的模型, 才能对自律机系统的安全性和可靠性进行分析.

铁路系统风险具有很大的模糊性和随机性[24], 分析铁路系统故障也成为了一个动态变化的随机过程. 近年来, Markov 模型作为一种常用的随机动态系统分析方法而日益受到国内外的关注[25−27]. 为方便建模过程, 本文对自律机系统的运行作出以下假设:

1) 所有自律机在初始化时均能正常工作, 系统运行状况良好;

2) 某一时刻只能有一台自律机出现故障;

3) 所有自律机故障的检出率 c 均相同;

4) 当故障被检测出来时, 故障处理不会出现错误, 系统始终导向安全状态;

5) 所有自律机仅存在两种状态: 故障与非故障, 并且故障率 λ 相同;

6) 所有自律机在出现故障后, 均不可维修;

7) 自律机系统的其他元器件, 包括切换单元、比较器、借口电路等完全可靠.

3.2　双机热备自律机系统的 R 和 S 建模

根据图 1 所示的结构及工作原理, 对双机热备自律机系统的 5 种状态作表 1 所示的定义及说明.

表 1　双机热备自律机系统的状态定义及解释说明

Table 1　Definition and explanation of double hot standby autonomous computer system state

状态定义	状态解释说明
状态 0	两台自律机均未发生故障, 系统处于正常工作状态.
状态 1	两台自律机中有且仅有一台自律机出现故障并且可测, 系统处于降级工作状态.
状态 2	两台自律机中的工作主机正常, 热备分机发生故障并且不可测, 系统处于降级工作状态.
状态 3	两台自律机均出现故障并且可测, 系统处于故障—安全状态.
状态 4	两台自律机中的工作主机出现故障并且不可测, 系统危险状态.

将表 1 中的 5 种状态转换为图 4 所示的 Markov 模型, 不同状态之间转换的相应描述如下:

1) 状态 0→状态 1: 对于两台均未发生故障的自律机, 当其中一台发生故障并可测时, 另外一台自律机将继续正常工作, 并且处于单独工作状态; 对于已经发生故障的自律机, 系统将会自动隔离.

2) 状态 0→状态 2: 对于两台均未发生故障的自律机, 当热备自律机发生故障并且不可测时, 主自律机的工作不受影响, 系统仍然继续正常工作.

3) 状态 0→状态 4: 对于两台均未发生故障的自律机, 当热备自律机正常, 但是正在工作的主自律机发生故障并且不可测时, 系统将无法实现自律

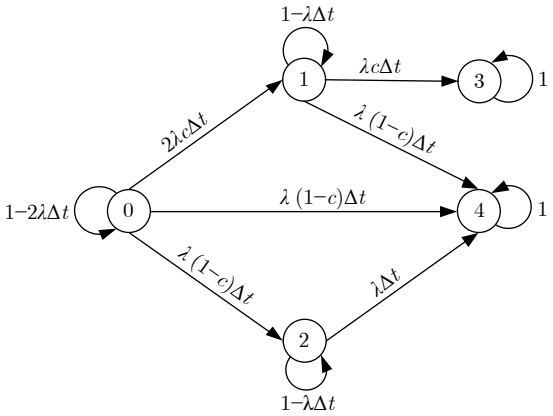


图 4 双机热备自律机系统的状态转移图

Fig. 4 The state transition diagram of double hot standby autonomous computer system

机之间的切换, 进而由正常工作状态转入危险状态.

4) 状态 1→状态 3: 对于仅有一台自律机正常工作的状态, 当工作自律机发生故障并可测时, 整个系统都无法正常工作, 进而由降级工作状态转入故障—安全状态.

5) 状态 1→状态 4: 对于仅有一台自律机正常工作的状态, 当正常自律机发生故障并且不可测时, 整个系统都无法正常工作, 并且可能导致事故的发生, 进而由降级工作状态转入危险状态.

6) 状态 2→状态 4: 对于工作自律机正常, 热备自律机发生故障并且不可测的状态, 当工作自律机出现故障并且不可测时, 整个系统都将无法正常工作, 进而由降级工作状态转入危险状态.

根据图 4 所示的状态转移及其描述, 得到式 (1) 所示的微分方程组.

$$\begin{cases} P_0^{'}(t) = -2\lambda P_0(t) \\ P_1^{'}(t) = 2\lambda c P_0(t) - \lambda P_1(t) \\ P_2^{'}(t) = \lambda(1-c)P_0(t) - \lambda P_2(t) \\ P_3^{'}(t) = \lambda c P_1(t) \\ P_4^{'}(t) = \lambda(1-c)P_0(t) + \lambda(1-c)P_1(t) + \\ \qquad \lambda P_2(t) \end{cases} \tag{1}$$

假设方程 (1) 初始条件 $P_0(0)=1$, $P_1(0)=P_2(0)=P_3(0)=P_4(0)=0$, 利用 MATLAB 求解, 5 种状态在 t 时刻的概率为

$$\begin{cases} P_0(t) = \mathrm{e}^{-2\lambda t} \\ P_1(t) = 2c(\mathrm{e}^{-\lambda t} - \mathrm{e}^{-2\lambda t}) \\ P_2(t) = (1-c)(\mathrm{e}^{-\lambda t} - \mathrm{e}^{-2\lambda t}) \\ P_3(t) = c^2(1 - 2\mathrm{e}^{-\lambda t} + \mathrm{e}^{-2\lambda t}) \\ P_4(t) = (2c+1)(c-1)\mathrm{e}^{-\lambda t} + \\ \qquad c(1-c)\mathrm{e}^{-2\lambda t} + 1 - c^2 \end{cases} \tag{2}$$

结合式 (2) 和表 1 的状态定义, 双机热备自律机系统的可靠度 $R_1(t)$ 和安全度 $S_1(t)$ 分别为

$$R_1(t) = P_0(t) + P_1(t) + P_2(t) = (1+c)\mathrm{e}^{-\lambda t} - c\mathrm{e}^{-2\lambda t} \tag{3a}$$

$$S_1(t) = P_0(t) + P_1(t) + P_2(t) + P_3(t) = (1+2c)(1-c)\mathrm{e}^{-\lambda t} - c(1-c)\mathrm{e}^{-2\lambda t} + c^2 \tag{3b}$$

3.3 二乘二取二自律机系统的 R 和 S 建模

根据图 2 所示的结构及工作原理, 对二乘二取二自律机系统的 5 种状态作表 2 所示的定义及说明.

表 2 二乘二取二自律机系统的状态定义及解释说明

Table 2 Definition and explanation of double 2-vote-2 autonomous computer system state

状态定义	状态解释说明
状态 0	四台自律机均未发生故障, 系统处于正常工作状态.
状态 1	两个比较子系统中, 其中一个子系统中的一台自律机出现故障并且可测, 系统处于降级工作状态.
状态 2	两个比较子系统中, 其中一个子系统中的一台自律机出现故障并且不可测, 系统处于降级工作状态.
状态 3	两个比较子系统中, 其中一个子系统中的两台自律机均出现故障, 系统处于降级工作状态.
状态 4	两个比较子系统都出现故障, 系统处于故障—安全状态.

将表 2 中的 5 种状态转换为图 5 所示的 Markov 模型, 不同状态之间转换的相应描述如下:

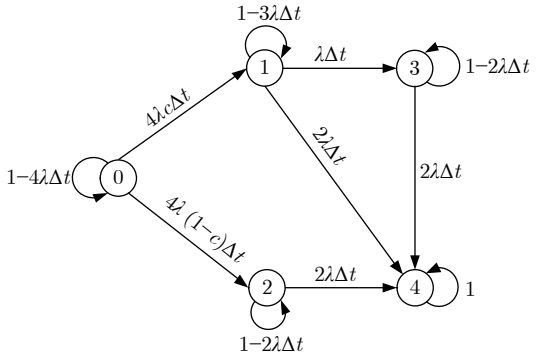


图 5 二乘二取二自律机系统的状态转移图

Fig. 5 The state transition diagram of double 2-vote-2 autonomous computer system

1) 状态 0→状态 1: 对于四台均未发生故障的自律机, 当其中一台自律机出现故障并且可测时, 对应的比较子系统被隔离, 另一比较子系统继续工作, 整个系统由正常工作状态转入降级工作状态.

2) 状态 0→状态 2: 对于四台均未发生故障的自律机, 当其中一台自律机出现故障并且不可测时,

根据比较器判断出对应的比较子系统存在故障, 可以将其隔离, 所有工作由另一个比较子系统完成, 整个系统由正常工作状态转入降级工作状态.

3) 状态 1→状态 3: 对于其中一个比较子系统中一台自律机出现故障并且可测的工作状态, 当该比较子系统中的另一个自律机也出现故障时, 可以将其隔离, 所有工作由另一个比较子系统完成, 整个系统仍然处于降级工作状态.

4) 状态 1、状态 2、状态 3→状态 4: 对于其中一个比较子系统出现故障并且已经隔离的工作状态, 当另一正常工作的比较子系统发生故障时, 整个系统将由降级工作状态转入故障—安全状态.

根据图 5 所示的状态转移及其描述, 得到式 (4) 所示的微分方程组.

$$\begin{cases} P_0'(t) = -4\lambda P_0(t) \\ P_1'(t) = 4\lambda c P_0(t) - 3\lambda P_1(t) \\ P_2'(t) = 4\lambda(1-c)P_0(t) - 2\lambda P_2(t) \\ P_3'(t) = \lambda P_1(t) - 2\lambda P_3(t) \\ P_4'(t) = 2\lambda P_1(t) + 2\lambda P_2(t) + 2\lambda P_3(t) \end{cases} \tag{4}$$

假设方程 (4) 初始条件 $P_0(0)=1$, $P_1(0)=P_2(0)=P_3(0)=P_4(0)=0$, 利用 MATLAB 求解, 5 种状态在 t 时刻的概率为

$$\begin{cases} P_0(t) = \mathrm{e}^{-4\lambda t} \\ P_1(t) = 4c(\mathrm{e}^{-3\lambda t} - \mathrm{e}^{-4\lambda t}) \\ P_2(t) = 2(1-c)(\mathrm{e}^{-2\lambda t} - \mathrm{e}^{-4\lambda t}) \\ P_3(t) = 2c\left(\mathrm{e}^{-2\lambda t} - 2\mathrm{e}^{-3\lambda t} + \mathrm{e}^{-4\lambda t}\right) \\ P_4(t) = 1 - 2\mathrm{e}^{-2\lambda t} + \mathrm{e}^{-4\lambda t} \end{cases} \tag{5}$$

结合式 (5) 和表 2 的状态定义, 二乘二取二自律机系统的可靠度 $R_2(t)$ 和安全度 $S_2(t)$ 分别为

$$R_2(t) = P_0(t) + P_1(t) + P_2(t) + P_3(t) = 2\mathrm{e}^{-2\lambda t} - \mathrm{e}^{-4\lambda t} \tag{6a}$$

$$S_2(t) = 1 \tag{6b}$$

对比式 (3b) 和式 (6b) 可以看出, 二乘二取二自律机系统并不存在双机热备自律机系统所出现的危险状态, 这是由于前者增加了可靠性极高 (本文假定为完全可靠) 的比较器的缘故.

4　实例分析

对于与安全相关的装置, SIL 是全世界广泛认可的方法. SIL 认证分为 4 个等级, SIL1、SIL2、SIL3、SIL4, 其中 SIL4 要求最高, 并且针对铁路或轨道交通类的产品、控制系统等, 一般都会要求 SIL4 认证.

为了比较双机热备自律机系统和二乘二取二自律机系统的安全性和可靠性, 参考 IEC 61508 和 EN 50129 所强加的 SIL 认证, 对 $0\sim2\times10^9$ h 的时间段内的两个系统的安全度和可靠度进行仿真实验. 参考中国铁道科学研究院、卡斯柯信号有限公司、北京全路通信信号研究设计院有限公司、广州铁路 (集团) 公司等单位共同完成的《调度集中系统 (CTC) 安全可靠性研究 (2014X004-C)》课题, 自律机的故障检出率 $c=0.9$, 故障率 $\lambda=2.5\times10^{-9}$/h 或 7.5×10^{-9}/h . 两个系统的可靠度和安全度比较分别见图 6 和图 7. 当仿真时间分别取 $t=5\times10^7$ h 和 1×10^8 h 的情况下, 对应故障率情况下的可靠度和安全度比较见表 3.

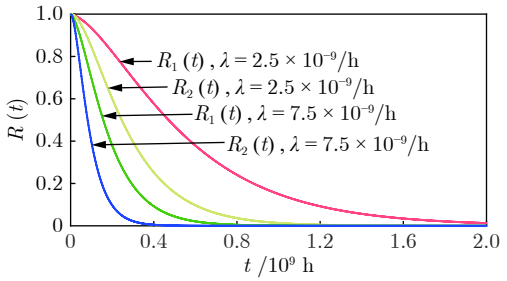


图 6　两个系统的可靠度比较

Fig. 6　Reliability comparison of the two systems

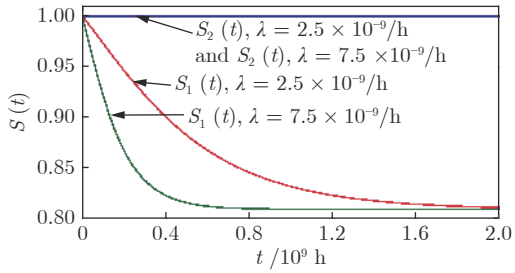


图 7　两个系统的安全度比较

Fig. 7　Safety comparison of the two systems

从图 6 可以看出, 在相同的故障率下, 双机热备系统的可靠度始终高于二乘二取二系统的可靠度, 并且随着时间的增加, 两者之间的差异率会加大; 在相同的仿真时间下, 双机热备系统的可靠度仍然高于二乘二取二系统的可靠度, 并且随故障率的增大, 两者之间的差异率也会加大. 例如, 当 $t=5\times10^7$ h 时, 与双机热备系统相比, 二乘二取二系统的 R 在 $\lambda=2.5\times10^{-9}$/h 和 $\lambda=7.5\times10^{-9}$/h 的情况下分别下降了 2.53 % 和 18.07 %; 当 $t=1\times10^8$ h 时, 与双机热备系统相比, 二乘二取二系统的 R 在 $\lambda=2.5\times10^{-9}$/h 和 $\lambda=7.5\times10^{-9}$/h 的情况下分别下降了 9.49 % 和 43.09 %.

从图 7 可以看出, 在相同的故障率下, 双机热

表 3 不同仿真时间和故障率下的安全度和可靠度比较

Table 3 The degree of reliability and safety at different failure rates and times

仿真时间t (h)	故障率 λ (h^{-1})	可靠度R (%)			安全度S (%)		
		R_1	R_2	$\frac{R_2-R_1}{R_1}$	S_1	S_2	$\frac{S_2-S_1}{S_1}$
5.0×10^7	2.5×10^{-9}	97.58	95.11	−2.53	98.70	100.00	1.32
5.0×10^7	7.5×10^{-9}	88.07	72.16	−18.07	95.99	100.00	4.18
1.0×10^8	2.5×10^{-9}	93.38	84.52	−9.49	97.35	100.00	2.72
1.0×10^8	7.5×10^{-9}	69.67	39.65	−43.09	92.22	100.00	8.44

备系统的安全度远远低于二乘二取二系统的安全度, 并且随着时间的增加, 两者之间的差异率会加大; 在相同的仿真时间下, 双机热备系统的安全度仍然低于二乘二取二系统的安全度, 并且随故障率的增大, 两者之间的差异率也会加大. 例如, 当 $t=5\times10^7$ h 时, 与双机热备系统相比, 二乘二取二系统的 S 在 $\lambda=2.5\times10^{-9}$/h 和 $\lambda=7.5\times10^{-9}$/h 的情况下分别上升了 1.32% 和 4.18%; 当 $t=1\times10^8$ h 时, 与双机热备系统相比, 二乘二取二系统的 R 在 $\lambda=2.5\times10^{-9}$/h 和 $\lambda=7.5\times10^{-9}$/h 的情况下分别下降了 2.77% 和 8.44%.

5 结论

目前, 智能 CTC 系统的关键设备大多采用双机热备方式, 包括车务终端、车站自律机和 CTC 中心服务器等[2]. 本文利用 Markov 模型, 构建了两种不同的系统结构车站自律机的安全性和可靠性计算模型. 实例表明:

1) 除了自律机系统的结构之外, 故障检出率和自律机故障率等因素也会影响车站自律机系统的安全度和可靠度.

2) 二乘二取二自律机系统与双机热备自律机系统相比, 可靠性较低, 但安全性较高.

3) 如何设计一种兼具安全性和可靠性的自律机系统, 将是未来的重要研究工作.

References

1 Chen Xian-Feng, Wang Zhong-Wei. The design and implementation of the double hot standby machine of autonomous machine. *Railway Signaling and Communication Engineering*, 2015, **12**(4): 86–87
(陈显锋, 王忠卫. 自律机双机热备倒机装置的设计与实现. 铁路通信信号工程技术, 2015, **12**(4): 86–87)

2 China Railway Corporation. Decentralized and autonomous CTC system. *Beijing: China Railway Publishing House*, 2014, 76–80
(中国铁路总公司. 分散自律调度集中系统. 北京: 中国铁道出版社, 2014, 76–80)

3 Samet R. Recovery device for real-time dual-redundant computer systems. *IEEE Transactions on Dependable and Secure Computing*, 2011, **8**(3): 391–403

4 Shi Wen-Lu, Hu Ping. The research and improvement in duplex hot-backup system. *Microprocessors*, 2008, **29**(3): 180–182
(史文路, 胡平. 双机热备份系统的研究与改进. 微处理机, 2008, **29**(3): 180–182)

5 Li Jie, Shen Rui. Analysis and comparison of reliability of computer redundancy architecture in space. *Journal of Deep Space Exploration*, 2018, **5**(6): 575–581
(李杰, 沈锐. 空间计算机冗余架构可靠性分析比较. 深空探测学报, 2018, **5**(6): 575–581)

6 Sun Guang-Lu, Zhang Luo-Shi, Xue Yi-Bo. Straw resource mass storage system's design and implementation. *Journal of Computer Research and Development*, 2011, **48**(S1): 78–83
(孙广路, 张洛什, 薛一波. 秸秆资源海量存储系统的设计与实现. 计算机研究与发展, 2011, **48**(S1): 78–83)

7 Park K, Kim S. Availability analysis and improvement of active/standby cluster systems using software rejuvenation. *Journal of Systems and Software*, 2002, **61**(2): 121–128

8 Mukherjee A, Dhar A S. Real-time fault-tolerance with hot-standby topology for conditional sum adder. *Microelectronics Reliability*, 2015, **55**(3–4): 704–712

9 Levitin G, Xing L, Dai Y. Cold vs. hot standby mission operation cost minimization for 1-out-of-N systems. *European Journal of Operational Research*, 2014, **234**(1): 155–162

10 Wang Jiang-Jiang, Li Zhi-Qiang, Zhao Liang. Research on switch of the dual machine hot standby system. *Railway Signaling and Communication*, 2015, **51**(2): 11–12
(王江江, 李志强, 赵亮. 双机热备系统的主备切换研究. 铁道通信信号, 2015, **51**(2): 11–12)

11 Yan Jian-Ping, Wang Xi-Shi. Reliability and safety analysis of two modes of dual module hot spare architecture. *Journal of the China Railway Society*, 2000, **22**(3): 124–127
(闫剑平, 汪希时. 两种方式双机热备结构的可靠性和安全性分析. 铁道学报, 2000, **22**(3): 124–127)

12 Hu Ai-Feng, Yang Yu-Qun. Design and research on the electric

control system for turnout of urban mass transit in Chongqing. *Journal of Railway Engineering Society*, 2009, **26**(11): 73−75
(胡爱锋, 杨玉群. 重庆单轨交通道岔电控系统的设计研究. 铁道工程学报, 2009, **26**(11): 73−75)

13 Wang Xiu-Juan. Research and realization of hot standby for centralized traffic control system. *Journal of Beijing Jiaotong University*, 2009, **33**(2): 26−29
(王秀娟. 调度集中系统中双机热备机制的实现. 北京交通大学学报, 2009, **33**(2): 26−29)

14 Sun Lei, Xu Hong-Ze. Study of security and usability of the dual module hot spare computer interlocking control system. *China Safety Science Journal*, 2004, **14**(7): 30−33
(孙蕾, 徐洪泽. 双机热备计算机联锁控制系统的安全性和可用性分析. 中国安全科学学报, 2004, **14**(7): 30−33)

15 Liu Fang, Wang Hai-Feng. Comparison of the performance of double 2-vote-2 computer-based interlocking system and double hot standby computer-based interlocking system. *Railway Signalling and Communication*, 2008, **44**(2): 26−29
(刘芳, 王海峰. 二乘二取二与双机热备计算机联锁系统性能比较. 铁道通信信号, 2008, **44**(2): 26−29)

16 Wen Jun, Su Hong-Sheng, Shen Qiang. Reliability and security analysis on two railway signal dual computer hot standby systems. *Railway Standard Design*, 2015, **59**(3): 110−113
(文俊, 苏宏升, 沈强. 两种铁路信号系统双机热备结构可靠性与安全性分析. 铁道标准设计, 2015, **59**(3): 110−113)

17 Li Jun-Li, Zhang You-Peng. Research on safety and performance analysis of computer based interlocking system based on dynamic fault tree analysis. *Journal of Railway Science and Engineering*, 2019, **16**(6): 1543−1552
(李军丽, 张友鹏. 基于动态故障树的计算机联锁系统安全性及性能分析研究. 铁道科学与工程学报, 2019, **16**(6): 1543−1552)

18 Kumar, K V, Chandra V. Transputer-based fault-tolerant and fail-safe node for dual ring distributed railway signaling systems. *Microprocessors and Microsystems*, 1994, **18**(3): 141−150

19 Kim H, Lee J, Lee K, Lee H. Design of dual-duplex system and evaluation of RAM. In: Proceedings of the 2001 IEEE Conference on Intelligent Transportation Systems, IEEE, 2001. 710−715

20 Zhang Zhen-Bo. Research and development trend of computer-based interlocking system. *Electronics World*, 2014, (3): 22−23
(张振波. 计算机联锁控制系统的研究与发展趋势. 电子世界, 2014, (3): 22−23)

21 Chen Guang-Wu, Fan Duo-Wang, Wei Zong-Shou, Fang Ya-Fei. All electronic computer interlocking system based on double 2-vote-2. *China railway science*, 2010, **31**(4): 138−144
(陈光武, 范多旺, 魏宗寿, 方亚飞. 基于二乘二取二的全电子计算机联锁系统. 中国铁道科学, 2010, **31**(4): 138−144)

22 IEC 62278—2002. Railway application-specification and demonstration of reliability, availability, maintainability and safety. *International Electrotechnical Commission*, 2002.

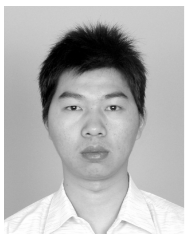
23 Wang Gui-Guo, Zhang Ying-Yi, Tan Li-Cheng, Li Na, Cao Yuan. RAMS engineering technology system construction for railway vehicle. *Journal of Beijing Jiaotong University*, 2014, **38**(2): 130−134, 140
(王贵国, 张莹驿, 谈立成, 李娜, 曹源. 轨道车辆 RAMS 工程技术体系研究. 北京交通大学学报, 2014, **38**(2): 130−134, 140)

24 Zhang You-Peng, Li Yuan-Yuan. risk assessment of railway signal system based on cloud model and evidence theory. *Journal of the China Railway Society*, 2016, **38**(1): 75−80
(张友鹏, 李远远. 基于云模型和证据理论的铁路信号系统风险评估. 铁道学报, 2016, **38**(1): 75−80)

25 Li Chun-Yang, Chen Xun, Yi Xiao-Shan, Li Hua-Wang, Yang Gen-Qing. Analysis of k/n(G) systems subject to common cause failures based on Markov process. *Systems Engineering and Electronics*, 2009, **31**(11): 2789−2792
(李春洋, 陈循, 易晓山, 李华旺, 杨根庆. 基于 Markov 过程的 k/n(G) 系统共因失效分析. 系统工程与电子技术, 2009, **31**(11): 2789−2792)

26 Wan Y, Huang H L, Das D, Pecht M. Thermal reliability prediction and analysis for high-density electronic systems based on the Markov process. *Microelectronics Reliability*, 2015, **56**(5): 182−188

27 Pilch R. Extending the possibilities of quantitative determination of SIL — a procedure based on IEC 61508 and the Markov model with common cause failures. *Quality and Reliability Engineering International*, 2017, **33**(2): 337−346

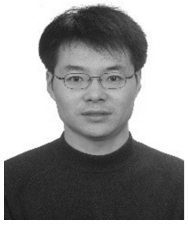


陈　峰　中国铁道科学研究院集团有限公司通信信号研究所副研究员. 2012 年获得北京交通大学博士学位. 主要研究方向为智能调度和列车运行控制. E-mail: chenfeng@bjtu.edu.cn
(**CHEN Feng**　Associate research fellow at the Signal and Communication Research Institute, China Academy of Railway Sciences Corporation Limited. He received his Ph.D. degree from Beijing Jiaotong University in 2012. His research interest covers intelligent dispatching and train operation control.)

袁志明　中国铁道科学研究院集团有限公司通信信号研究所研究员. 2016 年获得中国铁道科学研究院博士学位. 主要研究方向为行车指挥自动化, 列车运行控制, 智能调度和多列车协同控制. 本文通信作者. E-mail: 13810696163@139.com
(**YUAN Zhi-Ming**　Research fellow at the Signal and Communication Research Institute, China Academy of

Railway Sciences Corporation Limited. He received his Ph.D. degree from China Academy of Railway Sciences in 2016. His research interest covers railway signal and communication, automatic train operation, train operation control, intelligent dispatching, and cooperative control of multiple trains. Corresponding author of this paper.)

闫 璐 中国铁道科学研究院集团有限公司通信信号研究所副研究员. 2008 年获得中国铁道科学研究院博士学位. 主要研究方向为行车指挥自动化, 列车运行控制, 智能调度和多列车协同控制.
E-mail: yanlu@rails.cn
(**YAN Lu** Associate research fellow at the Signal and Communication Research Institute, China Academy of Railway Sciences Corporation Limited. She received her Ph.D. degree from China Academy of Railway Sciences in 2008. Her research interest covers railway signal and communication, automatic train operation, train operation control, intelligent dispatching, and cooperative control of multiple trains.)



许 伟 中国铁道科学研究院集团有限公司通信信号研究所研究员. 主要研究方向为智能调度和列车运行控制. E-mail: 13911519347@139.com
(**XU Wei** Research fellow at the Signal and Communication Research Institute, China Academy of Railway Sciences Corporation Limited. His research interest covers intelligent dispatching and train operation control.)

苗义烽 中国铁道科学研究院集团有限公司通信信号研究所研究员. 2014 年获得中国铁道科学研究院博士学位. 主要研究方向为铁路通信信号, 行车指挥自动化和多列车协同控制.
E-mail: 13910256619@139.com
(**MIAO Yi-Feng** Research fellow at the Signal and Communication Research Institute, China Academy of Railway Sciences Corporation Limited. He received his Ph.D. degree from China Academy of Railway Sciences in 2014. His research interest covers railway signal and communication, automatic train operation, train operation control, intelligent dispatching, and cooperative control of multiple trains.)

高博文 中国铁道科学研究院集团有限公司通信信号研究所助理研究员. 2017 年获得中国铁道科学研究院博士学位. 主要研究方向为铁路通信信号, 行车指挥自动化和多列车协同控制. E-mail: gaobw@rails.cn
(**GAO Bo-Wen** Assistant Research fellow at the Signal and Communication Research Institute, China Academy of Railway Sciences Corporation Limited. He received his Ph.D. degree from China Academy of Railway Sciences in 2017. His research interest covers railway signal and communication, automatic train operation, train operation control, intelligent dispatching, and cooperative control of multiple trains.)