Fault-tolerant satellite computing with modern semiconductors

Fuchs, C.M.

Resumen en Español

La tecnología de semiconductores modernos permite la construcción de satélites miniaturizados, los cuales son económicos para lanzar y sirven como plataformas de bajo costo para una amplia variedad de instrumentos científicos y comerciales. Los satélites más pequeños y livianos están especialmente situados para realizar misiones espaciales que previamente eran técnicamente imposibles, imprácticas, o simplemente costosas. Particularmente, los satélites construidos como CubeSats pueden ser fabricados rápidamente a bajo costo con los limitados recursos en ámbitos académicos. Sin embargo, en la actualidad estas naves espaciales presentan baja fiabilidad. Por ello se han utilizado principalmente para misiones de bajo presupuesto y menos críticas en donde los riesgos son aceptables.

Muchas aplicaciones sofisticadas, tanto de tipo científicas como comerciales, se prestan para el formato de los satélites miniaturizados, lo cual hace misiones de más larga duración deseables. Teoréticamente, dichas naves espaciales pueden ser utilizadas actualmente en una variedad de misiones críticas y polifacéticas complejas, al igual que para misiones científicas de alta prioridad como para la exploración del sistema solar y aplicaciones astronómicas. Sin embargo, debido a su baja fiabilidad, estas naves espaciales han sido utilizadas hasta ahora para realizar tareas secundarias.

Los electrónicos modernos constituyen una parte significativa de dichas naves espaciales, y componen varias partes de los subsistemas más críticos de la nave. Tomando en cuenta el restringido peso de estas, los electrónicos deben ser más livianos, pequeños, y además deben ofrecer mejor rendimiento por watt que los tradicionales componentes con resistencia a radiación. Por ende, los CubeSats avanzados en la actualidad utilizan arquitecturas de computadoras derivadas de tecnologias móviles e industriales innovadoras. Con un costo mínimo, estos ofrecen alto rendimiento, requieren menos energía, y son más fáciles de trabajar que sus contrapartes con resistencia a radiación, las cuales tienen un largo legado de uso en el espacio.

Sin embargo, las computadoras basadas en sistemas en chip convencionales también carecen de la capacidad para la tolerancia a fallos de las arquitecturas de computadoras a bordo de naves espaciales grandes. El análisis de naves espaciales lanzadas y desplegadas en el espacio determinaron que los sistemas en chip eran los responsables de la mayoria de fallas en las misiones. Debido a restricciones de presupuesto, energía, masa y volumen en satélites miniaturizados, las actuales técnicas de tolerancia a fallos, originalmente desarrolladas para naves espaciales grandes, no pueden ser adoptadas y aplicadas.

Hasta la fecha de esta tesis, no existen arquitecturas de computadoras con tolerancia a fallos que se puedan utilizar a bordo de nanosatélites con semiconductores integrados y móviles sin que se quiebre con el concepto de satélites de bajo costo, simples, energéticamente eficientes y livianos que puedan ser fabricados en masa y lanzados a bajo costo. Por consiguiente, los siguientes métodos existen para desarro-

llar satélites miniaturizados:

Escalamiento: Utilización de componentes tradicionales para uso espacial. Esto requiere incrementar las dimensiones del diseño de la nave espacial, ya que estos componentes requieren más energía y ofrecen menos funcionalidad, flexibilidad, y rendimiento. En práctica, esta opción incrementa drásticamente el costo, mano de obra, y tiempo de desarrollo requerido. Como tal, esta opción no es constructiva para la mayoria de misiones con el objetivo de mantener las naves espaciales pequeñas, con bajo presupuesto, y de rápido desarrollo.

SpareSats: Reducir y mitigar el riesgo de fallos tempranos mediante el desplegamiento de SpareSats para reemplazar un CubeSat que ha fallado. En práctica, este método no solo incrementa el presupuesto necesario, pero también incrementa la posibilidad de fallos ya que el número de componentes lanzados y desplegados se duplica. Debido a las limitaciones mencionadas, este método se convierte en una solución viable solo cuando se ha logrado suficiente robustez. Por ello, SpareSats es principalmente viable para misiones de constelación donde generaciones de satélites son reemplazados continuamente a un paso acelerado (por ejemplo, Planet Lab), y para satélites individuales con un prosupuesto abundante (por ejemplo, MarCo).

Aceptación: Aceptar el riesgo de baja fiabilidad. Este método se basa en que la misión sea de corta duración con la esperanza de alcanzar los objetivos principales antes que la nave espacial eventualmente falle. Para futuras misiones de satélites miniaturizados con una larga duración, esperanza, fe y suerte no deberian ser factores sobre los cuales este basada la ingeniería.

Cuando se escribio esta tesis, la mayoria de satélites miniaturizados tuvieron que seguir la tercera opción, aceptación, durante el desarrollo de la misión. Para misiones de CubeSats sencillas y breves, este método resultó en exito más amenudo de lo esperado, pero también llevo a fallos en etapas tempranas de la misión. No obstante, jugarse contra el tiempo y aferrarse a la esperanza que los efectos ambientales en el espacio no impacten la misión en el momento equivocado es inaceptable, y, cada vez más, menos tolerado por gobiernos, agencias espaciales e inversionistas. Para asegurar que las misiones avanzadas de larga duración con CubeSats sean exitosas, mejores arquitecturas de sistemas con alta fiabilidad son indispensables. Por ello son necesarios conceptos de tolerancia a fallos que sean adecuados para las computadoras a bordo de satélites basadas en semiconductores comerciales modernos.

Esta Tesis y sus Resultados

Para superar los déficits tecnológicos que impactan el uso de satélites muy pequeños en la actualidad, esta tesis detalla una novedosa arquitectura de computadoras con tolerancia a fallos. El método y enfoque presentado en esta tesis es adecuado para integración en satélites de todo tamaño, incluyendo los CubeSats livianos para misiones científicas, los cuales estan basados en semiconductores comerciales modernos.

Para desarrollar la arquitectura presentada en esta tesis, resultados y conceptos de varias areas de ciencias e ingienerias son utilizados. La experiencia necesaria para desarrollar esta arquitectura trasciende la ciencia e ingieneria individualmente. Lo mejor de ambos campos es combinado: avances científicos, conocimiento conceptual y nociones teoréticas son combinadas con la implementación práctica y pruebas minuciosas que son estándar en el ámbito de ingeniería espacial y eléctrica.

Con el objetivo de hacer esta tesis más accesible para ambos cientéficos e ingenieros, el segundo y tercer capítulo introducen el tema a tratar y definen el modelo de tolerancia a fallos tratado en esta tesis. El segundo capítulo sirve como motivación de la tesis, y presenta un resumen breve sobre aspectos claves del vuelo espacial y conceptos relacionados a la arquitectura de computadoras con tolerancia a fallos. Para poder diseñar y desarrollar efectivas y eficientes computadoras a bordo de satélites con tolerancia a fallos, se necesita entender los efectos del ambiente espacial en computadoras. Por ello, el tercer capitulo detalla estos efectos, las restricciones en el diseño de dispositivos electrónicos para el espacio, y las consideraciones necesarias durante misiones espaciales, tales como tiempos de comunicación y mecánica celeste.

Con base en los capítulos anteriores, el cuarto capítulo presenta una arquitectura de computadora que combina conceptos de tolerancia a fallos implementados via software junto con reconfiguración de arreglo de compuertas programables en el campo, o FPGA[2] y criticalidad mixta. A esto se le agrega otras medidas más convencionales de tolerancia a fallos y corrección de errores. Tolerancia a fallos en esta arquitectura es implementada mediante varias etapas entrelazadas que permiten una computadora a bordo de una nave espacial envejecer con elegancia.

Para hacer posible toda esta funcionalidad, se utiliza la ejecución sincronizada periódicamente (coarse-grained lockstep) implementada mediante software, lo cual está descrito en detalle en el cuarto capítulo. Esta funcionalidad por si sola ofrece una fuerte capacidad para tolerancia a fallos, pero sería insuficiente para recuperar misiones de larga duración. Por ello, en el quinto capítulo, se describe como la lógica reconfigurable puede ser utilizada para reuperar un sistema defectuoso causado por una variedad de fallas. Se utiliza un FPGA reconfigurable para asegurar la integridad del diseño del sistema en chip, con el objetivo de extender la vida útil de una computadora a bordo de una nave espacial, y maximizar la cobertura contra fallos de los recursos de repuesto. En misiones espaciales de larga duración, partes defectivas de un FPGA eventualmente no podrán ser recuperables mediante reconfiguración. Por ende, la cantidad disponible de lógica programable intacta dentro de los sistemas a bordo disminuye con el tiempo. En el sexto capítulo, se demuestra como la criticalidad mixta permite a una computadora adaptarse a la degradación, en lugar de fallar espontáneamente como lo hacen sistemas tradicionales. Esta funcionalidad se puede utilizar para intercambiar rendimiento con ahorro de energía y robustez autónoma durante el tiempo de ejecución. Esto permite que la funcionalidad central del software de vuelo sea protegida cuando fallos ocurren, logrando envejecimiento con elegancia y reuniendo recursos de repuesto para maximizar supervivencia.

Toda esta funcionalidad existe como software, y es ejecutada en un sistema en chip con un multiprocesador implementado dentro de un FPGA. El software, información sobre la carga útil, y la lógica programada dentro de un FPGA son datos, la integridad de los cuales debe ser protegida durante la duración de la misión. El sétimo capítulo describe conceptos para la protección de las diferentes tecnologias de memoria

[2]Arreglo de compuertas programable en el campo, o FPGA por sus siglas en inglés.

presentes a bordo de un satélite moderno.

Conceptos previos de tolerancia a fallos basados en software que se pueden aplicar a semiconductores modernos parecen funcionar en teoría. Sin embargo, estos resultan ser imprácticos para aplicaciones reales. Hasta la fecha de esta tesis no se ha implementado y validado tales conceptos en práctica, pero esto es un paso crítico y necesario. Los capítulos del ocho al diez detallan la implementación y validació del método de la arquitectura presentada en esta tesis.

La funcionalidad de lockstep utilizada en la arquitectura de esta tesis es validada mediante el método de injección de fallas en el octavo capítulo. En el noveno capítulo, se describe un diseño de un sistema en chip con multi-procesador implementado en un FPGA que sirve como plataforma ideal para la arquitectura presentada en esta tesis. El décimo capítulo se dedica a la implementación práctica de los conceptos y diseños descritos en los capítulos anteriores. De esta manera, se demuestra como una computadora a bordo de una nave espacial con esta arquitectura puede ser en la realidad, con la prueba de concepto construida a base de placas de desarrollo. Esto fue hecho con seis FPGA de Xilinx:

- Kintex UltraScale KU60,
- Kintex UltraScale+ KU11p, KU3p, el KU5p de la placa de desarrollo Xilinx KCU116, y el
- Virtex UltraScale+ VU9P de la placa de desarrollo Xilinx VCU118.

Para tres de estos FPGA, KU60, KU11p, y KU3p, datos detallados sobre utilización y consumo de energía son proporcionados.

Conclusiones

La pregunta principal de esta tesis es:

¿Se puede lograr una arquitectura de computadora con tolerancia a fallos utilizando tecnologias modernas integradas y móviles, sin quebrar las restricciones de masa, dimensiones, complejidad y presupuesto para aplicaciones con satélites miniaturizados?

Un doctorado, varios artículos publicados, y varias catástrofes después, ahora es posible responder esta pregunta de la siguiente manera:

Sí. *Una arquitectura de computadora con tolerancia a fallos para satélites miniaturizados es técnicamente factible con tecnología contemporánea de nivel industrial y para el consumidor. Cuando el prototipo esté completamente implementado, se podrá utilizar para extender drásticamente la vida de CubeSats modernos, y así permitir su uso en misiones espaciales críticas y de larga duración.*

Los componentes de software para la arquitectura presentada en esta tesis pueden ser implementados de manera no invasiva. Estos proveen protección para las aplicaciones pre-existentes sin la necesidad de escribir software específicamente para esta arquitectura. Utilizando software se demuestra que estos mecanismos pueden detectar fallos rápidamente y con alta probabilidad, y que se puede recuperar exitósamente de fallos con bajos costos computacionales en la mayoria de casos. Se demuestra que el

costo de rendimiento de esta arquitectura es económico, y permanence efectivo aún cuando opera en ambientes espaciales con fuerte irradiación.

Con componentes comerciales contemporáneos, un diseño de sistema en chip que funciona como plataforma ideal para esta arquitectura puede ser implementado aún en el FPGA Ultrascale+ más pequeño, con solo un consumo de 1.94 W de energía. Por ello, esta arquitectura de computadora a bordo de una nave espacial puede ser aplicada a CubeSats con dimensiones mínimas de 2U.

A medida que escala con la tecnología, avances en fabricación de semiconductores en la siguiente generación de FPGA hara el método presentado en esta tesis aún más atractivo, y también podra proteger naves espaciales aún más pequeñas que 2U. La eficacia y escalabilidad pueden ser mejoradas cuando se implementa a bordo de naves espaciales más grandes y pesadas que se utilizan en la actualidad para ciencia y exploración espacial. En un futuro, quizás podamos explorar más alla de los límites del sistema solar.