

基于COTS产品的高效能空间计算技术研究

张 越, 章宇兵, 马天琦, 李 斌, 石叶楠

(中国电子科技集团公司电子科学研究院, 北京 100041)

摘 要: 针对COTS产品的空间环境适应性问题, 通过采用跨层协同的软件容错技术, 开展空间计算样机的容错加固, 设计并研制基于COTS产品的空间计算机, 通过搭载末子级火箭, 在轨开展了为期6个月的技术试验, 试验结果表明, 该方法能够提升COTS产品的空间环境适应性, 对于推动商业货架产品的航天应用具有指导意义。

关键词: 容错计算; 单粒子效应; 空间计算; 软件容错

中图分类号: TN393

文献标识码: A

doi: 10.11959/j.issn.2096-8930.20200107

Research on High Efficiency Computing Technology Based on COTS Products

ZHANG Yue, ZHANG Yubing, MA Tianqi, LI Bin, SHI Yenan

China Academy of Electronics and Information Technology, Beijing 100041, China

Abstract: Aiming at the problem of space environment adaptability of COTS products, the fault tolerance reinforcement of space computer was carried out through cross layer collaborative software fault tolerant technology. The space computer based on COTS product was designed and developed. Through carrying the last stage rocket, the on orbit technical test was carried out for six months. The test results show that the proposed method can improve the space environment adaptability of COTS products, it has guiding significance to promote the aerospace application of commercial shelf products.

Key Words: fault tolerant, single event phenomena, on-board computing, software fault tolerance

1 引言

航天电子设备往往暴露于大量宇宙射线的强辐射环境中, 包括银河宇宙射线、太阳宇宙射线、地球辐射带等。环境中充满了大量的质子、 α 粒子和重离子等高能带电粒子, 穿透能力很强, 对电子元器件危害十分突出^[1-2], 其中单粒子效应所引起的瞬态故障更是已经成为影响航天产品正常运行的主要挑战之一。

单粒子效应所引起的故障已经成为影响计算类产品在轨正常运行、可靠运行的关键问题。通过单粒子所引起的瞬时故障一般不会永久存在, 不会导致硬件物理设备的损伤, 但是会影响其运行的逻辑, 可能导致数据错误、控制逻辑错误等, 影响任务执行, 文献[3]统计表明计算机系统中80%~90%的失效都是由瞬态故障引起的。

为了消除瞬态故障的影响, 一般采用检错与纠错相结合的方法, 传统航天在面对由于空间高能粒子所带来

的单粒子问题时, 主要采用两种手段来解决: 一是通过硬件的冗余设计来提升系统的任务可靠性, 但是其带来了较大的体积、重量、功耗等问题^[4-5]; 二是通过采用宇航级元器件提升产品的空间环境适应性, 但是这类器件通常性能、功能指标都比较受限。两种思路的效费比不高。相比而言, 基于软件实现的容错技术能够通过重复执行程序来达到错误检测和恢复的目的, 从而换取高可信性和与硬件无关的快速实现, 而且软件容错技术在成本、功耗和灵活性等方面都具有优势。

2 问题概述

2.1 空间环境概述

宇宙中存在大量的银河宇宙射线、太阳宇宙射线以及地球辐射带粒子等, 这些粒子会对航天器造成影响, 有时甚至引起航天器故障, 导致任务失败。

(1) 银河宇宙射线是宇宙空间中能量较高的带电粒子，主要是质子约85%和 α 粒子约13%，能量从几个MeV到几个GeV，但通量小，约为几个粒子/cm²。

(2) 太阳宇宙射线（又称为太阳质子）主要指太阳发生耀斑时喷射出的高能带电粒子，这些粒子可在很短时间内达到很高的强度，其能量一般在10~10 000 MeV。绝大部分的太阳宇宙射线是质子，其次是 α 粒子，少量是电子。能量大于2 MeV的太阳质子全部进入同步轨道。

(3) 地球辐射带是指在近地空间被地磁场俘获的高强度带电粒子区域，主要由电子、质子以及少量的重离子组成。

不同轨道情况下主要空间环境因素对航天器的影响见表1。

2.2 单粒子效应

单粒子效应的分类如图1所示。

目前，人们已经发现了多种单粒子效应。这些单粒子效应按其器件产生的影响不同大致可以划分为以下两类。

(1) 单粒子硬错误效应（Hard Error）。单粒子硬错误是不可恢复性错误，例如：单粒子门锁效应，如果不采取措施控制，单粒子门锁会烧坏芯片，使芯片不能工作。

(2) 单粒子软错误效应（Soft Error）。单粒子软错误是可恢复性错误，例如单粒子翻转效应仅改变了内部存储单位的状态，可以通过对电路进行复位，让芯片正常工作。

常见单粒子效应的定义见表2。

表1 主要空间环境因素对航天器的影响

对比项	低轨道 (10 ² ~10 ³ km)	中轨道 (10 ³ ~10 ⁴ km)	地球同步轨道 (36 000 km)	行星际飞行轨道
中性大气	阻力对轨道影响严重，原子氧对表面腐蚀严重	没有影响	没有影响	没有影响
等离子体	影响通信，电源泄漏	影响微弱	航天器表面充电问题严重	影响微弱
高能带电粒子	辐射带南大西洋异常区和高纬地区宇宙线诱发单粒子事件，辐射带电子造成总剂量效应	辐射带和宇宙线的总剂量效应和单粒子效应严重	辐射带和宇宙线的总剂量效应和单粒子效应严重	辐射带和宇宙线的总剂量效应和单粒子效应严重
地球磁场	磁力矩对航天器姿态影响严重，磁场可作为姿态测量参考系	磁力矩对航天器姿态有影响	影响微弱	没有影响
太阳电磁辐射	对表面材料性能有影响	对表面材料性能有影响	对表面材料性能有影响	对表面材料性能有影响
地球大气辐射	对航天器辐射收支有影响	影响微弱	没有影响	没有影响
流星体	有低碰撞概率	有低碰撞概率	有低碰撞概率	有低碰撞概率

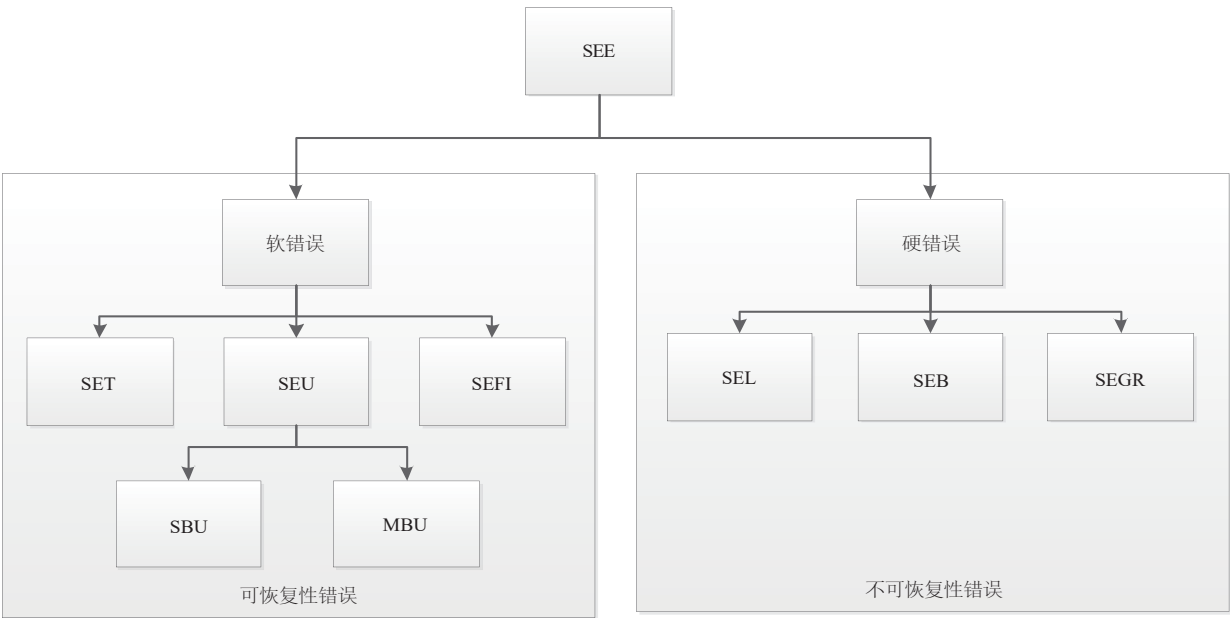


图1 单粒子效应分类

表2 单粒子效应定义

单粒子效应	含义
单粒子翻转 (Single Event Upset, SEU)	存储单元逻辑状态改变
单粒子闭锁 (Single Event Latchup, SEL)	PNPN 结构中的大电流再生状态
单粒子烧毁 (Single Event Burnout, SEB)	大电流导致器件烧毁
单粒子栅穿 (Single Event Gate Rupture, SEGR)	栅介质因大电流流过而击穿
单粒子多位翻转 (Multiple Bit Upset, MBU)	导致多位存储信息翻转
单粒子扰动 (Single Event Disturb, SED)	存储单元逻辑状态出现瞬时改变
单粒子瞬态脉冲 (Single Event Transient, SET)	电流引起的瞬态电压变化, 通常是毛刺
单粒子快速反向 (Single Event Snapback, SES)	MOS器件中产生的大电流再生状
单粒子功能中断 (Single Event Function Interrupt, SEFI)	一个翻转导致控制部件出错
单粒子位移损伤 (Single Particle Damage, SPDD)	因位移效应造成的永久损伤
单粒子位硬错误 (Single Hard Error, SHE)	单个位出现不可恢复性错误

2.3 低轨环境分析

根据300 km的轨道条件、空间环境影响因素及其主要影响, 可以基本确定在预定轨道上SEE效应的主要空间环境因素如下。

(1) 高能粒子来源

高能粒子来源主要为: 银河宇宙线、太阳宇宙线以及地球辐射带。

(2) 高能粒子种类

高能粒子种类主要为: 辐射带质子、SAA质子、极区高能质子、太阳耀斑质子、太阳耀斑重离子、银河宇宙线质子、银河宇宙线重离子。

(3) 高能粒子影响模式

根据表 1, 高能粒子的影响主要见表 3。

表3 轨道下高能粒子的敏感对象分析

故障模式	粒子类型	敏感对象
单粒子翻转	高能质子/重离子	逻辑器件、单/双稳态器件
单粒子锁定	高能质子/重离子	CMOS器件
单粒子烧毁	高能质子/重离子	功率MOSFET
单粒子栅击穿	高能质子/重离子	功率MOSFET

3 计算系统设计

3.1 系统架构

搭载试验系统由FPGA+ARM处理板卡、Flash存储板卡、一块机箱背板、一台高可靠V5计算机组成, 其结构如图 2所示。

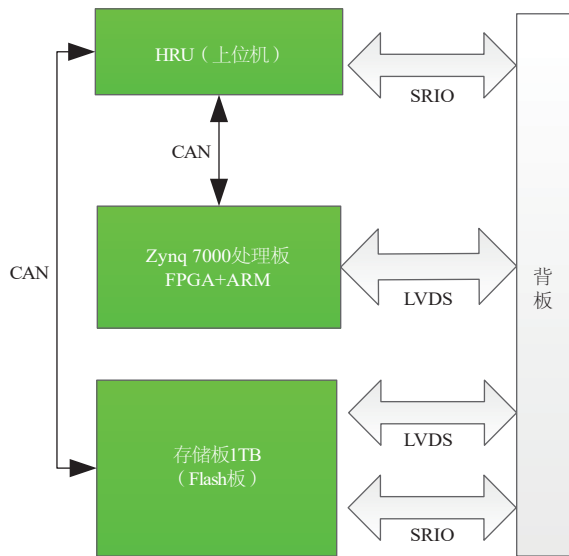


图2 系统框图

3.2 计算系统

处理板选用Zynq 7000可编程SoC板卡, 其中主要由双核Processing System (ARM Cortex A9 MPCore, 简称PS部分) 和Programmable Logic (Xilinx FPGA, 简称PL部分) 组成, 拥有双核 ARM Cortex-A9 MPCore的高性能、低功耗特性, 板卡结构如图3所示。

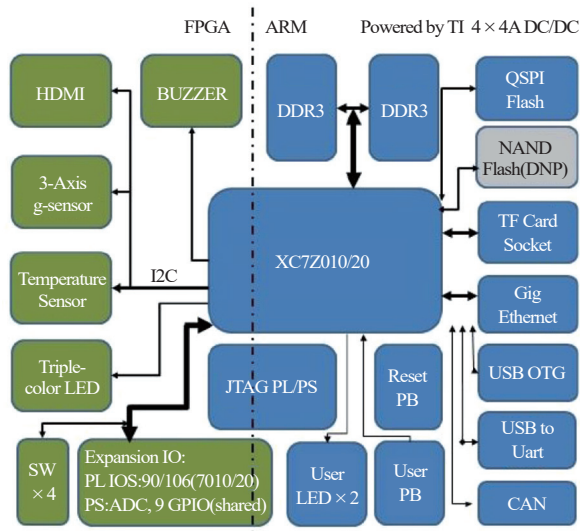


图3 Zynq 7000板卡

基于米尔科技公司推出的以Xilinx Zynq 7000作为主处理器的嵌入式开发板Z-turn board, 板卡设计情况见表4。

表4 板卡硬件情况

类别	对比项	描述
处理器系统单元 (PS)	处理核心	双核ARM Cortex-A9 标准ARM指令集合Thumb-2、Jazelle RTC 和Jazelle DBX Java加速
	协处理器	NEON 128位SIMD协处理器和VFPv3每核
	最高主频	866 MHz
	一级I缓存	32 kB指令Cache每核 支持奇偶校验
	一级D缓存	32 kB数据Cache每核 支持奇偶校验
	二级缓存	512 kB 双核共享, 支持奇偶校验
	片内内存OCM	256 kB 支持奇偶校验
	片外内存	DDR3, 1 GB
	存储容量	4 GB TF卡
可编程逻辑单元 (PL)	Logic核心	28 nm Xilinx 7 Series Artix-7 FPGA
	可编程逻辑单元	2.8逻辑单元 (约43万ASIC逻辑门)
	LUTs	17 600个
	触发器	35 200个
	RAM	240 kB
	DSP slice	80个
其他情况	外设	2×CAN 2.0 B, 1 000 Mbit/s以太网
	供电	1路, 5 V/2 A
	裸板尺寸	102 mm×63 mm×1.6 mm

3.3 系统接口

本方案由HRU、SoC和Flash组成，各部分之间的接口交互关系如图4所示。

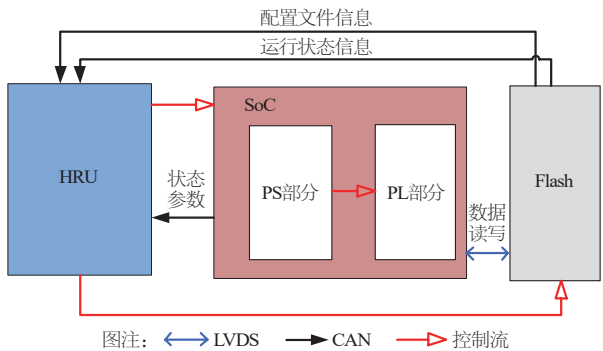


图4 接口交互关系

HRU通过CAN总线将控制流输入到SoC。
HRU通过CAN总线将控制流输入到Flash。
SoC通过CAN总线将数据流上传至HRU。
SoC通过SRIO总线与Flash之间进行读写操作。
Flash通过CAN总线将状态信息上传至HRU。

Flash通过CAN总线将配置文件信息上传至HRU。

4 系统容错设计

4.1 基本思想

面向空间环境的容错设计，其主要目标是在能够取得相同的检错与纠错能力的目标上尽可能地降低对系统资源的开销，比如：系统的时间资源、硬件资源等，才能够将系统能力尽可能地提供给应用使用。

本文中的考虑基于以下基本条件：空间环境中可以认为相同时间内统一程序段连续发生两次翻转的事件为小概率时间。本文不考虑空间环境下的多位翻转所带来的系统影响，重点针对单位翻转所导致的系统运行逻辑错误、系统执行出局处理错误等问题。

本方案容错设计遵循以下两个原则。

原则一：为充分发挥片上系统的处理能力，应当尽可能避免高可靠单元（High Reliable Unit，HRU）参与到计算过程中。

原则二：为保证系统的可靠运行，HRU应当具有对片上系统监测和控制的能力。

遵循以上两点设计原则，针对本项目系统组成，本项目容错架构可分为两层，如图5所示。第一层为由商用SoC组成的片上系统，根据内部软件加固，可以完成不同的任务；第二层为通过HRU来监控片上系统的运行，完成对片上系统的诊断、控制、调配和重启。

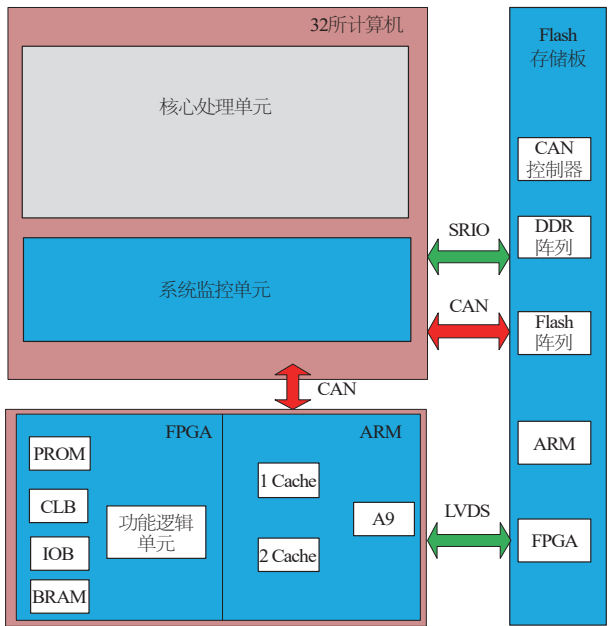


图5 系统容错架构

CAN总线负责单元间传递监控数据、控制指令、工

作状态等参数，SoC与Flash之间通过高速总线LVDS进行数据通信。

4.2 故障分析

在故障分析的基础上，结合本系统的组成结构，分析得到本系统单粒子效应的敏感器件，具体见表5。

表5 系统敏感器件分析

组成	薄弱环节		单粒子效应的主要表现
处理板	ARM	1级D Cache	数据错误、计算结果错误
		1级I Cache	功能错误、程序跑飞等
		2级Cache	数据错误、计算结果错误
	FPGA	配置存储器	FPGA配置错误、功能失效
		用户存储器	数据错误、计算结果错误
	DDR缓存		数据错误、计算结果错误
	NAND Flash存储（512 MB）		数据错误、计算结果错误
存储板	QSPI Flash存储（16 MB）		数据错误、操作系统崩溃等
	FPGA		存储功能失效、数据读写异常
	ARM		存储地址错误、数据读写异常
	DDR2		存储数据错误、计算结果错误
总线	Flash阵列		存储数据错误、计算结果错误
	CAN控制器		功能失效
	SRIO控制器		功能失效

4.3 总体设计

在空间环境中，系统使用过程中既要能够尽量地发挥产品的性能，将系统能力提供给应用使用，又要在此基础上尽可能地提升产品的空间环境适应性。受软件功能、业务需求等影响，不同的应用软件对于系统的可靠性要求各不相同，其对错误的容忍能力也不相同。

通常而言，指令级、进程级等越向底层容错，系统的容错开销也越大，而在应用层则能够通过一些面向应用的算法取得轻量级的容错效果。本文考虑采用多种容错技术来实现面向不同应用的不同程度的容错能力。

本文提出了一种跨层协同的混合容错技术，分别应用应用级、指令级、系统级以及模块级采用不同的容错技术，通过各层容错算法之间的协同来实现系统的整体容错效果最优，系统的容错架构如图6所示。

跨层协同的容错架构在不同层间所采用的技术特点也不相同，各层关系及特点如下：

（1）应用层主要是通过对应用算法的特点分析，挖掘其不变量的关系，通过断言检错等方法，以轻量级的代价提升系统的检错能力；

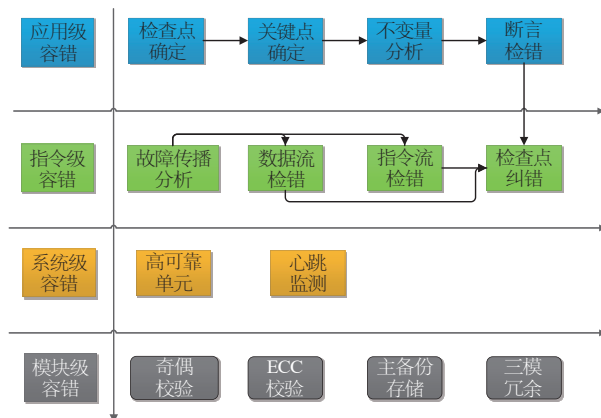


图6 跨层软件容错架构

（2）指令层是通用的容错算法，其主要通过时间、空间等冗余手段来实现系统的检错、纠错，确保系统能够正确运行；

（3）系统层主要依赖于外部高可靠单元，重点针对致命的故障，通过高可靠单元的心跳等手段保证系统在故障面前的存活；

（4）模块级主要是实现数据的可靠存储，对于不同类型的故障能够将所需要的检错、纠错信息可信存储，以实现以上各层算法的正常执行。

5 在轨试验

本文采用典型的计算系统开展跨层协同软件容错架构的设计与实现，为打造面向航天应用的高性能空间容错计算系统提供理论基础与应用指导。

5.1 试验目的

通过在轨空间试验及数据分析，拟评估系统的容错效果，达到对于空间容错计算的验证。

5.2 系统组成

在线测试方案的总体架构主要包括上位机、末子级卫星平台、片上系统以及地面站4个部分，如图7所示。

由片上系统将原始的系统应用运行结果、存储数据等信息上传至上位机并存储；上位机周期性地对存储的信息进行统计分析，得到目标值，并在规定时间内将数据传送到卫星平台；平台在卫星运行至与地面站可通信的轨道时，在规定时间内将数据下传至地面站保存。

5.3 试验场景

本文选用常用的图像处理中的FFT作为基本的应用

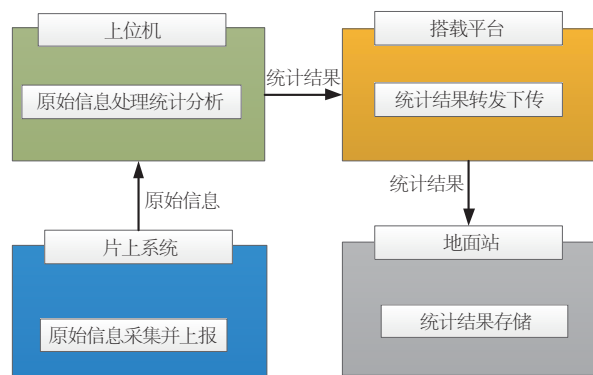


图7 系统组成

程序，在Linux操作系统上运行FFT处理程序，同时在此基础上，通过跨层协同的容错设计完成对FFT算法的加固，采用编译层容错、混合容错开展技术验证。另一方面，通过FPGA开展viterbi编码译码，以及FPGA容错技术验证。

5.4 结果分析

根据任务描述，主要遥测状态包括：计算机1健康状态、应用层容错测试情况、通信编译码容错测试情况。测试时间509 s，根据遥测数据绘制曲线，如图8~图13所示。

根据遥测状态曲线可以看出，计算机电压、温度等健康状态正常。应用层容错运行正常，未检测到错误。通信编译码功能数据生成和译码情况正常、编码器情况正常、译码器情况正常。

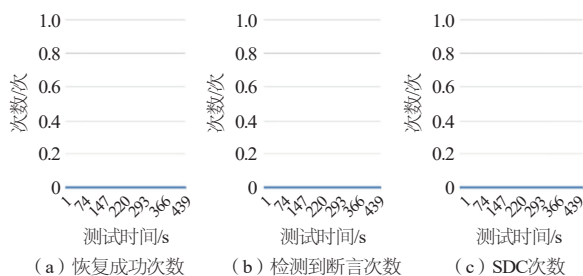


图8 应用层容错-恢复成功/断言/SDC次数

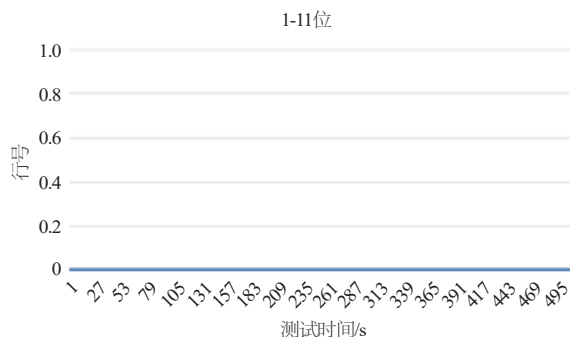


图9 应用层容错-第一次出错行号

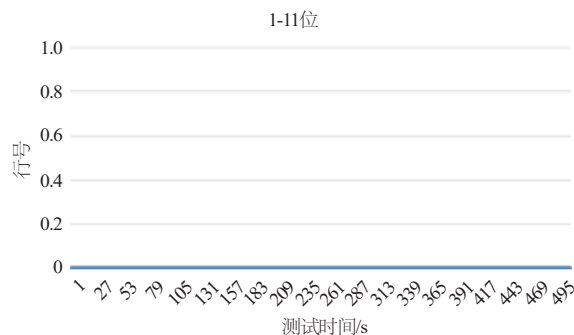


图10 应用层容错-第二次出错行号

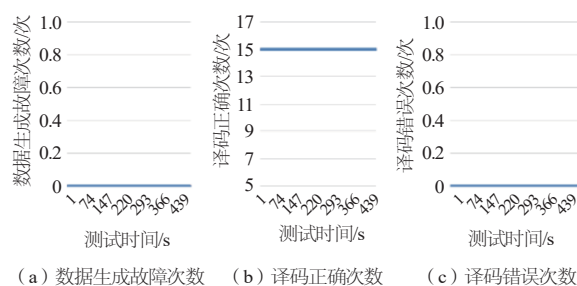


图11 通信编译码容错-数据生成和译码情况

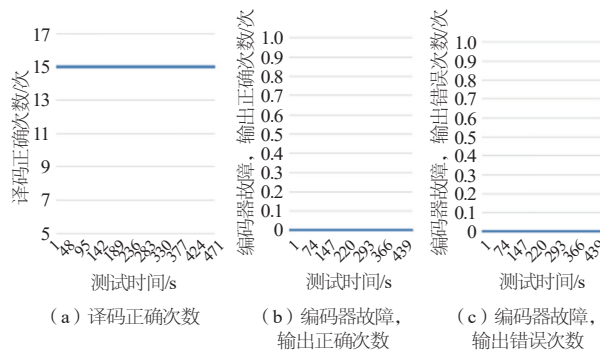


图12 通信编译码容错-编码器情况

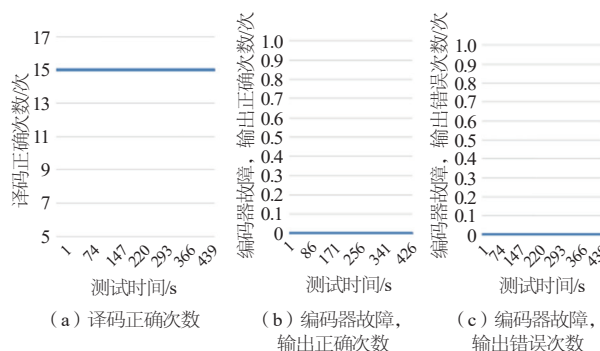


图13 通信编译码容错-译码器情况

参考文献：

- [1] 沈自才, 闫德葵. 空间辐射环境工程的现状及发展趋势[J]. 航天器环境工程, 2014,31(3):229-240.
SHEN Z C, YAN D K. The status quo and development trend of space radiation environmental engineering[J]. Spacecraft Environment Engineering, 2014,31(3):229-240.
- [2] 沈自才. 空间辐射环境工程[M]. 北京: 中国宇航出版社, 2013.
SHEN Z C. Space radiation environmental engineering[M]. Beijing: China Aerospace Publishing House, 2013.
- [3] CLARK J A, PRADHAN D K. Fault injection: a method for validating computer-system dependability[J]. Computer, 1995, 28(6): 47-56.
- [4] 徐建军, 谭庆平, 熊荫乔, 等. 面向瞬态故障的软件容错技术[J]. 计算机工程与科学, 2011, 33(11):132-139.
XU J J, TAN Q P, XIONG Y Q, et al. Software fault-tolerant technology for transient faults[J]. Computer Engineering & Science, 2011,33(11):132-139.
- [5] 田文波, 章斌. 基于SRAM的XILINX FPGA单粒子翻转的测试和试验方法研究[C]//第十届全国抗辐射电子学与电磁脉冲学术年会论文集, 2009.
TIAN W B, ZHANG B. Research on SRAM-based XILINX FPGA single event flip test and experimental method//

Proceedings of the 10th National Anti-Radiation Electronics and Electromagnetic Pulse Academic Annual Conference, 2019.

[作者简介]



张越 (1990-), 男, 山西人, 博士, 工程师, 主要研究方向为航天系统工程、空间计算、系统容错。



章宇兵 (1971-), 男, 河南人, 硕士, 研究员, 主要研究方向为航天综合电子信息系统, 空间计算。



马天琦 (1989-), 男, 北京人, 硕士, 工程师, 主要研究方向为空间计算、卫星通信。



李斌 (1985-), 男, 河北人, 博士, 高级工程师, 主要研究方向为空间计算、航天综合电子信息系统。