Challenge Problems in Reliable Aerospace Electronic Systems

Microelectronics used for aerospace applications, whether for aircraft or spacecraft, are subject to a variety of stringent requirements that include, but are not limited to:

- Significant size, weight and power (SWaP) constraints.
- Extreme reliability requirements in often harsh operating environments such as radiation, temperature, humidity, shock, or vibration. For example, many systems must be able to operate in the natural space or upper atmosphere radiation environment and many military systems must also be able to survive and operate in the radiation environment created by the detonation of nuclear weapons.
- High performance requirements based on the need for real time data signal processing and/or high data storage capability.

The failure or even transient mal-operation of a device in a critical circuit could result in either the loss of a satellite or prolonged unavailability, both of which could have severe economic or national security implications. Although the general scenario for an aircraft is less severe, microelectronics failures can also result in costly downtime and extreme passenger inconvenience with attendant deleterious economic impact.

Because of the extreme operating environment and the strict safety or mission requirements, it is easy to pigeonhole aerospace systems as an extreme exception to normal computational systems. As many aerospace organizations are often using the same or similar hardware as other consumers of commercial electronics, aerospace systems are a canary for impending reliability problems in other types of systems. Already, we have found similar problems in large-scale terrestrial applications, as the lessons learned from aerospace systems did not transition to supercomputer design. Without changes to system design, smaller safety-critical systems, such as medical and automotive technologies, will have more reliability issues as technologies scale. Therefore, the challenges that aerospace designers are facing currently are very likely an indicator of how terrestrial and safety-critical systems will be in the future, if the reliability problems are allowed to worsen as technology scales.

In the following sections of this report we will identify and discuss the most critical challenges imposed on aerospace microelectronics by the conflicting needs that arise when one is faced with the requirement to provide a system based on simultaneous SWaP, reliability, performance and cost constraints.

1 Background

While many organizations that build aerospace computing systems are not electronics manufacturers, they do significant amounts of system-level design, making aerospace organizations some of the most expert consumers of electronics. Most organizations also undertake a great deal of the necessary environmental testing, including radiation, mechanical, and thermal testing, to ensure part and system reliability. Much of this data is being published openly in journals, such as the IEEE Transactions on Nuclear Science and IEEE Device and Materials Reliability. While there has been an increasing use of modeling tools for predicting radiation reliability of analog devices, these tools are not sophisticated enough to predict unexpected problems from bad design or manufacturing. For complex computational devices, such as field-programmable gate arrays (FPGAs), fault injection tools that simulate single-event upsets have been useful for predicting workload-specific behaviors, which have allowed organizations to use accelerated radiation experiments as a final verification tool instead of a discovery tool.

Since many organizations are trying to leverage as much commercial electronic technology as possible, the testing necessary to qualify devices for space and avionics programs puts them in a unique position to observe trends in both commercial and radiation-hardened technology. Modern SRAM devices often not only suffer from single-event upsets, but shrinking feature sizes have caused multiple-bit upsets to dominate [14, 11]. Both SRAM and DRAM memory devices are often plagued with either single-event latchup or high-current events that force the device to be frequently rebooted to avoid permanent device destruction, and single-event functional interrupts can cause widespread corruption of the memory array that stymie the most commonly used error correcting codes [15, 10, 13]. Many organizations are trying to use commercial computation devices, such as microprocessors and FPGAs, to increase the amount of computation that can be done in-situ before sending data off system [8]. Commercial devices have problems with single-event latchup and are particularly sensitive to accumulated dose effects, such as total ionizing dose and displacement damage [6, 5]. FPGAs can have a complex array of single-event functional interrupts, single-event transients and single-event upsets that cause device availability and data reliability issues [12, 3, 17]. As commercial computational components become more common in space systems, commercial analog devices for data movement have become more common. While commercial analog devices can provide faster data rates than radiation-hardened analog devices, commercial analog devices often experience single-event latchup in high radiation environments. Furthermore, many radiation problems are interlocked with power and thermal problems, where increases in temperature and decreases in voltage can cause a non-linear increase in radiation sensitivity [4].

In the next two sections we will discuss specific challenges for satellites and airplanes separately. For the remaining document, the discussion will summarize common challenge problems and potential solutions.

2 Satellite Overview

In comparison to traditional computing systems, satellite systems are relatively “flat” systems. Often, most of the computation is done in specialized hardware using a real-time operating system and very little software. Satellites can have complex hardware designs with relatively little use of software. As it is, many current satellites do not have enough software to make complex decisions and are commanded manually. On top of it, large satellites with multi-organization, multi-country collaborations often maintain isolation between separate sub-systems and limit manually commanding the individual instruments. In smaller satellites, much of the fault-protection system can be reduced to putting the system into a “safe state” by turning the satellite to the sun and waiting for a manual command from the ground station. While more autonomous satellites are desired, the satellite would need to be able to make complex and reliable decisions on error-prone hardware. On one hand, automating some decisions will allow for quicker response in cases where the instruments might be damaged, such as overriding commands that could potentially damage instruments. On the other hand, there remain concerns that mal-functioning satellites can either potentially damage other spacecraft [1] or reveal sensitive information or hardware to other countries [2].

Future planned and envisioned spacecraft pose a number of unique challenges concerning microelectronics that can be delineated into two distinct categories:

- Traditional spacecraft are generally large and very costly systems that are expected to last for at least a decade on orbit. For example, this class of spacecraft can weigh more than 10,000 pounds, cost over $1B USD/satellite, take a decade to build, last longer than a decade on orbit, and be a multi-national collaboration with dozens of payloads. Satellites are deployed to accomplish specific missions, such as navigation (GPS), communications (Cable TV), intelligence gathering, or weather forecasting (NOAA).
- Micro or mini satellites are small satellites specifically designed for short duration missions. This class of spacecraft can weigh less than 100 pounds, cost $25M USD/satellite to build, take years to build, and last two to three years on orbit. Small satellites might only achieve one mission, such as a space weather experiment or a specific surveillance need. Small satellites might need to operate in a "swarm" of similar satellites to accomplish an overall mission.

The microelectronic challenges for each are somewhat different but equally daunting. Both are discussed in the following sections.

2.1 New Challenges for Traditional Spacecraft

Emerging requirements for this class of spacecraft now call for extending mission life to greater than 15 years and flexible payload capabilities. In addition, to provide a better remote sensing capability many satellites will be required to either operate in a Medium Earth Orbit (MEO) at 2,000–25,000 kilometers above the earth or a prolonged South-Atlantic Anomaly (SAA) environment [18] which will impose the need for increased radiation hardening and fault tolerance.

Typical payload needs involve phased array antennas that may require significant on-board signal and data processing, which in the end will also drive a commensurate increase in data-storage capability; "smart" power management and distribution systems; far more capable command, control and data handling for the spacecraft; and built-in payload flexibility through hardware and software reconfiguration. In order to meet the processing needs, it will be necessary to employ an increasing number of advanced microelectronics devices, including > 500 MIPS microprocessors, solid state recorders, Gb SDRAMS, > 14-bit ADCs, > 1 Mgate SRAM-based FPGAs and other types of deep submicron (< 130 nm) devices with little or no space heritage and that are not, in general, designed for either high reliability or radiation exposure. Based on this increasing dependence on commercial technology, a "layered" approach to fault mitigation and tolerance will be needed for large-scale satellites systems. Already, there are some point solutions of using multiple devices to increase reliability, such as memory or FPGA scrubbing devices [7] that remove errors from memory-based devices. For FPGAs, the scrubbing circuit plays the role of a watchdog that monitors the state of the health of the other device. In addition, improved and cost-effective testing, screening and qualification approaches will be needed.

Thus, the basic challenges for the advanced technology microelectronics for this class of system are:

- Reducing the cost of testing and qualifying components and instruments for space

- Allowing for more systematic and complete exploration of reliability, robustness, and performance while reducing design time and costs
- Removing the isolation between design layers which prevent opportunities for synergistic, multi-layer system optimization resulting in reduced capabilities in size/weight/power/reliability envelope

2.2 Micro/Mini Satellite Challenges

While many of the above noted challenges apply, there are a few added ones imposed by this class of spacecraft. The challenges for small satellites include, but are not limited to:

- The need for increasingly robust microelectronics based on the added vulnerability from the use of composite materials for the satellite structure that are thinner and lighter than previous materials used. As these materials provide less shielding from radiation, devices will experience an increase of radiation effects from single-event effects and the accumulation of dose.
- Multi-dimensional design tools that can address satellite “swarm” availability and performance requirements to simultaneously optimize performance, number of assets required, and individual asset requirements/capability.

2.3 Space Discussion

Based on the above discussion concerning satellite system needs, we can provide a listing of cross-layer challenges that must be addressed to support future aerospace microelectronics and electronic system design. The satellite-specific challenges include, but are not limited to:

- Reducing the cost of testing and qualifying components and instruments for space
- Allowing for more systematic and complete exploration of reliability, robustness, performance, weight, and survivability while reducing design time and costs.
- Allowing for reliable circuit and sub-system designs using state-of-the-art hardware, including multicore processors, so that mission requirements for reliability and radiation robustness can be met with modern hardware devices.
- Calculating overall system fault grading and composable error rates/failure estimates for multi-component systems.

Thus, it is recommended that a program that addresses cross-layer challenges be initiated.

3 Airplane Overview

Airplane systems have similar challenges to satellite systems, because many airborne applications use commercial electronics in harsher environments with longer life requirements than typical ground applications. Airplane systems contrast to space systems in that their usage environments may be less severe in terms of thermal extremes or radiation exposure, but more severe in terms of vibration and thermal cycling. Airplanes may have several cycles (takeoff, cruise, landing) daily and operate in a variety of locations with significantly different thermal, moisture and contaminant exposures. Unlike space systems, aircraft also have comparatively easy and frequent access to maintenance.

Reliability requirements for airborne electronic systems vary depending on the criticality of application, often characterized by three major levels: flight critical, mission critical, and non-critical. Flight critical applications are those involved with controlling flight, have the highest level of reliability and safety requirements, and often utilize older, established legacy electronics for which reliability can be assured. Mission critical applications in military aircraft are those involved with mission planning, identification and response to threats, situation awareness, and communication with other platforms. For airplane systems, performance and reliability are both important, but newer electronics are desired to provide faster, more accurate, and more detailed solutions. Multilevel reliability and fault tolerance are important considerations for mission critical applications. Non-critical applications are any other type of electronics, such as those providing office functions or passenger entertainment.

Although aircraft can have a platform life requirement of 30 years or more, the electronics on board may be replaced more often, and may have planned technology refresh cycles of 5 to 10 years.

3.1 New Challenges for Aircraft Applications

There is a growing dependence on Commercial-Off-The-Shelf (COTS) electronics in military and commercial aircraft platforms to provide unique, faster and more competitive functional capabilities while minimizing total ownership costs. As feature sizes decrease, electronics become more susceptible to airborne environments, especially atmospheric radiation. Newer technologies (< 100 nm) may have shorter expected life than required or needed, due to increased susceptibility to environmental fatigue factors.

Some specific airplane challenge areas:

- Environmental qualification and testing to provide reliability of commercial electronics in airborne environments.
- Security and prevention of unauthorized access or sabotage. This challenge may drive additional fault-tolerance measures incorporated in a multi-layer system design.
- Lightweight solutions that tolerate increasing aging effects and in-system device failures. Examples might include multi-layer data integrity assurance features, such as health monitoring, troubleshooting and health management features. Reliability sensors and/or circuitry designed to indicate exposure levels to harsh environments (e.g. “cage canary” circuits) could help in this.
- Efficiently addressing a wide range of reliability requirements. This might suggest tunable reliability, where the ability to tune in high-reliability features or not would allow the airplane or the operator to change the reliability of the system depending on mission needs at different times (e.g. ability to go to “red alert”).

4 Discussion of Challenge Problems

There are a number of challenge problems identified by the Aerospace working group:

- Widening Gap Between Mil/Aero and Commercial Parts
- Design for Worst-Case Environment
- Multidimensional Optimization Problem
- Testing Bottleneck
- Part vs. System Reliability
- Flexible Mission/Science vs. Fixed Capabilities
- Assuring Supply Chain
- Increased Aging Effects

An overview of the aerospace challenge problems is provided below.

Widening Gap Between Mil/Aero and Commercial Parts: Over the years, radiation-hardened space technologies have lagged commercial technologies by as much as 10–20 years. Despite the fact that existing defense and space semiconductor markets are becoming increasingly nonviable, a recent push for “trusted foundry” [16] electronics are forcing designers to use Mil/Aero devices. Leveraging commercial technologies would allow designers to employ more aggressive components in aerospace systems, but would require part- and system-mitigation techniques.

Design for Worst-Case Environment: Many satellites are expected to endure years in a harsh radiation environments with rapid temperature cycling and an initial intense vibration. Airplanes are also designed for a similar environment with more mechanical problems caused by repeated turbulence and landing conditions. As many designers are margining for worst-cases in thermal, radiation, and mechanical situations, it is possible that designers will margin for the scenario when all three areas are in problematic scenarios at once, which could lead to extreme worst-case margining for a scenario that is unlikely to occur.

Multidimensional Optimization Problem: Most satellite/avionics designers are trying to optimize performance, reliability, power, thermal and weight. Mission requirements often impose fixed hard limits on power, thermal, reliability and weight. Optimizing these limits can be very hard to manage as changes along one dimension (power, thermal, reliability, weight) affect the other dimensions. Furthermore, the power, thermal, reliability, and weight problems are often the responsibility of different teams with different skill sets. As no tool currently exists to optimize all of the problems at one time, it is currently done manually. While experienced systems-design teams often come to very good solutions, the tendency is to over-design the system.

While there is a low power density for space, aircraft have a far less constrained power supply. Unfortunately, more powerful systems often translate to heavier systems and heavier systems cost more money to fly. Therefore, minimizing weight for airplanes is necessary.

Testing Bottleneck: Many organizations are responsible for initial environmental testing to determine worst-case reliability calculations in an attempt to eliminate parts that will not meet mission requirements or be too difficult to work with. The advantage of using Mil/Aero or “heritage” parts (i.e., devices used in previous space missions) is that initial testing can be eliminated or minimized. The disadvantage of using commercial parts is that often times the organization will need to do all of the initial environmental testing, which can be costly. In recent years, dynamic testing to determine workload-specific reliability has become necessary. For some devices, such as FPGAs, fault injection can be helpful in minimizing the testing burden for dynamic testing. Because inadequate/incomplete testing can lead to a false security and in-field system failures, most organizations will pay to get it right, which leads to conservative over-design or over-testing of the system.

Part vs. System Reliability: System reliability is often considered intractable, so many organizations focus on part reliability. While part-specific error mitigation methods can be useful and should be encouraged, there are only a few point solutions available for solving reliability problems at a system level. The side effect of this situation is that it encourages wide "margin of error" design practices that can lead to slow, heavy, power-hungry, and expensive solutions.

Flexible Mission/Science vs. Fixed Capabilities: Currently, the science and national security concerns that drive our space programs change several times over the course of a satellite's lifetime. Most satellites are commissioned and designed for a specific science and/or national mission need and the only access to post-deployment changes are through software. On top of it, satellites can be damaged during and after deployment, making them unusable. Due to the growing need for "opportunistic" missions, many satellite operators do attempt to make "heroic" changes to the satellite to collect necessary data, which can irreparably damage a satellite. The only current solution is to launch new satellites, which could cost billions and take years to build. More adaptive satellite design could weather changes in the science, the mission, and the satellite while deployed.

There is a similar need in airplanes to be more flexible. Currently, even minor modifications to the software of an airplane can force the airplane to be re-certified. As re-certification can take months, this situation deprives designers of the ability to use late-bound information to change the system for the better.

Assuring Supply Chain: For the military and national security missions, guaranteeing that parts are not counterfeit or have not been tampered with has become difficult. This problem has lead to heavy reliance on trusted foundry hardware.

Increased Aging Effects Newer technologies (< 100 nm) may have expected lifetimes that are too short to be economically accommodated, demanding frequent manual repair and/or excessive over-provisioning of resources. These shorter lifetimes arise from increasing susceptibility to environmental fatigue factors and aging mechanisms [9]. Without new mitigation techniques, this could prevent access to advanced technologies.

The above set of problems leads to a culture of conservative over-design of aerospace systems. The aerospace community is often forced to avoid deploying new electronics that could enable better in-situ processing and/or decision making. Currently, our satellites are becoming rapidly overburdened. Over the past decade as our threats have increased, the need for more satellite coverage and more data collection has out-stripped our satellites' capacities. At the same time, other countries have found access to space easier, as these countries are not as concerned with mission failure. Even though we are currently technologically superior to nearly every other nation in space, this gap could close rapidly. Conservative, manual over-design to meet strict mission requirements will not help us remain technologically superior. Remaining technically aggressive by leveraging new computational technology with shorter lifetime and experimental spacecraft will help us not only maintain our technological superiority but can increase national security at the same time. Doing this responsibly demands that we find suitable system-level techniques to mitigate the reliability problems of modern, commercial technologies so that system reliability goals are not compromised in the process.

5 Potential Solutions

The working group proposed and discussed a number of solutions to the challenges described above. These discussions are detailed below for reference, but they should be no way regarded as a complete discussion of potential approaches.

Modeling the (Performance, Reliability, Power, Thermal) Tradespace: By encapsulating information from the devices, designers can work at the system level, instead of at the part level. To be able to help designers, modeling tools that manage the complexity of these problems are needed:

- Memory architecture solutions for known device sensitivities
- System reliability analysis
- (Reliability, Performance, Power, Temperature) optimization
- Methods for managing multiple reliability problems
- Simulation of lifetime aging problems
- "Day in the Life" simulations

Agile Satellite Solutions: By using adaptive or multi-level reliability solutions, satellite capabilities would not be as static. More adaptable satellites would be able to change reliability requirements over different phases of the mission life. By linking satellites to radiation monitoring systems (either in the loop or data updates from ground stations), the spacecraft should be able to adapt to changing space weather conditions once a threshold for corrective action is met. Furthermore, multi-level reliability solutions that use either software-based hardware checking for fault tolerance, such as the Hubble servicing mission, or reconfiguration to adapt to space weather, lifetime aging, and science changes will create more flexible satellites. Finally, to make this type of satellite work, autonomous analysis tools and methods for assuring continued functionality are needed.

Multi-Core Solutions that Address a Wide Application Space: Currently, many aerospace organizations are catching up to multi-core computing. At this stage, there is very little understanding about how multicore devices will work in high-reliability environments. As long as common failure modes are not likely, many possible mitigation strategies will exist, but there is currently not enough information about multicore-specific failure modes.

Dual Purpose Reliable and Secure Computing Solutions: Many of the same ideas that researchers have been working on for reliability would also be good for security. In particular, fault encapsulation could be useful for both reliability and security by keeping intentional or random errors from hurting the data or the system. Tools that can handle both problems are needed as well. Combined reliability/security tools will allow designers to achieve both secure and reliable designs, will provide test methodologies (modeling, fault injection, field tests) to validate systems, and will provide system tests for in-field operation.

6 Conclusions

In this paper, we have presented a number of challenges that face aerospace designers. Due to the strict constraints on aerospace systems and the harsh operating environments, designers are often trying to find the best solution to multiple reliability problems. The use of cross-layer reliability solutions would allow designers to build more flexible and agile systems that would allow them to adapt to the many challenges ahead for aerospace systems.

References

[1] Intelsat rogue satellite: Nothing to worry about. http://www.networkworld.com/community/node/61291 last accessed on May 17, 2010.

[2] U.S. to shoot down satellite wednesday, official says. http://www.cnn.com/2008/TECH/space/02/19/satellite.shootdown/index.html last accessed on May 17, 2010.

[3] Greg Allen, Gary Swift, and Carl Carmichael. Virtex-4VQ static SEU characterization summary. Technical Report 1, Xilinx Radiation Test Consortium, 2008.

[4] J.M. Armani, G. Simon, and P. Poirot. Low-energy neutron sensitivity of recent generation SRAMs. *Nuclear Science, IEEE Transactions on*, 51(5):2811–2816, Oct. 2004.

[5] H.J. Barnaby, C.R. Cirba, R.D. Schrimpf, D.M. Fleetwood, R.L. Pease, M.R. Shaneyfelt, T. Turflinger, J.F. Krieg, and M.C. Maher. Origins of total-dose response variability in linear bipolar microcircuits. *Nuclear Science, IEEE Transactions on*, 47(6):2342–2349, Dec 2000.

[6] H.J. Barnaby, R.D. Schrimpf, A.L. Sternberg, V. Berthe, C.R. Cirba, and R.L. Pease. Proton radiation response mechanisms in bipolar analog circuits. *Nuclear Science, IEEE Transactions on*, 48(6):2074–2080, Dec 2001.

[7] M. Berg, C. Poivey, D. Petrick, D. Espinosa, A. Lesea, K.A. LaBel, M. Friendlich, H. Kim, and A. Phan. Effectiveness of internal versus external SEU scrubbing mitigation strategies in a Xilinx FPGA: Design, test, and analysis. *Nuclear Science, IEEE Transactions on*, 55(4):2259–2266, Aug. 2008.

[8] M. Caffrey, W. Howes, D. Roussel-Dupre, S. Robinson, A. Nelson, A. Salazar, M. Wirthlin, and D. Richins. On-orbit flight results from the reconfigurable Cibola flight experiment satellite (CFESat). In *Field-Programmable Custom Computing Machines 2009*, 2009.

[9] L. Condra, J. Qin, and J.B. Bernstein. State of the art semiconductor devices in future aerospace systems. In *Proceedings of the FAA/NASA/DoD Joint Council on Aging Aircraft Conference*, April 2007.

[10] J.-P. David, F. Bezerra, E. Lorfvre, T. Nuns, and C. Inguimbert. Light particle-induced single event degradation in SDRAMs. *Nuclear Science, IEEE Transactions on*, 53(6):3544–3549, Dec. 2006.

[11] G. Gasiot, D. Giot, and P. Roche. Multiple cell upsets as the key contribution to the total SER of 65 nm CMOS SRAMs and its dependence on well engineering. *Nuclear Science, IEEE Transactions on*, 54(6):2468–2473, Dec. 2007.

[12] Jeff George, Rocky Koga, Gary Swift, Greg Allen, Carl Carmichael, and Wei Tseng. Single event upsets in Xilinx Virtex-4 FPGA devices. In *Radiation Data Workshop of the Nuclear and Space Radiation Effects Conference*, pages 109–113, 2006.

[13] R. Harboe-Sorensen, F.-X. Guerre, and G. Lewis. Heavy-ion SEE test concept and results for DDR-II memories. *Nuclear Science, IEEE Transactions on*, 54(6):2125–2130, Dec. 2007.

[14] D. F. Heidel, P. W. Marshall, J. A. Pellish, K. P. Rodbell, K. A. LaBel, J. R. Schwank, S. E. Rauch, M. C. Hakey, M. D. Berg, C. M. Castaneda, P. E. Dodd, M. R. Friendlich, A. D. Phan, C. M. Seidleck, M. R. Shaneyfelt, and M. A. Xapsos. Single-event upsets and multiple-bit upsets on a 45 nm SOI SRAM. *Nuclear Science, IEEE Transactions on*, 56(6):3499–3504, Dec. 2009.

[15] P. Layton, S. Kniffin, S. Guertin, G. Swift, and S. Buchner. SEL induced latent damage, testing, and evaluation. *Nuclear Science, IEEE Transactions on*, 53(6):3153–3157, Dec. 2006.

[16] Richard McCormack. DOD broadens "trusted" foundry program to include microelectronics supply chain.

[17] Gary M. Swift. Virtex-II static SEU characterization. Technical Report 1, Xilinx Radiation Test Consortium, 2004.

[18] S. N. Vernov, E. V. Gorchakov, P. I. Shavrin, and K. N. Sharvina. Radiation belts in the region of the south-atlantic magnetic anomaly. *Space Science Review*, 7:490–533, 1967.