文章编号:1671-4598(2024)08-0001-07 DOI:10.16526/j.cnki.11-4762/tp.2024.08.001 中图分类号:TP277 文献标识码:A

液体火箭发动机故障诊断系统冗余容错技术研究综述

盖佳林，弭 艳，马兵兵
（北京航天动力研究所，北京 100076）

摘要：综述了液体火箭发动机故障诊断系统冗余容错技术研究，介绍了液体火箭发动机故障诊断系统在航天任务中的重要性及其不断发展的需求，强调了高可靠性和安全性对于航天任务成功的关键作用，详细分析了当前国内外在这一领域的研究现状，展示了不同国家和研究机构在故障诊断系统冗余容错技术方面的最新进展和具体应用实例，阐述了冗余容错技术对于火箭发动机故障诊断系统的重要性并探讨了该技术的发展历程、关键技术及当前研究成果；通过对比几种经典冗余容错手段，指出各冗余结构对于火箭发动机故障诊断系统的可行性与优缺点，详细介绍了发动机故障诊断系统的双机热备实现方案，为相关研究者提供参考依据；从理论基础到实际应用，从当前研究遇到的技术挑战再到未来发展方向的展望，为液体火箭发动机故障诊断系统冗余容错技术的研究提供了全面的综述和分析。

关键词：液体火箭发动机；冗余容错；故障诊断；容错控制；双机热备

Review of Redundancy and Fault Tolerance Techniques for Liquid Rocket Motor Fault Diagnosis System

GAI Jialin，MI Yan，MA Bingbing
（Beijing Aerospace Propulsion Institute，Beijing 100076，China）

Abstract：This paper summarizes the research on redundancy and fault-tolerance technology for liquid rocket engine fault diagnosis system，introduces its importance and continuous development needs，emphasizes the crucial role of high reliability and safety in the success of space missions，analyzes the current research status both domestically and internationally in detail，presents the latest progress and specific application examples from different countries and research institutions，explains the importance of redundancy and fault-tolerance technology on rocket engine fault diagnosis system，and discusses the development history，key technology and current research results of this technology. By comparing several classical redundancy and fault-tolerant means，it points out the feasibility and advantages and disadvantages of each redundant structure on the system，and introduces the two-node and hot-backup scheme in detail，which provides researches a reference basis. From theoretical basis to practical application，and then from current technological challenges in the research to future development directions，it provides a comprehensive overview and analysis of the research on redundancy and fault-tolerance technology for liquid rocket engine fault diagnosis system.

Keywords：liquid rocket engine；redundant；fault diagnosis；fault-tolerant control；two-node hot-backup

0 引言

中国航天运输系统的建设起步于20世纪60年代，经过数十年的发展，取得了举世瞩目的成就。如今，随着世界航天进入以大规模互联网星座、太空资源开发与利用、载人月球探测和大规模深空探测等为代表的新阶段[1]，我国的航天运输系统迎来向航班化技术发展的重要机遇期。发展可重复使用技术是向航班化运输前进的必经之路，而火箭发动机作为运载火箭的动力核心面临着更高的任务要求，尤其是其多次使用的特点使火箭发动机具备了全新的生命周期概念[2]，同时动力系统故障在航天系统总故障中一直占有很大的比例[3]，因此，高可靠的故障诊断功能已经成为未来发动机必须实现的技术手段之一。目前，尽管故障诊断算法已经广泛应用于诸多领域当中，但在火箭发动机的计算机系统当中还没有得到深度应用，其中一个重要的原因在于航天任务对可靠性和安全性的要求极高，故障诊断算法必须搭载在能够执行高可靠性测量任务的硬件设备上。综上，提升液体火箭发动机故障诊断系统的硬件可靠性，对于可重复使用运载火箭重大工程的持续推进有重大意义，由此国内外学者开展了较多研究[4]。

对于提高液体火箭发动机故障诊断系统的硬件可靠性，经过长期研究，容错技术成为构成高可靠性系统的重要手段。容错技术的思想是允许系统中出现某些故障，在出现这些故障时，系统仍能正常运行，并且执行结果中不包含系统中故障所引起的差错[5]。容错技术不仅能够提高航天任务的成功率，也大大降低任务失败可能导致的经济损失和安全风险，是提高液体火箭发动机计算机控制系统可靠

收稿日期:2024-05-21； **修回日期**:2024-06-05。
作者简介:盖佳林(1999-),男,硕士研究生。
通讯作者:马兵兵(1982-),男,硕士,研究员。
引用格式:盖佳林,弭 艳,马兵兵.液体火箭发动机故障诊断系统冗余容错技术研究综述[J].计算机测量与控制,2024,32(8):1-7.

性、确保航天任务顺利完成的关键。本文将从当今液体火箭发动机故障诊断功能需求角度出发，重点针对发动机故障诊断系统硬件冗余容错技术发展进行探讨，对比分析了几种冗余容错技术手段对于液体火箭发动机故障诊断系统可靠性提高的可实施性。

1 国内外研究现状

火箭发动机故障诊断系统的冗余容错技术是保障火箭发动机可靠运行的关键领域，国内外在这方面的研究和应用已有丰富的积累。

美国在这一领域目前处于领先位置。美国国家航空航天局（NASA，national aeronautics and space administration）在火箭发动机的冗余容错设计方面有着丰富的经验，尤其是在载人航天任务中。NASA 的航天飞机主发动机（SSME，space shuttle main engine）和用于新一代太空发射系统（SLS，space launch system）的 RS-25 发动机均采用了高度冗余和容错设计，以确保在多种故障模式下依然能够安全运行。SpaceX 的猎鹰 9 号（Falcon 9）和星舰（Starship）火箭都采用了先进的故障诊断系统，并结合了硬件冗余和容错算法。例如，猎鹰 9 号的每台 Merlin 发动机都配备多个冗余传感器，实时监测发动机状态，并通过先进的算法进行故障检测和诊断。波音在其火箭和太空探索器中也采用了高度冗余的故障诊断系统。波音的 CST-100 Starliner 载人飞船配备了先进的故障诊断和容错系统，以确保宇航员的安全。

欧洲空间局（ESA，european space agency）在阿丽亚娜 5 号和阿丽亚娜 6 号火箭中引入了先进的故障诊断系统，采用多重冗余传感器和自适应诊断算法，以提高系统的可靠性和容错能力。作为阿丽亚娜火箭的主要制造商，ArianeGroup 在其发动机和系统设计中广泛应用了冗余和容错技术，通过实时监测和诊断，确保发射任务的成功。俄罗斯的 Energia 公司在其重型火箭和航天器中也采用了冗余故障诊断技术，特别是在载人航天和深空探测任务中。RD 系列发动机配备了多重传感器和冗余系统，确保在不同故障情况下能够有效诊断和容错。

目前冗余容错技术还没有深度地参与到我国的火箭发动机控制系统当中，一方面，我国目前的火箭发动机搭载的故障诊断算法是以红线算法为主的较为基础的算法，其诊断结果对于容错控制的需求不高。另一方面，对于以往的航天运输系统，单机控制即可满足其可靠性需求。而随着可重复使用运载火箭重大工程的持续推进，航天科技集团在火箭的发动机控制系统中已经逐步采用冗余容错控制技术。同时，一些私人航天企业，如蓝箭航天和零壹空间等新兴的中国私人航天公司也在其火箭发动机设计中积极采用冗余和容错技术，致力于提高商用发射服务的可靠性和竞争力。

尽管国内外各国在这方面进行了大量的研究和开发，但仍面临一些困境和挑战。其主要体现在高复杂度与成本和系统重量和尺寸限制两个方面。硬件冗余和容错技术需要在火箭发动机中增加额外的传感器、控制系统和执行器，显著增加了系统的复杂性和成本。NASA 的 RS-25 发动机在进行冗余系统集成时面临高昂的研发和测试成本。而增加冗余硬件会导致系统重量和尺寸的增加，这在火箭设计中是一个重大问题，因为每增加一点重量都会显著影响火箭的性能和成本。SpaceX 在 Raptor 发动机设计中，必须在保持高性能的同时尽量减少冗余系统对重量和尺寸的影响。此外，多重冗余系统增加了故障诊断和管理的复杂性，需要更先进的故障检测和隔离算法来确保系统的可靠性。在 RS-25 发动机的应用中，NASA 采用了复杂的 FDIR（故障检测、隔离和恢复）算法，但实现这些算法需要高性能计算资源和大量的验证工作。以上这些难点意味着研发需要高度专业化的人才和长期的技术积累，使得新兴的私人航天公司如蓝箭航天和零壹空间在发展冗余技术时，可能面临专业人才短缺和技术积累不足的问题。

火箭发动机故障诊断系统硬件冗余容错技术在国际上已经取得了显著的进展，包括多级冗余传感器、先进的故障检测与隔离（FDIR，fault detection，isolation，and recovery）算法和智能容错控制等。然而，仍面临一些挑战，如系统复杂性、成本和新技术的应用验证等。未来的发展将侧重于智能化、分布式和高可靠性的方向，不断提高火箭发动机的容错能力和可靠性。

2 液体火箭发动机故障诊断系统

液体火箭发动机作为运载火箭中故障频发的关键部件，其可靠性直接影响到发射任务的成败。据报道，至 2006 年底，美国的液体火箭发动机故障占运载器故障的 60％以上。为了有效降低发动机故障的风险，美国自 20 世纪 70 年代起便开始在火箭发动机上应用发动机健康管理系统（EHMS，engine health management system），该系统基于故障诊断算法，相比于传统的遥测系统，EHMS 专门针对火箭发动机的实时健康监测和故障预测，采用高级算法和人工智能技术进行数据分析，以提高火箭的可靠性和安全性；而传统的遥测系统则侧重于从远程位置收集和传输数据，在数据有效性以及后续的数据分析方面准确性以及时间的敏感性不足。相比之下，中国的液体火箭发动机健康管理系统以红线算法为主，通过监测缓变参数判断发动机是否工作异常，部分发动机健康管理任务还是由遥测系统承担，与国际先进水平仍有差距，迫切需要发展更为成熟的 EHMS。

如今，EHMS 的核心已不再局限于故障诊断算法，而是逐渐拓展为液体火箭发动机故障诊断系统。如图 1 所示，液体火箭发动机故障诊断系统是一种集成了传感器、数据处理单元和先进算法的复杂系统，旨在实时监测和分析液体火箭发动机的运行状态，以便及时发现并诊断潜在的故障。这些系统通过收集发动机工作过程中的各种参数数据，如温度、压力、流量和振动等，利用信号处理技术、基于模型的方法、人工智能技术等手段，对数据进行深入分析，从而识别发动机可能出现的性能下降、异常行为或其他故障征兆。

为了确保火箭发动机在多次飞行任务中的可靠性和安全性，采用冗余容错技术成为提高故障诊断系统效能的关

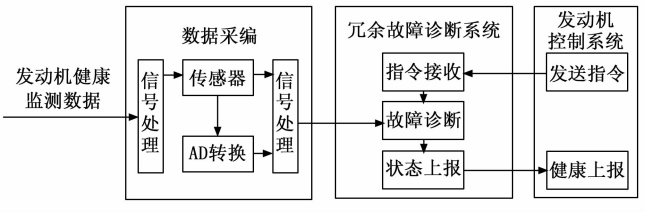

图 1　液体火箭发动机故障诊断系统框图

键策略。这种技术的应用显著提升了系统的容错能力，即使在部分组件失效的情况下，也能保证火箭发动机的正常运行和任务的顺利完成。

3　冗余容错技术

3.1　容错技术发展概述

容错技术最早由冯诺依曼（John Von Neumann）提出[6]，指的是应用于计算机系统中，以提高系统在发生故障或错误时可靠性的各种技术手段，包括冗余设计、错误检测与纠正、备份与恢复等。容错技术在早期计算机系统中的应用主要集中在硬件冗余和基本的错误检测上。20 世纪 50 年代末，随着计算机系统在军事、航天等关键领域的应用，系统的可靠性和稳定性变得极为重要，容错技术开始受到更多关注。在 20 世纪 60 年代，美国和苏联的太空竞赛催生了对高可靠性系统的需求，这一时期的容错策略主要集中在硬件冗余、简单的错误检测和恢复机制上。美国的阿波罗月球登陆计划是早期采用容错技术的典型例子，尤其是在阿波罗导航计算机的设计中，采用了多种技术来确保计算精度和操作可靠性，使得容错技术达到了一个新的高度。到了 70 年代，容错技术成为计算机科学研究的重要领域。研究者开始探索不同的容错模型和算法，如重启、软件和硬件冗余技术等，系统的规模越来越大。在 80 年代，处理器的运算效率相比于先前得到了显著的提高。硬件冗余成为常见的设计策略，同时，软件技术和相关理论进一步完善，软件在航天飞行器中扮演着越来越重要的角色。开发者采用了多种软件容错技术，包括但不限于错误检测、错误恢复和软件多版本设计，以确保软件系统的稳定性和可靠性。90 年代以后，容错技术从硬件和软件两个方面同时发展，逐步从静态的故障隔离转变为动态的自我修复，应用场景越来越广泛。如今容错技术不再局限于硬件和软件层面，技术的应用范围已经扩展到了系统的网络、存储和数据库等方面[7]，能够在更广泛的应用场景下提高系统的可靠性。随着航天技术的国际合作，对于容错系统的设计和评估方法也逐渐呈现标准化趋势，旨在确保不同的航天器能够兼容并保持高可靠性。如今，随着计算能力的提升和算法的进步，航天器开始采用更加智能化的容错策略，这包括使用先进算法来预测和诊断潜在故障实现故障诊断，以及自动化的硬件冗余决策制定过程以最小化任务失败的风险。随着人工智能技术的进步，未来的航天容错系统将更加智能和自主，能够实时分析数据，自我诊断并隔离、修复系统故障，甚至在设计阶段就能预测和规避潜在的故障点。

3.2　冗余技术

冗余技术是实现计算机系统容错的重要手段。所谓冗余技术是指采用多余的元件、信号或信息，在原本的设计方案中增加系统冗余元素，一般可分为硬件冗余、软件冗余、时间冗余和信息冗余[8]。在实践中，航天计算机系统常常采用混合冗余策略，结合上述一种或多种冗余技术，以提供更高级别的容错能力。按照系统的冗余度来划分，冗余计算机系统可分为双控制器冗余和多控制器冗余。

3.2.1　双控制器冗余

双机备份结构有 4 种备份方式，即冷备、温备、热备和双工[9]。它们的拓扑结构如图 2 所示，左机为工作机，右机为备份机。

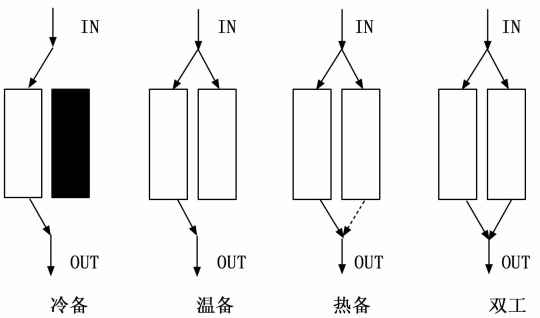

图 2　双机备份结构拓扑图

双机冷备配置中，主机和备份机是两套独立的系统，其中主机在正常运行并处理数据，而备份机则处于待命状态，当主机发生故障无法继续提供服务时，系统通过故障检测机制触发备份机上电启动。周宇杰等人[10]考虑到立方星在太空环境中面临的特殊挑战，如总剂量效应和单粒子效应，选择了适合其特点的冷备份策略以优化可靠性、降低功耗，并减小硬件冗余规模。楼智翔[11]介绍了一种信号切换模块的设计原理和实现方法，信号切换是双机冷备计算机系统实现的关键功能，负责两套计算机之间 I/O 接口的正确和可靠切换，对系统整体可靠性有重要影响。尽管双机冷备提供了一种相对简单的方式来增加系统的可靠性，但其较长的切换时间和低自动化程度限制了其在对实时性和连续性要求较高的应用场景中的适用性。

双机温备技术是在双机冷备的基础上发展而来，通过在备用机中始终上电的数据备份单元，使得当主机出现故障时，备份机可以立即使用之前主机的运行现场数据进行工作，无需从外部系统获取数据，从而缩短了恢复周期，提高了效率。双机温备技术在一定程度上解决了传统冷备份对实时性和性能提升的限制问题。贾文涛等人[12]提出的新型双机温备设计通过功能上的划分提高了系统的效率和可靠性：主机负责高效运行星务程序，从机则专注于提高系统可靠性。这种设计在保证高可靠性的同时，提高了实时性并减少了备份机制对性能的消耗。在可实现方面，黄影等人[13]提出的基于 FPGA 的双机温备方案，通过良好的可扩展性和易于定制的容错逻辑，实现了故障判断与自我

修复功能。此方案还支持根据主机的标志来决定是否执行应用程序，具备重新配置的能力，进一步增强了系统的灵活性和可靠性。付剑课题组[14]专注于抗单粒子效应的硬件容错设计研究，提出了一个可通信的高可靠双机温备方案和具备刷新功能的存储器容错技术。这些技术结合形成了基于 FPGA 的多级容错机制，提升了整个系统的抗辐射能力。此外，他们还设计了一个可控重启时间的电路，以确保关键设备和系统的正常运行[15]。

双机热备是一种高度自动化的容错机制，主要特点包括主机和备机同时加电工作，以及在主机故障时自动切换到备机继续工作，保证了系统的实时性和可靠性[16]。这种结构保证了机器切换前后的工作一致性，具有较高的任务可靠性和自检测能力，满足关键和实时性的任务要求。双机热备系统的关键在于实现双机间的有效协调和管理。殷杰波等人[17]针对双机热备总线上的控制器没有热备份的问题，提出了一种通过软件实现总线控制器双机热备份的设计思想和方法，解决了一旦总线控制器出现故障，整个总线系统会瘫痪的问题。罗贵舟等人[18]提出的多策略双机热备方法针对网络环境和程序故障引起的服务中断问题，通过主备节点间的心跳信号和数据库时间同步机制实现双重心跳检测，避免裂脑问题。马丽娜[19]在双机热备技术中引入了仲裁比较机制，通过仲裁比较模块的判断，可以选择当前正确的控制结果输出，显著提高了系统的整体性和可靠性。

双机双工的工作方式也称为双模冗余结构，与双机热备相比都是双机同时上电工作，一起采集处理数据，但两机的结果双机热备方式由当前主机输出，而双模冗余结构存在比较裁决模块，起到系统检测和通道切换的作用，主机和备机的输出先在裁决模块中进行比较，结果一致才对外输出，但是裁决部位会出现单点故障失效问题，且表决机制的制定会加大设计难度，增加了设计成本[20]。采用无中心裁决结构的双机备份结构，可靠性通常要高于采用有中心裁决结构的双模冗余系统[21]。学者们针对双模冗余结构特点进行了各种提高可靠性的研究。在系统的总体结构设计方面，Zhu 等人[22]研究了一种去中心化的仲裁切换逻辑和架构设计，旨在通过每个子系统中加入 FPGA 控制逻辑来实现状态检测、主备切换和同步控制，提高了系统的可靠性。陈玉坤等人[23]则是从自主切换的策略角度出发，提出了一种改进的自主切换策略，采用软件表决和软件选通的方式，有效地消除了硬件比较器的关键单点故障问题。关于双模冗余单机故障后的恢复技术研究，Kahe 等人[24]设计介绍了一种双冗余可恢复探空火箭计算机系统。设计了主管监视操作单元，进行故障检测，并通过用备份单元替换的方式恢复故障单元，尝试重新再修复。Samet 等人[25]从切机时间及可靠性角度出发，提出了一种以纯硬件实现的容错方式实时运行的双模冗余系统结构。缩短了单机恢复时间，减少了恢复过程的逻辑段数量。

3.2.2 多控制器冗余

三模冗余技术（TMR，triple modular redundancy）是一种经典的容错技术，其核心思想是通过三份相同的硬件模块并行执行相同的任务，并通过一个仲裁器来决定最终的输出，如图 3 所示。这样，即使一个模块发生故障，系统仍然能够依靠其他两个模块的正确结果继续运行，从而大大提高了系统的可靠性和容错能力。针对不同可靠性的要求 TMR 还可以扩充为五模冗余、七模冗余等多模冗余方法，其可靠性正比于冗余模数[26]，但同时，系统成本和体积也会随之增加。

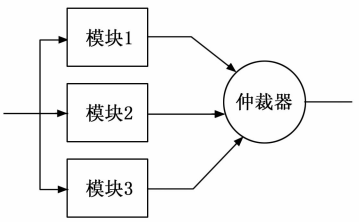

图 3 三模冗余结构示意图

在 TMR 系统中，3 个模块必须在同一时刻执行相同的操作以便仲裁器可以正确地比较和选择输出结果，因此同步技术成为确保所有冗余模块能够以准确一致的状态执行相同任务的关键。熊庭刚等人[27]提出并实现了一种基于操作系统调用的同步机制，通过软硬件结合的方式执行同步算法，对应用程序完全透明，无需人工设置同步点，简化了系统的使用和管理。安占新等人[28]则是针对多模异构冗余软件系统不同步的问题，从不同步的时机、方式等角度出发，提出了消除这些影响因素的软件设计思想，给出了软件同步设计方案。故障的消除与系统的恢复方面，沈霏等人[29]通过采用三模冗余设计，结合硬件和软件的容错措施，提高了计算机系统的可靠性和安全性。这种设计消除了单点故障，引入了故障重构和降级策略，提升了飞行器计算机系统的实时性和可靠性。Shubham 等人[30]提出了一种基于 FPGA 的容错技术实现方法，这项技术能够快速识别故障是影响了冗余单元还是仲裁判别系统，并区分故障的性质是永久的还是暂时的。此外，该方案通过重新计算延迟方法，能够从单一暂态故障中有效恢复计算系统，特别适合实时应用场景，故障识别和恢复过程的时间需求小于 8 ns，显示出极高的效率和适应性。理论研究方面，Aguiar 等人[31]针对表决电路的重要性，提供了用于辐射环境（如航天任务）的多数表决架构设计探索。提出了一种基于信号概率的特定单一事件瞬变特性（SET，single－event transient）研究方法。该研究通过基于信号概率的 SET 特性化方法优化了 TMR 策略，特别是在面对航天应用这种辐射环境时，不同表决器架构表现出的 SET 率和输入依赖性有明显差异，为选择最适合特定环境的表决器架构提供了依据。

3.2.3 复合冗余结构

除以上介绍的典型冗余结构外，针对一部分领域对系统可靠性特化要求，研究者们提出了一些新型冗余结构。朱明俊[32]在面对传统冗余设计中的体积劣势问题时，提出了一种新型的双机容错结构方案，该方案对星载计算机处

理器的最小系统进行备份，而非整个系统，从而有效减少了电路面积。王新志[33]设计了一种针对微小卫星需求的智能冗余容错系统，该系统具备两套能够完全独立操作的计算机，支持双机热备和双机冷备两种工作模式。梁立柱[34]通过构建各种箭载控制计算机结构的可靠性模型进行可靠性计算和分析，发现采用结合三取二表决电路的 1553B 总线控制器的双冗余结构方案，有效提高了系统的可靠性和容错能力。满梦华等人[35]针对复杂电磁环境下嵌入式控制系统的可靠运行问题，考虑到不同类型的芯片（如 ARM 和 FPGA）对相同电磁干扰的敏感性存在差异，设计了一种基于 ARM 和 FPGA 的可重构双机并行处理模型，并采用双机热备策略来保证系统的可靠性。设计策略的核心在于利用 ARM 和 FPGA 两种芯片的互补优势，并行处理提高系统的处理能力，同时通过双机热备策略显著提高系统在恶劣电磁环境下的可靠性和稳定性。“二乘二取二冗余”（D2V2R，two-out-of-two redundancy）结构在安全关键系统的设计中，提供了一种有趣的可靠性与安全性增强方案。如图 4 所示，这种结构通过将两个双模比较子系统结合使用，并在这些子系统间实行热备份，从而在不依赖于传统的多数表决机制的情况下提高系统的容错能力。

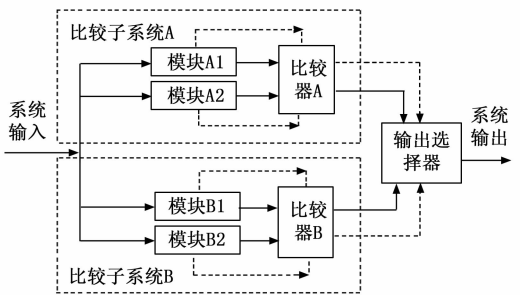

图 4　“二乘二取二冗余”（D2V2R）系统结构

陆阳等人[36]对 D2V2R 结构的工作原理进行了详细的分析，提出了两种不同的控制策略。研究团队通过使用马尔可夫过程模型，量化系统在长期运行中的可靠性和安全性表现。这种分析方法不仅能够揭示不同控制策略和系统结构对于提高系统可靠性和安全性的效果，还能够为设计更加复杂和安全关键的系统提供理论依据和指导。

4　发动机故障诊断系统冗余方案

4.1　冗余方案对比

液体火箭发动机故障诊断系统能够持续监测发动机的关键参数，如温度、压力、转速等，识别和诊断发动机运行中的异常情况和潜在故障，进而对发动机的健康状况进行评估，并预测未来的性能和潜在故障。为实现以上功能，要求系统必须高度可靠，以确保在极端条件下也能正常工作。需要快速识别和响应故障，以避免或减轻潜在的损害。另外考虑到火箭发动机严苛的工况，系统重量应尽可能轻且功耗可控，体积应紧凑，以适应火箭有限的空间。根据这些需求，对比 4 种典型的冗余方案如表 1 所示。

表 1　冗余容错方案对比

冗余方案	可靠性	响应速度	重量体积	功耗
双模冗余	较差	较快	较小	较低
三模冗余	高	较快	大	高
双机冷备	较高	慢	较小	低
双机热备	较高	快	较小	较低

较为理想的设计方案需具备良好的可靠性，实时性响应速度越快越好，同时，较低的功耗和体积使系统能够灵活搭载在火箭发动机上。对比可知双模冗余由于仲裁模块单点失效的问题，导致其在可靠性方面较差，近年来的研究多偏向于使用软件方法进一步提高可靠性。三模冗余和多模冗余结构虽然提供了很高的可靠性，但由于需要更多的硬件组件，这导致了体积和重量的显著增加。双机冷备常应用于抗辐射空间环境中，但存在切换响应速度慢的问题，这在对实时性要求极高的火箭发动机故障诊断系统中是不可行的。相比之下，双机热备当主系统发生故障时，备份系统可以立即接管任务，确保了发动机的正常运行和数据的连续监测，同时相比于三模冗余，其重量、体积可控，功耗偏低。因此，双机热备成为液体火箭发动机故障诊断系统中一个比较理想的冗余解决方案。

4.2　发动机故障诊断系统的双机热备实现方案

4.2.1　系统架构

双机热备冗余架构为两个独立的部分，它们同步执行相同的任务，如果其中一个部分发生故障，另一部分直接接管任务，从而保证系统的正常运行。

发动机故障诊断系统的双机热备实现方案总体系统设计架构如图 5 所示。

系统根据发动机检测参数的重要性设置冗余传感器，多个采编单元分别采集传感器数据，通过双冗余总线与发动机故障诊断器通讯。故障诊断器主、备机同时启动工作，并进行时间同步，主机控制冗余总线与采编单元通讯，备机同步接收总线上采编单元的数据，主备机同时对数据进行计算分析。优先使用总线 A 的数据，当总线 A 无应答或数据校验错误时，使用总线 B 的数据。故障诊断器主机与备机通过握手信号监测彼此工作状态，当主机发生故障时，备机会监测到握手信号异常，备机将接管总线的控制权，关闭主机的总线接口，之后由备机计算分析数据，并将结果上传到总体故障检测系统。

4.2.2　关键技术及挑战

双机热备系统的关键在于实现双机间的有效协调和管理。为保证系统功能及运行操作的正确性，需掌握双机同步、故障检测及仲裁切换 3 项核心技术[37]。

双机同步技术用于消除双机间工作的差异，确保备机跟随当班机工作。根据同步的严格程度和应用场景的不同，可以分为紧同步、松散同步和任务级同步 3 种类型。紧同步要求两台机器在任何时刻都保持完全一致的状态，包括内存数据、程序计数器、寄存器状态等。松散同步允许两

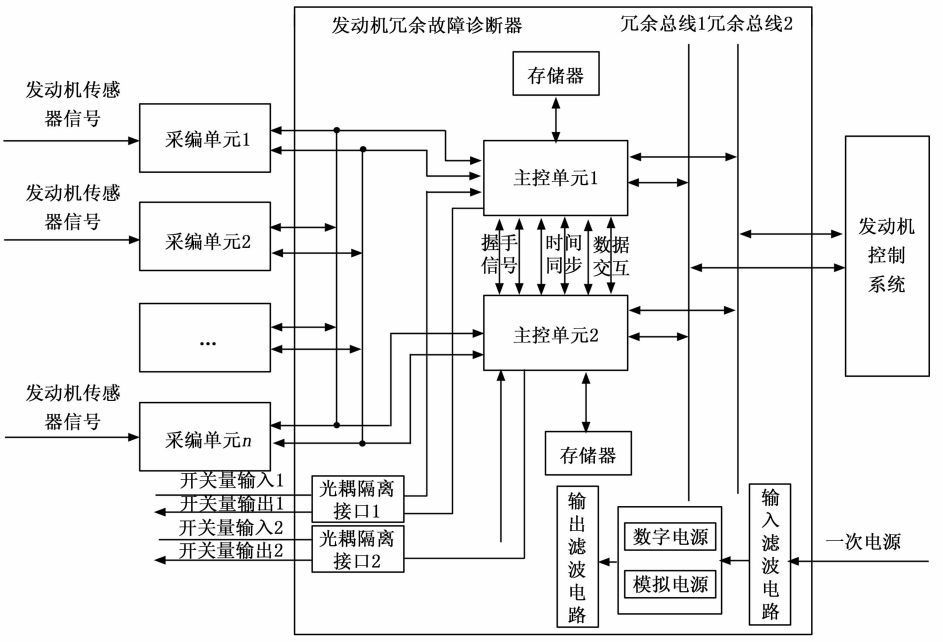

图 5 发动机故障诊断系统框图

台机器在一定时间窗口内不完全一致，但必须在特定时刻或条件下达到一致状态。任务级同步是指在执行特定任务或操作时保持同步，而在其他时间则可能不同步。选择合适的同步类型对于确保系统的可靠性和效率至关重要。对于发动机冗余故障诊断系统，可以采用松散同步，每个通讯周期同步一次。

故障检测技术用于实时监控系统状态，从而在出现问题时迅速识别并采取措施[38]。常用的故障检测方法有自主式故障检测、比较式故障检测和看门狗故障检测[39]。自主式故障检测是每台机器独立运行检测算法，监测自身的健康状况。比较式故障检测方法为两台机器相互比较彼此的输出结果或对方发送的握手信号（心跳信号），如果存在差异或异常，则表明其中一台机器出现了问题。看门狗故障检测则是使用看门狗定时器来监控系统或进程的运行状态，如果系统无响应，则触发重启或其他恢复操作。在发动机冗余故障诊断系统设计方案中，互相检测彼此心跳信号并结合看门狗故障检测是比较推荐的设计方案。

仲裁切换技术负责在检测到故障后，决定并执行从故障机器到无故障机器的工作切换。这通常涉及到一个仲裁策略，它根据故障检测结果和系统状态来决定是否需要切换以及如何切换。切换策略可能包括自动切换、手动切换或基于预定义规则的智能切换。对于发动机故障诊断系统，由于发动机工作时间短，因此工作时不考虑二重故障的情况，总线切换策略只会从主机到备机单向切换一次。

5 未来与展望

目前，火箭发动机故障诊断系统冗余容错技术的相关研发已经较为成熟，但仍面临诸多技术挑战。各国在火箭发动机中广泛应用多级冗余传感器系统，如何有效集成多级传感器数据，以及如何进行可靠的数据融合和冗余检测仍然是关键挑战。此外，系统重量和体积的增加，以及系统集成复杂性的增加是当前面临的挑战之一。另一方面，智能化和自适应系统是未来火箭发展的必然趋势，引入人工智能（AI）和机器学习（ML）技术，能够使系统实时学习和调整，提高自适应能力和容错能力，如何在实时操作环境中实现快速响应和准确预测，以及如何处理大量实时数据是当前的挑战之一。最后，尽管国际上越来越多的合作项目，推动了发动机冗余容错技术的标准化发展，但不同国家和组织之间的技术标准和规范上的差异成为标准化发展道路上的阻力。这些技术挑战预示着未来火箭发动机故障诊断系统冗余容错技术的发展方向。

随着人工智能和机器学习技术的进一步成熟，火箭发动机的冗余容错系统将会更加智能化和自适应，能够更精确地预测和响应各种故障情况，智能化和自适应技术的应用会越来越深入地参与到系统当中。此外，未来系统会集成多源数据和数据融合技术，集成不同类型和来源的传感器数据，并应用先进的数据融合技术，提高数据的准确性和系统的整体可靠性。对于冗余系统对火箭整体重量和性能的影响，未来可能会引入轻量化和高效能材料的应用。国际标准化和合作能够进一步推动国际间的技术标准和规范的统一，促进全球范围内的技术交流和合作，积累相关领域技术人才，共同推动火箭发动机故障诊断系统冗余容错技术的进步。

6 结束语

液体火箭发动机故障诊断系统要求其具备较高的可靠性及冗余度，冗余技术的研究可以帮助检测并诊断系统的故障，从而及时发现问题并采取措施以防止故障进一步扩大，达到缩小损失并降低事故风险的目的。未来，冗余容错技术在火箭发动机故障诊断系统中的应用预计将朝着智能化、集

成化和自动化方向发展。这包括发展先进的智能传感技术，实现健康监测与故障诊断技术的深度融合，以及推进任务重构与控制重构技术的进步。该技术对于支持未来的深空探索任务也至关重要，确保了在极端环境下的成功率和成本效益。总之，冗余容错技术是实现火箭可重复使用、降低发射成本、并推动航天技术向前发展的关键因素。

参考文献

[1] BAO W M，WANG X G. Develop highly reliable and low-cost technology for access to space，embrace the new space economy era [J]. Aerospace China，2019，20 (4)：23－30.

[2] 包为民，汪小卫. 航班化航天运输系统发展展望 [J]. 宇航总体技术，2021，5 (3)：1－6.

[3] 张振臻，陈　晖，高玉闪，等. 液体火箭发动机故障诊断技术综述 [J]. 推进技术，2022，43 (6)：20－38.

[4] 包为民. 可重复使用运载火箭技术发展综述 [J]. 航空学报，2023，44 (23)：8－33.

[5] 郭　林. 基于 FPGA 的星载机容错技术研究与设计 [D]. 北京：清华大学，2009.

[6] 袁由光，陈以农. 容错与避错技术及其应用 [M]. 北京：科学出版社，1992.

[7] 李洪超. 计算机系统的容错技术方法 [J]. 单片机与嵌入式系统应用，2010 (11)：19－21.

[8] 党崇伦. 基于 FPGA 的关节伺服控制器容错技术研究 [D]. 北京：北京邮电大学，2008.

[9] 胡华平，金士尧，王　维. 分布式实时系统的高可靠性研究与实现 [J]. 计算机研究与发展，1998 (9)：74－78.

[10] 周宇杰. 基于双模冗余的立方星高可靠星载计算机设计 [D]. 南京：南京理工大学，2016.

[11] 楼智翔，张　吉. 双机冷备计算机信号切换的设计与实现 [J]. 电子技术，2011，38 (2)：20－21.

[12] 贾文涛，张春元，付　剑，等. 一种高可靠双机温备星载计算机的设计与实现 [J]. 计算机研究与发展，2010，47 (s1)：127－132.

[13] 黄　影，张春元，刘　东. SRAM 型 FPGA 的抗 SEU 方法研究 [J]. 中国空间科学技术，2007 (4)：57－65.

[14] 付　剑. 星载计算机的硬件容错设计与可靠性分析 [D]. 长沙：国防科学技术大学，2009.

[15] 李　毅，李　瑞，黄　影，等. 基于 COTS 的空间信息处理系统单粒子闭锁保护技术实现 [J]. 宇航学报，2007 (5)：1283－1287.

[16] 贾文涛. 高可靠星载双机备份系统的设计与评估 [D]. 长沙：国防科学技术大学，2010.

[17] 殷杰波，张书滨. 1553B 总线控制器双机热备份设计 [J]. 现代电子技术，2010，33 (7)：39－40.

[18] 罗贵舟，王锦杰，杨旭斌，等. 一种多策略双机热备方法 [J]. 计算机测量与控制，2019，27 (3)：231－234.

[19] 马丽娜. 双通道冗余智能伺服控制器的研究与设计 [D]. 西安：西安工程大学，2015.

[20] 童天成. 全三模冗余星载计算机系统设计与实现 [D]. 上海：东华大学，2015.

[21] 诸　磊. 基于 VPX 的双模冗余计算机的设计与实现 [D]. 北京：中国航天科技集团公司第一研究院，2018.

[22] ZHU L，YU L. A design of decentralized dual mode redundant hot standby arbitration switch-over logic and architecture [C] //2018 International Conference on Electronics Technology (ICET). Beijing Microelectronics Technology Institute，Beijing Microelectronics Technology Institute，Beijing，China，2018.

[23] 陈玉坤，张声艳，刘　冬，等. 双模冗余器载计算机设计与实现 [J]. 计算机测量与控制，2016，24 (12)：130－132.

[24] KAHE G. Reliable flight computer for sounding rocket with dual redundancy：design and implementation based on COTS parts [J]. International Journal of System Assurance Engineering and Management，2017，8 (3)：560－571.

[25] SAMET R. Design and implementation of highly reliable dual-computer systems [J]. Computers & Security，2009，28 (7)：710－722.

[26] 铁玉峰，吉小军，吴建铭，等. 基于 FPGA1553B 的星载数据采集系统设计 [J]. 宇航计测技术，2021，41 (3)：79－85.

[27] 熊庭刚，马　中，袁由光. 基于操作系统调用的容错计算机系统同步技术研究 [J]. 计算机研究与发展，2006 (11)：1985－1992.

[28] 安占新，许传明，王晓玲. 多模异构冗余软件系统同步技术研究 [J]. 航天控制，2019，37 (5)：46－50.

[29] 沈　雳，郑璧青，叶　恒，等. 高可靠飞行器计算机系统设计 [J]. 数字技术与应用，2019，37 (4)：158－159.

[30] ANJANKAR S C，KOLTE M T，PUND A，et al. FPGA Based multiple fault tolerant and recoverable technique using triple modular redundancy (FRTMR) [J]. Procedia Computer Science，2016，79：827－834.

[31] AGUIAR Y Q，WROBEL F，AUTRAN J L，et al. Design exploration of majority voter architectures based on the signal probability for TMR strategy optimization in space applications [J]. Microelectronics Reliability，2020，114 (11)：1－6.

[32] 朱明俊. 立方星星载计算机系统容错技术研究 [D]. 南京：南京理工大学，2016.

[33] 王新志. 微小卫星星务计算机智能容错与冗余系统研究 [D]. 南京：南京理工大学，2021.

[34] 梁立柱. 箭用 1553B 总线控制器双冗余方案研究 [D]. 上海：上海交通大学，2012.

[35] 满梦华，原　亮，丁国良，等. 嵌入式高可靠性异构双机冗余系统的设计 [J]. 计算机应用，2009，29 (8)：2143－2145.

[36] 陆　阳，张本宏，魏　臻，等. “二乘二取二”和“双模冗余-比较”结构对比研究 [J]. 电子测量与仪器学报，2009，23 (3)：15－22.

[37] 李利军. 星载双机热备份计算机系统设计 [D]. 西安：西安电子科技大学，2010.

[38] 刘慕霄，刘宪忠，赵昶宇. 嵌入式系统双机热备技术研究 [J]. 科技与创新，2022 (6)：119－121.

[39] 徐美荣. 基于实时操作系统的多机冗余、容错技术研究 [D]. 杭州：浙江大学，2006.