文章编号:1671-4598(2023)06-0137-06 DOI:10.16526/j.cnki.11—4762/tp.2023.06.021 中图分类号:TP368 文献标识码:A

失速告警系统应用异构双核处理器的安全性分析研究

宣晓刚，魏璐达，贾少龙，杨　飞，张美仙
（太原航空仪表有限公司，太原　030006）

摘要：飞机失速会影响飞机的飞行安全，失速告警计算机作为失速告警系统的核心控制部件，在失速发生前通过灯光告警、语音告警、振杆器抖动等方式为飞行员提供告警，提醒驾驶员进行操作，避免飞机进入失速状态；按照SAE ARP4754A中研制保证等级的分类，将失速告警计算机某些功能确定为灾难级，确定其研制保证等级定级为A类；采用异构双核处理器进行失速告警计算机的设计，由于ARP4761中的分析方法对相似性设计有着复杂性和难以模拟仿真的问题，故文章设计参照了IEC 61508参考标准，对采用异构双核处理器的失速告警计算机的安全性能进行了梳理和分析；分析研究结果表明，相比于采用传统的单核处理器或同构双核处理器设计的失速告警计算机，选择异构双核处理器进行失速告警计算机的设计有其独有的优势，其优势在于异构双核处理器所具备的“1oo2D”结构，通过计算分析满足失速告警计算机对于高安全性、高可靠性的要求；依照IEC 61508相关标准，结合失速告警计算机的高性能要求，选择正确的分析设计路径，可以确保失速告警计算机的功能安全完整性等级有效达成，为其他航空产品的设计开发提供参考。

关键词：飞机失速；失速告警系统；失速告警计算机；异构双核处理器；IEC 61508；ARP 4761；安全性分析

Research on Safety Analysis of Stall Warning System Using Heterogeneous Dual Core Processor

XUAN Xiaogang, WEI Luda, JIA Shaolong, YANG Fei, ZHANG Meixian
(AVIC Taiyuan Aero-instruments Co., Ltd., Taiyuan　030006, China)

Abstract: Aircraft stall will affect the flight safety of aircraft, as the core control component of a stall warning system, a stall warning computer provides a warning to pilot by means of light alerts, aural alerts and stick shaker before stall occurs, and it reminds pilots to operate and avoid stall. According to the classification of development assurance level in SAE ARP4754A, the functions of the stall warning computer are determined as catastrophic level, and its development assurance level is determined as Class A. A heterogeneous dual-core processor is used to design the stall warning computer. Due to the complexity and difficult simulation of similarity design in ARP4761, this design also refers to the IEC61508 reference standard, the safety performance of stall warning computer using the heterogeneous dual-core processor is combed and analyzed. The analysis results show that, compared with traditional single-core processor or homogeneous dual-core processor, the stall warning computer with heterogeneous dual-core processor has its unique advantages. The advantage lies in the "1oo2*D*" structure of the heterogeneous dual-core processor, which can meet the requirements of high safety and high reliability for the stall warning computer for through calculation and analysis. In accordance with relevant IEC 61508 standard, and combined with the high performance requirements of the stall warning computer, the correct analysis and design path can ensure that the functional safety integrity level of the stall warning computer can be effectively achieved, which provides a reference for the design and development of other aviation products.

Keywords: aircraft stall; stall warning system; stall warning computer; heterogeneous dual-core processor; IEC 61508; ARP 4761; safety analysis

收稿日期:2022-08-02； **修回日期**:2022-11-23。
基金项目:山西省关键核心技术和共性技术研发攻关专项项目(2020XXX019)。
作者简介:宣晓刚(1969-),男,山西太原人,大学本科,研究员,主要从事飞行器大气数据系统方向的研究。
通讯作者:魏璐达(1991-),女,河北衡水人,大学本科,助理工程师,主要从事机载测试与告警方向的研究。
引用格式:宣晓刚，魏璐达，贾少龙，等.失速告警系统应用异构双核处理器的安全性分析研究[J].计算机测量与控制,2023,31(6):137-142.

0 引言

飞机失速会导致飞机失控，引发飞行事故。为保证飞行安全，民航局规定需要在民用飞机上加装失速告警系统(SWS，stall warning system)[1-2]。飞行员通过失速告警系统获得飞机运行时的失速告警、保护信息，以及相应的控制指令，执行相应的操作，确保飞机不进入失速危险状态。失速告警系统中的核心控制部件，即失速告警计算机的设计就显得尤为重要。

传统的失速告警计算机基本上都是采用单核处理器，如欧美、俄罗斯等国家的军用和民用飞机上加装的失速告警计算机，或者会采用多处理器同步时钟的方法构建余度告警计算机，并采用双余度失速告警计算机的方法来满足适航法规对安全性的要求。

如今，仅通过提高单核处理器时钟频率的手段来提升计算速度与安全性能已无法满足目前的需求。而将两个处理器内核整合在同一个芯片上，可大大提升计算处理性能。相比于单核处理器，多核处理器无论在结构设计、能耗以及安全性设计等方面都有着巨大优势。出于对失速告警计算机安全性、满足适航性及输出数据可信度的考虑，需将多种飞行参数引入失速告警计算机用于对失速的判断，提出了一种基于异构双核处理器的失速告警计算机的设计方案。

在航空电子产品设计中一般会应用到 SAE ARP4761 进行安全性分析，但其某些分析方法具有复杂性和难以模拟仿真。但随着 IEC 61508 功能安全国际标准的正式发布，使得人们越来越关注功能安全要求。这些标准可以对安全关键系统的非功能属性进行有效分析和评估，分析所得结果能给设计者提供所需的信息和设计指导，使得设计者在系统设计阶段可以尽早对系统安全性进行分析与评估[3-4]。

因此，应用 IEC 61508 标准作为失速告警计算机设计的依据，为其安全性分析研究提供了有力保证。

1 失速告警计算机功能及设计

失速告警系统通过在飞机接近失速时向飞行员发送告警和控制信息，确保飞行员及时操纵飞机，使飞机迅速恢复到正常状态来保证飞行安全[2]。失速告警系统一般由迎角传感器、失速告警计算机、告警装置等组成[1]。其中，迎角传感器用于采集飞机迎角信号并发送给失速告警计算机。振杆器作为告警装置根据失速告警指令进行抖振来提醒驾驶员进行操作，避免飞机进入失速状态。

失速告警计算机作为失速告警系统中的核心控制部件，通过迎角传感器采集飞机迎角信息修正得出真迎角，并接收机上其他系统发送的马赫数、高度、襟缝翼构型、结冰等信息，判断飞机真迎角是否接近气动失速，并在接近气动失速时发出失速告警、自动点火和失速保护指令，为飞行员提供告警指示，保护飞机不进入失速危险状态。

失速告警计算机设计具有以下功能：

1）为迎角传感器提供激励信号，接收迎角传感器输出的两路迎角信号，根据采集的信号数据计算飞机局部迎角，同时对迎角传感器的加温状态进行监控；

2）通过数据总线接收外部输入数据；根据接收的数据信息解算真实迎角、临界迎角和失速速度；

3）当真实迎角接近临界迎角或空速接近失速速度时，输出告警驱动信号给同侧振杆器和灯光、音响系统，提醒飞行员采取措施；同时输出告警状态给机组告警系统；

4）当真实迎角继续增大到失速保护控制迎角，发出保护指令给推杆器，同时发出保护状态给机组告警系统；当真实迎角小于失速保护控制迎角一定数值时，停止发出保护指令和保护状态；

5）当真实迎角继续增大至点火迎角，持续发出点火指令给左和右发动机；同时发出点火状态给机组告警系统；若真实迎角小于点火迎角一定数值时，停止发出点火指令和点火状态。

2 功能安全标准介绍及其发展

2.1 SAEARP 4761 相关介绍及其发展

美国汽车工程师学会（SAE，society of automotive engineers）于 1996 年发布了 SAEARP 4761《民用机载系统与设备的安全评价过程实施指南方法》，ARP 4761 引入了飞机级安全评估的概念，提出了对民用飞机认证进行安全评估的指南和方法，以及确定了表明适航性的系统方法[5]。它主要用于表明系统符合 FAR/JAR 25.1309 有关的条款。

ARP 4761 文件提供了进行行业公认的安全评估的指南，包括功能危害评估 FHA、初步系统安全评估 PSSA 和系统安全评估 SSA。本标准还提供了有关进行安全评估所需的安全分析方法的信息。这些方法包括故障树分析 FTA、因果关系图 DD、马尔可夫分析 MA、失效模式和影响分析 FMEA、失效模式和影响总结 FMES 和共因分析 CCA(CCA 由区域安全分析 ZSA、特定风险分析 PRA 和共模分析 CMA 组成)[5]。ARP 4761 文件中提供的指南和方法旨在与其他适用的指南一起使用，包括 ARP 4754A，RTCA/DO-178，RTCA/DO-254，以及与 FAR/JAR 25.1309 相关的咨询文件。自 ARP 4761 发布以来，在全球航空业得到了广泛应用，并成为获取适航批准过程中的事实标准。经过 20 多年的工业实践，目前已经发布了 ARP 4761A。

为了在工业领域更好地使用 ARP 4761，SAE 于 1997 年将 SAEARP926《故障/失效分析方法》更新到 B 版，明确使用 ARP 4761 作为飞机安全性评估的方法。ARP 926B 中明确提出了诸如共模分析 CMA 的分析方法等某些分析方法的复杂性和难以模拟仿真的问题，因此该标准对新技术的使用也是开放式的，在其附录 C 中申明了在未来使用更加适用的新分析技术。

2.2 IEC 61508 相关介绍及其发展

国际电工委员会（IEC，international electrolechnicai

commission）于 1998 年发布了第一版 IEC61508 标准，该标准针对电气/电子/可编程电子部件（E/E/PE）和系统，并于 2010 年更新至第二版[6-7]。IEC61508 标准基于系统和随机故障的性能目标，涵盖了安全管理、系统/硬件设计，软件设计、生产和安全关键 E/E/PE 系统的操作。因其广泛的适用性使得大到整个系统小到零部件，都可以参考该标准来提升系统或零部件的安全性能[8]。

IEC61508 对 E/E/PE 系统和软件有特定的要求。在第一版中，没有识别除硬件以外的系统，而在第二版中，引入了“ASIC”的硬件组件要求。但 IEC 61508 对 ASIC 的定义并不是百分之百准确，它可以解释为包括许多产品：例如为特定安全系统设计的定制 IC，为安全系统类型设计的半定制 IC 和 FPGA、PLD 和 CPLD 器件。

IEC61508 标准共分为 8 个部分：第 0 部分为技术报告，介绍了功能安全和 IEC 61508；第 1 部分为一般要求；第 2 部分为 E/E/PE 系统要求；第三部分为软件要求，第 4 部分为定义和缩写；第 5 部分为安全完整性等级测定方法示例；第 6 部分为 IEC 61508-2 和 IEC 61508-3 应用指南；第 7 部分为技术措施概述[7,9]。

2.3　ARP 4761 和 IEC 61508 在安全性分析方法上的差异

ARP 4761 描述了民用飞机适航合格审定的安全性评估指南和方法[9]。该标准安全性评估的对象是机载系统及其失效问题，适用于支持机载系统的安全性设计和适航审定。该标准所提出的民机系统安全性评估过程是一个自上而下的分析过程：以飞机级功能危险分析为起始，再到系统级功能危险分析，并在故障树分析中把系统级功能危险分析的结果作为顶事件，最后进入 PSSA 的过程[10]。但 ARP 4761 中安全性分析方法有以下不足：1）仅考虑组件之间直接的功能交互；2）欠缺危险因素与人为因素之间相互影响的安全性分析；3）各种安全性分析仍偏重于概念、实施原则的顶层描述，缺少分析程序，难以细化和应用到具体的案例中[9,11]。

而 IEC61508 标准对安全完整性进行了定义，表明安全完整性是在规定条件下、规定时间内，安全相关系统成功实现所要求的安全功能的概率[12]。为量化安全完整性，IEC61508 定义了安全完整性等级的概念。安全完整性等级是一个重要指标，它用于规定电气/电子/可编程电子部件（E/E/PE）和系统的安全功能的安全完整性要求，并作为一个必要措施，规定了安全系统在安全性上必要风险降低的概率。IEC 61508 作为国际安全标准，将安全完整性等级分为 4 个等级，分别为 SIL4、SIL3、SIL2、SIL1 等级划分表明：SIL 等级越高，系统的安全性能就越高[7-8,13-14]。并且 IEC61508 中描述了计算 PFD（probability of dangerous failure on demand）和 PFH（average frequency of a dangerous failure per hour）的基本原理，解释了公式的导出过程。

在低要求模式下需使用 PFD_{avg}（average probability of dangerous failure on demand）评价安全完整性等级，而高要求和连续模式使用 PFH 来评价评价安全完整性等级。因此能够根据实际需求进行精确的计算，且能符合实际应用中各种假设和应用条件，对安全性设计分析给出了相关依据。

因此，本文在对失速告警系统的安全性分析上选择依据 IEC 61508 标准。

3　处理器技术发展

3.1　单核处理器

单核处理器将一个芯片集成在一个处理器中。通常，传统方法提升单核处理器的主频性能是通过增大数据宽度来实现[15]。但随着技术的发展，单核处理器主频的提升已达到工艺加工的极限。除此之外，单核处理器的局限性还有以下几点：1）单核处理器的单一线程不能提高系统的并行能力，并且处理速度比双核或多核处理器慢；2）处理器主频的提升也增加了功耗，加大了散热量，并且目前没有适配的散热系统处理散热，来确保处理器工作正常稳定；3）在计算或功能处理要求较高的情况下，单核处理器有很多缺陷和不足[16]。

总之，频率、功耗和设计各方面均限制了单核处理器的性能的提升和发展[16]。而多核处理器把任务合理分配后利用多个内核协同处理，解决了以上问题[17]。

3.2　多核处理器

多核处理器（CMP，chip multiprocessor）将多个处理器集成在一个芯片中。并根据芯片中集成内核的结构是否相同，可将多核处理器分为同构多核处理（homogeneous multi-core processor）和异构多核处理器（heterogeneous multi-core processor）。同构多核处理器将两个或多个结构、地位对等的内核集成在一个芯片中[18]。而异构多核处理器则将不同架构或特性的内核集成在一块处理器上，并且可根据不同的计算任务，将其分配给不同的内核进行计算、处理，双核并行处理方式使得处理器执行复杂任务效率更高，资源配置更加合理[19-20]。双核 CPU 基本架构如图 1 所示。

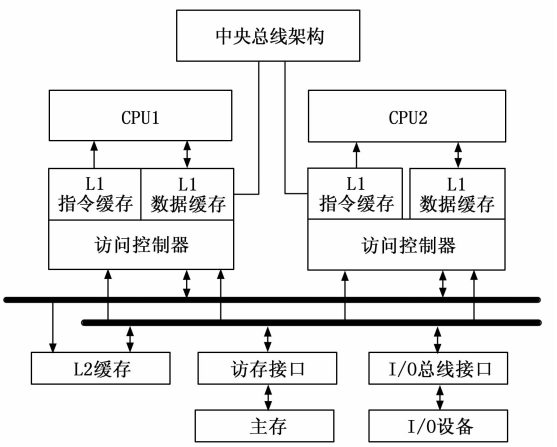

图 1　双核 CPU 基本架构

在航空产品中，失速告警计算机对于可靠性和安全性的要求较高。文中失速告警计算机的设计采用异构双核处理器，该处理器可通过异构双核处理器中的数据共享内存机制进行数据共享和交互，从而任务的处理和执行更加高效。

4 失速告警计算机安全性分析与研究

4.1 处理器安全性分析

为保证硬件故障容错能力，IEC 61508 标准提出了一系列技术手段。其中，提高系统可靠性和可用性的一个重要手段就是采用冗余结构，冗余结构包括 N 取 M 冗余架构、冗余校验等[8,13]。下面着重介绍 N 取 M 冗余架构。

N 取 M 冗余架构也被称作冗余表决结构，一般记作“Moo$N$”，表示“M out of N”，即从 N 中取 M，冗余数 $K=N-M$。N 中取 M 冗余架构要求架构中共有 N 个单元，但至少有 M 个单元正常工作时，系统才能正常工作[14]。MooN 结构系统可靠性如图 2 所示。图中 λD 代表子系统中通道的危险失效率（每小时）。

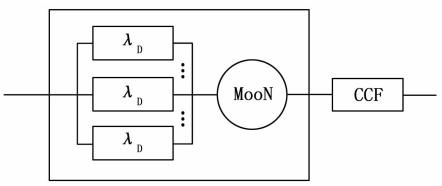

图 2 Moo$N$ 结构系统可靠性框图

常见的冗余表决结构有“1oo1”、“2oo2”、“1oo2D”等。冗余通道的存在使得有故障出现时，还有备用设备可以暂时维持系统的正常运转，这样的做法提高了系统安全性和可用性。但是冗余通道越多，系统就越复杂，并且不同通道之间是否存在相互影响的关系也会很难分析，增加了系统的误操作率，即会增加系统的安全失效率，同时还会引入共因失效的问题。因此，并不是冗余通道越多越好，还需根据实际情况分析系统的可靠性和可用性之后再选择不同的冗余架构[8]。

共因失效（CCF，common cause failure）是指由于某种相同的原因导致系统中两个或多个部件失效或故障。虽然冗余架构可以有效提高系统的可靠性[4,7]，但是在产品的设计、运行和维护各阶段，由于内因或者外因均可能引起共因失效，共因失效率与系统结构有关，即与冗余架构的通道数有关[21-22]。

4.1.1 基于单核处理器的失速告警系统的安全性分析

对于失速告警系统，不允许单点故障，因此通常采用 2 台失速告警计算机构成“1oo2”系统，但出于对运营成本等约束条件的考虑，系统一般会采用 2 台相同的失速告警计算机进行设计，故而对于单台失速告警计算机就可以等效为“1oo1”结构。该结构只由一个通道构成，通道的任何危险失效都将引起降低失速告警系统的安全功能[8]。“1oo1”物理框图如图 3 所示，“1oo1”可靠性块图如图 4 所示。

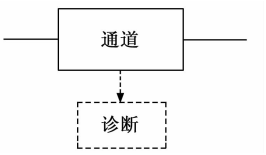

图 3 “1oo1”物理框图

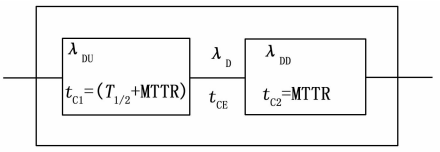

图 4 “1oo1”可靠性块图

图 4 表明，单个通道可以被认为由两部分组成：一部分具有由未被检测到的失效导致的失效率 λ_{DU}，另一部分具有由已被检测到的失效导致的失效率 λ_{DD}，λ_D 表示为整体失效率，整体失效率 λ_D 与个体失效率 λ_{DU} 和 λ_{DD} 的关系是：

$$\lambda_D = \lambda_{DU} + \lambda_{DD} \tag{1}$$

通道的等效平均停止工作时间为 t_{CE}，等于两部分各自的停止工作时间 t_{c1} 和 t_{c2} 相加，它与各部分对通道失效概率的贡献直接成比例：

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \tag{2}$$

式中，T_1 表示手动检查测试的时间间隔。对于一个具有由危险失效而导致关闭时间为 t_{CE} 的通道：

$$PFD_{avg} = 1 - e^{-\lambda_D t_{CE}} \approx \lambda_D t_{CE} \tag{3}$$

因为：

$$\lambda_D t_{CE} \ll 1 \tag{4}$$

PFD 是指安全相关系统被要求时执行安全功能的失效概率，即安全功能的不可用性。上式中，PFD_{avg} 是 PFD 在给定时间段内的平均值。

因此，对于“1oo1”结构，在要求时的平均失效概率为：

$$PFD_{avg} = (\lambda_{DD} + \lambda_{DU})\, t_{CE} = \lambda_D t_{CE} \tag{5}$$

考虑到 $MTTR$ 与 T_1 相比，数量级差别较大，公式可以进一步简化为：

$$PFD_{avg} = (\lambda_{DD} + \lambda_{DU})\, t_{CE} = \lambda_D t_{CE} =$$
$$\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right) + \lambda_{DD} MTTR \approx \frac{T_1 \times \lambda_{DU}}{2} \tag{6}$$

PFH 的含义是给定时间内安全相关系统执行安全功能的平均危险失效频率。假设在高要求或连续模式下，需计算 PFH，当诊断模块检测出危险故障时，立即驱使受控设备（EUC，equipment under control）进入安全状态。因此得出“1oo1”结构的 PFH 为：

$$PFH = \lambda_{DU} \tag{7}$$

此外，失速告警系统中还需对振杆器进行操纵，对于

单核处理器，其控制电路如图 5 所示。

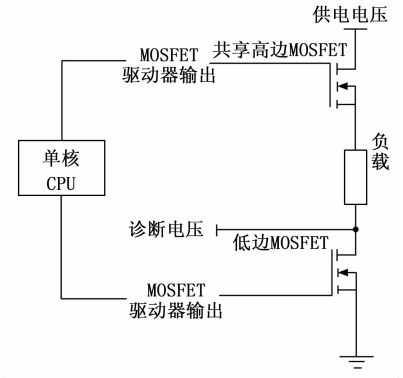

图 5　单核处理器下振杆器硬件控制电路

由于采用单核处理器，在需要导通 MOSFET 时，单核处理器将同时导通高边/低边 MOSFET。如果处理器存在故障，则有相应的概率会同时导通或截止高边/低边 MOSFET，即使有相应的检测短路接地故障向 MCU 发送信号，也无法阻止错误的导通或截止高边/低边 MOSFET。因此，该设计缺乏处理器对这个单点故障的诊断覆盖。虽然在系统级采用了“1oo2”的架构，但是对于成本约束而采用的相似失速告警计算机的设计上，在系统架构设计中仍无法避免共模故障的存在。

4.1.2　基于异构双核处理器的失速告警系统的安全性分析

而对于采用异构双核处理器设计的单台失速告警计算机，可等效于两种非相似计算机，其共模失效可简化为“与”的架构，其等效于“1oo2D”架构。“1oo2D”架构的输出与其它架构不同，该架构是在“1oo2”架构的基础上增加了诊断功能。当诊断到两个通道中的任一通道出现故障，则输出切换到另一通道采用备用通道进行正常输出控制信号。当诊断到两个通道同时出现故障，或者检测到两个通道的信号存在差异并且不确定是哪个通道故障时，输出将会进入安全状态。该结构模式下，任何一个通道都能够通过一种独立于另一个通道的方式获取另一个通道的状态[23]。此架构能够有效保证系统设计的高安全性和高可靠性。“1oo2D”物理框图如图 6 所示，“1oo2D”可靠性块图如图 7 所示。

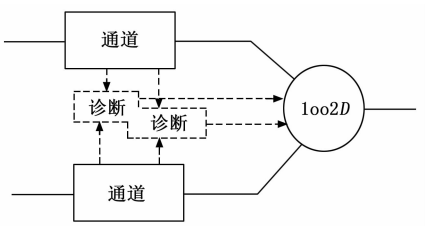

图 6　“1oo2D”物理框图

λ_{SD}表示为可诊断安全失效率，每个通道中被检测的安全失效概率如下：

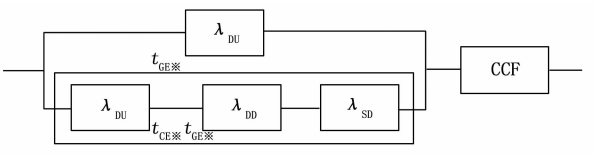

图 7　“1oo2D”可靠性块图

$$\lambda_{SD}=\frac{\lambda}{2}DC \tag{8}$$

本架构等效平均停止工作时间的值与其他架构给出的数值不同，因此他们被表示为 t'_{CE}与 t'_{GE}。

$$t'_{CE}=\frac{\lambda_{DU}\left(\frac{T_1}{2}+MTTR\right)+(\lambda_{DD}+\lambda_{SD})MTTR}{(\lambda_{DU}+\lambda_{DD}+\lambda_{SD})} \tag{9}$$

$$t'_{GE}=\frac{\lambda_{DU}\left(\frac{T_1}{3}+MTTR\right)+(\lambda_{DD}+\lambda_{SD})MTTR}{(\lambda_{DU}+\lambda_{DD}+\lambda_{SD})} \tag{10}$$

“1oo2D”架构在要求时的平均失效概率如下：

$$PFD_{avg}=2(1-\beta)\lambda_{DU}((1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU}+\lambda_{SD})t'_{CE}Et'_{GE}E+\beta_D\lambda_{DD}MTTR+\beta\lambda_{DU}\left(\frac{T_1}{2}+MTTR\right) \tag{11}$$

与“1oo1”架构相似，在计算 PFH 时，假设在高要求或连续模式下，当诊断模块检测出任一危险故障时，立即驱使 EUC 进入安全状态。因此最后失效通道不应包含 λ_{DD} 的成分，因此得出“1oo2D”架构的 PFH 为：

$$PFH=2(1-\beta)\lambda_{DU}((1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU}+\lambda_{SD})t'_{CE}+\beta_D\lambda_{DD}+\beta\lambda_{DU} \tag{12}$$

“1oo1”架构与“1oo2D”架构在设计上各有利弊，如“1oo1”结构相对简单，开发成本和硬件复杂度较低，但在功能设计上要求比较高，SIL2 要求达到不低于 90％的诊断覆盖率；“1oo2D”架构引入了诊断模式，且由于异构处理器双通道架构将共因失效概率大大降低，虽然在架构设计上增加了一定的复杂性，但可以获得高安全性[24]。

对于失速告警系统，2 台基于单核处理器的失速告警计算机可以构成“1oo2”结构，但对于单台失速告警计算机来说就是“1oo1”架构，这个架构虽具有诊断功能，但诊断覆盖率 DC 是有限的。而基于异构双核处理器的失速告警计算机除本身就是“1oo2D”结构外，在整个系统的构成上也是“1oo2”结构，且 DC 对比单核要高很多。异构双核处理器因其有两个架构或特性不一样的内核，所带来的非相似性可以避免基于单核处理器所构成的失速告警系统自身“1oo2”结构产生的共因问题。

对于异构双核处理器操纵振杆器的方式，其控制电路如图 8 所示。

如图 8 所示，高边 MOSFET 与低边 MOSFET 分别由异构处理器的两个核控制作为一种安全机制。

4.1.3　安全性分析结果的对比

基于上述对单核处理器的失速告警系统和异构双核处

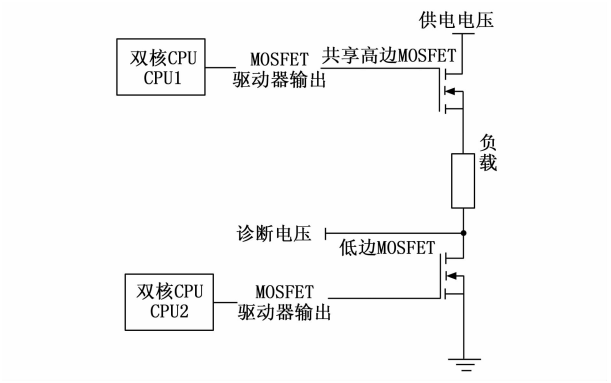

图 8 异构双核处理器下振杆器硬件控制电路

理器的失速告警系统的安全性分析，通过前面所列公式可以得出：将所要求的平均失效概率 PFD_{avg} 作比较，“1oo2D”结构的 PFD_{avg} 远小于“1oo1”结构。并且在抖杆器控制电路一样的情况下，异构双核处理器分别控制高边 MOSFET 与低边 MOSFET，使得有更低的概率导致误操作，安全机制更为可靠。

从以上定性分析可以看出，异构双核处理器相比于单核处理器有更高的安全性和可靠性，并且“1oo2D”结构可以进行更加完整的故障诊断，从另一维度提升了系统的性能。

5 结束语

本文从处理器、IEC 61508 和 ARP 4761 标准的介绍和发展为背景，先是对两个标准进行了简单介绍，随后简要描述了从单核处理器到多核处理器的发展。从处理器入手，在设计时充分考虑失速告警计算机功能设计需求及安全性、可靠性等多方面要求，选择采用异构双核处理器对失速告警计算机的任务进行合理分配，并应用双核处理器特有的核间共享内存通信机制进行数据的交互，还同时增加了在同一处理器上对解算结果监控和数据一致性判断这一功能。通过 IEC 61508 标准中对于不同冗余架构的安全性进行分析，确认采用异构双核处理器进行失速告警计算机的设计有助于产品安全性能的提升，并且满足整个系统对于安全性的设计要求，该安全性研究方法可为今后其他对安全性能要求较高的设计提供了参照和依据。

参考文献：

[1] 王延刚．民用飞机失速告警系统设计概述 [J]．科技视界，2017 (14)：165.

[2] 马乔兵，任 剡．飞机失速告警系统发展技术综述 [J]．西安航空技术高等专科学校学报，2012，30 (1)：6－9.

[3] 陈 丹，徐建平，李佳嘉．新功能安全标准 IEC61508-2 的研究 [J]．信息技术，2014 (3)：111－113.

[4] 鲁守荣．基于 IEC 61508 开发安全关键系统 [J]．工业控制计算机，2016，29 (12)：1－2.

[5] SAE ARP 4761 Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment [S]．U. S. A：SAE International，1996.

[6] IEC 61508：Functional safety of electrical/electronic/programmable electronic safety-related systems [S]．International Electrotechnical Commission，1998.

[7] 靳江红，吴宗之，胡 玢．对功能安全基础标准 IEC61508 的研究 [J]．中国安全生产科学技术，2009，5 (2)：71－75.

[8] 张瀚方．基于 IEC61508 标准的功能安全型安全栅的设计研究 [D]．上海：华东理工大学，2015.

[8] 李佳玉，员春欣．IEC61508 功能安全国际标准及安全性分析 [J]．中国铁路，2001 (1)：44－45.

[9] 崔利杰，田 宇，丛继平，等．STPA 与 ARP4761 中的安全性分析方法对比研究 [J]．航空工程进展，2020，11 (4)：508－516.

[10] 尹树悦，杨 云．军机研制中安全性标准的应用 [J]．航空标准化与质量，2010 (3)：23－26.

[11] 陈圣斌，曾曼成，王 斌，等．民用飞机安全性分析技术在军用直升机中的应用研究 [J]．直升机技术，2015 (1)：44－49.

[12] 中国机械工业联合会．电气/电子/可编程电子安全相关系统的功能安全 第 4 部分：定义和缩略语 [S]．GB/T 20438.4－2017. 2017－12－29.

[13] 谷荧柯，崔同兵，任 军，等．基于 IEC61508 标准的功能安全芯片设计方法探讨 [J]．铁路通信信号工程技术，2016，13 (5)：1－5.

[14] 李 成．IEC61508 功能安全标准在电厂安全系统设计中的研究与应用 [D]．上海：上海交通大学，2010.

[15] 英特尔软件学院教材编写组．多核多线程技术 [M]．上海：上海交通大学出版社，2011.

[16] REILLY M. When multicore isn’t enough：trends and the future for multicore systems [C] //Proceedings of Workshop on High Performance Embedded Computing，2008.

[17] KAISHUN W U，XIAO J，LIONEL M N I. Rethinking the architecture design of data center networks [J]．Frontiers of Computer Science，2012，6 (5)：596－603.

[18] 王 璇．基于异构多核处理器的多级安全任务调度算法研究 [D]．西安：西安电子科技大学，2017.

[19] 夏近伟．异构多核处理器系统的资源管理方法研究 [D]．合肥：合肥工业大学，2020.

[20] 范蟠果，陈思宇，梁贵毅．一种双核并行处理网络化数据采集系统设计 [J]．计算机测量与控制，2010，18 (4)：965－967.

[21] 李志强，徐廷学，安 进，等．冗余系统共因失效动态贝叶斯网络建模 [J]．仪器仪表学报，2018，39 (3)：190－198.

[22] 孙景全，于洪浩．安全仪表系统安全功能失效评估方法 [J]．中国石油和化工标准与质量，2017，37 (16)：116－117.

[23] 靳江红．安全仪表系统安全功能失效评估方法研究 [D]．北京：中国矿业大学 (北京)，2010.

[24] 袁宜峰，凌志浩．基于 IEC61508 的嵌入式软件可靠性设计与验证 [J]．南京工业大学学报 (自然科学版)，2011，33 (6)：82－86.