Universiteit
Leiden
The Netherlands

Fault-tolerant satellite computing with modern semiconductors

Fuchs, C.M.

Citation
Fuchs, C. M. (2019, December 17). *Fault-tolerant satellite computing with modern semiconductors*. Retrieved from https://hdl.handle.net/1887/82454

Version:	Publisher's Version
License:	Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden
Downloaded from:	https://hdl.handle.net/1887/82454

Note: To cite this publication please use the final published version (if applicable).

Cover Page

Universiteit Leiden

The handle http://hdl.handle.net/1887/82454 holds various files of this Leiden University dissertation.

Author: Fuchs, C.M.
Title: Fault-tolerant satellite computing with modern semiconductors
Issue Date: 2019-12-17

中文摘要（简体）

现代半导体科技让小型卫星的建造不再是梦想。 其低廉的发射成本，能够在有限的预算情况下，实现多样的科学及商业途用。 也就是说，这些小而且轻的卫星可以实现过去技术无法完成，或过于昂贵的太空任务。 这些小型卫星，尤其是立方卫星（CubeSats），其的造价便宜，而且可以快速生产，这使得即使在有限的学术资源环境下也能够进行卫星的研究。 但是由于其可靠性较低，当今这种小型卫星只能够应用于对安全系数要求不高且预算较低的任务。

现代许多成熟的科学及商业应用可以适用于这种小型卫星。 这就使得小型卫星的持久续性越来越受到重视。 理论上来说，这种小型卫星也可以完成许多极关键且复杂的多面任务，比如太阳系的探勘以及天文学的应用。 然而正如前文所言，由于低可靠性，这种小型卫星只能够执行一些次要任务。

小型卫星的关键子系统的建造依赖于电子制造工业，因此电子工业在这种小型卫星中扮演极其重要的角色。 由于小型卫星的整体必须轻巧，所以相关电子零件必须更轻、更小，还要具有比传统太空等级零件更好的效能功耗比。 因此，所有先进的立方卫星都使用了最尖端的工业级嵌入式以及商业通信系统。 这些零件不仅价格低廉，而且能够提供充足的效能，消耗更少的能源，同时相对于传统的太空等级元件更容易使用。

然而，传统基于片上系统（System-on-Chip-based）的计算机并不具备较大型的太空船所另有的容错能力。 相关的研究表明，使用这种基于片上系统的组件是太空船在发射和部署过程中主要的故障起原因。 而且，由于受到预算、能耗、重量及空间的限制，当今应用于较大型太空船的电脑容错技术，仍无法应用小型卫星。

截至2019年，尚没有任何一个可容错的计算机架构，可以在不破坏低价、简单、轻盈、节能的原则下，将嵌入式及商业手机中的半导体应用在这类可被大量生产且易于发射的小型卫星上。 因此，这些小型卫星的设计者有以下三个选择：

尺度提升： 采用传统的太空零件。 这通常需要将整个太空船的设计变大，而且这种零件的功耗较高、功能较少，还缺少设计弹性，甚至计算效能也较低。 实际上，这会大幅增加开发成本、人力开销以及卫星的开发时间。 因此，这种方法对于那些要求开发迅速、太空船体积要小、价格便宜或可支付的起的先进设计理念来说，是不可行的。

备用卫星： 部署一或多个备用卫星（SpareSats）以缓解立方卫星在早期发生错误的风险。 实际上，随着发射上去的零件数量的增加，不仅增加成本，还会让错误发生几率升高。 因此，这个方法只能在系统达到一定的稳定性之后才能使用。 现在这个方法只能用在卫星世代频繁更替的星座计划（Constellation Missions），例如Planet Lab，以及具有超多预算的卫星，例如Marco。

接受： 接受其不可靠的事实。 让任务保持精简，希望它可以在太空船发生故障

> 前完成所有主要工作。 而对于未来那些需要较长持续时间的小型卫星，它们的系统工程不应该基于任何不切实际的期望和侥幸。

在本论文中，大部分小型卫星任务的开发人员都只能遵照第三个选项。 对于那些立方卫星任务，这个方法通常都会成功，但有时也会发生早期的错误。 然而，去赌何时卫星会出错或者迷信器件不会受环境的影响是不能被接受的，更不用说政府、太空局或是投资者了。 为了保证可长期执行任务的立方卫星任务成功，必须要有更好的、更可靠的系统架构。 因此，适用于基于现代商业半导体的机载电脑的容错概念就显得尤为重要。

本论文书及其结果

为解决现代科技对于超小卫星的技术缺陷，本论文提出了一个全新的容错计算机架构。 这个架构甚至可以整合进使用现代半导体产业技术制造的立方卫星。

为了开发本论文所提出的架构，我们使用了来自各种科学和工程领域的方法和概念，而且我们所涉及到的专业技术超越了现有的科学和工程技术。 我们利用实际可行的操作方式与电机工程领域最严谨的测试方式将两个不同领域最先进的技术、概念与理论结合在一起。

为了使科学家和工程师更容易理解本文的工作，第二章和第三章简单介绍论文所涉及到的容错定义与技术。 第二章会为不熟悉该领域的读者介绍与当代航太技术相关的要点以及容错计算机设计的概念，阐述本论文的研究动机。 为在航天装置上设计有效的容错架构，我们必须要清楚宇宙环境对于电脑装置的影响，所以第三章会介绍这些宇宙射线的影响、太空电路设计的限制以及太空任务中时常考量的的因素等(如：天体力学以及通讯时间)。

第四章将介绍本论文所提出的容错机载计算机架构。 我们的架构结合了FPGA可重新组态的容错概念以及混合关键系统的技术，这进一步完善了传统错误容错检测与错误恢复的方法。 我们提出的方法被设计成多个不同但相关的过程，这使得我们的机载计算机能更稳定的老化。

在第四章中，为了实现以上功能，我们利用软件模拟出的一个简化版的锁步技术。 仅使用这个模式就可以有非常强大的容错能力，但它不能满足宇宙任务中长期运行的需求。 因此，第五章介绍可重新组态的逻辑如何协助修复各式各样的错误。我们利用FPGA的可重新组态特性来确保系统单晶片的完整性。 这将帮助我们延长整台计算机的寿命，并且尽可能地妥善利用备用资源。 然而，对于长期的太空任务，那些损坏的FPGA部件终究无法再次利用重新组态来修复，可以被可重新编写的程序逻辑将会随着时间越来越少。 因此在第六章中，我们将展示如何混合关键技术使得一台计算机慢慢被降级而不是像传统的计算机立即无法使用。 我们可利用这样的技术使得计算机自动将效能的损失转换为电力上的节约以及整体完善性。 这使得即便有错误的发生，我们在航天上的核心功能还是可以安全地被维持住，达到整体寿命的延长以及备用资源利用的最大化。

我们将上述全部的功能安装在一个FPGA多核的单片系统上。 软件、负载通信以及逻辑程序对于FPGA来说都是重要的数据。 在整个太空任务的过程中，这些信息都必须要保持完整性。 为此在第七章中，我们将介绍在现代的卫星中，如何保护各种不同存储介质中的资料。

在现有基于软件方面的容错技术，理论上应用于现代的半导体制程技术也都很合适。 然而事实上，这些技术对于现实中的应用需求是不切实际的。 目前为止还没有人成功把那些技术实现并验证。 为此，在本研究中，第八章至第十章阐述我们的实现方法。

第八章中，我们利用错误注入（Fault Injection）的方式来验证我们所提出的锁步系统模式。 在第九章，针对前面提出的架构，我们提出一个实际可行的多核的单晶片系统设计。 而在第十章中，我们说明前面章节所提到的观念以及设计和实现方法。 更进一步，我们用开发板以及概念验证的方式展现出采用这种架构的机载计算机在现实生活当中可能的样子。 我们利用以下六种Xilinx的FPGA来展示我们设计:

- Kintex UltraScale KU60,
- Kintex UltraScale+ KU11p, KU3p, KU5p 开发板 Xilinx KCU116, 和
- Virtex UltraScale+ VU9P 开发板 Xilinx VCU118.

对于 KU60、 KU11p 与 KU3p 这三种FPGAs，我们提供完整详细的功耗与利用率数据。

结论

在本论文的开始，我们提出过这样的疑问:

”我们能否在不打破小型卫星应用所需要的质量、大小、预算与复杂度的前提下，利用现代的嵌入式技术与移动装置技术完成具容错功能的架构？”

依照近三年的研究文献以及一些重大事故的纪录，我们或许可以使用下面的说法来回答这个问题:

“是的，利用现代一般用户级或是工业级技术确实可以达到这样的容错计算机结构。 一旦能完成雏形，我们就可以大幅度延长现代立方卫星的寿命，从而使其可被用来完成重大或长期的太空任务。”

本论文提出的架构能用非侵入的方式运行完成。 我们的架构支持目前已经存在的应用，并不需要针对那些服务重新设计来符合这个架构。

我们提出的机制可以快速且准确的检测出实际应用软件的故障问题，并且在大多处状况下，仅需要很低的计算量就能将错误更正。 我们展示了这种架构的高成本效益，且即使长期运行在高太阳直射的太空区域，也能维持正常的工作。

利用现代的元件，我们提出的架构甚至可以运行在耗电仅有1.94瓦的Ultrascale+ FPGA上。 因此，这样的机载电脑架构可以被应用在许多小型卫星上 (如: 2U 立方卫星)。

随着科技的发展，下一代FPGAs的半导体制造程技术会使得我们的方法更具有应用前景。 利用新的制成技术，我们可以更有效地制造那些被用来协助科学与太阳系探索的太空飞船。 在未来，我们将有机会探索更广阔、未知的宇宙。