

基于 Markov 链的嵌入式系统硬件可靠性研究

郭荣佐^{1*}, 黄君², 王霖³

(1. 四川师范大学 计算机科学学院, 成都 610068; 2. 四川工商职业技术学院 基础部, 四川 都江堰 611830;

3. 成都纺织高等专科学校 电子信息与电气工程系, 成都 611731)

(* 通信作者电子邮箱 gyz00001@163.com)

摘要:嵌入式系统产品在使用过程中经常出现硬件故障,从而影响系统的安全可靠性。从嵌入式系统硬件层面研究其可靠性。首先定义嵌入式系统硬件目标,简单介绍了 Markov 过程理论;建立了单个 IP 硬核和嵌入式系统硬件的 Markov 模型;应用所建立的模型,对嵌入式站间自动闭塞控制器硬件进行了可靠度计算和分析。实验结果表明,该 Markov 模型能够准确描述嵌入式系统硬件的状态变迁,并能计算和分析其可靠度,具有一定的实用价值。

关键词:可靠性;硬件;嵌入式系统;Markov 链;站间自动闭塞

中图分类号: TP302.1, TP202.1 **文献标志码:** A

Hardware reliability study of embedded system based on Markov chain

GUO Rong-zuo^{1*}, HUANG Jun², WANG Lin³

(1. College of Computer Science, Sichuan Normal University, Chengdu Sichuan 610068, China;

2. Department of Grounding Instruction, Sichuan Technology and Business College, Dujiangyan Sichuan 611830, China;

3. Department of Electronic Information and Electrical Engineering, Chengdu Textile College, Chengdu Sichuan 611731, China)

Abstract: The products of embedded system often have hardware failure while in use, which affects the safety and reliability of the system. In this paper, its reliability was researched from the embedded system hardware level. At first, it defined the goal of the embedded system hardware, and introduced the theory of Markov process. And then, a single IP hardcore and embedded system hardware Markov model was set up. At last, the reliability of the embedded controller hardware automatic block was calculated and analyzed through the established model. The results show that the Markov model can accurately describe the embedded system hardware state change, and can calculate and analyze their reliability. Therefore, the model has certain practical value.

Key words: reliability; hardware; embedded system; Markov chain; inter-station automatic block

0 引言

嵌入式系统的可靠性是指系统在规定的条件下,在规定的时间内,系统完成规定功能的能力。嵌入式系统由硬件和软件构成,其可靠性包括硬件可靠性和软件可靠性两方面。嵌入式系统硬件可靠性包括元器件可靠性、设备(功能部件)可靠性和系统可靠性。嵌入式系统硬件可靠性主要体现为系统可靠性,而系统可靠性以印刷电路板的可靠性来体现。因此,嵌入式系统硬件电路板的可靠性对整个嵌入式系统的正常运行起到至关重要的作用,若电路板在运行中发生故障或出现不可靠因素,则该嵌入式系统的可靠性将受到极大的影响。

在使用嵌入式系统产品时,软件方面的问题比较少见,而硬件故障却是经常出现,比如手持设备使用一段时间后,会出现键盘、电源和存储卡等故障。嵌入式系统越来越多地应用于各种控制系统中,比如微波炉、洗衣机和空调等家用电器;在工业领域,越来越多的嵌入式实时控制系统服务于生产过程,比如各种工业生产现场使用的仪器仪表、数据采集终端和现场驱动等;在军事、航空领域等领域,使用的控制系统,也是嵌入式实时控制系统。人们总是期望这样的嵌入式系统在有效期内,能够安全可靠地运行,完成各种控制功能。

国内外学者对计算机系统硬件的可靠性进行了相关研

究。Bobbio 等^[1]将 Markov 模型引入单部件的可靠性分析,对一个具有多种失效模式的硬件部件进行了研究。Kuo 等^[2]总结了 k/n 表决系统的可靠性模型,并提出了改进系统可靠性的优化策略。Arulmozhi^[3]进一步研究了 k/n 表决系统的可靠性模型,针对异构部件组成的表决系统提出了一种简单有效的计算模型。Sherwin 等^[4]对热备和冷备系统进行了可靠性分析。对于硬件系统的可靠性分析,Pukite 等^[5]对一些常见的硬件结构进行了总结并且完成了对这些硬件结构的 Markov 建模。国内的梅登华等^[6]对控制系统硬件可靠性进行了研究。虽然这些基于 Markov 的可靠性研究取得了一定的成果,但这些研究,没有专门对嵌入式系统硬件可靠性进行研究,更没有专门对嵌入式实时控制系统硬件的可靠性进行研究。由此可见,研究嵌入式系统硬件可靠性是十分必要的,也是迫在眉睫的。

本文以 Markov 过程为理论基础,从嵌入式系统硬件的单个 IP 硬核到系统,全面深入研究嵌入式系统硬件的可靠性及建模,并应用所建立的可靠性模型对具体的嵌入式实时控制系统进行硬件可靠性分析。

1 嵌入式系统目标定义

在对嵌入式系统硬件(Embedded System Hardware, ESH)可靠性进行研究之前,需先定义其硬件构成。任何嵌入式系

收稿日期:2011-11-01;修回日期:2011-12-15。 基金项目:四川省教育厅自然科学基金重点项目(10ZA008)。

作者简介:郭荣佐(1973-),男,四川开江人,副教授,主要研究方向:嵌入式系统、实时控制系统、物联网感知; 黄君(1974-),女,重庆丰都人,讲师,硕士,主要研究方向:应用数学; 王霖(1970-),男,四川遂宁人,副教授,主要研究方向:计算机网络。

统的硬件子系统,由嵌入式处理器和各种功能单元组成,功能单元主要有 IP 核和软件组件,IP 核无论是 IP 硬核、软核还是固件核,都是一种功能硬件,在此将 IP 核统称为 IP 硬核。IP 硬核由电子元器件(Electronic Component, EC)、电路及其结构(Circuit and its Structure, CiS)、电路板(Circuit Board, CB)和执行装置(Executive Device, ED)等组成。

要实现特定嵌入式系统的功能,必须在需求分析完成后,对系统功能进行划分,给出各个功能得以实现的硬件基础。嵌入式系统硬件组成及其约束:电子元器件 I_{EC1} 不超过 B_1 、可选电路及其结构 I_{CiS2} 不能超过 B_2 、……,电路板布线方式 I_{CBn} 不能超过 B_{n-1} ,执行装置可选种类或可选装置不超过 B_n ;而某种功能的可选硬件有很多种,这些可选的硬件又具有不同的可靠性参数。

定义 1 设 C_{ESH} 为嵌入式系统硬件设计中的硬件 IP 核,则为一个 n 元组,即 $C_{ESH} = (I_{EC1}, I_{CiS2}, \dots, I_{CBn-1}, I_{EDn})$,其中 $I_{EC1}, I_{CiS2}, \dots, I_{CBn-1}, I_{EDn}$ 是与组成 IP 核硬件相关的 EC、CiS、CB 和 ED。

定义 2 设嵌入式系统硬件由若干功能单元组成,即: $E_{ESH} = \{F_1, F_2, \dots, F_M\}$,则每个功能单元对应多个可选的 IP 核集合,即:

$$\begin{aligned} F_1 &\rightarrow \{C_{ESH11}, C_{ESH12}, \dots, C_{ESH1a}\} \\ F_2 &\rightarrow \{C_{ESH21}, C_{ESH22}, \dots, C_{ESH2b}\} \\ &\vdots \\ F_M &\rightarrow \{C_{ESHm1}, C_{ESHm2}, \dots, C_{ESHmn}\} \end{aligned}$$

其中: C_{ESH} 为服从定义 1; a, b, \dots, n 是常数,分别表示 F_1, F_2, \dots, F_M 所对应的可选 IP 核的数目。

由定义 1、2 可知,嵌入式系统硬件设计问题就是寻求一个 C_{ESH} 的组合算法或组合模型,组合满足:

$$\begin{aligned} 1) &S_1(I_{EC1i}, I_{EC2j}, \dots, I_{ECmk}) \leq B_1, \\ 2) &S_2(I_{CiS1i}, I_{CiS2j}, \dots, I_{CiSmk}) \leq B_2, \\ &\vdots \\ n-1) &S_{n-1}(I_{CB1i}, I_{CB2j}, \dots, I_{CBmk}) \leq B_{n-1}, \\ n) &S_n(I_{ED1i}, I_{ED2j}, \dots, I_{EDmk}) \leq B_n; \end{aligned}$$

其中: S_1, S_2, \dots, S_n 分别对应为不同硬件组成部件 $I_{EC1}, I_{CiS2}, \dots, I_{CBn-1}, I_{EDn}$ 和约束 B_1, B_2, \dots, B_n ,用来分析和计算由多个 IP 核组成的嵌入式系统硬件,它们的计算方法由对应的功能和可靠性指标共同决定^[7]。因此,所定义的嵌入式系统硬件如图 1 所示。

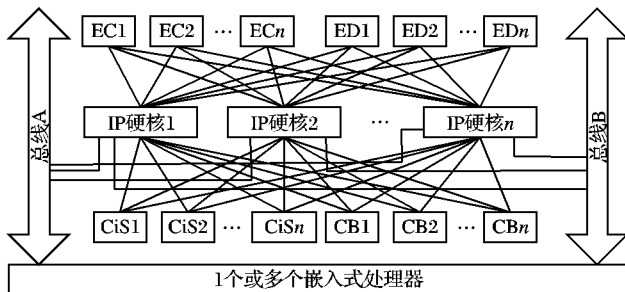


图 1 嵌入式系统硬件目标形式化模型

2 系统硬件可靠性模型

2.1 Markov 过程简介

Markov 过程是一类重要的随机过程,由前苏联学者 Markov 在研究随机过程中得到的^[8]。

定义 3 设 $\{X(t), t \geq 0\}$ 是取值在 $E = \{0, 1, 2, \dots\}$ 或 $E = \{0, 1, 2, \dots, N\}$ 上的一个随机过程。若 $\exists \forall n$, 及 $\forall n$ 个时

间点 $0 \leq t_1 < t_2 < \dots < t_n$, 均有:

$$\begin{aligned} P\{X(t_n) = i_n | X(t_{n-1}) = i_{n-1}, \dots, X(t_1) = i_1\} = \\ P\{X(t_n) = i_n | X(t_{n-1}) = i_{n-1}\} \end{aligned} \quad (1)$$

其中 $i_1, \dots, i_n \in E$, 则称 $\{X(t), t \geq 0\}$ 为离散状态空间 E 上的连续时间 Markov 过程。

Markov 过程根据参数空间与状态空间的离散与连续类型分为四种类型:离散参数集,离散状态集 Markov 过程;离散参数集,连续状态集 Markov 过程;连续参数集,离散状态集 Markov 过程;连续参数集,连续状态集 Markov 过程。其中第一种类型,称之为 Markov 链,简称 Markov 链。

定义 4 设 $\{X(n), n = 0, 1, 2, \dots\}$ 为一随机过程,状态集为 $E = \{i_0, i_1, i_2, \dots\}$,若对于任意 n 及 $\{i_0, i_1, \dots, i_{n-1}\}$,对应的随机变量 $(X(0), X(1), X(2), \dots, X(n+1))$ 满足:

$$\begin{aligned} P\{X(n+1) = j | X(n) = i_n, X(n-1) = i_{n-1}, \dots, \\ X(1) = i_1, X(0) = i_0\} = P\{X(n+1) = j | \\ X(n) = i_n\} \end{aligned} \quad (2)$$

则称随机过程 $\{X(n), n = 0, 1, 2, \dots\}$ 为 Markov 链。

由定义 4 可知,Markov 链在状态 $X(0) = i_0, X(1) = i_1, \dots, X(n) = i_n$ 已知的条件下, $X(n+1) = j$ 的条件概率与 $X(0) = i_0, X(1) = i_1, \dots, X(n-1) = i_{n-1}$ 无关,仅与 $X(n)$ 所处的状态 i_n 有关。

定理 1 若 Markov 链的状态空间 E 为可列集 $\{0, \pm 1, \pm 2, \dots\}$ 或 $\{0, 1, 2, \dots\}$, 则称之可列状态的 Markov 链;若 E 中状态是有限多个,则称之为有限状态的 Markov 链。

定理 2 若 Markov 链 $\{X(n), n = 0, 1, 2, \dots\}$ 在时刻 k 所处状态 i , 而下一步将处于状态 j 的一步转移概率为:

$$P\{X(k+1) = j | X(k) = i\} = p_{ij}(k); k = 0, 1, \dots \quad (3)$$

其中 $p_{ij}(k)$ 表示在时刻 k 时 $X(k)$ 取 i 的条件下,在下一个时刻 $X(k+1)$ 取 j 的一步转移概率。

由定理 2 可知, $p_{ij}(k)$ 具有以下性质:

$$\begin{aligned} 1) &p_{ij}(k) \geq 0; \forall i, j \in E; \\ 2) &\sum_{j \in E} p_{ij}(k) = 1; \forall i \in E \end{aligned}$$

定理 3 设 $\{X(n), n = 0, 1, 2, \dots\}$ 是 Markov 链,状态空间为 $E = \{0, 1, 2, \dots\}$,若其一步转移概率与 Markov 链现在所在时刻无关,即满足等式:

$$P\{X(k+1) = j | X(k) = i\} = p_{ij}; \forall k \in E \quad (4)$$

则称 $\{X(n), n = 0, 1, 2, \dots\}$ 为齐次 Markov 链,也称为具有平稳转移概率的 Markov 链。

由定理 3 可知, p_{ij} 具有如下性质:

$$\begin{aligned} 1) &p_{ij} = p_{ij}(1) \geq 0; \forall i, j \in E; \\ 2) &\sum_{j \in E} p_{ij} = \sum_{j \in E} p_{ij}(1) = 1; \forall i \in E. \end{aligned}$$

2.2 嵌入式系统硬件失效模式

2.2.1 系统硬件可用性

要建立嵌入式系统硬件可靠性模型,首先建立其可用性模型。嵌入式系统硬件可靠性模型是对多个 IP 硬核构成的系统的可靠性进行建模。由定义 1、2 可知,嵌入式系统硬件的每个 IP 核由 EC、CiS、CB 和 ED 组成,每个组成部分都有可用性要求,因此,每个 IP 核的可用性就构成整个嵌入式系统硬件的可用性。而研究系统的可用性,需先量化每个 IP 核的可用性,然后计算系统的整体可用性。

定义 5 由定义 2 可知,嵌入式系统硬件由 M 个 IP 硬核

构成,即 $E_{ESH} = \{F_1, F_2, \dots, F_M\}$,若:

- 1) 每个 IP 硬核的失效率和修复率均服从指数分布;
- 2) IP 硬核要么完全正常的,要么完全失败;
- 3) IP 硬核 F_i 的失效率和修复率分别 λ_i 和 μ_i ;
- 4) 所有 IP 硬核的失效和修复被假定为对独立的随机事件,系统当且仅当所有 IP 硬核可用时系统可用;

则整个嵌入式系统硬件稳态可用性 A 定义为:

$$A = \prod_{i=1}^M P\{F_i \text{ 是可用的}\} = \prod_{i=1}^M \frac{\mu_i}{\lambda_i + \mu_i} \quad (5)$$

嵌入式系统硬件是可用的条件为:当且仅当所有 IP 硬核可用,且所有 IP 硬核的可用性概率是独立随机事件。因此,系统的稳态可用性的概率就是所有 IP 硬核在同一时刻的可用性概率之积。

2.2.2 系统硬件失效模式

引起嵌入式系统硬件失效的因素很多,有工作条件、环境应力及时间对系统性能的劣化或失效所产生的影响,也有组成嵌入式系统硬件的物理和化学等微观因素导致的。失效发生过程既是原子、分子微观变化过程,又是整体上宏观变化过程。在一定条件下,系统本身会由正常状态逐渐向不正常状态转化,最终将不可逆地退化为失效状态。

嵌入式系统硬件失效模式,是指嵌入式系统硬件设计过程中,通过对系统组成模块(包括元器件、零部件、和电路板等细节)可能发生的失效模式进行分析,并得到其对系统功能的影响,提出预防嵌入式系统硬件失效的措施,以提高嵌入式系统硬件的可靠性^[9]。

嵌入式系统硬件从寿命特征来分析,服从如图 2 所示的曲线^[10]。从曲线可知,嵌入式系统硬件失效率随时间变化大致可分为三个阶段:早期失效期 I、偶然失效期 II、耗损失效期 III。因此,在嵌入式系统硬件使用寿命内,系统将出现失效的可能性较早期和耗损期要小,但会出现失效,从而引起系统的不可靠。

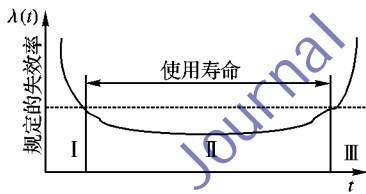


图 2 嵌入式系统硬件失效率曲线

嵌入式系统硬件失效,依据持续时间可分为永久性失效和暂时性失效。永久性失效是嵌入式系统硬件物理性能随着工作时间的推移而发生的失效,是修复或更换才能恢复的失效,因此,可将其分为局部永久性失效和全局永久性失效;暂时性失效由外部或内部不确定因素引起的,持续时间短暂,不需要进行修复或更新。而嵌入式系统硬件失效主要由全局失效、未能及时予以恢复的暂时性失效和超过系统容错能力的局部硬件失效等引起。为消除暂时性失效对系统的影响,常采用重复操作直至失效消除,但在系统运行中,可能出现未能及时予以恢复的暂时性失效或超过系统容错能力的局部硬件失效,此时系统执行失效点检测、隔离和重组等来消除失效,使系统从失效状态中恢复^[11]。

2.3 嵌入式系统硬件的 Markov 模型

2.3.1 单个 IP 硬核的 Markov 模型

由前面定义 1、2 可知,单个 IP 硬核由 I_{EC1} 个电子元器件、

I_{CS2} 种可选的电路及其结构和 I_{CB3} 种电路板布线方式等构成。而 IP 硬核在设计完成之后,其假设使用器件或部件的种类为 n 。

定义 6 单个 IP 硬核,若所有 EC 的失效率相互独立且服从相同的指数分布,且 EC 仅有正常和失效两种状态,所有 EC 均正常 IP 硬核才能正常工作;则 IP 硬核所有 EC 的失效率为 λ_{IPEGi} 定义为:

$$\lambda_{IPEGi} = \sum_{i=1}^n N_i (\lambda_G \pi_Q)_i \quad (6)$$

其中: λ_G 表示第 i 类器件或部件的通用失效率; π_{Qi} 表示第 i 类器件或部件的质量系数; N_i 表示第 i 类器件或部件的数量; n 为不同器件或部件的种类数。

IP 硬核的 CiS 经过比选,选择失效率最小的 CiS,且假定为 λ_{CiSi} ; IP 硬核的 CB 选择失效率最小,且假定为 λ_{CBi} ; IP 硬核的 EC、CiS 和 CB 等构成串联模型,当且仅当所有部件正常工作时,IP 硬核可正常工作;故有 IP 硬核的失效率为 $\lambda_{IPi} = \lambda_{IPEGi} + \lambda_{CiSi} + \lambda_{CBi}$ 。

定义 7 单个 IP 硬核的可靠度计算模型为:

$$R_{IPi}(t) = e^{-\lambda_{IPi} t} \quad (7)$$

其中 λ_{IPi} 为给定的 IP 硬核失效率。

由定义 6、7 可知,单个 IP 硬核仅有正常和失效两种状态。依据前面 Markov 链的理论可知,单个 IP 硬核能够用 Markov 链建立可靠性模型^[12]。

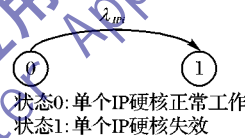


图 3 单个 IP 硬核状态转移图

图 3 为单个 IP 硬核在 Δt 时间内的状态转移图(假设单个 IP 硬核不可维修)。其中 $\lambda_{IPi}(t)$ 失效函数。由状态转移图可得状态转移速度矩阵 A :

$$A = \begin{bmatrix} -\lambda_{IPi} & 0 \\ \lambda_{IPi} & 0 \end{bmatrix} \quad (8)$$

由 Markov 链可得到单个 IP 硬核的状态微分方程为:

$$(P_0'(t), P_1'(t)) = (P_0(t), P_1(t))A \quad (9)$$

其中初始条件为 $(P_0(0), P_1(0))$ 。

假设时刻 0 时,单个 IP 硬核处于正常工作状态,初始条件为 $(P_0(0), P_1(0)) = (1, 0)$ 。解此微分方程有:

$$\begin{cases} P_0(t) = P_0(0) \cdot e^{-\lambda_{IPi} t} \\ P_1(t) = 1 - P_0(t) \end{cases} \quad (10)$$

从而得到单个 IP 硬核在不考虑维修的情况下的瞬时可靠度。

2.3.2 系统硬件 Markov 模型

单个 IP 硬核的可靠性可用 Markov 链建立模型,由多个独立 IP 硬核构成的嵌入式系统硬件同样可用 Markov 链建立其可靠性模型。用 Markov 链来评估嵌入式系统硬件可靠性时,系统的各个状态可以看作是一个连续时间、离散状态的 Markov 过程,为系统可靠性模型现作如下假设^[13]:

- 1) 假设嵌入式处理器的可靠度恒定,且独立于其他 IP 硬核;
- 2) 所有 IP 硬核失效率独立且服从系统的指数分布,每个 IP 硬核的失效率由定义 6 确定;
- 3) 设硬件局部退化导致系统失效的失效率为 λ_1 ; 设嵌入式系统硬件局部失效被检测到的概率为 p_1 , 检测到的局部失效能够在规定时间内修复的概率为 p_2 ;
- 4) 未检测到的硬件退化而导致系统失效的失效率为 λ_5 , 检测到的硬件退化系统失效的失效率为 λ_6 ;

5) 局部硬件失效软件方法修复率为 μ_1 , 非软件方法修复率为 μ_2 。

6) 局部失效的硬件可能导致系统完全失效, 若局部硬件退化被检测而无软件方法恢复的概率为 λ_2 , 硬件退化被检测能通过软件方法恢复的概率为 λ_3 , 硬件局部退化未被检测到的概率为 λ_4 。

依据单个 IP 硬核建模过程, 对嵌入式系统硬件的多个 IP 硬核构成的系统进行建模时, 其状态还需进行定义^[14]。嵌入式系统硬件状态为:

状态 0 系统的所有 IP 硬核及嵌入式处理器工作正常;

状态 1 局部硬件暂时性失效, 且失效的 IP 硬核未被软件检测, 系统可降级工作;

状态 2 局部硬件暂时性失效, 且失效的 IP 硬核被软件检测到, 系统可降级工作;

状态 3 局部硬件永久性失效, 但不影响系统工作, 系统可降级工作;

状态 4 系统局部 IP 硬核发生失效, 造成系统不能降级工作, 从而导致系统完全失效;

状态 5 软件导致硬件完全失效;

状态 6 系统发生全局失效, 系统失效。

由定义可知, 状态 0 为系统的正常工作状态, 状态 1、2、3 为退化工作状态, 状态 4、5 和状态 6 为失效状态。因此, 在 Δt 时间内, 系统各状态间的状态转移如图 4 所示。

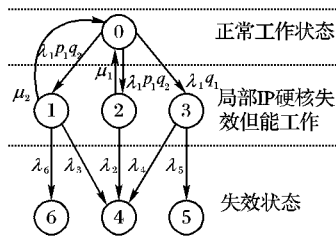


图4 嵌入式系统硬件状态转移图

设 $p_i(t)$ 表示状态 i 在时间 t 的概率, 则由 Markov 过程相关理论可得以下微分方程:

$$\begin{pmatrix} p'_0(t) & p'_1(t) & p'_2(t) & p'_3(t) & p'_4(t) & p'_5(t) & p'_6(t) \end{pmatrix} = \begin{pmatrix} p_0(t) & p_1(t) & p_2(t) & p_3(t) & p_4(t) & p_5(t) & p_6(t) \end{pmatrix} * A \quad (11)$$

其中 A 为状态转移矩阵, 由状态转移图可得状态转移矩阵 A (其中 $q_1 = 1 - p_1, q_2 = 1 - p_2$) 为:

$$A = \begin{bmatrix} -\lambda_1 & \lambda_1 p_1 p_2 & \lambda_1 p_1 q_2 & \lambda_1 q_1 p_2 & 0 & 0 & 0 \\ \mu_1 & -\mu_1 - \lambda_2 & 0 & 0 & \lambda_2 & 0 & 0 \\ \mu_2 & 0 & -\mu_2 - \lambda_3 - \lambda_6 & 0 & \lambda_3 & 0 & \lambda_6 \\ 0 & 0 & 0 & -\lambda_4 - \lambda_5 & \lambda_4 & \lambda_5 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (12)$$

要求解此微分方程的初始条件假设为:

$$\begin{pmatrix} p_0(0) & p_1(0) & p_2(0) & p_3(0) & p_4(0) & p_5(0) & p_6(0) \end{pmatrix} = (1, 0, 0, 0, 0, 0, 0)$$

解上微分方程即可得到各个状态的瞬时概率, 除去失效状态就能方便计算出嵌入式系统硬件的可靠度为:

$$R_{HWSys}(t) = p\{t \text{ 时间内无失效状态} \} =$$

$$p_0(t) + p_1(t) + p_2(t) + p_3(t) \quad (13)$$

而嵌入式系统硬件由 n 个 IP 硬核构成, 因此, 可计算出系统的可靠度为:

$$R_{HESys}(t) = \left(\sum_{i=1}^n R_{IPi} \right) \times (p_0(t) + p_1(t) + p_2(t) + p_3(t)) \quad (14)$$

其中 R_{IPi} 由定义 6、7 确定, $(p_0(t), p_1(t), p_2(t), p_3(t))$ 为微分方程的解。

3 模型应用实例

文献[15]设计了一个嵌入式站间自动闭塞控制器的硬件系统, 应用本文建立的嵌入式系统硬件可靠性模型对其进行可靠性分析。

3.1 控制器硬件的可靠性框图

自动站间闭塞控制器采用冗余核心板结构, 单控制器核心板硬件包括 MCU、通信模块和比较电路等, 具体硬件设计参见参考文献。

依据可靠性理论, 对自动站间闭塞控制器的单个 MCU 的各个组成模块进行分析, 分析其基本任务可靠性框图和特殊任务可靠性框图。基本任务可靠性框图即保证整个系统正常工作的框图, 对自动站间闭塞控制器而言, 其基本任务可靠性框图就是保障各模块正常运行, 其单个 MCU 的可靠性框图如图 5 所示。特殊任务可靠性框图即保障系统不停机的框图。对于自动站间闭塞控制器, 特殊任务就是在系统的局部故障时, 要保证系统的运行在一定允许范围内, 允许系统降级工作, 但是不允许系统无输出而导致事故^[16]。单个 MCU 的特殊任务可靠性框图如图 6 所示。

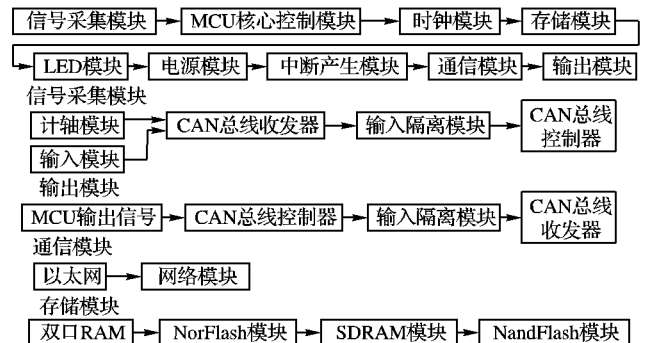


图5 基本任务可靠性框图

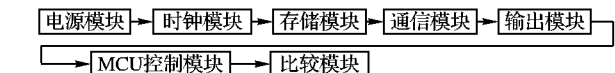


图6 特殊任务可靠性框图

3.2 各 IP 硬核可靠度

每个模块就是一个 IP 硬核, 都有其自身的失效率和可靠度。依据单个 IP 硬核和 GJB/Z 299B-98《电子设备可靠性预计手册》, 可方便计算 IP 硬核的可靠性预计。

经过比选, 选择失效率最低的集成芯片和电子元器件, 然后依据定义 6、7 计算各个 IP 硬核 (即各个模块) 的总的失效率, 最后根据定义 7 计算出 IP 硬核的可靠度。

以站间自动闭塞控制器的比较电路为例, 查阅各组成电路的手册, 得到如表 1 所示的各种芯片及器件的失效率 (表 1 仅给出了部分元器件的失效率)。

经过计算, 得到^[11]:

$$\lambda_{IPBJ} = \left(\sum_{i=1}^n N_i(\lambda_c \pi_Q)_i \right) + \lambda_{CIS} + \lambda_{CB} + \lambda_{ED} =$$

$$(0.08237 + 0.01375 + 0.01634) \times 10^{-6} =$$

$$0.11246 \times 10^{-6} \quad (15)$$

从而得到该 IP 硬核的 MTBF(单位:h) 为:

$$MTBF_{IPBJ} = 1/\lambda_{IP12} = 8.8920505 \times 10^6$$

依据定义 7 可计算该 IP 硬核工作 10000 h 的可靠度为:

$$R_{IP12}(t) = e^{-\lambda_{IPBJ}t} = e^{-0.11246 \times 10^{-6} \times 1 \times 10^4} = 0.99883$$

表 1 芯片及部分元器件失效率表

元器件	失效率 $\lambda (\times 10^{-6})$	元器件	失效率 $\lambda (\times 10^{-6})$
74LS06	0.00127	电阻	0.00101
LM358	0.00127	电容	0.00194
74LS142	0.00126	NCOMS	0.00270
74LS178	0.00126	NPN 管	0.00154

采用同样的方法可计算得到各 IP 硬核的失效率如表 2 所示。

表 2 各 IP 硬核失效率

编号	IP 硬核名称	失效率 $\lambda (\times 10^{-6})$	编号	IP 硬核名称	失效率 $\lambda (\times 10^{-6})$
1	信号采集	0.01197	6	电源模块	0.16389
2	MCU 控制	0.01249	7	中断产生模块	0.01139
3	时钟模块	0.13175	8	通信模块	0.14578
4	存储模块	0.13658	9	输出模块	0.06412
5	LED 模块	0.31294	10	比较模块	0.11246

3.3 系统可靠性

控制器采用热备方式实现站间自动闭塞运算,以提高控制系统的安全可靠。而控制器两个 MCU 又自成系统,每个 MCU 的基本任务可靠性框图为各 IP 硬核串联组成,由表 2 可计算每个 MCU 的失效率为:

$$\lambda_{MCU} = \sum_{i=1}^9 \lambda_i = 0.99091 \times 10^{-6}$$

比较模块的作用是对两个 MCU 的所计算的列车轴数进行比较,若比较得到两个 MCU 计算结果一致,则结果与通过网络接收到的上一站的计轴结果进行比较,以确定下一步操作;否则重新从计轴模块得到数据,重新进行计算并比较;若进行三次这样的重复操作,结果还是不一致,则通过网络报告监控机,显示报警。由此可知,控制器为两个 MCU 并联后与比较模块串联。而每个 MCU 作为一个单独的控制主体,对输入的计轴数据进行计算,由前面 Markov 模型可知,单个 MCU 服从图 4 的状态转移图,故可计算出单个 MCU 子系统的可靠度为:

$$R_{MCU}(t) = \left(\sum_{i=1}^n R_{IPi} \right) \times (p_0(t) + p_1(t) + p_2(t) + p_3(t)) =$$

$$e^{-\lambda_{MCU}t} \times (p_0(t) + p_1(t) + p_2(t) + p_3(t)) \quad (16)$$

解式(11)微分方程,并将经过实验得到的 $p_1, p_2, \mu_1, \mu_2, \lambda_i (i=1, 2, \dots, 6)$ 代入式(11)的解,经过计算得到单个 MCU 子系统工作 10000 h 的可靠度为:

$$R_{MCU} = e^{-1.12156 \times 10^{-6} \times 10^4} \times \sum p_j \approx e^{-5.1917 \times 10^{-2}} = 0.949356$$

其中:

$$p_1 = 0.96, p_2 = 0.98, \mu_1 = 0.96, \mu_2 = 0.92,$$

$$\lambda_1 = 0.01 \times 10^{-6}, \lambda_2 = 0.1 \times 10^{-6},$$

$$\lambda_3 = 0.02 \times 10^{-6}, \lambda_4 = 0.13 \times 10^{-6},$$

$$\lambda_5 = 0.01 \times 10^{-6},$$

$$\lambda_6 = 0.11 \times 10^{-6}$$

在此假设 MCU A 和 B 工作失效率为 λ_{MCU} , 两 MCU 轻载储备失效率为 λ_{MCU}' , 检测切换装置失效率为 λ_k , 则由热备冗余系统可靠度公式可得:

$$R_{Rsys}(t) = e^{-\lambda_{MCU}t} + \frac{\lambda_{MCU}}{\lambda_{MCU}' + \lambda_k} [e^{\lambda_{MCU}t} - e^{-(\lambda_{MCU} + \lambda_{MCU}' + \lambda_k)t}]$$

假设 $\lambda_{MCU}' = 0.1\lambda_{MCU}, \lambda_k = \lambda_{12}$, 则用 R_{Rsys} 的公式, 可计算出控制器工作 10000 h 的可靠度为:

$$R_{Rsys}(t) = 0.949356 + \frac{1.12156}{0.112156 + 0.11246} \times$$

$$0.00937 = 0.996143$$

通过实例分析与计算可知, 嵌入式站间自动闭塞控制器的硬件子系统采用本文的 Markov 模型可量化计算其可靠性; 进而可知, 本文所建立的模型适合复杂系统、新系统设计时可靠性设计, 能够对系统硬件可靠性进行量化计算, 适合错误关联和处理顺序依赖事件的可靠性分析与计算, 同时, 该模型适合对嵌入式系统硬件可靠性进行分配与计算, 具有可接受性、普遍性和数据真实性, 符合 IEC61165 标准。

4 结语

随着嵌入式系统应用的不断发展和需求的不断变化, 使得嵌入式系统在软件、硬件两方面都变得越来越复杂, 从而使嵌入式系统设计面临极大的挑战; 而嵌入式系统设计要使其在软件、硬件等多方面具有较高的可靠性、安全性。本文针对嵌入式系统硬件进行了硬件可靠性建模与分析。

本文针对嵌入式系统硬件动态可靠性分析的难点, 在定义嵌入式系统硬件目标之后, 简单介绍了 Markov 过程的相关理论, 然后建立了单个 IP 硬核和嵌入式系统硬件的 Markov 模型, 最后应用所建立的模型, 对嵌入式站间自动闭塞控制器硬件进行了可靠性计算和分析, 通过计算可知, 本文建立的 Markov 模型能够准确分析其可靠性。因此, 嵌入式系统硬件可靠性的 Markov 模型是可行的, 具有一定的实用价值。

参考文献:

- [1] BOBBIO A, PREMOLI A, SARACCO O. Multi-state homogeneous Markov models in reliability analysis[J]. Microelectronics Reliability, 1980, 20(6): 875-880.
- [2] KUO W, ZUO M J. Optimal reliability modeling: Principles and applications[M]. New York: Wiley, 2003: 20-135.
- [3] ARULMOZHI G. Direct method for reliability computation of k-out-of-n: G systems[J]. Applied Mathematics and Computation, 2003, 143(2-3): 421-429.
- [4] SHERWIN D J, BOSSCHE A. The reliability, availability and productiveness of systems[M]. London: Chapman & Hall, 1993: 20-156.
- [5] PUKITE J, PUKITE P. Modeling for reliability analysis, Markov modeling for reliability, maintainability, safety and supportability analyses of complex systems[J]. New York: IEEE Press, 1998.
- [6] 梅登华, 周美玉. 微机联锁系统的硬件及可靠性分析[J]. 西南交通大学学报, 1997, 32(2): 223-228.
- [7] 郭荣佐, 王霖. 嵌入式系统原理[M]. 北京: 北京航空航天大学出版社, 2008: 1-20.
- [8] 李裕奇, 李永红. 随机过程[M]. 长沙: 国防工业出版社, 2005: 214-252.
- [9] 李能贵. 电子元器件的可靠性[M]. 西安: 西安交通大学出版社, 1990: 9-145.

(下转第 1164 页)

延是相位 I 的 20 倍;高流量场景(场景 3)时,相位 IV 的平均时延是相位 I 的 11.7 倍。即使用 LQF-MWM 表现出非常不公平。在所有调度算法中,最小最大公平调度在不同相位的

平均时延中表现出最小的差异,比例公平调度表现稍逊。但在高流量场景下,最小最大公平调度的平均时延比比例公平调度的平均时延高出 41% 左右。

表 3 场景 2 中车流流量时的仿真结果

调度方案	平均时延/s	相位 I 平均时延/s	相位 II 平均时延/s	相位 III 平均时延/s	相位 IV 平均时延/s	最大时延/s	时延标准差
固定周期	18.8	10.1	42.2	31.9	55.0	195	21.0
LQF-MWM	9.1	4.1	24.1	11.3	65.9	426	17.8
最小最大公平调度	8.5	7.5	12.6	9.6	15.3	31	6.2
比例公平调度	8.0	6.0	15.9	9.3	22.8	63	7.4

表 4 场景 3 高车流流量时的仿真结果

调度方案	平均时延/s	相位 I 平均时延/s	相位 II 平均时延/s	相位 III 平均时延/s	相位 IV 平均时延/s	最大时延/s	时延标准差
固定周期	23.5	14.0	55.4	34.9	78.3	208	23.5
LQF-MWM	16.9	10.0	43.0	17.2	116.7	515	26.5
最小最大公平调度	24.2	25.3	23.6	20.5	29.2	61	12.4
比例公平调度	17.1	14.7	28.3	17.6	46.3	161	12.4

表 2~4 列出的最大时延和时延标准差同样反映出不同调度算法的公平性。LQF-MWM 的最大时延在低流量和高流量下分别是最小最大公平调度的 18.5 倍和 8.5 倍;时延标准差分别是 3.9 和 2.1 倍。而且,比例公平调度的时延标准差与最小最大公平调度的非常相近。

各方面的比较结果得出,比例公平调度同时表现出较低的平均时延和较好的公平性。

4 结语

交通信号实时调度的有效性和公平性研究至关重要。结果表明,最小最大公平交通信号调度对待车辆最公平,但会表现出较差的有效性;但比例公平交通信号调度算法在任何车流强度下,同时表现出较好的平均时延、最大时延和时延标准差。仿真结果为寻找既有效又公平的交通信号的实时调度提出合适的解决方案。

参考文献:

- [1] WEBSTER F V. Traffic signal settings [M]. London: Road Research Technical, 1958.
- [2] ZHOU BIN-BIN, CAO JIAN-NONG, ZENG XIAO-QIN, *et al.* Adaptive traffic light control in wireless sensor network-based intelligent transportation system [C]// IEEE Vehicular Technology Conference Fall. [S. l.]: IEEE, 2010: 1-5.
- [3] MILANES V, PEREZ J, ONIEVA E, *et al.* Controller for urban intersections based on wireless communications and fuzzy logic [J]. IEEE Transactions on Intelligent Transportation Systems, 2010, 11(1): 243-248.
- [4] NEWELL G F. The rolling horizon scheme of traffic signal control [J]. Transportation Research Part A, 1998, 32(1): 39-44.
- [5] AZIMIRAD E, PARIZ N, SISTANI M B N. A novel fuzzy model and control of single intersection at urban traffic network [J]. IEEE Systems Journal, 2010, 4(1): 107-111.
- [6] 何兆成, 杨文臣, 梁诗, 等. 城市单交叉路口交通信号实时优化控制与仿真 [J]. 计算机工程和应用, 2010, 46(33): 239-243.
- [7] 彭成斌, 李新玉, 安利峰. 一种倒计时交通灯的控制算法 [J]. 计算机工程, 2009, 35(14): 243-246.
- [8] MIRCHANDANI P B, ZOU NING. Queuing models for analysis of traffic adaptive signal control [J]. IEEE Transactions on Intelligent Transportation Systems, 2007, 8(1): 50-59.
- [9] 朱文兴, 贾磊. 主干路交通信号控制仿真研究 [J]. 系统仿真学报, 2005, 17(12): 3060-3064.
- [10] WUNDERLICH R, LIU CUIBI, ELHANANY I, *et al.* A novel-signal-scheduling algorithm with quality-of-service provisioning an isolated intersection [J]. IEEE Transactions on Intelligent Transportation Systems, 2008, 9(3): 536-547.
- [11] KUSHNER H J, WHITING P A. Convergence of proportional-fair sharing algorithms under general conditions [J]. IEEE Transactions on Wireless Communications, 2004, 3(4): 1250-1259.
- [12] WIERING M, VREENKEN J, van VEENEN J, *et al.* Simulation and optimization of traffic in a city [C]// IV'04: Proceedings of the IEEE Intelligent Vehicles Symposium. [S. l.]: IEEE, 2004: 453-458.
- [13] TENG XIAO-LIN, PHAM H. Reliability modeling of hardware and software interactions, and its applications [J]. IEEE Transactions on Reliability, 2006, 55(4): 571-577.
- [14] 于敏, 何正友, 钱清泉. 基于 Markov 过程的硬/软件综合系统可靠性分析 [J]. 电子学报, 2010, 38(2): 474-481.
- [15] 郭荣佐, 郭进, 张风荔, 等. 基于 ARM 的嵌入式站间自动闭塞控制器硬件设计 [J]. 微电子学与计算机, 2010, 27(2): 103-106.
- [16] 程凯, 王晓丹, 杨公训, 等. 监控系统硬件电路板可靠性计算 [J]. 计算机测量与控制, 2006, 14(11): 1492-1496.
- [10] ZHANG TIE-LING, XIE MIN. Reliability and modeling of systems integrated with firmware and hardware [J]. International Journal of Reliability, Quality and Safety Engineering, 2005, 12(3): 227-239.
- [11] 任鑫, 赵新文, 蔡琦. 基于状态转移法的冷却水系统动态可靠性分析 [J]. 中国舰船研究, 2011, 6(2): 81-85.
- [12] HASSETT T F, DIETRICH D L. Time-varying failure rates in the availability & reliability analysis of repairable systems [J]. IEEE Transactions on Reliability, 1995, 44(1): 155-160.

(上接第 1156 页)