Fault-tolerant satellite computing with modern semiconductors

Fuchs, C.M.

日本語の要約

現代の半導体技術により、衛星の小型化が可能になっている。 安価な打ち上げを特徴とする小型衛星は、様々な科学・商業機器を搭載できる低コストなプラットフォームである。 特に、最も小さくて軽い衛星は、今までは技術的に実行不可能、非実用的、または単に不経済であった宇宙ミッションを可能にしている。 特に、CubeSatとして作られた衛星は、限られたリソースしかない学術環境でも、低コストで迅速に製造できる。 しかし今、そのような宇宙船は低い信頼性という問題に直面している。 そのため、これまでは主に、リスクを許容できるような、重要性の低い低予算ミッションに利用されてきた。

今日、多くの洗練された科学・商用アプリケーションを目的として、小型衛星を利用する事も可能である。この様な場合、ミッション期間をできるだけ長くすることが望まれる。 理論的には、このような宇宙船は今日、様々な重要かつ複雑な多段階ミッションや、太陽系内探査や天文学の観測への応用といった高優先度の科学ミッションにも利用できる。 しかし、これらの宇宙船は信頼性が低いため、これまで副次的なタスクを達成するための助けとしてのみ利用されてきた。

現代の電子機器はそのような宇宙船の重要な部分や、最も重要なサブシステムのいくつかを構成している。 これらの電子機器は、宇宙船自体が軽量であることを考慮すると、従来の宇宙用コンポーネントよりも軽く、小さく、ワットあたりの性能が優れている必要がある。 従って、今日の全ての高度なCubeSatは、産業用組込み機器やモバイル機器にも使われる最先端のコンピューター設計を利用している。 これによって、最小限のコストで豊富なパフォーマンスを提供できる他、消費エネルギーが少なく、長年使用されてきた宇宙級同等品よりも操作が簡単である。

しかし、従来のSoCを使用したコンピューターには、大型宇宙船に搭載されているコンピューターアーキテクチャのフォールトトレランス機能がない。 従来研究では、これらの部品を使用したサブシステムは、宇宙船が打ち上げられて配備された後の大部分の障害の原因であると判断されている。 小型衛星の予算、エネルギー、重量、及び体積の制限により、大型宇宙船用に開発された既存のフォールトトレラントコンピュータソリューションは採用できない。

2019年現在、産業用組込み機器やモバイル機器にも使われる半導体を搭載したナノサテライトで利用できるフォールトトレランス機能を備えたコンピューターアーキテクチャは存在していない。 従って、小型衛星開発者には、次のような選択肢が残されている。

アップスケーリング： 従来の宇宙級部品を利用する。 これには通常、宇宙船の設計をより大きなフォームファクターにアップスケールする必要がある。 そのような部品はより多くのエネルギーを必要とし、機能性、柔軟性、処理性能が低いためである。 実際には、これにより、コスト、人件費、および衛星開発時間が大幅に増える。 従って、このアプローチは、短開発期間化、小型化、拡張可能化、低維持費を特徴とする宇宙船の利用を中心としたほとんどの新しいミッション

構想に対して建設的ではない。

予備衛星利用： 1つまたは複数の予備衛星を投入して、障害が発生したCubeSatを代替することにより、早期障害のリスクを軽減する。 実際には、これによりコストが増加するだけでなく、使用した部品の総数が倍増するため、障害発生の可能性が高くなる。 従って、このアプローチは、十分なレベルの堅牢性が達成された後にのみ実行可能になる。 現在、このアプローチは、衛星世代が急速なペースで継続的に交換される星座ミッション（例えば、Planet Lab）、及び非常に豊富な予算を持つ個別の衛星プログラム（例えば、MarCo）でのみ実行可能である。

受け入れ： 信頼性の欠如を受け入れる。 宇宙船が最終的に偶然に失敗する前に、すべての主要な目的を達成することを期待して、ミッションの簡潔化を図る。 しかし、将来の長運用期間の小型衛星ミッションの場合、希望、信仰、幸運をシステムエンジニアリングの基盤とすることは避けるべきである。

この論文が書かれたとき、ほとんどの小型衛星ミッションの開発者はこの3番目の選択肢に従うことを余儀なくされた。 非常にシンプルで運用期間の短いCubeSatミッションの場合、このアプローチは多くの場合成功したが、多くの初期の失敗ももたらした。 しかし、時間に賭けて、悪いタイミングで環境効果の影響を受けない様との希望に固執することは、政府、宇宙機関、及び投資家から益々容認されなくなってきている。 それは、より優れた、より信頼性の高いシステムアーキテクチャが必要とされる高度な長期CubeSatミッションの成功を確実にするためである。 従って、現代の商用半導体に基づいたオン・ボード・コンピューターに適したフォールトトレラントの概念が必要です。

本論文とその成果

本論文では、今日の小型衛星の利用に影響を与える技術的欠陥を克服するために、新しいフォールトトレランス機能を備えたコンピュータアーキテクチャについて詳述する。 これは最新の市販半導体を用いた科学用途の軽量CubeSatにも適用できる。

本論文で詳述されるアーキテクチャを開発するには、幅広い科学および工学分野の成果と概念が利用された。 また、このアーキテクチャの開発に関わる専門知識は、科学と工学の両方を個別に超えている。 代わりに、これらの両方の長所を組み合わせて、科学の進歩、概念的知識、理論的概念を、宇宙および電気工学の分野で実用的な実装と徹底的なテストを通じて統合している。

本論文の研究内容を科学者と技術者の両方にとって分かりやすいものにするために、第２章と第３章では、この論文で対象とされる故障モデルの紹介と定義について述べる。 第２章は、このトピックに精通していない読者のために、今日の宇宙飛行の重要な側面について概述している内容が含まれており、本論文の動機づけとなっている。 第２章では、フォールトトレラントコンピューターの設計に関連する概念についても紹介する。 効果的かつ効率的なフォールトトレラントオンボードコンピューターアーキテクチャの設計および開発を行うために、コンピューターの宇宙環境の影響に関して把握することが重要である。 従って、第3章では、これらの効果、宇宙電子機器の設計上の制約、通信時間や天体力学などの宇宙ミッション中の運用上の考慮事項について詳しく説明する。

第４章では、ソフトウェアで実装されたフォールトトレランスの概念とFPGAの再構成および混合重要度を組み合わせたフォールトトレラントオンボードコンピューターアーキテクチャについて述べる。 これは、他のいくつかの従来のフォールトトレランスおよびエラー修正手法でさらに補完される。 このアーキテクチャのフォールトトレランスは、オンボードコンピューターの無害劣化を可能にするいくつかの相互リンクされたステージとして実装される。

これらの全ての機能を有効にするために、ソフトウェアで実装された粗粒度lockstepロックを利用する。 これについては、第４章で詳述する。 この機能だけでも強力なフォールトトレランス機能を提供できるが、長期的なミッションには不十分である。 従って、第５章では、様々な障害から欠陥のあるシステムを回復するために再構成可能なロジックを使用する方法について述べる。 FPGAの再構成を利用して、システムオンチップ設計の整合性を確保し、オンボードコンピューターの耐用年数を延ばし、スペアリソースのフォールトカバレッジの可能性を最大化する。 非常に長期の宇宙ミッションでは、FPGAの欠陥部分は最終的には再構成によって回復できなくなる。 従って、オンボードコンピューター内で利用可能な正常プログラマブルロジックの量は、時間の経過とともに減少する。 第５章では、従来のシステムのように自然に失敗するのではなく、混合重要度によりコンピュータが劣化に適応させる方法を示す。 この機能を使用して、実行時に性能を節電と堅牢性と自律的にトレードオフすることができる。 これにより、障害が発生したときにフライトソフトウェアのコア機能を保護し、無害劣化を実現し、予備リソースをプールして、存続可能性を最大化できる。

この機能はすべてソフトウェアとして存在する。 FPGA内に実装されているマルチプロセッサシステムオンチップで実行される。 ソフトウェア、ペイロード情報、及びFPGAにプログラムされたロジックはデータであり、宇宙ミッション全体を通してその整合性を保護する必要がある。 第７章では、最新の衛星に搭載されている様々なメモリテクノロジー保護の概念について説明する。 現代の半導体に適用可能な以前のソフトウェアベースのフォールトトレラントの概念は、多くの場合理論的には良さそうである。 しかし、これらは実際のアプリケーションでは実用的ではない。 これまで、このようなフォールトトレランスアーキテクチャは実際に実装および検証されていないが、そうすることは重要である。 本論文の第８章から第１０章の内容はこのような実装と検証に関するものである。

アーキテクチャで使用されるlockstep機能は、第８章の故障挿入を用いて検証する。 第９章では、FPGAに実装するための実用的なマルチプロセッサシステムオンチップ設計について説明する。 この設計は、上記のアーキテクチャの理想的なプラットフォームとして機能する。 第９章は、前章で説明した概念と設計の実用的な実装について述べる。 これにより、開発ボードから構築されたブレッドボードベースの概念実証を使用して、このアーキテクチャを備えたオンボードコンピューターが実際にどのように見えるかを示す。 これは、次の6つのXilinx FPGAに対して行われた。

- Kintex UltraScale KU60、
- Kintex UltraScale + KU11p、KU3p、Xilinx KCU116開発ボードのKU5p、
- Xilinx VCU118開発ボードのVirtex UltraScale + VU9P。

これらのFPGAのうち、KU60、KU11p、およびKU3pの3つについて、詳細な電力および使用率データを提供する。

結論

本研究が始まったとき、私は次の質問を提起した。

「小型衛星アプリケーションの重さ、大きさ、複雑さ、および予算の制約を解消することなく、最新の組込みおよびモバイル市場向けの半導体技術でフォールトトレランスコンピューターアーキテクチャを実現できるか？」

その後の3年間、多くの研究論文が発表され、またいくつかの大惨事が発生したが、次のようにこの質問に答えることができた。

「**はい。** 小型衛星用のフォールトトレラントコンピュータアーキテクチャは、現代の消費者や産業向けのテクノロジで技術的に実現可能である。 プロトタイプとして完全に実装されると、現代のCubeSatの寿命を大幅に延長するために使用できるため、重要かつ長期的な宇宙ミッションでの使用が可能になる。」

本論文で提案されたアーキテクチャのソフトウェアコンポーネントは、非侵襲的な方法で実装できる。 これらは、既存のアプリケーションを保護し、このアーキテクチャをサポートするためにアプリケーションをカスタム作成する必要はない。 実際のソフトウェアを使用して、これらのメカニズムが障害を迅速かつ高い確率で検出でき、ほとんどの場合、低計算コストで障害から正常に回復できることが示された。 このアーキテクチャのパフォーマンスコストは経済的であり、非常に放射線量の高い空間領域で動作する場合でも効果的であることも実証されている。

最新の商用部品を使用すると、このアーキテクチャの理想的なプラットフォームとして機能するシステムオンチップ設計を、わずか1.94Wの消費電力で最小のUltrascale + FPGAに実装することができる。 従って、このオンボードコンピューターアーキテクチャは、2U CubeSatほどの小さい衛星に適用できる。

技術に合わせて拡張できるため、次世代FPGAの半導体製造の進歩により、このアプローチはさらに魅力的になり、小型宇宙船の保護にも使用できるようになるだろう。 現在、私たちが高優先度の科学と太陽系の探査に使用しているより重い宇宙船に実装されると、効率とスケーラビリティを改善できる。 そして、おそらく将来的には、その境界を越えて何が存在するのかを探ることが期待できる。