

Fault-Tolerant Soft RISC-V Linux SoCs on SRAM-based FPGAs in Space

Andrew E. Wilson, Nathan G. Baker, and Michael Wirthlin

Abstract—A fault-tolerant soft RISC-V Linux System-on-Chip (SoC) for space applications is presented, featuring a robust combination of Triple Modular Redundancy (TMR), Error Correction Code (ECC), and strategic placement constraints to mitigate radiation-induced faults in FPGA-based designs. Implemented using the LiteX framework and a VexRiscv core, the design supports Linux operation on modern SRAM-based FPGAs, offering the flexibility and scalability necessary for demanding space missions. A comprehensive evaluation was performed using static net sensitivity analysis and radiation testing with a high-energy neutron beam at the ChipIr facility. Radiation tests validated the system’s resilience under conditions representative of the space environment, revealing a dramatic reduction in single event upset (SEU) sensitivity—up to a 25-fold improvement over unmitigated designs. Detailed fault analysis of 105 failure events further identified residual vulnerabilities, including DDR ECC error accumulation, unmitigated I/O, and parity issues, which present opportunities for further refinement. The results demonstrate that the integration of TMR, ECC, and optimized placement constraints substantially enhances the Mean Time Between Failures (MTBF), marking a significant step toward developing reliable, radiation-hardened soft RISC-V processors for future space missions.

Keywords—RISC-V; Fault tolerance; redundancy; Triple Modular Redundancy (TMR); Single Event Upset (SEU); radiation testing; FPGA; soft processor; Radiation hardening by design

I. INTRODUCTION

RISC-V processors are transforming space system design by providing an open and flexible solution for implementing soft processors on modern SRAM-based FPGAs. Leveraging the open instruction set architecture (ISA) of RISC-V, designers can map cores onto reprogrammable resources—such as lookup tables (LUTs), flip-flops (FFs), digital signal processing (DSP) units, and block RAM (BRAM)—to create highly adaptable systems suitable for the rigors of space.

In space missions, harsh radiation and related hazards such as total ionizing dose (TID) and latch-up failures can significantly impact system reliability. This is especially critical for FPGA designs that implement soft RISC-V processors, as both the reconfigurable fabric and the soft cores are vulnerable to upsets. Factors such as orbit characteristics, FPGA device selection, and shielding determine the system’s exposure to these hazards. Although physical shielding offers some protection, it does not fully prevent single event effects (SEEs)—notably

single event upsets (SEUs) that can corrupt the operational state and configuration memory [1]–[4]. Without additional fault-tolerance measures, these issues may lead to mission-critical failures.

To mitigate these challenges in systems employing soft RISC-V processors, robust fault-tolerance techniques must be integrated into the FPGA’s digital design. The flexibility of FPGAs allows designers to develop customized solutions that combine hardware-based and software-based approaches. For example, triple modular redundancy (TMR) can be used to triplicate critical logic to mask single-point failures, though this approach increases power consumption and resource usage [5]. Additionally, dynamic configuration memory scrubbing continuously corrects SEUs, preventing error accumulation and preserving system integrity [6]. These strategies, along with software-based mitigation integrated within the RISC-V core, ensure that soft RISC-V processors remain robust even under the harsh conditions of space.

This paper presents an evaluation of several harden-by-design techniques aimed at enhancing the reliability and availability of a RISC-V-based system-on-chip (SoC) tailored for space missions. This work builds on previous research of TMR-protected RISC-V processors, which were tested in both bare-metal [7] and Linux environments [8]. The methodology combines static netlist analysis, fault injection, and radiation testing to assess these techniques under realistic conditions. The study focuses on key strategies such as triple modular redundancy (TMR) for core logic, ECC-protected DDR memory for data integrity, and SEU-aware placement for non-triplicable I/O subsystems. A simple fault analysis is provided at the end.

II. FAULT-TOLERANT SOFT RISC-V LINUX SOC

Our system under test is built using the LiteX framework, an open-source environment that simplifies the development of complex hardware. LiteX provides a comprehensive suite of processors, peripherals, and high-level components, enabling rapid deployment of Linux-capable SoCs on a variety of FPGA platforms [9]. A notable configuration available through LiteX is “Linux on LiteX with VexRiscv” [10], which leverages the highly customizable VexRiscv core developed in SpinalHDL [11].

In this implementation, Linux images are loaded onto the FPGA via an SD card, while UART interfaces provide real-time monitoring and diagnostics. The Buildroot-provided Dhrystone benchmark [12] is integrated into the file system to capture performance metrics and diagnostic data during experimentation.

This work was supported by the IUCRC Program of the National Science Foundation under Grant No. 1738550.

The authors are associated with the NSF Center for Space, High-performance, and Resilient Computing (SHREC), and Brigham Young University, Provo, Utah, USA (email: {andrew.e.wilson, nathangarybaker, wirthlin}@byu.edu)

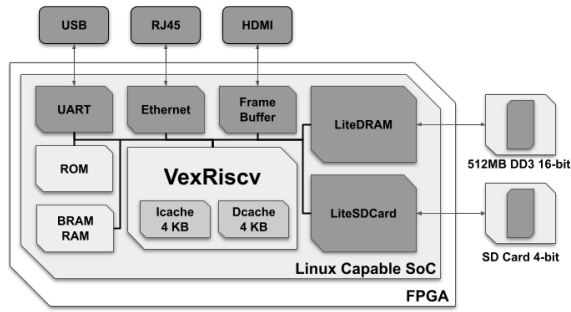


Fig. 1. VexRiscv Block Diagram

A. Triple Modular Redundancy (TMR)

Triple Modular Redundancy (TMR) is employed to enhance the reliability of the soft RISC-V processor against single event upsets (SEUs) through spatial redundancy. In a TMR configuration, three identical processing domains operate in parallel, with majority voters continuously comparing their outputs. If one domain fails, the voters select the output from the other two, effectively masking the error and ensuring correct system operation [13].



Fig. 2. TMR with triplicated voters.

In this work, TMR designs are generated using SpyDrNet, a Python-based netlist tool [14]. SpyDrNet performs fine-grained TMR at the netlist level by triplicating essential FPGA primitives—such as flip-flops (FFs), lookup tables (LUTs), block RAMs (BRAMs), and DSP units—and strategically inserting voters between them. The process starts with a vendor-independent Electronic Design Interchange Format (EDIF) file exported from Xilinx Vivado. After processing, the TMR-enhanced EDIF file is re-imported into Vivado as a post-synthesis design, enabling seamless place and route in the final implementation (see Figure 2).

B. Error Correction Code (ECC)

The design under test employs the open-source DDR4 controller LiteDRAM, which integrates a 72-bit ECC mechanism to improve memory reliability against transient faults such as SEUs. During write operations, an 8-bit codeword is appended to each memory word. On reads, the controller compares the data with its associated codeword to generate a syndrome that detects and corrects single-bit errors while flagging multi-bit discrepancies. This error correction is performed without additional CPU overhead, significantly enhancing data integrity, system reliability, and mean time between failures (MTBF).

C. SEU-aware Placement

To further mitigate SEU-induced faults, the design incorporates strategic placement constraints to shorten critical routing

paths and minimize single-point failures. For example, reduction output voters for OSERDES primitives and triplicated flip-flop inputs for ISERDES primitives are manually placed near their associated cells, reducing the number of programmable interconnect points (PIPs) required. Additionally, the configuration columns within the FPGA are partitioned among TMR domains to isolate shared routing resources. These combined strategies effectively reduce net sensitivity and enhance overall system robustness.

D. Design Under Test

The soft RISC-V Linux SoC was implemented on the Antmicro Data Center DRAM Tester—an open-source hardware platform for testing various DDR4 RDIMMs—using an AMD-Xilinx xc7k160t-ffg676 FPGA [15]. To generate a TMR version of each processor design, all digital logic (LUT, FF, BRAM, and CARRY) was targeted for triplication by the SpyDrNet TMR tool. The tools did not target input/output buffers, SERDES, MMCM, VCC, or GND primitives.

TABLE I
VEXRISCv SoC KINTEX 7 DESIGN UTILIZATION

Design	LUT	LUTRAM	FF	BRAM	IO
Unmitigated	10979 (10.8%)	395 (1.13%)	9766 (4.82%)	54.5 (16.8%)	141(35.3%)
ECC	13744 (13.6%)	395 (1.13%)	11742 (5.79%)	54.5 (16.8%)	153(38.3%)
TMR+ECC	48780 (48.11%)	1233 (3.52%)	35226 (17.4%)	163.5 (50.3%)	153(38.3%)
TMR+ECC+PAR	53244 (52.5%)	1233 (3.52%)	35229 (17.4%)	163.5 (50.3%)	153(38.3%)

Table I lists the resource utilization for the VexRiscv SoC on a Kintex 7 FPGA across four design variations. The baseline Unmitigated design is implemented without any fault-mitigation techniques. The ECC design integrates error-correcting code for DDR memory, resulting in modest increases in LUT and flip-flop usage while maintaining similar LUTRAM, BRAM, and IO levels. In the TMR+ECC configuration, triple modular redundancy is combined with ECC, which significantly increases the utilization of LUTs and flip-flops due to the triplication of logic and the insertion of voters. Finally, the TMR+ECC+PAR design further refines the TMR+ECC approach by applying placement constraints to optimize routing, yielding a slight additional increase in LUT usage while other resources remain comparable.

III. EVALUATION OF MITIGATION

A comprehensive evaluation of the mitigation techniques for the soft RISC-V processor in space applications was performed using three complementary methods: static net sensitivity analysis, fault injection experiments, and radiation testing. Each approach provides unique insights into the system’s resilience against radiation-induced faults.

A. Static Net Sensitivity

To assess the vulnerability of FPGA-based designs to single-bit CRAM upsets, the Bitstream Fault Analysis Tool (BFAT) [16] is employed. BFAT statically analyzes Design Checkpoint (DCP) files to identify sensitive configuration bits and their associated routing resources—specifically Programmable Interconnect Points (PIPs) and Basic Elements of

TABLE II
NEUTRON RADIATION TEST DATA

Design	Fluence (n/cm ²)	Observed CRAM Upsets	Failures	Cross Section (cm ²)	Normalized Reduction	CRAM Sensitivity	Normalized Reduction
Unmitigated Kintex 7	4.21×10^{10}	15656	161	3.82×10^{-9}	1.00×	1.028%	1.00×
ECC Kintex 7	8.04×10^{10}	14121	128	1.59×10^{-9}	2.40×	0.906%	1.13×
TMR+ECC Kintex 7	5.45×10^{11}	198225	105	1.93×10^{-10}	19.84×	0.053%	19.414×
TMR+ECC+PAR Kintex 7	9.36×10^{11}	213351	82	8.76×10^{-11}	43.59×	0.038%	26.76×

Logic (BELs). This mapping is essential for refining fault-tolerant designs, especially for RISC-V systems destined for space missions. Global nets, such as VCC and GND, are excluded to avoid skewing the results.

The BFAT utility offers flexible analysis options, allowing either a comprehensive review of all nets or a focus on a user-defined subset. It also includes an option to filter out triplicated nets in TMR designs, thereby highlighting unprotected areas where vulnerabilities may persist. Table III summarizes the static net sensitivity across various design configurations, underscoring the importance of advanced mitigation strategies for ensuring the robust operation of soft RISC-V processors in the harsh environment of space.

Design	Unmitigated Nets	Percent	Improvement
Unmitigated	1,655,702	4.16%	1.00×
ECC	2,002,516	5.031%	0.83×
TMR+ECC	219,864	0.552%	7.53×
TMR+ECC+PAR	94291	0.237%	17.56×

TABLE III
STATIC NETLIST SENSITIVITY OF MITIGATED DESIGNS

B. Fault Injection

Fault injection is a testing technique used to deliberately introduce errors into a system in order to evaluate its ability to detect and recover from faults. By injecting faults in a controlled manner, the resilience of the soft RISC-V processor design for space applications can be rigorously evaluated. The key metrics recorded include the total number of fault injections, the number of failures observed, the resulting sensitivity (i.e., the percentage of injections that lead to a failure), and the improvement factor relative to the unmitigated design.

Design	Injections	Failures	Sensitivity	Improvement
Unmitigated	13,183	168	1.274%	1.0×
ECC	81,299	886	1.090%	1.17×
TMR+ECC	220,687	78	0.035%	36.06×
TMR+ECC+PAR	83,965	28	0.036%	35.20×

TABLE IV
FAULT INJECTION RESULTS OF MITIGATED DESIGNS

Table III-B summarizes the outcomes across various mitigation schemes. The results clearly demonstrate that combining TMR with ECC significantly reduces the occurrence of SEU-induced failures—an essential improvement for the reliability of soft RISC-V processors in space.

C. Radiation Testing

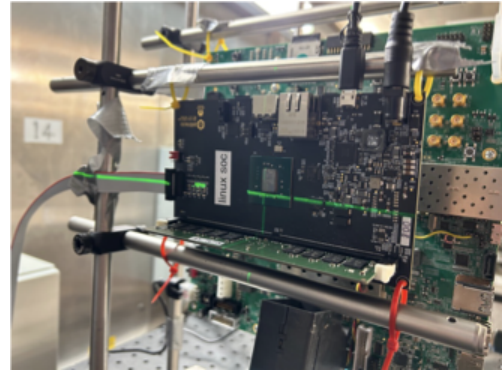


Fig. 3. ChipIr Radiation Test Setup with Antmicro Board

Radiation tests were performed to validate the robustness of the fault-tolerant soft RISC-V Linux SoC for space applications by accelerating single event effects (SEEs) [17]. The devices under test (DUTs) were exposed to a high-energy neutron beam at the ChipIr facility at the Rutherford Appleton Laboratory in the UK [18]. This neutron beam—widely used for assessing the sensitivity of integrated circuits to atmospheric neutrons [19]—was directed at the board (see Figure 3) while the system operated at room temperature. A collimator ensured that only the FPGA, which hosts the soft RISC-V processor, was irradiated, thereby shielding the DDR memory from exposure.

Radiation test results for the TMR and ECC mitigated SoC design (see Table II) indicate significant improvements in reliability, a critical factor for space missions. Baseline “Unmitigated” and “TMR+ECC” Kintex 7 designs were tested in 2022, with additional experiments conducted in 2024. During testing, a JTAG-controlled JCM operating at 25 Mbps continuously scrubbed the configuration memory (CRAM), detecting and correcting upsets via partial reconfiguration. Each scrub cycle involved reading the entire CRAM and

comparing it to a golden reference copy, with errors corrected in real time and logged with precise timestamps. Although the average scrub cycle lasted about 3 seconds, the frequency of upsets varied between cycles.

Throughout the radiation tests, the soft RISC-V processors ran the Dhrystone Linux benchmark continuously. A failure was recorded if the processor produced an incorrect output over the serial interface. Mitigation effectiveness was quantified by calculating the neutron cross section—the ratio of observed failures to the total neutron fluence—while CRAM sensitivity was determined by correlating observed upsets with JTAG telemetry. Notably, the 2024 experiments revealed a discrepancy between the neutron fluence and the recorded CRAM upsets, an anomaly that will be further analyzed in future publications.

IV. FAULT ANALYSIS

Fault analysis was conducted on 105 failure events from the TMR+ECC design using BFAT tools to identify residual vulnerabilities in the soft RISC-V processor intended for space applications. This comprehensive assessment, which combined post-radiation fault injection, sensitive bit mapping, and netlist review, revealed that 25 failures (23.81% of total) are due to unmitigatable aspects of the FPGA or inherent limitations of the digital design.

Failure Category	Count	Percent
Unmitigatable Failures	25	23.81%
XDC-Based Placement	12	11.43%
ADDR & CMD Parity	12	11.43%
DDR Error Accumulation	56	53.33%
Total	105	100%

TABLE V
FAILURE CATEGORIES FOR THE FINAL 5% OF VULNERABILITIES

Specifically, 12 failure events affected unmitigated I/O, targeted by SEU-aware placement in the TMR+ECC+PAR configuration, while DDR4 address/command errors account for an additional 12 events. The remaining 56 failures are attributed to DDR ECC error accumulation, which could potentially be mitigated through DDR memory scrubbing.

These findings provide critical insights into the residual vulnerabilities of soft RISC-V processors in space environments. Although significant reliability improvements have been achieved, further enhancements are limited by practical constraints—namely, a failure coverage ceiling of about 98% and a maximum Mean Time Between Failures (MTBF) improvement of roughly 50×. Consequently, this analysis outlines a clear roadmap for future targeted enhancements in space-grade RISC-V designs.

V. CONCLUSION

This work demonstrates that integrating TMR, ECC, and optimized placement constraints into a soft RISC-V Linux SoC significantly enhances fault tolerance in radiation-prone space environments. Comprehensive evaluations—including

static analysis, fault injection, and radiation testing—confirm a marked reduction in SEU sensitivity and an improved MTBF. These promising results pave the way for further refinements in radiation-hardened FPGA designs for space applications.

REFERENCES

- [1] E. Smith, "Effects of realistic satellite shielding on see rates," *IEEE transactions on nuclear science*, vol. 41, no. 6, pp. 2396–2399, 1994.
- [2] R. C. Moore, "Satellite rf communications and onboard processing," 2003.
- [3] P. Graham, M. Caffrey, J. Zimmerman, D. Eric Johnson, P. Sundararajan, and C. Patterson, "Consequences and categories of SRAM FPGA configuration SEUs," *Proc. 5th Annu. Int. Conf. Military Aerosp. Program. Logic Devices*, 01 2003.
- [4] H. Quinn, P. S. Graham, K. Morgan, J. Krone, M. P. Caffrey, and M. J. Wirthlin, "An introduction to radiation-induced failure modes and related mitigation methods for xilinx SRAM fpgas," in *Proceedings of the 2008 International Conference on Engineering of Reconfigurable Systems & Algorithms, ERSA 2008, Las Vegas, Nevada, USA, July 14-17, 2008*, T. P. Plaks, Ed. CSREA Press, 2008, pp. 139–145.
- [5] Y. Ichinomiya, S. Tanoue, M. Amagasaki, M. Iida, M. Kuga, and T. Sueyoshi, "Improving the robustness of a softcore processor against SEUs by using TMR and partial reconfiguration," in *2010 18th IEEE Annual International Symposium on Field-Programmable Custom Computing Machines*, May 2010, pp. 47–54.
- [6] M. Berg, C. Poivey, D. Petrick, D. Espinosa, A. Lesea, K. LaBel, M. Friendlich, H. Kim, and A. Phan, "Effectiveness of internal vs. external SEU scrubbing mitigation strategies in a xilinx FPGA: Design, test, and analysis," in *2007 9th European Conference on Radiation and Its Effects on Components and Systems*, 2007, pp. 459–466.
- [7] A. E. Wilson, S. Larsen, C. Wilson, C. Thurlow, and M. Wirthlin, "Neutron radiation testing of a tmr vexriscv soft processor on sram-based fpgas," *IEEE Transactions on Nuclear Science*, vol. 68, no. 5, pp. 1054–1060, 2021.
- [8] A. E. Wilson, N. Baker, E. Campbell, and M. Wirthlin, "Improving fault tolerance for fpga socs through post-radiation design analysis," *ACM Transactions on Reconfigurable Technology and Systems*, vol. 17, no. 3, pp. 1–21, 2024.
- [9] F. Kermarrec, S. Bourdeauducq, H. Badier, and J.-C. Le Lann, "Litex: an open-source SoC builder and library based on Migen Python DSL," in *OSDA 2019, collocated with DATE 2019 Design Automation and Test in Europe*, 2019.
- [10] F. Kermarrec. (2020) Linux on LiteX VexRiscv. Accessed: 3-Feb-2020. [Online]. Available: <https://github.com/litex-hub/linux-on-litex-vexriscv>
- [11] C. Papon. (2021) Vexriscv. SpinalHDL. Accessed: 1-Feb-2021. [Online]. Available: <https://github.com/SpinalHDL/VexRiscv>
- [12] "Buildroot Dhrystone package." [Online]. Available: <https://github.com/buildroot/buildroot/tree/master/package/dhrystone>
- [13] J. M. Johnson and M. J. Wirthlin, "Voter insertion algorithms for FPGA designs using triple modular redundancy," in *Proceedings of the 18th Annual ACM/SIGDA International Symposium on Field Programmable Gate Arrays*, ser. FPGA '10. New York, NY, USA: ACM, 2010, pp. 249–258.
- [14] D. Skouson, A. Keller, and M. Wirthlin, "Netlist Analysis and Transformations Using SpyDrNet," in *Proceedings of the 19th Python in Science Conference*, Meghann Agarwal, Chris Calloway, Dillon Niederhut, and David Shupe, Eds., 2020, pp. 40 – 47.
- [15] Antmicro, "Data center rdimm ddr4 tester," 2025, accessed: 2025-01-01. [Online]. Available: <https://openhardware.antmicro.com/boards/data-center-rdimm-ddr4-tester/?view=top-ortho>
- [16] A. E. Wilson, N. Baker, E. Campbell, J. Sahleen, and M. Wirthlin, "Post-radiation fault analysis of a high reliability fpga linux soc," in *Proceedings of the 2023 ACM/SIGDA International Symposium on Field Programmable Gate Arrays*, ser. FPGA '23. New York, NY, USA: Association for Computing Machinery, 2023, p. 123–133. [Online]. Available: <https://doi.org/10.1145/3543622.3573191>
- [17] H. Quinn, "Challenges in testing complex systems," *IEEE Transactions on Nuclear Science*, vol. 61, no. 2, pp. 766–786, April 2014.
- [18] "ISIS ChipIr technical information," 2019. [Online]. Available: <https://www.isis.stfc.ac.uk/Pages/Chipir-technical-information.aspx>
- [19] C. Cazzaniga and C. D. Frost, "Progress of the scientific commissioning of a fast neutron beamline for chip irradiation," *Journal of Physics: Conference Series*, vol. 1021, p. 012037, May 2018.