POLITECNICO DI TORINO
Repository ISTITUZIONALE

On the Analysis of Radiation-Induced Faults in FPGA-Based Optical Communication for Space Applications

Original
On the Analysis of Radiation-Induced Faults in FPGA-Based Optical Communication for Space Applications / Cora, G., Sajjadikaboudi, S., Amini Bardpareh, A., Azimi, S.. - (2026), pp. 224-229. (23rd ACM International Conference on Computing Frontiers: Workshops and Special Sessions Catania (ITA) May 19 - 21, 2026) [10.1145/3801488.3808244].

Availability:
This version is available at: 11583/3013170 since: 2026-07-16T09:33:18Z

Publisher:
ACM

Published
DOI:10.1145/3801488.3808244

Terms of use:

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright

(Article begins on next page)

13 September 2026

On the Analysis of Radiation-Induced Faults in FPGA-Based Optical Communication for Space Applications

Invited Paper

Giorgio Cora
Politecnico di Torino
Turin, Italy
giorgio.cora@polito.it

Seyedmohammadhossein Sajjadikaboudi
Politecnico di Torino
Turin, Italy
seyedmohammadhossein.sajjadikaboudi@polito.it

Arash Amini Bardpareh
Politecnico di Torino
Turin, Italy
arash.aminibardpareh@polito.it

Sarah Azimi
Politecnico di Torino
Turin, Italy
sarah.azimi@polito.it

Abstract

Space-oriented computing platforms are increasingly relying on multi-board FPGA clusters, making reliable and efficient inter-board communication a key design requirement. In this context, commercial off-the-shelf (COTS) FPGAs represent an attractive solution thanks to their high computational capability and flexibility. Their adoption in radiation-prone environments, however, raises significant reliability concerns, as radiation-induced effects may alter both the implemented logic and the configuration memory, potentially compromising the communication infrastructure. This paper presents a reliability assessment of an optical-fiber FPGA-to-FPGA communication system, evaluating the resilience of the data link layer against Single-Event Upsets (SEUs) and the impact of Single-Event Transients (SETs) on the transceiver control logic. In addition, a lightweight encoder/decoder stage is introduced at the data link layer to assess the effect of a simple mitigation strategy on communication robustness. The results highlight a non-negligible vulnerability of the communication chain, with error rates reaching approximately 6.4% and 3% on the RX and TX sides of the data link layer, respectively, and a transceiver sensitivity of about 15%, confirming the need for dedicated mitigation strategies to ensure reliable communication in FPGA-based space computing systems.

CCS Concepts

• **Computer systems organization → Reliability**.

Keywords

FPGA, Optical Fiber, Reliability, SEE

ACM Reference Format:
Giorgio Cora, Seyedmohammadhossein Sajjadikaboudi, Arash Amini Bardpareh, and Sarah Azimi. 2026. On the Analysis of Radiation-Induced Faults in FPGA-Based Optical Communication for Space Applications: Invited Paper. In *Proceedings of the 23rd ACM International Conference on Computing Frontiers (CF Companion '26), May 19–21, 2026, Catania, Italy*. ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3801488.3808244

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.
CF Companion '26, Catania, Italy
© 2026 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-2569-2/26/05
https://doi.org/10.1145/3801488.3808244

1 Introduction

FPGAs are becoming increasingly attractive for space applications thanks to their flexibility, reconfigurability, and high computational performance [13]. In particular, commercial off-the-shelf (COTS) devices enable efficient onboard architectures without relying exclusively on radiation-hardened components, which are generally more expensive and may also provide lower performance. For these reasons, COTS SRAM-based FPGAs are now considered a promising option for many onboard processing tasks, especially where performance, design flexibility, and rapid development are required.

At the same time, the growing volume of onboard data and the increasing relevance of AI-oriented and data-intensive workloads are driving a transition from single-board solutions to clustered computing platforms. In such systems, multiple processing nodes cooperate to sustain the throughput demanded by modern missions, making inter-board communication a key architectural element. If not properly designed, the communication subsystem can easily become a bottleneck, limiting parallel execution and reducing overall platform efficiency. In this context, optical-fiber links are an attractive solution for high-speed board-to-board communication, while high-speed serial protocols implemented on FPGA transceivers are already recognized as enabling technologies for demanding communication infrastructures [10].

Despite these advantages, the use of COTS SRAM-based FPGAs in radiation-prone environments raises important reliability concerns. These devices are particularly vulnerable to radiation-induced faults in the configuration memory, where the implemented hardware functionality is stored [13]. Single-Event Effects (SEEs), especially Single-Event Upsets (SEUs), can alter configuration bits and consequently modify the behavior of the implemented logic. Such events may compromise processing elements, control modules, and communication subsystems, reducing the overall dependability of the platform. This issue is even more critical in clustered architectures, where communication faults may affect not only a single node but also the capability of the entire system to exchange data and sustain coordinated computation.

This concern is particularly relevant for the data link layer implemented in the FPGA fabric. Since this layer handles framing, transfer management, and communication control between nodes, configuration-memory upsets can directly impair the integrity and continuity of inter-board communication. Reliability issues also involve the circuitry supervising the physical interface. Even when supported by dedicated hardware, transceiver control logic may still be affected by transient radiation-induced phenomena. In particular, Single-Event Transients (SETs) can generate short glitches that propagate through the control path, interfering with channel operation and potentially causing transmission errors, protocol violations, or corrupted data exchanges [12].

This paper presents a detailed reliability analysis of the optical-fiber communication infrastructure connecting two FPGA boards. The investigation focuses on two complementary parts of the communication chain. First, an SEU-oriented analysis is conducted on the data link layer to evaluate the impact of configuration-memory faults on the FPGA-based communication logic. Second, a dedicated SET fault-injection campaign is conducted on the transceiver control logic to assess the physical communication layer's susceptibility to transient disturbances that affect channel management and data transmission. In addition, a lightweight encoder/decoder mechanism is introduced in the data link layer, and its impact on system resilience is experimentally evaluated, with the goal of understanding how much a simple mitigation strategy can improve communication reliability without significantly increasing design complexity.

The remainder of the paper is organized as follows. Section 2 reviews the state of the art. Section 3 presents the hardware setup used for the experimental campaign. Section 4 describes the fault-injection framework adopted to assess the reliability of the system against SEUs and SETs. Section 5 discusses the experimental results, while Section 6 concludes the paper.

2 State of the Art

The adoption of FPGA-based computing platforms is steadily increasing in application domains that require high computational capability and design flexibility. This trend is particularly relevant in space systems, where onboard processing is progressively taking over tasks that were traditionally offloaded to the ground segment. As a consequence, reliability has become one of the primary concerns, especially for SRAM-based devices. Over the years, extensive effort has been devoted to understanding the effects of radiation-induced faults in SRAM-based FPGAs and to assessing their impact through both irradiation campaigns and fault-injection methodologies [13]. For example, the authors in [6] present a detailed analysis of radiation-induced faults in a Kintex-7 SRAM-based FPGA, discussing the susceptibility of the device to SEE phenomena and, in particular, to SEUs. Similarly, the work in [4] investigates how SEUs in the configuration memory of SRAM-based FPGAs can disrupt a RISC-V-based processor for space applications. Besides irradiation testing, fault emulation is also widely adopted to evaluate the effects of radiation-induced faults at lower cost and with higher campaign flexibility. In this context, frameworks such as PyXEL provide advanced bitstream manipulation and support several types of reliability-oriented analyses, including fault injection and sensitivity assessment [5].

Alongside analysis and validation, a broad range of mitigation strategies has been proposed for SRAM-based FPGAs. Among the most widely adopted approaches are logic redundancy and configuration memory recovery techniques. Triple Modular Redundancy (TMR) remains one of the most established strategies for masking the effects of configuration upsets at logic level, and several works have shown how its effectiveness can be significantly improved through careful design partitioning and selective replication. Configuration scrubbing is another key mitigation mechanism, as it periodically repairs corrupted configuration frames and restores the intended functionality of the device [8]. Beyond these traditional approaches, more application-oriented solutions have also been explored, especially for high-speed data-transfer systems. In particular, communication-specific mitigation schemes based on information redundancy, coding, interleaving, and localized hardware hardening have been proposed to improve the robustness of serial links implemented on SRAM-based FPGAs [11].

When moving from a single-board architecture to a clustered platform, however, additional reliability concerns emerge. While the failure of a node already limits the overall computational capability of the system, the presence of dedicated communication logic introduces a second class of critical elements whose malfunction may compromise the whole interconnect subsystem. In this context, different studies on high-speed serial communication under radiation have been conducted, but most of them focus either on older devices or radiation-hardened ones. For instance, FPGA-based high-speed serial communication channels have been experimentally characterized under radiation in [10], while the behavior and recovery mechanisms of Aurora over MGT-based links have been investigated in [7]. Similarly, the SEE sensitivity of embedded high-performance SerDes blocks has been characterized in [12], and the impact of SEUs on FPGA-based digital communication systems has been discussed in [9]. Reliable clustered architectures have also been proposed, such as the one in [3], but the literature still leaves a gap in the dedicated analysis of the communication logic required to sustain board-to-board communication in COTS FPGA clusters based on otical fiber interconnect systems.

This paper addresses this gap by presenting a dedicated investigation of an optical-fiber communication channel between COTS FPGAs, with specific emphasis on the reliability of the data link layer under SEUs and of the transceiver control logic under SETs. The work also evaluates the impact of a lightweight encoder/decoder stage introduced at the data link layer, thus providing additional insight into the effectiveness of simple communication-oriented mitigation strategies.

3 Implementation of Optical Fiber-Based Communication

The evaluated communication chain is composed of two main blocks: the data link layer and the transceiver control logic. The platform under test is highlighted in Fig. 1. In particular, the light-blue components correspond to the blocks considered in the data link layer analysis, including the encoder/decoder and the Aurora

IP, whereas the light-yellow components identify the transceiver logic targeted by the SET evaluation.

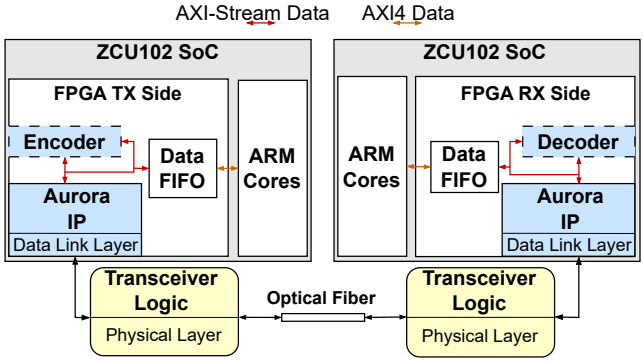

Figure 1: Aurora based communication platform under test

3.1 Data Link Layer

For the data link layer, the Aurora IP, based on the 64B/66B protocol, was selected. Aurora is a lightweight point-to-point link-layer protocol designed to transfer data over one or more high-speed serial lanes, including flow-control messages, clock-compensation sequences, and idle blocks. Additionally, Aurora automatically distinguishes between hard errors, which require a channel reset, and soft errors, which are recoverable or data-related events reported to the user application. This makes the protocol a suitable candidate for implementing high-speed board-to-board communication, while also making it interesting to evaluate how radiation-induced faults at the configuration-memory level affect its actual robustness.

3.1.1 Encoder/Decoder.

While standard communication IPs such as Aurora provide robust link initialization and soft-error monitoring, radiation-induced SEUs in FPGA configuration memory may still alter routing or logic and eventually lead to Silent Data Corruption (SDC). To improve end-to-end data integrity and evaluate the impact on the overall Aurora reliability against SEU, a custom Hamming encoder and decoder were implemented in Vitis High-Level Synthesis (HLS). The design targets streaming applications and uses AXI4-Stream interfaces to simplify integration into FPGA-based data paths. More specifically, the implemented architecture follows an extended Hamming Single Error Correction, Double Error Detection scheme (SECDED) and operates continuously as a free-running component.

The encoder generates a $(64, 57)$ SECDED codeword composed of 57 payload bits, 6 Hamming parity bits, and 1 overall parity bit, resulting in a 64-bit protected word that can be directly transmitted over AXI4-Stream. To sustain high throughput, the encoder was optimized with loop unrolling and pipelining, so that one word can be processed every clock cycle after the initial pipeline fill. Packet boundaries are preserved by forwarding the `TLAST` signal, while the `USER` field is kept to zero at the encoder output because no correction status is generated at this stage.

The decoder verifies and, when possible, corrects incoming protected codewords. It distinguishes among valid codewords, single-bit errors, overall-parity-bit errors, and detected but uncorrectable multi-bit errors. When a correctable fault is identified, the corresponding bit is flipped and the original payload is reconstructed from the non-parity positions. The decoded payload is returned as a 57-bit value embedded into a 64-bit AXI stream word. Correction and detection status are exported through dedicated `USER` bits, allowing the system to signal whether a correctable or uncorrectable event has been observed. As for the encoder, the decoder is fully pipelined with an initiation interval equal to one clock cycle, thus preserving high-throughput streaming operation.

3.2 Transceiver Logic

To investigate the effects and propagation of transient faults in the transceiver control logic, a dedicated transceiver model derived from an Optical Time-Domain Reflectometer (OTDR) architecture was considered as a representative case study. The schematic of the logic under test is reported in Fig. 2 An OTDR is commonly used to monitor and diagnose optical fiber links by injecting short optical pulses into the channel and analyzing the signal reflected back to the transmitter side. The acquired trace is typically characterized by a low-amplitude distributed Rayleigh backscattering component, which provides information on attenuation along the fiber, and by localized Fresnel reflections, which appear as peaks in correspondence with discontinuities such as connectors, splices, bends, or breaks. By evaluating the time of flight of the generated pulses and averaging multiple acquisitions, the OTDR is able to identify and localize events occurring along the optical path.

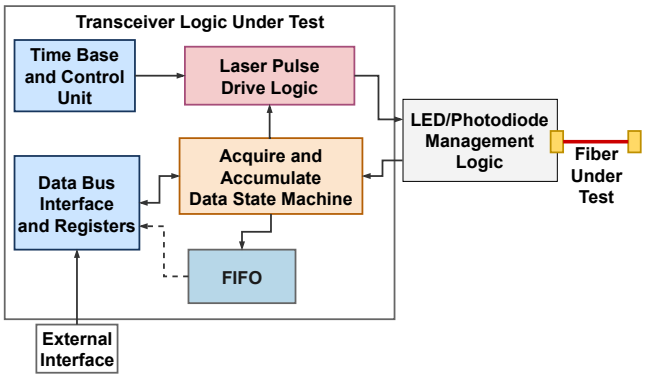

Figure 2: Transceiver logic under test

This type of architecture was selected because it includes the main mechanisms typically involved in transmission control, timing management, and signal supervision, thus representing a meaningful target for transient fault propagation analysis in transceiver-oriented logic. In particular, the adopted model includes a pulse generator with programmable delay stages, timing-control resources based on dedicated registers and PLL synchronization, an interface toward the laser/LED driving circuitry, routing logic for the transmission and reception paths, an ADC interface for the acquisition of backscattered and reflected signals, and a high-speed RAM buffer for temporary data storage during the measurement phase.

4 Fault Injection Framework

To evaluate the effect of radiation-induced faults on the optical-fiber communication channel between FPGAs, two complementary analyses were conducted. Since the data link layer is implemented in the FPGA fabric, its validation requires an SEU-oriented analysis targeting configuration memory. Conversely, the transceiver control

logic is usually based on dedicated communication circuitry and associated control paths rather than on the reconfigurable fabric alone. Therefore, its reliability was investigated through a dedicated SET-oriented campaign focused on transient propagation.

4.1 SEU Analysis Framework

The validation of radiation-induced faults in FPGA configuration memory can be carried out in different ways. One option is radiation testing, which provides a realistic assessment of the system by reproducing both the origin of the fault and its physical effect on the device. Although this approach is extremely valuable, it is constrained by the limited availability of irradiation facilities and associated costs. For this reason, a widely adopted alternative is to emulate only the effect of the radiation-induced event, namely the upset in the configuration memory.

This methodology consists of inducing controlled bit flips in the configuration memory of the target device. A straightforward approach is to generate the bitstream, corrupt it by injecting a single-bit fault, and then reload the modified bitstream into the FPGA. While conceptually simple, this flow becomes inefficient for devices with large configuration memories, since each injection requires a complete reprogramming step. Given that fault-injection campaigns typically involve thousands of injections and that each reconfiguration may take several seconds, the total campaign time rapidly becomes impractical.

For this reason, the methodology adopted in this work relies on runtime injection through dedicated vendor-supported infrastructure. More specifically, AMD FPGAs provide the SEM-IP[1], a built-in interface originally intended for configuration-memory error detection and correction that also includes features for fault injection. In order to perform targeted injections, the exact addresses of the configuration bits associated with the Aurora IP had to be identified. To this end, the PyXEL toolkit [5] was used to extract the relevant configuration-memory locations, and a dedicated Python script was developed to automate the injection and validation flow throughout the campaign. The whole injection flow has been highlighted in Fig. 3

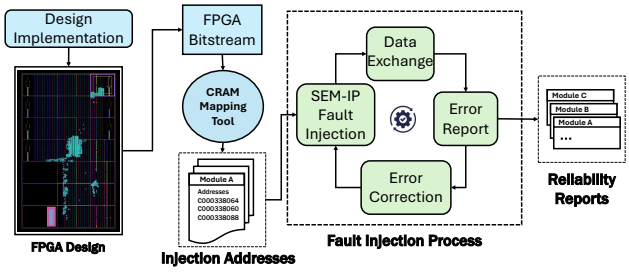

Figure 3: SEU analysis flow.

After each injection, data is exchanged between the two boards and the transmission outcome is evaluated. Whenever an error is detected, a report is generated and stored for post-analysis. The injected error is then corrected, and a new fault is injected at a different address. This procedure is repeated until all the targeted addresses have been analyzed.

4.2 SET Analysis Framework

The validation of the transceiver logic against Single-Event Transients was carried out through a dedicated analysis flow, distinct from the SEU campaign adopted for the data link layer, and represented in Fig. 4. Starting from the VHDL description of the OTDR-based transceiver logic, the design was synthesized and implemented onto a target Microchip FPGA logic, obtaining a post-synthesis representation of the circuit suitable for transient propagation analysis. The implemented design was then analyzed through the pySETA tool [2], which enables the evaluation of radiation-induced transient effects in digital circuits by identifying sensitive nodes and estimating how injected glitches propagate through the logic.

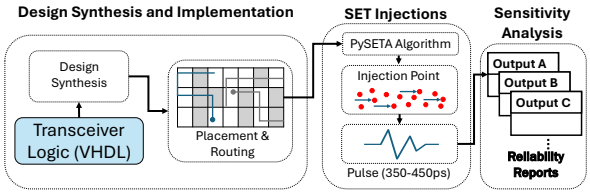

Figure 4: SET analysis flow.

More specifically, the adopted framework first analyzes the synthesized design to identify the internal nodes that may act as potential transient injection points. Starting from these locations, the tool performs fault-oriented simulations to assess whether a transient pulse can propagate across the logic and eventually reach sequential elements or observable outputs. This approach makes it possible not only to identify the portions of the architecture that are more exposed to SET effects, but also to estimate the actual error susceptibility of the design by considering pulse propagation conditions and masking phenomena.

In this way, the analysis provides a more realistic view of the vulnerability of the transceiver control logic. Rather than simply classifying nodes as sensitive or non-sensitive, the framework allows the identification of the logic regions in which transient faults are more likely to be propagated and observed at the outputs. This information is particularly useful for highlighting critical portions of the architecture and for guiding the definition of possible mitigation strategies aimed at improving the robustness of the transceiver subsystem against radiation-induced transient events.

5 Experimental Results

The optical-fiber communication system based on the Aurora IP was implemented on the AMD UltraScale+ ZCU102 development board. The corresponding resource utilization is reported in Table 1. As discussed in the previous sections, two versions of the design were considered: one implementing the Aurora-based communication chain only, and one including the additional encoder/decoder units. The overhead introduced by the encoder/decoder pair is reported separately in Table 2.

Additional logic, reported as glue logic, was required to manage the Aurora communication through the Processing System (PS) available on the ZCU102 SoC. This auxiliary logic was used to coordinate data transmission on both the RX and TX sides and to supervise the communication process through the Python-based validation framework introduced in the previous section.

Table 1: Resource utilization for the ZCU102.

Target	Component	LUT	FF	BRAM	DSP
RX Side	Aurora IP	592	1494	1	0
	Glue Logic	1506	2248	4	0
	TOTAL(%)	0.79	0.69	0.54	0
TX Side	Aurora IP	511	1448	1	0
	Glue Logic	1236	2077	1	0
	TOTAL(%)	0.65	0.65	0.22	0

Table 2: Encoder/Decoder Resource utilization.

Component	LUT	FF	BRAM	DSP
ENCODER	130	256	0	0
DECODER	365	393	0	0

The fault-injection campaigns specifically targeted the FPGA regions containing the Aurora IP, both with and without the encoder/decoder stage. Although this does not reproduce the most general case in which the entire device is exposed to configuration upsets, it enables a more focused evaluation of the communication subsystem itself. A total of 50,000 injections were performed for each design version. In addition, to emulate operational conditions in which all boards are exposed to the same environment, injections were carried out simultaneously on both the TX and RX sides. The results of the two campaigns are reported in Tables 3.

Table 3: 50,000 Fault injection results for the Aurora IP without Encoding

Side	Failure rate (%) No encoding	Failure rate (%) With encoding
TX	2.89	3.4
RX	6.91	3.21
Both	0.15	0.28

For both campaigns, faults were classified according to whether the observed failure affected only the TX side, only the RX side, or whether it emerged only when both sides were simultaneously exposed. The results show that the introduction of the encoder/decoder stage produces a non-uniform effect across the communication chain. In particular, the protected version clearly reduces the error rate at the receiver, whereas the transmitter exhibits a slight increase in failure rate.

This behavior is consistent with the asymmetry in logic utilization between the RX and TX sides of the Aurora-based design. The receiver side already contains a larger amount of logic dedicated to channel management and data handling; therefore, the addition of the decoding stage introduces a relatively limited structural perturbation while at the same time providing protection against a relevant class of communication errors. On the transmitter side, by contrast, the baseline logic is smaller, and the encoder represents a proportionally more significant addition. This helps explain both the lower fault sensitivity of the unprotected TX path and the moderate increase in failure rate observed after the insertion of the encoding stage. To obtain a more detailed view of the observed failures, the outcomes of both campaigns were further classified according to the type of error that they caused. The corresponding distributions are reported in Tables 4 and 5.

Table 4: Failure types for TX, RX, and BOTH sides without Encoding

	Failure Type	Failure Rate (%)
Transmitter	SDC	1.26
	EXTRA	0
	MISSED	0
	HALT	1.00
Receiver	SDC	5.56
	EXTRA	0.02
	MISSED	0.04
	HALT	1.30
Both	SDC	0.051
	EXTRA	0
	MISSED	0
	HALT	0.099

Table 5: Failure types for TX, RX, and BOTH sides with Encoding

	Failure Type	Failure Rate (%)
Transmitter	SDC	2.61
	EXTRA	0.01
	MISSED	0.03
	HALT	1.00
Receiver	SDC	2.37
	EXTRA	0.01
	MISSED	0.06
	HALT	0.75
Both	SDC	0.05
	EXTRA	0
	MISSED	0
	HALT	0.11

SDC identifies a mismatch between transmitted and received data with respect to the golden reference. EXTRA indicates that one or more additional words were received, MISSED denotes the loss of expected words, and HALT indicates that the TX side, the RX side, or both sides stopped operating.

The results show that SDC remains the dominant error mode in both configurations, which is consistent with the fact that the adopted ECC can correct only a limited class of faults and cannot address all possible error manifestations generated by configuration-memory upsets. Even when the overall receiver failure rate decreases, the residual faults are still largely associated with corrupted data rather than with complete loss of functionality. On the transmitter side, a similar trend can be observed, although the relative impact of HALT events decreases when the protection logic is introduced. Overall, the experimental results shows how the encoder/decoder stage is effective in mitigating part of the communication vulnerability, especially at the RX side, but it does not eliminate the predominance of data-corruption events under SEU conditions.

Alongside the validation of the data link layer, the transceiver logic was also evaluated. As detailed in the previous section, a dedicated investigation against SET-induced transients was conducted through pySETA. A total of 837 sensitive nodes were identified

and stimulated through different transient injections. In particular, two pulse widths, equal to 350 ps and 450 ps, were considered to evaluate how transient duration affects propagation toward the output nodes. The results of the campaign are reported in Figures 5 and 6.

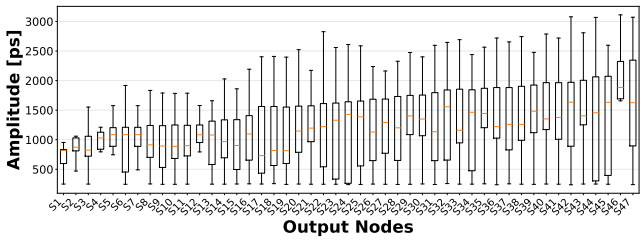

Figure 5: Pulse propagation distribution across 837 test nodes for input pulses of 350 ps

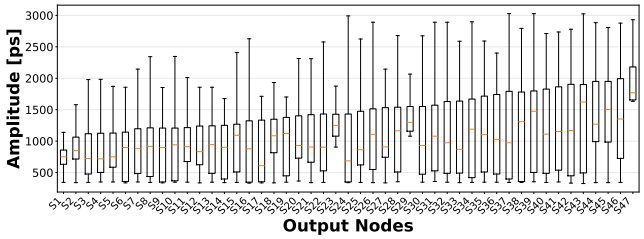

Figure 6: Pulse propagation distribution across 837 test nodes for input pulses of 450 ps

Each boxplot corresponds to one output node and summarizes the distribution of the pulses that, after being injected in one of the 837 internal nodes, were able to propagate and be sampled at the corresponding output. The red line marks the mean value of the propagated pulse widths. The results indicate a non-negligible sensitivity of the design to transient events for both pulse widths. Although the overall distributions remain comparable across the considered outputs, the 450 ps injections exhibit a larger number of cases in which the propagated pulse width reaches or exceeds approximately 3 ns. This confirms that the transceiver control logic can amplify or preserve transient effects long enough to make them observable at the output interface.

Finally, sensitivity and vulnerability metrics were computed for the SET campaign and results are reported in Table 6. Sensitivity is defined as the percentage of circuit nodes susceptible to radiation-induced transients, while the Vulnerability Factor quantifies the tendency of the design to propagate a transient toward sequential elements and eventually translate it into an observable output error.

Table 6: SET sensitivity and error-propagation vulnerability.

Glitch amplitude (ps)	SET sensitivity (%)	Vulnerability factor
350	14.6	16
450	13.7	14

The results show that the design exhibits a measurable susceptibility to SET propagation for both pulse widths. Interestingly, the shorter transient leads to slightly higher sensitivity and vulnerability values. This suggests that even relatively narrow glitches can be effectively captured and propagated by the transceiver control logic, and therefore cannot be neglected when assessing the robustness of the communication infrastructure. Overall, these results highlight the need for mitigation mechanisms not only at the data link level, but also within the circuitry responsible for physical-layer management and channel control.

6 Conclusions

This paper presented a reliability analysis of an optical-fiber communication infrastructure for FPGA-based clustered platforms, considering both the data link layer and the transceiver control logic. Results showed that the communication chain is significantly affected by radiation-induced faults. In particular, the data link layer proved sensitive to SEUs, especially on the receiver side in the unprotected configuration, while a lightweight encoder/decoder improved RX resilience. The SET campaign also highlighted the sensitivity of the transceiver logic to transient perturbations. Overall, the results indicate that reliable inter-board communication in COTS FPGA clusters requires protection mechanisms at both data link and physical-control levels.

Acknowledgments

This study was carried out within the "REASE - REsilient computing Architecture in the Space quantum communication Era" project, CUP number E53D23008300006 – funded by the Ministero dell'Università e della Ricerca – within the PRIN 2022 program (D.D.104 - 02/02/2022). This manuscript reflects only the authors' views and opinions and the Ministry cannot be considered responsible for them.

References

[1] AMD: Soft Error Mitigation Controller v4.1, (PG036) 2018.
[2] S. Azimi et al. 2019. A new CAD tool for SET analysis and mitigation on flash-based FPGAs. Integration (2019).
[3] Ludovica Bozzoli et al. 2023. EUFRATE: a High-Perfomance Reconfigurable Architecture for Radiation-hardened Telecom Payloads. In 2023 European Data Handling & Data Processing Conference (EDHPC). doi:10.23919/EDHPC59100.2023.10396517
[4] Giorgio Cora et al. 2024. A New Reliability Analysis of RISC-V Soft Processor for Safety-Critical Systems. In 2024 27th International Symposium on Design & Diagnostics of Electronic Circuits & Systems (DDECS). doi:10.1109/DDECS60919.2024.10508921
[5] Corrado De Sio et al. 2023. PyXEL: Exploring Bitstream Analysis to Assess and Enhance the Robustness of Designs on FPGAs. 1–4. doi:10.1109/SMACD58065.2023.10192116
[6] Boyang Du et al. 2019. Ultrahigh Energy Heavy Ion Test Beam on Xilinx Kintex-7 SRAM-Based FPGA. IEEE Transactions on Nuclear Science (2019). doi:10.1109/TNS.2019.2915207
[7] Alex Harding et al. 2013. Characterization and Mitigation of the MGT-Based Aurora Protocol in a Radiation Environment. In IEEE Radiation Effects Data Workshop (REDW). 1–4.
[8] Aaron Stoddard et al. 2017. A Hybrid Approach to FPGA Configuration Scrubbing. IEEE Transactions on Nuclear Science 64, 1 (2017), 497–503. doi:10.1109/TNS.2016.2636666
[9] Brian Pratt et al. 2008. Practical Analysis of SEU-induced Errors in an FPGA-based Digital Communications System. In Proceedings of the Military and Aerospace Programmable Logic Devices Conference (MAPLD). Annapolis, MD, USA.
[10] Kevin Ellsworth et al. 2012. Radiation Testing of FPGA-Based High-Speed Serial Communication. In Proceedings of the International Conference on Radiation Effects on Components and Systems (RADECS).
[11] R. Giordano et al. 2018. Radiation-Tolerant, High-speed Serial Link Design with SRAM-based FPGAs. arXiv:1806.10677. doi:10.48550/arXiv.1806.10677
[12] Shu Wang et al. 2021. Measurement and evaluation of the Single Event Effects of high-performance SerDes circuits. Nuclear Instruments and Methods in Physics Research Section A 1012 (2021), 165618. doi:10.1016/j.nima.2021.165618
[13] Zhe Liu et al. 2024. Recent advances on reliability of FPGAs in a radiation environment. Microelectronics Journal 148 (2024), 106176. doi:10.1016/j.mejo.2024.106176