

文章编号: 1005-0523(2010)02-0068-03

TMR 微机联锁系统的可靠度与安全度分析

占自才

(华东交通大学 电气与电子工程学院 江西 南昌 330013)

摘要: 分析了微机联锁的可靠度与安全度对于指导微机联锁系统在铁路运行系统中的应用。在分析中, 采用马尔可夫模型, 并考虑故障覆盖率影响情况, 对 TMR 微机联锁系统的可靠度与安全度进行了推导, 得出 TMR 微机联锁系统可靠度与安全度的定量表达式, 分析了在通常情况下的系统可靠度与安全度。

关键词: TMR 系统; 状态转移; 故障; 安全

中图分类号: TP302.8

文献标识码: A

计算机联锁系统的可靠度包括硬件可靠度和软件可靠度两部分, 本文只对系统的硬件可靠度与安全度进行讨论。微机联锁系统为了达到故障—安全的要求, 广泛采用了冗余结构容错系统, 有双模冷、热备结构与三模冗余结构。不论采用何种结构, 系统的可靠度与安全度都是一项非常重要的指标。对于双模系统分析起来相对简单, 可以参阅相关文献^[1]。TMR 冗余系统状态组合多, 可靠侧与安全侧的状态不是唯一。本文利用马尔可夫模型^[2]对 TMR 的可靠度与安全度进行评估分析, 得出了定量的推理结论, 对计算机模拟设计有一定的指导作用^[3-4]。

1 TMR 微机联锁系统可靠度模型与分析

在计算系统的可靠度时, 如果某一模块的失效将导致整个系统失效, 这时对后面模块的失效状况就不再予以考虑, 且设每个模块的失效率都相同。TMR 系统具有 $2^3 = 8$ 种状态, 分别设为 0(000), 1(001), ..., 7(111)。当某一模块发生故障时, 不会影响系统的正常工作, 但当失效模块大于或等于 2 时, 则系统失效。这个状态可视为马尔可夫吸收态^[5]。考虑到可修复 TMR 系统, 当一个模块发生故障时, 整个系统并未失效, 且失效模块有修复的可能性, 修复率为 μ , 可得到如图 1 所示的 TMR 系统的状态转移图^[6]。

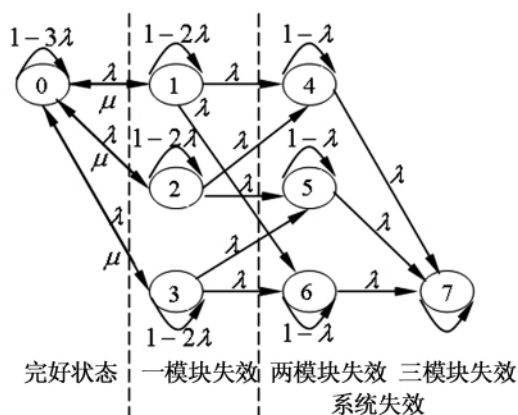


图1 TMR 系统的状态转移图

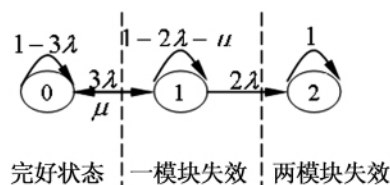


图2 TMR 系统简化状态转移图

由于系统进入 2 个模块失效的状态时, 整个系统实际上已经失效, 以后的状态变化就没有必要再考虑

收稿日期: 2009-07-12

基金项目: 江西省教育厅项目(GJJ09222)

作者简介: 占自才(1969-), 男, 副教授, 研究方向为自动化控制及其装置。

了。因此,系统状态完全可简化为3个模块正常工作,1个模块失效和2个模块失效。简化状态图如图2所示。

系统的状态转移矩阵为

$$P = \begin{bmatrix} 1-3\lambda & 3\lambda & 0 \\ \mu & 1-2\lambda-\mu & 2\lambda \\ 0 & 0 & 1 \end{bmatrix}$$

将状态转移矩阵 P 中与状态2(2个模块失效)有关的行和列去掉可得正常工作转移矩阵为

$$Q = \begin{bmatrix} 1-3\lambda & 3\lambda \\ \mu & 1-2\lambda-\mu \end{bmatrix}$$

平均故障间隔时间为: $t_{MTBF} = B(I - Q)^{-1}A$

其中: $B = (1 \ 0 \ 0 \cdots 0)$; I 是单位矩阵; A 是元素为1的列向量。令 $t = \tau + t$ 为整数, $0 \leq \Delta t \leq 1$, 于是有: $R(t) = 1 - (II \cdot P)C$ 。其中: 初始概率分布 $II = 1 \ 0 \ 0 \cdots 0$; C 为最后一个元素是1, 而其余皆为0的列向量 $P = RDR^{-1}$ 。

$$\text{其中 } D = \begin{bmatrix} a_1 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & a_l \end{bmatrix} \text{ 式中: } a_i (1 \leq i \leq l) \text{ 为矩阵 } P \text{ 的特征值}$$

根据前式,可计算出可修 TMR 系统的 $t_{MTBF_{TMR}} = \frac{\mu}{6\lambda^2} + \frac{5\lambda}{6\lambda^2}$ 。

2 TMR 微机联锁系统安全度模型与分析

假设 TMR 系统3个同时工作的冗余模块分别为 A、B 和 C。由于采用三取二表决方式,所以一个模块故障不影响系统的正常工作,只有当两个或两个以上的模块发生故障时,系统才会失效。TMR 系统具有一个突出的优点即能检测出单模块的故障,这就大大提高了系统的安全性。我们将3个冗余模块以外的其它模块作为一个整体,统称为外围设备,并把它称为 D 模块。为了简化分析过程,不妨作以下假设^[7]:

- (1) 由于两个或两个以上模块同时发生故障的概率很小,与单模块的故障概率相比可忽略不计;
- (2) 单模块的故障不会导致危险输出,并且单模块故障可被检出,理论推导可以采用这个假设,实际应用中可以不考虑这个假设;
- (3) 当发生单模块故障,并且在故障未被检出期间,如果有另一模块又发生故障,则保守地认为系统会给出危险侧输出;
- (4) 故障是随机的,其运行符合马尔可夫过程;
- (5) 系统修复后,完好如初。

系统中每个模块都存在两种状态:正常工作状态和故障状态。那么4个模块共有16种工作状态,其中3个模块都故障的4种情况和4个模块全部故障的1种情况不在考虑范围之内,其余的11种工作状态分列如下:这里按照1、2、3和4的顺序构成各个状态,以“H”代表四模块正常工作状态,H(14)代表一模块故障状态四种情况,H12、H13、H14、H23、H24、H34代表两模块故障状态的6种情况。系统的状态转移图如图3所示。

λ_i 是一个模块坏的概率, μ_i 是单个模块修复的概率, μ_{ij} 是两个坏模块同时修复的概率。由于上述状态转移图太复杂,我们假定各模块的故障率和修复率都是相同的,以简化分析过程。设: $\lambda_1 = \lambda_2 = \lambda_3 = \lambda_4 = \lambda$, $\mu_1 = \mu_2 = \mu_3 = \mu_4 = \mu$, $\mu_{12} = \mu_{13} = \mu_{14} = \mu_{23} = \mu_{24} = \mu_{34} = \nu$, 则可以得到简化的系统状态转移图,见图4。图4中 A 为系统正常工作状态; B 为系统非危险故障状态; C 为系统危险故障状态。

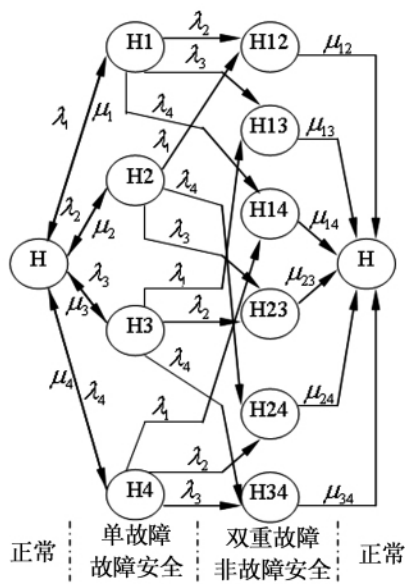


图3 TMR 系统状态转移图

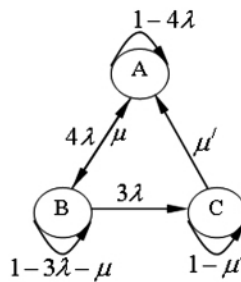


图4 TMR 系统简化后状态转移图

对图4的状态转移系统列出以下微分方程,且知它们的初始值为: $P_A(0) = 1$, $P_B(0) = 0$, $P_C(0) = 0$, 并利用拉氏变换原理求出

$$P'_A(t) = -4\lambda P_A(t) + \mu P_B(t) + \nu P_C(t), \quad P'_B(t) = -(3\lambda + \mu) P_B(t) + 4\lambda P_A(t), \quad P'_C(t) = -\nu P_C(t) + 3\lambda P_B(t)$$

解微分方程组的解如下

$$P_A(t) = \frac{3\lambda\nu + \mu\nu}{12\lambda^2 + 7\lambda\nu + \mu\nu}, \quad P_B(t) = \frac{4\lambda\nu}{12\lambda^2 + 7\lambda\nu + \mu\nu}, \quad P_C(t) = \frac{12\lambda^2}{12\lambda^2 + 7\lambda\nu + \mu\nu}$$

以上就是评估过程所推算出的各种状态下的稳态概率,将相关参数代入,可得 TMR 系统处于各状态的概率为

安全度为

$$S(t) = P_A(t) + P_B(t) = \frac{7\lambda\nu + \mu\nu}{12\lambda^2 + 7\lambda\nu + \mu\nu}$$

故障安全度为

$$D(t) = \frac{P_B}{P_B + P_C} = \frac{4\lambda\nu}{12\lambda^2 + 4\lambda\nu}$$

3 结论

从 $S(t)$ 表达式可以看出:当 λ 很小,即模块发生故障的概率很小,而修复的概率 μ 和 ν 一般较大,所以 $S(t)$ 的值基本上是接近 1 的,也就是系统几乎整个时间段是安全的,同理可得出故障安全度 $D(t)$ 也接近 1,系统也是故障安全的。也就是说,三模系统在能快速修复或排除故障的情况下,可以保证系统是安全的,根据这个指导,可以对计算机联锁进行安全性仿真,这个不是本文的重点,可以参考相关文献^[8]。

参考文献:

- [1] 胡谋. 计算机容错技术[M]. 北京: 中国铁道出版社, 1995.
- [2] 傅佩琛, 赵霖, 张军英. 计算机系统硬件软件可靠性理论及其应用[M]. 北京: 国防工业出版社, 1990.
- [3] 宓涟. 计算机联锁系统的辅助设计[J]. 铁道通信信号, 2000, 36(7): 7-8.
- [4] 赵志. 计算机辅助设计在微机联锁中的应用[J]. 电气化铁道, 1999(4): 44-46.

(下转第 81 页)

- [4] 刘建辉, 冀常鹏. 单片机智能控制技术[M]. 北京: 国防工业出版社, 2007. 4.
- [5] 韩兆祥, 李学英, 万鑫, 等. 利用 PLC 和触摸屏实现多阶段 PID 温度控制[J]. 实验技术与管理, 2008, 25(6): 56-59.
- [6] 王志凯, 郭宗仁. PLC 实现模糊控制的两种设计方法[J]. 中国仪器仪表, 2002(1): 4-6.

Furnace Temperature Control System Based on the PLC

Shi Xiaoying, Xu Zhibang

(School of Electrical and Electronic Engineering, East China Jiaotong University, Nanchang 330013, China)

Abstract: Based on the PLC temperature control system, which is composed of the input/output expansion module FX2N-4AD-TC, FX2N-2DA, the thermo-element, mainly takes Mitsubishi FX2N PLC as the control core. According to fuzzy language variable assignment table which is already established and fuzzy control rule, the fuzzy reasoning and the fuzzy decision are conducted to establish the off-line the fuzzy control query table, and give the resistance furnace temperature fuzzy control procedures. Using Fuzzy-PID compound control, the system gets a good dynamic performance and steady performance.

Key words: FUZZY control; Fuzzy-PID compound control; FX2N-4AD-TC; FX2N-2DA

(责任编辑 王建华)

(上接第 70 页)

- [5] 西沃赖克 D P. 可靠系统的设计理论与实践[M]. 袁由光, 译. 北京: 科学出版社, 1988.
- [6] 赵志熙. 计算机联锁系统技术[M]. 北京: 中国铁道出版社, 1995.
- [7] 赵志熙. 车站信号控制系统[M]. 北京: 中国铁道出版社, 1992.
- [8] 陈杰. 基于仿真技术的铁路计算机联锁培训系统的研究[J]. 微型电脑应用, 2003, 19(5): 11-13.

An Analysis of Reliability and Safety of Computer Interlocking System Based on TMR

Zhan Zicai

(School of Mechanical and Electrical Engineering, East China Jiaotong University, Nanchang 330013, China)

Abstract: This paper analyzes reliability and safety of computer interlocking system, which can instruct interlocking system in rail application. Based on Markov model and taking into account of failure covering, this paper discusses in detail reliability and safety of TRM computer interlocking system. The quantitative expression for reliability and safety of the system is given. Its reliability, safety and practical application under normal circumstances is analyzed and conclusion of safe simulation is drawn.

Key words: TMR system; state-transfer; failure; safety

(责任编辑 刘棉玲)