International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

Low Power and Radiation Tolerance System on Chip (SoC) Architecture: A Review

Misbah Husain
Research Scholar, Department of Electronics and Communication, Sagar Institute of Research and Technology, Bhopal
Prof Shivraj Singh
Assistant Professor, Department of Electronics and Communication, Sagar Institute of Research and Technology, Bhopal

Abstract
The literature related to low-power and radiation-tolerant System-on-Chip design has expanded rapidly. The key problem pointed out by recent research is to continue to work reliably without the fault-tolerance systems introducing prohibitive power, area or time overhead. This review presents eighteen recent papers published in 2025 which are directly related to the development of low-power and radiation-tolerant SoC designs. The selected studies cover radiation characterisation and fault injection in FPGA and RISC-V systems; hardware redundancy and error-correcting techniques such as TMR, ECC, parity and scrubbing; low-power RISC-V and SoC techniques such as clock gating, power gating, architectural specialisation and energy-efficient acceleration; and circuit-level hardening of memories and logic cells. Across the research, a constant trade-off has been seen: higher dependability often means more hardware, storage, checking logic, or recovery activity, whereas low-power design strives to eliminate switching, wasteful computation, and idle resource utilisation.
Keywords: low-power SoC, radiation tolerance, RISC-V, FPGA, fault injection, TMR, ECC, parity, scrubbing

I. INTRODUCTION

Reconfigurable computing, RISC-V processors, advanced CMOS technologies and commercial off-the-shelf devices are increasingly considered for embedded, aerospace, industrial and edge-computing platforms. The literature related to low-power and radiation-tolerant System-on-Chip design has expanded rapidly. The key problem pointed out by recent research is to continue to work reliably without the fault-tolerance systems introducing prohibitive power, area or time overhead. This problem is of particular relevance for SRAM-based FPGAs and tiny embedded processors, because radiation-induced upsets may impact configuration memory, user registers, memories or control logic while the application itself may function under stringent energy limitations.

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

The emphasis of the current M. Tech study is on the latest research released in 2025. This chapter is focused on The selected studies cover four closely related topics: radiation characterisation and fault injection in FPGA and RISC-V systems; hardware redundancy and error correcting techniques such as TMR, ECC, parity and scrubbing; low-power RISC-V and SoC techniques such as clock gating, power gating, architectural specialisation and energy efficient acceleration; and circuit level hardening of memories and logic cells. Special emphasis is given to works reporting quantifiable reliability, power, area, time or recovery related results, since these criteria are directly comparable with the assessment methodology established in the reviewed design direction.

II. RADIATION CHARACTERISATION AND FPGA FAULT INJECTION

Rogenmoser et al. (2025) [1] introduced Trikarenos, a fault tolerant RISC-V based System-on-Chip built in a 28 nm technology and experimentally characterised under the effect of the atmospheric neutron and 200 MeV proton radiation. This study is especially noteworthy since it integrates physical radiation test with simulation-based fault injection, instead of a single validation technique. The design employs error-correcting protection for memory and a triple-core lockstep mechanism for processor-level robustness. Reported findings indicated that the scrubber fixed ECC-protected memory faults and the lockstep system dealt with a broad class of core failures. Gate-level fault injection also revealed that most injected faults resulted in proper outcomes, indicating a good correlation between architectural hardening and measured experimental results. This investigation demonstrates two crucial elements for the present review. First, RISC-V provides a feasible platform for radiation-aware SoC research. Second, we demonstrate that combining memory correction with selective redundancy at the processor level may give significant fault tolerance without having every piece of the SoC to be hardened in the same manner. However, Trikarenos is focused more on reliability characterisation than low-power management. There is opportunity for a design that couples power reduction directly with selective fault prevention.

Austin et al. (2025) [2] The fault-injection approach using the RadPC radiation resistant computer architecture was used to study single-event upsets in FPGA configuration memory. The inspiration was based on in-orbit observations from payloads placed on the International Space Station, where a rare multi-core malfunction indicated that an upset may occur either in a voter or in the FPGA configuration memory controlling the implemented hardware. Researchers have designed a systematic configuration-memory injection mechanism for an Artix-7 FPGA and integrated it into a quad-modular-redundant processor system with memory checking and scrubbing support. They injected faults throughout configuration memory, identified susceptible spots and observed how configuration corruption propagates into active logic design. The importance of the research is that the protection of user level registers is not enough in SRAM-based FPGAs. The configuration memory might change routeing or logic behaviour and is a system level vulnerability. It also highlights the utility of using redundancy, error detection, and scrubbing in combination. For the

present review, the article advocates the integration of repetitive fault injection and centralised error monitoring, but also clarifies that FPGA configuration-memory scrubbing is a platform-specific expansion beyond the fundamental RTL protection techniques assessed in this review.

Kim et al. (2025) [3] We examined eight radiation fault-tolerance techniques for spaceborne electronic systems using a similar assessment methodology based on reliability and resource consumption. Their investigation included hardware and informational redundancy systems including DMR, DMR+, TMR, QMR, parity based approaches, two-dimensional parity, Hamming coding and a combined Hamming-TMR approach. Statistical RTL fault injection was utilised to identify architectural vulnerability and Vivado-based implementation data was used to assess power, latency and area. One key contribution of the research is the direct proof that the most resource-efficient approach is not always the most reliable one. Hamming-based protection gave extremely low vulnerability, but at the cost of a significant extra resource. TMR offered a rather good trade-off between dependability and resources among hardware-redundancy schemes. Therefore, the authors urged for the selection of fault tolerance techniques based on the application needs, instead than using the strongest methodology across the board. This finding is directly in favour of the selective-hardening theory advocated in the present review. Critical SoC condition might justify TMR. Memory can be dealt with by ECC. Lower criticality registers could be parity. The research further emphasises the necessity to assess power, delay and area in addition to dependability rather than reporting fault coverage alone.

Huang et al. (2025) [4] suggested and experimentally assessed an ECC-based hardening approach for the SRAM-based FPGAs against atmospheric-like neutrons. Their technique was meant to detect problems impacting configuration memory and flip-flops, to determine the location of corruption, and to automatically refresh the afflicted circuit. The experimental comparison included an unprotected generic matrix multiplication design, a distributed-TMR version, and an ECC-hardened version under neutron irradiation. The scientists claimed that the ECC technique could limit the soft mistakes efficiently. The authors employed the Geant4 analysis to study the physical causes of the neutron-induced single-event effects. Their data indicated that the neutron-energy range of 1 MeV to 10 MeV was a substantial contribution to the observed effects. From the architectural point of view, the study is useful for the comparison of redundancy and coding based protection in a physical radiation environment. Error repair and targeted refresh may provide an alternative to wide logic triplication, particularly when protection has to be put in place with a regulated resource cost. Therefore, this review supports the usage of ECC and scrubbing for storage-oriented resources. It also does not give a comprehensive low power processor-SoC architecture at the same time which is still a major difference from the proposed approach.

Zhang et al. (2025) [5] single-event effects in 28nm Zynq-7000 SRAM-based FPGAs were studied under various test settings, coupling high-linear-energy-transfer irradiation with fault injection. The aim of the work was to analyse the behaviour of SEE and SEFI in a contemporary FPGA family, and to offer a dynamic-reconfiguration mechanism to refresh erroneous

configuration frames following detection of multi-cell upsets. The error-detection scheme was three-dimensional parity checking, using interleaving of the parity bits. Importantly, the approach connects physical data on irradiation to an engineering recovery mechanism, rather of seeing problem detection as the end of the dependability process. It means that multi-cell and configuration level events need active repair or reconfiguration to operate for a lengthy duration. In the present review the investigation emphasises the notion that radiation tolerance should be structured in the sequence of detection, classification, correction and recovery. The reviewed design direction follows the same system level concept at RTL as TMR mismatch detection, ECC syndrome analysis, Watchdog recovery and safe mode control. However, the RTL-level implementation deliberately does not claim direct physical-radiation validation and employs controlled RTL fault injection, making the technology more accessible while maintaining repeatability for comparative assessment.

Baker et al. (2025) [6] post-irradiation fault injection as a means to investigate the behaviour of complicated FPGA designs following neutron-radiation studies. The authors replayed the configuration-memory upset locations and time information from the irradiation instead of injecting faults just before the beam test. This enabled them to duplicate several known design faults and to examine why certain configuration upsets generated system-level dysfunction. Their work on fault-mitigated FPGA soft-processor systems shown that not all configuration upsets instantly lead to system failure and that the persistence, location, interaction and board context of faults might impact the ultimate system reaction. From a methodological perspective, the work is relevant since it demonstrates the limits of a merely random injection of faults and illustrates how experimental evidence may inform more realistic injection campaigns. This allows the use of deterministic target selection, timed injection, error tracking and result logging in the RTL testbench for the proposed SoC. It emphasises the significance of differentiating between detected, masked, corrected and unrecoverable results. The review does not include radiation-beam data to replay, but it does follow the notion that fault injection should be systematic and visible, not just an informal demonstration of a few bit flips.

Siecha et al. (2025) [7] investigated the single-event-upset tolerance of an FPGA-based time-to-digital converter by means of emulation-based fault injection. The study deals with a class of applications, where reliable timing has to be maintained under harsh environmental circumstances. There the dependability of the configuration-memory becomes especially crucial. The authors deployed an FPGA-based SEU monitoring and repair environment to insert and observe configuration defects without disturbing the regular functioning of the system. We show how a fault-injection system may identify vulnerable parts of a design and measure the impact of configuration-memory damage on functional performance. The importance is not restricted to the TDC application, since the research demonstrates how radiation susceptibility can be examined at the implemented-FPGA level while maintaining realistic circuit behaviour. The main lesson for the present review is that fault injection should be related to clear pass/fail criteria and visible error

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

flags, so that dependability may be represented quantitatively. This makes it possible to utilise fault detection coverage, rectification or recovery coverage and recovery delay as assessment factors. The study also points out the need of hardware monitoring methods that work in concert with the functional design, a notion embodied in the suggested fault-tolerance controller and status-register architecture.

III. CIRCUIT-LEVEL RADIATION-TOLERANT MEMORY AND LOGIC

Lee and Jo (2025) [8] suggested WRTU-16T, a write enhanced low power radiation resistant SRAM cell for space applications. The paper deals with a major trade-off in the design of reliable memories. While TMR and ECC may increase reliability, they may lead to large area, power, and delay overheads in tiny satellites or severely limited systems. WRTU-16T employs a 16-transistor structure with read decoupling and charge sharing suppression to increase the isolation of the storage node and recovery from single event and multi-node disturbances. The study is significant to the present review because memory represents one of the biggest collections of state elements in a SoC and thus needs a security method that scales efficiently. The research also demonstrates the possibility of designing radiation tolerance directly into the memory cell, although such transistor level approaches need technology specific circuit design and cannot be readily ported to a general FPGA RTL implementation. The present review uses SEC-DED ECC at the memory border, instead of a bespoke hardened SRAM cell. This contrast helps to validate the chosen abstraction level: ECC is less physically specialised and may be assessed on FPGA, whereas protected SRAM cells are better suited for future ASIC-oriented additions.

Oliveira et al. (2025) [9] We studied soft-error mitigation at the circuit level for 7-nm FinFET full adders, typical building blocks of arithmetic datapaths. The impact of single-event transients is assessed and mitigation approaches based on decoupling cells, transistor size and a combination approach are examined. A major contribution was the discovery of vulnerable internal nodes and input circumstances, whose susceptibility varied depending on the hardening approach employed. Results indicate that increased process scaling does not eliminate radiation problems and that mitigation efficacy is significantly dependent on circuit architecture and implementation specifics. For a SoC designer, this means that a uniform hardening approach may waste resources on insensitive circuitry and may not effectively handle the most crucial nodes. This work therefore gives proof at the circuit level of the more general idea of selective protection. In the present review, selective protection is performed at RTL level instead of transistor level: important control state is protected by TMR, memory is protected by ECC and regular peripheral registers are protected by lighter parity-based protection. The work also exposes a key weakness of the M.Tech study: RTL fault injection is not able to simulate the analogue pulse form, charge collection or transistor level propagation processes explored in FinFET circuits, so these effects are modelled using logical abstractions.

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

Reis et al. (2025) [10] investigated radiation-tolerant 2:1 CMOS multiplexers at a 32 nm technology node and analysed transistor-level mitigation techniques and their performance trade-offs. Multiplexers are especially important as they are widely used in datapath selection, branch logic, routeing, control networks and reconfigurable structures. The scientists pointed out that the vulnerability to radiation-induced soft mistakes might grow while lowering CMOS dimensions, therefore it is vital to examine both the reliability and the electrical cost when applying hardening. Their investigation investigated the impact of several mitigation measures on the capacity of a multiplexer to withstand transient disturbances and also power, timing and implementation parameters. The research is beneficial for the proposed SoC, since majority voters, branch-selection logic, bus multiplexers and control routes are based on compact combinational structures, and their added protection may increase time and switching. This so underlines the necessity to keep voters and protection logic minimal and prevent random duplication of the whole datapath. The present review takes this system-level interpretation, emphasising redundancy primarily at the critical state with simple majority logic. Hardened standard cells and transistor-level multiplexer optimisation are considered as possible ASIC extensions, not required parts of the FPGA-oriented implementation.

Naveed and Dix (2025) [11] demonstrated a radiation-hardened 4-bit flash analogue to digital converter in 22 nm FD-SOI technology and proposed a compact fault-tolerant logic system for SEU mitigation. Rather of using a standard TMR, the design employs a dual-modular structure with error checking to lower the hardware load while still providing reliable operation. The study is relevant to the current literature review in the sense that it shows a common feature of radiation-aware design, that is, robust redundancy works well, but reduced overhead alternatives may be better if the protected function and fault model let it . The architectural lesson applies straight to digital control systems, even if the goal circuit is an ADC rather than a CPU SoC. Different blocks need different degrees of protection and resource-aware fault tolerance may be provided by a combination of redundancy and lightweight detection. The reviewed design direction embodies this notion with the selective TMR for crucial states and parity for the less critical registers. The research also shows the advantage of technology choices like FD-SOI for radiation robustness. However, the current work is kept intentionally process-independent at RTL level so that the same architecture may be synthesised for FPGA and then ported to ASIC implementation with suitable libraries.

IV. SYSTEM-LEVEL RELIABILITY AND RISC-V FAULT TOLERANCE

Zhou et al. (2025) [12] Developed system level reliability evaluation methodology for relay protection devices under single-event impacts. They used Monte Carlo simulation, alpha-particle radiation testing, fault injection and fault-tree analysis to explore the effect of radiation-induced faults on a comprehensive protection device, not just a single logic cell. The authors also studied soft-error probability for general and application specific processor workloads, and compared behaviour with and without hardening. The relevance of this multi-method approach is that it ties

device level radiation processes to workload dependent system failure. For the proposed SoC, it supports the perspective that dependability should be assessed by true functional activity, not by inserting faults into an otherwise inactive architecture. The proposed technique follows this idea by comparing the baseline and protected variations using the identical processor workload, memory-access sequence, peripheral activity, and fault campaign. The research also illustrates that fault tree and system-level reasoning may be useful in identifying what failures are really crucial to the final application. The study does not implement a formal fault tree, but rather takes a similar criticality-based approach where various levels of protection are assigned to programme control, interrupt status, power management, memory integrity, and watchdog recovery depending on their possible influence on the system.

Iskin et al. (2025) [13] studied fault-tolerance techniques for RISC-V architectures, including spatial, temporal and information redundancy and comparing their application in single-core and multi-core systems. The work covers DMR, TMR, ECC and related ideas of redundancy along with techniques of assessment from simulation to actual radiation exposure. An important benefit of the study is its framing particular to the RISC-V. With the ISA being open and flexible, protection may be added at many levels, from processor state and pipeline architecture to memory and multicore organisation. Authors also stress that fault tolerance impacts performance, energy efficiency and cost, such that reliability cannot be optimised irrespective of implementation resources. This design philosophy directly supports the present review . A complete redundant multicore approach may be used to give a robust coverage but it may clash with the low power target whereas a selective system can concentrate high-cost protection on control-critical resources. Thus, this analysis justifies the use of a low complexity RV32I core together with selective TMR, ECC, parity and watchdog recovery. It also emphasises the need for further study into effective mixed protection techniques, particularly when low power operation and radiation tolerance must be controlled simultaneously inside a single SoC.

Kumar et al. (2025) [14] Design and implementation of error correction circuits for RISC-V based computers for space applications. They employed an implementation of an RV32IM processor and studied hardware error-correction support for radiation-induced single event upsets, such as Hamming-based protection approaches. The research illustrates the feasibility of embedding an error correction around an underlying RISC-V processing platform and testing the resultant architecture on FPGA hardware. Its relevance to the present review is in the direct connection between RISC-V, FPGA realisation and radiation-aware error correction. The study does not see ECC as an external storage function, but rather as part of the reliable processor system. This validates the present review choice to embed SEC-DED circuitry right on the memory barrier and provide error flags to a centralised fault-tolerance controller. At the same time , error-correcting codes alone do not guard against all failure modes at the system level . Memory-oriented ECC may not be required for a corrupted programme counter, interrupt state, power-management state, or watchdog configuration; redundancy or recovery could be required instead. The actual design

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

extends hence an ECC method with a mix of coding, selective TMR, parity, watchdog monitoring and controlled recovery . It also includes low-power activity management.

V. LOW-POWER RISC-V AND SOC TECHNIQUES

Santhosh and Deshpande (2025) [15] Studied low power implementation of RISC-V processor with fine grained clock gating and power gating. Their work considers dynamic and static power by selectively turning off idle resources of the CPU instead of having all functional units on all the time. This is especially crucial for pipelined RISC-V processors because various stages or submodules may be idle for certain parts of the workload. Fine-grained gating decreases wasteful switching activity, while power gating lowers leakage in blocks that are totally powered off. This study offers a more contemporary RISC-V specific foundation for the low-power aspect of the present review. However, the two strategies are heavily implementation technology dependent for portability. Direct power gating needs power switches, isolation, retention and physical-design support, which are inherent in ASIC flows, but are not commonly accessible for arbitrary internal logic on conventional FPGAs. Hence, the reviewed design direction is based on the functional theory of activity-based control and implements it principally by means of synchronous clock-enable signals, memory enables, peripheral sleep modes and operand isolation on FPGA. The research, thus, validates the low power approach and helps identify ASIC directed power gating from FPGA suited methodologies employed for the experimental assessment.

Nguyen et al. (2025) [16] presented AES-RV, a RISC-V accelerator that offers bespoke low-latency AES instruction extensions for secure embedded and IoT applications in a hardware efficient manner. The design has a high bandwidth internal buffering, a dedicated AES processing unit and pipelined data transfer via a ping-pong memory system. Developed on a Xilinx ZCU102 FPGA SoC and benchmarked against software and hardware alternatives. The presented findings demonstrated massive processing delay reductions and significant energy-efficiency increases, suggesting that careful hardware-software co-design may greatly enhance performance per unit energy. Although the study is concerned with cryptographic acceleration, not radiation endurance, it is pertinent to the present review for two reasons. Firstly, it shows that RISC-V offers a flexible basis for FPGA-based integration of application-specific SoCs. 2. It illustrates that energy economy is not only a function of voltage or frequency, but also of eliminating wasteful data transfer and structuring computing to allow active hardware to do valuable work. 2. The reviewed design direction is using the same larger approach at system level by decreasing idle peripheral, bus, memory and data channel activity. However, unlike AES-RV, the present review introduces a reliability layer and assesses the power-reliability trade-off induced by the injected faults.

Xu et al. (2025) [17] proposed a low-power RISC-V based SoC to integrate blockchain data on IoT edge devices. The design teams a RISC-V processing core with a dedicated security coprocessor and a trusted dual-core architecture to speed up data-on-chain activities while keeping conventional and secure execution separate. The SoC was described in Verilog and prototyped on

a Kintex-7 FPGA. The authors claim a significant performance improvement of the hardware coprocessor over a high-performance CPU, while keeping relatively low static and dynamic power. This work is interesting because it shows how RISC-V may be used as the control core of a heterogeneous SoC that includes memory, specific accelerators and system-level management capabilities. It also shows a real example of energy-aware FPGA SoC architecture where the use of dedicated hardware is reducing the execution time and energy cost. The study presented in this review validates the choice of modular RISC-V SoC architecture. It also confirms the significance of monitoring both static and dynamic power. But its dependability techniques are essentially security-oriented, not radiation-oriented. Thus, the low-power and radiation-tolerant architecture expands the low-power SoC viewpoint by adding selective TMR, ECC, parity, watchdog supervision and explicit radiation-style fault injection.

Raisiardali et al. (2025) [18] presented an automated approach to generate RISC-V instruction-subset processors for extreme-edge applications with aggressive size and power constraints. Rather than implementing the whole base instruction set irrespective of the workload demands, the approach determines the subset of the complete base instruction set needed by a target application and creates a processor from pre-verified instruction hardware blocks. Significant reductions in synthesised areas and power relative to a processor implementing the entire RISC-V ISA were reported by the authors, with additional savings achieved when the designs were implemented in flexible integrated-circuit technology. The study is essential to low-power SoC research because it shows how architectural specialisation may minimise energy by removing technology that never contributes to the goal workload. The present review does not limit the RV32I instruction set in this manner, since the goal is to preserve a standard embedded processor and evaluate power and fault tolerance under a common workload. Nonetheless, the work supports a fundamental premise of the low-power and radiation-tolerant architecture: reduce idle hardware activity rather than treat it as an inevitable expense. This notion is implemented in this review in a dynamic way by using clock-enable control, operand isolation, memory enable management and peripheral sleep. Fault-tolerance techniques are applied selectively according to criticality.

VI. RESEARCH GAP

A survey of current 2025 studies show a distinct split between low power RISC-V development and radiation resistant computer technology. Low-power processors and SoC studies largely optimise the switching activity, architectural specialisation, accelerator utilisation, clock gating, power gating, or data movement, but do not often assess the same design under radiation-style register and memory errors. In contrast, radiation tolerant research focuses on TMR, lockstep processing, ECC, scrubbing, hardened cells, configuration recovery or fault injection. Power management is seen as second order or not quantitatively incorporated into the protective architecture.

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

Another disparity is the level of protection. In certain high-reliability systems, the processor is replicated extensively or strong redundancy is used. Circuit-level research focuses on individual memories, flip-flops, arithmetic blocks, or multiplexers. Few studies offer a compact SoC-level paradigm where various protective measures are allocated based on functional criticality and assessed jointly. There is a need for an architecture that uses strong redundancy only for high impact control state, coding for memories, lightweight detection for non-critical registers and watchdog-based recovery for system hangs, rather than one expensive method applied uniformly across the complete SoC.

The third gap is the coordination between power management and fault recovery. When a SoC goes inactive or into sleep, it must still be able to react appropriately to ECC events, voter mismatches, interrupts, watchdog timeouts, and recovery requests. The recent literature offers powerful individual solutions for power reduction and radiation mitigation, but relatively little attention is paid to a shared supervisory framework where low-power mode control may be securely overridden during fault management. The present review fills this gap with a Power Management Unit and Fault-Tolerance Controller that coordinates module enabling, wake-up, correction, reset, status recording and safe-mode behaviour.

Finally, some sophisticated radiation research depends on built test chips, beam facilities, technology-specific hardened cells or configuration-memory trials which may not be available in an M. Tech laboratory. Thus, a reusable RTL-level framework that is technically relevant and can be implemented with standard Verilog/SystemVerilog, FPGA synthesis, simulation, and deterministic fault injection, is valuable. The proposed work fills this practical gap by comparing an unprotected baseline with low-power, radiation-protected and combined variants under the same workload and implementation assumptions. The trade-off among power, area, timing and fault coverage can be quantified in a reproducible way.

VII. CONCLUSION

This chapter presents a survey of eighteen recent papers published in 2025 which are directly related to the development of low-power and radiation-tolerant SoC designs. Literature included experimental radiation characterisation of RISC-V and FPGA systems, configuration-memory fault injection, post-irradiation fault replay, ECC and TMR hardening, circuit-level radiation tolerant memory and logic, RISC-V-specific error-correction approaches, and modern low-power processor and SoC techniques. Across the research, a constant trade-off has been seen. Higher dependability often means more hardware, storage, checking logic, or recovery activity, whereas low-power design strives to eliminate switching, wasteful computation, and idle resource utilisation.

REFERENCES

[1] M. Rogenmoser, P. Wiese, B. Endres Forlin, F. K. Gürkaynak, P. Rech, A. Menicucci, M. Ottavi, and L. Benini, "Trikarenos: Design and Experimental Characterization of a Fault-Tolerant 28-nm RISC-V-Based SoC," IEEE Transactions on Nuclear Science, vol. 72, no. 8, pp. 2783-2792, 2025, doi: 10.1109/TNS.2025.3564739.

[2] H. Austin, C. Major, C. Barney, J. Williams, Z. Becker, M. Smith, and B. LaMeres, "Single-event upset simulation and detection in configuration memory," Frontiers in Space Technologies, vol. 6, Art. no. 1610424, 2025, doi: 10.3389/frspt.2025.1610424.

[3] C. Kim, D. Lee, and J. Na, "A Comparison of Reliability and Resource Utilization of Radiation Fault Tolerance Mechanisms in Spaceborne Electronic Systems," Aerospace, vol. 12, no. 2, Art. no. 152, 2025, doi: 10.3390/aerospace12020152.

[4] Z.-Q. Huang, H.-T. Jing, L.-H. Mo, Z.-L. Hu, G.-P. Shen, Z.-H. Zhou, and C. Cai, "Research of hardening strategies based on the single event effect induced by atmospheric-like neutrons," Nuclear Engineering and Technology, vol. 57, no. 9, Art. no. 103666, 2025, doi: 10.1016/j.net.2025.103666.

[5] Y. Zhang, L. Cai, B. Ye, Q. Chen, X. Yan, Y. Jin, T. Chen, Y. Liu, Y. Jiao, S. Zhao, X. Li, J. Duan, and J. Liu, “Evaluating single event effects on 28 nm FPGAs under multi conditions: high-LET ion irradiation and fault injection,” Radiation Effects and Defects in Solids, vol. 180, no. 9-10, pp. 1353-1366, 2025, doi: 10.1080/10420150.2025.2467351.

[6] N. G. Baker, E. Campbell, A. E. Wilson, and M. J. Wirthlin, "Post-Irradiation Fault Injection for Complex FPGA Designs," IEEE Transactions on Nuclear Science, vol. 72, no. 8, pp. 2919-2927, 2025, doi: 10.1109/TNS.2025.3566344.

[7] R. T. Siecha, G. Alemu, J. Prinzie, and P. Leroux, "Analysis of the SEU Tolerance of an FPGA-Based Time-to-Digital Converter Using Emulation-Based Fault Injection," Electronics, vol. 14, no. 11, Art. no. 2176, 2025, doi: 10.3390/electronics14112176.

[8] S.-H. Lee and S.-H. Jo, "WRTU-16T: Write-Enhanced Low-Power Radiation-Tolerant SRAM for Space Applications," Applied Sciences, vol. 15, no. 13, Art. no. 7295, 2025, doi: 10.3390/app15137295.

[9] R. Oliveira, R. B. Schvittz, and C. Meinhardt, "Exploring Circuit-Level Techniques for Soft Error Mitigation in 7 nm FinFET Full Adders," Electronics, vol. 14, no. 15, Art. no. 2937, 2025, doi: 10.3390/electronics14152937.

[10] A. F. D. Reis, B. B. Sandoval, C. Meinhardt, and R. B. Schvittz, "Design and Evaluation of Radiation-Tolerant 2:1 CMOS Multiplexers in 32 nm Technology Node: Transistor-Level Mitigation Strategies and Performance Trade-Offs," Electronics, vol. 14, no. 15, Art. no. 3010, 2025, doi: 10.3390/electronics14153010.

[11] Naveed and J. Dix, "A Radiation-Hardened 4-Bit Flash ADC with Compact Fault-Tolerant Logic for SEU Mitigation," Electronics, vol. 14, no. 21, Art. no. 4176, 2025, doi: 10.3390/electronics14214176.

[12] H. Zhou, H. Yu, Z. Zou, Z. Su, Z. Xu, W. Yang, and C. He, "Relay Protection Device Reliability Assessment Through Radiation, Fault Injection and Fault Tree Analysis," Micromachines, vol. 16, no. 1, Art. no. 69, 2025, doi: 10.3390/mi16010069.

[13] M. E. Iskin, B. O. Yalcin, and A. Yilmazer, "Exploring Fault-Tolerance in RISC-V Architectures," in Proc. 2025 12th International Conference on Electrical and Electronics Engineering (ICEEE), Istanbul, Turkey, 2025, pp. 19-23, doi: 10.1109/ICEEE67194.2025.11261941.

[14] R. Kiran Kumar, Sk. Abdul Azeez, P. Bharath Kumar, and K. Ganesh, "Design and Implementation of Error Correction Circuits for RISC-V Based Systems in Space Applications," in Proc. 1st International Conference on Research and Development in Information, Communication, and Computing Technologies (ICRDICCT 2025), SciTePress, 2025, pp. 622-627, doi: 10.5220/0013939500004919.

[15] V. Santhosh and A. Deshpande, "Low Power Implementation of RISC V Processor with Fine Grained Clock Gating/Power Gating," in Proc. 2025 9th International Conference on Computational System and Information Technology for Sustainable Solutions (CSITSS), 2025, pp. 1-6, doi: 10.1109/CSITSS67709.2025.11295650.

[16] V. T. Nguyen, P. H. Pham, V. T. D. Le, H. L. Pham, T. H. Vu, and T. D. Tran, "AES-RV: Hardware-efficient RISC-V accelerator with low-latency AES instruction extension for IoT security," IEICE Electronics Express, vol. 22, no. 16, Art. no. 20250329, 2025, doi: 10.1587/elex.22.20250329.

[17] W. Xu, X. Li, Q. Xu, Y. Zhang, X. Wu, W. Li, R. Wang, G. Liang, and H. Guo, "A RISC-V based SoC for blockchain data integration in IoT edge devices," Microelectronics Journal, vol. 161, Art. no. 106697, 2025, doi: 10.1016/j.mejo.2025.106697.

[18] A. Raisiardali, K. Iordanou, J. Kufel, K. Gudimetla, K. Myny, and E. Ozer, "Flexing RISC-V Instruction Subset Processors to Extreme Edge," in Proc. 58th IEEE/ACM International Symposium on Microarchitecture (MICRO 2025), pp. 1147-1159, 2025, doi: 10.1145/3725843.3756036.