

文章编号:1000-8055(2012)04-0920-10

开放式 FADEC 系统的数据总线研究

刘冬冬, 张天宏, 陈 建

(南京航空航天大学 能源与动力学院, 南京 210016)

摘 要: 研究了容错数据总线这个从集中式向开放式架构过渡的关键技术. 在深入研究确定性、一致性、开放性、拓扑结构、调度策略、容错机制和传输带宽等开放式 FADEC(全权限数字电子控制)数据总线关键特征的基础上, 分析了总线数据传输的时间不确定性问题. 从性能、可靠性和可用性的角度深入研究了 TTP/C(time-triggered protocol/automotive class C), ARINC659, TTCAN(time-triggered controller area network)和 FlexRay 这 4 种时间触发架构数据总线的关键特征. 研究结果表明: TTP/C 总线是开放式 FADEC 的最佳选择. 最后提出了一种基于 TTP/C 总线的航空发动机模块化 DEEC(digital electronic engine controller)硬件架构.

关 键 词: 开放式 FADEC(全权限数字电子控制); 容错数据总线; 确定性; 时间触发; 事件触发; TTP/C(时间触发协议/C 级)总线

中图分类号: V233.7

文献标志码: A

Study on data bus of open FADEC system

LIU Dong-dong, ZHANG Tian-hong, CHEN Jian

(College of Energy and Power Engineering,

Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)

Abstract: The study of fault-tolerant data bus is one of the key technologies for transition from a centralized architecture to an open architecture. The key characteristics of data bus for open FADEC (full authority digital electronic control) system such as consistency, open, transmission bandwidth, scheduling strategies, topologies and fault-tolerant mechanism were studied. Time uncertain problem of bus data transmission was analyzed. The key characteristics of four data bus based on time trigger architecture, which are TTP/C (time-triggered protocol/automotive class C), ARINC659, TTCAN and FlexRay (time-triggered controller area network), were researched from the angle of performance, reliability and availability. The study results show that the TTP/C data buses is the best choice for open FADEC system, and the hardware architecture of modular DEEC (digital electronic engine controller) based on TTP/C data bus was proposed finally.

Key words: open FADEC (full authority digital electronic control);
fault-tolerant data bus; determinism; timer trigger; event trigger;
TTP/C (time-triggered protocol/automotive class C) data bus

当前航空发动机 FADEC(full authority digital electronic control)系统普遍采用集中式双通

收稿日期:2011-06-05; 修订日期:2011-09-02

基金项目:江苏省研究生培养创新工程(CX09B_086Z); 2011 年江苏省优势学科建设项目

作者简介:刘冬冬(1983—),男,陕西西安人,博士生,主要从事开放式 FADEC 系统建模与容错控制技术研究.

道冗余架构,这种架构的计算资源高度集中在机箱内部的微处理器上,这带来了以下问题^[1-5]:①复杂、笨重的布线管理,而且这种布线结构对于不同的发动机都是独一无二的;②数据采集预处理、控制及诊断等实时任务的开发、测试、验证难度极大;③高度铰链的系统架构给故障检测、隔离和重构等容错设计带来的极大挑战;④系统软件模块之间高度铰链,任意局部的软件修改都可能导致很大一部分系统软件需要额外的硬件在回路测试和机载测,导致系统后期的升级、维护成本急剧增加;⑤软/硬件模块可重用性差,在设计新的FADEC系统时大部分模块必须重新设计、验证,降低了开发效率,增加了开发成本。

因此,当代集中式FADEC系统的软件和硬件的实施是针对特定发动机的高度定制过程,设计、测试、集成、制造、维护高度定制与结构复杂的集中式FADEC系统的LCC(life cycle cost)是非常高昂的^[2]。目前航空发动机控制正朝着进气道/发动机/尾喷管综合控制、飞行/推进系统综合控制、直接推力/喘振裕度控制等方向发展,并集成状态监视和健康管理功能^[3],控制功能和控制变量的增加使得FADEC系统的研制难度、周期和费用不断增加。若仍采用传统的集中式结构,上述的5个问题将会更加突出。因此基于总线的软/硬件模块可重用,易升级的开放式多处理器分布式体系结构将是下一代FADEC系统的必然选择^[2-5]。开放式FADEC的实施需要解决高温电子器件、分布式供电、容错数据总线、智能传感器和智能执行机构等关键基础技术问题^[4-5]。在高温电子器件技术成熟之前,有必要提前研究除温度外其他所有特性均满足开放式FADEC需求的数据总线,基于该总线构建开放式FADEC系统快速原型,研究关键的控制和诊断功能。

在这种背景下,本文将深入研究开放式FADEC系统的体系结构及其数据总线的关键技术特征,分析总线数据传输的不确定问题,从性能、可靠性和可用性的角度出发深入研究TTP/C(time-triggered protocol/automotive class C),ARINC 659, TTCAN(time-triggered controller area network)和FlexRay这4种时间触发架构数据总线的关键特性,给出最优的总线方案。

1 系统架构及其总线特征研究

取决于高温电子器件和智能机电系统的技术水平,开放式FADEC可以采用图1中的4种架构实施。图1(a)所示的模块化DEEC(digital electronic engine controller)将控制器机箱内的核心计算、输入/输出等电路模块通过容错数据总线互联,构成一个分布式冗余度数字处理机。这种架构可以简化并行、实时任务的开发和测试难度,通用的电路模块可用于快速构建面向不同发动机的DEEC,美国Honeywell公司2008年已经开发出

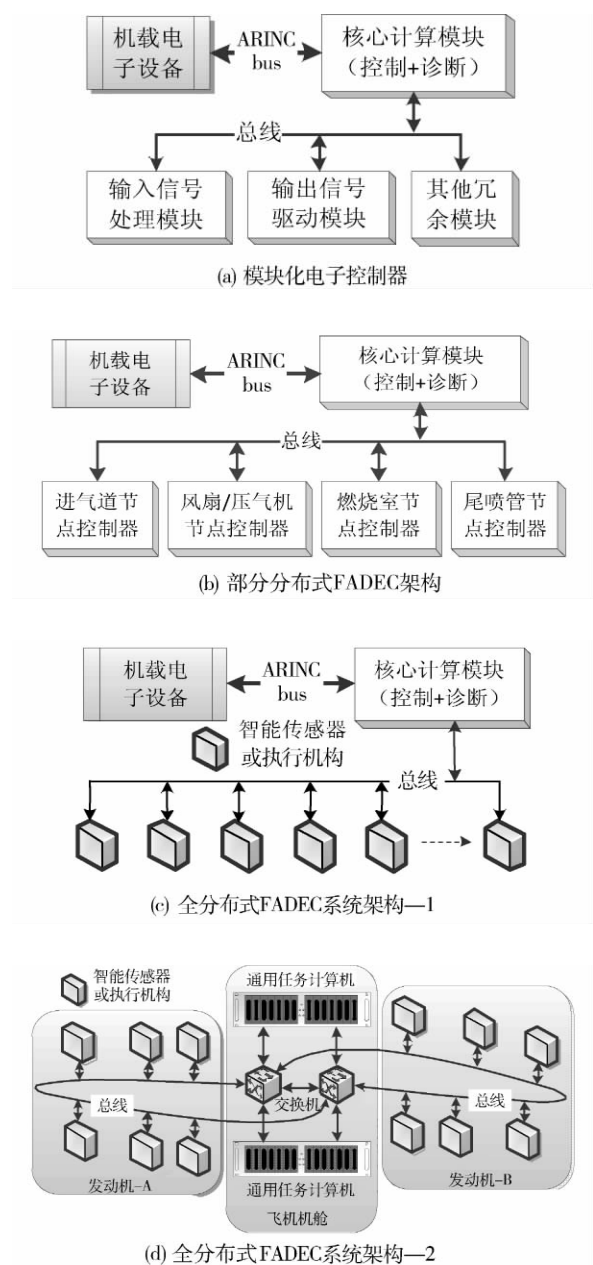


图1 典型的开放式FADEC系统架构

Fig. 1 Typical system architectures of open FADEC

这种架构的 DEEC, 并成功应用于多型发动机. 图 1(b) 所示的部分分布式架构将 FADEC 系统按照功能分为核心计算模块和进气道、风扇、燃烧室、尾喷管等节点控制模块, 通过容错数据总线将各个模块互联^[6]. 这种架构可以减轻线缆质量, 各个子节点也具备一定的可重用性. 部分分布式 FADEC 架构目前还处于研究、实验阶段, 国外预计 2015 年左右将首先在大型民用发动机上使用^[5]. 图 1(c) 所示的全分布式架构给系统的每个传感器和执行机构都分配一个微处理器, 使其成为智能传感器和智能执行机构, 并将这些智能模块通过容错数据总线与核心计算模块互联. 这是理想的开放式 FADEC 架构, 能最大限度的减轻线缆质量, 通用的智能传感器和执行机构可快速构建用于不同发动机的 FADEC 系统. 受制于高温电

子器件及分布式供电等技术水平限制, 全分布式 FADEC 架构目前还处于基础技术研究阶段, 国外预计 2030 年左右进入工程应用阶段^[5]. 图 1(d)^[6] 和图 1(c) 的架构类似, 只是将 FADEC 的核心计算模块移到了飞机内部的通用任务计算机. 除前面几种架构的优点外, 由于通用任务计算机安装在温度适中、空间大的飞机内部, 可以采用异地备份、多路表决、加固等可靠性措施和多线程并行计算技术, 这将极大的提高 FADEC 系统的计算性能和任务可靠性.

这几种开放式 FADEC 系统本质上都属于分布式多余度多处理器的容错数字控制系统, 其核心组件是实现节点间信息交换的数据总线. 如图 2 所示, 总线的本质作用是为运行在各个节点处理器的诊断和实时控制等应用程序提供一个虚拟

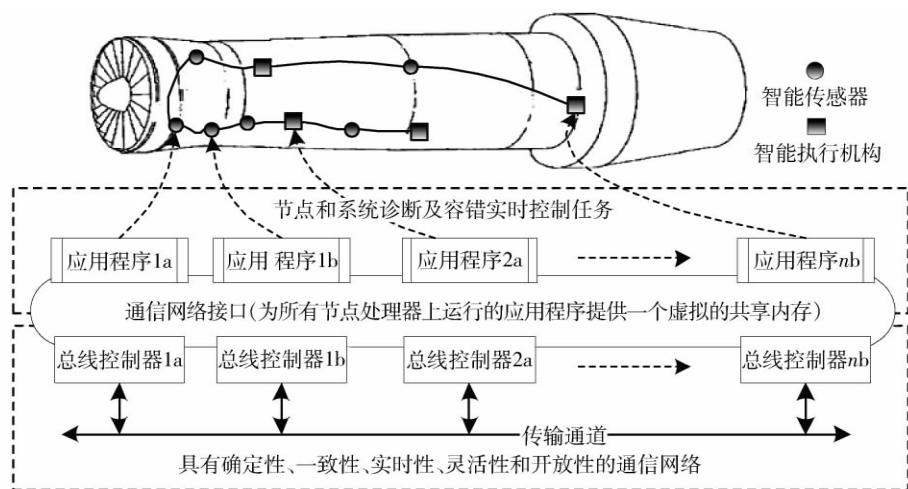


图 2 分布式 FADEC 系统中数据总线的功能说明图

Fig. 2 Function of data bus for distributed FADEC system

的共享内存, 为实现此目标总线应具备以下特征:

1.1 确定性

数据通过总线在发送和接收节点之间传递时存在延时和抖动现象. 发送开始和接收完成事件之间的时间间隔称为传输延时, 这个时间受数据帧长度、传输带宽、总线调度和传输距离的影响. 抖动是指两次完全相同的数据传输延时之差, 这个时差受到节点晶振漂移、传输阻塞及物理层特性变化等因素影响. 所谓确定性是指总线数据传输的延时和抖动必须有确定的边界^[7-8], 这是开放式 FADEC 这类硬实时控制系统在设计前就必须确定的参数.

1.2 一致性

运行在开放式 FADEC 系统中各个节点处理器上的实时数据采集、诊断和容错控制等任务是紧密耦合地. 所有节点必须有一个统一的时间和系统状态信息才能协调一致的完成各自任务, 这个统一的信息就是开放式系统中的时间和成员关系一致性^[9]. 时间一致性服务确保所有正常节点之间的当地时间误差在设定的范围内, 成员关系一致性服务将某个通信节点失效事件实时通知所有其他节点, 这两个一致性服务为开放式 FADEC 系统的应用层提供了一个统一的多核处理平台. 节点的晶振频率漂移和单粒子反转事件会破坏时间一致性, 节点失效、SOS(slight of speci-

fication) 等故障会破坏成员关系一致性^[10], 因此开放式系统的一致性服务还必须具备容错特性. 鉴于一致性的重要性, 容错一致性服务应由总线协议层以基本服务的形式提供给 FADEC 系统应用层. 也可以在应用层通过软件实现一致性服务, 但会增加应用软件的开发和集成难度, 并降低一致性服务的实时性和可靠性.

1.3 容错机制

应用于 FADEC 系统等航空领域数据总线的永久失效故障率应低于 10^{-6} 次/h, 而普通电子元器件的故障率约为 10^{-4} 次/h^[9-10]. 为了实现数据总线的高可靠性指标, 需要采用多余度体系结构和完备的容错机制. 容错机制的目的是阻止由任意单个故障导致整个通信永久失效事件, 完备的

容错机制是以精确的故障假设为前提的, 在共享信道的总线型拓扑结构中一般会发生表 1 所示的 5 种致命故障. 总线应能在通信协议层实时的检测、隔离这些故障, 并重构通信系统, 确保任意单故障不能使通信失效. 当表 1 之外的极低概率致命故障(例如强干扰导致的瞬态多故障)发生时, 协议若没有对应的容错机制, 则应采取 NGU (never give up) 策略^[11], 即协议层必须能检测到这种未知故障模式, 并通知应用层启动复位操作使开放式系统恢复到一个确定的状态重新开始通信. 评估总线协议 NGU 策略好坏的一个重要指标是从故障发生到通信恢复的时间间隔, 这个时间间隔越短越好. 对于 FADEC 系统, 在执行 NGU 复位过程中必须确保执行机构处于安全位置.

表 1 致命故障模式^[9-12]
Table 1 Characteristics of different critical failure modes

故障模式	阻塞故障	化妆舞会	SOS	节点失效	邻近空间故障
故障特征	故障节点独占传输通道	故障节点的消息 ID(识别码)被修改	故障节点的消息被部分节点接受, 部分节点拒绝	故障节点失去通信能力	节点或传输通道物理损坏
故障影响	若故障持续将导致整个通信失效	若故障在整个系统传递将导致通信失效	破坏底层节点间的成员关系一致性, 并导致系统分裂为两个并行的子集	破坏底层节点间的成员关系一致性	单个节点通信失效或整个通信系统失效

1.4 拓扑结构和调度策略

总线拓扑结构包括总线型、星型、环形或者这几种类型的混合. 文献[10-11]的研究结果表明, 星型架构可以完全避免 SOS 故障, 并对临近空间故障有较强的免疫能力, 具有最高的可靠性. 但是对安装空间有限的发动机, 采用星型架构将增加线缆物理质量和系统结构复杂度. 而总线型架构结构简单、易扩展, 即使发生 SOS 故障也可以采用容错机制进行探测和隔离. 因此, 应用于开放式

FADEC 系统的总线协议应支持共享信道的总线型拓扑结构.

此外, 为了保证 FADEC 系统的开放特性, 总线协议应具备灵活的组网能力和调度策略. 如图 3(a)所示可以通过网关扩展一个局部子网络, 该模块和核心节点的只有有限的状态信息交换. 如图 3(b)所示通过多个通信周期组成一个集群周期, 在每个集群周期内可以完成特殊的周期性非实时数据传输任务.

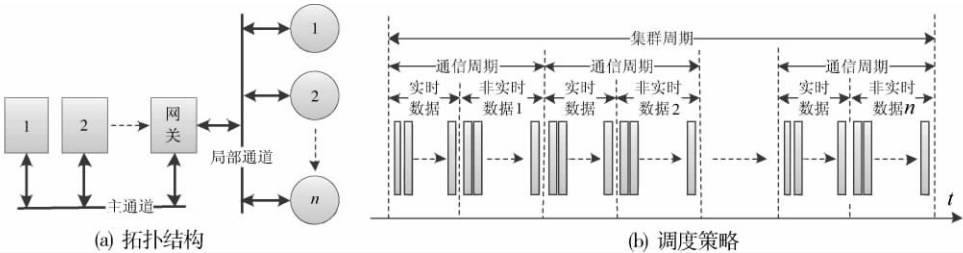


图 3 总线的拓扑结构和调度策略

Fig. 3 Scheduling strategy and topology of data bus

1.5 传输带宽

在共享信道的总线型通信架构中,传输带宽取决于消息结构、节点数目和控制步长^[13-15].本文以复杂的民用大涵道比涡扇发动机的全分布式FADEC系统为例论证传输带宽需求,这代表了FADEC系统对总线传输带宽需求的上限.

为了保证系统架构的一致性和数据传输可靠性,除有效值和ID识别码外消息还需要包含节点当地时间、成员关系列表、节点BIT(built-in test)信息和消息校验等附加信息,本文采用表2所示的消息格式.民用大涵道比涡扇发动机包含用于控制、状态监视的冗余传感器及冗余执行机构,除

智能执行机构自身的反馈传感器外,其它所有的传感器和执行机构都需连接在总线上.以某型发动机为例,需要通过总线互联的传感器和执行机构约为60个^[13-15].控制步长取决于传感器时间常数、执行机构响应时间和控制规律,在集中式架构中发动机的主控制步长一般为20ms,执行机构小闭环控制步长为5ms,为了评估出带宽需求上限,取控制步长10ms.分布式FADEC系统在每个控制步长完成的任务包括传感器数据采集预处理、节点和系统级故障诊断、数据传输、控制规律计算及执行机构小闭环控制等,分配给控制用数据的总线传输时间为控制步长的20%.按照前面的分

表 2 数据帧结构(单位:Byte)
Table 2 Frame structure(unit:Byte)

消息头	消息 ID	有效值	BIT 信息	时间信息	成员关系列表	预留	校验信息
2	4	4	4	4	4	4	4

析,经过简单计算可得此型民用大涵道比涡扇发动机全分布式FADEC系统对总线的传输带宽需求为7.2Mbps.

此外,未来的系统功能扩展也将带来不确定的带宽需求,例如部件主动控制和健康管理.这些功能往往需要对传感器进行高频采样,有的高达数千赫兹^[14],这将极大地增加总线传输负担.可以采用两个方法来解决这个不确定的带宽需求,一个是采用独立的传输通道来传输这些数据,但这将增加系统的物理质量和结构复杂度;另外一个方法是采用具有灵活拓扑结构和调度策略的总线协议,如图2所示,在局部网络实现部件主动控制功能模块,该模块只向核心任务计算机发送状态信息.与控制相比用于状态监视和健康管理的对实时性要求相对较低,而在一个控制步长内控制用数据传输任务只有20%的时间占用总线,可将健康管理用的非实时数据在其余80%的时间传输到核心任务计算机,并在一个集群周期内完成一个完整健康管理处理周期所需的数据传输.

1.6 开放性

总线的确定性、一致性和容错等功能与系统可靠性高度相关,需要经过复杂的设计验证并实时的实现.通过总线控制器以标准组件的形式封装这些功能,可降低应用软件的复杂度和开发成本、简化开放式系统的开发和集成过程.总线控制器应采用FPGA(field programmable gate array)

方式实现,以消除组件废弃带来的成本风险.确定性、一致性和足够的传输带宽是数据总线为开放式FADEC系统提供的基本服务,而完备的容错机制保证在部件故障情况下仍能提供上述基本服务,灵活的拓扑结构和调度策略是为了降低系统开发、测试、集成和升级、维护难度,提高开发效率、降低全寿命周期费用.

2 数据传输的时间不确定性研究^[14-17]

目前应用于不同安全等级的商业化的标准数据总线类型很多,例如CAN(controller area network),ARINC 664, ARINC 629, ARINC 659, FlexRay, Ethernet, TTCAN, MIL-STD-1553B, TTP/C等.不同总线的协议差别很大,但所有的总线协议都基于两个基本架构设计,一个是ETA(event trigger architecture),一个是TTA(timer trigger architecture).CAN, ARINC 664, Ethernet, ARINC 629, MIL-STD-1553B等都采用ETA架构或其改进. TTP/C, ARINC 659, FlexRay, TTCAN则采用TTA架构.如图4所示,ETA架构中的任何节点可以在任何时候向总线发送数据,具体发送时刻取决于外部事件的发生时刻,易发生总线冲突.普通Ethernet协议采用CSMA/CD(carrier sense multiple access with collision detection)机制避免总线冲突,CAN协议采用CSMA/CA+AMP(carrier sense multiple access with collision avoidance + arbitration on mes-

sage priority)机制避免总线冲突,但高优先级节点可能长期独占总线而延迟其他低优先级节点的数据传输. ETA 架构固有的不确定性使其数据传输延时无法预测,导致开放式系统只能采取保守的控制参数,也降低了分布式同步时钟和成员关系服务的实时性. ETA 架构中的数据帧需要包含地址信息用于消息定位,这不可避免的会发生化装舞会故障,降低系统可靠性. 基于 ETA 架构的分布式控制系统在集成和扩展过程中,节点间数据传输的时间特性可能会发生变化,这将影响对时间抖动敏感的实时控制任务的性能.

如图 4 所示,TTA 的通信组织方式是通过 TDMA(time division multiple address,时分多路复用)实现的,每个通信节点在时间轴上指定的 slot(时间槽)发送信息. TTA 架构基于全局同步时钟和预先设计的静态全局调度列表驱动 TDMA 模式的数据传输,与外部事件无关. 这种传输模式使得 TTA 能以最小的抖动和可预测的延时在节点间提供数据传输服务,并避免总线冲突. TTA 架构的消息由全局调度列表定位,数据帧不需要包含地址信息,这既节约了传输带宽,又避免了化装舞会故障. TTA 架构预先定义的全局调度表确保了数据传输的时间确定性,而且节点间数据传输的时间特性不会随着系统集成或扩展而发生变化,这是简化开放式实时控制系统设计的关键特征.

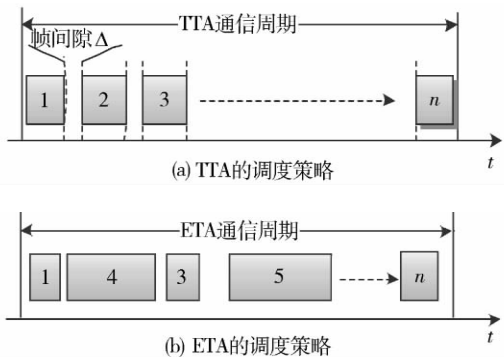


图 4 ETA 和 TTA 的调度策略

Fig. 4 Scheduling strategies of ETA and TTA

TTA 的 TDMA 通信组织方式使其在通信议层就为应用层提供了可靠、实时的分布式同步时钟,并使可靠、实时的成员关系服务成为可能.

因此,只有基于 TTA 架构的数据总线才能为 FADEC 系统应用层的实时控制任务构建一个确定、可靠、实时、可扩展、易集成的一致性分布式计算平台. 下面将从性能(传输带宽等)、可用性

(物理层特征、控制器实现方式、成本等)和可靠性(容错特性)这 3 个方面对 TTP/C, ARINC 659, FlexRay, TTCAN 这 4 种基于 TTA 架构的总线协议的关键特性进行对比分析,选择出适合于开放式 FADEC 系统的最优总线方案.

3 典型 TTA 总线对比研究

3.1 TTP/C 协议^[4,9-12,16]

TTP/C 是由奥地利维也纳理工大学研究,TTTech 公司进行商业化开发的面向汽车、铁路、航空等高可靠性领域的硬实时容错总线规范,其中 C 是指该协议达到了 SAE(Society of Automotive Engineers)的 C 类标准. 该总线是一种基于 TTA 架构的无主机多点串行通信协议,采用 Welch-Lynch 算法实现分布式容错同步时钟,调度策略支持将多个基本 TTA 周期构成一个集群周期. TTP/C 在通信协议层提供时间触发数据传输、分布式容错同步时钟、故障节点探测与隔离、成员关系一致性算法、CRC(cyclic redundancy check)、隐式接收确认、冗余管理等服务. 基于 TTP/C 协议可以为应用程序提供了一个确定、可靠、实时的一致性分布式计算平台. 图 5 为 TTP/C 总线控制器的硬件功能框图(包括主机 CPU(中央处理器)、动态随机处理器(DRAM),等),其 TR(transceiver)、传输通道、BG(bus guardian)等硬件功能模块都采用双冗余设置.

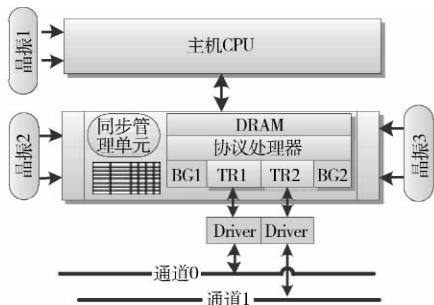


图 5 TTP/C 总线控制器的硬件架构

Fig. 5 Hardware architecture of TTP/C's bus controller

具有独立时钟源的 BG 可以有效地避免阻塞故障. 协议本身的成员关系算法能在 1 个 TDMA 周期内检测、隔离单个故障通信节点并维持底层状态同步,可以在 2 个 TDMA 周期内检测到 SOS 故障并通知应用层处理. TTP/C 支持总线、星型或混合的拓扑结构,在星型架构中总线控制器的 BG 功能被转移到两个冗余的星型耦合器

中,这样能避免 SOS 故障并降低系统成本. TTP/C 的完备容错机制可以容忍 1 个 TDMA 周期内发生的任意单故障,对于瞬态多故障则采取 NGU 策略(10 ms 重后).

3.2 ARINC659 协议^[12,16]

ARINC659 是由美国 Honeywell 公司发明的硬实时容错总线规范,主要用于 Boeing 777 飞机的 AIMS (airplane information management system, 飞机信息管理系统),其注册商标为 SAFEbus. ARINC659 是一个基于 TTA 架构的无主机多点串行通信总线,采用 4 冗余专用时钟线实现容错同步时钟.图 6 为一个 ARINC659 总线节点的硬件功能框图,其核心是负责时钟同步、总线调度、总线监控、交叉校验等功能的 BIU(bus interface unit).总线对 A 和 B 分别有 x 和 y 两组总线,每一组总线都有各自独立的 1 条时钟线和 2 条数据线,每个时钟传送两个数据位.完整的总线系统由 12 条线组成,每一组总线都有独立的 TR,因此每个总线节点包含 4 个 TR.

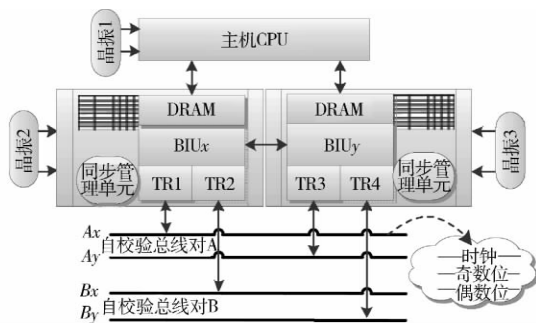


图 6 ARINC659 总线控制器的硬件架构

Fig. 6 Hardware architecture of ARINC659's bus controller

每个通信节点的 BIU 采用双冗余设计,两个 BIU 之间通过交叉监控避免阻塞故障. 每一个 BIU 接收所有 4 组总线发送的数据,并进行交叉校验: $Ax=Ay, Bx=By, Ax=By, Bx=Ay$. 物理层的复杂设计减少了数据帧结构的复杂性和开销,数据帧中不需要位同步头和地址信息,交叉校验消除了 CRC 和其它差错控制字段. ARINC 659 双双冗余异地备份的硬件架构使其对邻近空间故障、单个节点故障和 SOS 故障都有极强的容忍能力,并能够容忍单个 BIU、总线和主机的并发故障.

3.3 TTCAN 协议^[12,14-15,17]

TTCAN 是 ISO 11898-4 协议规定的处于标

准 CAN 协议之上的面向汽车线控领域的总线规范,该协议通过预先设定的系统消息矩阵在一个通信周期内实现 TTA 和 ETA 混合的总线传输调度.如图 7 所示,TTCAN 通过指定的主节点(最多可采用 8 冗余设置)发送基准消息实现节点时间同步,在独占窗口采用 TTA 模式,在竞争窗口采用标准 CAN 协议的 CSMA/CA+AMP 通信模式,两个窗口的数据帧格式完全相同,只是在独占窗口没有仲裁过程.

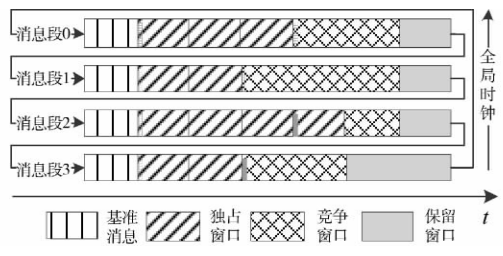


图 7 TTCAN 协议的系统消息矩阵

Fig. 7 System message matrix of TTCAN protocol

TTCAN 实现了 TTA 和 ETA 的混合数据传输,带宽利用率高、灵活性强、数据传输延时的上边界可以预测.但传输带宽只有 1 Mbps,协议层不支持冗余管理,对阻塞故障没有采取对应措施,ETA 段有发生化妆舞会故障的风险. TTCAN 的 TTA 段还取消了 CAN 协议原本的出错重发功能,降低了传输可靠性,所有的一致性和容错功能都需要在应用层完成,也没有在协议层提供 NGU 策略.因此 TTCAN 协议不适用于 FADEC 这类安全苛刻系统.

3.4 FlexRay 协议^[9-12,16-17]

FlexRay 是由 BMW (宝马), Motorola 和 Philips 等公司联合开发的面向汽车线控领域的容错总线规范,该总线是一种基于 TTA 架构的无主机多点串行通信协议,采用 Welch-Lynch 算法实现分布式容错同步时钟.该协议的最大特点是总线拓扑结构和通信方式的灵活性大, FlexRay 可以采用星型、总线或混合架构,并且可以选择使用单一或双冗余传输通道,在星型架构中两个传输通道可以同时被不同节点占用,如图 8 所示. FlexRay 采用和 TTP/C 相同的 BG 功能避免阻塞故障.为了克服 TTA 架构灵活性差和带宽利用率低的缺点, FlexRay 协议将每个通信周期分为静态段和动态段,静态段采用标准的 TTA 模式通信,动态调度段采用 Byteflight 协议规定的通信模式.动态段按照节点优先级顺序被

分割为若干 minislot,在每个空闲的 minislot 内对应节点决定是否是否需要发送数据,若需要则 minislot 被扩展为当前数据帧的长度,否则总线空闲 minislot 时间后下个节点在其对应 minislot 判断是否需要发送数据。

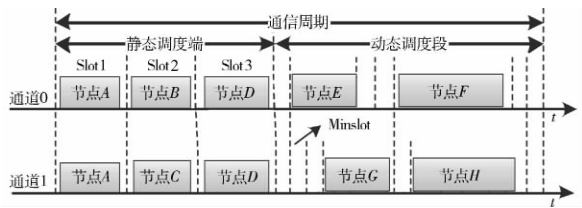


图 8 FlexRay 协议的调度策略
Fig. 8 Scheduling strategy of FlexRay protocol

相比前面 3 种 TTA 协议 FlexRay 的灵活性最强,但没有提供成员关系服务和 NGU 策略,故障节点探测和隔离需要在应用层完成,没有对 SOS 故障给出明确的应对机制,动态段被作为一个统一的时间槽由 BG 监控,有发生阻塞故障的风险。

表 3 列出了这 4 种总线的部分特性对比,其协议控制器均可采用 FPGA 或 ASIC(application

specific integrated circuit) 实现。TTCAN 和 FlexRay 主要面向对可靠性、灵活性和成本都要求较高的汽车线控领域,虽然也采用了 TTA 架构,但是没有完备的容错机制,不能用于对可靠性要求极高的 FADEC 系统。ARINC 659 为专门为航空系统设计,是目前最为可靠成熟的技术,已经过 Boeing 777 飞机十几年的飞行验证,但其双双冗余异地备份的硬件架构不适合在体积、质量要求很高的开放式 FADEC 系统中实施,而且其价格昂贵、可用性差。TTP/C 协议以相对简单的硬件架构提供了完备的容错机制、灵活的拓扑结构和调度策略,足够的传输带宽和节点触目,并在通信协议层封装了所有的一致性服务和关键容错机制。其软硬件协同的协议实现方式简化了协议升级过程,其协议和物理层独立的特性使其可以满足不同类型开放式 FADEC 系统的技术需求。而且 TTP/C 是目前唯一同时应用于航空和汽车线控领域的容错硬实时总线规范,这使得 TTP/C 总线同时具备高可靠和低成本特性。因此,从性能、容错和可用性的角度考虑 TTP/C 总线是开放式 FADEC 系统的最佳选择。

表 3 TTA 通信架构的关键特性对比^[4,9-12,14-17]
Table 3 TTA communication architecture comparison matrix

协议类型	TTP/C	ARINC 659	TTCAN	FlexRay
传输带宽	5/25 Mbs, 1 Gb/s	60 Mb/s	152 kb/s, 1 Mb/s	10 Mb/s
节点数据	64	32	120	64
拓扑结构	总线、星型或混合	总线型	总线型	总线、星型或混合
帧校验方式	CRC	总线对交叉校验	CRC	CRC
物理层	RS485、双绞线、光线	IEEE1194.1 标准	双绞线	双绞线
成员关系	支持	不支持	不支持	不支持
冗余管理	支持	支持	不支持	不支持
实现方式	FPGA 或 ASIC	FPGA 或 ASIC	FPGA 或 ASIC	FPGA 或 ASIC
NGU 策略	支持	不支持	不支持	不支持

4 基于 TTP/C 总线的模块化 DEEC 总体方案

在高温电子技术成熟之前,可以基于 TTP/C 总线设计具有开放特性的模块化 DEEC,图 9 为本文提出的模块化 DEEC 硬件功能框图。采用 TTP/C 的总线型拓扑结构构建控制器架构,将 BG 模块外置并为其提供独立的晶振、容错同步时钟和电源用于降低共模失效概率,使用传输速

率为 25 Mb/s 同步通信模式。为了平衡系统的可靠性、复杂性和可扩展性设计,将整个 FADEC 按照功能划分为安全关键控制模块,EMU(engine monitoring unit)模块和非安全关键输入/输出模块。图 9 中的安全关键控制模块完成主燃油控制,尾喷口控制、导叶角控制、与飞机系统的通信、超转超温保护等核心功能,这部分采用非相似冗余架构。非安全关键输入输出模块用于完成地面维护、信号指示等非核心功能,这部分的传感器和执

行机构可以采用冗余设置,但仅采用一个节点处理器处理,没有备份模块。EMU 模块用于监视发动机的运行状态,需要完成高频信号采样及预处理,发动机自适应实时模型等复杂的功能,十分适合采用具有内嵌处理器的高性能 FPGA 实现^[18]。EMU 内部的 AMD(advanced micro devices)处

理器用于核心控制规律计算,该处理器的输出与主通道的主控制节点 Power PC(personal computer)处理器、热备份通道的主控制节点 DSP(digital signal processor)处理器的输出形成 2/3 表决关系,增加控制输出可靠性。

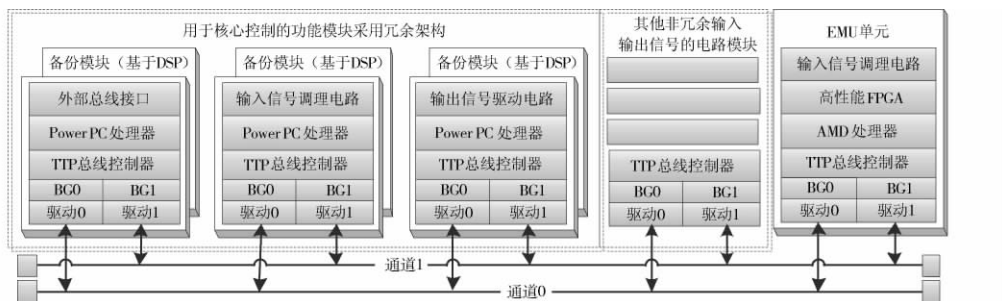


图 9 基于 TTP/C 总线的模块化 DEEC 硬件架构

Fig. 9 Hardware architecture of DEEC based on TTP/C data bus

5 结 论

通过本文的研究得到以下结论:

1) 确定性、一致性、完备的容错机制、足够的传输带宽、灵活的拓扑结构和调度策略、协议的开放特性是用于开放式 FADEC 系统的数据总线应具备的特征。

2) 基于事件触发架构的数据总线存在固有的时间不确定性问题,不适用于 FADEC 这类安全关键硬实时容错控制系统。

3) 基于时间触发架构的 TTP/C 总线是开放式 FADEC 系统的最佳总线方案。

4) 基于 TTP/C 总线的模块化 DEEC 应划分为安全关键控制模块、EMU 模块和非安全关键模块。在基于 TTP/C 总线的开放式架构下,FADEC 系统的诊断和容错控制策略会和传统的集中式架构有较大区别,这也是本文的后续研究重点。

参考文献:

[1] 黄金泉,徐科. 航空发动机分布式控制系统结构分析[J]. 航空动力学报,2003,18(5):698-704.
HUANG Jinquan,XU Ke. Distributed control systems for aeroengines:a survey[J]. Journal of Aerospace Power, 2003,18(5):698-704. (in Chinese)

[2] Bhal T,Alireza R B,Richard M. Vision for next generation modular adaptive generic integrated controls for military/commercial turbine engines[R]. AIAA-2007-5710,2007.

[3] Alireza R B. Advanced,adaptive,modular,distributed,ge-

neric universal FADEC framework for intelligent propulsion control systems[R]. NASA Paper, AFRL-RZ-WP-TP-2008-2044,2008.

[4] Jeffrey J,Dr K,Sivak P. Design and system implementation considerations for high-temperature distributed engine control[R]. AIAA-2010-6674,2010.

[5] Alireza R B,Dennis C,Bert S,et al. Status vision and challenges of intelligent distributed engine control architecture[R]. NASA Paper, AFRL-RZ-WP-TP-2008-2042,2008.

[6] Brendan H,Michael P. Jet engine control using ethernet with a BRAIN[R]. AIAA-2008-5291,2008.

[7] Zhang W,Branicky M S,Phillips S M. Stability of networked control systems[J]. IEEE Control Systems Magazine,2001,21(1):84-99.

[8] Hespanha J P,Naghshabrizi P,Xu Y G. A survey of recent results in networked control systems[J]. Proceedings of the IEEE,2007,95(1):138-162.

[9] Bauer G,Opetz H,Puschner P. Assumption coverage under different failure modes in the time-triggered architecture[C]//Proceedings 8th IEEE International Conference on Emerging Technologies and Factory Automation. Italy: IEEE,2001:333-341.

[10] Bauer G,Kopetz H,Steiner W. The central guardian approach to enforce fault isolation in the time-triggered architecture[C]//Proceedings of the 6th IEEE International Symposium on Autonomous Decentralized Systems. Italy: IEEE,2003: 37-44.

[11] Ademaj A. Slightly-off-specification failures in the time-triggered architecture[C]//Proceedings of the 7th IEEE International Workshop on High Level Design Validation and Test. France:IEEE,2002:7-12.

[12] John Rushby. A comparison of bus architectures for safety-critical embedded systems[R]. NASA/CR-2003-212161,

- 2003.
- [13] Hannius O, Ring D, Johan K. Derivation of diagnostic requirements for a distributed UAV turbofan engine control system[J]. *Journal of Engineering for Gas Turbines and Power*, 2008, 130(2): 0216021(11 pages).
- [14] Dennis E, Cule, Alireza R B. Communication needs assessment for distributed turbine engine control[R]. AIAA-2008-5281, 2008.
- [15] Thompson H A, Benitez-Pereza H, Leea D, et al. A CAN bus-based safety-critical distributed aeroengine control systems architecture demonstrator[J]. *Microprocessors and Microsystems*, 1999(23): 345-355.
- [16] Gwaltney D A, Briscoe JM. Comparison of communication architectures for spacecraft modular avionics systems[R]. NASA/TM-2006-214431, 2006.
- [17] Leen G, Heffernan D. TTCAN: a new time-triggered controller area network [J]. *Microprocessors and Microsystems*, 2002, 26(2): 77-94.
- [18] Eric M, Marcian N. FPGA design methodology for industrial control systems-a review[J]. *IEEE Transactions on Industrial Electronics*, 2007, 54(4): 1824-1842.