引用格式:解文涛,王锐. 基于分级容错技术的高完整计算机系统设计[J]. 电光与控制,2019,26(10):106-110. XIE W T, WANG R. High-integrity computer system design based on hierarchical fault-tolerant technology[J]. Electronics Optics & Control, 2019, 26(10):106-110.

基于分级容错技术的高完整计算机系统设计

解文涛, 王 锐
(中国航空计算技术研究所,西安 710068)

摘 要: 对国内外三代机、四代机及民机中的机载安全性关键系统发展情况进行深入分析,总结了多通道表决、比较对故障静默等典型容错计算机架构的技术特点,围绕新一代飞机对机载安全关键计算机系统的可靠性、容错能力、故障检测隔离能力、实时性的新挑战,提出了基于分级容错技术实现的高完整计算机系统设计思路,描述了分层分级实现高完整性容错的设计原理,并对其所涉及的Lock-step技术、时间触发网络等关键技术给出了解决途径,可满足下一代飞行器的发展需要,提升机载安全关键计算机系统的安全性、可靠性。

关键词: 飞行控制系统; 安全性关键系统; 容错; 锁步; 时间触发架构
中图分类号: TP302.8 **文献标志码**: A **doi**:10.3969/j.issn.1671-637X.2019.10.021

High-Integrity Computer System Design Based on Hierarchical Fault-Tolerant Technology

XIE Wen-tao, WANG Rui
(Aeronautical Computing Technique Research Institute, Xi'an 710068, China)

Abstract: A detailed analysis is made to the development of airborne safety-critical system onboard the third and the fourth generation civil aircrafts at home and abroad. The technical characteristics of such typical fault-tolerant technology as the multi-channel voting etc., are summarized. Aiming at the challenges of the new-generation aircrafts on the reliability, fault-tolerant capability, fault-detection/fault-isolation capability, and real-time performance of the airborne safety-critical computer systems, a design idea of a high-integrity computer system based on hierarchical fault-tolerant technology is proposed. The design principle of the hierarchical high-integrity fault-tolerant system is described, and the critical technologies of Lock-step and time-trigger network are given. The strategy can satisfy the development requirements of the next-generation aircrafts, and can improve the safety and reliability of the airborne safety-critical computer systems.

Key words: flight control system; safety-critical system; fault tolerance; Lock-step; time-triggered architecture

0 引言

容错是机载安全性关键系统在其组成部分出现特定故障或差错的情况下仍能执行规定功能的一种设计特性,而系统容错设计是保证系统可靠性的重要手段。以飞行控制系统、飞行管理系统为代表的机载平台安全性关键系统,其可靠性指标需要满足失效率小于每飞行小时10^{-7}(军机飞控系统)和每飞行小时10^{-9}(大飞机飞控系统)。经典的系统容错设计方法是采用余度技术,余度计算机的同步工作可以保证系统出现故障时不出现错误输出,这种具有输出正确服务的能力也被定义为完整性的能力,即故障情况下可靠工作的能力[1]。但是,余度容错技术实现往往建立在冗余的昂贵硬件资源的基础上,特别是对于机载电子系统而言,随之引起的元器件数量的激增、维修难度增大、升级困难和费用昂贵等问题时刻困扰着设计师们。为了进一步提升系统容错效能,国内外一直在寻求更高效的机载安全性关键系统的容错解决方案。

1 基于多通道表决的容错计算机架构

最早使用数字电传飞行控制系统的是美国F-16战斗机,后来国内外研制的一些三代机也都采用了数字式四余度电传系统,容错方式是基于通道的多数表

收稿日期:2018-10-08 **修回日期**:2019-07-12
作者简介:解文涛(1977—),男,湖北武汉人,硕士,研究员,研究方向为抗恶劣高可靠嵌入式容错计算机相关技术。

决容错系统,4 个余度计算机通道采用同步运行机制,采集的数据在计算机之间进行表决,同时进行输出并确保计算机具有相同的输出结果,在 2 次故障后通过剩余的 2 台计算机保证飞机的可靠飞行,见图 1。

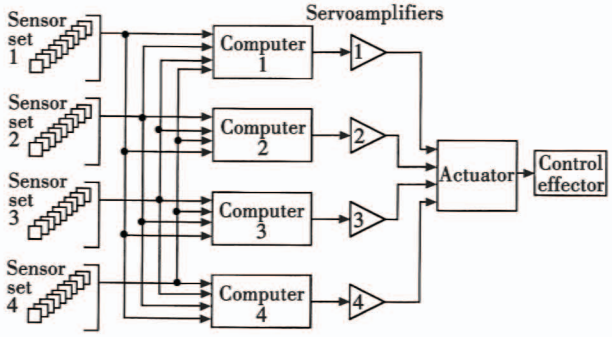

图 1　典型四余度基于多通道表决容错架构

Fig. 1　Four-redundancy fault-tolerant architecture based on multi-channel voting

F-16,F-18,F-117 和 JAS39 均采用四余度的电传飞行控制系统配置,经过长时间的飞行已经证明该架构的有效性[2]。上述机型的安全性关键系统采用的是以小帧同步或异步的结构,是基于静态余度,即表决监控(交叉通路监控)的基本的失效检测与隔离的方法。在这类架构中,自测试(通路内监控)不是主要防御手段,但是提高计算机的失效检测覆盖率和辅助设施(如传感器和作动器)的可用性可以明显改进整个系统的可靠性。

这种基于通道的多数表决容错架构需要占用庞大的系统硬件资源:首先,配套的传感器、计算机、作动器数量较多,这就造成体积、重量和功耗的挑战;其次,当时对操作系统的不信任也造成了软件与硬件的紧密捆绑,而元器件的换代周期往往远小于飞机平台的更新周期,因此系统的后续维护及升级的难度是可想而知的;再次,由于单通道不具备完整性,也就是不能解决拜占庭故障的问题,因此其容错架构在理论上就存在 2:2 奇异故障陷阱,这就造成余度管理策略比较复杂。这种相似余度的典型代表,在需要更高可靠性及安全性的环境中,例如在民航飞机中几乎无能无力。

因此,波音 777 客机的主飞控计算机(PFC)在多数表决容错架构上增加了非相似设计,构建出 3×3 余度的非相似多数表决容错架构,这种架构可以认为是多级嵌套的多数表决容错架构。飞控计算机通过飞控数据总线 ARINC629 与其他飞控组件进行通讯,每个计算机结构如图 2 所示。波音 777 软件的 3 个版本由不同的小组独立设计、禁止交流,软件编程采用高级语言和低级语言搭配,由 ADA、汇编、C 语言编写,并采用不同的编译器完成软件编译。但是这种极其复杂的容错架构使得庞大的软硬件成本和开销成倍上升,让设计人员苦不堪言,最终导致飞机的飞行计划一拖再拖。

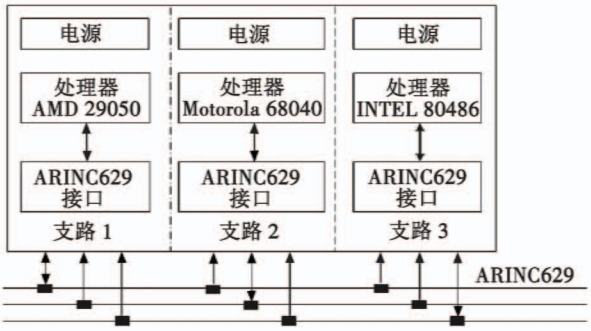

图 2　单台计算机结构示意图

Fig. 2　Structure schematic of single computer

2　基于“比较对”的故障静默容错计算机架构

根据国内外对故障容忍及余度配置的多年研究(见表 1),可以得出以下结论:如果故障自检覆盖率达到 100%(完整性不低于 10^{-5}),并且交叉通道可信,即不存在拜占庭故障,则只需 3 个余度,就可实现对 1 次故障、2 次顺序故障和 2 次同时故障的容忍。

表 1　故障容忍及余度配置要求

Table 1　Failure tolerance and redundancy configuration requirements

需要容忍的故障数	自检测覆盖率/%	交叉通道可信度	所需余度配置数
0			≥1
1	100	可信	≥2
	<100	可信	≥3
	<100	拜占庭故障	≥4
2 次顺序故障	100	可信	≥3
	<100	可信	≥4
	<100	拜占庭故障	≥5
2 次同时故障	100	可信	≥3
	<100	可信	≥5
	<100	拜占庭故障	≥7

国外在后续民机、军机的开发和研制中,为了解决基于多通道表决容错架构的缺点,并进一步提升系统效能,采用了基于比较对的故障静默容错架构[3],在容错能力不降低的情况下寿命周期内的低成本成为这一代飞机设计的主要目标。

这种架构最早用于以空客 A320 为代表的民机飞控系统,一般采用 5 ~ 7 个比较对架构,每个比较对组成一个完整的控制节点计算机,即使在 4 ~ 6 次故障后也能通过剩余的 1 个节点保证飞机的可靠飞行,同时还加入非相似余度设计使系统的失效率更小。空客民机飞控计算机系统从 A320 开始到 A380 也一直采取了基于比较对的故障静默容错系统结构,即命令支路和监控支路的互比结构,采用故障静默的工作策略,提供单台计算机的完整性,故障被动输出,典型的应用为 $N\times2$ 系统结构,由多个比较对节点组成,该体系构型的特点

为节点完整性高,系统安全可靠。在任何时候,只需要一台计算机即可完成飞行控制。

后来以 F-22 和 F-35 战斗机为代表的四代机也采用了这种容错架构。F-35 还创新性地对飞机平台的多项功能进行了综合管理,包括飞行控制、发动机控制、公共设备管理等,这种飞控、机电等隔离功能向飞机平台管理融合的方式转变,对飞行器管理计算机(VMC)的容错能力也提出了新的挑战。因此,飞行器管理计算机系统不得不采用总线分布式系统架构、三余度配置,为保证飞机安全性,其必须保证三余度中的每个节点均能独立可靠地工作,即每个节点都必须具备高完整性,采用比较对可有效提高单节点计算机的完整性,降低计算机系统的余度数量[4],见图 3。每台 VMC 包含 2 个 PowerPC 处理器,节点内的 2 个处理器组成比较对,对节点数据进行实时比较,确保了节点内数据的完整性,比较一致时,节点计算机继续工作,当节点内的两个处理器比较不一致时,则节点自动切除,实现故障静默。由于节点完整性的提高,三节点 VMC 实现了"2 次故障工作"的故障容限。

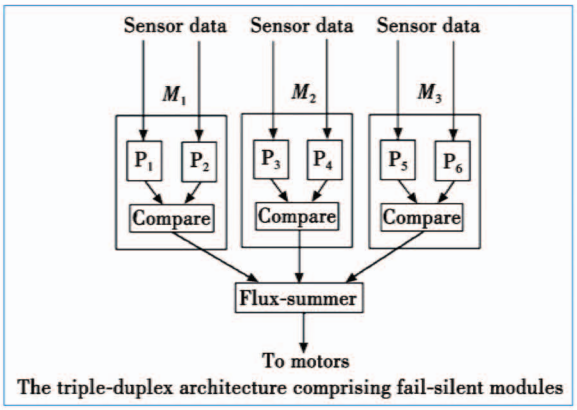

图 3 典型 3×2 比较对故障静默容错架构

Fig. 3 A typical 3×2 comparison pair of silent fault tolerant architecture

基于比较对的故障静默容错架构并不是对多数表决策略的否定,而是在此基础上的进一步发展,多个传感器信号源及余度总线上数据的多数表决仍然是不可或缺的安全保障策略。这种发展变化的收益是改变了以前粗枝大叶的容错模式,开启了细颗粒度容错的大门,为后续分级容错系统的发展奠定了基础。

3 基于分级容错的高完整容错计算机架构

在新一代战机平台的超高速、长航时、超远程、智能化等新需求的牵引下,对飞机平台管理系统的技术发展提出了新的挑战:首先,需满足对飞控、机电等飞机平台安全关键功能的复杂控制与管理能力,这就需要更高完整性计算机平台的支持;其次,超长的航时要求系统可靠且有效的工作能力必须得到进一步提升,要做到这一点,计算机系统在更深层次的容错能力上必须提供帮助;另外,还有超高速与高机动下的实时智能控制能力的挑战,即故障的检测与恢复时间需要由原来的数百毫秒量级提升到几毫秒,以减轻扰动影响和控制误差,这就使得仅靠软件实现的余度管理难以实现。以上需求及挑战使得人们必须进一步优化目前的容错计算机架构。

基于分级容错的高完整容错计算机架构就是在这样的前提下应运而生的,它是基于比较对的故障静默容错架构的补充和完善。2006 年最先由 Honeywell 完整提出了分级容错设计的理念,按照不同的容错粒度将系统分为功能部件级、模块级、节点(整机)级、网络级、子系统级、系统级等多个等级,如图 4 所示,通过不断提升各个等级的完整性、故障容错能力,进一步提高容错系统的效费比。一方面,逐级抑制了故障的传播,确保低一级向上一级上报信息的完整;另一方面,在故障诊断与恢复的时间上也显著提高,能够从整机故障恢复时间的毫秒级提升到纳秒级[5]。

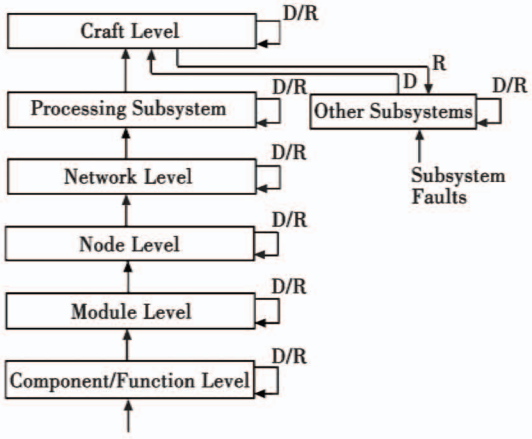

图 4 分级容错结构

Fig. 4 Hierarchical fault-tolerant structure

3.1 锁步(Lock-step)计算机技术

基于分级容错的高完整容错计算机架构的核心硬件技术是 Lock-step 计算机硬件技术,通过处理器间不间断地检查其操作以检测执行的正确性,一个完整的、实用的 Lock-step 处理器系统应该包括错误检查、隔离和恢复逻辑,能够恢复一个或两个处理器功能[6],简言之,应该具有瞬态故障自诊断和修复的能力。

目前采用基于 Lock-step 的高完整容错系统的是以 A400M 和 B787 为代表的军用运输机及民用客机。B787 飞控系统采用三余度的 FCM,每台飞行控制模块(FCM)由命令支路和监控支路组成,其中,命令支路采用 Lock-step 设计技术,包含两个锁步运行的 PowerPC 处理器,实现了模块计算的高完整性。监控支路采用单

个 MIPS 处理器，支路间构成非相似设计。

Lock-step 技术是比较对容错技术的进一步发展，双处理器锁步（DMR Lock-step）是将采用任务同步的双处理节点提升到指令级同步，可大幅度提升节点机比较的实时性，由硬件实现指令级的比较监控，监控的时间粒度由毫秒级提升到纳秒级，在节点机任务可靠性不变的情况下，提升了节点机的实时性与安全性，降低了节点机软件复杂度。DMR Lock-step 确保节点在 1 次故障的情况下实现故障静默。三处理器锁步（TMR Lock-step）则是对 DMR Lock-step 技术的进一步发展，支持节点在 1 次故障的情况下继续可靠工作，在 2 次故障的情况下实现故障静默，进一步提升模块的任务可靠性，更好地实现了完整性与故障降级能力之间的平衡，实现了容错技术向模块级、节点级、网络级、系统级的多级容错架构的发展。

受目前 TMR Lock-step 成熟度限制，国外也仅在 A400M 飞机的舱门控制系统中进行验证，为后续在以飞行器管理系统为代表的安全性关键系统的应用奠定基础，TMR Lock-step 的容错系统包含 3 个相同的 PowerPC 处理器，实现节点的 1 次故障工作、2 次故障静默（故障可恢复）。国外 Lock-step 容错结构发展如图 5 所示[7]。

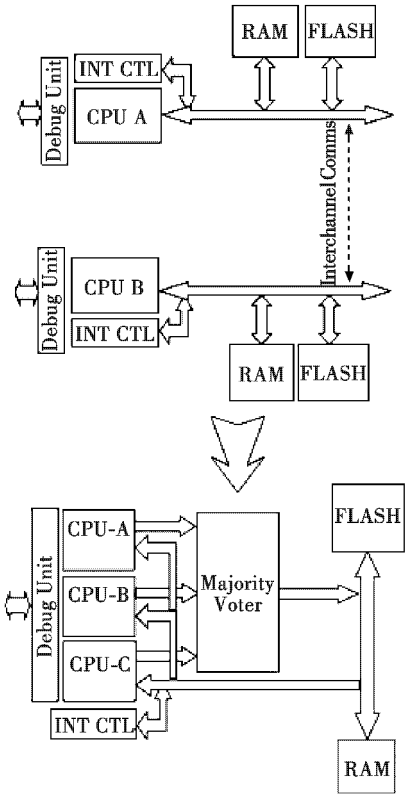

图 5　国外 Lock-step 容错结构发展

Fig. 5　The development of foreign Lock-step fault-tolerant structure

3.2　混合结构容错时间触发网络

基于分级容错的高完整容错计算机架构中除了需要锁步技术的支撑外，计算机与传感器的交联网络是另一项核心关键技术。分布式实时控制系统的任务执行是由触发条件控制的，随着系统内的数字化设备（计算机、控制器以及智能传感器）逐渐增多，系统功能的日益复杂，系统需要传输的信息和数据量不断加大，网络化也经历着从事件触发系统向时间触发系统发展的过程。时间触发架构（Time-Triggered Architecture，TTA）系统和事件触发架构（Event-Triggered Architecture，ETA）系统的工作原理不同[8]。前者的控制信号来源于时间进程，后者的控制信号来源于事件的发生。在 TTA 系统中控制总是驻留在计算机系统的内部，TTA 系统是一个物理上封闭的确定性系统。在 ETA 系统中，控制信号可能源自计算机内部，也可能源自计算机系统外部的环境，不可预测的事件将导致计算机系统的不确定性行为。

TTA 具有如下基本特征[9]。

1）带宽利用率高：时间触发通信采用基于全局统一时间基的静态调度，有效避免了消息之间的冲突，其带宽利用率可以达到 80%，而事件触发通信的带宽利用率一般不超过 30%。

2）可预见性：由于采用确定的时间触发调度机制，计算时延是可预见的。

3）易测性：自动按时间触发协议和调度在恰当的时刻对计算结果进行检测。

4）集成：容易由独立设计和测试的组件或子系统来构成系统。

5）复制确定性：复制组件的行为在组件之间有一致性；每个组件都在同一时刻或某一预定的偏移时刻做同样的事情。

6）成员制：故障状态将依靠通讯网络上的“成员”在某一个时间触发架构中自动广播。

目前，新一代的机载安全关键计算机系统已广泛采用了时间触发技术，涉及飞行控制、发动机控制以及电源管理等实时控制系统。目前，时间触发技术已经成为先进飞机以及老机升级（如 F-16）实时控制系统的优选解决方案。庞巴迪 C 系列飞机基于 TTP 总线的三余度分布式电传飞行控制系统已首飞成功，Honeywell 先进技术平台验证系统中使用了 1 Gibit/s 和 10 Mibit/s 的 TTE 技术以及 TTP 技术，两台控制计算机之间海量数据交换采用高速实时容错 1 Gibit/s TTE 网络，执行器控制信息采用 10 Mibit/s TTE 网络进行通信，执行器内部采用 TTP 作为背板总线进行模块互联，不同拓扑形式的时间触发架构分层设计与管理成为时间确

定性控制系统的关键技术。

4 结束语

国外三代机、四代机及民机飞管等安全性关键系统容错计算机技术正在向高完整性的细粒度容错方向发展。未来飞行器平台的机动性与续航时间将进一步提升,这对机载安全关键计算机系统的可靠性、容错能力、故障检测隔离能力、实时性提出更大挑战。本文通过对机载安全关键计算机系统发展趋势的分析,提出了计算机系统在节点层面、通讯网络层面和系统架构层面分层分级实现高完整性容错的设计思路,这种分级容错技术思想可满足下一代战斗机、民用飞机、无人机等飞行器的发展需要,可进一步提升机载安全关键计算机系统的安全性、可靠性。

参 考 文 献

[1] 郭丽娟,刘双与,张激. 基于时间触发的高可靠性实时系统架构[J]. 计算机工程,2006, 32(4):272-274.

[2] RUSHBY J. A comparison of bus architectures for safety-critical embedded systems[R]. Menlo Park:SRI International, 2003.

[3] 王树义,南建国,赵松云. 综合化航电核心处理系统容错设计[J]. 计算机测量与控制,2012, 20(8):2248-2250.

[4] 陈益,程俊强,林坚. 新型飞行管理计算机的设计[J]. 计算机技术与发展,2006, 16:222-225.

[5] 冯晓旺,蓝海文. 新一代航空航天总线技术[J]. 航空制造技术,2012(3):98-99.

[6] KOPETZ H. The time-triggered architecture[J] Proceedings of the IEEE, 2003, 91(1):112-126.

[7] 姚学礼. 网络通信协议一致性测试研究[J]. 通信技术,2009, 42(5):172-173, 176.

[8] DOERENBERG F M G, TOPIC M. Fault tolerant data communication network:US7206877B1[P]. 2002-10-15.

[9] 徐拾义. 可信计算系统设计和分析[M]. 北京:清华大学出版社,2006.

(上接第77页)

(2):178-182.

[7] 赵进平. 异常事件对EMD方法的影响及其解决方法研究[J]. 青岛海洋大学学报,2001, 31(6):805-814.

[8] 王婷. EMD算法研究及其在信号去噪中的应用[D]. 哈尔滨:哈尔滨工业大学,2010.

[9] 林婉如,熊盛武,谢啸虎. 局部经验模态分解算法[J]. 计算机工程与应用,2011, 47(13):123-126.

[10] 胡重庆,李艾华. EMD间歇信号的检测和提取方法[J]. 数据采集与处理,2008, 23(1):108-111.

[11] 刘代志,钱昌松,吴晓露. 经验模态分解中模态混叠的若干问题探讨[C]//第八届全国信号与信息处理联合学术会议,2009:110-114.

[12] 邬肖敏,李世平,程双江. 基于EMD和误差匹配的动态测试系统误差溯源[J]. 电光与控制,2015, 22(4):92-95.