A SENSE AMPLIFIER BASED BULK BUILT-IN CURRENT SENSOR FOR DETECTING LASER-INDUCED CURRENTS

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR

THE DEGREE OF

M.Tech in Electronics and Communication Engineering

BY
Debjit Batabyal

Electronics and Communication Engineering

INDRAPRASTHA INSTITUTE OF INFORMATION TECHNOLOGY DELHI
NEW DELHI– 110020

July 2022

Acknowledgement

I would like to thank my advisor, Dr. Anuj Grover, who has immensely supported and guided me throughout my thesis work. I would also like to thank my co-advisor Dr. Ashish Kumar from STMicroelectronics for his support and insightful guidance during my thesis. Additionally, I would also like thank my Parents, Brothers and Friends who had been a source of constant support throughout the course of this project. Special thanks to the IIIT Delhi for giving me such an amazing research environment.

Abstract

Soft errors can occur when integrated circuits (ICs) are subjected to hostile conditions in space, the upper atmosphere, or even on Earth. For more than four decades, researchers have been studying similar phenomena. Among the different existing effects, Single-Event Effects (SEEs) caused by ionizing particles may cause the affected circuit to behave incorrectly. Since then, significant study has been devoted to the understanding and mitigation of SEEs in order to cope with the repercussions of such events. In this context, pulsed lasers were used to simulate SEEs at the experimenter's bench. However, pulsed lasers can be used to introduce defects (as a result of SEEs) into the computations of security-dedicated Integrated circuits in order to get the secret information they may store. Fortunately, additional strategies developed by the experts in the radiation community to minimize SEEs may be adopted to better deal with the issue of laser fault-injection. Monitoring the currents that occur with SEEs was a fruitful concept. The notion of Bulk Built-in Current Sensors (BBICS) was designed to monitor transient currents generated in the bulk of Integrated circuits when struck by ionizing particles or a pulsed laser.

This thesis work presents a novel approach to detect laser induced faults. This method uses a combination of sense amplifiers that evaluates the sampled substrate current in a time-interleaved manner. The proposed method can detect low-energy laser injection in the nanosecond range that does not always necessarily result in Single Event Transient (SET) / Single Event Upset (SEU). A current as low as 20 uA sustained for 10ns under typical operating conditions can be detected. It can also detect high-energy laser injection in the picosecond range that would result in SET or SEU. The design shows a leakage of 42 nA and consumes 41 nW/MHz at worst case. The simulations and analysis are being performed at 1.08 V using CMOS 65nm Low Standby Power (LSTP) process.

Research Papers under submission from this work

1. A Sense Amplifier Based Bulk Built-In Current Sensor for Detecting Laser-Induced Currents, VLSID (2023)

Contents

1 Introduction **1**
- 1.1 Laser Interaction with Silicon Matrix . . . 1
- 1.2 Single Event Effects (SEEs) . . . 2

2 Established Work **5**
- 2.1 Bulk Built-In Current Sensor (BBICS) Principles . . . 5
- 2.2 BBICS Architecture . . . 5
- 2.3 Limitations of the BBICS Architecture . . . 7

3 Proposed Architecture Iteration - 1 **9**
- 3.1 Motivation . . . 9
- 3.2 Circuit Diagram . . . 9
- 3.3 Design Components . . . 10
- 3.4 Design Decisions . . . 11
- 3.5 Mechanism of Operation . . . 12
- 3.6 Characterization and Simulation Results . . . 13
- 3.7 Design Validation . . . 15
- 3.8 Drawbacks of the proposed Architecture - Iteration 1 . . . 17

4 Proposed Architecture Iteration - 2 **18**
- 4.1 Motivation . . . 18
- 4.2 Circuit Diagram . . . 18
- 4.3 Design Components . . . 19
- 4.4 Design Decisions . . . 20
- 4.5 Mechanism of Operation . . . 21
- 4.6 Characterization and Simulation Results . . . 21
- 4.7 Design Validation . . . 24
- 4.8 Drawbacks of the proposed Architecture - Iteration 1 . . . 26

5 Final Proposed Architecture **28**
- 5.1 Motivation . . . 28
- 5.2 Circuit Diagram . . . 28
- 5.3 Detection Coverage . . . 29
- 5.4 Simulation Results . . . 31
- 5.5 Power and Leakage Estimation . . . 33
- 5.6 Comparison with Previous Works . . . 34
- 5.7 Layout Design . . . 35

6 Other Works - Proposed Design 2 **37**
- 6.1 Circuit Diagram . . . 37
- 6.2 Design Components . . . 37
- 6.3 Design Decisions . . . 38
- 6.4 Mechanism of Operation . . . 38

6.5 Simukation Results 39

7 Conclusion **42**

8 Future Work **43**

9 References **44**

List of Tables

3.1 Variation of Mean/Sigma of the Sense Amplifier 13

4.1 Variation of Mean/Sigma of the Sense Amplifier 22

List of Figures

1.1 Laser Intrusion in Silicon Matrix 1
1.2 Transient Current Profile due to laser Injection 2
1.3 The effect of induced current during laser intrusion on an Inverter [4] 3
1.4 A Single Event Transient in an Inverter [5] 3
1.5 A Single Event Upset in a Latch [5] 4

2.1 Principle of SEE detection by a nBBICS [1] [8] 5
2.2 Principle of SEE detection by a nBBICS [1] 6
2.3 Cross sectional view of an Inverter Monitored by BBICS showing the path of photocurrent [1] 8

3.1 A Sense Amplifier based design (Iteration - 1) used to detect laser induced transient current 9
3.2 Latching Circuit used with the Sense Amplifier 10
3.3 Variation of Resistance of NMOS used for sampling Photocurrent . 12
3.4 A current pulse is injected to the PWELL node 14
3.5 Minimum Detectable Injected Current at PWELL 15
3.6 Minimum Detectable Injected Current for confirm detection 16
3.7 Minimum Detectable Injected Current for No detection 16

4.1 A Sense Amplifier based design (Iteration - 2) used to detect laser induced transient current 18
4.2 Latching Circuit used with the Sense Amplifier 19
4.3 A current pulse is injected to the PWELL node 23
4.4 Minimum Detectable Injected Current at PWELL 24
4.5 A current pulse is injected to the PWELL node 25
4.6 Minimum Detectable Injected Current for No detection 25
4.7 Window Masking Effect in the Proposed Architecture iteration - 2 . 27

5.1 Two detectors Interleaved in Time Domain 28
5.2 A Double exponential current signal used for the simulations [2] . . 29
5.3 A double exponential current signal is fed into the PWELL node during the precharge phase of the First Detector 30
5.4 Minimum Detectable Injected Current at the PWELL 31
5.5 Minimum Detectable Induced Voltage at the PWELL 31
5.6 Minimum Detectable Injected Charge at the PWELL 32
5.7 Leakage Current of the Proposed Design 33
5.8 Total Power Dissipation of the Proposed Design 33
5.9 Minimum Detectable Injected Current comparison with the established work 34
5.10 Layout Design of the Proposed Design 35
5.11 Layout Design of the Proposed Design (Annotated) 36
5.12 Common Centroid Layout of NMOS M6 and M7 Transistors 36

6.1 Proposed Architecture - 2 37
6.2 Mechanism of Operation of the Proposed Architecture - 2 39
6.3 A double exponential signal is injected at PWELL node 39
6.4 Minimum Detectable Injected Current and Charge at the PWELL . 40
6.5 Minimum Detectable Induced Voltage at the PWELL 40
6.6 Comparison of Proposed Architecture - 1 and 2 showing Minimum Detectable Current at TT 25 ^{o}C 41

Chapter 1

Introduction

In secured Integrated Systems, hardware attacks can be carried out in various ways, including side-channel observation (for example, monitoring computing time, energy usage, or electromagnetic radiation) and exploitation of incorrect behavior. Fault-based attacks aim to obtain sensitive information, such as a secret cryptographic key. To retrieve the encryption keys, techniques like Differential Fault Analysis (DFA) exploit the discrepancies between the faulty and correct output response of encryption algorithms. The use of a laser is one of the most efficient methods of inducing defects in a circuit.

Lasers have evolved into one of the most effective techniques for breaching the security of integrated systems. The actual faults or defects introduced into the system are determined by various factors, including circuit technology node and laser properties. Understanding the physical impacts is required to appropriately analyze the potential implications of a laser-based attack throughout the design cycle and apply efficient counter-measures.

1.1 Laser Interaction with Silicon Matrix

When a laser strikes a CMOS device, the photoelectric effect converts its energy into electrical current. If the photons released by the laser have enough energy, they will form electron/hole pairs as they pass through the silicon. As a result of the photoelectric effect, two processes move the charges generated by the laser, resulting in a transitory current. In Fig. 1.1 [1], a reverse-biased PN junction is used to demonstrate these phenomena.

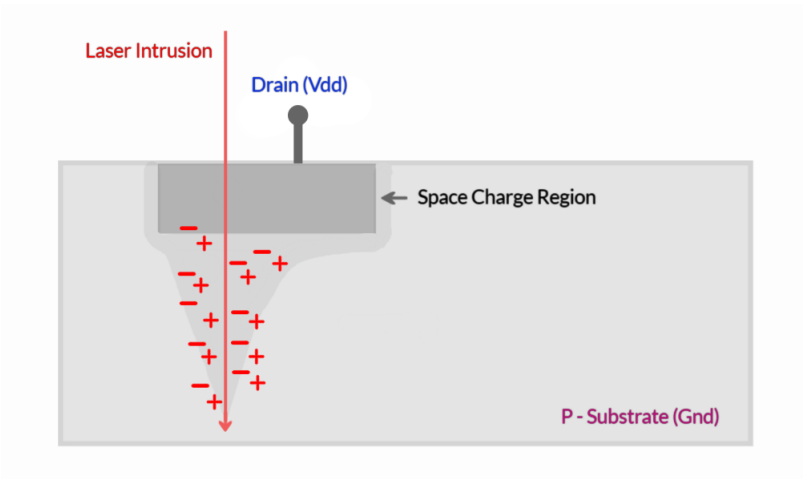

Figure 1.1: Laser Intrusion in Silicon Matrix

Biasing increases the region of the space charge area at the junction of the P and N regions. As the laser beam passes through the silicon and PN interface, electron and hole pairs are generated. The charges near the junction are then moved (attracted or repelled based on the polarity of charge) by the combined influence of the diffusion effect and the electric field. The charges away from the interface recombine without impacting the generated current at the junction's drain [2].

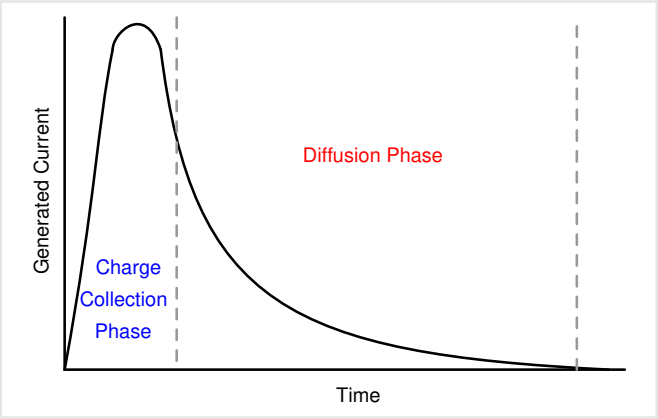

Figure 1.2: Transient Current Profile due to laser Injection

The typical shape of transient current induced due to the laser fault injection is depicted in Fig. 1.2. The diffusion and the electric field effects can be distinguished from the transient current characteristics. The prompt charge collection creates a large current in a short time due to the electric field effect. The diffusion-induced current has a lower amplitude and lasts longer than the prompt collection phase. This is owing to the rate at which the diffusion phenomenon occurs in silicon. The transient current can be realized from the following Equation [3].

$$I(t) = [Q/\tau_a - \tau_b] * [e^{-t/\tau_a} - e^{-t/\tau_b}]$$

With Q being the total charge generated during the laser inrusion, ta is the collection time which is depends on the process node, and the ion-track development time constant is tb, which is generally independent of process node. If the induced current during the laser intrusion is large enough to then it can briefly reverse the output of a logic circuit, thereby causing an error in computation.

1.2 Single Event Effects (SEEs)

When a laser travels through the silicon matrix, it generates electron and hole pairs. In general, these electrical charges recombine with little discernible influence on IC computations. On the other hand, the electric field seen in reverse-biased PN junctions can split the electron-hole pairs, resulting in a transient parasitic current. This generated transient current can change the voltage of the IC's internal nodes,

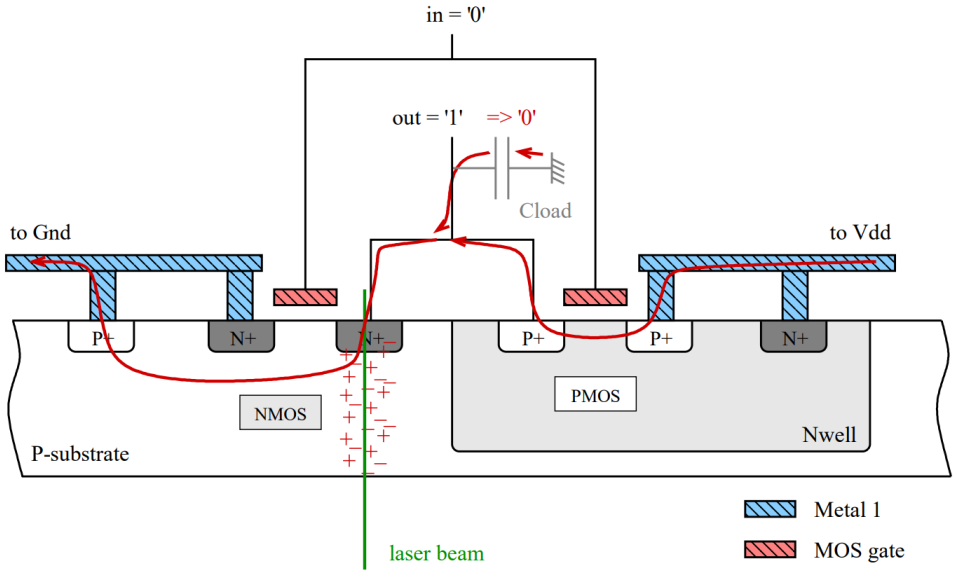

Figure 1.3: The effect of induced current during laser intrusion on an Inverter [4]

resulting in computational errors.

Initially, pulsed lasers were utilized to simulate SEE in integrated circuits for radiation hardness measurement. Since then, they have also been used to cause failures in secure circuits to retrieve secret data stored in that device.

A Single Event Transient (SET) is caused by high-intensity laser fault intrusion in a combinational logic circuit. As depicted in Fig. 1.3, SET propagates down the data path and generates computational errors. A photocurrent induced by laser fault intrusion is represented by a current source, as depicted in Fig. 1.4, which can be injected via the reverse-biased PN junction between the NMOS's N-type drain (biased at VDD) and P-type substrate (GND). As a result, the output voltage of the inverter may decrease from '1' to '0' if the injected photocurrent exceeds the saturation current of the PMOS transistor. As a result, this outputs voltage transient, also known as SET (Single Event Transient), may travel through the circuit logic, causing errors.

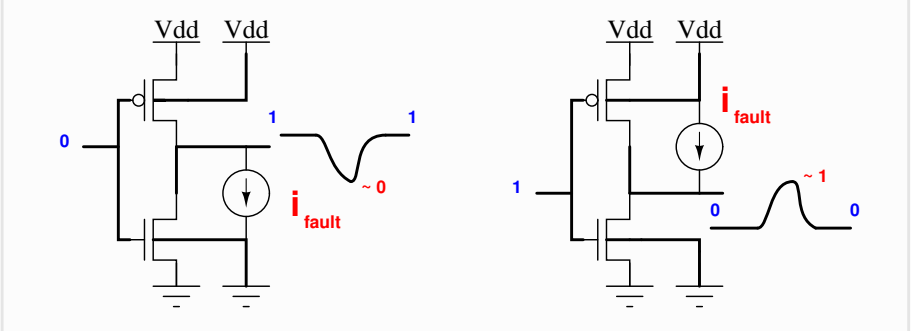

Figure 1.4: A Single Event Transient in an Inverter [5]

When a laser attack occurs in a memory element, such as a latch flipflop or a latch, the stored data is altered, causing a Single Event Upset (SEU), as depicted in Fig. 1.5. Similarly, an SRAM cell's core comprises two cross-coupled inverters. When a SET occurs in one of the two inverters, it spreads to the other, causing the cell to enter its opposite steady state. Because the cell is stable, it does not revert to its original state when the transitory current disappears, and the stored value is flipped.

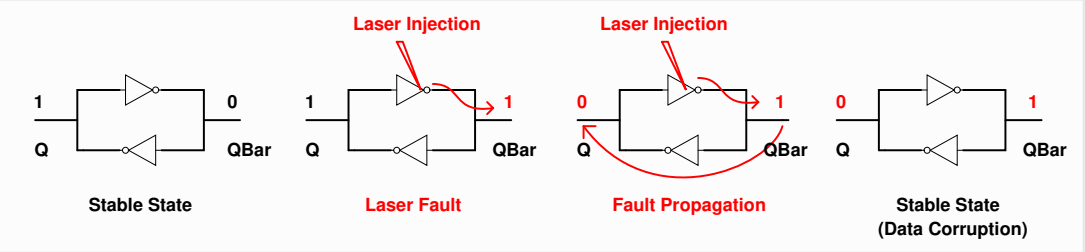

Figure 1.5: A Single Event Upset in a Latch [5]

Chapter 2

Established Work

2.1 Bulk Built-In Current Sensor (BBICS) Principles

Bulk currents produced during normal operation Integrated Circuits operation are in the range of few uA's, but during particle or laser-induced faults, bulk currents are typically more than two orders of magnitude that cause a Single Event Transient on the corresponding gate output. Bulk Built-In Current Sensors (BBICS) are built to take advantage of this feature by monitoring bulk currents. As a result, they may identify anomalous currents during a laser fault intrusion. The inclusion of a BBICS in between bulk (i.e., the P substrate) of NMOS transistors and the ground is represented in Fig. 2.1. As a result, any transitory photocurrent will pass via the BBICS, as shown.

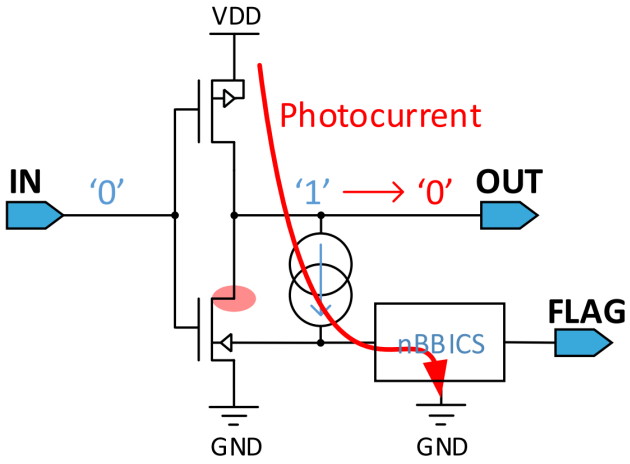

Figure 2.1: Principle of SEE detection by a nBBICS [1] [8]

The objective of the BBICS is to raise a warning flag, signaling that the circuit functionality may be disrupted. It should be noted that the BBICS must also provide bulk/body biasing for the transistor, as well as ground biasing in the case of NMOS. nBBICS is the term given to the BBICS that is used to monitor NMOS transistors. There are also pBBICS specialized for monitoring the PMOS transistors. Although pBBICS and nBBICS have distinct designs, they both rely on the same concept: monitoring bulk currents.

2.2 BBICS Architecture

Over the years, many BBICS architectures have been developed that monitor the bulk current in the PWELL and NWELL, relying on the above-explained principle. Among various architectures, the most common architecture that is being used is depicted in Fig. 2.2.

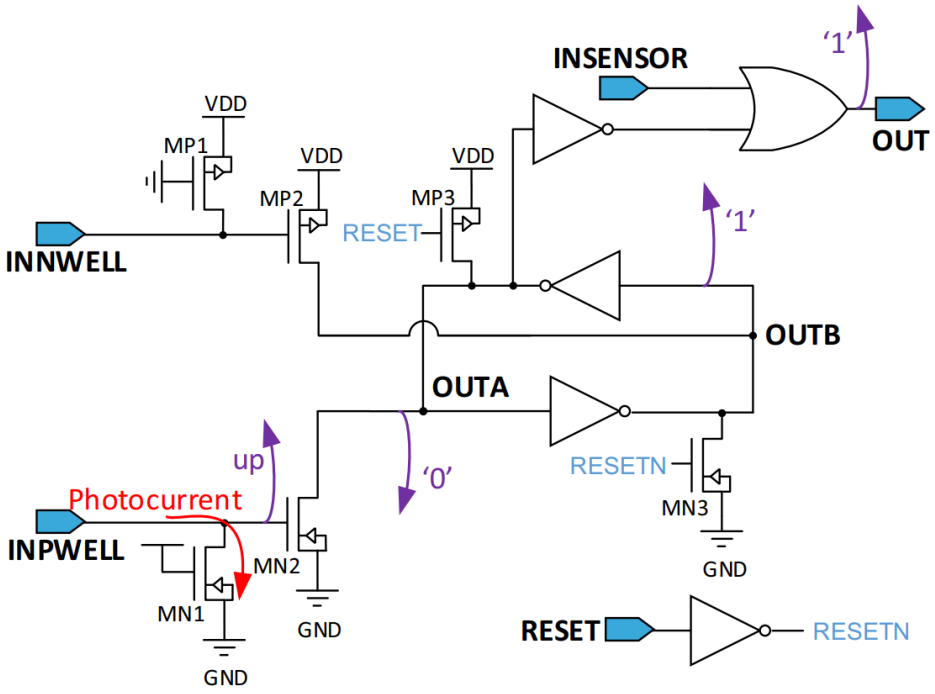

Figure 2.2: Principle of SEE detection by a nBBICS [1]

A double BBICS architecture is illustrated in Fig. 2.2. Its key feature is the ability to monitor both NMOS as well as PMOS transistors at the same time. The logic of a warning flag is stored using two cross-coupled inverters: OUT node. In monitoring mode, OUT rises to a high level to signify the detection of any unexpected rise in the bulk current but remains low during the normal operating condition. The INPWELL and INNWELL nodes are the BBICS connection points for biasing contacts of NMOS and PMOS bulks, respectively. At ground and VDD, transistors MN1 and MP1 are employed to bias the INPWELL and INNWELL nodes, respectively. Thus, it is ensured correct biasing of the corresponding bulk [8].

The transistors MN1 and MP1 are always in the ON state. The drains of transistors MN2 and MP2 are linked to the OUTA and OUTB nodes, respectively. The OUTA and OUTB nodes raise the alert flag in the event of a SEE. Thanks to transistors MP3 and MN3, the single BBICS design also provides a reset mechanism (RESET input). Finally, an OR gate and an inverter gate are inserted between OUTB and OUTA nodes. This helps accumulate various alarm flags by utilizing the INSENSOR input [].

When the laser intrusion induces a bulk current, OUTB and OUTA change their stable states in the latch, and the sensor's output (OUT) becomes '1'. To detect a slight change in its input voltage, thus the latch must be extremely sensitive. Because the latch retains a state if a transitory bulk current occurs, it must be reset after each acquisition.

The sequence of events associated with the detection of abnormal rise in the bulk current by a single BBICS is highlighted in purple, as depicted in Fig. 2.2. The scenario in which a radiative or laser-induced SEE aimed at an NMOS is being monitored by the BBICS; a substantial bulk current will flow to the ground via MN1 transistor. The red arrow in Fig. 3 denotes the direction of the Photocurrent. As a result, the voltage at the INPWELL node rises as denoted by the letter 'up'. Thus switching the MN2 transistor to transition from the OFF to the ON state, connecting node OUTA to the ground. Thus, the OUTB node will transition to logic 1 latching BBICS in alarm mode. Bulk currents in PMOS transistors exhibit a similar characteristic (due to transistors MP1 and MP2).

The sensitivity of the detector can be increased by skewing the core back-to-back connected inverters and also by employing MN2 and MP2 transistors in parallel. This would help in increasing the discharging or charging rate. Thus, during a laser attack, the OUTA node can discharge, or the OUTB node can charge at a faster rate.

2.3 Limitations of the BBICS Architecture

During a laser fault injection, the magnitude of the total photocurrent generated depends on the laser properties, process node, and temperature. Various limitations of the BBICS architecture are listed as follows:

- At lower temperatures, the magnitude of the peak current generated would be lesser as a lesser number of electrons would be available in the conduction band. So, more energy would be required for the electrons to jump from the valance band to the conduction band. Thus, higher sensitivity would be required at a lower temperature which is not the case for this architecture.

- The threshold voltage of the sampling transistor MN1 would vary highly with process corner and temperature. This would result in varying resistance and a varying amount of sampled voltage at the gate of the MN2 transistor. Thus, the sensitivity would vary highly with the temperature and process corner.

- The threshold voltage of MN2 would vary highly with process corner and temperature. The threshold voltage of MN2 would decrease with the increase in temperature. This would facilitate faster discharge of the OUTA node. Indicating lesser sensitivity at a lower temperature.

- To increase the sensitivity of the detector, the inverters in the latch can be skewed, but it might result in spurious detection at higher temperatures during normal operation. Also, this method would increase the leakage across the inverter.

- Most importantly, for the detector to respond to any laser fault intrusion, the sampled voltage should rise above the threshold voltage of MN2. Also, the discharge rate of MN2 should surpass the ON current of PMOS, supporting the logic value at the OUTA node. This might not always happen. Since a

laser fault intrusion may build up a voltage lesser than the threshold voltage of MN2. This can occur if laser attacks take place in the picosecond range.

- Photocurrents generated during the laser intrusion flowing to the ground from VDD can take two routes: through the BBICS tappings or to the chip GND. The broader arrow denotes the photocurrent's lower resistive route. Thus, the photocurrent will preferentially follow this less resistant channel; as a result, depending on the location of the laser spot (in relation to the biasing contacts), the photocurrent might flow partially via the PGN or BBICS taps, depending on their resistance. Therefore, the laser-induced transient current flowing through the BBICS might be diminished, decreasing its capability to detect SEE or laser attack. This phenomenon is depicted in Fig. 2.3 below.

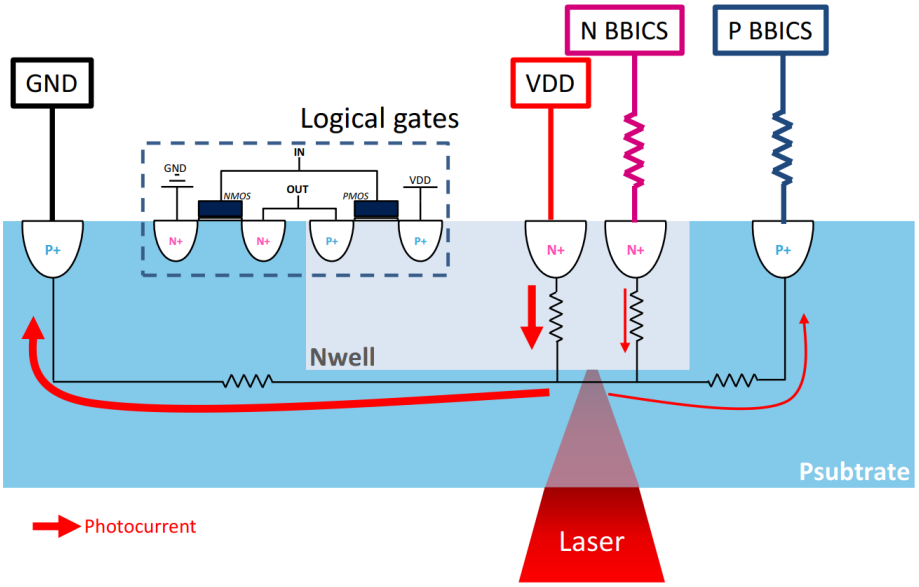

Figure 2.3: Cross sectional view of an Inverter Monitored by BBICS showing the path of photocurrent [1]

Chapter 3

Proposed Architecture Iteration - 1

3.1 Motivation

The existing BBICS architectures show good enough sensitivity, but still, there are some flaws that need to be addressed. The threshold voltage sampling NMOS would vary with respect to process and temperature. This would result in a varying value of sampled voltage owing to different sensitivity. Thus, some arrangements should be made to mitigate this issue.

OUTA node is driven by an always ON PMOS, which reduces the sensitivity towards a smaller transient current. This is because the discharging transistor needs to overcome the strength of an always-ON device.

3.2 Circuit Diagram

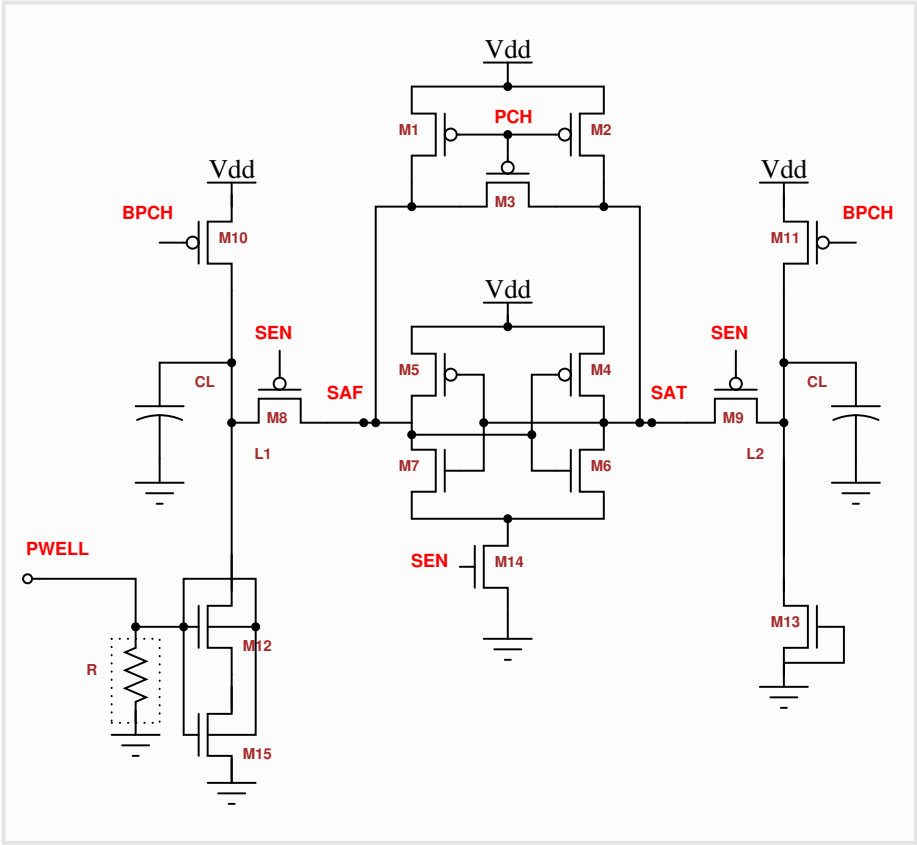

Figure 3.1: A Sense Amplifier based design (Iteration - 1) used to detect laser induced transient current

3.3 Design Components

The Proposed Architecture consists of a sense amplifier at its core. It also contains pre-charge circuits, a voltage sampling unit, load lines, discharging unit, and a latching circuit. The design is also comprised of various signals that facilitate the sensing operation.

The functionality of various parts of the proposed design is given as follows:

- Sampling Unit: The sampling unit here is a unsilicided P+ poly resistor (20 KOhms) that helps to sample the transient current generated during a laser fault intrusion in the form of voltage.
- Load lines: Load lines (5 fF) are connected to the precharge unit and the sense amplifier. They remains floating during the sensing phase. Any abnormal discharge in load lines indicates a laser fault intrusion.
- Precharge Circuits: The design contains two precharge circuits that precharge the load lines and internal nodes of the sense amplifier during the reset/precharge phase.
- Discharging Unit: The discharging unit comprises two NMOS in a stack that are dynamically body biased, facilitating the discharge of the load lines.
- Sense Amplifier: It senses the discharge suffered by the load lines during the

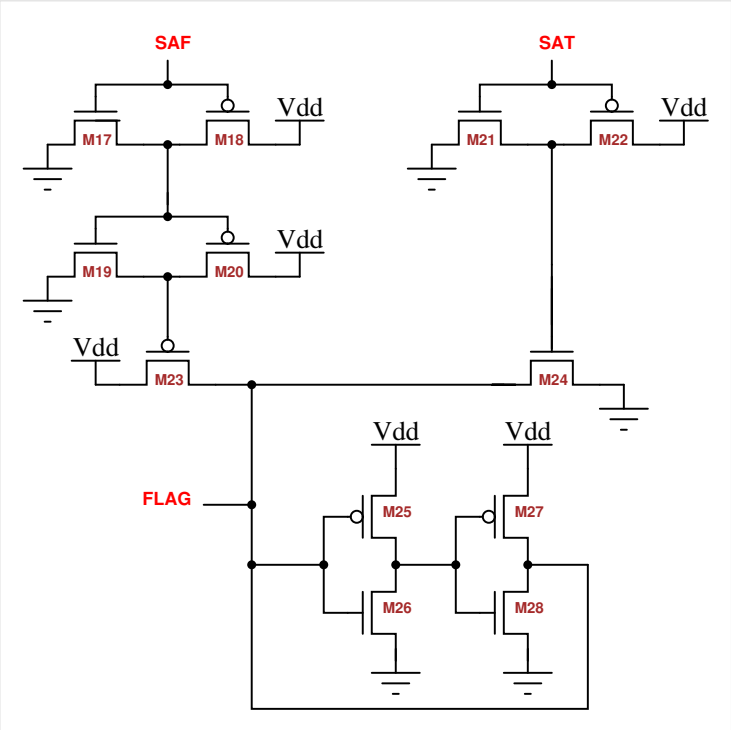

Figure 3.2: Latching Circuit used with the Sense Amplifier

sensing phase and dissolves the internal nodes into definite logic levels during the evaluation phase of the operation.

- Latching Circuit: It is connected to the internal nodes of the sense amplifier. Based on the logic levels of the internal nodes, it produces a FLag output that signifies whether there is a laser fault intrusion. The latching circuit used is depicted in Fig. 3.2.

  The latching circuit consists of inverters connected to the SAF and SAT nodes that transfer the logic levels to the connected PMOS and NMOS. Based on the logic levels, the Flag output is either charged or discharged by the PMOS and NMOS, respectively. The value of the Flag is then latched to the back-to-back connected inverters till the next evaluation phase.

The Operation of the proposed designed is fulfilled by using the signals discussed as follows:

- Precharge Signals: PCH and BPCH signals are taken low in every Precharge phase. PCH turns ON M1, M2, and M3 transistors that charge the internal nodes. BPCH turns on the M10 and M11 transistors that charge the load lines.

- Sense Enable Signal: SEN signal is taken to 1 during the evaluation phase of the operation, otherwise kept at 0. This ensures that Pass Gates M23 and M24 are ON.

  During the sensing phase, the pass transistors are turned OFF, and footer NMOS M14 is turned ON. This decouples the internal nodes from the load lines and internal nodes. Internal nodes are resolved to definite logic levels through positive feedback as they are discharged to the ground via M14.

3.4 Design Decisions

Various design decisions that are undertaken to optimize the sensitivity of the detector are given as follows:

- Instead of using an always ON NMOS for sampling the transient photocurrent, unsilicided P+ poly resistor is used. This is used to mitigate the effect of variation of the sampling transistor across different process corners. Also, this would help reduce the variation of the threshold voltage of NMOS with temperature. The variation of resistance across different process corners is depicted in Fig. 3.3.

- Dynamic body biasing is used to mitigate the variation of the threshold voltage of the discharging NMOSs (M12 and M15). This would help increase the discharge rate at slow corners and low temperatures.

- During the sensing phase, the load lines would be floating. Thus, there is no need to discharge them completely. Utilizing the sub-threshold conduction of M12 and M15 during a laser intrusion would be sufficient to raise a Flag.

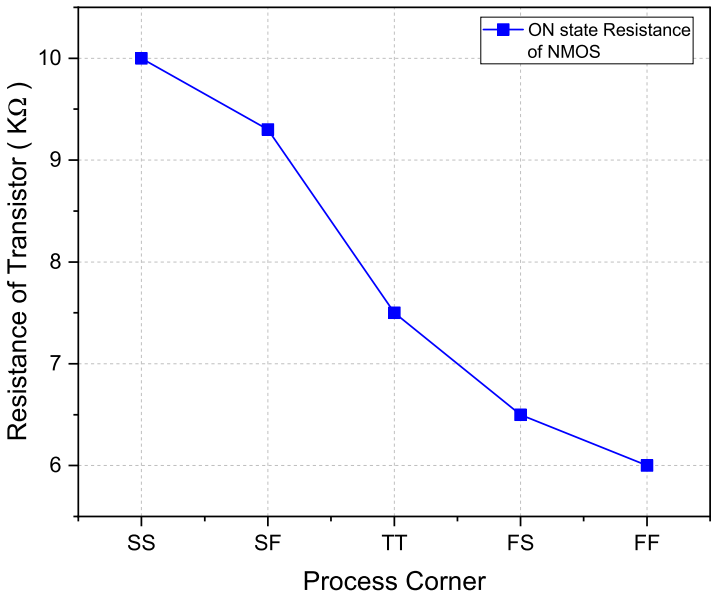

Figure 3.3: Variation of Resistance of NMOS used for sampling Photocurrent

From the Fig. 3.3 we can see that the variation of ON-Resistance of an always ON NMOS is +33% to -20% across the process. Where as the maximum variation of an unsilicided P+ poly resistor is $\pm 14\%$.

3.5 Mechanism of Operation

The proposed architecture is a synchronous design. The circuit is governed by various signals coordinated with each other. Each monitoring cycle consists of three phases: Precharge, Sensing, and Evaluation. Various phases of operation are explained as follows:

- Precharge Phase: During this phase, PCH and BPCH signals are taken low. The load lines and the internal nodes of the sense amplifier are charged to VDD. During this phase, the sense enable signal is at logic 0. Thus the footer NMOS M14 is OFF.

- Sensing Phase: During the sensing phase, the precharge signals are taken high. Thus Load lines and internal nodes of the sense amplifier are floating. During this phase, any laser fault intrusion would lead to the discharge of the load line through the M12 and M15 transistors. Also. since the SEN signal is low (M8 and M9 are ON), any discharge in the load line would be reflected to the internal nodes of the sense amplifier.

- Evaluation Phase: During this state, the Sense Enable signal is taken high. The precharge signals are kept high as well. The pass transistors M8 and M9 are turned OFF. This decouples the internal nodes from the load lines. Thus no further discharge at the load lines will not be reflected to the internal nodes.

The footer NMOS M14 is also turned ON, facilitating the discharge of the internal nodes. Based on the voltage level of the internal nodes, they are resolved to definite logic levels through positive feedback. The latching circuit updates the Flag based on the logic resolved by the sense amplifier.

3.6 Characterization and Simulation Results

To avoid any spurious detection, the sense amplifier is skewed sufficiently such that during no normal operation when there is no laser attack, the always Flag is at 0. In order to do so, the size M6 is taken 2.5 / 0.18 and M7 is 0.5 / 0.18. So, during normal operation SAT node will always discharge since the drive strength of M6 is sufficiently greater than M7.

During a laser fault intrusion, the SAF node will discharge much more than SAT during the sensing phase. A positive detection response will be produced when the discharge of the Load line and SAT node is sufficiently greater to overcome the skewness of the sense amplifier. The sizing of the pulldown devices (M6 and M7) is taken such that during regular operation, the SAT node discharge with 3-sigma confidence in the worst case.

Process	**Temperature (C)**	**Mean (mV)**	**Sigma (mV)**	**Mean / Sigma**
SS	-40	45.13	11.86	3.8
	25	67.9	11.2	6.02
	125	119.63	11.52	10.38
TT	-40	46.57	12.06	3.86
	25	77.88	11.96	6.51
	125	121.15	11.62	10.42
FF	-40	46.51	12.42	3.74
	25	78.29	12.23	6.4
	125	122.3	11.83	10.33
FS	-40	50.52	11.67	4.32
	25	81.6	11.63	7.01
	125	125.68	11.45	10.97
SF	-40	41.05	12.46	3.29
	25	72.8	12.29	6.41
	125	115.69	11.92	9.7

Table 3.1: Variation of Mean/Sigma of the Sense Amplifier

The operating frequency for design at the initial phase is taken as 40 MHz (T = 25 ns) for the proof of concept. The precharge phase is taken as 5ns, the sensing phase is 13.75 ns, and the evaluation phase is 6 ns. To avoid any abrupt leakage of the load line L1 during a regular operation, two NMOS are used in a stack.

Dynamic body biasing is used to enhance the sensitivity at cold and slow corners.

This helps us to lower the threshold voltage of M12 and M15 transistors. LVT is used for M12 and M15. Also, M13 is used as an LVT device to balance the leakage during regular operation.

To simulate the sensitivity of the circuit in the initial phase of design, a current pulse is used to simulate. This is only used to simulate the sensitivity of the design, later replaced by a double exponential current function depicted in the figure. At various corners, the current signal is injected at the PWELL node of the design, and values of voltage and current are recorded. The graph is given below, Fig. 3.4, depicts the operation of the design.

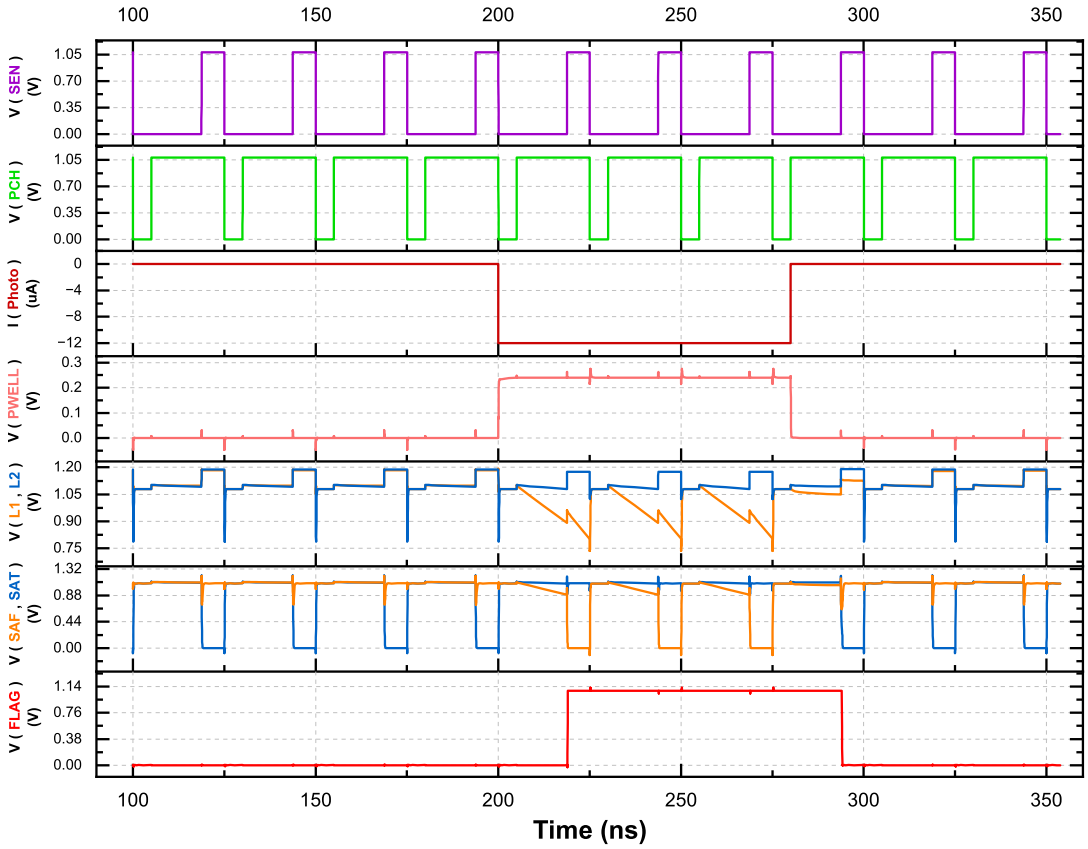

Figure 3.4: A current pulse is injected to the PWELL node

As illustrated in the figure, after the current pulse is injected, the load line L1 discharges. In the evaluation phase, the SAF and SAT nodes are resolved to 0 and 1, respectively. The latching circuit sets the Flag high by evaluating SAF and SAT nodes. As soon as the value of the injected pulse is reduced to 0, the Flag also goes to zero, indicating a self-resetting mechanism.

Similarly, a current pulse was injected into the PWELL node to test the design's sensitivity at different temperatures and corners. The values of current and voltage at the PWELL node are recorded. The sensitivity at various process corners is recorded in the Fig. 3.5.

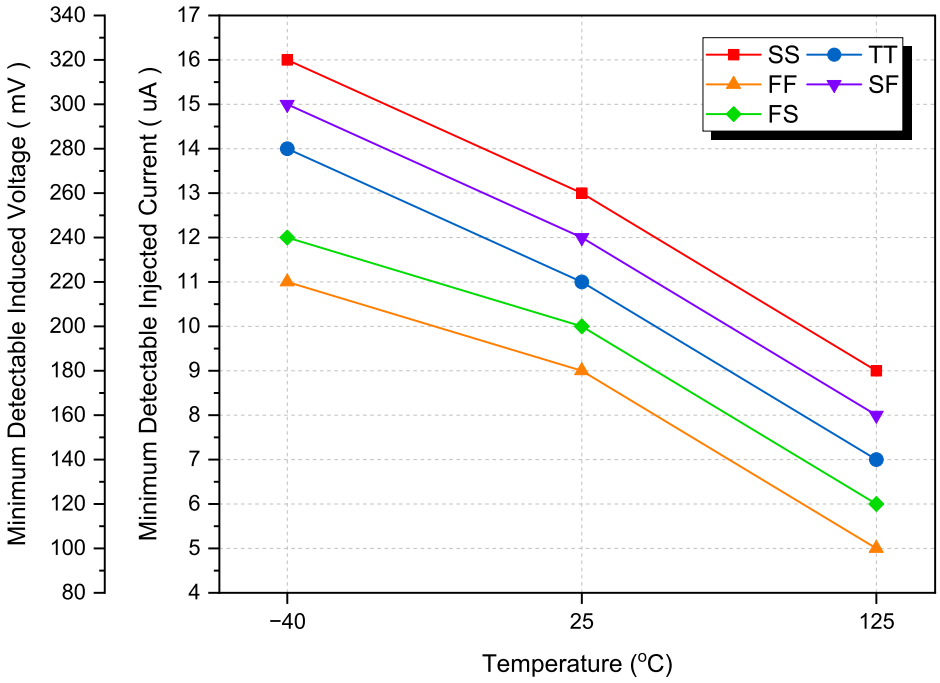

Figure 3.5: Minimum Detectable Injected Current at PWELL

From the above figure, it can be deduced that the sensitivity at FF 125 C is highest. This is because the threshold voltage of the transistor would reduce at FF 125 C. Thus, the stack of NMOS M12 and M15 would leak more with lesser induced gate voltage. Similarly, the sensitivity of the SS -40 would be worst since the threshold voltage will increase at SS -40. Also, in general, the sensitivity is more at higher temperatures and lower at cold. This is because the leakage increases at higher temperatures due to threshold voltage lowering.

3.7 Design Validation

To validate the design for the case of false detection 1000 Monte Carlo simulations are run. This is done to check the minimum current for no detection and confirmed detection. The case of confirmed detection is depicted in Fig. 3.6. It can be inferred that at lower temperatures and slow corners, it takes more current for detection, indicating a lower sensitivity. Similarly, it is evident that the sensitivity is high at higher temperatures and Fast corners.

The case for no detection is also depicted in Fig. 3.7. From the figure, it can be inferred that the current requirement is significantly less at higher temperatures and fast corners. Thus, such a detection system should always be validated at higher temperatures and fast corners to avoid a false alarm. A minimum no detection margin should be maintained to avoid any false alarms and hence the robustness of the design. For a given process and temperature, the region between the no detection and confirmed detection threshold is in the region of uncertainty. Any current injection between this region may not get detected.

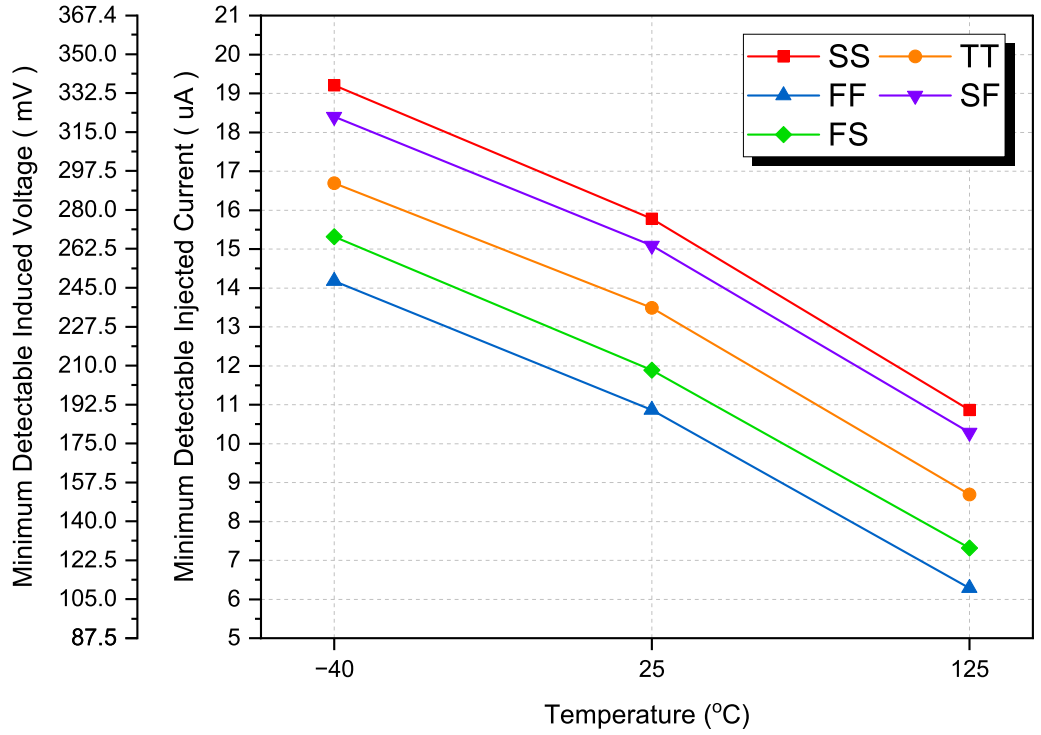

Figure 3.6: Minimum Detectable Injected Current for confirm detection

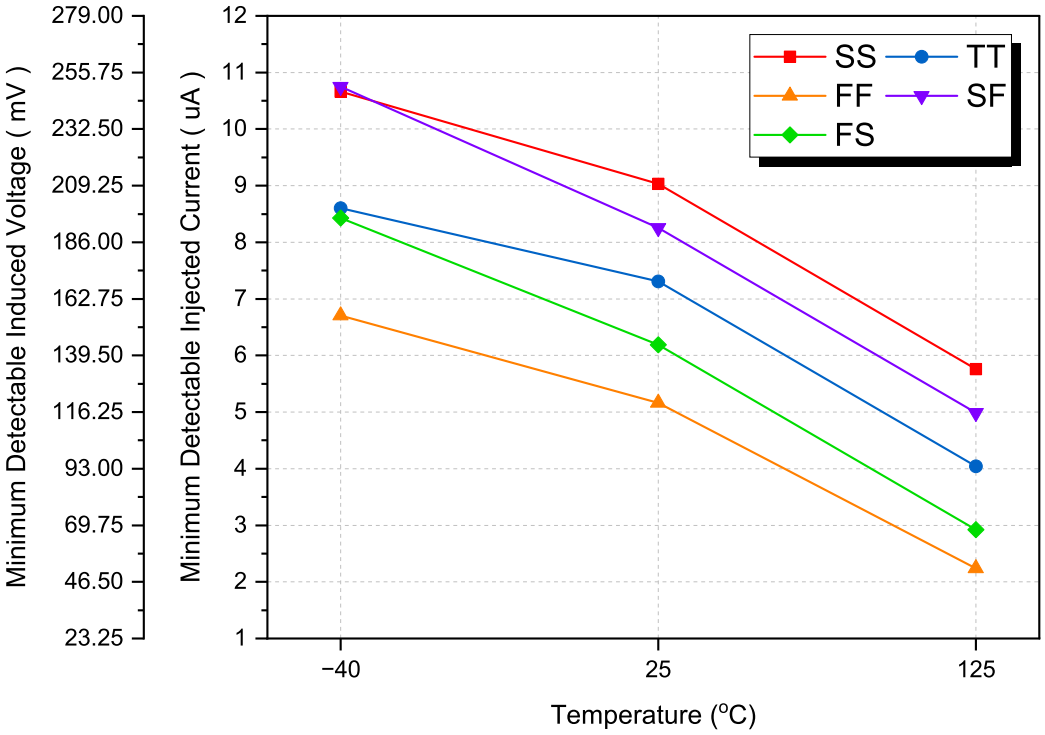

Figure 3.7: Minimum Detectable Injected Current for No detection

3.8 Drawbacks of the proposed Architecture - Iteration 1

The proposed architecture (iteration - 1) addresses and resolves various drawbacks of the established design. However, some issues still need to be addressed and resolved. Various drawbacks of the proposed architecture (iteration - 1) are as follows:

- The skewness of the sense amplifier varies highly with the process and temperature. This results in varying sensitivity across the process and temperature. Thus, instead of skewing the sensitivity of the pulldown devices, some alternate methods need to be used.
- The sensitivity of the design with respect to temperature is not constant or favorable. This is due to the varying discharge rate of M12 and M15. Thus, the discharge rate should be regulated at a higher temperature.
- The value sampling resistance used is high. It should not be kept too high; else to current sunk would reduce. It should be kept comparable to the ON resistance of an NMOS device.
- The sensitivity obtained is generally lower at cold, but the amount of photocurrent generated would also be low. At higher temperatures, more photocurrent would be generated because electrons would require less energy to jump from the valance band to the conduction band. Thus, the sensitivity should be higher at a lower temperature.

Chapter 4

Proposed Architecture Iteration - 2

4.1 Motivation

The proposed design in the iteration - 1 addresses various issues of the established work, but some design flaws also need to be addressed. The skewness of the sense amplifier varies highly with the process and temperature. This results in varying sensitivity across the process and temperature. The sensitivity of the design with respect to temperature is not constant or favorable. This is due to the varying discharge rate. The value sampling resistance used is high. It should be kept comparable to the ON resistance of an NMOS device. The sensitivity obtained is lower at cold. Though the amount of photocurrent generated would also be low at cold. Thus, the sensitivity of the detector at cold should be enhanced.

4.2 Circuit Diagram

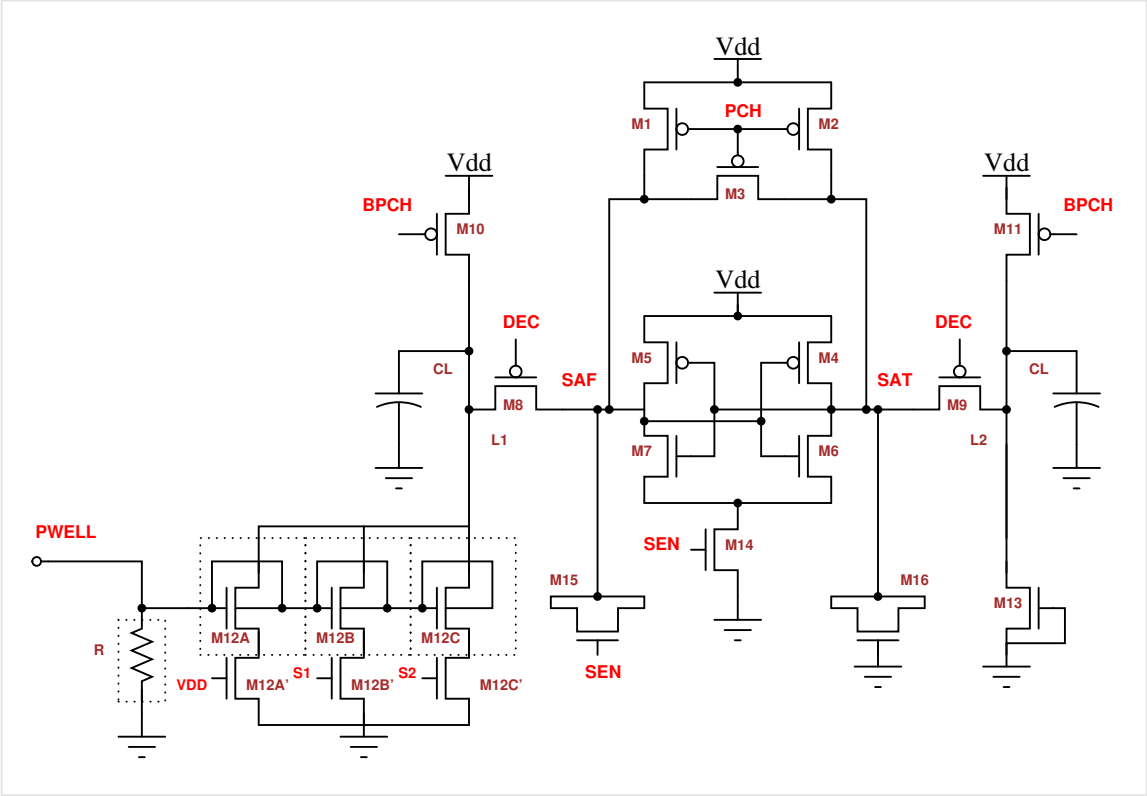

Figure 4.1: A Sense Amplifier based design (Iteration - 2) used to detect laser induced transient current

4.3 Design Components

The Proposed Architecture iteration - 2 also consists of a sense amplifier at its core. It also contains pre-charge circuits, a voltage sampling unit, load lines, discharging unit, and a latching circuit. The design is also comprised of various signals that facilitate the sensing operation.

The functionality of various parts of the proposed design is given as follows (already discussed sections are omitted):

- Sampling Unit: The sampling unit used here is a P+ Poly High Resistor (12 KOhms) that helps to sample the transient current generated during a laser fault intrusion in the form of voltage. The sampling resistance used in this case is also not too high and is comparable to the ON resistance of an NMOS.
- Discharging Unit: In this case, the discharging unit comprises 3 stacks of NMOSs between the load line (L1) and GND. The first NMOS transistor in each stack that is dynamically body biased facilitates the faster discharge of the load lines. The second NMOS in the stack is regulated by signals (S1, S2, and VDD) to control the discharge rate as per requirement.
- MOSCAP: MOS capacitance (M15 and M16) selectively inject charge to the internal nodes of the sense amplifier. This is used to create an imbalance.

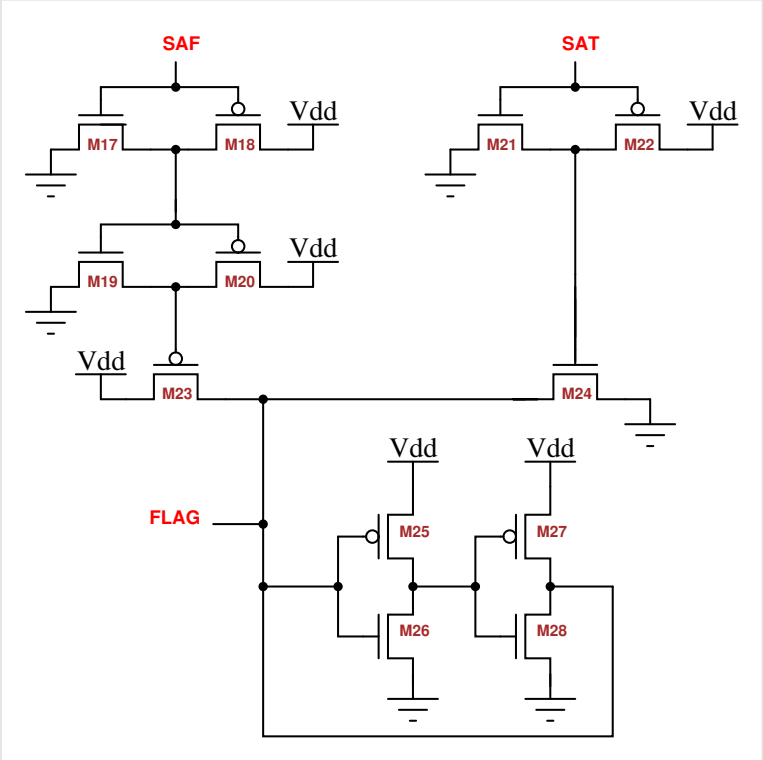

Figure 4.2: Latching Circuit used with the Sense Amplifier

The Operation of the proposed design is fulfilled by using the signals discussed as follows:

- Precharge Signals: PCH and BPCH signals are taken to 0 in every Precharge phase. PCH turns ON M1, M2, and M3 transistors that charge the internal nodes. BPCH turns on the M10 and M11 transistors that charge the load lines.

- Sense Enable Signal: SEN signal is taken high during the evaluation phase of the operation. It is kept low during the precharge and evaluation phase. During the sensing phase, the footer NMOS M14 is turned ON. Internal nodes are resolved to definite logic levels through positive feedback as they are discharged to the ground via M14.

- DEC signal: DEC signal is taken to 0 during the sensing phase. This ensures that Pass transistors M23 and M24 are ON. DEC signal is high during the precharge and the evaluation phase. Thus, ensuring the load lines are decoupled from the internal nodes of the sense amplifier.

  DEC signal must be taken high slightly before the SEN signal goes to 1. This is to ensure the injected charge is only fed to the internal nodes of the sense amplifier and not to the load lines.

- S1 and S2: These are the signals controlled by the operating temperature. S1 is set high as soon as temperature falls below 25 degrees Celsius. S2 is set high as soon as temperature falls below 0 degrees Celsius.

  These signals helps to regulate the discharge rate of the load line (L1) during a laser fault intrusion

4.4 Design Decisions

Various design decision that is undertaken to optimize the sensitivity of the detector is given as follows:

- Instead of using high sampling resistance, lower sampling resistance comparable to the ON resistance of the NMOS device is used.

- Temperature-sensitive signals are used to mitigate the varying discharge rate of L1. This would help increase the discharge rate at cold when the threshold voltage of the device increases.

- Instead of skewing the pulldown, devices of sense amplifier charge injection are used to create imbalance. This would reduce the process and temperature variation.

4.5 Mechanism of Operation

The proposed architecture is a synchronous design. The circuit is governed by various signals coordinated with each other. Each monitoring cycle consists of three phases namely: Precharge Phase, Sensing Phase and Evaluation Phase. Various phases of operation are explained as follows:

- Precharge Phase: During this phase PCH and BPCH signals are taken low. The load lines and the internal nodes of the sense amplifier are charged to VDD. During this phase the sense enable signal is at logic 0. Thus the footer NMOS M14 is OFF. Also DEC signal is kept high that decouples the internal nodes from the sense amplifier.

- Sensing Phase: During the sensing phase the precharge signals are taken high. Thus Load lines and internal nodes of the sense amplifier are in the floating state. During this phase any laser fault intrusion would lead to the discharge of load line through the discharging unit. Also. Durinn this phase the DEC signal is low so (M8 and M9 are ON), any discharge in the load line would be reflected to the internal nodes of the sense amplifier.

- Evaluation Phase: During this state the Sense Enable signal is taken high. The PCH and DEC signals are kept high as well. The pass transistors M8 and M9 are turned OFF. This decouples the internal nodes from the bitlines. Thus no further discharge at the loadlines will not be reflected to the internals nodes.

  The footer NMOS M14 is also turned ON. This facilitate the discharge of the internal nodes. Based on voltage level of the internal nodes they are resolved to definite logic levels through a positive feedback. The latching circuit updates the Flag based on the logic resolved by the sense amplifier.

4.6 Characterization and Simulation Results

In order to avoid any spurious detection the sense amplifier is skewed sufficiently such that no false alarm is triggered during normal operation. When there is no laser attack always Flag is at 0. In order to do so, MOSCAPs are used inject charge at the SAF node of the sense amplifier. The charge is injected during the onset of evaluation phase. This would increase the voltage at SAF node by 200 - 250 mV. Thus, SAT node always discharges during the normal operation.

During a laser fault intrusion SAF node will discharge much more than SAT during the sensing phase. A positive detection response will be produced when the discharge of the Load line and SAF node is sufficiently greater to over come the skewness of the sense amplifier due to charge injection. The sizing of MOSCAP (M15 and M16) are taken such that during normal operation the SAT node discharge with atleast 3-sigma confidence at worst case. Also, to maintain similar sensitivity as the previous iteration.

Process	Temperature (C)	Mean (mV)	Sigma (mV)	Mean/Sigma
SS	-40	43.16	9.25	4.66
	25	43.64	9.32	4.68
	125	41.81	9.39	4.45
TT	-40	45.43	9.43	4.81
	25	45.21	9.48	4.76
	125	44.34	9.56	4.63
FF	-40	48.30	9.59	5.03
	25	48.16	9.65	4.99
	125	47.24	9.78	4.83
SF	-40	45.86	9.36	4.89
	25	45.95	9.43	4.87
	125	45.48	9.56	4.75
FS	-40	45.02	9.46	4.75
	25	44.61	9.5	4.69
	125	43.49	9.6	4.53

Table 4.1: Variation of Mean/Sigma of the Sense Amplifier

It can be inferred from the table that the sense amplifier used has constant Mean/Sigma value. The amount of charge injected to the SAF will be same across process and temperature. Thus, the sense amplifier would have same sensitivity with change in process and temperature.

To enhance the sensitivity at cold and slow corners dynamic body biasing is used. This help us to lower the threshold voltage of M12A, M12B and M12C transistors. Also, LVT devices are used for M12A, M12B and M12C. Also, M13 is taken as a LVT device to balance out the leakage during the normal operation.

The operating frequency for design is taken as 100 MHz (T = 10 ns) for the proof of concept. The precharge phase is taken as 1.5ns, the sensing phase is 2.5 ns and evaluation phase is 5.9 ns.

To simulate the sensitivity of the circuit in the initial phase of the design a current pulse is used to simulate. This is only used to simulate the sensitivity of the design, later replaced by an double exponential current function depicted in figure. At various corners the current signal is injected at the PWELL node of the design and values of voltage and current recorded. The graph given below Fig. 22 depicts the operation of the design.

As illustrated in the figure after current pulse is injected the load line L1 discharges. In the evaluation phase the SAF and SAT nodes are resolved to 0 and 1 respectively. The latching circuit sets the flag high by evaluating SAF and SAT node. As soon as the value of the injected pulse reduced to 0 the Flag also goes to zero, indicating a self reseting mechanism.

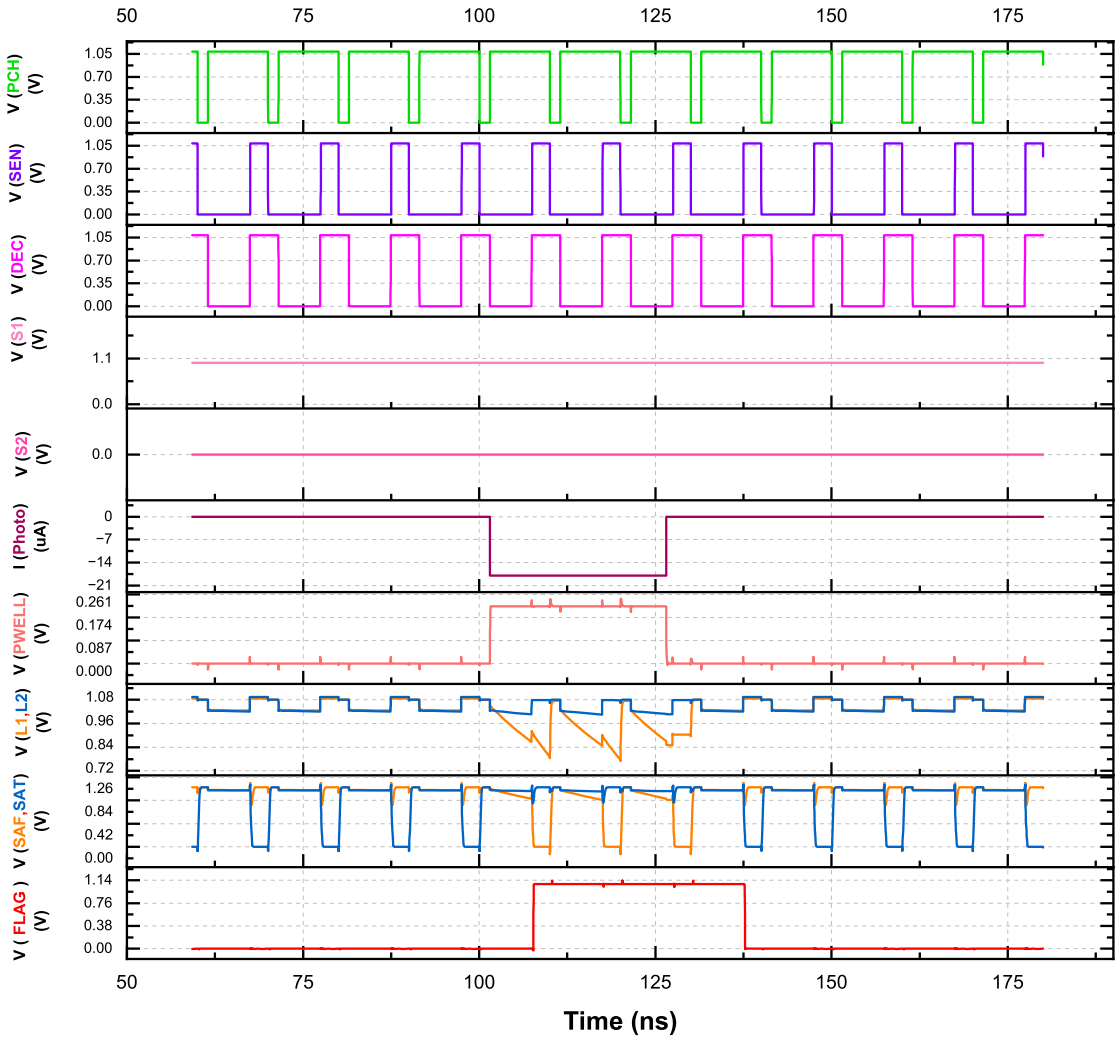

Figure 4.3: A current pulse is injected to the PWELL node

Also whenever DEC signal is taken high a rise in voltage is observed at the SAF node due to charge injection. A rise in voltage is observed in the SAT node as well due to the gate drain coupling capacitance.

To test the sensitivity of the design at different temperature and corners a current pulse injected in the PWELL node. The values of current and voltage at the PWELL node is recorded. The sensitivity at various process corners is recorded in the table.

From the above table it can be inferred that the sensitivity at across temperature for a given corner is almost constant. This is due to the fact that at cold signal S1 and S2 would facilitate the discharge of L1. Thus the lower sensitivity at cold is mitigated by the use of S1 and S2. A constant sensitivity can be achieved by using more number of temperature sensitive signals.

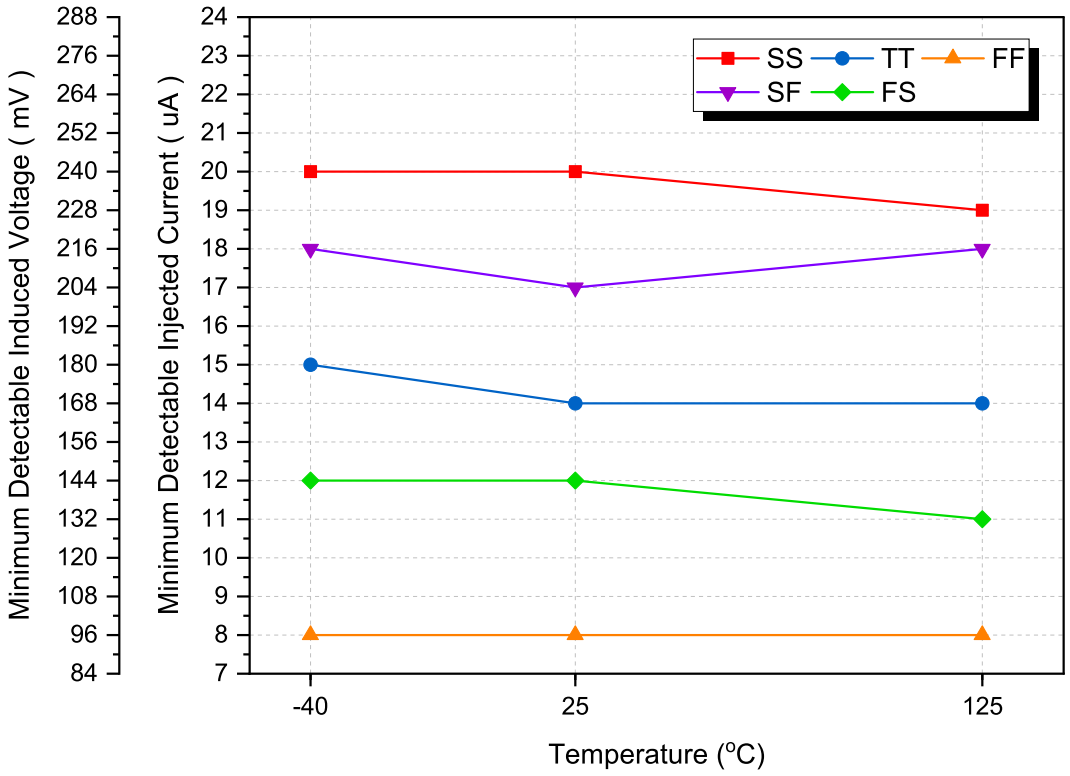

Figure 4.4: Minimum Detectable Injected Current at PWELL

4.7 Design Validation

To validate the design for the case of false detection, 1000 Monte Carlo simulations are run. This is done to check the minimum current for no detection and confirmed detection. The case of confirmed detection is depicted in Fig. 4.5. It can be inferred that sensitivity is almost the same across the temperature for a given corner. In general, slow corners demand more current due to the increased threshold voltage of the transistors.

The case for no detection is also depicted in Fig. 4.6. From the figure, it can be inferred that at fast corners, the current requirement is very lower. Thus, the detection system should always be validated at fast corners to avoid a false alarm. A minimum no detection margin should be maintained to avoid any false alarms and hence the robustness of the design. For a given process and temperature, the region between the no detection and confirmed detection threshold in the region of uncertainty. Any current injection between this region may not get detected.

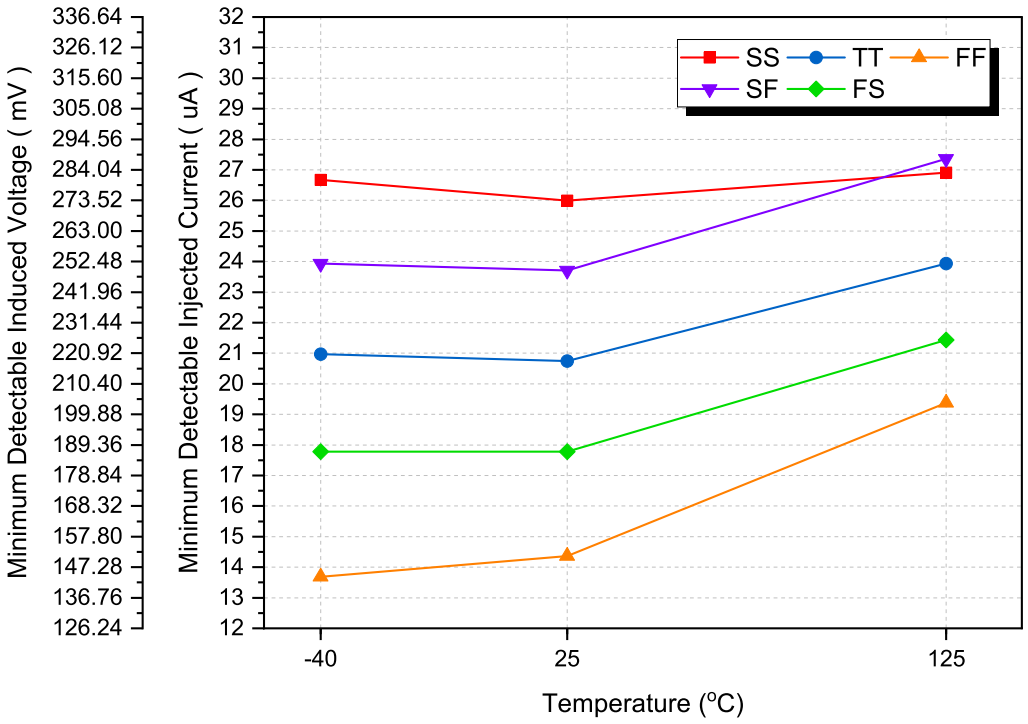

Figure 4.5: A current pulse is injected to the PWELL node

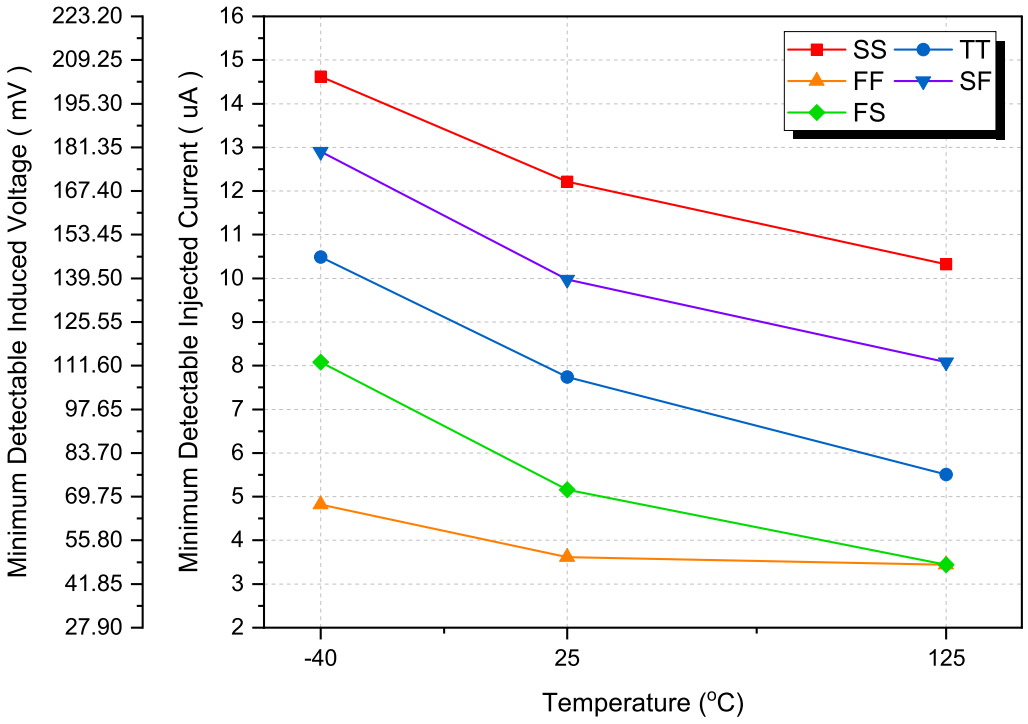

Figure 4.6: Minimum Detectable Injected Current for No detection

4.8 Drawbacks of the proposed Architecture - Iteration 1

The proposed architecture (iteration - 2) addresses and resolves various design drawbacks in iteration - 1. However, some issues still need to be addressed and resolved. Various drawbacks of the proposed architecture (iteration - 2) are as follows:

- Window Masking: When a laser intrusion takes place during the precharge or evaluation phase of operation (DEC signal is at 1), then the design will not be able to detect the transient current. During this phase, the load lines are decoupled from the internal nodes of the sense amplifier. So, any discharge in load line L1 will not be transparent to the internal nodes. So, a method should be developed to avoid the window masking effect. The window masking effect is depicted in Fig. Here a double exponential signal is injected when the DEC signal is high. We can observe that though we have injected current, it still doesn't get detected.

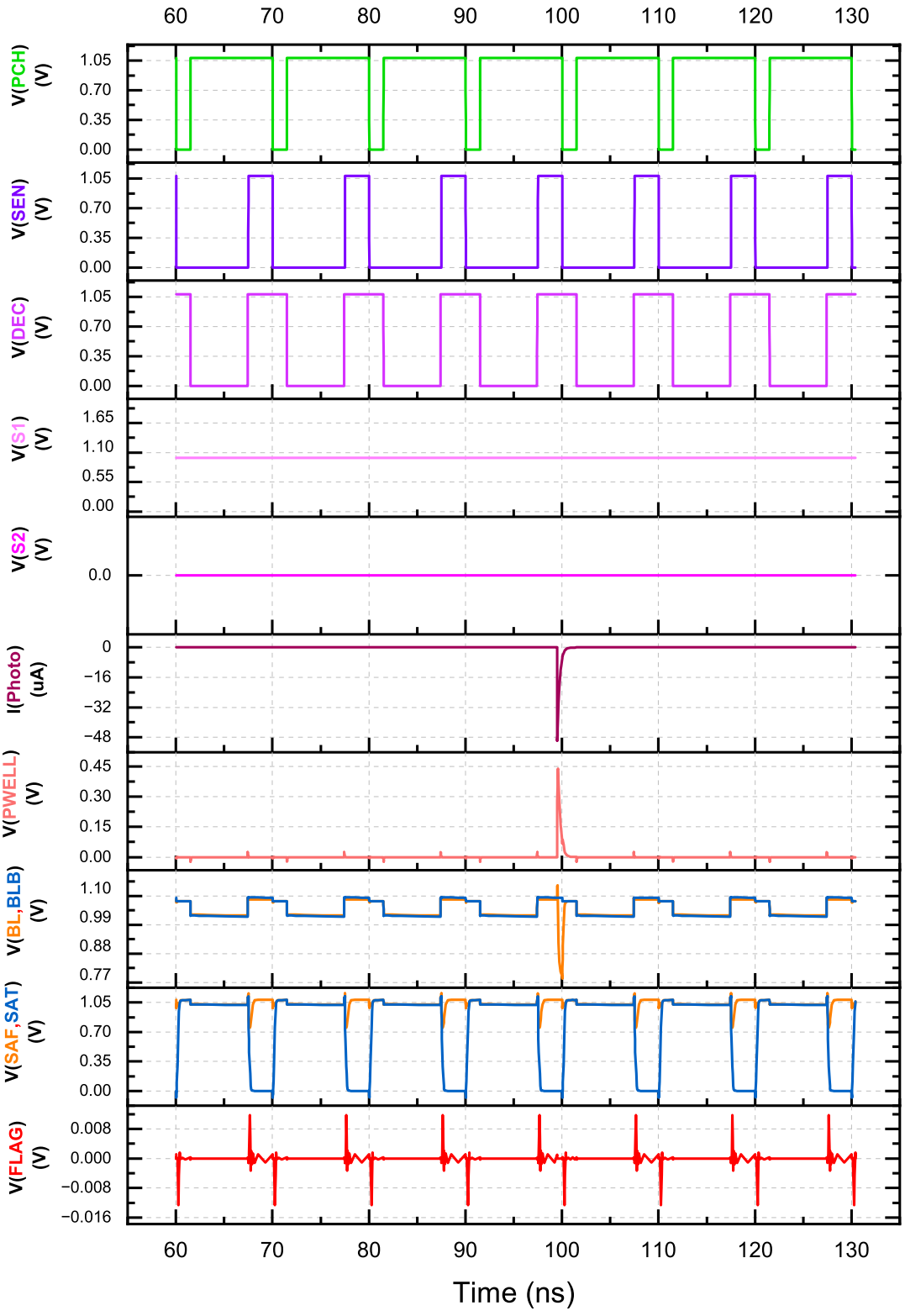

Figure 4.7: Window Masking Effect in the Proposed Architecture iteration - 2

Chapter 5

Final Proposed Architecture

5.1 Motivation

The architecture proposed in the previous chapter is more sensitive to cold. Also, it mitigates various other issues in the previous designs. But it suffers from the Window Masking Effect. This would result in laser intrusions not getting detected when the DEC signal is 1. Thus, this issue needs to be worked upon.

5.2 Circuit Diagram

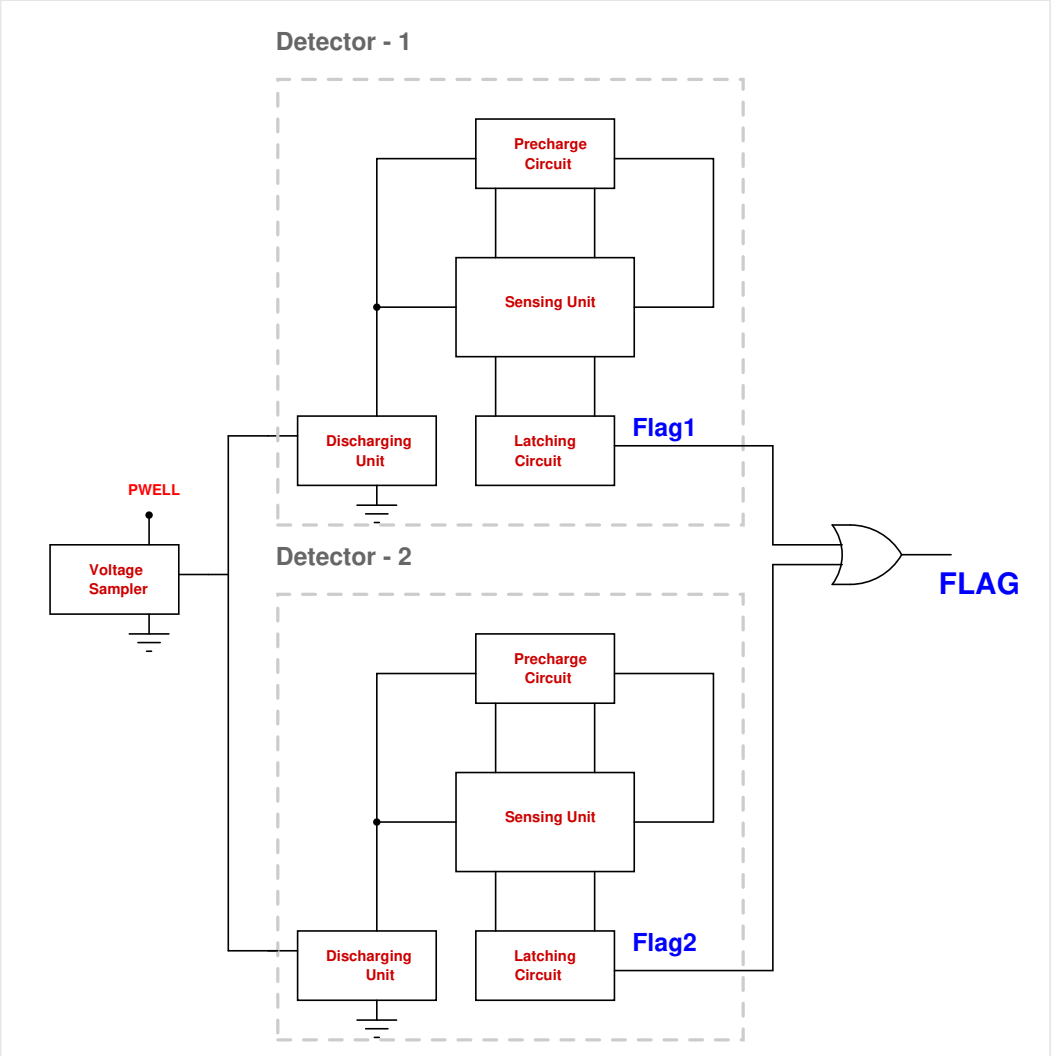

Figure 5.1: Two detectors Interleaved in Time Domain

5.3 Detection Coverage

Two detectors are used in parallel with sampled voltage as input to mitigate the window masking effect. The detectors are interleaved in the time domain. They are interleaved in such a fashion that the sensing and precharge phase of the first detector coincide with the evaluation phase of the second detector. Thus, always one of the detectors would always be in the evaluation phase, and the design would never fail to detect an intrusion within its sensitivity range. The flag output of the detectors is OR-ed together to a single FLAG output. This would increase the detection coverage and make the decision more robust.

A double exponential signal is injected into the PWELL node of the voltage sampling unit (sampling resistor) to simulate the operation. The double exponential signal can be realized in the following way:

$$I_p(t) = I_o[e^{\frac{-t}{\tau_F}} - e^{\frac{-t}{\tau_R}}] \tag{5.1}$$

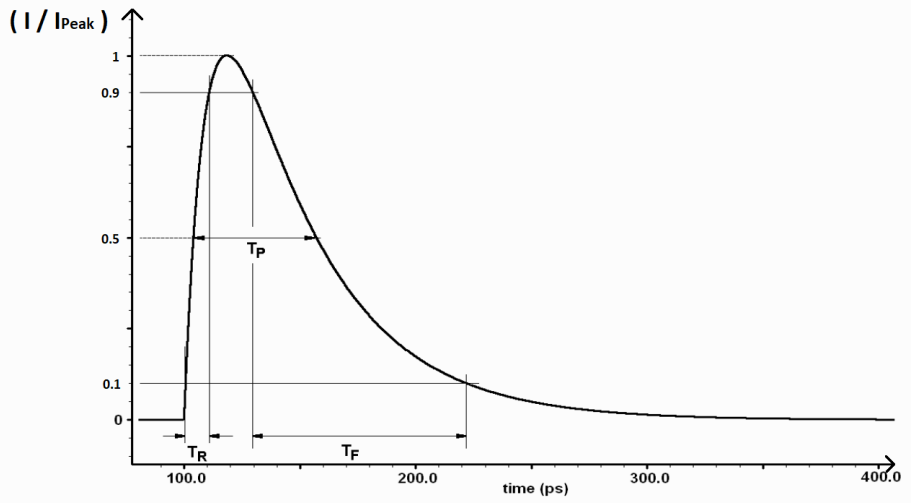

Figure 5.2: A Double exponential current signal used for the simulations [2]

The various parameters of the injected current pulse are given as follows:

- I_o : Peak Current
- τ_R: Rise Time Constant
- τ_F: Fall Time Constant
- T_P: Pulse Width

A current pulse was injected into the proposed design in Fig. during the precharge phase of the detector to simulate the possibility of window masking, as depicted in Fig. 5.3.

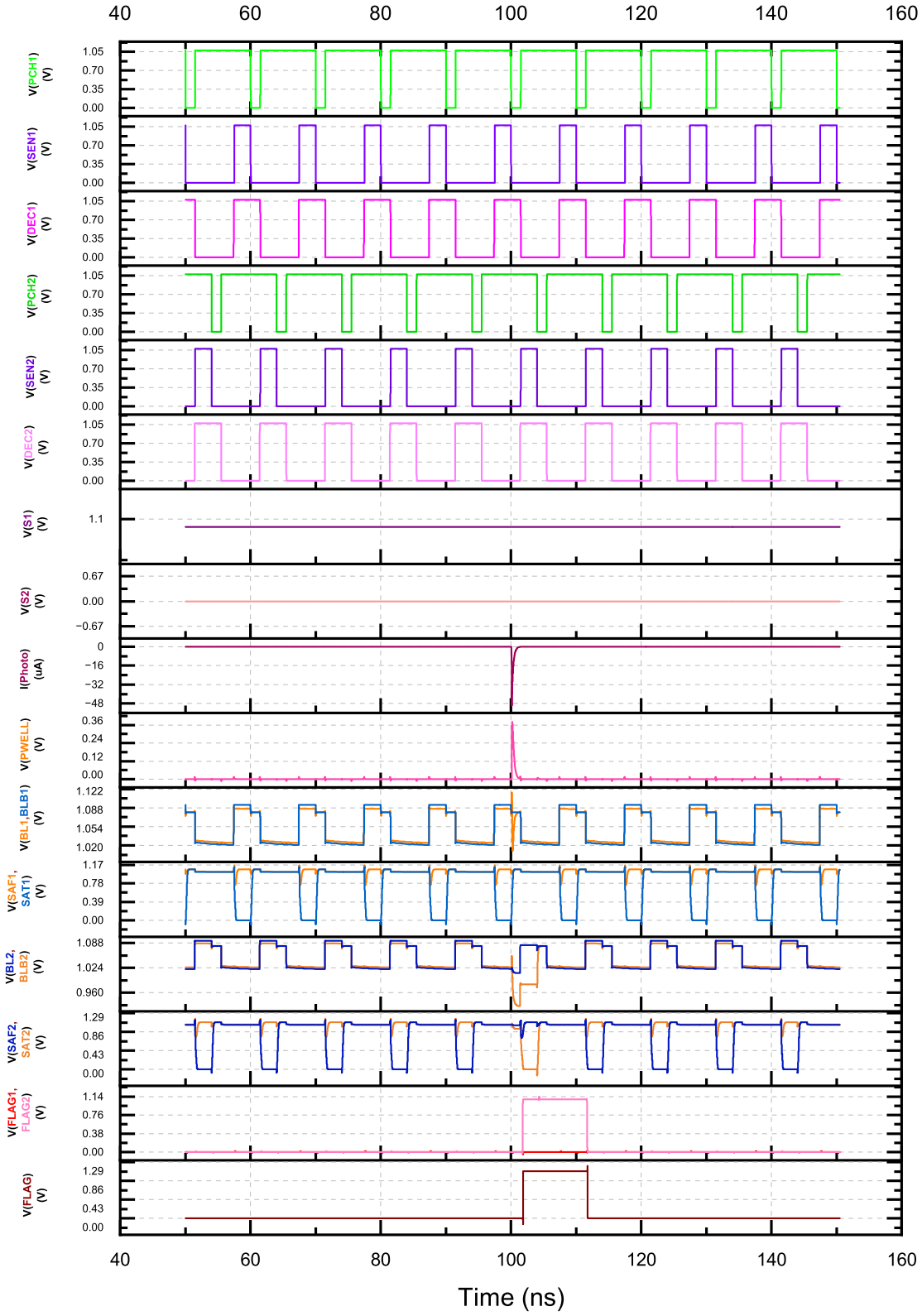

Figure 5.3: A double exponential current signal is fed into the PWELL node during the precharge phase of the First Detector

From the figure, it can be inferred that the first detector didn't produce an output flag due to the window masking. But since the second detector was in the evaluation phase, it produced a positive detection.

5.4 Simulation Results

To simulate the sensitivity of the detector double exponential signal is injected into the PWELL node. The rise time of the signal is taken as 5 ps. The fall time is varied from 20ps to 2ns. The values of minimum detectable current and charge and voltage induced at PWELL is recorded at various process and temperatures.

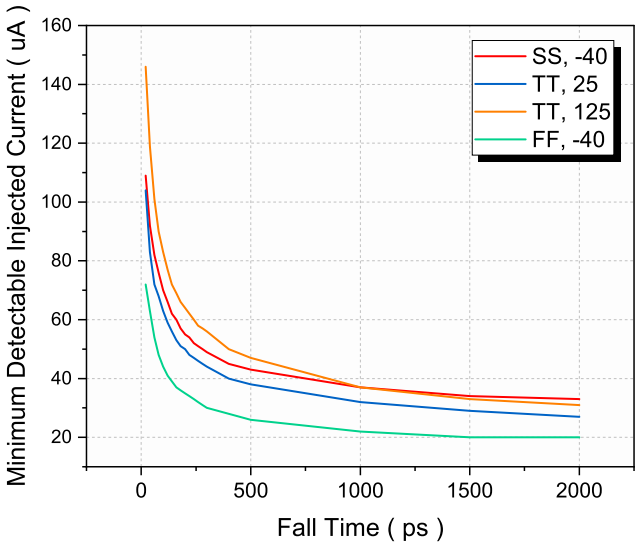

Figure 5.4: Minimum Detectable Injected Current at the PWELL

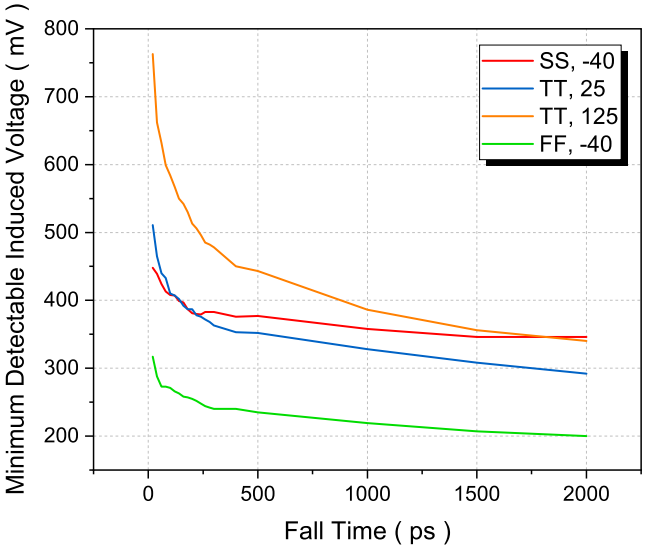

Figure 5.5: Minimum Detectable Induced Voltage at the PWELL

It is observed from Fig. 5.4 that as fall time increases, the peak current required for detection decreases. This is because, as the fall time increases, the sampled voltage remains at the PWELL node for a longer period of time. As a result, the Load line discharges for a prolonged duration. Similarly, for the same reason minimum detectable voltage also reduces with an increase in the fall time.

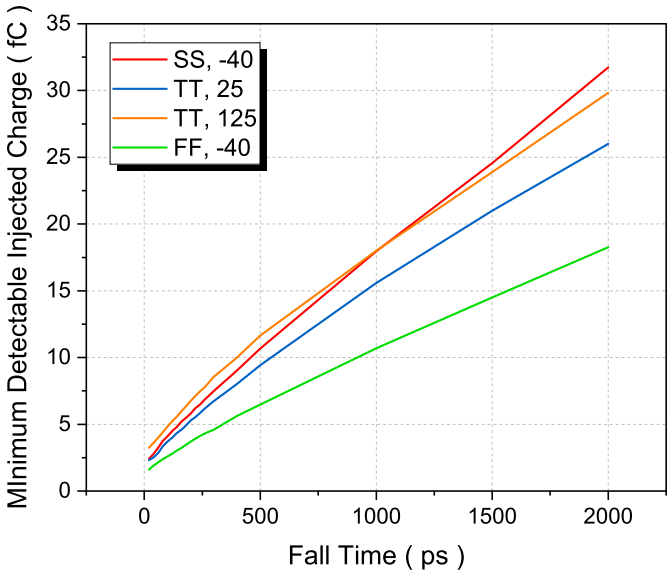

Figure 5.6: Minimum Detectable Injected Charge at the PWELL

From the figure, it can be inferred that the critical charge increases with the increase in the fall time. The minimum charge required for detection depends on the topology of the injected current.

5.5 Power and Leakage Estimation

The design sensitivity towards photocurrent is achieved with leakage and total power consumption under control. To avoid leakage, HVT (High Threshold Voltage) devices are used (Stacked LVT is used only for Discharging Unit).

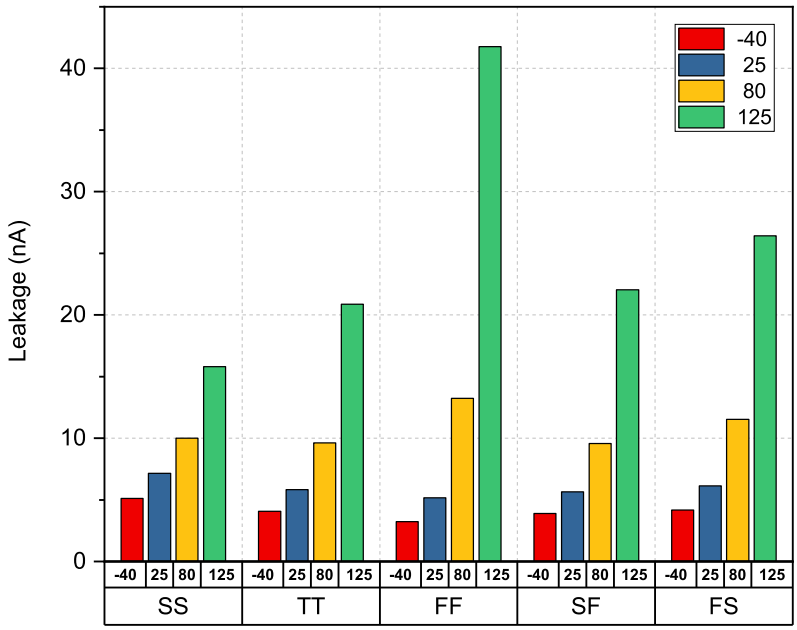

Figure 5.7: Leakage Current of the Proposed Design

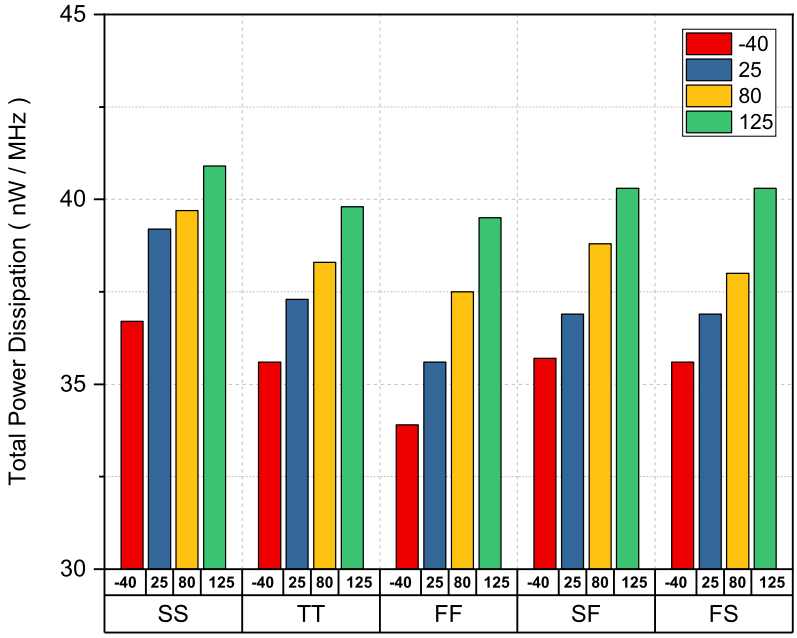

Figure 5.8: Total Power Dissipation of the Proposed Design

At typical operating conditions, the leakage is less than 6 uA. At works case FF 125, the leakage is 42 nA. The leakage is measured when the DEC signal is 1, and there is no output or input signal transient. The leakage is contributed by the load lines and the internal nodes of the sense amplifier. Total power at typical operating conditions is about 37 nW/MHz.

5.6 Comparison with Previous Works

The current demanded by the detector to produce a FLAG is lower at shorter fall times than in previous works. This is simply because the scheme relies on the partial discharge of a floating node, unlike previous architectures where a constantly driven node is attempted to charge/discharge through a transistor. Fig. 5.9 shows the current sensitivity of different BBICS architectures compared with the proposed design. At shorter fall times, the compared architectures fail to produce any output. Also, at a larger fall time, the current requirement doesn't reduce as some minimum voltage greater than the threshold voltage of charging/discharging transistor to be maintained to turn ON transistor.

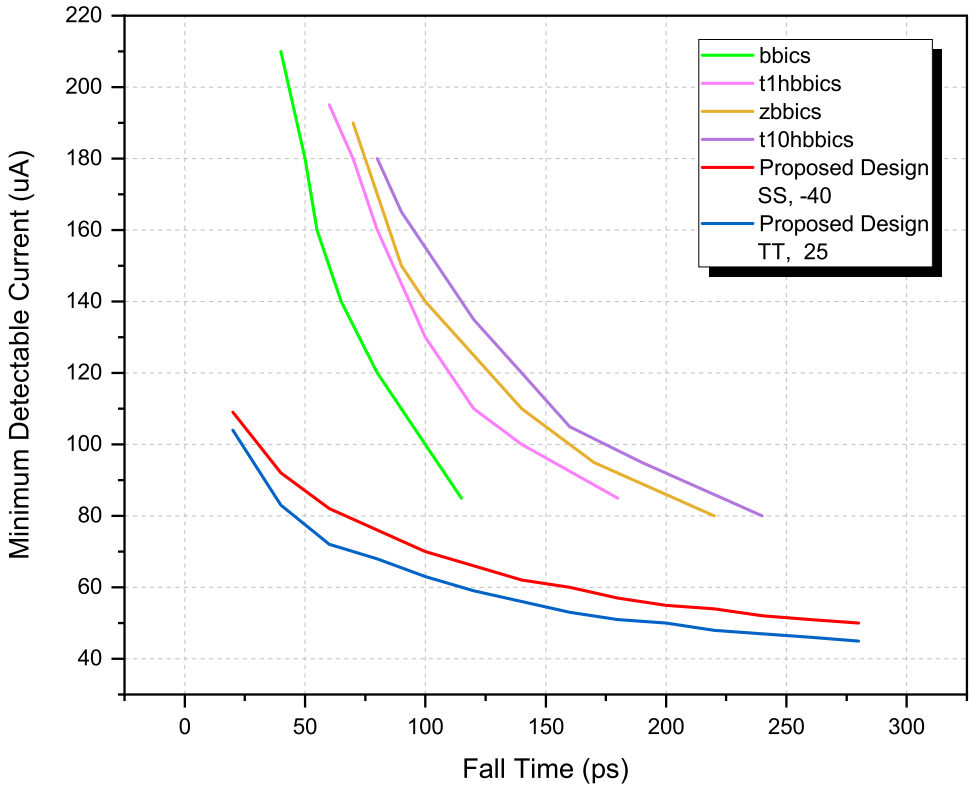

Figure 5.9: Minimum Detectable Injected Current comparison with the established work

5.7 Layout Design

Along with power and performance, an estimate of the area and physical design is also essential for any circuit implementation. The proposed methodology consists of two Sense Amplifiers interleaved in the time domain for continuous detection. In the physical design, the circuit is segmented into five parts:

- Sense Amplifier - 1
- Sense Amplifier - 2
- Sampling Unit - Unisilicided P+ Poly Resistor
- Dynamically Biased Set of NMOSs
- Lower NMOSs in the Stacks A, B and C

The complete physical design implementation of the proposed design is depicted in Fig. 5.10. Also, an annotated version of the layout is also displaced in Fig. 5.11. The two Sense Amplifiers are laid on the two sides of the layout. The sampling resistor is put in the middle of the two sense amplifiers. The dynamically biased transistors and Lower NMOSs in Stacks A, B, and Care are below the sampling resistor. Also the layout is shielded by M3 metal layer to avoid any laser intrusion in the detection arrangement.

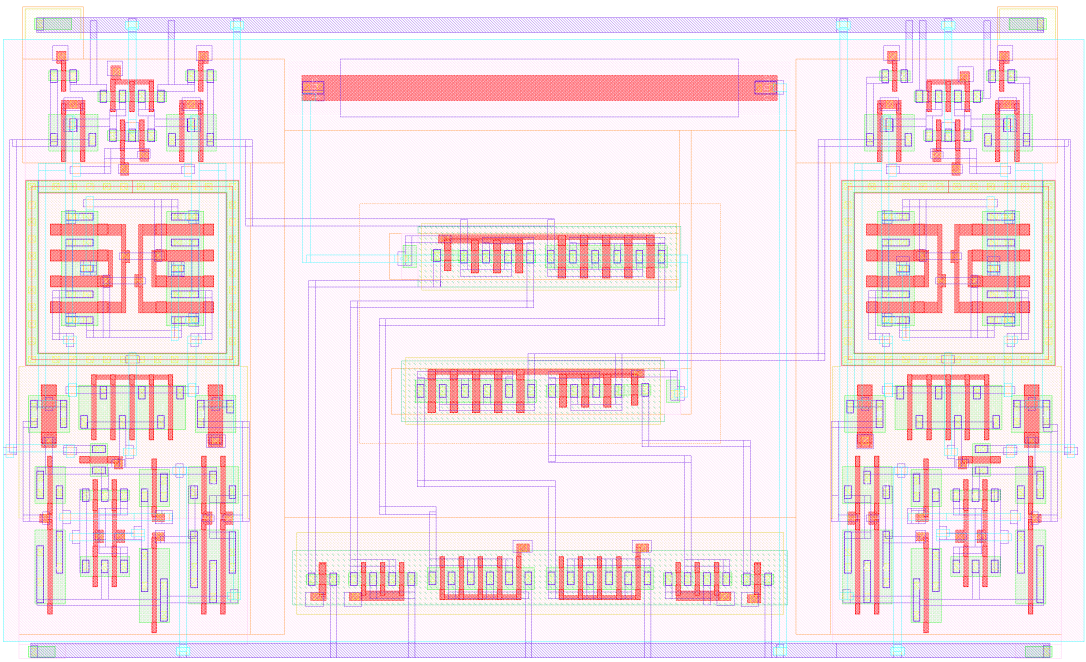

Figure 5.10: Layout Design of the Proposed Design

To make the capacitance equal at the SAT and SAF nodes common centroid is made for NMOS M6 and M7. The transistors are broken into four fingers and are structurally matched to achieve the proper matching, as depicted in Fig. 5.12. The common centroid is also isolated using a guard ring to avoid any substrate noise.

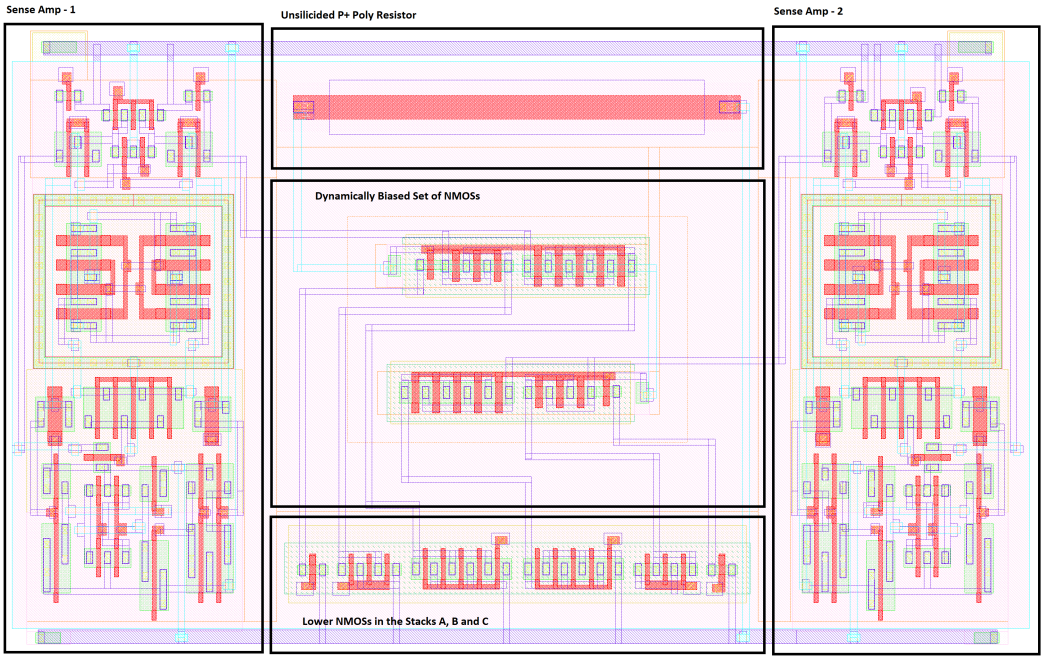

Figure 5.11: Layout Design of the Proposed Design (Annotated)

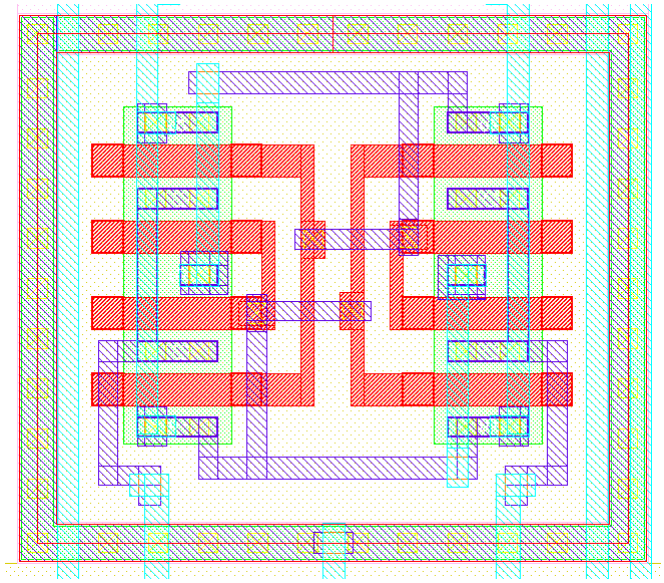

Figure 5.12: Common Centroid Layout of NMOS M6 and M7 Transistors

To implement the dynamic body biasing, Deep Nwell is made inside the N-Well, and using crop function in virtuoso properties of the N-WELL is removed to form an isolated P-Well.

Chapter 6

Other Works - Proposed Design 2

6.1 Circuit Diagram

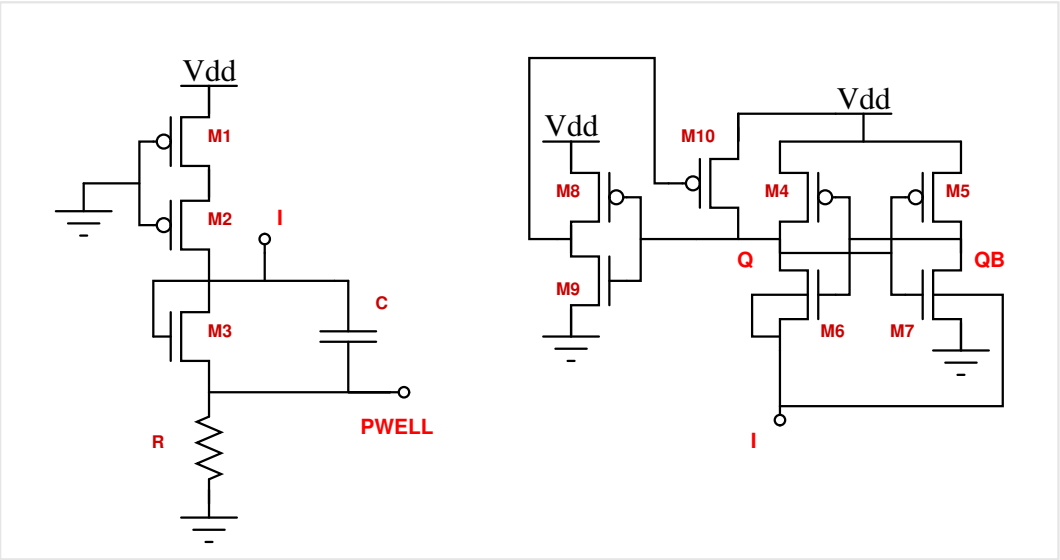

Figure 6.1: Proposed Architecture - 2

6.2 Design Components

The functionality of various parts of the Proposed design are given as follows:

- M1 and M2 Transistors supply current to the always ON stack to maintain a voltage continuously at the I node.
- M3 is a diode whose M3 is tied to give a constant voltage drop at the I node. It also prevents any backflow of current when current is injected via PWELL (to simulate a laser fault).
- Also, parallel to the diode, a capacitance is attached that facilitates the quick rise in voltage at the I node whenever there is a laser fault intrusion.
- Sampling Unit: Here a resistance of 12 KOhms is used to sample the voltage. Instead of using an NMOS and constant P+ Poly High Resistor is used to avoid any variation due to process and temperature.
- M4, M6, and M5, M7 consist of a back-to-back connected inverter. Inverters are skewed to facilitate the flipping action whenever a voltage rise occurs at

PWELL. NMOS M6 is source as well as body biased. NMOS M7 is also body biased.

- Half latch: M8 and M9 transistors form an inverter whose output is connected to the gate of M10.

6.3 Design Decisions

Various design decisions undertaken to optimize the detector's sensitivity are given as follows:

- M1 and M2 are taken as HVT devices. Also, their length is increased to limit the always ON current of the stack to GND.
- Inclusion of capacitor parallel to diode facilitates the immediate rise in voltage when the voltage at PWELL increases.
- The back-to-back connected inverters are skewed to make it unstable and ease the flipping action. The length of M5 and M7 are increased to prevent leakage.
- The length of transistors in the half latch is also increased to reduce leakage.

6.4 Mechanism of Operation

The proposed architecture is an asynchronous design. Various phases of operation are explained as follows:

- Normal Operation: During regular operation, the I node is set below the trip point of the back-to-back connected inverters (around 420 mV). This is achieved by sizing the PMOS M1, M2, and diode M3.

  Q node is initialized to 0, and the QB node is set to 1. Q node is used as flag Output. Q going high indicates a laser fault injection. During no-fault PWELL node is at 0 (sampled voltage).

- Fault Detection: When there is laser fault injection, there would be an increase in the PWELL voltage. Incoming photocurrent would only flow through the sampling resistor; since it would not flow through the diode in the opposite direction.

  The sharp increase in voltage at the PWELL node is reflected in the I node through the capacitor. The jump in voltage at the I node is reflected at the Q node, which initiates the flipping action. As the voltage at the Q node increases, the M7 transistor turns ON and discharges the QBAR node. The Half latch also turns M10 ON, charging the Q node to a full logic 1, indicating a laser fault injection.

  The behavior of the circuit during the fault detection case is illustrated in Fig. 6.2.

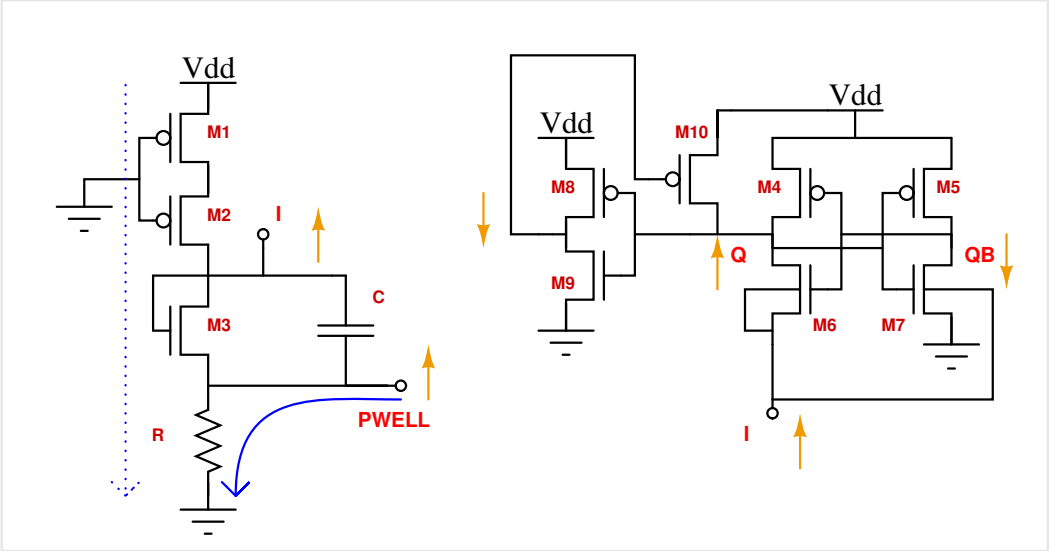

Figure 6.2: Mechanism of Operation of the Proposed Architecture - 2

6.5 Simukation Results

A double exponential signal is injected at the PWELL node with a rise time of 5 ps and a fall time of 2ns to illustrate the circuit's functionality, as depicted in Fig. 6.3.

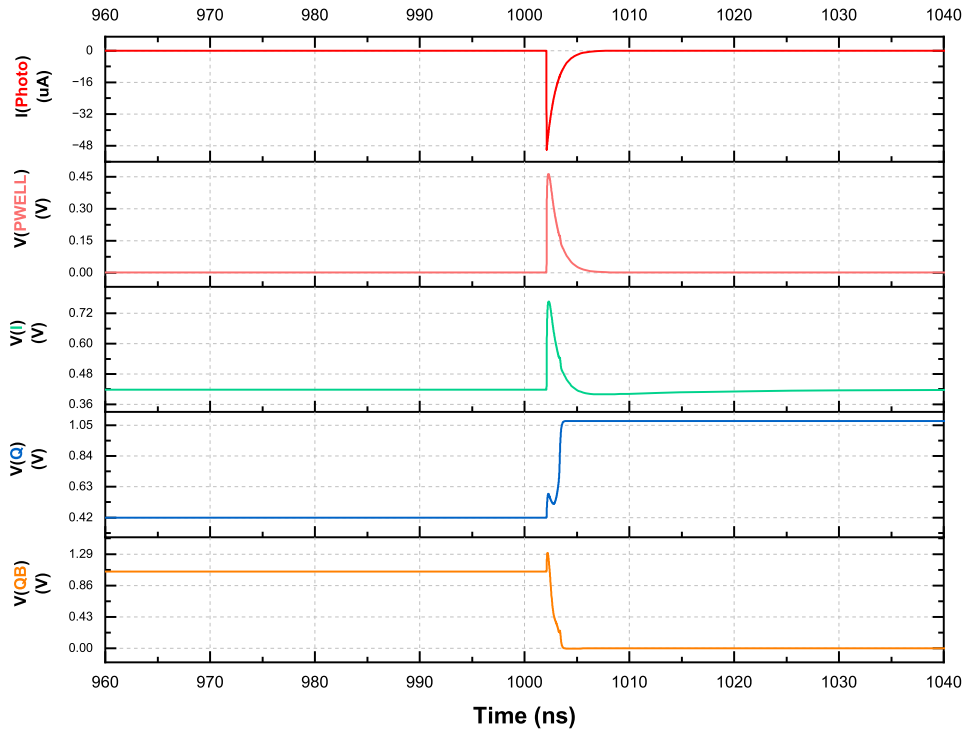

Figure 6.3: A double exponential signal is injected at PWELL node

To simulate the sensitivity of the detector double exponential signal is injected into the PWELL node. The rise time of the signal is taken as 5 ps, and The fall time is varied from 60ps to 2ns. The values of minimum detectable current and charge and voltage induced at PWELL is recorded at various process and temperatures. All the simulations are performed at TT 25 C.

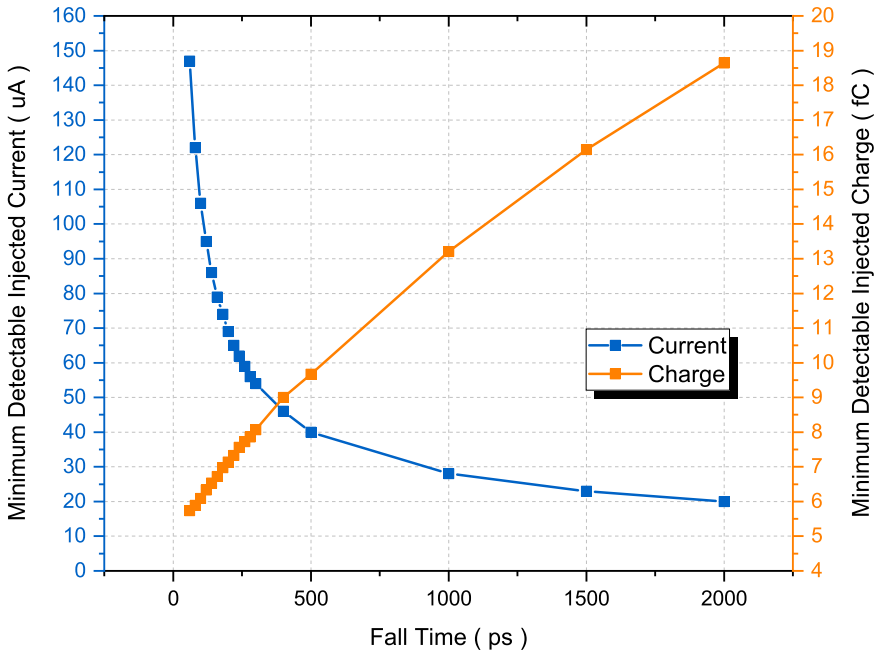

Figure 6.4: Minimum Detectable Injected Current and Charge at the PWELL

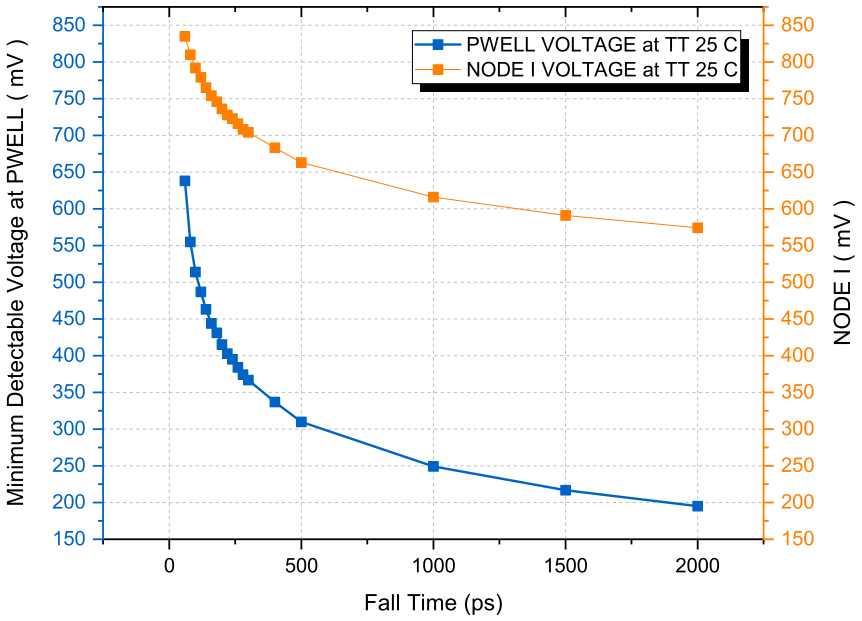

Figure 6.5: Minimum Detectable Induced Voltage at the PWELL

It is observed from Fig. that as fall time increases, the peak current required for detection decreases. This is because, as the fall time increases, the sampled voltage remains at the PWELL node for longer. As a result, the Load line discharges for a prolonged duration. Similarly, for the same reason minimum detectable voltage also reduces with an increase in the fall time.

From the figure, it can be inferred that the critical charge increases with the increase in the fall time. The minimum charge required for detection depends on the topology of the injected current.

The total leakage of the design during its regular operation at TT 25 C is 280 nA. Total power consumption during normal conditions is 302 nW.

In Fig. 6.6, the sensitivity of both the Proposed design is depicted. Clearly, the sensitivity of the proposed design - 2 still needs further enhancement. Also, at a very low fall time (60 ps), the proposed design - 2 is unable to detect the photocurrent injection. This is because the voltage at PWELL cannot rise sufficiently at lower fall time.

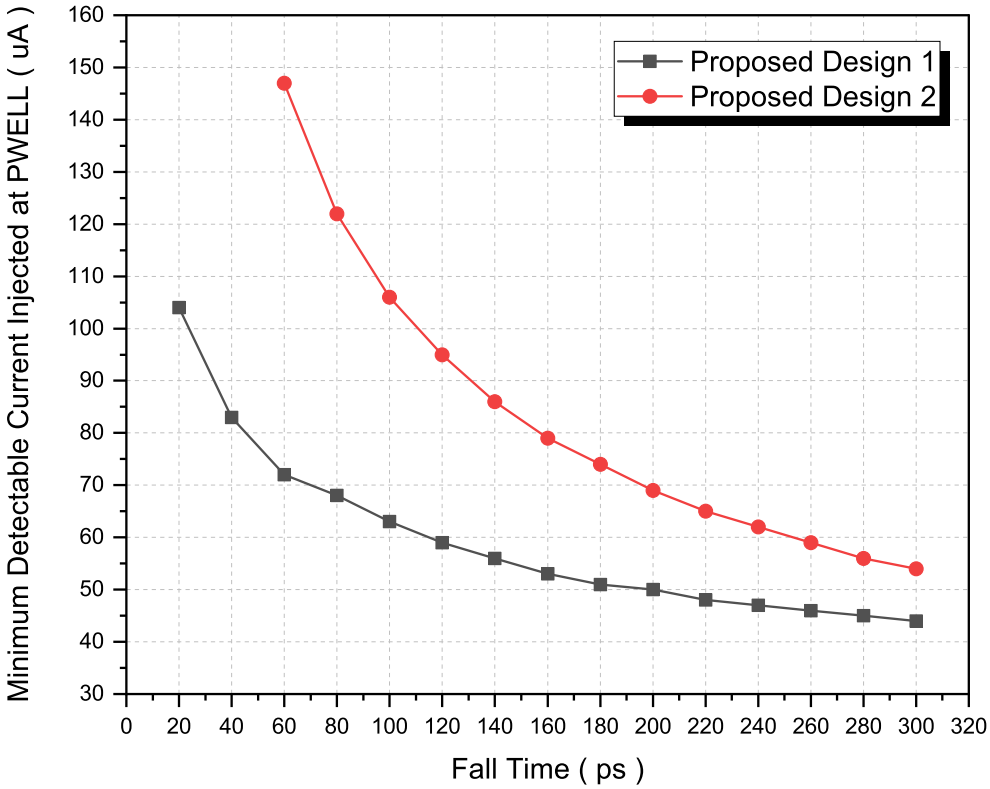

Figure 6.6: Comparison of Proposed Architecture - 1 and 2 showing Minimum Detectable Current at TT 25 ^{o}C

Chapter 7

Conclusion

In this work, we have proposed a circuit and method to detect side-channel attacks in secure ICs. The Conventional methods to detect laser-induced currents are also discussed in brief. The design is implemented and optimized for leakage, power, and sensitivity. It is characterized and simulated using the 65nm LSTP (Low Standby Power) Process at 1.08 V. To benchmark the performance of the proposed design, it is simulated with exponential current signals, and minimum detectable current, voltage, and the charge is recorded. The proposed method has evolved in various iterations. Each iteration is explained with its contribution (improvement over the previous) and drawbacks. The conventional approach to detect laser-induced current lacks sensitivity for a shorter current pulse and has high leakage current. The proposed method is 1.5x -2.4x more sensitive toward the current pulse with a fall time of 100ps and below. The design being synchronous has a greater degree of control. The worst leakage recorded is 42 nA, and power is 41 nW/MHz. Due to the higher sensitivity of the proposed design, lesser repetition of the arrangement is required in the SoC.

Chapter 8

Future Work

The proposed design - 2 doesn't show good sensitivity as compared to the Design - 1 towards shorter pulse and lower injected photocurrent. The goal is improve the sensitivity of the design. Also, the leakage of the design should also be reduced during normal operating condition. The improved sensitivity and lower leakage of the design can prove to be a better solution in terms of area.

Chapter 9

References

1. C. Champeix, N. Borrel, J. -M. Dutertre, B. Robisson, M. Lisart and A. Sarafianos, "Experimental validation of a Bulk Built-In Current Sensor for detecting laser-induced currents," 2015 IEEE 21st International On-Line Testing Symposium (IOLTS), 2015, pp. 150-155, doi: 10.1109/IOLTS.2015.7229849.

2. A. Simionovski and G. I. Wirth, "A Bulk Built-in Current Sensor for SET detection with dynamic memory cell," 2012 IEEE 3rd Latin American Symposium on Circuits and Systems (LASCAS), 2012, pp. 1-4, doi: 10.1109/LASCAS.2012.6180338.

3. R. P. Bastos, J. -M. Dutertre and F. S. Torres, "Comparison of bulk built-in current sensors in terms of transient-fault detection sensitivity," 2014 5th European Workshop on CMOS Variability (VARI), 2014, pp. 1-6, doi: 10.1109/VARI.2014.6957089.

4. R. P. Bastos, F. S. Torres, J. -. Dutertre, M. -. Flottes, G. Di Natale and B. Rouzeyre, "A single built-in sensor to check pull-up and pull-down CMOS networks against transient faults," 2013 23rd International Workshop on Power and Timing Modeling, Optimization and Simulation (PATMOS), 2013, pp. 157-163, doi: 10.1109/PATMOS.2013.6662169.

5. M. Lacruche et al., "Laser fault injection into SRAM cells: Picosecond versus nanosecond pulses," 2015 IEEE 21st International On-Line Testing Symposium (IOLTS), 2015, pp. 13-18, doi: 10.1109/IOLTS.2015.7229820.

6. Z. Zhang, T. Wang, L. Chen and J. Yang, "A new Bulk Built-In Current Sensing circuit for single-event transient detection," CCECE 2010, 2010, pp. 1-4, doi: 10.1109/CCECE.2010.5575124.

7. R. P. Bastos, F. S. Torres, J. . -M. Dutertre, M. . -L. Flottes, G. Di Natale and B. Rouzeyre, "A bulk built-in sensor for detection of fault attacks," 2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2013, pp. 51-54, doi: 10.1109/HST.2013.6581565.

8. C. Champeix et al., "Laser testing of a double-access BBICS architecture with improved SEE detection capabilities," 2016 16th European Conference on Radiation and Its Effects on Components and Systems (RADECS), 2016, pp. 1-4, doi: 10.1109/RADECS.2016.8093172.

9. D. Zooker, A. Fish, O. Keren and Y. Weizman, "Compact Sub-Vt Optical Sensor for the Detection of Fault Injection in Hardware Security Applications," 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2019, pp. 1-5, doi: 10.1109/NTMS.2019.8763825.

10. Jean-Max Dutertre, Rodrigo Possamai Bastos, Olivier Potin, Marie-Lise Flottes, Bruno Rouzeyre, et al.. Sensitivity tuning of a bulk built-in current sensor for optimal transient-fault detection. Microelectronics Reliability, Elsevier, 2013, European Symposium on Reliability of Electron Devices, Failure Physics and Analysis, 53 (9), pp.1320-1324. ff10.1016/j.microrel.2013.07.069ff. ffemse-01100723