Not All Fault Containment Regions are the Same: How Apogee Semiconductor's RelBridge™ can limit the impact of COTS failures in Commercial Space

Mark Hamlyn, Greg Carr, Abhijeet Ghoshal, Josh Cortman, David Grant

In Affiliation With The Jet Propulsion Laboratory, California Institute of Technology

The entrepreneurial vision driving the NewSpace era has led to remarkable technological milestones in the last decade. Through innovative approaches and the integration of commercial off-the-shelf (COTS) components and technologies, new space operators are pushing the boundaries of economic viability, making the vision of commercial space exploration scalable and sustainable. This white paper illustrates how COTS components, when used in conjunction with Apogee Semiconductor's Relbridge™ components, can substantially enhance reliability to ensure success in commercial satellite missions.

Our thesis proposes that by integrating COTS components with RelBridge™ technology at strategically determined fault containment boundaries, the risk of a total system failure from electronic components can be effectively mitigated without a significant increase in spend on the electronic bill of materials (BOM). This improvement can be achieved by supplementing a fraction of the COTS BOM with RelBridge™ components resulting in an overall increase in the long-term return on investment (ROI) for NewSpace operators.

1 Market Overview

Over the past decade, the NewSpace or commercial space industry has experienced remarkable growth, primarily attributed to significant cost reductions in launching payloads into orbit. This reduction is driven by factors such as re-usability, cost-consciousness, and accelerated development cycles. The prime emergent players in the launch business include SpaceX, Rocket Lab, United Launch Alliance, Blue Origin, and Firefly Aerospace, each contributing unique innovations and advancements to the commercial space sector. As a result, an unprecedented number of companies are entering the commercial space market.

SpaceX's success in deploying cost-effective launch solutions and large satellite constellations exemplifies the industry's transformative commercial potential. In 2023 SpaceX successfully launched close to 100 Falcon 9 payloads to orbit (Figure 1), accounting for over 1200 metric tons of mass. This number is approximately three times greater than the rest of the planet combined (Figure 2). In 2024, SpaceX forecasts 150 launches which will eclipse the previous year's numbers [1].

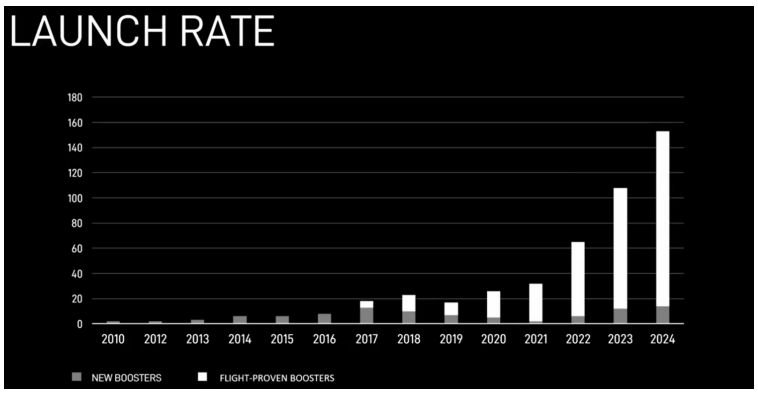

Figure 1: SpaceX Launch Rate [1]

More than 80% of total mass carried to orbit in 2023 was accounted for by Low Earth Orbit (LEO) Satellites [2]. A large portion of this was from SpaceX's Starlink satellites which make up large clusters of communication constellations used to provide millions of subscribers with low latency high speed internet around the globe. A recent report by Quilty Space forecasts Starlink's 2024 revenue to exceed $6.5 billion USD, up from $1.4 billion USD in 2021. This data is a good indicator of the potential of this market, as only 12% of the planned constellation (42,000 satellites) is deployed at the time of publication [3].

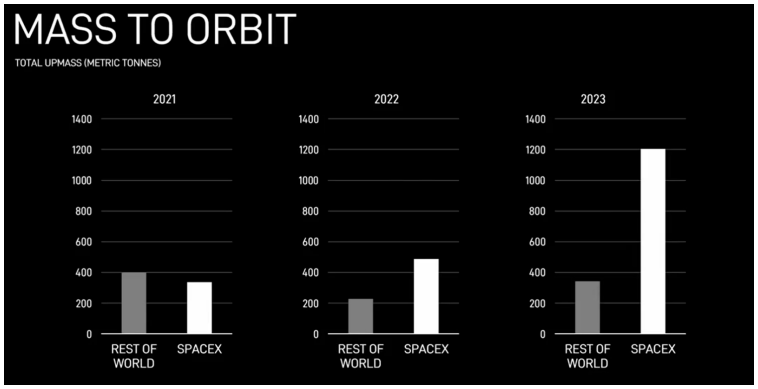

Figure 2: SpaceX Mass to Orbit Comparison [1]

SpaceX Falcon 9 and Falcon Heavy programs have introduced an order of magnitude reduction in launch cost. Prior to Falcon 9 launch cost was around $8,100 per kg via Atlas V. Falcon 9 reduced the cost to $2,600 per kg and Falcon 9 Heavy further reduced cost to $1,500 per kg [4]. Starship is intended to further

reduce launch cost by an additional order of magnitude to somewhere between $10-$150 per kg [5]. Other launch vehicles like New Glenn from Blue Origin and Neutron from Rocket Lab are also driving launch cost competitiveness. This reduction in launch cost is a key driver for the growing commercial space market, which in turn is fueling the increased use of COTS components.

2 Challenges of COTS in Commercial Space

COTS refers to readily available components that are manufactured for broad commercial applications and sold through commercial distribution channels. These components are standardized products not specifically tailored for space applications that are often orders of magnitude less expensive than radiation hardened military grade components. Additionally, COTS provide state-of-the-art electrical performance since their design and manufacturing are driven by current market forces. Although COTS are designed for terrestrial applications, commercial space companies have been increasingly adopting them over traditional military grade components. This is primarily driven by the emerging need to create higher performance but lower cost systems for the new commercial space market, with some companies targeting up to a 10% reduction in total cost.

The benefits of using COTS components for new space systems are substantial. However, the associated risks, particularly from radiation exposure in space cannot be ignored. Effective mitigation of these risks is crucial to prevent hardware failures that could lead to significant financial losses, especially for NewSpace companies planning large constellations or critical missions. For example, if a service provider launches a constellation of 13,000 satellites at a cost of $1M per satellite (including amortized launch costs), a 2% failure rate would result in the loss of 260 satellites. This would equate to a loss of over $260M, not including the opportunity cost and the cost to launch additional satellites. LEO commercial space operators may underestimate the acceptable failure rate since they are mostly in the development phase. As the industry matures, the increased growth in revenue and customer base that needs to be protected will drive a lower risk appetite. Additionally, the trends in insurance underwriting for LEO missions means that providers must adopt more robust risk mitigation strategies to protect their investments and reduce potential costs. Addressing the vulnerabilities associated with COTS components is vital for the long-term success and sustainability of space missions [6].

COTS components are not designed for the space environment. The use of COTS components necessitates additional testing to ensure they can withstand space conditions, particularly radiation. This is referred to as ‘upscreening’. Traditional high reliability components rely on multiple stages of qualification and screening. This includes technology level qualification, radiation characterization, device qualification, lot level qualification, and burn-in. When space customers choose to use COTS, they often take on the cost and engineering overhead of the additional qualification and screening to meet the reliability requirements for their mission.

Radiation performance characterization is a significant driver for the final cost of upscreening. Electronic components in space are subjected to a harsh radiation environment that can degrade their performance through several mechanisms. One major mechanism is total ionizing dose (TID) effects, where prolonged exposure to ionizing radiation accumulates in the component’s materials, leading to shifts in electrical parameters and potential failure. Another critical mechanism is single event effects (SEEs), caused by single high-energy particle strikes, which can induce single event transients (SET), single event latch-up (SEL), or even permanent damage to the components. The cumulative impact of these radiation-induced mechanisms can lead to increased leakage currents, threshold voltage shifts, and reduced operational lifespans, ultimately compromising the reliability and functionality of COTS components in space applications.

In addition to the cost, the methodology of radiation characterization also poses a challenge for end users due to a lack of insight into the IC design process compounded by the lack of support from COTS manufacturers. A common result that engineers observe when performing heavy ion SEL is non-destructive latch up events. It would be easy to assume that if the part recovers after cycling power that it would be suitable for space missions since no catastrophic consequences were immediately observed. To fully appreciate the potential consequences of selecting a part that has demonstrated non-destructive latchup susceptibility, it is important to understand that IC designers never design an IC with the expectation that it will latchup. In practice, IC designers set internal metal widths in the IC based on process electromigration

capabilities and expected currents for normal operating conditions. When latchup occurs, currents in the IC can easily exceed the specified maximum operating current. If latchup is caused by a SEL, whether the event is immediately catastrophic depends on the size of the internal metal traces at the location of the ion passage and the duration of the exposure. So although not immediately catastrophic, non-destructive SEL can cause substantially larger currents than the IC's internal metal traces were designed to handle, leading to premature IC degradation and early failure. To have a complete understanding of the life expectancy of any component that shows non-destructive SEL, a carefully designed reliability study on a population of ICs using accelerated testing would be required to extrapolate post SEL current exposure failure in time (FIT) rates, which is unlikely to be performed as it would be cost prohibitive [7].

3 Fault Containment Boundaries

Due to the unpredictable behavior of COTS components in radiation-rich environments, it's important to design a system which can tolerate failures. There are various architectural approaches which could be implemented depending on the level of fault tolerance for a given subsystem and its mission.

The highest risk architecture, particularly for critical subsystems like power conversion, is to design them as single string or no-fault tolerant (Figure 3). If one part in the subsystem fails, the entire subsystem is no longer functional and there is no backup. This may be appropriate for non-critical systems on short-duration missions, but for any other condition, a level of fault tolerance will be desirable.

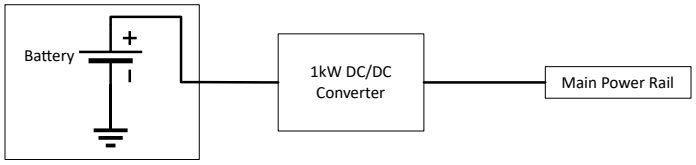

Figure 3: Single String Block Diagram

To build a fault tolerant system, it is necessary to understand the concept of a fault containment boundary. When designed properly, a fault containment boundary allows for the failure of circuitry within the boundary without the failure impacting surrounding circuitry. A fault tolerant system can be built with COTS if fault boundaries are maintained in the proper locations and some level of redundancy is implemented. This allows for the use of COTS parts within each fault containment boundary where a single failure won't take out the entire functionality of the subsystem.

The simplest way to achieve single fault tolerance is block redundancy or a 2N approach where N is the total capacity need of the subsystem (Figure 4). While this is a significant reliability improvement, it results in twice the component cost and mass.

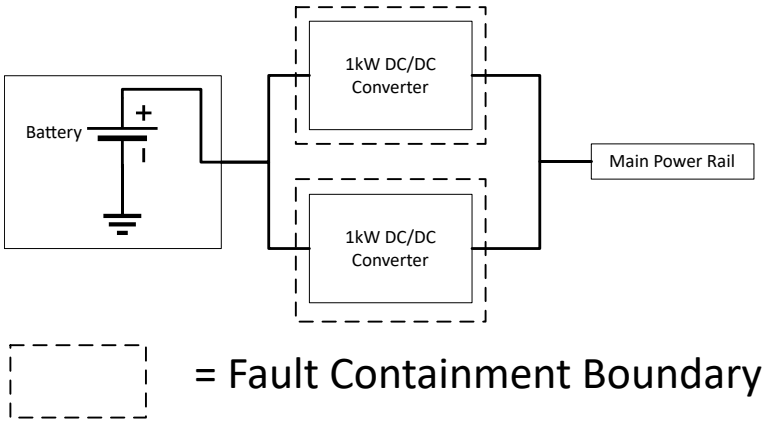

Figure 4: Block Redundant or 2N Block Diagram

A more cost and mass efficient approach is a N+k approach where k is a backup which can act as a hot or cold spare (Figure 5).

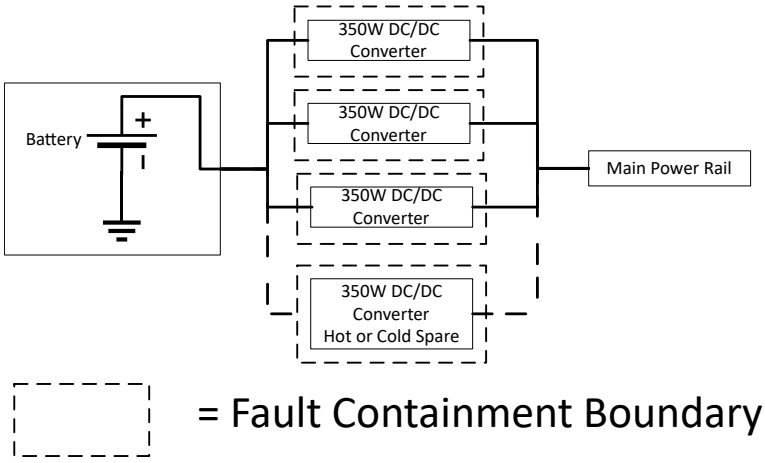

Figure 5: N+k Block Diagram

4 NASA's Architectural Approach to Fault Containment

NASA's approach to building highly reliable systems has evolved over time. In the past, NASA did not use COTS components due to extreme fault tolerance requirements placed upon their missions. In more recent years, NASA has adopted additional risk, particularly on experimental missions, including the use of upscreened COTS components. Architectural redundancy and fault tolerance strategies are implemented to maintain overall system reliability. The document *Recommendations on the Use of Commercial-Off-The-Shelf (COTS) Electrical, Electronic, and Electromechanical (EEE) Parts for NASA Missions – Phase II* [8] contains a detailed outline of how NASA approaches COTS screening to reduce cost and achieve higher electrical performance while maintaining a highly reliable system. A variety of architectural approaches were implemented in some of NASA's recent missions.

NASA has performed several high risk missions including Mars Pathfinder and Ingenuity in order to demonstrate new technology. It was agreed at the beginning of the development to accept risk in order to demonstrate a new technology within a rover or helicopter on Mars. The overall cost of each mission was low enough to accept additional risk. However, once the technology has been demonstrated; the follow-on missions have the standard expectation of first pass success. The Mars Exploration Rovers (MER) were the follow-on after Pathfinder and needed to provide research data to justify the investment. The program decided to launch and fly two completely independent missions to get a return on their investment. The rovers were small enough so that the launch vehicle cost was not prohibitive. The penalty was flying double the mass resulting in an increase in cost.

The next mission after MER was the Mars Science Laboratory (MSL) with a more challenging science objective resulting in a very large and more capable rover. At this point, a double build and double launch would be cost prohibitive so a single fault tolerant approach was accepted to increase the reliability of the rover. Most of the avionics were single fault tolerant with selective redundancy for the instruments. Most of the non-avionic subsystems were block redundant (Figure 4) resulting in a significant mass increase for each block. Overall, the block redundant structure was still lower in mass than than two complete systems. As block redundancy was implemented, fault containment regions were set up to prevent single faults from propagating outside of each containment zone. The first boundary is at the subsystem level with each interface undergoing intensive analysis and scrutiny to make sure the faults are contained within the region. Development cost increases with each new interface, so standard re-usable interfaces are designed to reduce overall development cost.

Some deep space missions like Cassini or Europa Clipper cannot accept the mass penalty of block redundant subsystems and need to reduce the size of the fault containment regions to limit the system impact. Many of these missions utilize an "N+K" architecture (Figure 5). Cassini used a fault tolerant housekeeping power supply for the power subsystem with load level fault containment regions. The power distribution provided 192 loads and each one was a fault containment region. In order to prevent the coupling of the load level fault containment regions, the housekeeping power had to be single fault tolerant to each interface. This was achieved by designing the power supplies to be cross-strapped at the output with the appropriate fault protection to maintain the containment region. The design was able to have one out of the two supplies to be held off as cold spare to enhance the radiation resilience. The overall mass penalty for single fault tolerance was a small percentage of the single string version (10%) at the subsystem level. Standard buses and interfaces were used at the boundaries to reduce the cost of development and analysis (Figure 6).

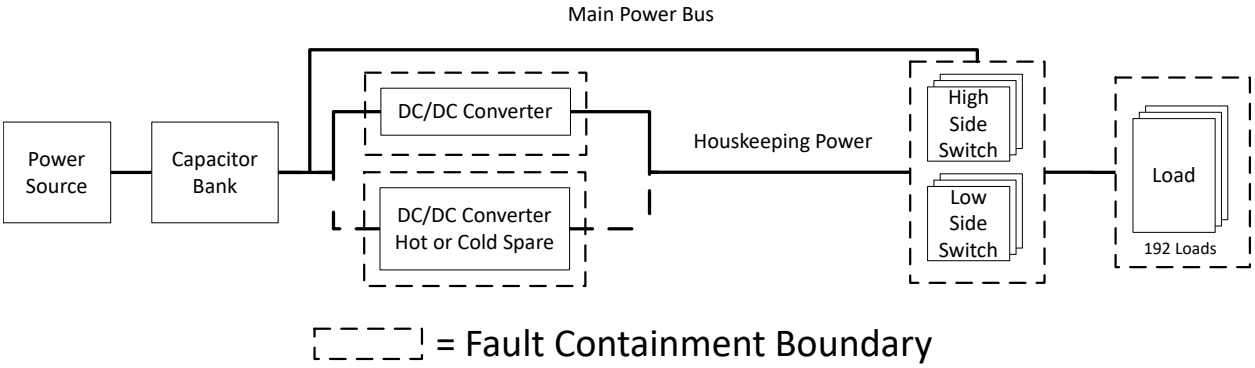

Figure 6: Cassini Block Diagram

The Europa Clipper Power Subsystem used a similar approach in the power control function. For the solar array power conversion, the subsystem used an architecture where it needed 3 out of 4 power converters to complete the mission. This results in a mass penalty of about 33% over the single string implementation for this function. As the system development matured, it turned out that the mission could be achieved with 2 out of 4 converters improving the overall reliability. The penalty at the subsystem level was closer to 20% overall.

One final example is that of Ingenuity, the first Mars helicopter. It had many significant challenges to the point that even the mass of a single string version with highly reliable components would be too much. The system had to rely on the smallest most compact components that could survive the environment. The first technology mission was accepted to be single string with the exception of functions or interfaces that could harm the host rover Perseverance. There were some functions that were designed to be fail safe off with few small fault containment regions. The battery charge function had single fault tolerant overcharge protection for safety on the ground and during the mission until it was released from the rover.

Future missions have two options, either deliver two complete copies similar to MER or develop a single tolerant approach similar to MSL. Either approach needs to use the most compact components available. For a larger helicopter, smaller fault containment regions with small footprints will be needed. The mass penalty for fault tolerance will need to be less than 10% similar to the deep space architectures to meet the stringent requirements of flight. The overall approach to system reliability is a combination of architecture and component reliability. The demanding requirements of a system could force an architecture with smaller fault containment regions to reduce the mass impact and still achieve the reliability goals. Implementing architectures with small fault containment regions and selective redundancy could enable the use of COTS components while maintaining higher reliability. The interfaces are key to improve the reliability and still maintain the overall cost.

5 Apogee Semiconductor's RelBridge™ components

Apogee Semiconductor's RelBridge™ components can be used throughout critical subsystems and at subsystem interfaces to help maintain reliability and cost effectiveness. RelBridge™ components are radiation-hardened by design offering first in class radiation performance for various logic functions which can be implemented throughout spacecraft and satellite subsystems.

The AP54RHC301 dual 3-input majority voter can be used to help with decision making in triplicated fault tolerant systems. One example of a possible application is shown in figure 7. This example shows the majority voter used in solar array switching to help maintain the fault containment boundary of each solar cell segment. Each solar cell is isolated by a bypass diode creating a fault containment region. Each string of solar cells is then isolated by a diode creating an additional containment region. Each segment is then contained by a switch which connects the segment to the main power rail. To allow for fault tolerance on the switch, it can be implemented with 4 total switches and a majority voter controlling each switch. These drive signals can be connected to a power controller to create a regulated power rail. This configuration ensures that if any switch gets stuck on or off, the segment can still be connected/disconnected. The AP54RHC301 can be used anywhere that highly reliable signal propagation is needed. Another example is UVLO sensing on the main power rail. Three UVLO sensors can be connected to the main power rail, then passed through a majority voter, then to the main FPGA for decision making. The majority voter can also be used as a dynamic "and"/"or" gate. If one of the three inputs is held high through a pull-up, the voter acts as an "or" gate. If that input is then pulled low, it acts as an "and" gate.

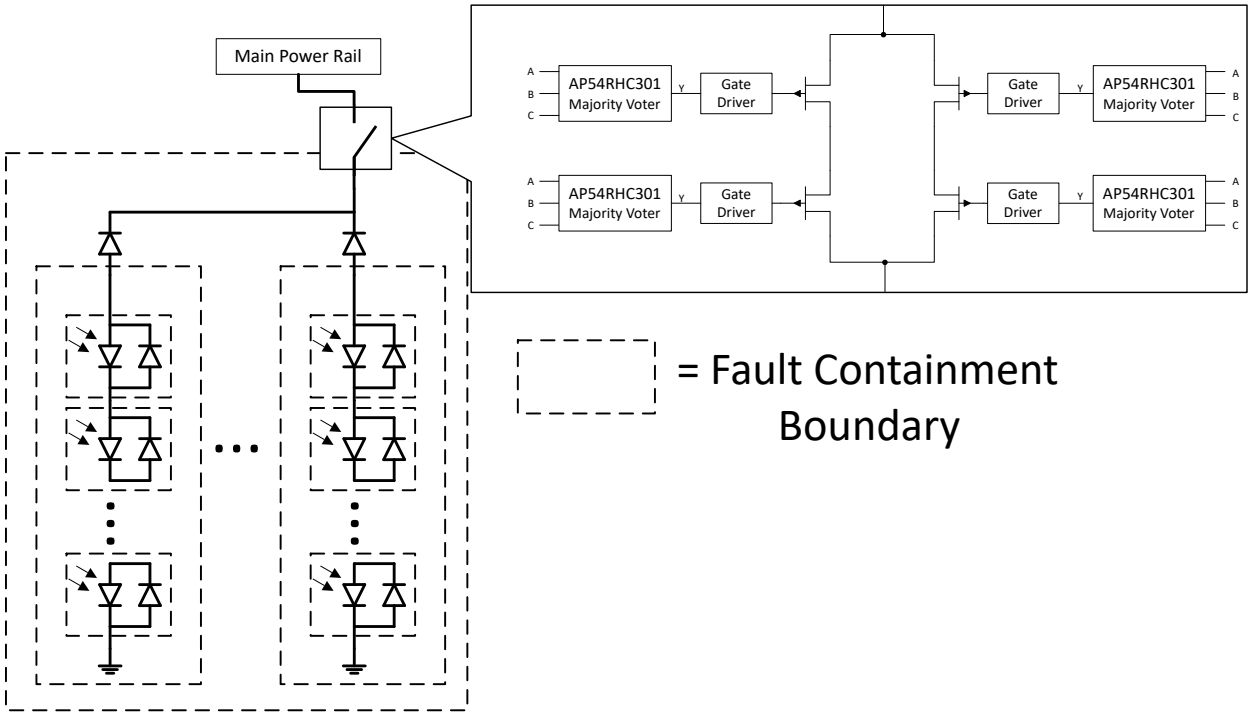

Figure 7: Example use case of the AP54RHC301 dual 3-input majority voter

Future NASA missions plan to use a power control architecture similar to what's shown in Figure 8. Both the AP54RHC301 dual 3-input majority voter and the AP54RHC164 8-bit shift register from the RelBridge™ family can be used to support this design. The AP54RHC164 is an 8-bit serial input parallel output (SIPO) shift register which is appropriate if the system can tolerate the timing constraints of reading data prior to the subsequent clock edge. Alternatively, the AF54RHC5942 8-bit shift register offers a latch input which allows the user to control when new data is shifted in. Both the AP54RHC164 and AF54RHC5942 use radiation-hardened dice latches which protect stored data from heavy-ions. These shift registers can be used to convert a data bus into multiple IO signals, ultimately saving routing space.

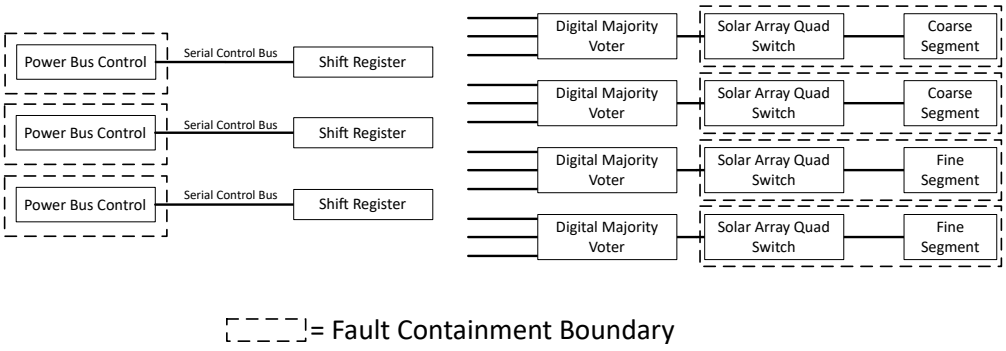

Figure 8: Bus Regulation For Future Missions

Another example from the RelBridge™ family is the AP54RHC288 two channel dual-input arbiter. Each channel of the arbiter passes two signals through and ensures that both are not high at the same time. This is helpful for preventing cross-conduction and shoot-through in series switches. Figure 9 shows an example use of the AP54RHC288 in a half bridge application. In this application, the AP54RHC288 ensures that both switches don't turn on at the same time helping to prevent shoot-through. The AP54RHC288 can be used in conjunction with COTS gate drivers and PWM controllers to increase the reliability of power converters like buck converters, half bridges, and full bridges. See this paper for more technical details on this type of application: *The Dangers of Cross-Conduction: Isolating Half-Bridge Faults with the AP54RHC288* [9]. The AP54RHC288 can also be used in stepper motor drive and three phase motor drive to ensure proper operation and prevent shoot-through.

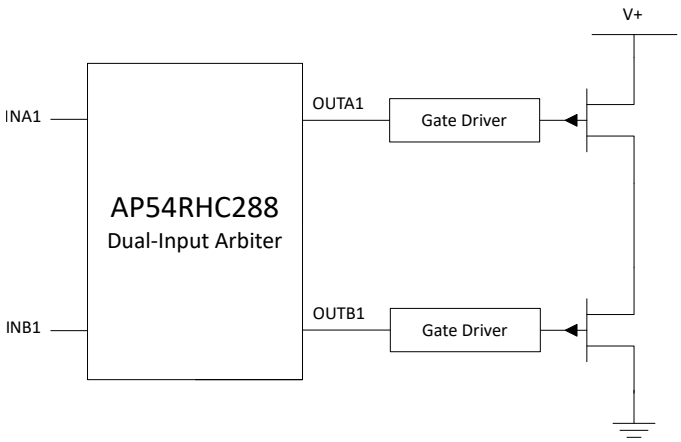

Figure 9: Example use case of the AP54RHC288 two channel dual-input arbiter

6 Summary

The reduced cost of launch is enabling a surge in the commercial space market. While the cost of launch has dropped dramatically and is expected to drop further, the same is not true for the cost of traditional radiation hardened electrical components. This has led commercial space system designers to adopt COTS components, with considerable success, but with increased failure rates.

The use of a wholly radiation hardened design is not acceptable from a performance and cost perspective. The use of a wholly COTS design has higher costs due to upscreening and degraded reliability. It is not necessary to go entirely one way or the other as not all fault containment regions are the same.

NASA has demonstrated considerable success in incorporating COTS components into highly reliable systems through careful selection of fault tolerant architectures based on mission risk tolerance. A nuanced approach can be implemented to leverage the cost and performance benefits of COTS while gaining significantly improved mission reliability through the use of radiation hardened components in key locations.

Apogee Semiconductor provides affordable radiation hardened components that can be used at subsytem boundaries and other critical locations to improve reliability and the ROI for the space system as a whole.

References

[1] SpaceX, "In 2023, spacex completed 96 successful missions, safely flew 12 more astronauts to orbit,launched two flight tests of starship, and more than doubled the number of people around the world connected by @starlink." *X (formerly Twitter)*, January 2024. [Online]. Available: https://x.com/SpaceX/status/1745941814165815717

[2] (2024, January) Recap of all global launches for 2023. Accessed: June 19, 2024. [Online]. Available: https://www.spaceworks.aero/recap-of-all-global-launches-for-2023/

[3] S. Erwin. (2024, May) Starlink soars: Spacex's satellite internet surprises analysts with $6.6 billion revenue projection. Accessed: June 6, 2024. [Online]. Available: https://spacenews.com/starlink-soars-spacexs-satellite-internet-surprises-analysts-with-6-6-billion-revenue-projection/

[4] T. Roberts. (2022, September) Space launch to low earth orbit: How much does it cost? Accessed: June 19, 2024. [Online]. Available: https://aerospace.csis.org/data/space-launch-to-low-earth-orbit-how-much-does-it-cost/

[5] B. Wang. (2024, January) How will spacex bring the cost to space down to $10 per kilogram from over $1000 per kilogram? Accessed: June 19, 2024. [Online]. Available: https://www.nextbigfuture.com/2024/01/how-will-spacex-bring-the-cost-to-space-down-to-10-per-kilogram-from-over-1000-per-kilogram.html

[6] J. Rainbow. (2024, May) India enters troubled space insurance market. Accessed: June 6, 2024. [Online]. Available: https://spacenews.com/india-enters-troubled-space-insurance-market/

[7] H. N. Becker, T. F. Miyahira, and A. H. Johnston, "Latent damage in cmos devices from single-event latchup," *IEEE TRANSACTIONS ON NUCLEAR SCIENCE*, 2002.

[8] R. Hodson *et al.*, "Recommendations on the use of commercial-off-the-shelf (cots) electrical, electronic, and electromechanical (eee) parts for nasa missions - phase ii," Tech. Rep., 2022, accessed: May 23, 2024. [Online]. Available: https://ntrs.nasa.gov/api/citations/20220018183/downloads/20220018183.pdf

[9] A. Billings, W. Vonbergen, and K. Schulmeyer, "The dangers of cross-conduction: Isolating half-bridge faults with the ap54rhc288," Apogee Semiconductor, Inc., Tech. Rep., May 2024, white Paper. [Online]. Available: https://www.apogeesemi.com

7 Revision History

REVISION	DESCRIPTION	DATE
A00	Initial release.	August 16, 2024

8 Legal

All product, product specifications and data are subject to change without notice. Apogee Semiconductor provides technical data (such as datasheets), design resources (including reference designs), reliability data (including performance in radiation environments), application or other design advice, safety information, and other resources **"as is"** and with all faults, and disclaims all warranties, express and implied, including without limitation any implied warranties of merchantability, fitness for a particular purpose or non-infringement of third party intellectual property rights. These resources are intended for skilled engineers with understanding of high reliability and high radiation environments and its complexities. Apogee Semiconductor is not responsible for: (1) selecting the suitable products for a given application, (2) designing, veri- fying, validating and testing it, or (3) ensuring that it meets any performance, safety, security, or other requirements. These resources are subject to change without advance notice. The use of these resources is restricted to the development of an application that uses the Apogee Semiconductor products described in them. Other reproduction and display of these resources is prohibited. No license is granted to any other Apogee Semiconductor intellectual property right or to any third- party intellectual property right. Apogee Semiconductor disclaims responsibility and reserves the right to demand indemnification for any claims, damages, costs, losses, and liabilities arising out of wrongful use of these resources. The products are provided subject to Apogee Semiconductor's Terms of Sale (https://www.apogeesemi.com/terms) or other applicable terms provided in conjunction with applicable products. The provision of these resources does not expand or otherwise alter applicable warranties or warranty disclaimers for Apogee Semiconductor products. Purchasers of these products acknowledge that they may be subject to and agree to abide by the United States laws and regulations controlling the export of technical data, computer software, electronic hardware and other commodities. The transfer of such items may require a license from the cognizant agency of the U.S. Government.

9 Acknowledgment

The research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration (80NM0018D0004). Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement by the United States Government or the Jet Propulsion Laboratory, California Institute of Technology.