

Fault Injection Attacks Based on Layout-Driven SER Analysis

Alexandra Takou¹, Pelopidas Tsoumanis¹, Georgios-Ioannis Paliaroutis¹, Nestor Evmorfopoulos¹, and George Stamoulis¹

¹Department of Electrical and Computer Engineering, University of Thessaly

August 03, 2025

Fault Injection Attacks Based on Layout-Driven SER Analysis

Alexandra Takou[†], Pelopidas Tsoumanis[†], Georgios-Ioannis Paliaroutis[†],
Nestor Evmorfopoulos, and George Stamoulis

Department of Electrical and Computer Engineering, University of Thessaly, Volos, Greece
{atakou, petsouma, gepaliar, nestevmo, georges}@e-ce.uth.gr

Abstract—The ongoing downscaling of CMOS technology has considerably increased the vulnerability of Integrated Circuits (ICs) to reliability issues, such as Soft Errors and Hardware Trojans (HTs). The combined impact of these threats poses an even more significant challenge to circuit security. The study of the Single Event Multiple Transients (SEMTs) generation and propagation through the circuits constitute the most critical process of the proposed methodology. In particular, a comprehensive layout-based analysis is presented to identify the most impactful regions (grids) in a circuit where HTs can be intentionally injected. Experimental outcomes demonstrate a significant average increase of approximately 32% in the Soft Error Rate (SER) of the utilized ISCAS '89 benchmarks, highlighting the need for a more robust system design to combat reliability-based threats.

Index Terms—Hardware trojan, SER, Soft errors, Fault injection, SEMT-driven HT, Pulse broadening.

I. INTRODUCTION

With the miniaturization of technology and the continuous pursuit of higher performance, modern Integrated Circuits (ICs) have become increasingly sensitive, raising significant concerns about their reliability. Hardware security and circuit reliability are closely related, as their objective is to ensure robust and trustworthy circuit operation. However, vulnerabilities in ICs can be exploited as security threats, highlighting the need to consider both aspects in the design and evaluation of modern hardware.

A critical reliability concern is ionizing radiation that poses a severe threat to modern ICs [1]. An ionizing particle, such as a neutron, striking a semiconductor device induces direct or indirect ionization, resulting in charge generation. When the charge carriers are collected from a contact, a Single Event Upset (SEU) may emerge in a memory cell as a bit-flip. In logic gates, the result is a glitch at the affected gate output, known as Single Event Transient (SET), or even multiple glitches, known as Single Event Multiple Transients (SEMTs), at adjacent affected gate outputs. Such glitches can potentially propagate along a circuit and be captured by a memory element, resulting in a soft error. Both effects constitute a major reliability concern, particularly for critical systems, such as those used in aerospace and automotive applications.

The globalization of the chip fabrication process, which inherently encourages the reliance on untrusted entities, has

facilitated hardware attacks at various IC manufacturing stages [2]. Reliability-based Hardware Trojans (HTs) have gained increasing attention recently, as malicious attackers exploit aging and wearout mechanisms, such as Bias Temperature Instability (BTI), Hot Carrier Injection (HCI), Time-Dependent Dielectric Breakdown (TDDB), and Electromigration (EM), to accelerate circuit degradation or induce soft or even hard failures [3]. Such attacks leverage subtle process modifications to deteriorate aging effects and manipulate BTI-induced degradation [4], or weaken the power grid by removing decoupling capacitances, thus, exacerbating EM [5]. Additionally, laser-based attacks exploiting circuit susceptibility to radiation pose a growing threat by inducing Single Event Effects (SEEs) [6]. These vulnerabilities highlight the need for robust countermeasures to ensure the dependability of electronic devices. Finally, a related work is [7], which analyzes gate sensitivity for HT injection but ignores layout in SER evaluation. To our knowledge, no other comparable methods exist.

In this paper, we propose a novel theoretical framework for injecting Soft Error Rate (SER) driven HTs to provide challenging benchmarks for radiation-induced attacks identification. Our approach targets the low-level sensitive regions of the circuit layout, while leveraging key SER metrics to strategically place stealthy HTs. The purpose of such HTs is to maximize the impact of SETs, thus, compromising circuit operation. Finally, we present some preliminary results to validate our methodology.

The rest of the paper is organized as follows. Section II provides the background on layout-aware SER estimation and reliability-based fault injection; Section III elaborates on the proposed theoretical framework for HT injection based on layout SER analysis; Section IV demonstrates the expected results of the proposed approach and, finally, Section V concludes this paper.

II. BACKGROUND

A. Modeling of SEMTs Generation and Propagation

Ongoing advancements in CMOS technology have made modern ICs increasingly susceptible to diverse phenomena that can seriously impact their functionality. In terms of radiation effects, the continued downscaling of transistor dimensions, along with supply voltage decrease and clock frequency increase, has led to a significant decrease in the critical charge (Q_{crit}) required to induce a disturbance. As a result, ICs

*This work has been done in the framework of EU-funded Horizon Europe Twinning project TWIN-RELECT, under the Grant Agreement No. 101160314.

[†] These authors contributed equally to this work.

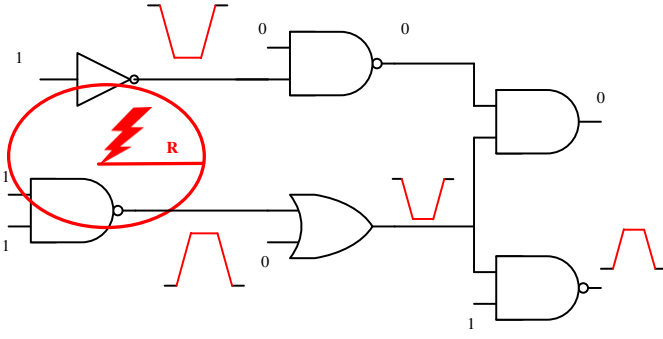


Fig. 1. Multiple affected gates by a single particle hit.

are more susceptible to hazards such as SETs, which are temporary electrical disturbances emerging at a gate output [8]. In addition, the reduced spacing between gates has increased the likelihood that a single high-energy particle strike can simultaneously affect multiple gates, leading to SEMTs. In such case, transient faults appear at multiple gate outputs, as shown in Fig. 1. Consequently, SEMTs pose a more severe threat to circuit reliability, since they significantly increase the probability of system failures by generating transient faults across multiple circuit paths [9].

Ionizing particles responsible for SETs, and especially SEMTs, may originate from various sources, including cosmic radiation, which generates energetic neutrons that interact with silicon, and alpha particles emitted from the radioactive decay of IC packaging materials. Soft errors, which compromise circuit reliability, arise when transient faults propagate through the circuit and are latched by memory elements. Masking mechanisms (i.e., Logical, Electrical, and Timing masking) inherently mitigate the impact of SEMTs, protecting IC functionality. Logical masking prevents a glitch from propagating through a gate due to the controlling value in another input; electrical masking attenuates the glitch due to the gate electrical characteristics; and timing masking occurs when a transient fault arrives outside a flip-flop's (FF) latching window, preventing it from being captured. Given the increasing susceptibility of modern ICs to radiation-induced faults, accurately modeling masking mechanisms in the presence of SEMTs is crucial for developing effective mitigation techniques that ensure the reliability of critical applications.

B. SEMT-driven Hardware Trojan

Hardware security and more specifically, fault injection attacks are a serious concern since they can alter the functionality of the IC either temporarily or permanently, with grievous repercussions [2], [10], [11]. A stealthier sub-category of fault injection attacks includes HTs that exploit and aggravate reliability issues, like SETs and Electromigration (EM), to generate a fault [5], [12]–[14]. Reliability-based attacks and HTs are by definition stealthier since their trigger is a side-channel parameter, thus more difficult to test.

A stealthy reliability-based HT facilitating the generation of a fault through SET pulse propagation was described in [7]. The payload of this SET-based trojan involves widening

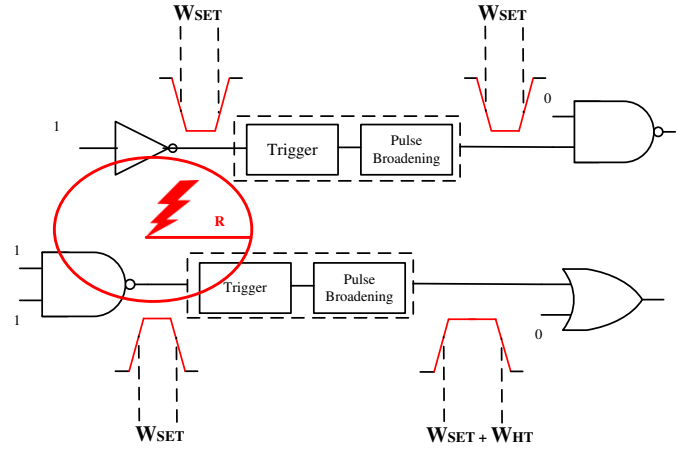


Fig. 2. SEMTs generation combined with HTs impact.

the SET pulse to increase the probability of a soft error. The attack requires two deliberate and coordinated particle hits: one to generate the initial pulse acting as the trigger of the HT, and another to broaden its width, ensuring its propagation through the design until it reaches a memory cell.

This requirement can be bypassed considering the effects of SEMTs. As already mentioned, a high-energy particle strike can affect more than one gate, creating SEMTs. Placing the trigger of the HT in close proximity to the gate under attack ensures that a hit would affect both of them, generating a SEMT, as depicted in Fig. 2. An additional advantage of this placement is the disengagement from the need to coordinate the particle hits from an external factor. Any naturally occurring ones can as easily trigger the SEMT-based HT and its malicious effect on the design, making them a concern even in commonplace devices and ICs. Further research and methodologies against them are of paramount importance, and the place to start is to create demanding benchmarks for evaluating their efficiency.

III. PROPOSED APPROACH

The evaluation of grid sensitivity across the IC constitutes the foundation of the proposed methodology, aiming to identify optimal regions for injecting the SEMT-driven HT based on circuits layout SER evaluation. In particular, each grid is treated as an individual sub-circuit and considered sensitive if the transient faults generated within its boundaries exhibit a high probability of resulting in soft errors.

Algorithm 1 Layout-driven SER evaluation

- 1: Read design files to identify placement and timing information.
- 2: Divide the circuit into grids to assess their vulnerability.
- 3: Inject a sufficient number of particle hits.
- 4: SER estimation through Monte Carlo simulations.
- 5: Apply DTA, SEMTs, and Masking Mechanisms.
- 6: SER evaluation for each grid and the entire circuit.

Algorithm 1 presents the layout-driven SER analysis in the presence of SEMTs. The first step involves parsing all relevant design files, which contain placement and timing information for each circuit to determine the exact location of each gate

along with its corresponding delay. In this way, SEMTs modeling is applied to identify which gates may be simultaneously affected by a single particle strike, while Dynamic Timing Analysis (DTA) is used to improve the accuracy of SET propagation analysis [9], [15]. Consequently, each circuit is divided into smaller regions—referred to as grids—to assess their vulnerability. To this end, a sufficient number of particle hits is injected into each grid to ensure the excitation of the entire die area. Finally, the proposed methodology integrates Monte Carlo simulation, SEMT analysis, and the modeling of masking mechanisms to evaluate the SER of both the entire circuit and its individual grids, since this metric directly reflects their susceptibility levels.

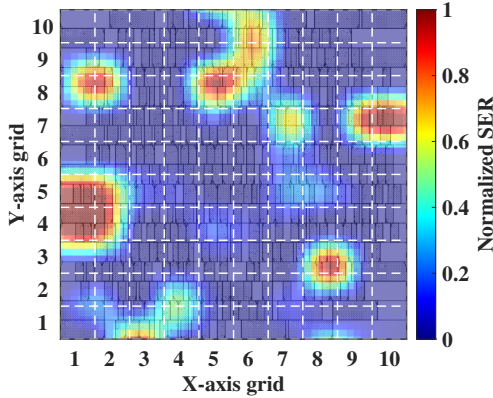


Fig. 3. Grid-based SER estimation of s1196 benchmark.

Fig. 3 illustrates the vulnerability profile of the ISCAS '89 s1196 benchmark, as computed utilizing Algorithm 1. Each grid is assigned a normalized SER value, highlighting varying levels of susceptibility to radiation (red color indicates higher vulnerability). This can be attributed to several factors, including the number of gates within the grid, the impact of masking effects, and the proximity to FFs [16]. This analysis guides the selection of sub-circuits (i.e., grids) for injecting SEMT-driven HTs. Specifically, trojans are injected at the outputs of the most sensitive gates within the selected grids. The objective is to assess whether the presence of SEMT-driven HTs increases the overall susceptibility of the grid, thereby making the circuit more vulnerable to soft errors.

Algorithm 2 outlines the subsequent steps of our methodology. Grids with the highest SER values are excluded from HT injection for two primary reasons. First, such regions are the perfect candidates for radiation-hardening techniques, such as Triple Modular Redundancy (TMR) and gate resizing, to be applied [17]. Second, SER denotes the probability of soft error generation per grid. As such, inserting a SEMT-driven HT into an already highly vulnerable region would have minimal additional impact. Thus, the optimum injection points are the grids with relatively lower SER values. In this work, any grid with a SER probability of 17% or less was considered appropriate and realistic for the injection. Note that this probability should be adjusted depending on the overall circuit susceptibility.

Algorithm 2 SEMT-driven HT injection

- 1: Implement Algorithm 1.
 - 2: Sort the grids based on their SER value.
 - 3: Choose as targeted grids those with SER value ≤ 0.17 .
 - 4: Exclude all the grids around the ones with the greatest SER values.
 - 5: Choose the most sensitive gates from the remaining grids.
 - 6: Extract from the selected gates the ones belonging to the critical timing paths.
 - 7: Pick up to 10% of the potential gates to be injected with the SEMT-driven HT.
-

Another critical factor to consider is the density of the injected HTs. A significant number of HTs in proximity may increase the likelihood of detection due to elevated power consumption and thermal signatures in the affected region. To mitigate this risk, the grids encircling the ones with the highest SER are excluded from the set of HT injection targets.

The final part of our algorithm involves selecting the targeted gates within the previously identified targeted grids. At this stage, the set of grids is already optimal, allowing for the selection of the most sensitive gates for the SEMT-driven HT injection. To minimize the impact on circuit timing and area, gates that belong to the critical path are excluded from consideration. Among the remaining gates, only up to 10% are selected for HT injection. The outcome of the proposed methodology is a challenging and effective benchmark that enables proper evaluation of detection techniques, which play a vital role in the ongoing effort to combat HTs.

IV. EXPERIMENTAL RESULTS

A. Experimental Setup

To evaluate our methodology, eight benchmarks from the ISCAS '89 suite were selected. The designs were synthesized using Synopsys Design Compiler, while floorplanning and place-and-route (PnR) were performed using Cadence Innovus. All experiments were conducted on a Linux machine with an 8-core Intel Xeon @3.5 GHz and 16 GB of memory. Each benchmark was evenly divided into square grids, with the number and size of grids adjusted to the circuits dimensions.

B. Methodology Evaluation

Table I presents the experimental results of the proposed methodology. Specifically, it highlights the impact of the SEMT-driven HT on the overall SER of each design, along with the percentage of targeted gates ultimately selected for injection. The total number of gates indicates the size of the each benchmark, while the number of FFs corresponds to the memory cells where soft errors may occur. Lastly, the table includes the percentage of the affected grids.

The first thing the results suggest is the importance of the quality in the placement of the trojans over their quantity in a circuit. For example, for the benchmark s9234 both the percentages of the targeted gates and the targeted grids are around 1%, yet the impact on the total SER of the benchmark is one of the highest among all the experiments, at +68%. Important factors in the effect of our methodology are the layout of the design after the floorplanning, as well as the

TABLE I
IMPACT OF THE SEMT-DRIVEN HT ON SER

Bench.	# Gates	# FFs	Targeted gates (%)	Targeted Grids (%)	Overall SER	Injected SER	Change (%)
s344	231	15	5.6	0.8	0.1758	0.1858	+5.69
s510	216	6	8.79	0.9	0.0768	0.0818	+6.51
s713	504	19	1.19	2.3	0.1232	0.1619	+31.51
s1196	596	17	8.6	3.6	0.0315	0.0539	+71.15
s1423	991	74	9.78	2.3	0.0119	0.0176	+ 47.78
s5378	3018	179	2.55	2.3	0.0095	0.0104	+9.11
s9234	6983	228	1.0	1.3	0.0084	0.0141	+68.43
s13207	9577	669	5.37	2.7	0.0024	0.0028	+16.70

masking mechanisms. This is evident from the fluctuations in the SER values after the insertion of the HTs, which do not follow a pattern in correlation either with the proportions of the circuits or with the final number of targeted gates. However, even if the magnitude of the effect is heavily dependent on the circuit, the results suggest that it is still sufficient attesting to the validity of the proposed methodology.

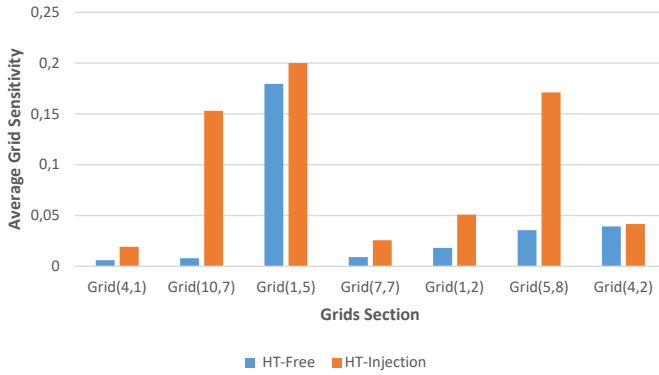


Fig. 4. Average targeted grids sensitivity before and after the HT injection.

In Fig. 4, we observe the SER evaluation before and after the HT injection for some indicative grids of the s1196 benchmark. According to the results presented in Table I, this benchmark was considerably more affected than the others due to the HT insertion, with an increase in SER of 72%. This is attributed to the fact that there are some grids, such as Grid(1,5) and Grid(5,8) (representing the Y and X axis, respectively, and according to Fig. 3) where the vulnerability level significantly increased. The basic reason for these results is that the HT injection in these regions leads to an increase in SEMT pulse widths, which results in more soft errors.

V. CONCLUSION

In this work, a comprehensive methodology is presented for the optimal placement of SEMT-driven HTs. The proposed approach efficiently determines the most susceptible circuit grids to identify the most effective gate locations for HT injection. First, we accurately estimate the SER of each region of a design and, subsequently, identify the appropriate grids and gates to insert the HTs. The results indicate that the proposed framework is expected to significantly increase the overall circuit vulnerability, by leveraging layout-driven SER analysis to identify the candidate grids for HT injection,

thus, contributing to the development of detection techniques against HT attacks.

REFERENCES

- [1] J. F. Ziegler, "Terrestrial cosmic rays," *IBM journal of research and development*, vol. 40, no. 1, pp. 19–39, 1996.
- [2] S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, "Hardware trojan attacks: Threat analysis and countermeasures," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1229–1247, 2014.
- [3] A. Sreedhar, S. Kundu, and I. Koren, "On reliability trojan injection and detection," *Journal of Low Power Electronics*, vol. 8, no. 5, pp. 674–683, 2012.
- [4] Y. Shiyankovskii, F. Wolff, C. Papachristou, D. Weyer, and W. Clay, "Exploiting semiconductor properties for hardware trojans," *arXiv preprint arXiv:0906.3834*, 2009.
- [5] A. Takou, P. Stoikos, M. Moysis, G. Floros, N. Evmorfopoulos, and G. Stamoulis, "An efficient security closure methodology for em-based attacks on power grid structures," in *2023 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, 2023, pp. 1–4.
- [6] P. Quintana, J. Mccollum, and W. A. Hill, "Single event effect hardware trojans with remote activation," 2017. [Online]. Available: <https://api.semanticscholar.org/CorpusID:53647140>
- [7] A. Takou, G.-I. Paliaroutis, P. Tsoumanis, N. Evmorfopoulos, and G. Stamoulis, "Sensitivity-aware hardware trojan injection for set propagation and soft error attacks," in *2024 20th International Conference on Synthesis, Modeling, Analysis and Simulation Methods and Applications to Circuit Design (SMACD)*. IEEE, 2024, pp. 1–4.
- [8] C. Georgakidis, D. Valiantzas, S. Simoglou, I. Lilitsis, N. Chatzivangelis, I. Golfos, M. Andjelkovic, C. Sotiriou, and M. Krstic, "Towards a comprehensive set analysis flow for vlsi circuits using static timing analysis," in *2023 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*. IEEE, 2023, pp. 1–6.
- [9] G. I. Paliaroutis, P. Tsoumanis, N. Evmorfopoulos, G. Dimitriou, and G. I. Stamoulis, "Multiple transient faults in combinational logic with placement considerations," in *2019 8th International Conference on Modern Circuits and Systems Technologies (MOCAS)*, 2019, pp. 1–4.
- [10] M. Choudhury, M. Gao, A. Varna, E. Peer, and D. Forte, "Transpose: Transitional approaches for spatially-aware lfi resilient fsm encoding," *arXiv preprint arXiv:2411.02798*, 2024.
- [11] R. Kumar, P. Jovanovic, W. Burleson, and I. Polian, "Parametric trojans for fault-injection attacks on cryptographic hardware," in *2014 Workshop on Fault Diagnosis and Tolerance in Cryptography*. IEEE, 2014, pp. 18–28.
- [12] A. Takou, O. Axelou, G. Floros, N. Evmorfopoulos, and G. Stamoulis, "An optimal methodology for em-based hardware trojan placement on clock tree networks," in *2023 IEEE 66th International Midwest Symposium on Circuits and Systems (MWSCAS)*, 2023, pp. 25–29.
- [13] H. Wei, W. Yueke, X. Kefei, and D. Wei, "Single event effect vulnerability analysis and on-orbit error rate prediction," in *2016 IEEE International conference on signal and image processing (ICSIP)*. IEEE, 2016, pp. 471–477.
- [14] B. Yin, L. Cai, H. Zhang, and W. Chen, "Electromigration based hardware trojan defense in integrated circuit," in *2024 2nd International Symposium of Electronics Design Automation (ISED)*. IEEE, 2024, pp. 504–509.
- [15] G.-I. Paliaroutis, P. Tsoumanis, D. Garyfallou, A. Vagenas, N. Evmorfopoulos, and G. Stamoulis, "Accurate soft error rate evaluation using event-driven dynamic timing analysis," in *2023 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, 2023, pp. 1–6.
- [16] G. I. Paliaroutis, P. Tsoumanis, N. Evmorfopoulos, G. Dimitriou, and G. I. Stamoulis, "A placement-aware soft error rate estimation of combinational circuits for multiple transient faults in cmos technology," in *2018 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, 2018, pp. 1–6.
- [17] C. Georgakidis, G. I. Paliaroutis, N. Sketopoulos, P. Tsoumanis, C. Sotiriou, N. Evmorfopoulos, and G. Stamoulis, "A layout-based soft error rate estimation and mitigation in the presence of multiple transient faults in combinational logic," in *2020 21st International Symposium on Quality Electronic Design (ISQED)*. IEEE, 2020, pp. 231–236.