计算机系统的可靠性技术

李烈彪,李 仙
(重庆大学 计算机学院,重庆 400045)

摘 要:计算机系统在实际工业现场中可能遇到的各种干扰和自身的随机性故障、现场恶劣的环境有可能使计算机系统发生异常,严重时,甚至使计算机系统出现工作混乱,酿成严重事故。因此应采用软件、硬件技术,在提高硬件系统抗干扰能力的同时,利用软件抗干扰方法设计灵活、节省硬件资源的特点,使计算机系统在错综复杂的环境里能保证程序稳定运行,提高系统的可靠性。介绍了计算机系统的软件、硬件可靠性技术,并从永久性故障和暂时性故障两方面对几种双机结构的可靠性进行了研究,证实了任务分担结构在提高计算机系统可靠性方面的优越性。

关键词:计算机系统;双机结构;抗干扰方法;可靠性
中图分类号:TP309.1 **文献标识码**:A **文章编号**:1673-629X(2007)11-0142-03

Dependability Technique of Computer Systems

LI Lie-biao, LI Xian
(Academy of Computer, Chongqing University, Chongqing 400045, China)

Abstract: The computer system is practically used in industry and meet all kinds of molestation and it sown random malfunction, Bad local circumstance may make the computer system crash, even the microcomputer system will be in a mess, causing severe accident. Therefore, should deal with the means of hardware and software, while to enhance the hardware system anti-interference ability, various anti-interference measures by the means of software with its design, the economical hardware resources, must be adopted to guarantee the safe and steady operation of the function in the bad circumstance, and enhances the reliability of the computer system. Introduce the basic conception of two kinds of dependability technique of software and hardware in computer systems in detail, meanwhile analyze reliability of various double-computer models on permanent-malfunction and temporary-malfunction.

Key words: computer system; double model; anti-interference method; reliability

0 引 言

在信息化高速发展的今天,计算机作为新技术革命的重要组成部分,其高可靠性技术是实现信息化社会的关键。

1 计算机系统的可靠性技术

计算机系统的可靠性是指系统在规定条件下、规定时间内完成规定功能的能力[1]。影响系统可靠性的因素主要来自两个方面:一是内部因素即组成系统的器件自身可靠性;二是外部条件的影响。器件的缺陷或损坏将导致系统的永久性故障。而温度、振动、操作人员过失等外部条件变化往往会引发系统间歇性故障。对于不同的故障应采取不同措施,提高系统可靠性[2]。

收稿日期:2007-01-23
作者简介:李烈彪(1949-),男,重庆人,副教授,研究方向为建筑智能化、嵌入式系统。

1.1 容错与避错技术

在系统设计中,主要有两种方法提高可靠性:避错和容错。减小故障出现的概率,解决器件本身缺陷或失效就可用避错法,即选用高品质的器件,在装配阶段进行严格的质量管理与控制,并创造系统良好的工作环境。但高品质器件一般价格高、应用费用大,其次器件本身的生存概率也有限,随着时间的增加,可靠度减少,在实际中应用不多。容错的基本思想是利用外加资源的冗余来掩蔽故障的影响[3]。

1.2 硬件冗余

目前多采用容错设计来提高系统的可靠性。常用的技术是采用冗余结构使构成系统的硬件适当冗余化。双机结构在工程应用中最广泛。其主要有三种:微同步、一用一备与任务分担。微同步是仅由一主机提供输出控制,另一主机在同一输入级上执行同一任务,响应结果通过通讯口送往主机与运行结果比较,不同则进行出错处理,实质上起监督作用;一用一备即主机投入任务处理,备机备用。当检测出主机故障时,备

机投入工作,主机脱机维修;而任务分担方式是两机在同一级上同时投入运行,同步复核,但在输出控制上任务分担,相互监督,当一机输出控制信号时另一机监督任务执行。任务分担较之其他两种方式,有独特的优越性,既可提高系统资源的使用率,又可增强系统运行性能,提高可靠性。仅以塔机遥控系统为例,从永久性故障和暂时性故障两方面进行可靠性分析比较。

1.2.1　永久性故障可靠性分析[4]

(1) 一用一备在系统正常运行时退化为单工模型。塔机系统信息流程如图 1 所示。只要任一芯片出现永久性故障,都将导致系统失效。内部各个芯片按悲观模型处理为串连关系。

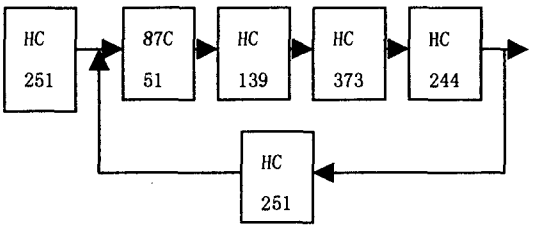

图 1　一用一备系统信息流程

设各芯片可靠度如下:

74HC251 为 $R1$,87C51 为 $R2$,74HC139 为 $R3$,74HC373 为 $R4$,74HC244 为 $R5$。

系统永久性故障可靠度 $Rs1 = R1^2 \cdot R2 \cdot R3 \cdot R4 \cdot R5$。

又设 74HC251 的失效率为 $\lambda1$,87C51 为 $\lambda2$,74HC139 为 $\lambda3$,74HC373 为 $\lambda4$,74HC244 为 $\lambda5$。依据永久性故障分布,可靠度计算公式

$$R(t) = e^{-\lambda t} \qquad (1)$$

得 $Rs1 = e^{-(2\lambda1+\lambda2+\lambda3+\lambda4+\lambda5)t}$

根据元件标准失效率"MIL－HDBK－217B"可计算出各个芯片失效率为:

$\lambda1 = \lambda3 = \lambda4 = \lambda5 = 3.566814 \times 10^{-7}/h$,$\lambda2 = 5.8432 \times 10^{-6}/h$

则 $Rs1 = \exp[-(2\lambda1 + \lambda2 + \lambda3 + \lambda4 + \lambda5)]t = \exp(-7.2699 \times 10^{-6}t)$

由此得系统在不同时间内的永久故障可靠度如表 1 所示。

表 1　一用一备永久故障可靠度

T/h	$Rs1$
10	0.99992730
100	0.99927326
1000	0.99275636
10000	0.92987975

(2) 任务分担由于并未重组系统功能,对某一特定控制任务,就其系统信息控制环节而言,按悲观模型各芯片仍为串连关系,其模型如图 2 所示。

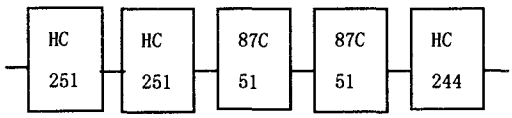

图 2　任务分担串连模型

设 74HC251 的可靠度为 $R1$,87C51 为 $R2$,74HC244 为 $R3$。则系统永久性故障可靠度 $Rs2 = R1^2 \cdot R2 \cdot R3$,且 74HC251 与 74HC244 的失效率 $\lambda1 = 3.566814 \times 10^{-7}/h$,87C51 为 $\lambda2 = 5.8432 \times 10^{-6}/h$,永久性故障分布服从指数分布,由式(1)得到 $Rs2 = \exp(-3\lambda1 - 2\lambda2) \cdot t = \exp(-1.11934 \times 10^{-5}t)$,得到不同时间内永久性故障可靠度如表 2 所示。

表 2　任务分担永久性故障可靠度

T/h	$Rs1$
10	0.99988072
100	0.99888128
1000	0.98886901
10000	0.89410326

(3) 微同步的永久性故障可靠性与任务分担相似,不再赘述。

1.2.2　暂态性故障可靠性分析

(1) 一用一备。当系统内部出现暂态故障时,可通过程序对其进行局部屏蔽。由图 1 可看出当芯片 74HC139,HC373 与 HC244 出现暂态故障时,可由 74HC251 校验检测得到。但 74HC251 不能屏蔽 87HC51 上出现的故障。故系统暂态可靠性模型如图 3 所示,为串并联结构[4]。

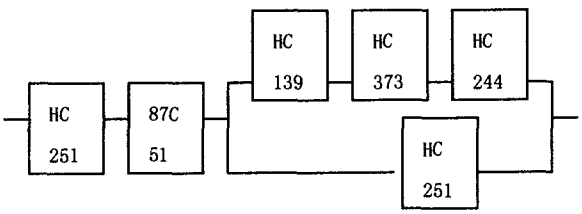

图 3　一用一备串并联结构

系统暂态可靠度:

$RT1 = R1 \cdot R2[1-(1-R1)(1-R3 \cdot R4 \cdot R5)] = R1 \cdot R2 \cdot R3 \cdot R4 \cdot R5 + R1^2 \cdot R2 - R1^2 \cdot R2\ R3 \cdot R4 \cdot R5$

一般而言,暂态故障分布服从韦伯分布,即其概率密度函数为 $pdf = f(t) = a\lambda(\lambda \cdot t)^{a-1}e^{-(\lambda t)^a}$,而可靠度 $R(t) = e^{-(\lambda t)^a}$,其中 a 为形状参数,λ 为标量参数(暂态失效率)。

在塔机系统中,随系统运行时间增加,元件恶化,性能不稳定因素增多,可认为失效率随时间而增加,则

应有 $a > 1$，为方便计算，按失效率线性增加，$a = 2$ 为特例，对系统进行暂态故障可靠性模型分析。又失效率的 90% 置信区间为每万小时 0.1 至 1 之间，5 种类型芯片均取中间量 0.5×10^{-4}/h，则算出

$$RT1 = \exp(-5 \times 10^{-8t^2}) + \exp(-3 \times 10^{-8t^2}) + \exp(-6 \times 10^{-8t^2})$$

由此得一备一用系统暂态可靠性随时间的变化值如表 3 所示。

表 3 一备一用系统暂态可靠性

T/h	Rt1
10	0.99999801
100	0.99970999
1000	0.97999554
5000	0.55374119

(2) 采用任务方式，系统内部双 87C51 通过不同的 74HC251 芯片，接受相同的输入信号，各自单独对任务进行处理，再通过串行复核模块进行结果复核，如果相同则送处理单元 74HC244。74HC244 的输出结果再经 74HC251 反馈给 87C51 进行输出校验。如图 4 所示，74HC251 起到对 74HC244 的故障屏蔽作用，而不能屏蔽 87C51 本身的出错，可靠性模型为两级串联结构。

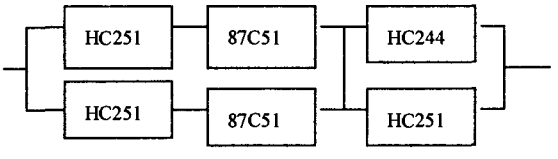

图 4 任务方式模型

此时系统总暂态可靠度：

$$RT2 = [1-(1-R1 \cdot R2)(1-R1 \cdot R2)][1-(1-R1)(1-R3)] = 2R1R2^2 + 2R1R2R3 - 2R1R2^2R3 - R1^2R2^3 - R1^2R2^3R3 + 2R1^2R2^3R3$$

由 $R(t) = \exp[(-0.5 \times 10^{-4}t)^2]$，得

$$RT2 = 4\exp(-0.75 \times 10^{-8}t^2) - 2\exp(-1.0 \times 10^{-8}t^2) - 2\exp(-1.25 \times 10^{-8}t^2) + \exp(-1.5 \times 10^{-8}t^2)$$

计算出不同时间内的可靠度变化值如表 4 所示。

表 4 任务方式可靠度

T/h	RT2
10	0.99999852
100	0.99998999
1000	0.99996888
10000	0.80382789

(3) 微同步时，虽双 87C51 仍通过不同的 74HC251 芯片，接受相同的输入信号，但没有独立的复核模块，结果校验直接由 87C51 之间通过通信完成。所以可靠性模型变为并串联结构，如图 5 所示。

系统总暂态性可靠度：

$$RT3 = [1-(1-R1 \cdot R2)(1-R1 \cdot R2)]R3 = 2R1R2R3 + R1^2R2^2R3$$

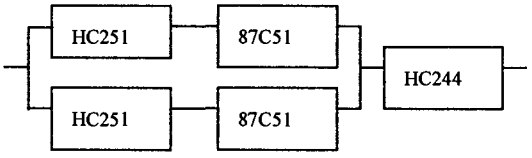

图 5 微同步串联模型

同样由 $R(t) = \exp[(-0.5 \times 10^{-4}t)^2]$ 得 $RT3 = 2\exp(-0.75 \times 10^{-8}t^2) - \exp(-1.25 \times 10^{-8}t^2)$ 得到表 5。

表 5 微同步可靠度

T/h	R T3
10	0.99999974
100	0.99997499
1000	0.99747830
10000	0.65822830

从以上各表可看出，任务分担与微同步，系统在永久性故障可靠性方面略劣于一备一用，而对暂态故障，任务分担最优，微同步次之，一备一用最后。任务分担大大提高了系统对瞬时和间歇性故障的处理能力。

1.3 软件可靠性

然而仅靠硬件的冗余设计实现系统可靠性的提高是极其有限的。使用环境、应用领域、费用等诸多因素往往不允许接受单纯依靠增加冗余器件而提高可靠性的系统。提高软件的可靠性迫在眉睫。

在工程中，有几种有效的软件抗干扰方法：

(1)指令冗余。即在关键地方人为插入一些单字节指令，或将有效单字节指令重写，使程序自动纳入正轨。

(2)拦截技术。是指将乱飞的程序引向指定位置，再进行出错处理。通常用软件陷阱来拦截乱飞的程序，先要合理设计陷阱，再将陷阱安排在适当的位置。软件陷阱是指用来将捕获的乱飞程序引向复位入口地址 0000H 的指令。

(3)软件“看门狗”技术 。若失控的程序进入“死循环”，通常采用“看门狗”使程序脱离。不断检测程序循环运行时间，若发现程序循环时间超过最大循环运行时间，则认为系统陷入“死循环”，运行出错处理[5]。

(4)系统主动复位技术。采用等间隔的脉冲或根据外部条件对系统进行复位唤醒。每次复位后，系统执行相应的程序，完成后及时进入休眠，等待下次复位。这些技术能有效解决死机、程序跑飞等系统缺陷。

2 结束语

可见，要提高系统可靠性，应按系统特性、所确定

(下转第 152 页)

加密是通过对信息的重新组合，使得自由收发双方才能解码还原信息的传统方法，它是以密钥为基础的。网络信息加密的目的是保护网内的数据、文件、口令和控制信息，保护网上传输的数据。网络加密常用的方法有链路加密、端点加密和节点加密三种。链路加密的目的是保护网络节点之间的链路信息安全。端点加密的目的是对源端用户到目的端用户的数据提供加密保护；节点加密的目的是对源节点到目的节点之间传输链路提供加密保护。各税务机关可根据各自的网络情况选择上述三种加密方法。

(2) 身份认证的安全检查。

身份认证是用户向系统出示自己证明的过程，以阻止非法用户的不良访问[4]。有多种方法可以鉴别一个用户的合法性，密码是最常用的，但由于有许多用户采用了很容易被猜到的单词或短语作为密码，使得该方法经常失败。还可以采用其他方法进行识别，例如利用人体生理特征(如指纹、眼睛视网膜底纹等)的识别、智能卡等。

(3) 数字签名。

这种技术主要用于防止非法伪造、假冒和篡改信息。接收者能够核实发送者，以防假冒；发信者无法抵赖自己所发的信息；除合法发信者外，其他人无法伪造信息。发生争执可由第三方做出仲裁。数字签名是基于公共密钥的身份验证[5]。

利用数字签名技术，在税务信息系统网上申报纳税的时候，纳税单位可以利用自己的单位证书在申报材料上签名，这样就可以确保材料的不可篡改性和单位的不可抵赖性。同样，数字签名也可以应用于公文流转当中，领导在审批材料当中利用自己的个人数字证书对其进行签名操作，以代替一般的手写签名，使得办公速度提高，而且更为安全、严密。

4 总 结

随着“金税三期”建设的全面进行，国税网络安全问题需要更加重视。最后需要说明的是，只有将防火墙、VPN、IDS、物理隔离系统和防病毒等安全技术相互结合，才能构建出安全强度更高、安全隐患和漏洞更少、安全风险更低的安全网络，才有可能使用户将关键数据业务安全地拓展到不信任网络上，或在互不信任的网络之间安全地行数据交换，使税务网络真正达到建以致用的目的。

参考文献：

[1] 徐伟清.构建安全网络架构保障网上申报安全[J].上海财税,2002(7):39-40.

[2] 国家税务总局信息中心.金税工程三期:将税收信息化进行到底[J].中国税务,2002(1):26-28

[3] 史文军.税收信息化的技术准备[J].山东税务纵横,2002(5):13-16.

[4] 陈彦学.信息安全理论与事务[M].北京:中国铁道出版社,2000.

[5] Adams C, Lloyd S.公开密钥基础设施——概念、标准和设施[M].北京:人民邮电出版社,1999.

(上接第144页)

的可靠性标准、成本诸因素选择适当的技术，以获得系统最佳的可靠性。

参考文献：

[1] 王东盛.软硬件可靠性设计结合可提高系统可靠性[J].质量与可靠性,1994,28(4):32-36.

[2] 祝 福,肖彦直.计算机控制系统的抗干扰技术[J].计算机与数字工程,2005,33(5):66-68.

[3] 郦 萌.软件容错技术[J].质量与可靠性,1994,21(2):27-30.

[4] 袁由光.可靠系统的设计理论与实践[M].北京:科学出版社,1988.

[5] 温如春,罗小燕,雷小华.单片机系统PC失控的软件措施[J].机电一体化,2004,27(5):95-96.

(上接第148页)

[4] Martin L. Identity-Based Encryption:A Closer Look[J]. The Global Voice of Information Security,2005,12:22-24.

[5] Price G, Mitchell C J. Interoperation between a Conventional PKI and an ID-based Infrastructure[C]//Chadwick D W, Zhao G. Public Key Infrastructure, Second European PKI Workshop:Research and Applications, EuroPKI 2005. Canterbury, UK, 2005. Revised Selected Papers, LNCS 3545, Berlin: Springer-Verlag, 2005:73-85.

[6] 路晓明,冯登国.一种基于身份的多信任域网格认证模型[J].电子学报,2006,34(4):577-581.

[7] Boneh D. Franklin M. Identity-based Encryption from the Weil Pairing[C]//Advances in Cryptology-CRYPTO 2001, LNCS 2139. Berlin:Springer-Verlag,2001:213-229.

[8] Chen L, Harrison K. Certification of Public Keys within an Identity-based System[C]//Information Security. 5th International Conference, ISC, LNCS 2433. Berlin: Springer-Verlag,2002:322-333.

[9] 王建国,李增智,王 宇,等.通用的主动网络安全机制[J].西安交通大学学报,2002,36(8):818-821.