可降级现场总线网系统可靠性的评价方法

黎忠文,雷 航,熊光泽
(电子科技大学计算机学院,成都 610054)

摘 要: 本文根据可降级现场总线网系统及其应用领域的特点,提出把可用性与可靠性(reliability)有机接合起来对系统广义可靠性(dependability)进行评估的方法,该方法建立在系统的性能级之上.

关键词: 现场总线; 可降级系统; 可靠性
中图分类号: TP302.7 **文献标识码**: A **文章编号**: 0372-2112 (2001) 02-0279-03

Dependability Evaluating Method of Degradable Fieldbus System

LI Zhong-wen, LEI Hang, XIONG Guang-ze
(Computer Science and Engineering College, University of Electronic Science and Technology, Chengdu 610054, China)

Abstract: This paper describes a dependability analysis algorithm for degradable fieldbus system. Our algorithm is valid for a general problem model: The system contains several performances (each performance consists of several particular functions), and can be at different performance at the beginning of work. In addition, the system's performance will be changed by some faults as it is working. Finally, the structure of system is scalability. In this paper, reliability and availability are connected to evaluate the dependability of system. Another difference between our algorithm with previous algorithms is that our algorithm is based on system performances.

Key words: fieldbus; degradable system; dependability

1 引言

对于可维修系统,系统可靠性(即广义可靠性,为与狭义可靠性相区别称之为 dependability)在于可靠性(即狭义可靠性,称之为 reliability)、维修性(maintainability)和可用性(availability)三方面[1]. 但人们谈及可靠性时,常常指的是可靠性 reliability. 比如组合、Markov、启发式、Montecorlor[2]及 RMM 等系统可靠性评估方法,尽管它们采用的评价途径不一样,但它们的主要目标都是根据系统的具体要求评估可靠性 reliability (诸如计算失效度、平均无故障时间、系统寿命等一些表征可靠性 reliability 的数学特征量).

随着科技的发展和进步,微处理器被嵌入到各种设备中去,形成分布式控制系统(DCS). 八十年代出现了现场网(规范化的 DCS)的概念,九五年 ISP 和 WorldFIP 两大组织合并,成立了现场总线基金会(简称 FF),致力于推出国际上单一的现场总线网络标准. 据 FF 的定义,现场总线是连接智能现场设备和自动控制化系统的数字式、双向传输、多分支结构的通信网络标准. 其代表有 BITBUS、LONWORKS、CAN 及 MIL-STD-1553B(简称 1553B 总线). 现场总线具有传输抗干扰性强,精度高和开放性等特点.

从系统的角度来看,现场总线系统有多个性能级:故障的不可完全避免性导致系统开工时可能处于不同的性能级上;系统在任务剖面上也可能从一个性能级降到另一个性能级. 系统具有可伸缩性和裁剪性[3]. 很难单纯用可靠性(reliability)来表征系统的可靠性(dependability),因为可靠性(reliability)的计算依赖于系统所处的运行剖面,而系统所处的运行剖面又是由系统的可用性来决定的. 另一方面,从系统的应用角度来看:现场总线系统常用于军备、航空和工控等重要领域. 这些领域对系统的可靠性要求至少包括:系统在任一随机时间可工作的概率以及系统在任务剖面中无故障工作的概率等二方面的指标[4]. 所以在现场总线系统中,可用性和可靠性都是不可忽视的,且有紧密的联系. 如前所述,已有的可靠性评估算法大都重在 reliability 的评估. 基于此,本文提出一种把可用性与可靠性有机结合起来,以评估系统可靠性的方法. 该方法也适于对可靠性进行评估.

2 定义

(1) V_i:系统结构树上的结点, $i = 0, 1, \cdots$: V_i 按其在树上的广度优先搜索顺序进行编号,即从树的第一层(根)开始依层从左至右对结点分别编号为 $V_0, V_1, \cdots$: 为方便说明,文中 V_i 的另一种表示式为 v_jV_k,即 V_j 结点的第 k 个孩子结点. 二种编号可通过一张表一一对应. V_i^d (V_i^e) 是 V_i 结点上的计算(通信)部份.

收稿日期:1999-10-21;修回日期:2000-03-15
基金项目:国防技术预研项目(No. 15.3.1.2)

(2) RV_i^d、RV_i^e:是 V_i 计算、通信部分的可靠性 reliability. $R\Phi \mid R\Psi$ 或 $R\Phi \mid (R\Psi \cap R\beta)$ 分别表示在 Ψ 可靠或 Ψ 与 β 均可靠的条件下 Φ 的可靠性 reliability. Φ、Ψ、β 代表 V_i^d, V_i^e, V_i, …(视具体而定).

(3) AV_i^d、AV_i^e:是 V_i 计算、通信部分的可用性.

(4) V_i:以 V_i 为根的树(子系统,常用于完成某一功能).

(5) $S(V_i, M)$:代表系统结构树以 V_i 为根,有 M 个性能级的可降级现场总线网系统.

$S(V_i, M)$ 的性能集合 $PREF(V_i, M) = \{ {}_{V_i}F_j \mid {}_{V_i}F_j$ 代表 $S(V_i, M)$ 的第 j 级性能, $j = 1, \cdots, M\}$,其中:

${}_{V_i}F_j = \{$为使 $S(V_i, M)$ 能处于第 j 级性能, $S(V_i, M)$ 中所有必须有效的结点$\}$.

$Y({}_{V_i}F_j)$ 为性能的级别,值越小,性能越好.

(6) $D(V_0')$:系统 V_0' 的可靠性(dependability).

3 系统结构的描述

现场总线网系统主要采用主从式结构,见图 1. 总线上,有专门的接口 COMU 板(1553B 的接口板为 MBI)用于将主机与总线连接起来,见图中灰色小圈. COMU 板是总线系统主要的功能部件,物理层、数据链路层和传输层都是在其上实现的. 图 1 中 C 代表主控计算机 CCU,它根据从孩子结点上收集来的系统状态,向各孩子发送控制信息,控制系统工作. CCU 的孩子可以是终端结点 T 或局部控制计算机 PCU(图 1 中用 P 代表,对于以它为根的子树而言,它就是子树的 CCU). T 直接用于执行任务,没有后继,PCU 负责与它的父、子交换控制信息,并协调管理其孩子的工作以完成特定的功能. PCU 的子孙可以是 T 或 PCU,系统结构树的叶子结点必为 T.

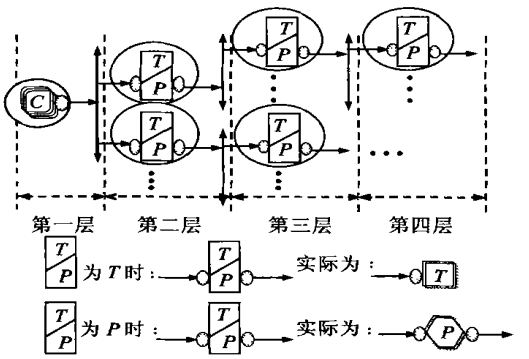

图 1 系统结构树

4 可降级现场总线网系统的可靠性(dependability)

建模假设:

(1) 故障是独立的.

(2) 系统中各组件的修复只能在停机状态下进行.

(3) 系统中各组件是专用的.

(4) 系统的性能具有包含关系. 即上一级性能失去某些功能后,成为下级性能.

4.1 系统的逻辑关系及可靠性(dependability)计算

据现场总线的高可靠性(1553B 的误字率为 10^{-7})、带宽窄(1553B 上,每条消息最大为 32 个字,最小为 1 个字)等特点,对系统可靠性进行分析时,我们把通信部分(总线传输介质及 COMU 板合在一起考虑)与计算部分(CCU、T 和 PCU)串联在一起作为一个结点 V_i($i = 0, 1, \cdots$)进行研究,即图 1 中的椭圆. 每一个 PCU 子树(或 CCU 的孩子 T)为一个子功能. 多个子功能在父结点处组成大功能. CCU 的子树数为系统功能数. 系统的每个性能都由一个或多个系统功能组成. 系统的逻辑关系见图 2.

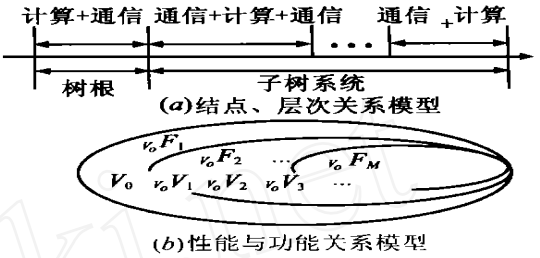

图 2 系统的逻辑关系图

根据建模假设及系统的逻辑关系有:

当 V_i 为 CCU 时:

V_i 的可用性 $AV_i = AV_i^d \times AV_i^e$

V_i 的可靠性 $RV_i = RV_i^d \times RV_i^e \mid RV_i^d = RV_i^d \times RV_i^e$

当 V_i 为 PCU 时:

V_i 的可用性 $AV_i = AV_i^d \times (AV_i^e)^2$

V_i 的可靠性 $RV_i = RV_i^e \times RV_i^d \mid RV_i^e \times RV_i^e \mid RV_i^e \cap RV_i^d$

$= RV_i^d \times (RV_i^e)^2$

当 V_i 为 T 时:

V_i 的可用性 $AV_i = AV_i^d \times AV_i^e$

V_i 的可靠性 $RV_i = RV_i^e \times RV_i^d \mid RV_i^e = RV_i^e \times RV_i^d$

系统 $S(V_0, M)$ 在不同时刻完全可能处于不同的运行剖面,因此在进行可靠性 reliability 计算时必须穷尽其所有的潜在的运行剖面. 由于在系统 $S(V_0, M)$ 中性能级与运行剖面一一对应,所以系统在某一时刻处于某一运行剖面的概率可以用其可用性来表征. 令 $A_{V_0}F_i$ 与 $R_{V_0}F_i$ 为系统 $S(V_0, M)$ 的第 ${}_{V_0}F_i$ 级性能的可用性及可靠性 reliability. 于是:

$$D(V_0') = \sum_{i=1}^{M} A_{V_0}F_i \times R_{V_0}F_i \qquad (1)$$

不妨设 ${}_{V_0}F_i = \{V_0, {}_{v_0}V_1', {}_{v_0}V_2', \cdots, {}_{v_0}V_{Ii}'\}$, $1 \le i, Ii \le M$,下面分别计算 $A_{V_0}F_i$ 及 $R_{V_0}F_i$.

4.2 $A_{V_0}F_i$ 的计算

$$A_{V_0}F_i = A_{V_0} \times A_{V_0}V_1' \times A_{V_0}V_2' \times \cdots \times A_{V_0}V_{Ii}'$$

$$= A_{V_0} \times AV_1' \times AV_2' \times \cdots \times AV_{Ii}' \qquad (2)$$

这里 $V_1', V_2', \cdots, V_{Ii}'$ 仍然是 S 类系统,不妨设 V_j' 为 $S(V_j, W)$, $1 \le j \le Ii$,即 $PREF(V_j, W) = \{ {}_{V_j}F_1, {}_{V_j}F_2, \cdots, {}_{V_j}F_w\}$,下面计算 AV_j,令:

${}_{V_j}F_i = \{V_j, {}_{v_j}V_1', {}_{v_j}V_2', \cdots, {}_{v_j}V_{Ji}'\}$,这里 J 不超过 V_j 的孩子

数且 $1 \leq i \leq W$,则:

$$A_{V_j}F_i = A_{V_j} \times A_{V_j}V'_1 \times A_{V_j}V'_2 \times \cdots \times A_{V_j}V'_{Ji}$$

这里 $_{V_j}V'_1, _{V_j}V'_2, \cdots, _{V_j}V'_{Ji}$ 仍然是 S 类系统,其可用性计算类似上述步骤,单结点的可用性见 4.1.因此经过简单的递归运算就能很容易计算出 $A_{V_0}F_i$,此过程适于编程实现.

4.3 $R_{V_0}F_i$ 的计算

当系统处于 $_{V_0}F_i$ 性能级时,其性能可降级区间为 $[_{V_0}F_{i+1}, _{V_0}F_M]$.不妨设系统由于 $_{V_0}V'_1, _{V_0}V'_2, \cdots, _{V_0}V'_k$ 失败而降级至 $_{V_0}F_k$,k 属于 $[i+1, M]$,所以 $R_{V_0}F_i$ 应为:

$$\begin{aligned} R_{V_0}F_i &= RV_0\Big(\prod_{j=1}^{Ii} R_{V_0}V_j \mid RV_0 + \sum_{k=i+1}^{M}\Big(\prod_{j=1}^{k}(1 - R_{V0}V_j \mid RV_0) \\ &\quad \cdot \prod_{j=k+1}^{Ii} R_{V_0}V_j \mid RV_0\Big)\Big) = RV_0\Big(\prod_{j=1}^{Ii} R_{V_0}V_j' \\ &\quad + \sum_{k=i+1}^{M}\Big(\prod_{j=1}^{k}(1 - R_{V_0}V_j')\prod_{j=k+1}^{Ii} R_{V_0}V_j'\Big)\Big) \end{aligned} \tag{3}$$

$_{V_0}V'_1, _{V_0}V'_2, \cdots, _{V_0}V'_{Ii}$ 分别属于 S 类,其可靠性的计算可参考 4.2 的步骤,根据各自的性能级进行相似计算即可,单结点可靠性的计算见 4.1.经过递归计算,可算出 $R_{V_0}F_i$,此过程适于编程实现.

把式(2)与(3)代入公式(1)就可求得整个系统的可靠性.

5 算法比较

算法(文献[5])评估的目标系统与本算法评估的目标系统在结构上较为类似,不同之处仅在于前者有冗余部件但系统不能降级,后者正好与之相反,所以选择它与本算法进行比较。考虑到上述区别及文献[5]算法只计算了系统可靠性等情况,为了公平比较,设文献[5]算法中冗余部件数参数为 0,而本算法中令系统性能级数参数为 1,且设待评系统只含三层(即 CCU、PCU 和 T 三层,因文献[5]算法只能对三层内的系统进行评估).根据文献[5]算法中的例子,设计了三个待评系统,然后用文献[5]算法和本算法分别对它们进行可靠性评估,结果如下:

表 1　系统可靠性评估表

i	m_i	n_i	l_i	R_{ti}	R_{pi}	R_{ci}	$R1$	$R2$
1	3	2	6	0.995	0.975	0.961	0.887	0.887
2	2	4	8	0.999	0.985	0.974	0.910	0.910
3	4	1	4	0.985	0.975	0.982	0.901	0.901

其中 i 为待评系统序号;n_i、m_i 分别代表系统 i 中 PCU 和每个 PCU 下 T 的个数;l_i 代表为确保系统 i 能正常工作的有效 T 的个数,表 1 中其值的设置正好消除冗余问题;R_{ci}、R_{pi} 和 R_{ti} 分别代表系统 i 中 CCU、PCU 和 T 的可靠性;$R1$ 和 $R2$ 则分别代表文献[5]算法和本算法的评估结果.从表 1 可看出两算法的评估结果是一致的.由于文献[5]算法没有涉及可用性,所以不能在可用性方面对两算法进行直观比较,但把可用性与可靠性 reliability 结合起来是可降级系统及其应用的特点所需要的.此外本算法的评估系统可以是结构可伸缩、可裁剪的可降级系统且不必局限于三层之内,算法还具有对可靠性进行评估的功能,与文献[5]算法相比更具有通用性.

6 结束语

根据系统结构及其应用领域的特点,本文提出了一种建立在系统性能级之上且把可用性与可靠性有机结合起来,对可降级现场网系统的可靠性进行评价的算法,该算法也适用于对系统可靠性进行评估.一些要求较高的现场总线系统常常采用结点镜像、网络备份等冗余措施,以备部件出错时系统重构.下一步将对此类系统的可靠性评估进行研究.

参考文献:

[1] 傅佩琛,赵霖,张军英著.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.

[2] Billiton R, Jonnavithula S. Calculation of frequency, duration, and availability indexes in complex networks [J]. IEEE Trans on Reliability, 1999, 48(3): 25 - 29.

[3] 邱公伟,赵祥元,巫淑萍等著.实时控制与智能仪表多微机系统的通信技术 [M].北京:清华大学出版社,1996.

[4] 曾天翔,丁连芬等译. RELIABILITY DESIGN HANDBOOK(第一卷) [M].北京:航空工业出版,1987.

[5] Vujosevic M, et al. Reliability analyses for a tree-structured hierarchic control system [J]. IEEE Trans on Reliability, 1992, 41(2): 190 - 193.

作者简介:

黎忠文　1970 年生于四川,1991 年毕业于四川师范大学数学系获理学学士学位,1998 年毕业于电子科技大学计算机系获工学硕士学位.现在电子科技大学微机所攻读博士学位.从事高可靠、高安全的实时系统的研究工作.

雷　航　1988 年毕业于电子科技大学,1997 年在该校获博士学位.主要从事实时系统的设计方法和实时软件可靠性评价及测试方面的研究工作.