文章编号:1671-4598(2021)02-0194-08 DOI:10.16526/j.cnki.11—4762/tp.2021.02.038 中图分类号:TP302.8 文献标识码:A

基于 COTS 的宇航计算单元冗余架构可靠性研究

雷华舟[1,2,3]，钟 杰[1,2]，吕升林[4]
(1. 中国科学院 空间光电精密测量技术重点实验室，成都 610209；
2. 中国科学院 光电技术研究所，成都 610209；3. 中国科学院大学 计算机科学与技术学院，北京 100049；
4. 中国人民解放军 空军装备部驻成都地区第五军事代表室，成都 610209)

摘要：随着商业航天的发展，为了能以更低成本使宇航计算单元得到应用，需要结合设计成本、预期寿命、实时性和系统复杂度等因素，对不同计算单元冗余架构的可靠性进行评估；目前在基于高性能商用货架（COTS，commercial off—the—shelf）器件的宇航计算单元研究多满足于工程应用，缺乏关于对不同架构可靠性的对比；首先，针对几种不同冗余计算单元冗余架构，简单介绍具体的拓扑结构和工作方式；其次，根据工作方式给出了他们的故障状态转移图；最后，根据上述几种架构，运用马尔可夫模型理论，对这些计算单元结构进行可靠性建模，在考虑失效率和维修率两个参数对系统可靠性影响的情况下，并以一个虚拟的长时期任务为背景对各结构的可靠性指标进行了评价；仿真结果为更低成本基于 COTS 器件制造宇航计算单元提供了设计支撑。

关键词：COTS 器件；马尔可夫模型；宇航计算单元；冗余架构；可靠性分析

Research on Reliability of Redundant Architecture of Based on COTS Device Space Computing Unit

Lei Huazhou[1,2,3], Zhong Jie[1,2], Lü Shenglin[4]
(1. Key Laboratory of Science and Technology on Space Optoelectronic Precision Measurement, CAS, Chengdu 610209, China;
2. Institute of Optics and Electronics, Chinese Academy of Sciences, Chengdu 610209, China;
3. School of Computer Science and Technology University of Chinese Academy of Sciences, Beijing 100049, China;
4. Fifth Military Representative Room, Air Force Equipment Department in Chengdu, PLA, Chengdu 610209, China)

Abstract: With the development of commercial aerospace, in order to apply space computing units at lower cost, it is necessary to evaluate the reliability of redundant architectures of different computing units in combination with design cost, life expectancy, real—time performance and system complexity. At present, the research on aerospace computing units based on high—performance commercial off the shelf (COTS) devices is mostly satisfied with engineering applications, and there is no comparison on reliability of different architectures. First of all, it introduces the specific topology structure and working mode of several redundant computing units. Second, it gives their fault state transition diagram according to the working mode. Third, according to the above—mentioned architectures, it uses Markov model theory to model the reliability of these computing unit structures, considering the failure rate and maintenance rate under the influence of parameters on the system reliability, the reliability indexes of each structure are evaluated against the background of a virtual long—term task. The simulation results provide the design support for the lower cost Aerospace computing unit based on COTS devices.

Keywords: COTS (commercial off—the—shelf) device; Markov model; spatial computing unit; redundant architecture; reliability analysis

0 引言

近年来，由于商业需求在航天领域的不断发展，商业载荷需求呈现爆发式增加。传统的以科技载荷为需求的 3～5 年的载荷研制周期不能满足商业航天的业务需求，而且航天级器件一般因为供货周期长，价格昂贵而且性能往往落后于地面上的同级别器件的原因，所以采用高性能商业级现货器件代替传统航天级器件作为商业航天公司在成本控制领域发展的一个方向。在宇航应用中，计算单元能否长时间地稳定、可靠工作对于目标任务的实现具有关键作用，由于高性能商业级器件不是为了宇航应用而生产，所以为了提升其在宇航应用中的可靠性，利用适当的容错策略和冗余设计，使其达到所需的设计目标。[1]随着计算技术的发展，在冗余设计上有传统采用静态的热备、冷备的方式[2-3]，也有较新的基于动态重构的方式[4-5]，不同的设计和策略因为应用场景不同各有特点。因此各种冗余设计的可靠性是一个值得研究的重要问题。

收稿日期:2020-07-03； **修回日期**:2020-07-29。
作者简介:雷华舟(1994-)，男，贵州人，硕士研究生，主要从事检测技术与自动化装置方向的研究。
引用格式:雷华舟，钟 杰，吕升林. 基于 COTS 的宇航计算单元冗余架构可靠性研究[J]. 计算机测量与控制，2021，29(2)：194-201.

目前针对冗余设计可靠性主要研究指向单一项目前对宇航电子设备进行设计前的预估，判断宇航电子设备是否能够满足系统的可靠性设计，为系统方案提供必要的技术支撑[6-7]。另外，从理论角度采用新的理论进行新的可靠性模型搭建和软硬件容错策略设计也是学者们研究的另一方向[8-9]。为了更低成本的商业化应用，部分学者尝试将方向引向商业设计上计算单元架构可靠性相互间比较研究[10]。

综上所述，以往的研究主要集中为单一项目提供技术支撑和新可靠模型的搭建，对于架构可靠性比较研究较少。本文在冗余设计可靠性理论基础上，用马尔可夫链模型数值分析计算方法，考虑计算单元的仲裁切换模块，针对商业航天任务周期时长的背景，对几种冗余设计架构可靠性进行仿真、比较分析，为商业航天载荷的设计提供参考。

1　计算单元容错设计结构

常见的基于 COTS 器件宇航计算单元一般采用“计算核心＋FPGA”的异构组合，近年来也出现了基于大容量 FPGA 构成的可重构计算单元[4,11-12]。对于常见的异构组合需要考虑其仲裁切换模块的可靠性，而对于基于 FPGA 构成的计算单元还需要考虑由其系统的最大特点是可以通过重新配置，进行系统的重构，通过可重构机制使得系统得以修复。

由于具有可修复能力的电子设备进行可靠性分析时过程相对比较复杂。本文以动态重构三模冗余作为可修复设备的代表进行可靠性分析。主要针对比较常用的双机冷备、双机热备、三模冗余以及两热一冷这几种冗余结构计算单元的可靠性进行分析。

1.1　双机冷备结构

双机冷备份结构设计原理如图 1 所示，正常状态下采用的主节点上电，备节点不上电。双机冷备份结构在仲裁切换模块正常，没有发生故障时，主节点正常工作进行运算处理，计算单元内的备节点不会发生故障；当主节点发生故障时，激活备节点，对主节点进行替换；当备节点也发生故障时，系统失效。当仲裁切换节点发生故障时，主节点正常工作，备节点不会发生故障；当主节点故障时，由于仲裁切换模块发生故障无法切换，系统失效。

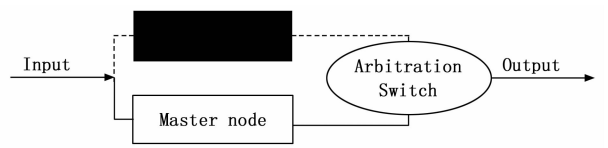


图 1　双机冷备份重组结构拓扑图

1.2　双机热备结构

双机热备份重构设计原理如图 2 所示，采用的双机热备份，热备份与冷备份不同在于正常情况下，计算单元内的备节点也有可能发生故障。双机热备份在仲裁切换模块正常，主节点正常工作时，计算单元工作正常；当备节点也发生故障时，系统失效。当仲裁切换节点发生故障时，主节点正常工作，备节点发生故障，系统正常工作；当主节点故障时，由于仲裁切换模块发生故障无法切换，系统失效。

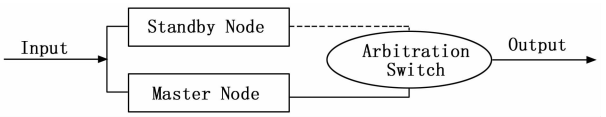


图 2　双机热备份重组结构拓扑图

1.3　三模表决冗余结构

常规三模表决设计原理如图 3 所示，采用的三模表决，正常状态下 3 个节点均正常工作对输入信号进行运算，仲裁切换模块表决，系统正常输出；当其中 1 个节点发生故障，另 2 个节点正常工作时，仲裁切换节点将会屏蔽故障节点的影响；当出现 2 个节点及以上节点发生故障时，系统失效。当仲裁切换节点出现故障时，由于无法进行仲裁或者仲裁出错，系统失效。

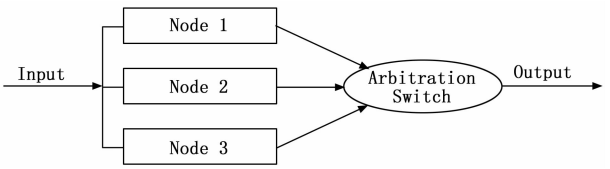


图 3　三模表决冗余结构拓扑图

1.4　三模冗余重组结构

三模冗余重组结构设计一般应用在大容量可重构 FPGA 上，其结构如图 4 所示，采用的三模表决的仲裁策略，正常状态下 3 个节点均正常工作，系统正常输出；当其中 1 个节点发生故障，另 2 个节点正常工作时，仲裁切换节点屏蔽故障节点的影响，系统通过内嵌的故障诊断、识别，然后进行故障清理等手段让故障节点恢复正常，在不影响计算单元工作的情况下，将其接入系统，恢复到三模表决的工作状态；当出现 2 个节点及以上节点发生故障时，系统失效。当仲裁切换节点出现故障时，由于无法进行仲裁或者仲裁出错，系统失效。

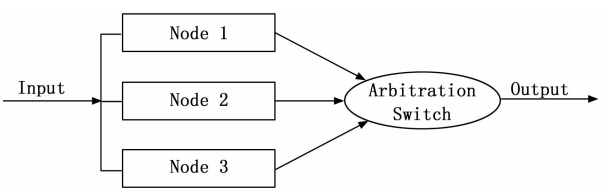


图 4　三模冗余重组结构拓扑图

1.5　两热一冷冗余结构

两热一冷冗余结构设计原理如图 5 所示，采用 1 个双节点热备加一个节点冷备的节点架构，正常状态下两个热节点均正常工作，系统正常输出；当其中 1 个热节点发生故障，仲裁切换节点激活冷节点，与正常节点重新构成双节点热备。

考虑仲裁切换节点出现故障的时间，其工作状态分为：首先仲裁切换节点出现故障，当其中 1 个热节点发生故障，系统只能以单节点状态工作；其中 1 个热节点首先发生故

障，之后仲裁切换节点出现故障，系统以双节点热备状态工作。

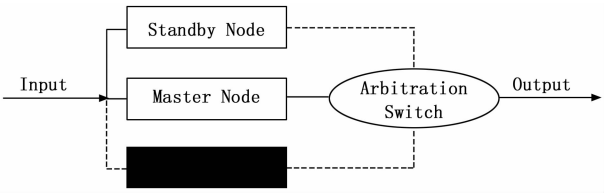


图 5 两热一冷冗余结构拓扑图

2 系统设计结构工作状态

由于计算单元的容错设计结构不一致，其在工作时遭受故障时的工作状态会产生变化以保证系统的正常运行，针对计算单元不同的工作状态，采用马尔科夫随机过程对其可靠性进行建模，考虑到不同单元失效率 λ_C、λ_{AW} 和维修率 μ_C，对不同结构计算单元的可靠性指标进行评价。

2.1 双机冷备结构工作状态

由图 1 所示的双机冷备结构，正常状态 S_{11}，没有故障节点，主节点当班；当主节点发生故障，由状态 S_{11} 变为状态 S_{12}，备节点被激活，作为当班节点；当仲裁切换节点发生故障，由状态 S_{11} 变为状态 S_{13}，主节点仍作为当班节点工作。当主节点、仲裁切换节点发生故障，由状态 S_{12} 变为状态 S_{14}，备节点被激活，作为当班节点；当主节点、备节点发生故障，由状态 S_{12} 变为状态 S_{16}，系统失效。当仲裁切换节点、主节点发生故障，由状态 S_{13} 变为状态 S_{15}，系统失效。当所有节点故障，变为状态 S_{17}，系统失效。其工作状态如表 1 所示。

表 1 双机冷备份重组结构工作状态表

工作状态	故障节点	当班节点	系统情况
S_{11}	无	主节点	正常
S_{12}	主节点	备节点	正常
S_{13}	仲裁切换节点	主节点	正常
S_{14}	主节点、仲裁切换节点	备节点	正常
S_{15}	仲裁切换节点、主节点	无	失效
S_{16}	主节点、备节点	无	失效
S_{17}	主节点、仲裁切换节点、备节点	无	失效

考虑状态 S_{15}、S_{16}、S_{17} 都为失效状态，其中 S_{15}、S_{17} 为马尔科夫随机过程中的吸收态，将 S_{16}、S_{17} 状态作为同状态，S'_{15} 有系统状态转移如图 6 所示。

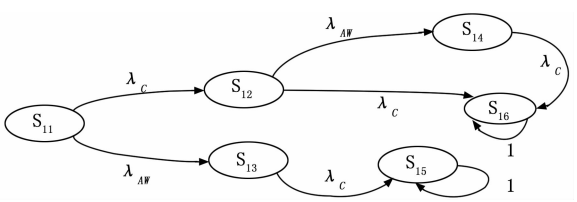


图 6 双机冷备结构系统状态转移图

2.2 双机热备结构工作状态

由图 2 所示的双机热备结构，正常状态 S_{21}，没有故障节点，主节点当班；当主节点或者备节点发生故障，由状态 S_{21} 变为状态 S_{22}，另一节点被激活，作为当班节点；当仲裁切换节点发生故障，由状态 S_{21} 变为状态 S_{23}，主节点仍作为当班节点工作。当主节点、仲裁切换节点或者备节点、仲裁切换节点发生故障，由状态 S_{22} 变为状态 S_{24}，另一节点被激活，作为当班节点。当仲裁切换节点、备节点发生故障，由状态 S_{23} 变为状态 S_{24}，主节点仍作为当班节点工作；当仲裁切换节点、主节点发生故障，由状态 S_{23} 变为状态 S_{25}，系统失效。当主节点、备节点发生故障，由状态 S_{22} 变为状态 S_{26}，无当班节点，系统失效；当所有节点故障，变为状态 S_{27}，系统失效。其工作状态如表 2 所示。

表 2 双机热备份重组结构工作状态表

工作状态	故障节点	当班节点	系统情况
S_{21}	无	主节点	正常
S_{22}	主节点	备节点	正常
	备节点	主节点	
S_{23}	仲裁切换节点	主节点	正常
S_{24}	仲裁切换节点、备节点	主节点	正常
	备节点、仲裁切换节点	主节点	
	主节点、仲裁切换节点	备节点	
S_{25}	仲裁切换节点、主节点	无	失效
S_{26}	主节点、备节点	无	失效
S_{27}	双节点、仲裁切换节点	无	失效

考虑状态 S_{25}、S_{26}、S_{27} 都为失效状态，其中 S_{27} 为马尔科夫随机过程中的吸收态，将 S_{25}、S_{26}、S_{27} 状态作为同状态 S'_{25}，有系统状态转移如图 7 所示。

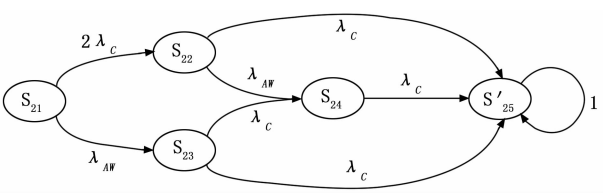


图 7 双机冷备结构系统状态转移图

2.3 三模表决冗余结构工作状态

由图 3 所示的三模表决冗余结构，正常状态 S_{31}，没有故障节点，仲裁节点 3/3 仲裁。当某计算节点发生故障，由状态 S_{31} 变为状态 S_{32}，仲裁节点 2/3 仲裁；当仲裁切换节点发生故障，由状态 S_{31} 变为状态 S_{35}，系统失效。当某计算节点再次发生故障，由状态 S_{32} 变为状态 S_{33}，仲裁节点 1/3 仲裁，系统失效；当某计算节点，仲裁切换节点发生故障，由状态 S_{32} 变为状态 S_{36}，系统失效。当仲裁切换节点、某计算节点发生故障，由状态 S_{35} 变为状态 S_{36}，系统失效。当所有计算节点发生故障，由状态 S_{33} 变为状态 S_{34}，系统失效；当某两计算节点、仲裁切换节点发生故障，由状态 S_{33} 变为状态 S_{37}，系统失效。当仲裁切换节点、某两计算节点发生故障，由状态 S_{36} 变为状态 S_{37}，系统失效。当所有节点发生故障，变为状态 S_{38}，系统失效。其工作状态如表 3 所示。

表 3　三模表决冗余结构工作状态表

工作状态	故障节点	仲裁情况	系统情况
S_{31}	无	3/3 仲裁	正常
S_{32}	节点 1/2/3	2/3 仲裁	正常
S_{33}	节点 1、节点 2	1/3 仲裁	失效
	节点 2、节点 3		
	节点 1、节点 3		
S_{34}	节点 1、节点 2、节点 3	0/3 仲裁	失效
S_{35}	仲裁切换节点	/	失效
S_{36}	仲裁切换节点、节点 1/2/3	/	失效
S_{37}	仲裁切换节点、节点 1、2	/	失效
	仲裁切换节点、节点 2、3		
	仲裁切换节点、节点 1、3		
S_{38}	所有节点	/	失效

考虑状态 S_{33}、S_{34}、S_{35}、S_{36}、S_{37}、S_{38} 都为失效状态，将 S_{33}、S_{34}、S_{35}、S_{36}、S_{37}、S_{38} 状态作为同状态 S'_{38}，有系统状态转移如图 8 所示。

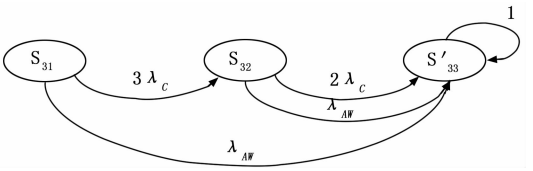


图 8　三模表决冗余结构系统状态转移图

2.4　三模冗余重组结构工作状态

由图 4 所示的三模表决冗余结构，工作模式与三模表决冗余结构基本一致，主要区别在于当某一计算单元出现故障之后，将以某一修复率对该计算单元进行修复，其工作状态如表 4 所示。

表 4　三模冗余重组结构工作状态表

工作状态	故障节点	仲裁情况	系统情况
S_{41}	无	3/3 仲裁	正常
S_{42}	节点 1/2/3	2/3 仲裁	正常
S_{43}	节点 1、节点 2	1/3 仲裁	失效
	节点 2、节点 3		
	节点 1、节点 3		
S_{44}	节点 1、节点 2、节点 3	0/3 仲裁	失效
S_{45}	仲裁切换节点	/	失效
S_{46}	仲裁切换节点、节点 1/2/3	/	失效
S_{47}	仲裁切换节点、节点 1、2	/	失效
	仲裁切换节点、节点 2、3		
	仲裁切换节点、节点 1、3		
S_{48}	所有节点	/	失效

由于需要考虑 S_{43}、S_{44} 状态的修复率，将两状态作为单独态。考虑状态 S_{45}、S_{46}、S_{47}、S_{48} 都为失效状态，将 S_{45}、S_{46}、S_{47}、S_{48} 状态作为同状态 S'_{45}，有系统状态转移如图 9 所示。

2.5　两热一冷冗余结构工作状态

由图 5 所示的两热一冷冗余结构，正常状态 S_{51}，没有故障节点，由主节点与备节点 1 构成双机热备结构，主节点当班。当主节点或者备节点 1 发生故障，启动备节点 2，组成新的双机热备结构，由状态 S_{51} 变为状态 S_{52}。当任意两个计算节点发生故障，转化为单机系统，由状态 S_{52} 变为状态 S_{53}；当一个计算节点和仲裁切换节点先后发生故障，由状态 S_{52} 变为状态 S_{54}。当仲裁切换节点和备节点 1 先后发生故障，主节点仍做当班机，系统正常，由状态 S_{51} 变为状态 S_{55}；当仲裁切换节点和主节点先后发生故障，仲裁切换失效，系统失效，由状态 S_{51} 变为状态 S_{56}。当仲裁切换节点、主节点、备节点 1 先后发生故障，系统失效，由状态 S_{55}、S_{56} 变为状态 S_{59}。当任意两计算节点故障后，仲裁切换节点失效，系统由状态 S_{53} 变为状态 S_{57}、S_{58}；当所有的 3 个计算节点故障后，系统由状态 S_{53} 变为状态 S_{5a}。当某计算节点和仲裁切换节点故障后，降为双机系统，此时如非当班节点发生故障，则系统工作正常，系统由状态 S_{54} 变为状态 S_{58}；此时如当班节点发生故障，则系统工作失效，系统由状态 S_{54} 变为状态 S_{5b}。当所有节点发生故障，变为状态 S_{5c}，系统失效。其工作状态如表 5 所示。

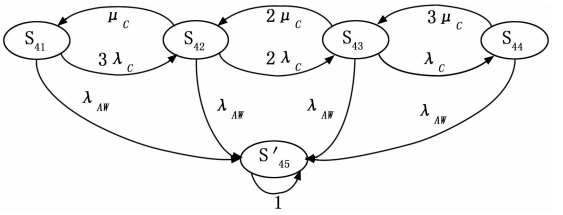


图 9　三模冗余重组结构系统状态转移图

表 5　两热一冷冗余结构工作状态表

工作状态	故障节点	当班节点	系统情况
S_{51}	无	主节点	正常
S_{52}	主节点	备节点 1	正常
	备节点 1	主节点	
S_{53}	主节点、备节点 1	备节点 2	正常
	主节点、备节点 2	备节点 1	
	备节点 1、备节点 2	主节点	
S_{54}	主节点、仲裁切换节点	备节点 1	正常
	备节点 1、仲裁切换节点	主节点	
S_{55}	仲裁切换节点、备节点 1	主节点	正常
S_{56}	仲裁切换节点、主节点	无	失效
S_{57}	主节点、仲裁切换节点、备节点 1	备节点 2	正常
S_{58}	备节点 1、仲裁切换节点、备节点 2	主节点	正常
	主节点、仲裁切换节点、备节点 2	备节点 1	
S_{59}	仲裁切换节点、备节点 1、主节点	无	失效
S_{5a}	主节点、备节点 1、备节点 2	无	失效
S_{5b}	备节点 1、仲裁切换节点、主节点	无	失效
	主节点、仲裁切换节点、备节点 1		
S_{5c}	所有节点	无	失效

考虑状态 S_{56}、S_{59} 和 S_{5a}、S_{5b}、S_{5c} 都为失效状态，S_{59}、S_{5c} 状态为系统的吸收态，将 S_{56}、S_{59} 和 S_{5a}、S_{5b}、S_{5c} 状态作为同状态 S'_{56} 和 S_{5abc}，有系统状态转移如图 10 所示。

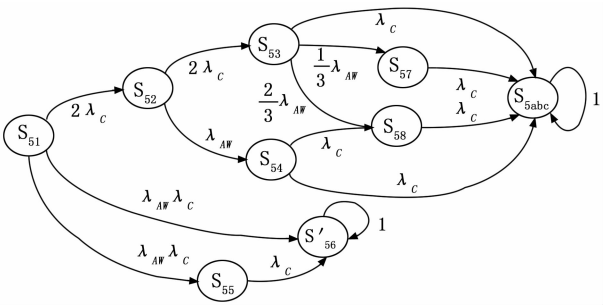


图 10 两热一冷冗余结构系统状态转移图

3 可靠性模型分析及计算

在研究系统的可靠性之前，首先对系统做如下假设：

1）假设系统中除了处理器模块和表决切换单元外，其他系统的可靠度均为 1；

2）每个计算核心模块的失效率为 λ_C，维修率为 μ_C，表决切换单元的失效率为 λ_{AW}，同时假设失效分布和维修时间分布为指数分布；

3）某一时刻只有一个模块发生故障；

4）系统开始工作时，各单元都为无故障状态，系统整体处于完好状态。

基于以上假设，对各结构的可靠性进行研究。

3.1 双机冷备结构

根据图 6，其马尔克夫状态可做以下的数学描述：时刻 $t+\Delta t$ 结构状态的条件概率与 t 时刻结构状态由全概率公式得到，考虑当 $\Delta t\to 0$ 时，得到如下状态微分方程组：

$$\begin{cases}\dfrac{dP_{S_{11}}(t)}{dt}=-(\lambda_C+\lambda_{AW})P_{S_{11}}(t)\\ \dfrac{dP_{S_{12}}(t)}{dt}=-(\lambda_C+\lambda_{AW})P_{S_{12}}(t)+\lambda_C P_{S_{11}}(t)\\ \dfrac{dP_{S_{13}}(t)}{dt}=-\lambda_C P_{S_{13}}(t)+\lambda_{AW}P_{S_{11}}(t)\\ \dfrac{dP_{S_{14}}(t)}{dt}=-\lambda_C P_{S_{14}}(t)+\lambda_{AW}P_{S_{12}}(t)\\ \dfrac{dP_{S_{15}}(t)}{dt}=-\lambda_C P_{S_{13}}(t)\\ \dfrac{dP_{S'_{16}}(t)}{dt}=\lambda_C P_{S_{14}}(t)+\lambda_C\lambda_{AW}P_{S_{12}}(t)\end{cases}\tag{1}$$

考虑系统的约束条件：

$$\sum_{i=0}^{5}P_{S_{1i}}(t)+P_{S'_{16}}(t)=1$$

初始条件：

$P_{S_{11}}(0)=1$，

$P_{S_{12}}(0)=P_{S_{13}}(0)=P_{S_{14}}(0)=P_{S_{15}}(0)=P_{S'_{16}}(0)=0$

将上述方程组进行 Laplace 变换解出后，进行反 Laplace 变换可得双机冷备重组结构可信度：

$$R_1(t)=P_{S_{11}}(t)+P_{S_{12}}(t)+P_{S_{13}}(t)+P_{S_{14}}(t)\tag{2}$$

3.2 双机热备结构

根据图 7 双机热备结构的状态转移图，其马尔克夫状态可做以下的数学描述：时刻 $t+\Delta t$ 结构状态的条件概率与 t 时刻结构状态由全概率公式得到，考虑 $\Delta t\to 0$ 当时，得到如下状态微分方程组：

$$\begin{cases}\dfrac{dP_{S_{21}}(t)}{dt}=-(2\lambda_C+\lambda_{AW})P_{S_{21}}(t)\\ \dfrac{dP_{S_{22}}(t)}{dt}=-(\lambda_C+\lambda_{AW})P_{S_{22}}(t)+2\lambda_C P_{S_{21}}(t)\\ \dfrac{dP_{S_{23}}(t)}{dt}=-2\lambda_C P_{S_{23}}(t)+\lambda_{AW}P_{S_{21}}(t)\\ \dfrac{dP_{S_{24}}(t)}{dt}=-\lambda_C P_{S_{24}}(t)+\lambda_{AW}P_{S_{22}}+\lambda_C P_{S_{23}}(t)\\ \dfrac{dP_{S'_{25}}(t)}{dt}=\lambda_C P_{S_{22}}(t)+\lambda_C P_{S_{24}}(t)+\lambda_C P_{S_{23}}(t)\end{cases}\tag{3}$$

考虑系统的约束条件：

$$\sum_{i=0}^{4}P_{S_{2i}}(t)+P_{S'_{25}}(t)=1$$

初始条件：

$P_{S_{21}}(0)=1$，$P_{S_{22}}(0)=P_{S_{23}}(0)=P_{S_{24}}(0)=P_{S'_{25}}(0)=0$

将上述方程组进行 Laplace 变换解出后，进行反 Laplace 变换可得双机热备重组结构可信度：

$$R_2(t)=P_{S_{21}}(t)+P_{S_{22}}(t)+P_{S_{23}}(t)+P_{S_{24}}(t)\tag{4}$$

3.3 三模表决冗余结构

根据图 8，其马尔克夫状态可做以下的数学描述：时刻 $t+\Delta t$ 结构状态的条件概率与时刻 t 结构状态由全概率公式得到，考虑当 $\Delta t\to 0$ 时，得到如下状态微分方程组：

$$\begin{cases}\dfrac{dP_{S_{31}}(t)}{dt}=-(3\lambda_C+\lambda_{AW})P_{S_{31}}(t)\\ \dfrac{dP_{S_{32}}(t)}{dt}=-(2\lambda_C+\lambda_{AW})P_{S_{32}}(t)+3\lambda_C P_{S_{31}}(t)\\ \dfrac{dP_{S'_{33}}(t)}{dt}=\lambda_{AW}P_{S_{31}}(t)+(2\lambda_C+\lambda_{AW})P_{S_{32}}(t)\end{cases}\tag{5}$$

考虑系统的约束条件：

$$P_{S_{31}}(t)+P_{S_{32}}(t)+P_{S'_{33}}(t)=1$$

初始条件：

$$P_{S_{31}}(0)=1,\ P_{S_{32}}(0)=P_{S'_{33}}(0)=0$$

将上述方程组进行 Laplace 变换解出后，进行反 Laplace 变换可得三模表决冗余结构可信度：

$$R_3(t)=P_{S_{31}}(t)+P_{S_{32}}(t)\tag{6}$$

3.4 三模冗余重组结构

根据图 9，考虑三模重组一般采用大容量 FPGA 构成的，其马尔克夫状态可做以下的数学描述：有 $\lambda_C=\lambda_{AW}$，时刻 $t+\Delta t$ 结构状态的条件概率与 t 时刻结构状态由全概率公式得到，考虑当 $\Delta t\to 0$ 时，得到如下状态微分方程组：

$$\begin{cases}\dfrac{dP_{S_{41}}(t)}{dt}=-(3\lambda_C+\lambda_{AW})P_{S_{41}}(t)+\mu_C P_{S_{42}}(t)\\ \dfrac{dP_{S_{42}}(t)}{dt}=-(2\lambda_C+\lambda_{AW}+\mu_C)P_{S_{42}}(t)+3\lambda_C P_{S_{41}}(t)+2\mu_C P_{S_{43}}(t)\\ \dfrac{dP_{S_{43}}(t)}{dt}=-(\lambda_C+\lambda_{AW}+2\mu_C)P_{S_{43}}(t)+2\lambda_C P_{S_{41}}(t)+3\mu_C P_{S_{44}}(t)\\ \dfrac{dP_{S_{44}}(t)}{dt}=-(\lambda_{AW}+3\mu_C)P_{S_{44}}(t)+\lambda_C P_{S_{43}}(t)\\ \dfrac{dP_{S'_{45}}(t)}{dt}=\lambda_{AW}(P_{S_{41}}(t)+P_{S_{42}}(t)+P_{S_{43}}(t)+P_{S_{44}}(t))\end{cases}\tag{7}$$

考虑系统的约束条件：

$$\sum_{i=0}^{4} P_{S_{4i}}(t) + P_{S'_{45}}(t) = 1$$

初始条件：

$P_{S_{41}}(0)=1$，$P_{S_{42}}(0)=P_{S_{43}}(0)=P_{S_{44}}(0)=P_{S'_{45}}(0)=0$

将上述方程组进行 Laplace 变换解出后，进行反 Laplace 变换可得三模表决冗余结构可信度：

$$R_4(t) = P_{S_{41}}(t) + P_{S_{42}}(t) \tag{8}$$

3.5　两热一冷冗余结构

根据图 10 三模冗余重组结构的状态转移图，其马尔克夫状态可做以下的数学描述：时刻 $t+\Delta t$ 结构状态的条件概率与 t 时刻结构状态由全概率公式得到，考虑当 $\Delta t \to 0$ 时，得到如下状态微分方程组：

$$\begin{cases}
\dfrac{\mathrm{d}P_{S_{51}}(t)}{\mathrm{d}t} = -(2\lambda_C + 2\lambda_C\lambda_{AW})P_{S_{51}}(t) \\
\dfrac{\mathrm{d}P_{S_{52}}(t)}{\mathrm{d}t} = -(2\lambda_C + \lambda_{AW})P_{S_{52}}(t) + 2\lambda_C P_{S_{51}}(t) \\
\dfrac{\mathrm{d}P_{S_{53}}(t)}{\mathrm{d}t} = -(\lambda_C + \lambda_{AW})P_{S_{53}}(t) + 2\lambda_C P_{S_{52}}(t) \\
\dfrac{\mathrm{d}P_{S_{54}}(t)}{\mathrm{d}t} = -2\lambda_C P_{S_{54}}(t) + \lambda_{AW} P_{S_{52}}(t) \\
\dfrac{\mathrm{d}P_{S_{55}}(t)}{\mathrm{d}t} = -\lambda_C P_{S_{55}}(t) + \lambda_{AW}\lambda_C P_{S_{51}}(t) \\
\dfrac{\mathrm{d}P_{S'_{56}}(t)}{\mathrm{d}t} = \lambda_C P_{S_{55}}(t) + \lambda_{AW}\lambda_C P_{S_{51}}(t) \\
\dfrac{\mathrm{d}P_{S_{57}}(t)}{\mathrm{d}t} = -\lambda_C P_{S_{57}}(t) + \dfrac{1}{3}\lambda_{AW} P_{S_{53}}(t) \\
\dfrac{\mathrm{d}P_{S_{58}}(t)}{\mathrm{d}t} = -\lambda_C P_{S_{58}}(t) + \lambda_C P_{S_{54}}(t) + \dfrac{2}{3}\lambda_{AW} P_{S_{53}}(t) \\
\dfrac{\mathrm{d}P_{S_{5dfc}}(t)}{\mathrm{d}t} = \lambda_C (P_{S_{53}}(t) + P_{S_{54}}(t) + P_{S_{57}}(t) + P_{S_{58}}(t)
\end{cases} \tag{9}$$

考虑系统的约束条件：

$$\sum_{i=0}^{5} P_{S_{5i}}(t) + P_{S'_{56}}(t) + P_{S'_{57}}(t) + P_{S'_{58}}(t) + P_{S_{5dfc}}(t) = 1$$

初始条件：

$P_{S_{51}}(0)=1$，$P_{S_{52}}(0)=P_{S_{53}}(0)=P_{S_{54}}(0)=P_{S_{55}}(0)=P_{S_{57}}(0)=P_{S_{58}}(0)=0$

$P_{S'_{56}}(0)=P_{S_{5dfc}}(0)=0$

将上述方程组进行 Laplace 变换解出后，进行反 Laplace 变换可得三模表决冗余结构可信度：

$$R_5(t) = P_{S_{51}}(t) + P_{S_{52}}(t) + P_{S_{53}}(t) + P_{S_{54}}(t) + P_{S_{55}}(t) + P_{S_{57}}(t) + P_{S_{58}}(t) \tag{10}$$

4　可靠度仿真及对比分析

宇航计算单元对可靠性的要求非常苛刻，在预计寿命内的可靠度不低于 0.99[13]。经过特别的处理和加固的宇航级或军品级的电子元器件，其失效率 λ 一般在 $10^{-9}\sim10^{-8}$/h 之间，目前的商用 VLSI 技术所能达到的失效率为 10^{-7}/h，但一般的商业级或工业级的电子元器件，其失效率 λ 在 $10^{-6}\sim10^{-5}$/h 之间[14]。

根据式（2）、（4）、（6）、（8）、（10）可以分析与比较失效率和修复率对不同形式系统可靠性的影响，对这 5 类结构组成的计算单元正常工作 5 年（4.38×10^4 h）的可靠度进行比较。选取计算核心失效率 $\lambda_C=10^{-6}$/h，仲裁切换单元失效率 $\lambda_{AW}=10^{-6}$/h，恢复率 $\mu_C=100\lambda_{AW}=10^{-4}$/h（恢复率主要对于三模冗余重组结构，其由大容量 FPGA 构成，故 $\lambda_{AW}=\lambda_C$，下文同理），所得曲线如图 11 所示。

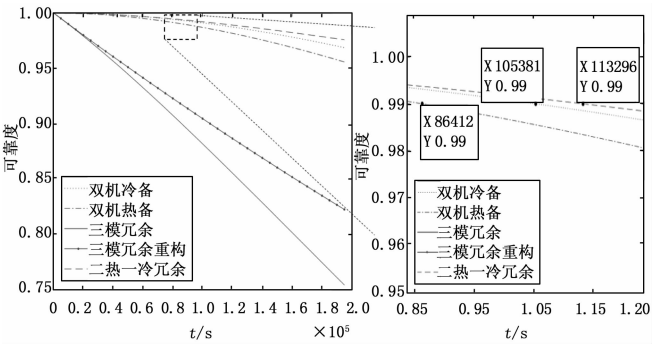


图 11　$\lambda_C=10^{-6}$/h，$\lambda_{AW}=10^{-6}$/h，$\mu_C=100\ \lambda_{AW}=10^{-4}$/h 各架构可靠度变化曲线

取计算核心失效率 $\lambda_C=10^{-5}$/h，仲裁切换单元失效率 $\lambda_{AW}=10^{-5}$/h，恢复率 $\mu_C=100\ \lambda_{AW}=10^{-3}$/h，所得曲线如图 12 所示。

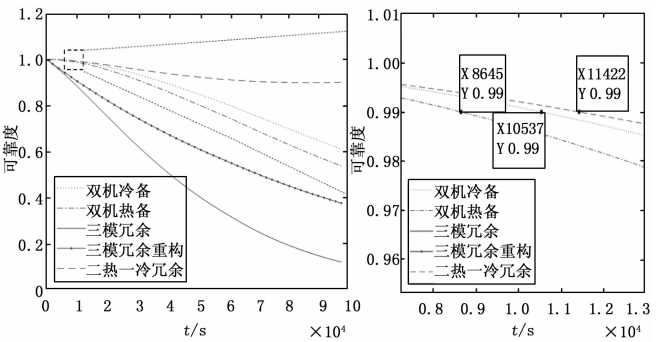
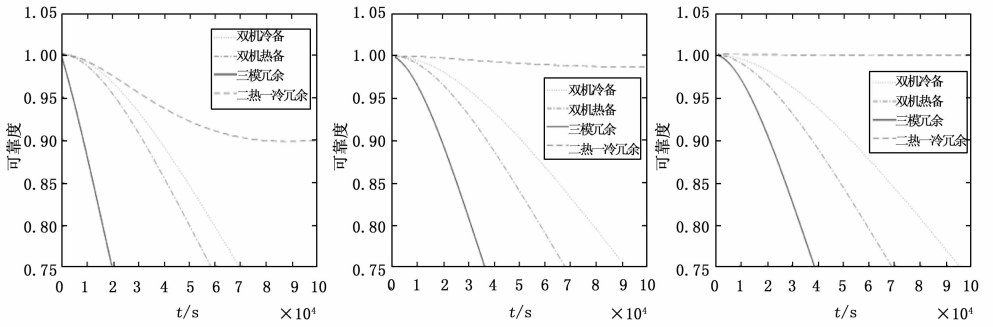


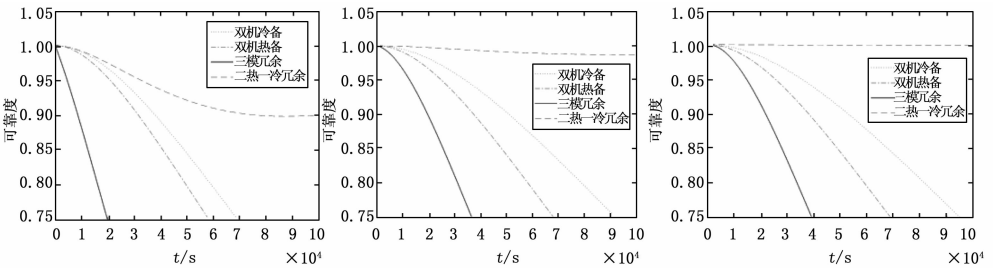
图 12　$\lambda_C=10^{-5}$/h，$\lambda_{AW}=10^{-5}$/h，$\mu_C=100\lambda_{AW}=10^{-3}$/h 各架构可靠度变化曲线

可以明显由图 12 看出，$\lambda_C=10^{-5}$/h，$\lambda_{AW}=10^{-5}$/h，失效率较大时，无论采取什么结构，系统保持可靠度不低于 0.99 的预期寿命不足 1.2×10^4 h，其中能保持可靠度不低于 0.99 最长结构为两热一冷，时间为 1.14×10^4 h，最远低于一般载荷正常工作 5 年（4.38×10^4 h）的预期寿命；而当选取的 $\lambda_C=10^{-6}$/h，$\lambda_{AW}=10^{-6}$/h，失效率较小时，双机热备、双机冷备和两热一冷结构能够保持可靠度不低于 0.99 的预期寿命超过一般载荷正常工作 5 年（4.38×10^4 h）的预期寿命，分别达到 8.6×10^4 h、10.5×10^4 h 和 11.3×10^4 h。由图 12、图 13 可明显看出三模冗余重组结构由于修复率的关系，相同工作时间内明显比一般三模冗余结构系统可靠性更高，但无论是常规的三模冗余还是三模冗余重组结构的计算单元其可靠度都极低，远不能达到一般载荷正常工作的预期寿命。



(a) $\lambda_{AW}=10^{-5}$ h^{-1} (b) $\lambda_{AW}=10^{-6}$ h^{-1} (c) $\lambda_{AW}=10^{-7}$ h^{-1}

图 13 $\lambda_C=10^{-6}$/h，不同 λ_{AW} 下各架构可靠度变化曲线（$t=2\times10^5$ h）



(a) $\lambda_{AW}=10^{-5}$ h^{-1} (b) $\lambda_{AW}=10^{-6}$ h^{-1} (c) $\lambda_{AW}=10^{-7}$ h^{-1}

图 14 $\lambda_C=10^{-5}$/h，不同 λ_{AW} 下各架构可靠度变化曲线（$t=10^5$ h）

分别选取计算核心失效率 $\lambda_C=10^{-6}$/h、$\lambda_C=10^{-5}$/h，仲裁切换单元失效率 λ_{AW} 在 $10^{-7}\sim10^{-5}$/h 下，分析和比较不同架构可靠性，所得曲线如图 13、图 14 所示。

在 $\lambda_C=10^{-6}$/h 情况下，双机冷备冗余结构可靠度不低于 0.99 的运行时间由 4.6×10^4 h 先后提升至 10.5×10^4 h、14.1×10^4 h；双机热备冗余结构可靠度不低于 0.99 的运行时间由 4.4×10^4 h 先后提升至 8.6×10^4 h、10.2×10^4 h；三模冗余结构可靠度不低于 0.99 的运行时间由 0.1×10^4 h 先后提升至 0.9×10^4 h、4.4×10^4 h；两热一冷冗余结构可靠度不低于 0.99 的运行时间由 3.4×10^4 h 先后提升至 11.1×10^4 h、51.1×10^4 h。

在 $\lambda_C=10^{-5}$/h 情况下，双机冷备冗余结构可靠度不低于 0.99 的运行时间由 1.0×10^4 h 先后提升至 1.4×10^4 h、1.4×10^4 h；双机热备冗余结构可靠度不低于 0.99 的运行时间由 0.8×10^4 h 先后提升至 1.0×10^4 h、1.0×10^4 h；三模冗余结构可靠度不低于 0.99 的运行时间由 0.1×10^4 h 先后提升至 0.4×10^4 h、0.5×10^4 h；两热一冷冗余结构可靠度不低于 0.99 的运行时间由 1.1×10^4 h 先后提升至 5.5×10^4 h、51.5×10^4 h。

如表 6 所示，相同 λ_{AW} 下，λ_C 的可靠度是决定系统可靠度的绝对因素，λ_C 的提高能大幅提高系统的可靠性。在 λ_C 不变情况下，不同冗余结构可靠度都随着 λ_{AW} 提高能有效提升系统整体的可靠性，λ_{AW} 在到达某一个值之后对系统可靠性的影响就会逐渐减弱。

表 6 不同结构不同失效率可靠度不低于 0.99 运行时间(10^4 h)

结构	$\lambda_C=10^{-5}$/h			$\lambda_C=10^{-6}$/h		
	$\lambda_{AW}=10^{-5}$	$\lambda_{AW}=10^{-6}$	$\lambda_{AW}=10^{-7}$	$\lambda_{AW}=10^{-5}$	$\lambda_{AW}=10^{-6}$	$\lambda_{AW}=10^{-7}$
双机冷备	1.0	1.4	1.4	4.6	10.5	14.1
双机热备	0.8	1.0	1.0	4.4	8.6	10.2
三模冗余	0.1	0.4	0.5	0.1	0.9	4.4
两热一冷	1.1	5.5	51.5	3.4	11.1	51.1

5 结束语

本文对 5 种典型宇航计算单元冗余架构建立了马尔可夫模型，根据可靠性理论对各架构的可靠性进行了计算、分析和比较。三模表决架构虽具有实时性强、发生一次故障系统工作不间断等优点，但从分析结果看，无论是常规三模表决架构还是动态重构的三模表决架构都不适合长时间任务。另一方面，在考虑制造成本、预期寿命、实时性和系统复杂度的不同影响的情况下，可以采取不同的冗余架构或者在计算核心和仲裁单元采用不同失效率的器件。具有双机冷备的冗余架构在制造成本占有一定优势，既能够满足较长预期寿命相对而言可靠性也能够达到要求；具有两热一冷的冗余架构在制造成本优势较小，既能够满足长时间的预期寿命和相对而言较高的可靠性要求，但结构相对复杂；具有双机热备的冗余架构在制造成本上占有一定优势，既能够满足一般的预期寿命相对而言可靠性也能够达到要求，并且在实时性上会表现较好。

参考文献：

[1] Strobel D, Czajkowski D S, Li E. Radiation hardened, high performance image processing system for new space missions [A]. AIAA Space 2009 Conference&Exposition [C]. 2009: 14-17.

[2] Gantois K, Teston F, Montenbruck, et al. Proba-2: mis-

sion and technologies overview [A]. 2006 Small satellite and system services—the 4S symposium [C]. China Laguna Sardinia, Italy: ESA, 2006: 25.
[3] Alena R, Ossenfort J, Laws K, et al. Communications for integrated modular avionics [A]. 2007 IEEE Aerospace Conference [C]. Big Sky, MT, USA: IEEE, 2007: 1-18.
[4] 李兴伟，白　博，周　军. 基于 FPGA 的立方星可重构星载处理系统研究 [J]. 计算机测量与控制，2018，26 (8)：172-176.
[5] 南京辰，谢永乐. 基于 FPGA 片上 PowerPC 实现动态重构 [J]. 电子质量，2009 (11)：5-7，20.
[6] 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.
[7] 李日和. 微纳卫星高可靠星务计算机容错系统设计 [D]. 南京：南京理工大学，2017.
[8] 秦　跌，巨新刚，卢　强，等. 一种新的基于云理论和随机过程的可靠性评估方法 [J]. 信息与控制，2012，41 (4)：454-458.
[9] 覃庆努，魏学业，黄赞武，等. 变环境变工作条件下电子系统的可靠性评价方法 [J]. 中南大学学报，2013 (8)：3254-3260.
[10] 李兴伟，白　博，周　军. 多模冗余可重构计算机可靠性研究 [J]. 计算机测量与控制，2017，25 (7)：309-312，316.
[11] 唐国斐，周海芳，谭庆平. 基于多核 DSP 的星载并行遥感图像压缩系统设计与实现 [J]. 计算机应用，2017，37 (5)：1246-1250.
[12] 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.
[13] Brown G. R. Radiation hardened PowerPC 603eTM based single board computer [A]. Proceedings of 2001 IEEE Aerospace Conference [C]. 2001: 2249-2261.
[14] Constantinescu C. Trends and challenges in VLSI circuit reliability [J]. IEEE Micro, 2003, 23 (4): 14-19.

(上接第 193 页)

测试验证，IWTWOA 算法较 WOA 算法在算法稳定性、计算精度和收敛速度上均有所提高；最后将 IWTWOA 算法应用在机器人路径规划问题中，经仿真实验证明了 IWTWOA 算法的有效性和稳定性。另外，鲸鱼优化算法还有诸多改进策略，下一步将进行深入的研究和比对；路径规划的实验环境相对简单，将对复杂环境下的路径规划进行深入的研究。

参考文献：

[1] Mirjalili S, Lewis A. The whale optimization algorithm [J]. Advances in Engineering Software, 2016, 95: 51-67.
[2] Xu T, Bai Y P, Hu H P. A whale optimization algorithm with inertia weight [J]. WSEAS Transactions on Computers, 2016, 15: 319-326.
[3] 龙　文，蔡绍洪，焦建军，等. 求解大规模优化问题的改进鲸鱼优化算法 [J]. 系统工程理论与实践，2017，37 (11)：2983-2994.
[4] Kaur G, Arora S. Chaotic whale optimization algorithm [J]. Journal of Computational Design and Engineering, 2018, 5 (3): 275-284.
[5] Zhou Y Q, Ling Y, Luo Q F. Lévy flight trajectory-based whale optimization algorithm for global optimization [J]. Engineering Computations, 2018, 35 (7): 2406-2428.
[6] 吴泽忠，宋　菲. 基于改进螺旋更新位置模型的鲸鱼优化算法 [J]. 系统工程理论与实践，2019，39 (11)：2928-2944.
[7] 肖子雅，刘　升. 精英反向黄金正弦鲸鱼算法及其工程优化研究 [J]. 电子学报，2019，47 (10)：2177-2186.
[8] Hany M, Hasanien. Performance improvement of photovoltaic power systems using an optimal control strategy based on whale optimization algorithm [J]. Electric Power Systems Research, 2018, 157: 168-176.
[9] Elham M N, Farnaz B. A multi-compartment capacitated arc routing problem with intermediate facilities for solid waste collection using hybrid adaptive large neighborhood search and whale algorithm [J]. Waste management & research: the Journal of the International Solid Wastes and Public Cleansing Association, ISWA, 2019, 37 (1): 38-47.
[10] 徐继亚，王　艳，纪志成. 基于鲸鱼算法优化 WKELM 的滚动轴承故障诊断 [J]. 系统仿真学报，2017，29 (9)：2189-2197.
[11] 谢建群，刘怡俊，李　生. 改进鲸鱼算法在云计算资源负载预测中的应用 [J]. 计算机工程与应用，2018，54 (13)：73-77，130.
[12] 杨　维，李歧强. 粒子群优化算法综述 [J]. 中国工程科学，2004 (5)：87-94.
[13] Jangir P, Trivedi I N, Jangir N, et al. A novel adaptive whale optimization algorithm for global optimization [J]. Indian J. Sci. Technol., 2016, 9 (38): 1-6.
[14] 肖人彬，王　磊. 人工免疫系统：原理、模型、分析及展望 [J]. 计算机学报，2002 (12)：2-14.
[15] 蒋新松. 机器人学导论 [M]. 沈阳：辽宁科学技术出版社，1994.
[16] 秦元庆，孙德宝，李　宁，等. 基于粒子群算法的移动机器人路径规划 [J]. 机器人，2004 (3)：222-225.
[17] 李　珣，吴丹丹，赵征凡，等. 一种改进 PSO 的室内机器人路径规划方法 [J]. 计算机测量与控制，2020，28 (3)：206-211.
[18] 朱庆保，张玉兰. 基于栅格法的机器人路径规划蚁群算法 [J]. 机器人，2005 (2)：132-136.
[19] 吴　坤，谭劭昌. 基于改进鲸鱼优化算法的无人机航路规划 [J]. 航空学报，2020，41 (s2)：724286.
[20] 宋晓茹，任怡悦，高　嵩，等. 移动机器人路径规划综述 [J]. 计算机测量与控制，2019，27 (4)：1-5，17.