Design and Simulation of Radiation Hardened SRAM Cell

Hitesh Paliwal[a], Pratyush Parashar[a], Sachindra Mane[a], Arun Dev Dhar Dwivedi*[b]
[a]Student
Department of Micro and Nano Electronics, School of Electronics Engineering
Vellore Institute of Technology, Vellore – 632014, Tamil Nadu, India.
[b] Associate Professor,
School of Electronics Engineering
Vellore Institute of Technology
Vellore – 632014, Tamil Nadu, India

E-mail:hitesh.paliwal2022@vitstudent.ac.in,pratyush.parashar2022@vitstudent.ac.in
mane.sachindra2022@vitstudent.ac.in, arundevdhar.dwivedi@vit.ac.in

***Abstract*—This paper introduces a novel approach aimed at enhancing the dependability of SRAMs utilized in space radiation settings. The presence of radiation-induced soft errors affects memory circuits, causing the alteration or disruption of their response. Consequently, safeguarding the memory unit becomes of utmost importance. Memory devices resistant to radiation find widespread applications in space-related contexts. To achieve error correction, the current verification process is conducted on the 6T-SRAM. The design's efficiency is evaluated by conducting tests to detect Single Event Upsets. These tests utilize the double exponential current model as the primary current source. To ensure the reliability of the design, it is thoroughly examined and confirmed using Cadence 180nm CMOS technology.**

Keywords—SRAM, Soft errors, Single event upset, Double exponential current mode

I. INTRODUCTION:

Radiation-induced soft errors pose a significant challenge to the reliable operation of electronic systems deployed in space, nuclear power plants, particle accelerators, and other high-radiation environments. These errors, also known as single-event upsets (SEUs), can cause unexpected bit flips in sensitive memory cells, leading to data corruption and system failures. SRAM cells are particularly susceptible to radiation-induced soft errors due to their high sensitivity to charge collection.

Addressing the critical need for enhanced radiation tolerance, this research paper focuses on the design and optimization of radiation-hardened SRAM cells. By developing robust and resilient SRAM cells, we aim to mitigate the impact of radiation-induced soft errors and improve the reliability of electronic systems operating in harsh radiation environments.

The objective of this research is to explore innovative techniques and circuit design methodologies that can effectively minimize the susceptibility of SRAM cells to radiation-induced soft errors. To achieve this goal, we will analyze the underlying physical mechanisms responsible for radiation-induced soft errors in SRAM cells. This analysis will enable us to identify critical weak points and vulnerabilities in the memory cell design. Subsequently, we will propose and evaluate novel architectural and circuit-level design solutions that are capable of mitigating the impact of soft errors and improving the robustness of SRAM cells.

The outcomes of this research have significant implications for numerous applications, including space exploration, satellite communication, nuclear reactors, and high-energy physics experiments. By developing radiation-hardened SRAM cells, we can enhance the reliability and longevity of electronic systems deployed in such challenging environments, reducing the risk of critical failures and safeguarding the integrity of mission-critical data.

Various approaches have been proposed to develop SRAM cells that are resilient to soft errors. These approaches can be categorized into three main categories: hardening of SRAM cell, recovery of SRAM cell and protection of SRAM cell. Hardening techniques involve adding additional circuitry to the SRAM cell, which may result in a duplication of transistors. Recovery techniques utilize current monitors within the SRAM cells to detect single event upsets and mitigate their effects. However, these techniques often face challenges in scalability. Protection methods employ capacitors within the SRAM cells to absorb extra available charges, offering adequate protection against soft errors. In this paper we are focusing on protection technique and will propose a new circuit to protect the SRAM cell.[1][2]

II. SINGLE EVENT TRANSIENT (SET)

When a radioactive particle interacts with a circuit, it generates electron-hole pairs. These pairs are then separated by the electrical field, resulting in the generation of a current. If the induced current is of

sufficient magnitude, it has the potential to alter the logic state of the transistor. The amplitude and duration of the current pulse are critical factors that determine whether the error spreads and if it can cause a logic failure in the digital circuit.

Four conditions must be fulfilled for a Single Event Transient (SET) to propagate and induce an error in a memory element:

1. The node where the SET originates should be sensitive.
2. The SET should occur either within a memory circuit node or should reach to a memory element.
3. Pulse magnitude and duration should have the ability to alter the memory state.
4. When pulse reaches the memory cell, it should be susceptible, creating the possibility for a bit flip to take place.

When a particle strikes an element, NMOS transistors generate broader pulses compared to PMOS transistors. Therefore, NMOS transistors are more likely to propagate errors. The critical charge, denoted as Qcrit, represents the minimum amount of charge required to change a binary state from “1" to a "0" or vice versa, but it must be less than the total stored charge. Qcrit is the difference between the charge at the storage node and the minimum required charge for correct reading by the sense amplifier[2][3].

III. Double Exponential Current Source:

The occurrence of a Single Event Transient (SET) involves the generation of a double exponential current signal when a charged particle or SEU strikes a node. This analytical model is commonly utilized to approximate the waveform of the transient current induced at the affected node. The current pulse exhibits a fast rise time followed by a gradual fall time.[4][5]

$$Iseu = \frac{Q}{T\alpha - T\beta}\left(exp^{-\frac{T}{T\alpha}} - exp^{-T/T\beta}\right)$$

$$Iseu(peak) = \frac{Q}{T\alpha - T\beta}$$

$$Qcrit = \int_0^{Tc} Iseu\,(t)dt$$

Iseu(peak): Peak value of the injected current pulse

Q: Total charge accumulated

Tα: Junction collection time constant

Tβ: Initial ion-track establishing time constant.

The constants Tα and Tβ are material-dependent and can be influenced by various factors, including technology node and other parameters. For the purposes of this research paper, we have chosen to utilize the recommended values of Tα=200ps and Tβ=50ps, as indicated in .

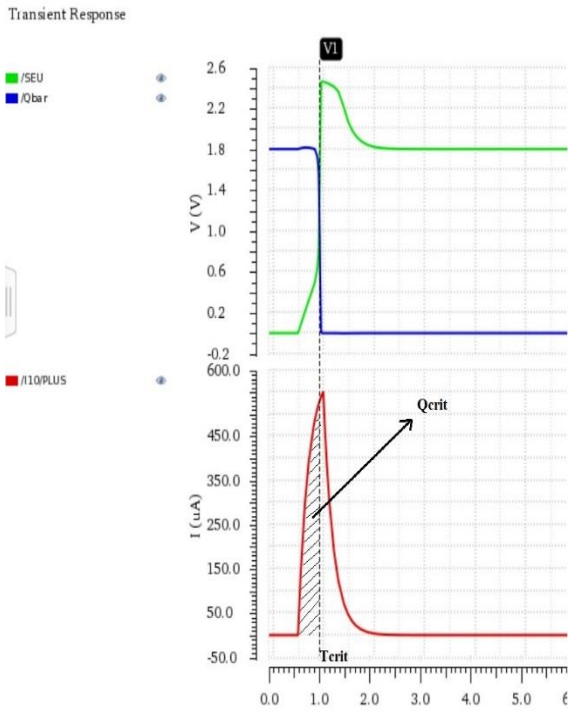

Figure 1: Critical charge Calculation

Critical Charge: It represents the threshold level of charge required on the storage node of the SRAM cell to ensure accurate detection and preservation of stored data, even in harsh radiation environments. Managing the critical charge effectively is of utmost importance to ensure the resilience and dependability of radiation-hardened SRAM cells in the face of radiation-induced effects.[6][7]

Recovery Time: The recovery time in radiation-hardened SRAM pertains to the duration required for memory cells to regain their data integrity and restore normal functioning following exposure to radiation-induced errors or upsets.

IV. Protection Circuit:

The SRAM cell consists of two nodes, Q and Qbar, which function as storage locations for the data stored within the cell. The data can be both read and written using the bit lines, BL and BLbar, respectively. The state of the SRAM cell is determined by the word line, WL. When the word line is active, the cell operates in a mode that allows both reading and writing operations. Conversely, when the word line is inactive, the cell enters a dormant state known as "standby" mode.

It is worth highlighting that the standby mode is particularly susceptible to a phenomenon called Single Event Upset (SEU). An SEU refers to a disturbance that has the potential to modify the data stored in the SRAM cell. Due to this vulnerability, most protection techniques are focused on safeguarding the SRAM cell during its standby mode. The primary objective is to prevent any unintended alterations to the stored information.

A. SRAM cell under the influence of SEU

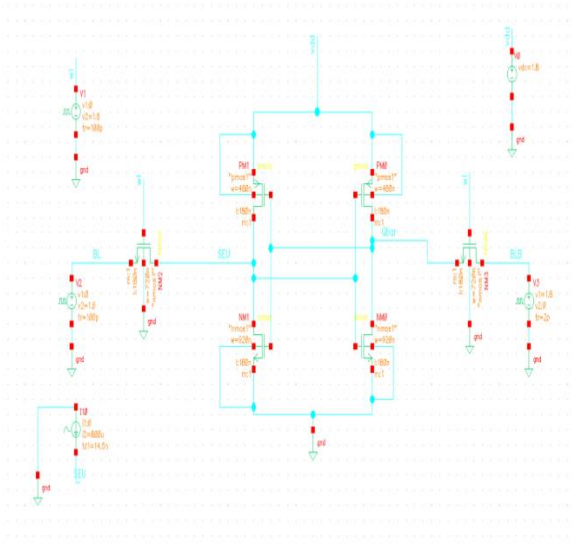

Figure 2:SRAM cell under the influence of SEU

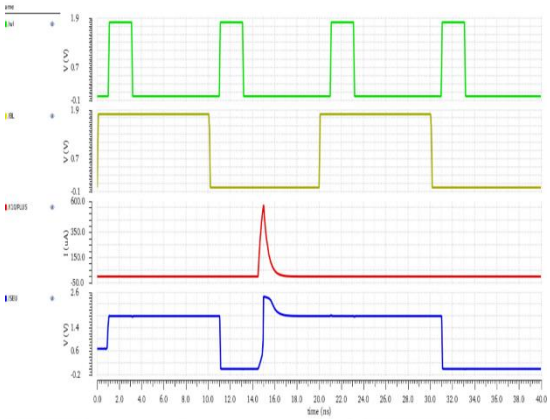

Figure 3:Graph of SRAM under the influence of SEU

B. SRAM Cell with Capacitance Protection

The capacitive-based protection models exhibit a common feature, which involves integrating capacitors as charge buffer nodes connected to the SRAM cell. While the specific configuration of these capacitors within the SRAM cell may vary among different models, the fundamental concept remains consistent.[7]

The purpose of incorporating capacitors is to establish buffer zones between the Q and Qbar nodes. This arrangement ensures that even if a Single Event Upset (SEU) occurs at one of these nodes, the overall state of the cell remains unaffected[10]. This is achieved by maintaining a constant potential difference between the Q and Qbar nodes.

The effectiveness of the SRAM's tolerance to SEU charges is determined by the size of the capacitors employed. Larger capacitors, characterized by a higher capacitance, result in elevated levels of charge tolerance. In other words, when larger capacitors are used, the SRAM cell becomes more resilient against SEUs.

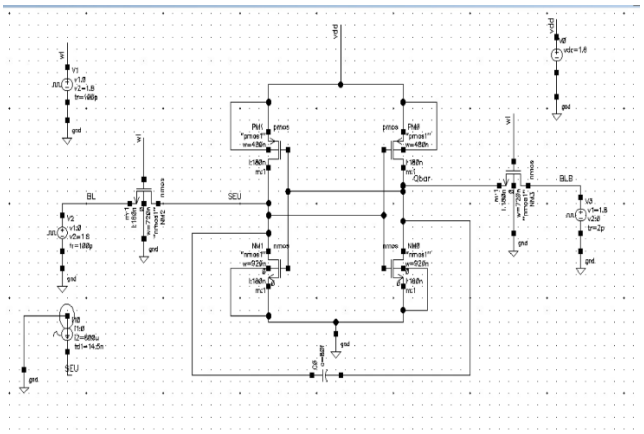

Figure 4: Schematic for Capacitance Protected SRAM cell

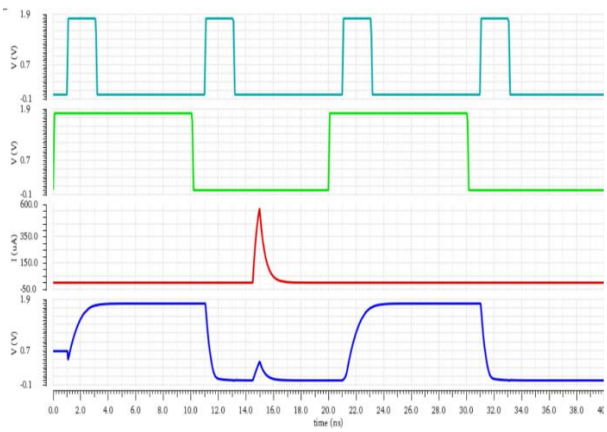

Figure 5:Graph of Capacitance Protected SRAM cell

The main disadvantage of incorporating capacitors in SRAM designs is their impact on the write mode's switching time. This represents a significant weakness observed in all these models. When capacitor nodes are introduced, the duration needed for the system to transition between different states during a write operation noticeably increases[9]. In

simpler terms, the process of writing data into the SRAM cell slows down due to the presence of capacitors. This elongated write time directly affects the overall performance of the SRAM cell, compromising the speed at which the cell can function. Consequently, this has a negative impact on the overall efficiency and responsiveness of the system utilizing the SRAM cell.

C. Proposed Circuit for SRAM Protection

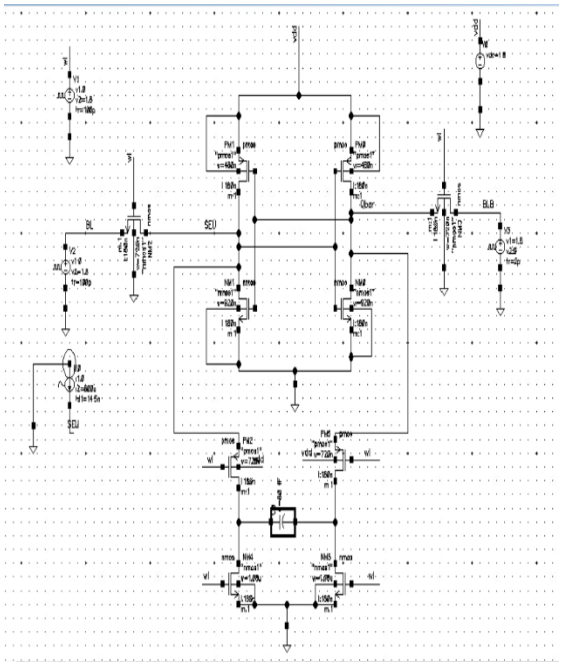

Figure 6 Proposed Circuit

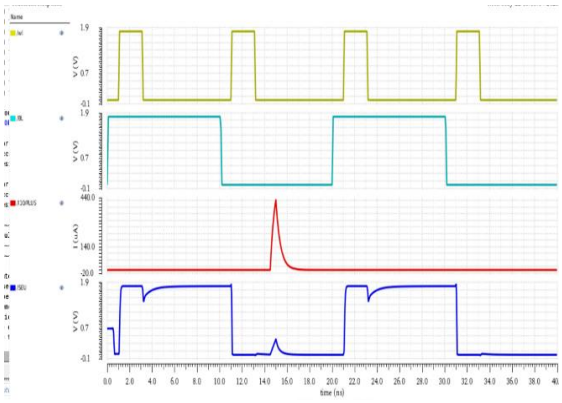

Figure 7:Graph for proposed SRAM Cell

V. OBSERVATIONS

1) Capacitance Protected SRAM Model

a. Write Time

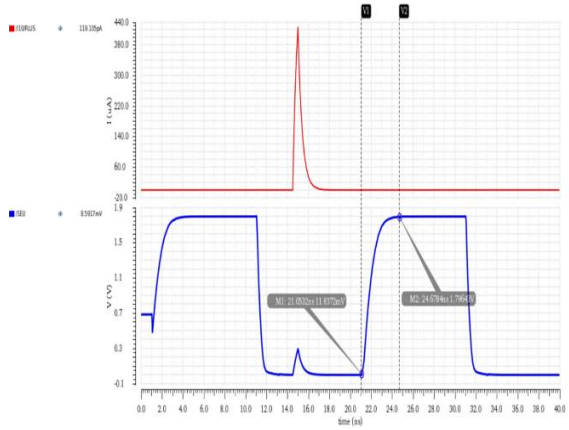

Figure 8:Graph for calculating write time of Capacitance Model

b. Recovery Time

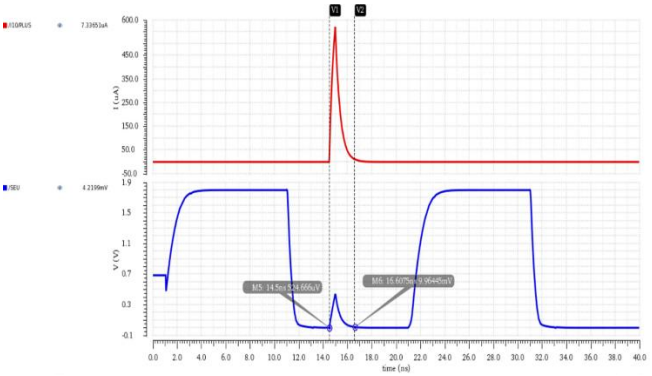

Figure 9: Graph for calculating recovery time of Capacitance Model

2) Proposed Circuit for SRAM Protection

a. Write Time

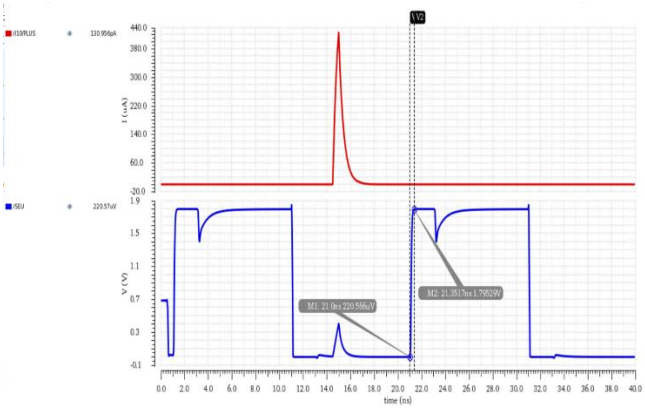

Figure 10: Graph for calculating write time of Proposed Model

b. Recovery Time

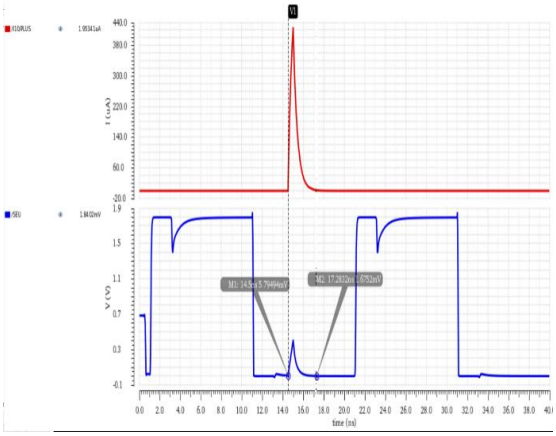

Figure 11:Graph for calculating recovery time of Proposed Model

Table 1 Write Time and Recovery Time for both the models

S.no	Model	Write Time (ns)	Recovery Time (ns)
1.	Capacitance Protected	3.625	2.107
2.	Proposed Circuit	0.3517	1.450

VI. CONCLUSION

This research paper has focused on enhancing the write time and recovery time of radiation-hardened SRAM cells. The study recognized the criticality of improving these parameters to ensure efficient and reliable operation of SRAM in radiation-prone environments, such as space or nuclear applications. Through extensive experimentation and analysis, various techniques and approaches were explored to enhance the write time of RH-SRAM cells. These includes investigating novel transistor configurations.The findings of this research demonstrated significant improvements in the write time of RH-SRAM cells, thereby enabling faster data storage and retrieval operations. Furthermore, the research also focused on enhancing the recovery time of RH-SRAM cells, which is crucial for maintaining data integrity after radiation-induced errors or upsets .The outcomes of this research underscore the importance of continuously improving the write time and recovery time of RH-SRAM cells to meet the stringent demands of radiation-prone applications. The advancements made through this study contribute to the overall reliability and performance of RH-SRAM technology, enabling its successful deployment in critical systems where radiation resilience is paramount.

VII. REFERENCES

[1]. Nicolaidis M, editor. Soft errors in modern electronic systems. Springer Science & Business

[2]. Diehl-Nagle SE, Vinson JE, Peterson EL. Single event upset rate predictions for complex logic systems. IEEE Transactions on Nuclear Science. 1984 Dec;31(6):1132-8

[3]. Friedman AL, Lawton B, Hotelling KR, Pickel JC, Strahan VH, Loree K. Single event upset in combinatorial and sequential current mode logic. IEEE Transactions on Nuclear Science. 1985 Dec;32(6):4216-8. Limbrick DB.

[4]. P. Hazucha and C. Svensson, “Impact of cmos technology scaling on the atmospheric neutron soft error rate,”IEEE Transactions on Nuclear Science, vol. 47, no. 6,pp. 2586–2594, 2000.

[5]. Mukherjee S. Architecture design for soft errors. Morgan Kaufmann; 2011 Aug 29.

[6]. F. Vargas and M. Nicolaidis, “Seu - tolerant sram design based on current monitoring,” Fault-Tolerant Computing, 1994. FTCS-24. Digest of Papers., pp. 106–115, 1994.

[7]. P. C. Murley and G. R. Srinivasan, “Soft-error monte-carlo modeling program, semm,” IBM J. RES. DEVELOP., vol. 40, no. 1, pp. 109–118, 1996.

[8]. L. Geppert, “A Static RAM Says Goodbye to Data Errors,” IEEE Spectrum, Feb. 2004

[9]. Media; 2010 Sep 24.Neto EH, Ribeiro I, Vieira M, Wirth G, Kastensmidt FL. Using bulk built-in current sensors to detect soft errors. Ieee Micro. 2006 Oct 16;26(5):10-8.

[10]. L. Atias, A. Teman, R. Giterman, P. Meinerzhagen and A. Fish, "A Low-Voltage Radiation-Hardened 13T SRAM Bitcell for Ultralow Power Space Applications," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 24, no. 8, pp. 2622-2633, Aug. 2016, doi: 10.1109/TVLSI.2016.2518220.