High-Performance Robust Latches
Martin Omaná, Daniele Rossi, Member, IEEE, and Cecilia Metra, Senior Member, IEEE

Abstract—First, a new high-performance robust latch (referred to as HiPeR latch) is presented that is insensitive to transient faults affecting its internal and output nodes by design, independently of the size of its transistors. Then, a modified version of the HiPeR latch (referred as HiPeR-CG) is proposed that is suitable to be used together with clock gating. Both proposed latches are faster than the latches most recently presented in the literature, while providing better or comparable robustness to transient faults, at comparable or lower costs in terms of area and power, respectively. Therefore, thanks to the good trade-offs in terms of performance, robustness, and cost, our proposed latches are particularly suitable to be adopted on critical paths.

Index Terms—Transient faults, soft errors, static latch, hardened latch, robust design.

1 INTRODUCTION

The continuous advances of microelectronic technology are leading to an aggressive reduction of device dimensions down to the nanometer region. Because of the consequent reduction of circuit node capacitances, together with the simultaneous decrease of power supply voltages, the amount of charge stored on a circuit node is becoming increasingly smaller, making circuits more susceptible to spurious voltage glitches, caused by cosmic ray neutron or alpha particle hits [1], [2], [3], [4], [5]. Such spurious voltage glitches are generally referred to as transient faults (TFs). If in the past, TFs had been a concern only for space applications, nowadays, they are recognized as a problem even at the sea level [6]. In particular, for terrestrial applications, high-energy neutrons are the dominating source of TFs, and the susceptibility of modern ICs to TFs is expected to increase with the scaling of technology node [7], [8], [9], [6].

When a TF affects a memory cell or a storage element (latch or flip-flop), it can cause a flip of the stored bit, thus giving rise to a soft error (SE), also referred to as single-event upset (SEU). Soft errors have traditionally been recognized as a problem for high-density memories, because of their small cell size [10], [11]. Error-correcting codes (ECCs), in particular, single error-correcting/double error-detecting codes, have been successfully employed to guarantee a satisfactory level of memory reliability. Recently, because of the increasing probability of having multiple bit upsets [12], memory designers are facing new and challenging problems.

An SE may also be generated because of a TF affecting combinational logic, when the generated spurious voltage glitch propagates till the input of a sampling element. In this regard, however, it has been proven [13], [14] that SEUs affecting storage elements (latches and flip-flops) within sequential logic are by far the largest contributor to soft error rate (SER) in logic. For this reason, extensive research efforts have been recently devoted to devising novel hardening schemes/approaches for latches and flip-flops. Some approaches rely on the modification of the latch structure in order to make it robust independently of the hitting particle energy. This is the case of the scheme proposed in [10], referred to as the DICE cell, and the latch in [11], [15]. These latches make use of two independent feedback loops controlling the output. This way, a TF affecting one of the loops cannot alter the output logic value. Also, the latches in [13], [16], and [17] present this characteristic. As for the latches in [13], [16], their robustness relies on the deactivation of the feedback loop (during the latching phase), thus avoiding the generation of soft errors due to TFs affecting their nodes. The latch in [17], instead, reuses the scan portion of a scan FF to duplicate the latch, thus producing two independent values that are feeding an output stage first exploited in [18] for robust latches, then denoted as C-element in [17]. For all these latches, TFs affecting any of their internal or output nodes cannot produce an output SE.

Other approaches aim at improving the latches’ robustness against TFs by increasing node capacitances and/or the strength of some transistors. For instance, this approach is adopted by the latches in [19], [20], [21], [18], [22], [23]. In particular, the robustness of [19], [20], [21], [18] derives from the idea of either splitting the internal nodes and adopting proper feedback structures, or using a Schmitt trigger-like scheme. Instead, solutions in [22], [23] improve the latch robustness by inserting either explicit capacitances, or transistors acting as filters for voltage glitches. All latches in [19], [20], [21], [18], [22], [23] include nodes that, if affected by TFs, may produce an output SE.

In this paper, first a new robust latch able to tolerate TFs independently of the hitting particle energy is presented. It is based on the latch structure introduced in [24], and will be hereinafter referred to as High-Performance Robust (HiPeR) latch. Then, a modified version of such a HiPeR latch, referred to as HiPeR-CG, is also proposed that is suitable to be used together with clock gating (CG) [25]. In fact, as shown in Section 4, TFs affecting some internal nodes of the HiPeR latch may leave its output in a high-impedance state. If this event happens when clock gating is activated to reduce power consumption, the high-impedance node may be improperly charged/discharged to an
incorrect logic value due to leakage current, and an SE may originate. This is not expected to be a problem if clock gating is not adopted. In fact, also in the perspective of increasing leakage currents with technology scaling [26], since the latch operation frequency will also increase, the output of the latch will remain in a high-impedance state for a time interval that will be too short to allow leakage currents to charge/discharge the output node.

To cope with the problem possibly arising in case of clock gating, the HiPeR-CG latch is proposed. Differently from HiPeR, HiPeR-CG is such that its output cannot remain in a high-impedance state when a TF affects any of its internal nodes, thus being suitable to be used together with clock gating.

The proposed latches are compared to each other, as well as to the standard latch [27], and to the most recently presented robust latches we are aware of [19], [13], [20], [15], [21], [16], [11]. The solution in [17] has not been considered for comparison purposes, since it is oriented to scan FFs.

It will be shown that the HiPeR and HiPeR-CG latches feature considerably better characteristics in terms of performance than all other considered robust latches, but for the latch in [20], which presents a comparable input-output delay. In addition, our proposed latches provide higher or comparable robustness to TFs compared to the considered alternative robust solutions, except for the latch in [15], which features the higher robustness. This latter, however, is the one with the highest cost in terms of area and power among all compared latches.

More in detail, our latches feature higher area than the latches presenting lower robustness [19], [13], [20], [21], [16] while, as for power, the latch in [16] is the less consuming robust solution, but it is considerably slower and less robust than our proposed latches. Finally, compared to the latch in [11], the proposed solutions present comparable area, power, and robustness, but are considerably faster. Therefore, thanks to the good trade-offs in terms of performance, robustness, and cost, our proposed latches are particularly suitable to be adopted on critical paths.

The rest of the paper is organized as follows: In Section 2, the HiPeR latch structure and behavior are described. In Section 3, some results of the electrical-level simulations performed to verify the HiPeR latch behavior are reported. In Section 4, the effects of leakage currents on the HiPeR latch, when clock gating is applied, are analyzed. In Section 5, the HiPeR-CG latch is introduced. In Section 6, some results of the electrical-level simulations performed to verify the HiPeR-CG latch behavior are reported. In Section 7, the proposed latches are compared to each other, and to alternative solutions (including the standard latch), considering cost and TF robustness as metrics for comparison. Finally, some conclusions are drawn in Section 8.

2 Proposed HiPeR Latch

The proposed HiPeR latch (Fig. 1) relies on two basic principles: 1) Triplication of the latch internal node driving a special output stage (first exploited in [18] for robust latches, then denoted as C-element in [17]) allowing the output to change its logic value accordingly to the value of the majority of the internal nodes and 2) design of two proper independent feedback loops that are activated during the latching phase (here assumed to occur when CK = 1).

The idea in 1) above allows to tolerate TFs affecting internal nodes, while the design principle in 2) allows to tolerate also TFs affecting the output node. As for TFs affecting the input node, as discussed in detail in Section 7, the HiPeR latch provides high robustness, similarly to the previous solutions in [13], [15], [16], [17], [11].

The electrical scheme of the proposed HiPeR latch is shown in Fig. 1. Transistors MN3 and MP4 (driven by the output Q) should be dominant over transistors MP3 and MN4 (driven by the internal node INT2), respectively. The behavior of the latch will now be described in detail.

When CK = 0, the latch is transparent, and the logic value d at the input node D propagates to the output Q and to the internal node INT2 through transfer gates TG1 and TG2, respectively. Then, the complemented logic value d’ propagates to the internal nodes driving the output C-element, that is INT3 (through inverter I2), INT1a (through the series MP3-MN3), and INT1b (through the series MP4-MN4). Thus, the C-element confirms the logic value d at the output node Q. It is worth noticing that, when CK = 0, transistors MP7 and MN7 are OFF to avoid possible contention on node INT2. Furthermore, TFs affecting the latch during the clock low phase are not of concern, since the output of the latch is not valid during such a clock phase.

Instead, when CK = 1, the transfer gates TG1 and TG2 are OFF and the input node D is disconnected from the output node Q. The value previously charged on node Q is maintained by the C-element, which is driven by two independent feedback loops (Fig. 1): 1) the feedback loop denoted by FL1, including the output node Q and the internal nodes INT1a and INT1b and 2) the feedback loop denoted by FL2, composed by the back-to-back inverters I1 and I2 and including internal nodes INT2 and INT3. This way, if a TF affects a latch internal node, it may change the state of only one of the two feedback loops, so that the logic value at the output Q is preserved. Furthermore, thanks to the previously mentioned dominance of transistors MN3.
and MP4 (driven by the output Q) over transistors MP3 and MN4 (driven by internal node INT2), TFs affecting nodes INT2 or INT3 cannot change the logic values of nodes INT1a and INT1b, so that they cannot alter the output value Q.

Let us now describe in detail the behavior of the latch in case of TFs affecting its internal and output nodes when CK = 1 (latching phase). In case of TFs affecting the internal node INT1a, the following two conditions can be distinguished: 1) \( Q = 1 \), thus \( INT1a = INT3 = 0 \) (the series MP5-MP6 is on) and 2) \( Q = 0 \), thus \( INT1a = INT3 = 1 \) (the series MP5-MP6 is OFF). In case 1), the TF makes \( INT1a \) flip to 1, thus temporarily turning OFF MP5, and leaving the output \( Q \) in a high-impedance state. However, the correct logic value of the output is not altered, and the conductive transistor MN3 restores the correct value 0 on \( INT1a \), thus making MP5 turn on again. In case 2), the TF makes \( INT1a \) flip to 0, thus temporarily turning ON MP5. However, since \( INT3 = 1 \), MP6 is kept OFF and the logic value of \( Q \) is not altered.

Similarly, in case of TFs affecting \( INT1b \), the following two conditions might be in order: 1) \( Q = 1 \), thus \( INT1b = INT3 = 0 \) (the series MN5-MN6 is OFF); 2) \( Q = 0 \), thus \( INT1b = INT3 = 1 \) (the series MN5-MN6 is on). In case 1), the TF makes \( INT1b \) flip to 1, thus temporarily turning ON MN6. However, since \( INT3 = 0 \) (it is not altered by the TF) MN5 remains OFF, and the logic value of \( Q \) is not altered. In case 2), the TF makes \( INT1b \) flip to 0, thus temporarily turning OFF MN6 and leaving the output \( Q \) in a high-impedance state, thus not altering its correct logic value.

As for TFs affecting INT2 and INT3, they may produce incorrect logic values on both nodes INT2 and INT3, since the positive feedback loop constituted by inverters I1 and I2 could confirm the wrong voltage value till the following CK cycle. The incorrect logic value on \( INT2 \) may turn on transistors MP3 or MN4, thus generating a contention between transistor MP3 and MN3 (that are driving node \( INT1a )\, or between transistors MP4 and MN4 (that are driving node \( INT1b )\). Despite the possible contention, \( INT1a \) and \( INT1b \) do not change their logic value, since MN3 and MP4 (driven by the output node \( Q \)) are dominant over MP3 and MN4. However, the electrical conflict gives rise to an increase in static power consumption till the following clock cycle. Moreover, both the series MP5-MP6 and MN5-MN6 are turned OFF, thus leaving node \( Q \) in a high-impedance state, so that the correct output value is maintained and the latch keeps on working correctly.

As for TFs affecting the output node \( Q \) when \( CK = 1 \), similarly to the case of the previous solutions in [11, 13], they generate only a voltage glitch, whose width and amplitude depend directly on the amount of charge injected by the hitting particle, and inversely on the strength of the transistor driving the node (that is, the series MP5-MP6 or MN5-MN6) and on the fan-out load. Afterward, since the series of transistors driving the output node keeps on conducting also after the TF exhaustion, the correct output value is restored.

Finally, let us consider the case of a TF affecting node INT2 or INT3 when the clock is gated. If a following TF affects node \( Q \), an incorrect logic value may be feedbacked, thus giving rise to an SE. However, the likelihood of this event (that is the combination of a TF affecting \( INT2 \) or \( INT3 \), followed by a second TF affecting node \( Q \)) can be considered negligible, especially for latches adopted for terrestrial applications.

3 HiPeR Latch Implementation and Verification

The proposed HiPeR latch has been implemented considering a standard 90 nm CMOS technology with \( V_{dd} = 1V \) and a clock frequency of 500 MHz. The transistors have the following aspect ratios (Fig. 1): 1) \( (W/L) = 1 \) for the transistors MN2, MN3, MN4, MN5, MN6, MN7, MP3, and the nMOS of inverters I1 and I2; 2) \( (W/L) = 2 \) for the transistors MN1, MP2, MP5, MP6, MP7 and the pMOS of inverters I1 and I2; 3) \( (W/L) = 4 \) for the transistors MP1 and MP4. As for the clock signal, it has been generated by a buffer with a conductance equal to \( 10\times \) that of a minimum-sized symmetric inverter.

The behavior of the HiPeR latch qualitatively described in the previous section has been verified by means of conventional and Monte Carlo electrical-level simulations, performed considering statistical variations (with uniform distribution) up to 20 percent of power supply, oxide thickness, transistor threshold voltage, and electron/hole mobility.

Transient faults producing both negative glitches (on nodes with a high logic value) and positive glitches (on nodes with a low logic value) have been emulated by connecting to the affected node an ideal current generator, denoted by \( I_{inj}(t) \). As proposed in [1], and reported in (1), it presents a double exponential pulse shape current, allowing to emulate the current produced by an alpha particle hit

\[
I_{inj}(t) = I_0(e^{-t/\tau_0} - e^{-t/\tau_1}).
\]  

The parameter \( I_0 \) depends on the amount of injected charge, while \( \tau_0 \) represents the collection time constant of the junction, and \( \tau_1 \) accounts for the ion track establishment time constant [28].

As an example, Figs. 2, 3, and 4 report the results of some simulations performed during the latching phase (i.e., when \( CK = 1 \), under nominal values of electrical parameters. Particularly, Figs. 2a and 2b show the effects of TFs affecting the internal nodes \( INT1a \) and \( INT1b \) respectively. As can be seen, the particle hits produce a voltage glitch that changes temporarily the logical state of the affected node. However, as described before, the correct logic values of \( INT1a \) and \( INT1b \) are restored by the respective driving transistors, so that the logic value of the output \( Q \) is not altered by these TFs.

Similarly, Figs. 3a and 3b report the effects of TFs affecting the internal nodes INT2 and INT3, respectively. The particle hits make the logic values of both nodes INT2 and INT3 flip. Although these incorrect logic values are maintained till the following falling edge of CK, the correct logic value of the output \( Q \) is not altered, and the latch keeps on working correctly.

Finally, Fig. 4 shows the effects of TFs affecting the latch output node \( Q \). The particle hits produce a voltage glitch on the output node that changes temporarily its logical state.
The correct output logic value is recovered within a time interval that depends directly on the amount of charge injected by the hitting particle, and inversely on the conductance of the transistors driving the output node (i.e., the series MP5-MP6 and MN5-MN6). It is worth noticing that, even though the correct value of \( Q \) is restored, the glitch generated at the output \( Q \) may propagate through the downstream logic and be captured by a memory element, or it may alter the value stored in a high-impedance node within a dynamic circuit, thus possibly resulting in an SE. However, this may also be the case for all robust latches. This will be taken into account in the evaluation of the robustness of the compared latches in Section 7.

Results analogous to those shown in Figs. 2, 3, and 4 have been obtained also by means of Monte Carlo simulations accounting for electrical parameter variations, as clarified at the beginning of this section.

4 Effects of Leakage Currents on the HiPeR Latch

In this section, we analyze the effects that leakage currents can produce on the HiPeR latch, when clock gating is employed to reduce power consumption.

As described in Section 2, TFs affecting nodes INT2 or INT3 when CK = 1 may produce incorrect logic values on both nodes INT2 and INT3. These incorrect logic values are
maintained till the next clock phase making the latch transparent (CK = 0). As a consequence, a contention between transistors MP3 and MN3 (driving node INT1a), or between transistors MP4 and MN4 (driving node INT1b) is generated. This contention does not change the logic values on INT1a and INT1b, thanks to the dominance of transistors MN3 and MP4 over transistors MP3 and MN4, respectively. However, it gives rise to static power consumption. Moreover, the flip of INT2 and INT3 moves one of the internal nodes INT1a (if Q = 0), or INT1b (if Q = 1) to a high-impedance state. In addition, the output C-element is turned OFF, thus making the output node Q to be also in a high-impedance state till the next clock low phase, thus retaining its correct logic value.

As introduced earlier, even in the perspective of significantly increased leakage currents with scaled technologies, since the latch operation frequency will also increase with scaling, the output Q and nodes INT1a or INT1b will remain in a high-impedance state for a time interval lower or equal to half clock cycle, which will not be long enough to allow also high leakage currents to change the logic value of these nodes.

Instead, if clock gating is implemented to reduce power consumption, the clock may be fixed to a constant value for long time intervals, which can be much longer than a single clock period. In this case, if a TF affects either INT2 or INT3, nodes Q and INT1a, or INT1b may remain in a high-impedance state for a time interval long enough to be possibly charged/discharged to incorrect logic values by leakage currents.

In order to analyze in detail the effects of TFs affecting INT2 or INT3 when clock gating is activated, electrical-level simulations have been performed, considering the same technology, power supply, and implementation of the HiPeR latch reported in the previous section. The obtained results are shown in Figs. 5a, 5b, 5c, and 5d.

Particularly, Fig. 5a shows the case of a TF occurring at time \( t_1 \) and affecting node INT2 when it presents a low logic value, while Fig. 5b reports the case of a TF affecting INT2 when it is at a high logic value. Similarly, the cases of TFs affecting node INT3 when it presents a low and a high logic value are shown in Figs. 5c and 5d, respectively.

It can be observed that, in all cases, after the particle hit, nodes INT2 and INT3 flip to an incorrect logic value, thus turning off the output C-element and leaving the output Q in a high-impedance state. Particularly, after the particle hit (at time \( t_1 \)), the voltage on the output node Q starts slowly swinging to an incorrect logic value due to leakage currents. After a time interval \( \Delta t = t_2 - t_1 \) ranging from 31 ns (Fig. 5a) to 149 ns (Fig. 5d), the output node Q moves to an incorrect logic value.

More in detail, from Figs. 5a and 5d it can be observed how leakage currents flowing through the series MP5-MP6 and MN5-MN6 start to slightly charge the node Q after \( t_1 \), while from Figs. 5b and 5c, we can observe how such leakage currents start to slightly discharge the node Q after
5 PROPOSED HiPeR-CG LATCH

In order to avoid the problems described in the previous section, which might originate if clock gating is adopted, a simple modification to the HiPeR latch is proposed here. This solution, hereinafter referred to as HiPeR-CG, is suitable to be used together with clock gating. In fact, it prevents the output $Q$ from being in a high-impedance state, after a TF affects any of its internal nodes. The electrical scheme of such a proposed latch is shown in Fig. 6.

The main differences with respect to the HiPeR latch are the following:

1. The pMOS transistor $MP7$ is now driven by the internal node $INT1a$, rather than by $CK$;
2. The nMOS transistor $MN7$ is now driven by the internal node $INT1b$, rather than by $CK$;
3. Addition of two transistors $MP8$ and $MN8$ driven by the output node $Q$; and
4. Addition of the transistor $MN10$, driven by $CK$, in series with $MN5$ and $MN6$, thus modifying the output C-element.

Let us now describe the behavior of the HiPeR-CG latch.

When $CK = 0$, the logic value ($d$) present at the input node $D$ propagates to the output $Q$ through transfer gate $TG1$, and to $INT2$ through transfer gate $TG2$. Since the voltage on $Q$ is equal to the voltage on $INT2$, the complemented logic value of the input is propagated to $INT3$ (through the C-element composed by $MP8$, $MN8$, and $I2$) and to $INT1a$ (through $MP3$ or $MN3$, depending on whether $d = 0$ or $d = 1$, respectively) and to $INT1b$ (through $MP4$ or $MN4$, depending on whether $d = 0$ or $d = 1$, respectively). Thus, $INT1a = INT1b = INT3$, and the logic value on $INT2$ is confirmed by the C-element composed by $MP7$, $MN7$, and $I1$. It is worth noticing that, when $CK = 0$, the additional transistor $MN10$ is OFF, thus avoiding possible contentions between the gate driving the latch input and the series transistors $MN10$-$MN5$-$MN6$.

Instead, when $CK = 1$, transfer gates $TG1$ and $TG2$ are turned off, while transistor $MN10$ is turned on. As a consequence, the value previously present on node $Q$ is maintained by the modified output C-element.

The behavior of the proposed HiPeR-CG latch in case of TFs is similar to that of the latch in Fig. 1, described in Section 2. However, node $INT2$ is now driven by a C-element composed by the transistors $MP7$ and $MN7$ and the inverter $I1$, thus avoiding that TFs generated on node $INT3$ can propagate to $INT2$. Similarly, node $INT3$ is driven by another C-element composed by the transistors $MP8$ and $MN8$ and the inverter $I2$, thus preventing TFs generated on node $INT2$ from being propagated to $INT3$. Therefore, differently from the HiPeR latch, TFs affecting nodes $INT2$ or $INT3$ of the HiPeR-CG latch produce a voltage glitch that is not confirmed, so that the correct voltage value is recovered on the hit node (i.e., $INT2$ or $INT3$), and the output node $Q$ is not left in a high-impedance state.

Finally, as for TFs affecting the other latch nodes (i.e., nodes $INT1a$, $INT1b$, and $Q$), similarly to the case of the HiPeR latch, they are tolerated.

6 HiPeR-CG LATCH IMPLEMENTATION AND VERIFICATION

The HiPeR-CG latch has been implemented considering a standard 90 nm CMOS technology with $V_{dd} = 1V$. The following transistor aspect ratios have been considered (Fig. 6): 1) ($W/L = 1$ for the transistors $MN2$, $MN3$, $MN4$, $MN5$, $MN6$, $MN7$, $MN8$, $MN10$, $MP3$ and the nMOS of inverters $I1$ and $I2$; 2) ($W/L = 2$ for the transistors $MN1$, $MP2$, $MP5$, $MP6$, $MP7$, $MP8$ and the pMOS of inverters $I1$ and $I2$; 3) ($W/L = 4$ for the transistors $MP1$ and $MP4$.

The particle hits have been emulated by connecting an ideal current generator to the affected node, as described in Section 3.

As for the HiPeR-CG latch behavior, considerations analogous to those given for the HiPeR latch hold true in case of normal operation (that is, without clock gating). Instead, when clock gating is applied, the HiPeR-CG latch

---

*Fig. 6. Electrical structure of the proposed HiPeR-CG latch.*
differs considerably from the HiPeR latch. The simulation results achieved for this latter case are reported here. Figs. 7a, 7b, 7c, and 7d show the cases of TFs affecting either INT2 or INT3 at a time instant denoted by \( t_1 \), while keeping the clock fixed at its latching value (\( CK = 1 \) in our case) for long time intervals.

More in detail, Figs. 7a and 7b report the cases of a TF affecting node INT2 when it presents a low and a high logic value, respectively. As can be seen, the particle hits produce a voltage glitch that changes temporarily the state of the affected node. However, the correct logic values of INT2 and INT3 are restored after a time interval depending on the particle energy, strength of the transistors driving the node, and node capacitance.

Analogous considerations hold true for the case of TFs affecting INT3, reported in Figs. 7c and 7d. However, the logic value of the output \( Q \) is not altered by these TFs in all considered cases.

7 Comparison with Alternative Solutions

In this section, the proposed HiPeR (Fig. 1) and HiPeR-CG latches (Fig. 6) are compared with the standard latch [27] and with the most recently proposed robust latches in [19], [13], [20], [15], [21], [16], [11], considering robustness against TFs and cost (in terms of area, power, and delay). The solution in [17] has not been considered for comparison purposes, since it has been proposed for scan FFs.

Electrical-level simulations of all compared latches have been performed employing a standard 90 nm CMOS technology, \( V_{dd} = 1V \), and a clock frequency of 500 MHz. Additionally, for the purpose of comparison, the case of minimal area design (i.e., minimum possible transistor sizes making the latches work properly) has been considered for all latches.

7.1 Robustness Against TFs

In this section, the robustness of the considered latches against TFs are evaluated and compared to each other. As discussed in [20], the SER of a latch can be expressed by the sum of several contributions, each referred to a node of the latch. In turn, the TF susceptibility of each node can be expressed as a function of: 1) the window-of-vulnerability (WOV), which is the time interval within a CK period (\( T_{CK} \)) during which a TF hitting the node can propagate till the output of the latch and give rise to an SE and 2) the critical charge (\( Q_{crit} \)) of the considered node, that is, the amount of charge collected by the hit node that produces a voltage glitch with an amplitude exceeding the logic threshold of the fan-out gate. Therefore, the total SER for a latch is given by:

\[
SER = \sum_{i=1}^{n} \frac{WOV_i}{T_{CK}} \cdot k_i \cdot \alpha \cdot e^{-\beta \cdot Q_{crit}(i)},
\]

where \( n \) is the number of nodes, \( k_i \) is a constant proportional to the area of the node \( i \), and \( \alpha \) and \( \beta \) are fitting parameters.
As discussed in [20], SEs caused by TFs affecting the internal/output nodes of a latch are the major contributors to the overall latch SER, while SEs caused by TFs affecting the latch input node have a marginal impact. This is mainly because the WOV of the latch input node (which is generally equal to the latch setup time) is considerably smaller than the WOVs of the latch internal and output nodes, which is generally equal to half of the CK period [20], that is, to the clock latching phase (CK = 1 for all considered latches). Therefore, for comparison purposes, the robustness of the latches has been evaluated by considering only TFs affecting their internal and output nodes when CK = 1.

In order to compare the robustness of the latches, the critical charges of internal and output nodes for all considered latches are evaluated. We can distinguish three kinds of nodes. Nodes of kind i) that is, nodes such that an affecting TF produces only a voltage glitch on the node, without propagating to (i.e., affecting) the output node Q, independently of the energy of the hitting particle. For these nodes, the critical charge is conventionally set to infinity: \( Q_{\text{crit}} \to \infty \). Nodes of kind ii) that is, nodes such that an affecting TF produces a voltage glitch that may propagate to the output Q, whose correct value is restored after a time interval depending on the particle energy, on the strength of the transistor driving the node, and on the node capacitance. As discussed previously, even though the correct value of Q is restored, the glitch generated at the output may propagate through the downstream logic and be captured by a memory element, or it may alter the value stored in a high-impedance node within a dynamic circuit, thus possibly producing an SE. For such nodes, the critical charge \( Q_{\text{crit}} \) is evaluated by means of Hspice simulations, as the amount of collected charge that generates an output glitch with an amplitude equal to half the power supply, that is, equal to the logic threshold of a symmetric fan-out gate. Finally, we can identify nodes of kind iii) namely, nodes such that an affecting TF produces an upset at the output of the latch. This is the most critical kind of nodes, since an output soft error may be generated. Analogously to nodes of kind ii) the critical charge \( Q_{\text{crit}} \) is evaluated by measuring (by means of Hspice) the amount of collected charge resulting in an output voltage glitch equal to the fan-out logic threshold.

As for the proposed HiPeR latch, TFs affecting the internal nodes INT1a and INT1b do not alter the logic value of the output Q (they are tolerated by design). Therefore, these nodes are of kind i) and their critical charge is assumed to be \( Q_{\text{crit(INT1a)}} = Q_{\text{crit(INT1b)}} \to \infty \). Analogous considerations hold true for nodes INT2 and INT3, so that \( Q_{\text{crit(INT2)}} = Q_{\text{crit(INT3)}} \to \infty \). As for TFs affecting directly the output node Q, they produce a voltage glitch on such a node that is recovered after a time interval depending on the particle energy, on the strength of the transistor driving the node, and on the node capacitance. Therefore, this node is a node of kind ii) and, from Hspice simulations, a critical charge \( Q_{\text{crit(Q)}} = 7.9fC \) has been estimated. Finally, considering the HiPeR-CG latch, results analogous to those obtained for the HiPeR latch have been found. Particularly, it is \( Q_{\text{crit(Q)}} = 7.9fC \).

In order to compare the robustness of all considered latches, two metrics are introduced. They are denoted by \( R_{\text{HiPeR}} \) and \( R_{\text{HiPeR-CG}} \), and report the ratios between the SER of the compared latches and that of the HiPeR and HiPeR-CG latch, respectively. They are defined as follows:

\[
R_{\text{HiPeR}}(\text{comp latches}) = \frac{SER(\text{comp latches})}{SER(\text{HiPeR})} = \frac{\sum_{i=1}^{n} P_{N_i} \cdot \alpha \cdot e^{-\beta Q_{\text{crit(i)}}}}{\sum_{i}^{n} P_{N_i} \cdot \alpha \cdot e^{-\beta Q_{\text{crit(i)}}}}_{\text{HiPeR}},
\]

\[
R_{\text{HiPeR-CG}}(\text{comp latches}) = \frac{SER(\text{comp latches})}{SER(\text{HiPeR-CG})} = \frac{\sum_{i=1}^{n} P_{N_i} \cdot \alpha \cdot e^{-\beta Q_{\text{crit(i)}}}}{\sum_{i}^{n} P_{N_i} \cdot \alpha \cdot e^{-\beta Q_{\text{crit(i)}}}}_{\text{HiPeR-CG}},
\]

If \( R > 1 \), the reference latch (HiPeR or HiPeR-CG) is more robust against TFs than the compared latch.

The factor \( P_{N_i} \) (proportional to parameter \( \kappa_i \) in (2)) accounts for the probability that a TF affecting the circuit hits a susceptible node. It is given by:

\[
P_{N_i} = \frac{A_{D_i}}{A_{TOT}},
\]

where \( A_{D_i} \) represents the (susceptible) area of the drain junctions of node \( i \), while \( A_{TOT} \) represents the area of all compared latches (employed as a normalization factor). For the HiPeR and HiPeR-CG latches, the following values of \( P_{N_i} \) have been found: \( P_{\text{INT1a}} = 0.007; P_{\text{INT1b}} = 0.018; P_{\text{INT2}} = 0.021; P_{\text{INT3}} = 0.011; P_Q = 0.032 \).

Evaluations analogous to those carried out for the proposed latches have been performed also for all compared latches. The obtained results are summarized in Table 1. For each latch, the table reports the number of susceptible nodes and their kind, the total susceptible area normalized to the

<table>
<thead>
<tr>
<th>Latch</th>
<th>Number of susceptible nodes</th>
<th>Normalized susceptible area (class i and ii)</th>
<th>Qcrit (fC)</th>
<th>RsER HipeR</th>
<th>RsER HipeR-CG</th>
</tr>
</thead>
<tbody>
<tr>
<td>HiPeR</td>
<td>4 of kind i 1 of kind ii</td>
<td>0.032</td>
<td>7</td>
<td>→+→</td>
<td>1.06</td>
</tr>
<tr>
<td>HiPeR-CG</td>
<td>4 of kind i 1 of kind ii</td>
<td>0.032</td>
<td>7.9</td>
<td>→+→</td>
<td>0.94</td>
</tr>
<tr>
<td>Standard</td>
<td>3 of kind ii</td>
<td>0.074</td>
<td>6</td>
<td>10.6</td>
<td>2.09</td>
</tr>
<tr>
<td>Latch in [11]</td>
<td>2 of kind i 3 of kind ii</td>
<td>0.085</td>
<td>20</td>
<td>→+→</td>
<td>0.97</td>
</tr>
<tr>
<td>Latch in [16]</td>
<td>4 of kind i 3 of kind ii</td>
<td>0.032</td>
<td>4.6</td>
<td>→+→</td>
<td>1.04</td>
</tr>
<tr>
<td>Latch in [21]</td>
<td>3 of kind ii</td>
<td>0.085</td>
<td>8.5</td>
<td>29.6</td>
<td>1.77</td>
</tr>
<tr>
<td>Latch in [15]</td>
<td>3 of kind ii 2 of kind ii</td>
<td>0.042</td>
<td>9.1</td>
<td>→+→</td>
<td>0.89</td>
</tr>
<tr>
<td>Latch in [20]</td>
<td>2 of kind i 3 of kind ii</td>
<td>0.042</td>
<td>8.7</td>
<td>→+→</td>
<td>1.18</td>
</tr>
<tr>
<td>Latch in [19]</td>
<td>2 of kind i 3 of kind ii</td>
<td>0.074</td>
<td>12.5</td>
<td>→+→</td>
<td>1.11</td>
</tr>
</tbody>
</table>

![Image](https://example.com/image.png)
total area of the latches, considering only nodes of kind ii) and iii), and the minimum and maximum values of the critical charge obtained considering all susceptible nodes. Finally, the last two columns report the values of the estimated \( R_{\text{HiPeR}} \) and \( R_{\text{HiPeR-CG}} \), as defined in (3) and (4), respectively, whose values have been computed deriving the value of the parameter \( \beta \) from [29] \( (\beta = 72 \times 10^{12} / C \) for the considered 90 nm CMOS technology).

As can be seen, the standard latch, as well as the robust latches in [19], [20], [21] include nodes of kind iii), so that a TF affecting these nodes may result in a soft error. Instead, all other latches, including the proposed ones, present only nodes of kind i) and iii), thus avoiding the generation of an SE at the latch output. Among all robust latches, the HiPeR and HiPeR-CG feature higher or comparable robustness, but for the latch in [15]. However, as clarified in the following section, this latter requires higher area overhead, propagation delay, and power consumption.

### 7.2 Cost Comparison

The cost of the latches has been compared in terms of required area overhead, propagation delay, power consumption, and power-delay product. Electrical-level simulations of all compared latches have been performed, considering a standard 90 nm CMOS technology, \( V_{dd} = 1V \), and a clock frequency of 500 MHz. The propagation delay has been estimated by evaluating the input-output delay \( (T_{\text{D-Q}}) \) when the latch is transparent. Particularly, it has been obtained by averaging the time elapsing between the occurrence of a transition at the latch input and the occurrence of the corresponding transition of the output transition (both measured at the 50 percent of \( V_{dd} \)) for both \( 0 \rightarrow 1 \) and \( 1 \rightarrow 0 \) input transitions. Finally, as for power consumption, it has been evaluated assuming an input switching activity of 25 percent. Moreover, the power consumption of the clock drivers has been included in the evaluation. For all latches, a clock driver composed by two cascaded inverters with aspect ratios \( (W/L)_{p} = 20 \) and \( (W/L)_{n} = 10 \) has been considered. The static power consumption due to leakage has been included as well.

For a detailed comparison, the relative costs in terms of area \( (\Delta A) \), power consumption \( (\Delta P) \), propagation delay \( (\Delta d) \), and power-delay product \( (\Delta (P \times d)) \) of the considered latches over the HiPeR and HiPeR-CG latches are reported in Table 3. In the last column, the relative SER \( (\delta \text{SER}) \) is also reported. For the HiPeR latch, the relative variations have been computed as: \( \Delta = 100 \times (\text{HiPeR} – \text{compared Latch}) / \text{HiPeR} \). Similar is the case for the HiPeR-CG latch.

Compared to the standard latch, similarly to all considered robust solutions, our latches require higher area overhead and power consumption.

As for propagation delay, our proposed latches are faster than all other considered latches (including the standard one). Particularly, the HiPeR-CG latch is the fastest one, with a propagation delay slightly lower (–6 percent) than that of the HiPeR latch. Compared to the HiPeR-CG latch, the increase in propagation delay of the alternative solutions ranges from +3.4 percent for the latch in [20], to +195 percent for the latch in [21].

As for robustness, the HiPeR and HiPeR-CG latches feature an SER that is lower than, or comparable to that of the other considered latches, but for the latch in [15], which features a lower SER, but requires a higher area overhead, propagation delay, and power consumption.

As for area overhead, our latches feature higher area than the latches in [19], [13], [20], [21], [16] which, however, are considerably slower and provide a higher SER.

As for power consumption, the HiPeR and HiPeR-CG latches consume more power than the scheme in [16], [20], [13], [19] which, however, are slower and less robust.

### 8 Conclusions

In this paper, first, a new high-performance robust latch (denoted as HiPeR latch) has been presented. It is insensitive to TFs affecting its internal and output nodes by design, independently of the energy of the hitting particles. Then, a modified version of the HiPeR latch (denoted as HiPeR-CG latch) has been proposed, that is suitable to be used together with clock gating. In fact, as shown in the paper, when clock gating is implemented to reduce power consumption, TFs affecting some internal nodes of the HiPeR latch may leave its output node in a high-impedance state, thus possibly allowing leakage.

<table>
<thead>
<tr>
<th>Table 2</th>
<th>Absolute Cost of the Compared Latches</th>
</tr>
</thead>
<tbody>
<tr>
<td>Latch</td>
<td>Area (( \mu )m²)</td>
</tr>
<tr>
<td>HiPeR</td>
<td>31</td>
</tr>
<tr>
<td>HiPeR-CG</td>
<td>35</td>
</tr>
<tr>
<td>Standard</td>
<td>18</td>
</tr>
<tr>
<td>Latch in [11]</td>
<td>37</td>
</tr>
<tr>
<td>Latch in [16]</td>
<td>27</td>
</tr>
<tr>
<td>Latch in [21]</td>
<td>21</td>
</tr>
<tr>
<td>Latch in [15]</td>
<td>40</td>
</tr>
<tr>
<td>Latch in [20]</td>
<td>24</td>
</tr>
<tr>
<td>Latch in [13]</td>
<td>21</td>
</tr>
<tr>
<td>Latch in [19]</td>
<td>27</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 3</th>
<th>Relative Cost and Robustness of the Compared Latches with Respect to Those of the HiPeR Latch (Fig. 1) and the HiPeR-CG Latch (Fig. 6)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Latch</td>
<td>( \Delta A )</td>
</tr>
<tr>
<td>HiPeR-CG</td>
<td>-</td>
</tr>
<tr>
<td>Standard</td>
<td>-0.5</td>
</tr>
<tr>
<td>Latch in [11]</td>
<td>1.3</td>
</tr>
<tr>
<td>Latch in [16]</td>
<td>2.8</td>
</tr>
<tr>
<td>Latch in [21]</td>
<td>3.2</td>
</tr>
<tr>
<td>Latch in [15]</td>
<td>1.3</td>
</tr>
<tr>
<td>Latch in [20]</td>
<td>2.8</td>
</tr>
<tr>
<td>Latch in [13]</td>
<td>3.2</td>
</tr>
<tr>
<td>Latch in [19]</td>
<td>1.3</td>
</tr>
</tbody>
</table>

\( \delta \text{SER} = \text{HiPeR-CG} - \text{compared Latch} / \text{HiPeR-CG} \)
currents to change the stored logic value, with consequent reliability risks. It has been shown that this problem is overcome by the proposed HiPeR-CG latch at the cost of 13 percent extra area, and with no impact on performance, which is, indeed, improved.

It has been shown that the HiPeR and HiPeR-CG latches feature considerably better characteristics in terms of performance compared to all other considered robust latches, but for the latch in [20], which presents comparable input-output delay, but features a considerably lower robustness to TFs. In addition, our proposed latches provide higher or comparable robustness to TFs compared to the considered alternative robust solutions, except for the latch in [15], which features the higher robustness, but requires higher costs in terms of area and power.

More in detail, our latches features higher area than the latches presenting lower robustness [19], [13], [20], [21], [16]. As for power, the latch in [16] is less consuming, but it is considerably slower and less robust than our proposed latches. Finally, compared to the latch in [11], the proposed solutions present comparable area, power, and robustness, but are considerably faster. Therefore, thanks to the good trade-offs in terms of performance, robustness, and cost, our proposed latches are particularly suitable to be adopted on critical paths.

ACKNOWLEDGMENTS

This work was partially supported by an Intel Corporation research grant.

REFERENCES


Martin Omaña received the degree in electronic engineering from the University of Buenos Aires, Argentina, in 2000, and the PhD degree in electronic engineering and computer science from the Electronics Department of the University of Bologna, Italy, in 2005, which he joined in 2002 after receiving a MADESS grant and is now a postdoctoral fellow. His research interests are in the field of design and test of digital systems, reliable and error-resilient systems, fault tolerance, online testing, fault modeling, and diagnosis and debugging.
Daniele Rossi received the degree in electronic engineering and the PhD degree in electronic engineering and computer science from the University of Bologna in 2001 and 2005, respectively. His research interests include fault modeling, online testing, and fault tolerance techniques, with particular focus on coding techniques for fault-tolerant and low-power buses, signal integrity for VDSM communication infrastructures, and robust design for soft error resiliency. He holds one patent. He is a member of the IEEE and the IEEE Computer Society.


For more information on this or any other computing topic, please visit our Digital Library at www.computer.org/publications/dlib.