Fault-tolerant satellite computing with modern semiconductors

Fuchs, C.M.

中文摘要（繁體）

現代的半導體科技讓小型衛星的建造不再是夢想，其發射之成本低廉，能夠在預算有限的情況之下作為多樣化的科學以及商業的用途。 也就是說，這些小且輕的衛星可以達到過去科技無法完成或是過於昂貴的太空任務。 尤其是一些衛星像立方衛星（CubeSats），它們的造價便宜，而且還可以被快速地生產，這使得資源有限的學術環境也能夠跨足衛星的研究。 然而，現在它們的可靠性還是太低。 因此，截至目前為止，它們主要還是被用在較無安全疑慮且低預算的任務。

如今，許多複雜的科學以及商業應用也適合在這種小型衛星上面運作，這使得太空任務的持續性越來越受到重視。 理論上來說，這種衛星也可以用來完成許多極關鍵與複雜的多面向任務，像是太陽系的探勘以及一些天文學的應用。 然而，正如前文所言，它們的可靠性尚且不足，所以現在只能執行一些次要任務。

現代電子工業在這種小型衛星中扮演極其重要的角色，造就了小型衛星內的一些關鍵子系統。 由於整體重量必須要輕巧，所以相關的電子零件必須更輕、更小，還要能夠比傳統的太空等級零件具有更好的效能功耗比。 是故，所有先進的立方衛星都使用了最尖端的工業級嵌入式及行動通訊市場導向的電腦設計技術。 在造價十分低廉的情況下，這些零件不僅提供足夠的效能，耗費更少的能源，同時比其已經有長期使用歷史之太空等級的對應元件更容易使用。

然而，傳統基於單晶片系統（SoCs）的電腦也缺少較大型的太空船所需要的容錯能力。 在相關的研究報告成果中，使用這種單晶片的子系統被認為是太空船發射並部署在太空中發生故障的主因。 由於小型衛星具有預算、能量、重量及空間的限制，當今被設計用來符合較大型太空船的電腦容錯技術，仍無法被採納。

時至西元2019年，還是沒有任何一個可容錯的計算機架構，在不破壞低價、簡單、輕盈、節能的原則之下，成功地將嵌入式及行動市場中的半導體應用在可以被大量生產且易於發射的小型衛星上。 因此，這些小型衛星的設計者有以下三個選項：

元件提升： 採用傳統的太空零件。 這通常會需要把整個太空船的設計變大，而且這種零件的功耗較高、功能較少，還缺少設計彈性，甚至連計算效能也較為低落。 在實務上來說，這會大幅地增加成本、人力以及衛星的開發時間。 因此，這種方法對於那些要求開發迅速、太空船要小、便宜或可支付的起的先進設計理念來說，是沒有建設性的。

備用衛星： 部署一或多個備用衛星（SpareSats）以緩解立方衛星在早期發生錯誤的風險。 實際上，這不僅增加成本，還會讓錯誤更可能發生，因為發射上去的零件數量倍增了。 因此，這個方法只能在系統達到一定的穩固性之後才能使用。 現在這個方法只能用在衛星世代頻繁更替的星座任務，例如Planet Lab，以及一顆具有超多預算的衛星，例如MarCo。

接受： 接受其不可靠的事實。 讓任務保持精簡，期望它可以在太空船意外故障前完成所有主要工作。 而對於未來那些需要較長持續性的小型衛星任務，它們的系統工程不應該基於任何不切實際的期望、信仰以及僥倖。

當這篇論文在撰寫的時候，大部分小型衛星任務的開發人員都只能遵照第三個選項。 對於那些簡單扼要的立方衛星任務，這個方法通常都會成功，但有時候也會發生早期的錯誤。 然而，去賭衛星不會在錯誤的時間被環境影響理應是不能被接受的，更不用說是政府、太空局或是投資者了。 為了保證進階且長期的立方衛星任務可以成功，更好的、更可靠的系統架構是必須存在的。 因此，適合現代商業半導體所組成之機載電腦的容錯概念，是一定要有的。

本書及其結果

為解決現代科技對於超小衛星的技術缺陷，本論文提出了一個全新的容錯計算機架構。 這個架構甚至可以被整合進使用現代半導體產業技術製造的立方衛星。

為了開發出本論文所提出的架構，我們使用了來自各種科學和工程領域的方法和概念，而且 我們所涉及到的專業技術分別超越了現在的科學和工程技術。 我們利用實務上可行的實作方式與電機工程領域最嚴謹的測試方式將兩個不同領域最先進的技術、概念與理論結合在一起。

此外，我們希望能讓這篇研究同時也可以輕易地被科學與工程人員理解，章節二與三的重點會簡單介紹這篇文章所涉及到的容錯定義與技術。 為了讓那些不熟悉這個領域的讀者可以更完整地理解本文的核心理念與動機，章節二大致會介紹與當代航太技術相關的要點以及容錯計算機設計的概念。 而如果要能在航太裝置上設計有效的容錯架構，我們必須要很清楚知道宇宙環境對於電腦裝置的影響。 所以章節三會介紹這些宇宙射線的影響、太空電路設計的限制以及太空任務中時常被考量的的因素等(如：天體力學以及通訊時間)。

第四章將介紹我們所提出的容錯機載計算機架構。 我們的架構結合了FPGA可重新組態的容錯概念以及混合關鍵系統的技術，這進一步的協助了其他傳統的錯誤容錯與錯誤更正的方法。 我們提出的方法被設計成了許多不同且環環相扣的過程，這使得我們的機載計算機能更穩定的老化。

在第四章中也會提到為了實現以上功能，我們利用軟體模擬出的一個簡化版鎖步系統模式。 僅使用這個模式就可以有非常強大的錯誤容忍能力，但它不能滿足宇宙任務中需要長期運行的需求。 因此，我們在第五章中介紹可重新組態的邏輯如何協助我們將各式各樣的錯誤修復。 我們利用FPGA的可重新組態特性來確保系統單晶片的完整性。 這將幫助我們延長整台計算機的壽命，並且盡可能地妥善利用備用資源。 然而，在十分長久的太空任務中，那些損壞的FPGA區塊終究無法再次利用重新組態來修復。 因此，可以被重新編寫的程式邏輯將會隨著時間越來越少。 在第六章中，我們將展示如何利用混合關鍵技術來使得一台計算機慢慢被降級而不是像傳統的計算機一瞬間就整台無法使用。 我們可利用這樣的技術使得計算機自動地將效能的損失轉換為電力上的節約以及整體的完善性。 這使得即便有錯誤的發生，我們在航太上的核心功能還是可以安全地被維持住，達到整體壽命的延長以及備用資源利用的最大化。

我們將上述全部的功能，使用軟體實作在一個FPGA多執行序的單晶片系統上。軟體、負載資訊以及邏輯程式對於FPGA來說都是重要的資料，在一整個太空任務的過程之中，這些東西都必須要保持其完整性。 在第七章中，我們介紹在現代的衛星之中，如何保護各種不同記憶體中資料。

在以往基於軟體方面的容錯技術，理論上應用於現代的半導體製程技術也都很適合。 然而這些技術事實上對於真實世界中的應用需求都是不切實際的。 到現在為止還沒有人成功地把那些技術實作出來並驗證，因此這將會是很困難的一步。 於本篇研究中，我們接受這個挑戰，並在第八章節至第十章節說明我們是如何達成的。

第八章中，我們利用錯誤注入的方式來驗證我們所提出的鎖步系統模式。 於第九章中，我們針對前面提出的架構提出一個實務上可行的多處理器的單晶片系統設計。

而於第十章節中，我們專注在說明前面章節所提到的觀念以及設計是如何實作的。更進一步，我們用開發板以及概念驗證的方式展現出採用這種架構的機載計算機在現實生活當中可能會長成甚麼樣子。 我們利用以下六種Xilinx的FPGA來展示我們設計:

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

對於 KU60、 KU11p 與 KU3p 這三種FPGAs，我們提供完整詳細的功耗與利用狀況數據。

結論

於文章開頭，我們提出過這樣的疑問:

「我們能否在不打破小型衛星應用所需要的質量、大小、預算與複雜度的前提下，利用現代的嵌入式技術與行動裝置技術完成具容錯功能的架構？」

依照近三年的研究文獻以及一些重大的災害紀錄，我們或許可以使用下面的說法來回答這個問題：

「是**的**。 利用現代一般用戶級或是工業級技術確實可以達到這樣的容錯計算機結構。 一旦能完成雛形，我們就可以用來大幅度延長現代立方衛星的壽命，從而使其可被用來完成重大或長期的太空任務。」

本文提出的架構能用非侵入的方式實作完成。 我們的架構都有支援那些已經存在的應用服務，完全不需要針對那些服務重新設計來符合這個架構。

我們提出的機制可以快速且準確的檢測出實際應用軟體的故障問題，並且在大多處的狀況下，僅需要很低的計算量就能將錯誤更正。 我們也展示出這種架構的成本效益很高，且即使長期運行在高太陽直射的太空區域，也能維持正常的工作。

利用現代的元件，我們提出的架構甚至可以實作在耗電僅有1.94瓦的Ultrascale+ FPGA之上。 因此，這樣的機載電腦架構肯定可以被應用在許多小型衛星上 (如: 2U立方衛星)。

隨著科技的發展，下一代FPGAs的半導體製程技術會使得我們的方法更加受到重視。 利用新的製成技術，我們可以更有效地製造那些被用來協助科學與太陽系探索的太空梭。 在未來，我們將有機會可以探索更廣大且未知的宇宙。