

文章编号: 1001-0920(2001)02-0226-04

基于现场总线的 $N+M$ 容错控制系统研究

杜志江, 路同浚, 高国安

(哈尔滨工业大学 机器人研究所, 黑龙江 哈尔滨 150001)

摘要: 以机器人化遥控铲掘机为例, 论述了基于现场总线的 $N+M$ 热切换容错控制系统的体系结构、热切换、容错策略等问题。与传统方法相比, 该方法具有结构简单、可靠性高、柔性好等特点, 是提高系统可靠性的一种全新的切实可行的途径, 对工程实际应用具有一定的现实意义。

关键词: 现场总线; $N+M$ 容错; 热切换; 机器人化遥控铲掘机

中图分类号: TP 302.8 文献标识码: A

Research on Fieldbus Based $N+M$ Fault Tolerant Control System

DU Zhi-jiang, LU Tong-jun, GAO Guo-an

(Robot Research Institute, Harbin Institute of Technology, Harbin 150001, China)

Abstract: The overall architecture of the $N+M$ thermal-switching fault tolerant system based on fieldbus is proposed. The fault tolerant strategy and thermal-switching of the system are also discussed in detail. An $N+M$ thermal-switching fault tolerant system based on CAN bus for roboticized remote shovel is introduced. It is indicated that the system is simple, reliable and flexible comparing with the traditional fault tolerant control system.

Key words: fieldbus; $N+M$ fault tolerant; thermal-switching; roboticized remote shovel

1 引言

容错是人们解决控制系统可靠性的有效方法。容错技术的核心是冗余技术, 常见的冗余技术有 $2N$ 型和 $N+M$ 型。后者在成本和可靠性等方面均优于前者, 但如果用传统的技术实现, 不仅部件间连接复杂, 而且连续性较差。因此在工程实践中, $N+M$ 型容错系统反而不如 $2N$ 型应用广泛。

现场总线技术的出现和发展, 为实现控制系统的 $N+M$ 容错提供了方便而可行的途径。现场总线是应用于生产现场、在微机化测量控制设备之间实现双向串行和多节点数字通讯的系统, 也称为开放式、数字化、多点通讯的底层控制网络, 已成为当今

自动化领域最受关注、发展最快的技术^[1]。由于遵循公开、规范的通讯协议, 现场总线控制系统具有很好的扩展能力和互操作性能, 为实现系统容错设计奠定了良好的基础。

2 基于现场总线的 $N+M$ 热切换容错系统

现场总线最重要的特点是将微处理器置入现场设备, 使现场设备智能化, 从而具备了数字通讯、数据处理和故障自诊断能力; 并以简单媒质将现场设备连接成可相互沟通信息、共同完成自控任务的网络系统。利用现场总线的互操作性能, 可完成基本

收稿日期: 2000-03-13; 修回日期: 2000-07-17

作者简介: 杜志江(1972—), 男, 辽宁北镇人, 博士生, 从事智能机器人技术及应用等研究; 路同浚(1939—), 男, 天津人, 教授, 从事智能机器人技术及应用研究。

单元与备用单元之间的信息传递和动态热切换, 实现系统的容错控制。

2.1 系统结构模型

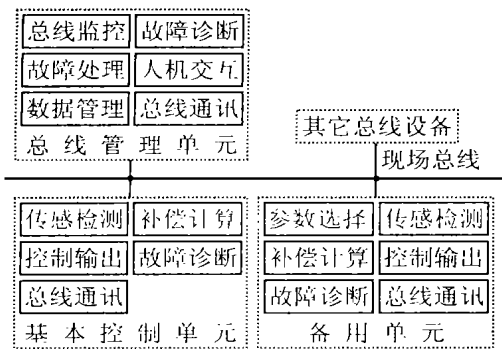


图 1 基于现场总线的 $N + M$ 容错系统模型

一个基于现场总线的 $N + M$ 容错系统应包括以下几部分: 一个总线管理单元, N 个基本控制单元, M 个备用单元和其它总线设备(见图 1)。总线管理单元是整个系统的灵魂, 它具有总线监控、故障诊断、故障处理(报警、切换备件或降级重构)、数据库管理、人机交互和总线通讯能力。 N 个基本控制单元分别对应于现场的 N 个受控对象, 具有传感检测、补偿计算、控制输出、故障诊断和总线通讯等功能, 完成对现场受控对象的直接控制。备用单元含有每个现场受控对象的控制模型和控制能力, 可对任一基本控制单元进行冗余。因此, 除基本控制单元应具有的功能外, 它还应具有按切换命令选择控制模型和控制参数的能力。备用单元的数量 M 主要由以下几方面因素确定: 1) 总线驱动能力; 2) 系统可靠性要求; 3) 任务时间。设现场总线驱动能力为 D , 当 $N < D$ 时, 因素 1 可以忽略。当基本单元与备用单元的可靠度均为 R , 且系统切换过程、总线通讯及总线管理单元等可靠度为 1 时, $N + M$ 容错系统的可靠度可近似表述为

$$R_{N,M} = \alpha [1 - (1 - R)^{M+1}]^N \quad (1)$$

其中 α 为近似系数。已知 R 和 $R_{N,M}$, 即可求得 M 。另外, Losq 指出^[2]: 在给定任务时间的条件下, 对系统最佳备件数有一定限制, 对于任务时间极短的情况, 一个备件为最好; 当任务时间小于单模平均寿命的 $1/10$ 时, 最佳备件数不能超过 5 个。

2.2 基本单元与备用单元之间的热切换

由于现场总线遵循公开、规范的通讯协议, 并且许多厂商为方便用户, 将通讯协议固化在集成芯片内, 因此通过简单的物理媒质(如双绞线)即可实现设备之间的串行通讯, 且具有很高的通讯速率和可靠性。但是, 为了实现基本控制单元与备用单元之间

的无扰热切换, 需要将基本控制单元的现场数据动态地传送给备用单元, 这就需建立存储这些数据的数据库。当基本单元出现故障时, 则无法完成数据传送任务, 因此数据库维护和数据传送工作应由总线管理单元完成。这也是设立总线管理单元的基本目的之一。

需要存储的信息包括: 操作指令、现场信息(传感器、执行器)、设备自身状态及故障诊断结果。整个数据库划分为两部分, 即动态数据库和静态数据库。首先, 由每个总线单元发来的信息数据经总线管理单元打包处理后, 存储在动态数据库中, 经过一段时间(现场操作开始到本次操作结束), 总线管理单元将数据包从动态数据库中清除, 并转存到静态数据库中保存。如果基本单元在操作过程中出现故障, 总线管理单元则从动态数据库提取相关数据, 通过总线传递给备用单元, 实现基本单元和备用单元之间的热切换。二者之间的信息交换如图 2 所示。

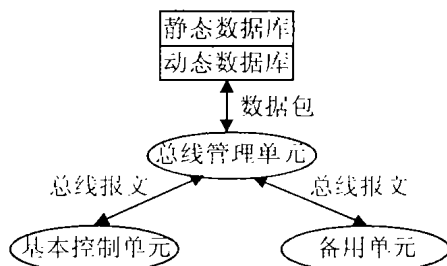


图 2 基本单元与备用单元间的信息交换

由于数据库容量有限, 需要对数据包进行压缩处理, 并在静态数据库中按 FIFO 顺序动态移动, 超出存储容量极限的数据包将自动遗弃。静态数据库必须具有至少一个工作日的存储容量。一个工作日结束后, 将数据读到外设中分析和保存。

2.3 故障容错策略

系统出现的故障可分为暂时性故障和永久性故障。对于暂时性故障, 可通过总线管理单元控制故障单元“重试”消除。永久性故障包括传感器故障、执行器故障和基本单元故障等。对于传感器或执行器故障, 可采用“降级重构”的方法, 即将出现故障的控制过程从系统中剔除, 以丧失部分功能来保证整个系统的稳定性。对于基本单元故障, 总线管理单元根据当时备用单元的情况做出故障处理, 如果尚有状态完好的备用单元, 总线管理单元则将故障单元的现场信息传递给备用单元, 使备用单元进入实际控制; 如果此时没有处于完好状态的备用单元, 则将系统“降级重构”。

对于上述每一操作, 总线管理单元都通过声光

进行报警。维修人员在工作结束后排除故障,并将系统恢复到原始状态。

3 实例

我们利用 CAN 总线实现对机器人化遥控铲掘机的 $N + M$ 热切换容错控制。CAN 是控制局域网的简称,最早由德国 BOSCH 公司推出。CAN 总线具有突出的可靠性、实时性和灵活性,其总线规范已被定为国际标准 ISO 11898,被公认为是目前最具有发展前途的现场总线之一^[3]。

机器人化遥控铲掘机(RRS)是以普通液压式铲掘机为载体,进行机器人化遥控改造,在保留手动驾驶功能的基础上,增加了自主运行和无线遥控功能。RRS 用于冶金、采矿和抢险等危险或苛刻的作业环境,以取代人工操作^[4]。因此要求 RRS 必须具备很高的可靠性,以满足实际使用要求。

3.1 系统组成

RRS 具有换档、换向、左制动、右制动、动臂、铲斗和油门 7 个受控对象,分布于车体的不同部位。各个受控对象均由电液操纵机构组成,由一个基本控制单元控制,形成基于 CAN 总线的现场总线控制系统。CAN 总线媒质选用双绞线,总线控制器选用 Philips 公司的 SJA 1000,总线物理接口为 82C250。这两种芯片都具有很高的可靠性,且应用方便。系统中还包含无线通讯单元,以满足无线遥控功能。该单元处于环境较好的中央控制柜中,失效概率较低。我们只对 7 个基本控制单元进行冗余,以实现对该系统的 $N + M$ 热切换容错控制。系统结构如图 3 所示。

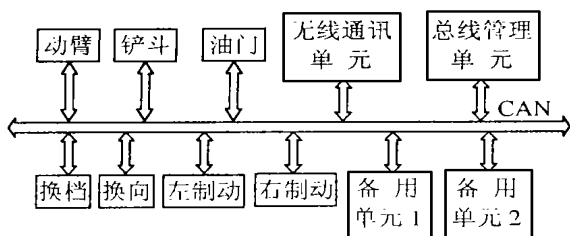


图 3 基于 CAN 总线的 RRS $N + M$ 容错系统

3.2 M 的确定及系统可靠度

CAN 总线具有良好的驱动能力,由 PCA82C250 驱动的物理总线可直接挂载 110 个总线设备,因此 M 的数量可不受总线驱动能力的限制。综合考虑 2.1 节关于 M 的确定因素,确定 $M = 2$,即系统中每个基本控制单元具有两个备件。设基本控制单元和备用单元单模可靠度为 0.90,并假定无线通讯单元、总线管理单元、切换过程和总线通讯的可靠度为 1。在

不进行 $N + M$ 容错时,系统可靠度近似为 $R = 0.90^7 = 0.478$,显然系统的可靠性很差;采用 $N + M$ 容错后,由式(1) ($\alpha = 0.94$) 可计算出系统的可靠度近似为 $R_{7,2} = 0.94 \times [1 - (1 - R)^{2+1}]^7 = 0.933$ 。采用 $N + M$ 容错后,在不增加单件硬件成本的前提下,系统的可靠度有了显著提高(增加了近 1 倍)。

3.3 系统操作原理

无线通讯单元负责接收由遥控器发来的本机遥控命令,经解码、校验形成符合 CAN 协议标准的“指令报文”传送到总线上。总线管理单元接收到“指令报文”后将其存储在动态数据库中;基本控制单元接收到“指令报文”后对其进行相容性检查,若相容,则执行报文中所含遥控命令。系统运行正常时,基本控制单元将遥控指令、现场信息、设备自身状态等整理成“现场报文”发送给总线管理单元,存储在动态数据库中。一个操作周期(从发送“指令报文”到遥控命令执行完毕)结束后,总线管理单元对动态数据库进行整理,保留本周期“现场报文”,抛弃“指令报文”,并将上一操作周期基本控制单元发来的“现场报文”压缩后存储到静态数据库中。

如果在操作过程中出现故障,系统则按以下两种情况进行处理:

1) 传感器或执行器故障:基本控制单元执行遥控命令时,如果检测出传感器或执行器故障,则立即发“故障报文”给总线管理单元,总线管理单元接到“故障报文”并确认后,将系统“降级重构”,维持系统的整体稳定性。

2) 基本控制单元故障:如果总线管理单元收到“指令报文”后,长时间(根据实际优化设定)收不到应执行该命令的基本控制单元的“现场报文”或“故障报文”,总线管理单元则通过总线呼叫该控制单元。如果应答,总线管理单元则命令基本控制单元“重试”“指令报文”中的遥控指令;如果控制单元不应答或“重试”后仍不正常,则判定为基本控制单元故障。这时总线管理单元应启动备用单元状态检测程序。如果此时尚有处于完好状态的备用单元,则立即将动态数据库中的“指令报文”和该基本控制单元上一操作周期发来的“现场报文”发送给备用单元,并控制备用单元选择相应的控制模型和控制参数进入实际操作,实现基本控制单元与备用单元之间的无扰热切换;如果此时没有完好的备用单元,总线管理单元则将系统“降级重构”。总线管理单元控制流程图略。

(下转第 232 页)

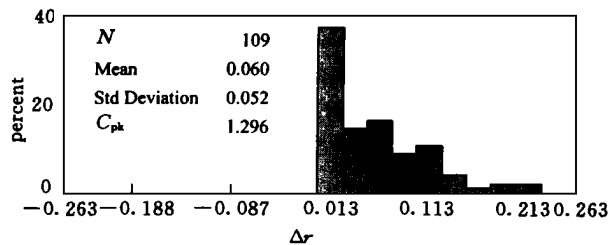


图2 Δr 控制情况

计算 C_{pk} 的下限值为 -0.260, 上限值为 0.260

过长时间的跟踪分析,在逐月进行SPC分析的同时计算出 C_{pk} ,利用多元回归分析和方差分析,找出 Δr 与 C 含量之间的关系。根据得到的关系及实验分析验证,调整工艺参数控制,使 Δr 值的控制情况大为改善。改善措施实施后的第一个月, Δr 值不符改判率就已控制在目标(5%)以内,且控制水平逐步提高。两个月后 Δr 值超标改判率为0, C_{pk} 值为1.65,达到历史最好水平。

4 结 语

在企业内大范围使用数据仓库技术,能有效地管理庞大的信息资源,更重要的是改变以往数据库

技术“以数据为中心”的理念,强调“以主题、业务分析为中心,以决策为目的”的思想,在质量分析工作中应用数据仓库,可大大提高质量管理工作的效率,管理大量洁净的模式一致的数据,为工业企业充分利用数据资源提供了途径。基于数据仓库的应用不但能节省用户的大量时间,而且可提供既准确又有权威性的统计分析结果,为及时掌握产品的质量趋势提供有效的保证,为企业的生产经营决策提供有力的支持。

参考文献:

- [1] M C Wu, A P Buchmann. Research issues in data warehousing[A]. Proc of BTW 97[C]. Ulm, 1997. 61-68.
- [2] 王珊. 数据仓库技术与联机分析处理[M]. 北京: 科学出版社, 1998.
- [3] H S Gill. 数据仓库——客户/服务器计算指南[M]. 王仲谋译. 北京: 清华大学出版社, 1997.
- [4] C Bontempo, G Zagelow. The IBM data warehouse architecture[J]. Comm of the ACM, 1998, 41(9): 38-48.

(上接第228页)

4 结 论

利用现场总线构成的 $N + M$ 容错系统,可以方便地实现基本控制单元与备用单元之间的无扰热切换和各种故障容错策略。与传统的方法相比,该系统具有结构简单、可靠性高、柔性好等特点,对提高复杂系统的可靠性很有成效。本文阐述的基于CAN总线的机器人化遥控铲掘机 $N + M$ 热切换容错系统,不仅适用于RRS系统,而且适用于其它工业控制系统。

参考文献:

- [1] 阳宪惠. 现场总线技术及应用[M]. 北京: 清华大学出版社, 1999.
- [2] Losq J. Influence of fault detection and switching mechanisms on the reliability of stand-by system[A]. Proc 5th Int Symp Fault-tolerant Computing[C]. American: IEEE Computer Academy Fault-tolerant Technology Committee, 1975. 81-86.
- [3] 邬宽明. CAN总线原理和应用系统设计. 北京: 北京航空航天大学出版社, 1996.
- [4] 路同浚, 孟宪超, 吴平川, 等. 机器人化炉渣铲掘机的研究[J]. 机器人, 1999, 20(4): 317-321.