IEICE TRANS. INF. & SYST., VOL.E105–D, NO.5 MAY 2022

PAPER

Evaluation and Test of Production Defects in Hardened Latches

Ruijun MA[†a)], **Stefan HOLST**[†b)], ***Nonmembers***, **Xiaoqing WEN**[†c)], ***Senior Member***, **Aibin YAN**[††d)], ***and*** **Hui XU**[†††e)], ***Nonmembers***

SUMMARY As modern CMOS circuits fabricated with advanced technology nodes are becoming more and more susceptible to soft-errors, many hardened latches have been proposed for reliable LSI designs. We reveal for the first time that production defects in such hardened latches can cause two serious problems: (1) these production defects are difficult to detect with conventional scan test and (2) these production defects can reduce the reliability of hardened latches. This paper systematically addresses these two problems with three major contributions: (1) Post-Test Vulnerability Factor (*PTVF*), a first-of-its-kind metric for quantifying the impact of production defects on hardened latches, (2) a novel Scan-Test-Aware Hardened Latch (STAHL) design that has the highest defect coverage compared to state-of-the-art hardened latch designs, and (3) an STAHL-based scan test procedure. Comprehensive simulation results demonstrate the accuracy of the proposed *PTVF* metric and the effectiveness of the STAHL-based scan test. As the first comprehensive study bridging the gap between hardened latch design and LSI testing, the findings of this paper will significantly improve the soft-error-related reliability of LSI designs for safety-critical applications.

key words: *soft-error, hardened latch, defect, scan test*

1. Introduction

The continuing trend towards lower power and higher integration leads to smaller feature sizes and lower supply voltages for Integrated Circuits (ICs). As a result, the amount of charge that defines the logic value of a storage element becomes smaller, making this storage element more vulnerable to soft-errors. They impact not only systems in high-radiation environments, such as aerospace [1], but also systems at the sea-level [2]–[4]. Soft-errors are caused by particles (such as heavy ions, alpha particles, muons, protons, neutrons, and electrons) striking the IC. The strikes can generate current pulses and possibly disrupt the states of storage elements [5]–[7]. Soft-errors can change data or disrupt a computer system, thus causing an erroneous operation. The impact of soft-errors depends on many factors, such as the angle of the strike, supply voltages, technology nodes, the energy of the particle, and process variations [8], [9]. It is important to protect ICs from the impact of soft-errors and maintain high reliability.

Sequential elements, such as latches and flip-flops, are most susceptible to soft-errors in logic circuits [7]. A flip-flop is commonly constructed of two latches. This paper focuses on latches because tolerating soft-errors in latches can reduce the vulnerability of flip-flops as well.

A soft-error in a latch that changes the state of one of its internal nodes is called single-event-upset (SEU). To tolerate SEUs, many hardened latches [10]–[16], [18], [19], [22] have been proposed by adding redundancy to their structures. The latch in [10] adds transistors at feedback loops to prevent SEUs from propagating. This latch has fewer transistors than most other hardened latches. The dual interlocked storage cell (DICE) [11] can tolerate SEUs by its interlocked structure. Triple modular redundancy (TMR) uses three standard latches to store the same data and uses a voter circuit to select the majority as its output. The hardened latches in [14]–[16] store logic values in multiple feedback loops and use a voter circuit (such as C-element) to select the correct output. The design in [17] can tolerate single-event-transients (SETs) and SEUs by its dual-modular structure. However, there are two major problems with these state-of-the-art hardened latches as follows:

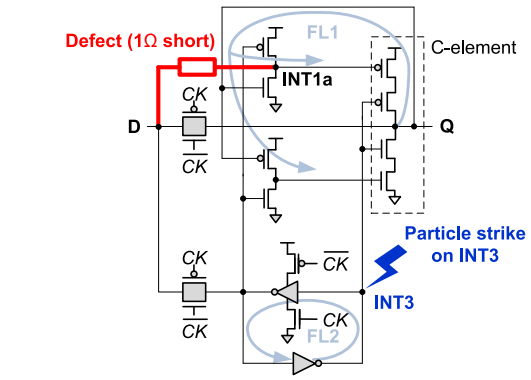
Problem-1 (Low Testability): Observability, the ability to obtain a circuit's internal state by checking its outputs, is an important metric to evaluate a circuit's testability. Some production defects within hardened latches cannot be observed at their outputs. This is because the impacts of these production defects are masked by the same circuitry designed to mask SEUs. Therefore, hardened latches have a low observability and thus a low testability.

Figure 1 illustrates this problem. Figure 1 (a) shows a typical hardened latch (HiPeR) [16], which has two feedback loops FL1 and FL2. Suppose that a short defect exists between D and INT1a due to imperfect production. The SPICE simulation result in Fig. 1 (b) shows that this defective latch still works functionally and this defect cannot be observed. Undetected defects may lead to early-life failures. Furthermore, a lower defect coverage of a hardened latch may lead to an overestimation of production quality.

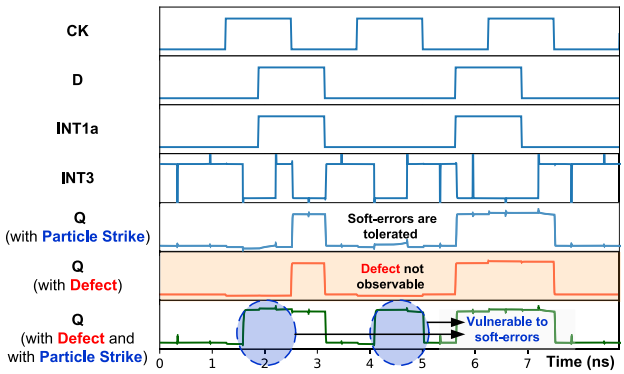
Problem-2 (Low Soft-Error Tolerability): If a defect exists in a hardened latch due to imperfect production, the hardened latch's soft-error tolerability may be reduced,

Manuscript received October 13, 2021.
Manuscript revised December 13, 2021.
Manuscript publicized February 7, 2022.

[†]The authors are with Kyushu Institute of Technology, Iizuka-shi, 820–8502 Japan.
[††]The author is with Anhui University, Hefei, 230000, China.
[†††]The author is with Anhui University of Science and Technology, Huainan, 232000, China.
a) E-mail: ruijun_ma@foxmail.com (Corresponding author)
b) E-mail: holst@csn.kyutech.ac.jp
c) E-mail: wen@csn.kyutech.ac.jp
d) E-mail: abyan@mail.ustc.edu.cn
e) E-mail: austxuhui@163.com
DOI: 10.1587/transinf.2021EDP7216



(a) HiPeR [16] with a short defect



(b) SPICE simulation

Fig. 1 The impact of production defects.

making it more vulnerable to SEUs.

Consider the hardened latch shown in Fig. 1 (a), which has an undetected short defect. Usually, when the node INT3 is hit by a particle, the change of state will be tolerated by the C-element and the output Q remains correct. However, the SPICE simulation in Fig. 1 (b) shows that a particle strike on INT3 cannot be tolerated by this defective latch. This is because an input (INT1a) of the C-element is compromised by the short defect. Consequently, this defective hardened latch suffers from SEUs while a defect-free one does not.

The above two problems are addressed in this paper through the following three major contributions:

Contribution-1 (*PTVF*): This work is the first to analyze the relationship between the soft-error tolerability of a hardened latch and production defects (**Problem-2**). A novel metric, called Post-Test Vulnerability Factor (*PTVF*), is proposed for quantifying the impact of production defects on hardened latches.

Contribution-2 (STAHL): To address **Problem-1**, we introduce a novel Scan-Test-Aware Hardened Latch (STAHL) which is hardened against SEUs and at the same time has the highest defect coverage among all state-of-the-art hardened latch designs.

Contribution-3 (An STAHL-based Scan Test): Taking full advantage of STAHL's high testability requires some changes to the Design-for-Test (DFT) infrastructure. We propose a novel minimal-overhead scan design and a novel test procedure based on the STAHL-based scan chains.

The rest of the paper is organized as follows: Sect. 2 describes the background on soft-error rate (SER) and testing. The proposed *PTVF* metric is introduced in Sect. 3. The structure of the STAHL is described in Sect. 4. Section 5 shows the usage of STAHLs in a scan chain and a novel test procedure for fully testing the STAHLs. Section 6 shows evaluation results and Sect. 7 concludes the paper.

2. Background

2.1 Soft-Error Rate

The soft-error rate (SER) is defined as the occurrence frequency of soft-errors. To reduce SER, various soft-error tolerance methods have been proposed. A lower SER means that these methods have better soft-error tolerability. Therefore, these methods can be evaluated by calculating their SER. There are some SER calculation metrics for combinational logic and memories [27], as well as for latches [7], [16].

The SER calculation metrics of latches usually consider two factors: timing vulnerability factor (TVF) and architectural vulnerability factor (AVF) [7]. The TVF is defined as the fraction of time that a node is susceptible to a soft-error. The AVF is defined as the probability that a soft-error in a node of a latch results in an erroneous output. In our previous research [21], we proposed an SER calculation metric for latches, called soft-error vulnerability (*SEV*). In the calculation of *SEV*, the TVFs are set to 1 for the following reasons.

(1) This research focuses on the AVF of latches;
(2) AVFs and TVFs are independent of each other;
(3) TVFs should be the same for a fair comparison.

Let c be a standard cell of a latch. Let $F(c)$ be a set of particles that may hit the cell c during operation. We assume that a cell is hit by a single particle $f \in F(c)$ at a time, but depending on the underlying soft-error model, particles may hit multiple nodes in the cell [4]. Let $P_F : f \in F(c) \rightarrow (0 \cdots 1]$ be the probability density function that gives the relative occurrence probability of a particular particle strike f. By definition, we have: $\sum_{f \in F(c)} P_F(f) = 1$. The particle set $F(c)$ and probabilities P_F are determined by the chosen soft-error model, e.g. [16]. This modeling does not put any restrictions on the number of nodes being hit by a particle. As multiple-node-upsets are becoming more common in modern technology nodes [4], they can be easily added as elements to $F(c)$ with their corresponding probabilities in P_F.

The soft-error vulnerability (*SEV*) is the probability that a latch cell shows erroneous outputs when the latch cell is hit by particles. The vulnerability of a latch cell c for a soft-error f can be defined as a characteristic function $v(c, f) : L \times F(c) \rightarrow [0 \cdots 1]$. This function gives a cell $c \in L$ (with L being the set of latch designs) and a soft-error

$f \in F(c)$ the probability that the output of the latch cell shows an error. The overall soft-error vulnerability of a latch cell c is calculated by:

$$SEV(c) = \sum_{f \in F(c)} P_F(f) \cdot v(c, f) \quad (1)$$

These SER metrics are for the defect-free hardened latches. However, production defects may occur during hardened latches' manufacturing and may make these defective latches vulnerable to soft-errors. Thus, there is a significant need to propose a new metric to evaluate the impact of production defects on the soft-error vulnerability of these hardened latches.

2.2 Testing

A production defect (such as a short or an open) is a flaw due to imperfect production and may cause a malfunction of a circuit. Testing is used to find defective manufactured devices. It applies test vectors to a circuit under test (CUT) and analyzes its test responses. A circuit that outputs correct test responses passes the test; otherwise, it fails the test [20].

To test a circuit efficiently, it is necessary to consider all possible production defects in the CUT and generate an efficient set of test vectors to detect these defects. However, it is difficult to generate the behavior of real defects for test generation. Hence, fault models are used to represent the physical condition of production defects. A good fault model can accurately show the behavior of a defect and can be efficient for simulation and test pattern generation [23]–[25].

2.2.1 Design-for-Test

Due to the complexity of modern circuits, it is difficult to set and check numerous internal states of sequential circuits from limited external pins. Design-for-test (DFT) techniques can overcome this difficulty by modifying storage elements and providing direct access to these storage elements.

Scan design is the most commonly used DFT technique [20]. In a full-scan design, all functional flip-flops in a circuit are replaced with scan cells, which are then connected into scan chains. The internal states of all scan cells can be set by shifting test vectors through these scan chains and be checked by shifting out the corresponding test responses.

Figure 2 shows a scan chain example with a combinational portion and three scan cells. Each scan cell has a multiplexer and a flip-flop constructed by two latches. The scan-enable (SE) signal switches each scan cell between shift mode and functional mode by controlling its multiplexer. The clock (CK) signal controls the operation of latches.

This scan chain can perform a scan test to fully test a sequential circuit and the operation is as follows. First, SE is set to 1 and this scan chain operates in shift mode. Scan cells work collectively as a shift register for shifting in

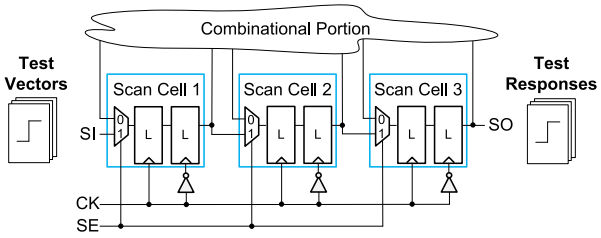


Fig. 2 Scan chain example.

test vectors from scan-in (SI). By this operation, each scan cell stores a logic value. A sequence of these stored logic values is called a test vector. The logic values stored in these scan cells then propagate to the combinational portion and generate corresponding test responses. Second, SE is set to 0, all scan cells operate individually as flip-flops (functional mode), and test responses are captured by each scan cell with the next clock. Finally, SE is set to 1 for shifting out these test responses through scan-out (SO) for analysis.

Before a scan test, flush tests are performed to make sure all scan cells work correctly. A flush test is a shift test where a chosen flush pattern (such as "01100" [20]) is shifted through a scan chain to verify that the same flush pattern reaches the end of the scan chain at the correct clock cycle. For example, Fig. 2 shows a scan chain with 3 scan cells. During a flush test, SE remains at 1. A flush pattern is shifted in from SI. The same flush pattern is expected to reach the SO after 3 clock cycles. If the shift-out pattern is changed or at a different clock cycle, then this scan chain contains production defects.

However, if these scan cells in a scan chain are based on hardened latches, many production defects in the scan cells may not be detected by flush tests due to the cell-internal redundancy. Yet, the defective hardened latches become more vulnerable to soft-errors. Also, these undetected defects may become more and more serious and cause chips to fail eventually. Hence, it is important to propose a new DFT for testing designs that contain hardened latches.

2.2.2 Defect Coverage

For evaluating the testability of a circuit, defect coverage (DC) is used to measure the portion of all possible cell-internal production defects that are detected in a complete production test setting [24]–[26].

The defect coverage of a hardened latch cell is calculated by simulating a simple flush test with all possible production defects. We use the fault model of every possible defect based on the latch structure because most published hardened latch designs do not provide actual cell layouts. Also, this fault model can identify these undetected defects and can provide a guide when making a layout of a standard hardened latch cell. Let d be a production defect. Let $D(c)$ be a set of defects that may occur in the cell c during manufacturing. A cell c may be affected by at most one defect d, and we denote the defective cell as c_d. Let

$P_D : d \in D(c) \rightarrow (0 \cdots 1]$ be a probability density function that gives the relative occurrence probability of a defect d. By definition, we have: $\sum_{d \in D(c)} P_D(d) = 1$. The set $D(c)$ and the probabilities P_D are determined by the used fault model.

After the production of the cell c, we assume a simple pass-fail test modeled by a characteristic function $t : C \rightarrow \{1, 0\}$ with C being the set of all instances of the defective cell c_d. For any production defect $d \in D(c)$, the characteristic function evaluates to $t(c_d) = 1$, if the cell c with defect d passes the production test, and to $t(c_d) = 0$, otherwise. Clearly, the test passes always for the defect-free cell: $t(c) = 1$.

The defect coverage of the test t is:

$$DC(c,t) = \sum\nolimits_{d \in D(c)} P_D(d) \cdot (1 - t(c_d)) \tag{2}$$

If the test t fails ($t(c_d) = 0$) for all possible defects in the defect set, then the defect coverage $DC(c,t)$ is 100%. If the test does not detect all possible defects, $DC(c,t)$ will be reduced by the probability that the cell contains these undetected defects. For evaluating the impact of defects on the hardened latches, the cases that pass the test t ($t(c_d) = 1$) need to be analyzed.

3. A Novel Metric: Post-Test Vulnerability Factor

There is no previous work considering the interplay among production defects, the redundancy in hardened latches, and the residual soft-error tolerability of latches with undetected defects. In this section, we address this problem by proposing the first-of-its-kind metric, called Post-Test Vulnerability Factor (*PTVF*), to evaluate the impact of production defects on hardened latches.

3.1 Definition of *PTVF*

In previous works, defect coverage $DC(c,t)$ and soft-error vulnerability $SEV(c)$ have only been considered independently. However, whenever the defect coverage $DC(c,t)$ is less than 100%, some defective cells c_d pass the test ($t(c_d) = 1$). While the original defect-free cell c can tolerate soft-errors, the defective cell c_d that escaped the test t may not. In other words, the soft-error vulnerability to some particles f can change if some defect d is present: $v(c,f) \neq v(c_d,f)$. We define a novel metric called Post-Test Vulnerability Factor (*PTVF*) that takes the probabilities of the test-escaping defects into account as follows:

$$PTVF(c,t) = \frac{\sum_{d \in D(c)} P_D(d) \cdot t(c_d) \cdot SEV(c_d)}{1 - DC(c,t)} \tag{3}$$

The *PTVF* indicates the vulnerability of a cell when the cell has production defects and is hit by particles. It depends both on the defect coverage and the soft-error vulnerability of cells with undetected defects. If all defects are detected, $DC(c,t) = 1$, we define $PTVF(c,t) = 0$. If all defects $d \in D(c)$ that escape the test ($t(c_d) = 1$) do not impact the soft-error vulnerability of the latch cell ($SEV(c_d) = 0$), then the $PTVF(c,t)$ is 0 as well. In the remaining cases, the value of *PTVF* is less than or equal to 1 since the denominator of Eq. (3) is always greater than or equal to the numerator.

For example, let's assume that there are 100 possible defects in a hardened latch cell and each defect has an equal occurrence probability of 1%. Assume that the defect coverage (*DC*) of this hardened latch is 95%. Thus, 5 undetected defects make $t(c_d) = 1$. Let $UD = \{ud1, \cdots, ud5\}$ be a set of these undetected defects. The numerator of Eq. (3) $\sum_{d \in D(c)} P_D(d) \cdot t(c_d) \cdot SEV(c_d)$ equals to $\sum_{ud \in UD} P_D(ud) \cdot SEV(c_{ud})$ because $t(c_d) = 0$ for all detected defects. The $P_D(ud)$ is 1% in this example and $SEV(c_{ud})$ can be calculated by Eq. (1). Assume that each calculated $SEV(c_{ud})$ is 30%. The numerator of Eq. (3) is then: $5 \times 1\% \times 30\% = 1.5\%$. The denominator of Eq. (3) is $(1 - DC)$, which is 5% in this example. So, the *PTVF* is $1.5\%/5\% = 30\%$. The *PTVF* is independent from the overall defect coverage and the overall soft-error vulnerability. It is useful for characterizing and comparing latch designs.

3.2 Calculation of *PTVF*

A series of SPICE simulations are performed to calculate the *PTVF*. The necessary inputs are the SPICE netlist of the latch cell c, the set of production defects $D(c)$ and their probabilities P_D, the set of particles $F(c)$ and their probabilities P_F, the test conditions, test procedure, and pass/fail criterions. Each defect $d \in D(c)$ must be injected into the SPICE netlist (e.g. by inserting additional components like resistances between nets). Each particle $f \in F(c)$ must be injectable during transient analysis, e.g., by using additional current sources. The test t is given in form of a set of measurement times, expected values, and tolerances at the output of the latch. Without loss of generality, we assume a latch cell to be exhaustively tested with all possible combinations of inputs and states. A defect in the latch is considered to be detected if the latch outputs a wrong logic value for longer than a quarter of a clock cycle. Each SPICE simulation is a transient analysis of a few clock cycles and varying inputs similar to the inputs shown in Fig. 1 (b). A particle strike is considered to lead to an erroneous output, whenever the output of the latch has settled on a wrong logic value until the end of the latching phase.

The calculation flow is shown in Fig. 3. After initialization of two variables $V = 0$ and $DC = 0$ for accumulating the results, a production defect $d \in D(c)$ is injected into the original SPICE netlist to generate a model of c_d. The new netlist is simulated and the output of the defective latch is checked for erroneous values. If the defect d is observable ($t(c_d) = 0$), DC is updated to reflect the defect coverage. The V will not be changed and the loop continues with the next production defect. If the defect d is not observable, all particles $f \in F(c)$ are injected into the model c_d. For each particle f, $v(c_d, f)$ is calculated. If the model c_d is vulnerable to a particle strike, $v(c_d, f)$ will be positive. V is increased by the combined probability of the defect, the particles occurring, and the particle strike leading to an erroneous output

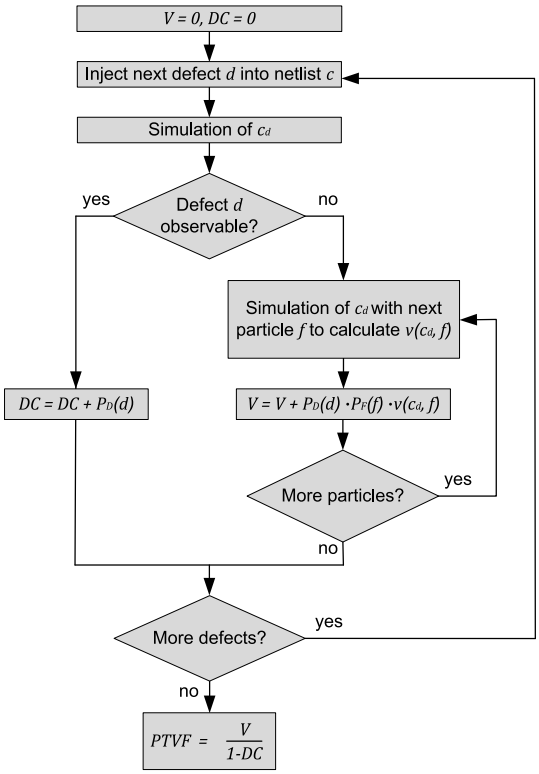


Fig. 3 *PTVF* calculation flow.

of the latch cell: $P_D(d) \cdot P_F(f) \cdot v(c_d, f)$.

Calculating the *PTVF* needs a large number of SPICE simulations since each latch is simulated with all possible production defects and the combinations of particles and undetected defects. However, each individual simulation is rather quick since it lasts only a few clock cycles on a single cell. Furthermore, most SPICE simulations are independent and can be executed in parallel. The worst-case computation complexity is $O(|D(c)| \cdot |F(c)|)$ with $|D(c)|$ being the number of defects and $|F(c)|$ being the number of particles.

4. Scan-Test-Aware Hardened Latch (STAHL)

To overcome **Problem-1 (Low Testability)**, a novel scan-test-aware hardened latch (STAHL) design is proposed [33]. The STAHL's structure is shown in Fig. 4.

Instead of using just one input D and one output Q as in a common latch, the STAHL has 2 inputs (D0 and D1) as well as 2 corresponding outputs (Q0 and Q1). In addition to the normal clock signals CK and $\overline{\text{CK}}$ (inverse signal of CK), the STAHL has an additional scan-enable (SE) signal that switches between shift mode (SE = 1) and functional mode (SE = 0). $\overline{\text{SE}}$ is the inverse signal of the SE. The STAHL contains 2 independent feedback loops (FL0 and FL1) formed by 2 clock-controlled transmission gates (TG2 and TG3), and 4 inverters (I0 to I3). The clock-controlled transmission gate TG0 (TG1) connects the input D0 (D1) to the feedback loop FL0 (FL1).

2 SE-signal-controlled transmission gates (TG4 and

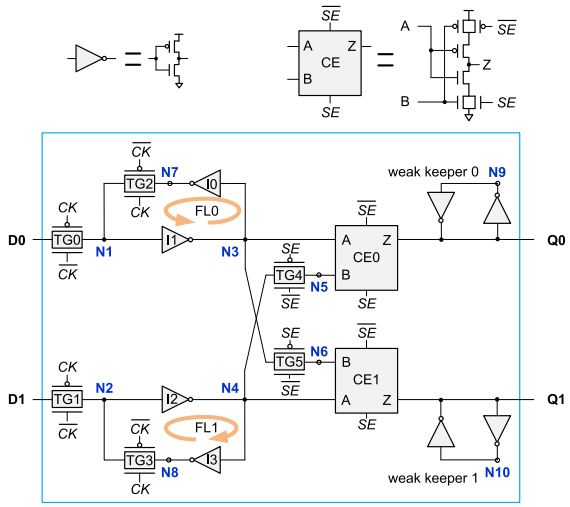


Fig. 4 Structure of the proposed STAHL.

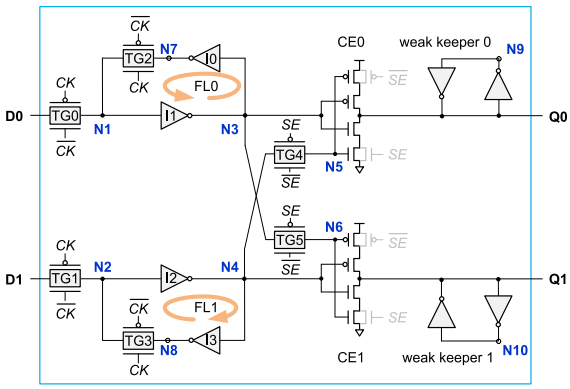


Fig. 5 SE = 0: functional (hardened) mode.

TG5) drive the inputs of 2 C-elements (CE0 and CE1). For each C-element, we add 2 SE-signal-controlled transistors (an $\overline{\text{SE}}$-controlled PMOS and an SE-controlled NMOS), which will be ON in shift mode and be OFF in functional mode. 2 C-elements work as 2 equivalent inverters in shift mode and can prevent SEUs from appearing at their outputs in functional mode. Note that weak keeper 0 (weak keeper 1) is at the output Q0 (Q1) to maintain the output value while the outputs of C-elements are in high-impedance.

Now, we describe the operation of the STAHL in both functional (hardened) mode and shift mode. The proposed STAHL and the latch design in [17] both use a dual-modular structure. The major difference between these two designs is that the proposed STAHL is a better testable design, because the additional SE-controlled C-elements and SE-controlled transmission gates can switch the STAHL between two modes.

4.1 Functional (Hardened) Mode

The STAHL is in functional mode when SE = 0. Figure 5 shows the circuit for this mode. In functional mode, the value to be stored in the latch needs to be applied to both

inputs D0 and D1. The transistors shown in gray in CE0 and CE1 are OFF. 2 SE-signal-controlled transmission gates (TG4 and TG5) are ON.

In the transparent phase (CK = 0), the transmission gates TG0 and TG1 are ON. The input value at D0 (D1) propagates through node N1 (N2), inverter I1 (I2), node N3 (N4), C-elements (CE0 and CE1) to outputs Q0 and Q1. Q0 or Q1 can be chosen as the main output.

In the latching phase (CK = 1), the transmission gates TG0 and TG1 are OFF, while TG2 and TG3 are ON. There are 2 feedback loops, FL0 and FL1. FL0 consists of inverters I0, I1, and TG2. FL1 consists of inverters I2, I3, and TG3. The input value is latched in 2 feedback loops. The inputs of the C-element CE0 (CE1) are driven by nodes N3 (N4) and N5 (N6).

SEUs can be tolerated by the STAHL as follows. Both feedback loops FL0 and FL1 will store the same value and are independent of each other.

Suppose that node N1 is affected by an SEU and its logic value is temporally changed. Node N3 is influenced through inverter I1. However, node N4 is not influenced, leaving the two C-elements in high-impedance. The correct output logic value at Q0 (Q1) will be kept by the weak keeper 0 (weak keeper 1). Similar analysis can be made for SEUs occurring on nodes N3, N5, and N7. Due to the symmetric nature of the STAHL, the same discussion holds for SEUs occurring on nodes N2, N4, N6, and N8.

Suppose that node Q0 is affected by an SEU and that the logic value of Q0 is temporally changed. However, nodes N3, N4, N5, and N6 are not influenced. The correct values at these nodes will continuously drive Q0 to a correct value. The same discussion holds for SEUs occurring on nodes Q1, N9, and N10.

4.2 Shift Mode

The STAHL is in shift mode when SE = 1. Figure 6 shows the circuit for this mode. The transistors shown in gray are OFF. 2 added SE-signal-controlled transistors in CE0 (CE1) are ON. The CE0 (CE1) acts as a simple inverter, which inverts the logic value stored in N3 (N4).

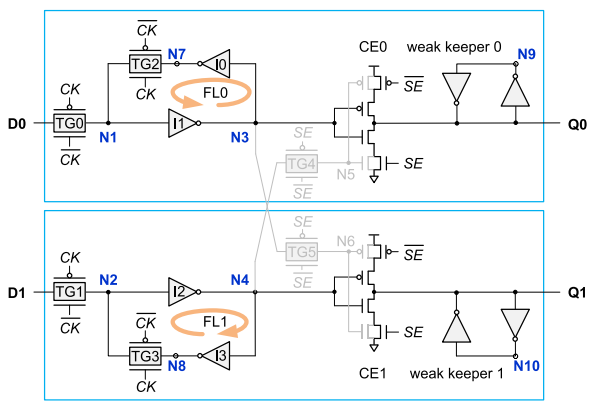


Fig. 6 SE = 1: shift mode.

In shift mode, both FL0 and FL1 are independent of each other, effectively forming 2 independent non-hardened latches D0 - Q0 and D1 - Q1. We need to apply test vectors to inputs of these two latches (D0 and D1) and observe their outputs (Q0 and Q1). Cross-connections from FL0 to CE1 and FL1 to CE0 (TG4 and TG5) can be tested in functional mode because open defects in them lead to small delay faults, which can be detected by a delay test. The other parts can be tested in shift mode because there is no redundancy in them.

5. Scan Test Based on STAHL

Scan test is the most popular DFT approach. The unique interface of the STAHL design (i.e., two inputs and two outputs) requires some changes to the scan chain structure and their control signals.

The following subsections will introduce the adapted DFT infrastructure with STAHL-based scan cells, and a new test procedure to fully test the latches as well as the circuit under test.

5.1 Scan Chain Structure

Figure 7 shows an STAHL-based scan cell. Two STAHLs (STAHL-A and STAHL-B) are used to form a flip-flop, and two additional multiplexers are used to make the scan cell. The input D and output Q connect with the combinational portion. Different from a conventional scan cell, the STAHL-based scan cell has two control signals: SE (scan-enable) and SA (scan-apply). The SE controls the input multiplexer to select between the data input (D) and the scan input (SI). The SE also switches the two STAHLs between shift mode and functional mode. The SA controls the output multiplexer to select between the outputs Q0 and Q1 of the STAHL-B.

When SA = 1, the Q0 of the STAHL-B connects to output Q. When SA = 0, the Q1 connects to output Q. When switching from shift mode to functional mode while the 2

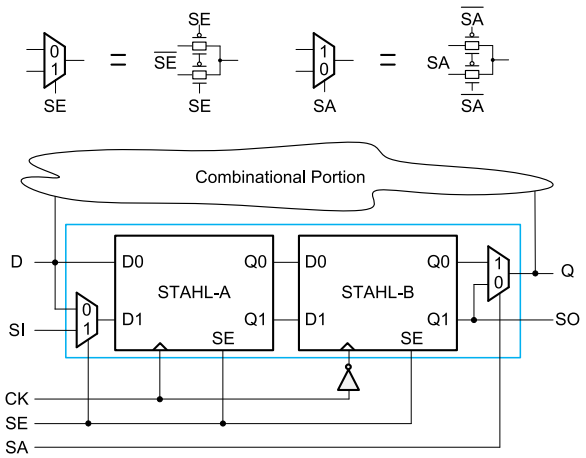


Fig. 7 STAHL-based scan cell.

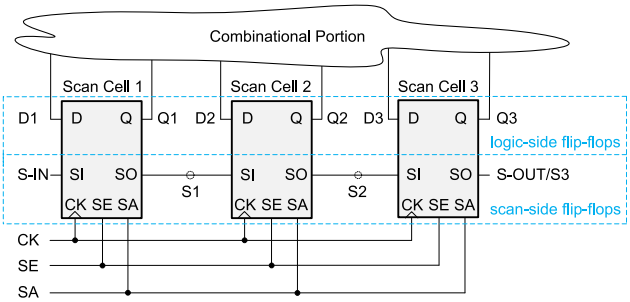


Fig. 8 STAHL-based scan chain.

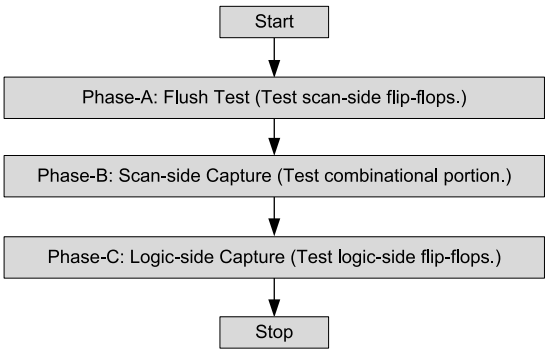


Fig. 9 Test procedure flow.

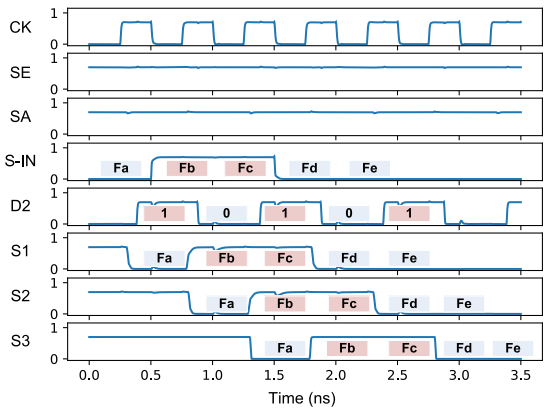


Fig. 10 SE = 1 and SA = 1: a test pattern of FaFbFcFdFe = 01100 flushes through the scan-side flip-flops.

independent latches of STAHL-B (D0 - Q0 and D1 - Q1) hold different values, the outputs of STAHL-B will remain different when SE is changed to 0 (functional mode). The weak keeper 0 and the weak keeper 1 of STAHL-B (Fig. 5) keep these different values. The SA selects the desired value stored in these two weak keepers to output from the scan cell flexibly.

When SE = 1 and SA = 1, the scan cell operates in shift mode. Two STAHLs operate as two independent flip-flops (logic-side flip-flop and scan-side flip-flop) and can store two values simultaneously. The logic-side flip-flop D0 - Q0 is connected to D and Q of the scan cell. The scan-side flip-flop D1 - Q1 is connected to the SI (scan-in) and SO (scan-out) of the scan cell. Since both flip-flops operate independently, the combinational portion of the design continues to operate just as in functional mode while test data is shifted from SI to SO.

When SE = 0 and SA = 0, the scan cell operates in functional mode. The STAHL-A and the STAHL-B are hardened against SEUs. The input D is applied to inputs D0 and D1 of the STAHL-A. The output Q of the scan cell is connected to node Q1 of the STAHL-B.

When SE = 0 and SA = 1, the scan cell operates in functional mode too. Different from the case of SE = 0 and SA = 0, the output Q of the scan cell is connected to the node Q0 of the STAHL-B instead of its Q1 node. With this setting, we can test the logic-side flip-flop. The detailed operation is shown in Sect. 5.5.

Figure 8 shows an example of an STAHL-based scan chain with three scan cells. All connections between the scan cells are the same as traditional scan design except for an additional control signal SA. The behavior of the STAHL-based scan chain is more similar to an enhanced scan approach [30], [31] than to a standard scan design. A standard scan design only stores one logic value in shift mode. The proposed STAHL-based scan design has two storage elements (a logic-side flip-flop and a scan-side flip-flop) to store two logic values simultaneously in shift mode just like an enhanced design.

5.2 Test Procedure Flow

The overall test procedure flow of an STAHL-based scan chain is shown in Fig. 9 with three phases: Phase-A, Phase-B, and Phase-C. Flush tests are applied to test for defects in the scan-side flip-flops in Phase-A. In Phase-B, a scan-side capture is applied to test for defects in the combinational portion. In Phase-C, a logic-side capture is applied to test for defects in the logic-side flip-flops. We use the combinational portion to test the logic-side flip-flops. Therefore, the scan-side capture in Phase-B is before the logic-side capture in Phase-C.

In this paper, the testing target is the STAHL-based scan cell. We aim to prove that the STAHL-based scan cell can be used to perform a scan test and can achieve a good test quality for the scan chain itself. Thus, we use inverters to build the combinational portion to make the test procedure easy to understand. The combinational portion receives data from the outputs of the scan cells and inverts the data. We take Scan Cell 2 in Fig. 8 as an example to explain the details of the test procedure.

5.3 Phase-A: Flush Test

During a flush test (SE = 1 and SA = 1), test data can be shifted from S-IN to S-OUT via the scan-side flip-flops (Fig. 8) in each scan cell. By controlling the shifted-in test vectors at S-IN and observing the test responses at S-OUT, defects in the scan-side flip-flops can be tested.

Figure 10 shows an example that 5 bits (FaFbFcFdFe =

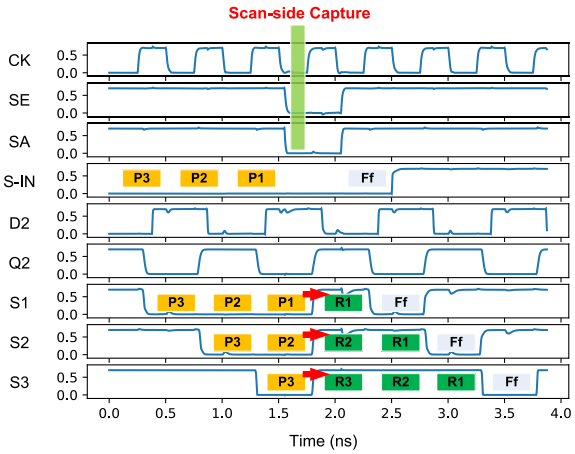


Fig. 11 SE = 0 and SA = 0: the next rising clock captures R1R2R3 = 111 (test response of the pattern P1P2P3 = 000).

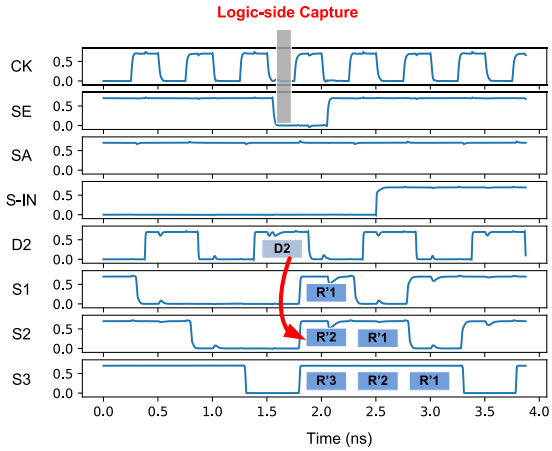


Fig. 12 SE = 0 and SA = 1: the next rising clock captures D2 = 1 (test response to the value stored in the logic-side flip-flop of Scan Cell 2).

01100) [20] are shifted through the scan-side flip-flops. With each clock cycle, the device under test (DUT) executes functional clock cycles via the logic-side flip-flops in each scan cell and the combinational portion. The data from the combinational portion will propagate via the inputs (D1, D2, and D3) of these logic-side flip-flops through their outputs (Q1, Q2, and Q3) back into the combinational portion. This is different from an enhanced scan [30], [31], where the inputs to the combinational parts of the design are held stable during shifting. The reason of having the DUT execute functional clock cycles in shift mode is to increase the defect coverage of the flush test. Loading different value combinations into logic-side flip-flops and scan-side flip-flops allows the detection of short defects between them. As shown in Fig. 10, S1 (input of the Scan Cell 2 in Fig. 8) receives a pattern of FaFbFcFdFe = 01100, while D2 (the other input of Scan Cell 2) receives a pattern of "10101". This pattern will be different for the combinational portion of a real circuit. For a real circuit, the generated pseudo-random patterns contain logic "1" and "0" combinations. We assume these patterns are still working for the flush test.

5.4 Phase-B: Scan-Side Capture

A series of scan-side capture operations (SE = 0 and SA = 0) are used to test the combinational portion. When a test pattern is completely shifted in, the SA signal and the SE signal are set to 0 in preparation for the capture operation. With the falling edge of SA, the output Q of each scan cell switches to the values of the shifted-in test pattern. With the falling of SE, each scan cell switches to functional mode. The shifted-in test pattern propagates through the combinational portion and generates corresponding test responses. These test responses from the combinational portion will be captured with the next clock CK.

The example is shown in Fig. 11. The test pattern P1P2P3 = 000 is present at the outputs of the scan cells at the falling edge of SA. The pattern starts to propagate through the combinational portion of the DUT and arrives at the inputs of the scan cells. Before the next rising clock, SE is already set to 0 to capture the test response (R1R2R3 = 111).

With the falling edge of SE, STAHLs switch from shift mode to functional mode. The logic-side flip-flop and the scan-side flip-flop are combined to form a single hardened flip-flop. If the logic-side flip-flop and the scan-side flip-flop of a scan cell held different values before, the C-elements in STAHL-B stop driving the outputs when SE is changed to 0 (functional mode). However, as mentioned previously, this will not cause a problem because the weak keeper 1 (shown in Fig. 5) at the node Q1 of STAHL-B will keep the logic value.

5.5 Phase-C: Logic-Side Capture

The values in the logic-side flip-flops are not observable directly. To test for defects in the logic-side flip-flops, we introduce a logic-side capture cycle. By capturing and observing the corresponding responses to the values stored in the logic-side flip-flops, we can test them.

For the logic-side capture, SA remains at 1 and the output of the scan cell connects to the Q0 of the STAHL-B. SE is set to 0 in preparation for the capture operation. Before the logic-side capture cycle, the combinational portion generates the responses to the values currently stored in the logic-side flip-flops of the scan cells. The logic-side capture cycle will capture these responses with the rising edge of the CK while SE = 0.

The logic-side capture example is shown in Fig. 12. The logic value at D2 is 1 and is captured at S2 (R'2 = 1). It is the same for D1 and D3 in Fig. 8. So, we have the test response (R'1R'2R'3 = 111).

5.6 Full Test Procedure

Figure 13 shows an example of a full test procedure containing three phases to completely test the scan chain. As mentioned above, we use inverters to build the combinational

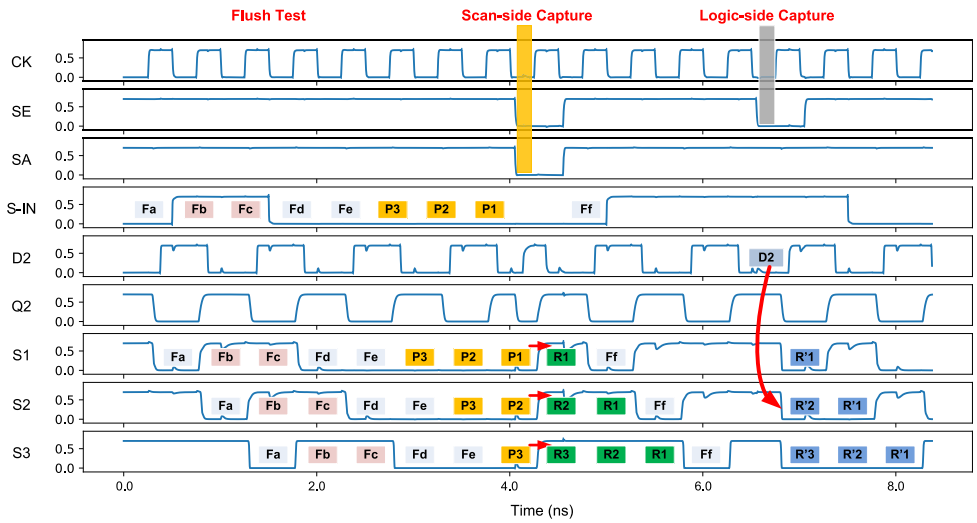


Fig. 13 Test procedure of the STAHL-based scan chain.

portion to make the test procedure easy to understand. With each consecutive clock cycle after capture, the combinational portion will continue to execute functional clock cycles based on the last test pattern. This can be seen in the waveform for D2, which continues to oscillate between 0 and 1 regardless of the test data loaded in the scan chain.

The test starts with applying 5 bits (FaFbFcFdFe = 01100) that are shifted through the scan chain in a flush test. This allows testing for defects in the scan-side flip-flops of the scan chain. Next, a test pattern (P1P2P3 = 000) is loaded into the scan chain and the scan-side capture is executed. The test response (R1R2R3 = 111) is captured. Third, a logic-side capture is applied to capture the corresponding data D2 = 0 at 6.9ns to load the current output of the combinational portion into the scan chain (R'1R'2R'3 = 000).

6. Experimental Results

The proposed latch was simulated using the 16nm predictive technology model [28] with a 0.7 V supply voltage and a clock frequency of 2GHz at room temperature. Transistors aspect ratios were set as follows: W/L = 1 for both PMOS and NMOS transistors in inverters I0, I3, two weak keepers, and transmission gates TG2, TG3, TG4, and TG5. W/L = 4 for the PMOS transistors and W/L = 2 for the NMOS transistors in inverters I1, I2, CE0, and CE1 as well as transmission gates TG0 and TG1. For a fair comparison, the minimum possible transistor sizes for making the latches work properly were applied [14] in the SPICE simulation.

6.1 Basic Statistics of Latch Cells

Table 1 shows the basic statistics of all considered latches. The columns show the name of the latches, the number of their transistors, D - Q delay, CK - Q delay, an average of the D - Q delay and the CK - Q delay, power consumption, and power-delay (average delay) product (PDP), respectively.

The D - Q delay is measured when the latch is transparent and is an average of the rising delay (time between a rising edge of D and the corresponding Q at a half supply voltage) and the falling delay (time between a falling edge of D and the corresponding Q at a half supply voltage). Usually, the input D is already stable before the next clock edge in a capture operation. The D - Q delay in the transparent phase cannot show the delay between the arriving time of the clock edge and the corresponding output Q. Hence, we add this CK - Q delay to measure the delay between the clock CK and its corresponding output Q at a half voltage. For power consumption, static power and dynamic power are both considered by assuming an input pattern of "00110011...".

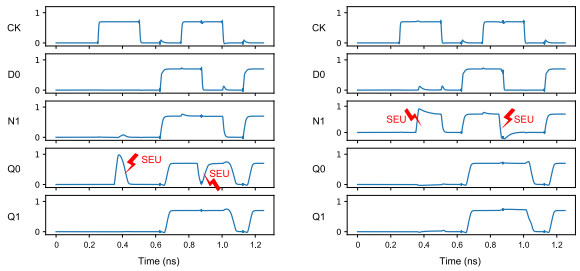
The standard latch is an unhardened latch used as the baseline, which has the lowest transistor numbers and power consumption. TMR consists of 3 standard latches and a voter and has the highest power consumption. The remaining 5 latches are hardened latches and the last one is the STAHL. The proposed STAHL has lower D - Q delay, CK - Q delay, and power consumption than TMR and FERST [13]. Other hardened latches show faster operation, less area, and lower power consumption than the STAHL. This is to be expected since the STAHL's primary design goal is related to testability rather than maximum speed or minimum power consumption. The advantages of the STAHL regarding defect coverage and *PTVF* are shown in the subsections below.

6.2 Hardness Against Soft-Errors

The hardness of a hardened latch is determined by the number of its sensitive nodes, the critical charge of these nodes, and the impact of SEUs at these nodes on the output of the latch. A node is the drain of a transistor in a latch. The critical charge is the minimum charge that must be collected at a node to lead to an SEU. According to the SEU's

Table 1 Basic statistics of latch cells

Latch	#Transistor	D - Q Delay (ps)	CK - Q Delay (ps)	Average Delay (ps)	Power (μw)	PDP ($10^{-18}J$)
Standard	12	15.54	10.33	12.94	0.09	1.16
TMR	48	34.90	40.31	37.61	0.61	22.94
FERST [13]	28	63.16	76.93	70.05	0.58	40.63
HLR [14]	24	4.91	6.94	5.93	0.10	0.59
HLR-CG2 [14]	24	4.81	6.34	5.58	0.11	0.61
ISEHL [15]	24	9.65	12.91	11.28	0.33	3.72
HiPeR [16]	18	9.27	12.07	10.67	0.24	2.56
STAHL	40	33.57	37.23	35.40	0.41	14.51



(a) An SEU at node Q0. (b) An SEU at node N1.

Fig. 14 Impact of SEUs on internal nodes.

impact on the output values, the internal sensitive nodes can be classified into three types [16]:

Type-1: A particle strike only generates an SEU on the same node without propagating to any output, regardless of the energy of the striking particle. The critical charge of such a node is commonly set to infinity: $Q_{crit} \rightarrow \infty$.

Type-2: A particle strike generates an SEU that may propagate to an output, whose correct value is restored within a time interval. Even though the correct value of the output of a latch is recovered, the wrong logic value generated at the output may propagate through the downstream logic and cause a wrong operation. The critical charge of Type-2 nodes is measured by calculating the amount of injected charge that leads to a voltage pulse equal to half of the supply voltage at the output. The greater the amount of critical charge, the more robust the sensitive node is.

Type-3: A particle strike generates an SEU that propagates to the output of the latch and cannot be restored. This type of node is the most critical one since a continuously erroneous output is generated. The measurement of the critical charge of this node is the same as for the Type-2 node.

A double exponential sharp pulse current was applied to simulate the particle striking caused SEUs and to calculate the critical charge [16], [31], [32].

$$I(t) = \frac{Q}{\tau_\alpha - \tau_\beta}\left(e^{-t/\tau_\alpha} - e^{-t/\tau_\beta}\right) \quad (4)$$

In Eq. (4), $I(t)$ denotes transient current pulse; Q denotes the total deposited charge; τ_α denotes collection time constant; τ_β denotes ion track establishment constant. The parameters τ_α and τ_β depend on the technology [29]. In this simulation, we use the values of $\tau_\alpha = 20ps$ and $\tau_\beta = 5ps$ [32].

As shown in Fig. 14 (a), SEUs were injected into the node Q0 of the STAHL. The logic value of Q0 was temporally changed. The correct logic value was recovered within a time interval. As shown in Fig. 14 (b), SEUs were injected into the internal node N1 of the STAHL. The logic value of N1 is changed. The SEUs at node N1 will not propagate to outputs Q0 and Q1. The Q0 and Q1 remain correct.

Table 2 Soft-error hardness of latch cells

Latch	*SEV*(%)	#Node	#Type-1	#Type-2	#Type-3	*Qcrit* (fC)
Standard	60.0	5	0	2	3	0.3
TMR	0.0	15	14	1	0	0.3
FERST [13]	0.0	14	12	2	0	0.7
HLR [14]	0.0	13	12	1	0	0.5
HLR-CG2 [14]	0.0	16	15	1	0	0.5
ISEHL [15]	0.0	15	14	1	0	0.5
HiPeR [16]	0.0	9	8	1	0	0.4
STAHL	0.0	16	12	4	0	0.8

Table 2 shows the results of soft-error vulnerability (*SEV*) of all considered latches, count of internal nodes, count of Type-1, count of Type-2, count of Type-3, and the critical charge Q_{crit}, respectively. The standard latch shows a *SEV* of 60% because it is an unhardened latch and has 3 Type-3 nodes of all 5 nodes. All hardened latches, including the STAHL, can tolerate SEUs (thus $SEV = 0$) if they are defect-free. For the proposed STAHL, there are 12 Type-1 internal nodes. The critical charge was assumed to be infinity. None of the hardened latches have Type-3 nodes. Therefore, the critical charge of the Type-2 nodes of these hardened latches becomes an important metric for evaluating their hardness. There are 4 Type-2 internal nodes (N9, N10, Q0, and Q1). For such nodes, a critical charge of $Q_{crit} = 0.8$fC was estimated by SPICE simulation.

6.3 Defect Coverage and *PTVF* of Single Latches

This section compares the STAHL with state-of-the-art hardened latches in terms of defect coverage (*DC*) and Post-Test Vulnerability Factor (*PTVF*). A short defect in a latch may cause excessive power consumption that leads to supply voltage drop in a real chip. Two resistors of 10Ω [34] were inserted into the VDD and GND lines to model the behavior of the power distribution network (PDN) of a real chip to allow for a similar voltage drop in simulation as well. Most published hardened latch designs do not provide actual cell layouts. For a fair comparison, we used the worst-case defect model (every possible defect based on the latch structure) instead of layout-based defect models.

The set of targeted production defects include transistor open defects and short defects between internal nets in a latch. The resistance of an open defect is usually in the range of 1MΩ to 1GΩ [24], [25]. We choose to inject a resistance

of 1MΩ at the source of each transistor since an open defect with this value is the most difficult to detect. Since there are 40 transistors in the STAHL, 40 transistor open defects were considered. As for short defects, the set of nets were classified into external and internal ones. External nets are D, GND, VDD, CK, $\overline{\text{CK}}$, SE, and $\overline{\text{SE}}$, while internal nets are the remaining nets as shown in the STAHL structure in Fig. 4. Since a short defect between two external nets (e.g., VDD and GND) can always be detected, such shorts are excluded from consideration. A short defect was injected into the SPICE netlist with a resistor of 1Ω between two nets. According to the statistics in [24], short defects of 1Ω have the highest occurrence frequency.

The worst-case defect model was used for the proposed STAHL with a total of 271 assumed defects, including 40 transistor open defects and 231 net short defects. The other latches were simulated in the same way. Table 3 shows the name of considered latch cells, the number of their external nets, the number of their internal nets, the number of their production defects, their defect coverage (*DC*), and their *PTVF*, respectively.

A high *DC* is a desirable result, which means a good test quality. The standard latch has high defect coverage; however, it cannot tolerate SEUs. The other hardened latches show low defect coverage due to their cell-internal redundancy. The STAHL has the highest defect coverage among all latches.

Post-Test Vulnerability Factor (*PTVF*) is used to evaluate the soft-error vulnerability of test-escaped defective cells. A lower *PTVF* means that cells with undetected defects can tolerate SEUs to a higher degree. The standard latch shows the worst *PTVF* value because of its highest soft-error vulnerability. The STAHL has the best *PTVF* among all latches.

Table 3 Defect coverage (*DC*) and *PTVF* of latch cells

Latch	#extNet	#intNet	#Defect	*DC* (%)	*PTVF* (%)
Standard	5	5	42	83.3	54.2
TMR	5	15	211	25.1	20.3
FERST [13]	5	14	184	60.3	13.8
HLR [14]	5	13	162	45.6	23.8
HLR-CG2 [14]	5	16	219	39.7	11.7
ISEHL [15]	5	15	199	50.7	19.1
HiPeR [16]	5	9	94	31.9	28.6
STAHL	7	16	271	85.6	9.2

6.4 Overall Comparison

Figure 15 shows the overall comparison. The percentage of *PTVF* from 100% to 0% is shown in the X-axis. 100% of *PTVF* represents the worst value and 0% represents the best value. The critical charge (Q_{crit}) ranges from 0fC to 1fC in the Y-axis. A higher critical charge means that the Type-2 node is more robust. The Z-axis shows defect coverage (*DC*), which ranges from 0% to 100%. A higher *DC* value is a better result. The colored triangle shows the overall comparison result. We introduce a *DC*-*PTVF*-Q_{crit} product (*DPQP*) to quantify the comparison results. The Eq. (5) shows the *DPQP* equation.

$$DPQP = DC \cdot (1 - PTVF) \cdot Q_{crit} \tag{5}$$

Table 4 shows the *DPQP* of these latches. A higher *DPQP* value means a better comparison result. The TMR latch shows the lowest *DPQP* because of its lowest defect coverage. The other hardened latches have low *DPQP* because of their low defect coverage. The standard latch also shows a low *DPQP* because of its high *PTVF* value. The STAHL shows the highest *DPQP*, which shows that the STAHL has the best overall comparison result.

6.5 *DC* of Latch Based Scan Cells in Scan-Test

This experiment was conducted to demonstrate the testability of an STAHL-based scan cell in a scan test. A scan chain with three STAHL-based scan cells (see Fig. 8) was simulated in SPICE simulation.

All possible open defects and short defects between internal nets were injected one by one into the second scan cell (Scan Cell 2 in Fig. 8). This time, all internal defects within the complete scan cell were considered and not just the defects within a single latch. Otherwise, the defect model is the same as in the previous experiment. As mentioned in the Sect. 6.3, an open defect was modeled by a resistor of 1MΩ [24], [25] at the source of a transistor and a short defect was modeled by a resistor of 1Ω [24] between two nets.

For each defect, the test procedure of a scan chain in

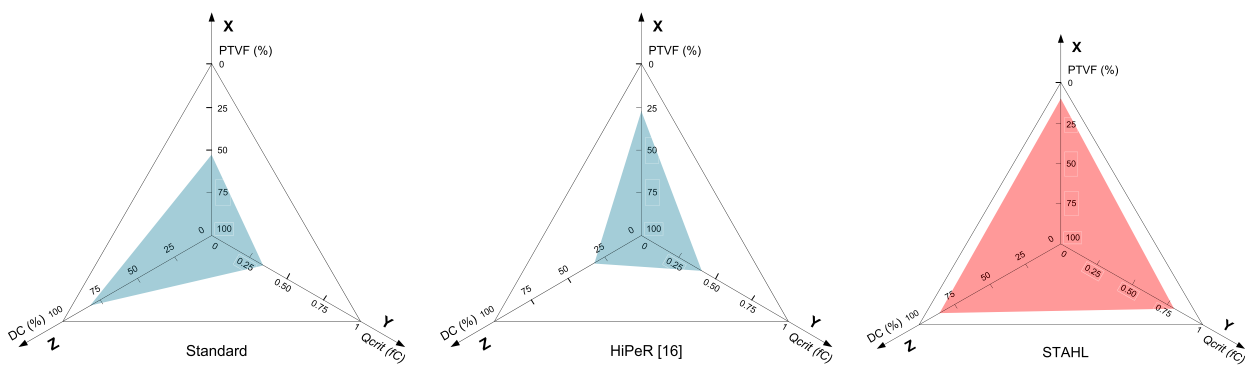


Fig. 15 Overall comparison of latch cells.

Table 4 Overall comparison results

Latch	$DPQP$ (10^{-3})
Standard	114
TMR	60
FERST [13]	364
HLR [14]	173
HLR-CG2 [14]	175
ISEHL [15]	205
HiPeR [16]	91
STAHL	622

Table 5 Defect coverage (DC) of scan cells

Scan Cell	#Defect	#Detected	#Undetected	DC (%)
Standard-based	244	185	59	75.8
TMR-based	902	287	615	31.8
FERST [13]-based	807	456	351	56.5
HLR [14]-based	724	300	424	41.4
HLR-CG2 [14]-based	961	346	615	36.0
ISEHL [15]-based	878	380	498	43.3
HiPeR [16]-based	452	216	236	47.8
STAHL-based	1227	957	270	78.0

Fig. 13 was executed and the scan-out signal was observed. For the STAHL-based scan chain, the test was considered to pass if all response bits from Fa to R'1 were correctly observed at S3. For scan chains based on other latches, only the bits from Fa to Ff were checked at S3. This is because these scan chains did not support the logic-side capture feature. We also test these latch based scan cells in their functional mode by setting the SE signal to 0 and checking their outputs.

Table 5 shows the test results for scan chains based on standard latches, TMR latches, other hardened latches, and the STAHLs.

The standard-latch-based scan cell shows a defect coverage of 75.8%. As expected, the defect coverage of the TMR-latch-based scan cell is the lowest (31.8%). The STAHL-based scan cell achieves a defect coverage of 78.0%, which is the best among all compared latch-based scan cells. Therefore, we can conclude that the STAHL-based scan cell provides significantly better testability than any other hardened latch.

7. Conclusions

This paper is the first that has analyzed the impact of production defects on the soft-error tolerability of hardened latches and has proposed a metric called Post-Test Vulnerability Factor (*PTVF*) to evaluate this impact. This paper has also proposed a novel Scan-Test-Aware Hardened Latch (STAHL) design that can tolerate SEUs and has high defect coverage. The proposed STAHL has two modes: functional and shift. In functional mode, it can tolerate SEUs. In shift mode, most cell-internal production defects become detectable. Simulation results have shown that its defect coverage is 85.6%, which is much higher than all compared hardened latch designs and its *PTVF* is 9.2%, which means that undetected defects in an STAHL have less impact on its soft-error tolerability.

Acknowledgments

This research was supported in part by NSFC-JSPS Exchange Program under Grant 62111540164 and JSPS Grant-in-Aid for Scientific Research (B) 21H03411.

References

[1] H. Cha and J. Patel, "A Logic-Level Model for α-Particle Hits in CMOS Circuits," Proc. IEEE Int'l Conf. on Computer Design, pp.538–542, Aug. 1993. DOI: 10.1109/ICCD.1993.393319

[2] B. Gill, N. Seifert, and V. Zia, "Comparison of Alpha-Particle and Neutron-Induced Combinational and Sequential Logic Error Rates at the 32-nm Technology Node," Proc. IEEE Int'l Reliab. Phy. Symp., pp.199–205, April 2009. DOI: 10.1109/IRPS.2009.5173251

[3] M. Hunger and S. Hellebrand, "The Impact of Manufacturing Defects on the Fault Tolerance of TMR-Systems," Proc. IEEE Int'l Symp. Defect and Fault Tolerance in VLSI Syst., pp.101–108, Oct. 2010. DOI: 10.1109/DFT.2010.19

[4] A. Yan, Y. Chen, Y. Hu, J. Zhou, T. Ni, J. Cui, P. Girard, and X. Wen, "Novel Speed-and-Power-Optimized SRAM Cell Designs with Enhanced Self-Recoverability from Single- and Double-Node Upsets," IEEE Trans. Circuits Syst., vol.67, no.12, pp.4684–4695, Dec. 2020. DOI: 10.1109/TCSI.2020.3018328

[5] R. Baumann, "Soft Errors in Advanced Computer Systems," IEEE Des. Test. Comput., vol.22, no.3, pp.258–266, May-June 2005. DOI: 10.1109/MDT.2005.69

[6] P. Dodd, M. Shaneyfelt, R. Flores, J. Schwank, T. Hill, D. McMorrow, G. Vizkelethy, S. Swanson, and S. Dalton, "Single-Event Upsets and Distributions in Radiation Hardened CMOS Flip-Flop Logic Chains," IEEE Trans. Nucl. Sci., vol.58, no.6, pp.2695–2701, Dec. 2011. DOI: 10.1109/TNS.2011.2169683

[7] S. Mitra, N. Seifert, M. Zhang, Q. Shi, and K.S. Kim, "Robust System Design with Built-in Soft-Error Resilience," IEEE Computer, vol.38, no.2, pp.43–52, Feb. 2005. DOI: 10.1109/MC.2005.70

[8] H. Zhang, H. Jiang, T. Assis, D. Ball, B. Narasimham, A. Anvar, L. Massengill, and B. Bhuva, "Angular Effects of Heavy-Ion Strikes on Single-Event Upset Response of Flip-Flop Designs in 16-nm Bulk FinFET Technology," IEEE Trans. Nucl. Sci., vol.64, no.1, pp.491–496, Jan. 2017. DOI: 10.1109/TNS.2016.2637876

[9] H. Zhang, H. Jiang, T. Assis, N. Mahatme, B. Narasimham, L. Massengill, B. Bhuva, S. Wen, and R. Wong, "Effects of Threshold Voltage Variations on Single-Event Upset Response of Sequential Circuits at Advanced Technology Nodes," IEEE Trans. Nucl. Sci., vol.64, no.1, pp.457–463, Jan. 2017. DOI: 10.1109/TNS.2016.2637873

[10] M. Nicolaidis, R. Perez, and D. Alexandrescu, "Low-Cost Highly-Robust Hardened Cells Using Blocking Feedback Transistors," Proc. IEEE VLSI Test Symp., pp.371–376, May 2008. DOI: 10.1109/VTS.2008.15

[11] T. Calin, M. Nicolaidis, and R. Velazco, "Upset Hardened Memory Design for Submicron CMOS Technology," IEEE Trans. Nucl. Sci., vol.43, no.6, pp.2874–2878, Dec. 1996. DOI: 10.1109/23.556880

[12] M. Omana, D. Rossi, and C. Metra, "Latch Susceptibility to Transient Faults and New Hardening Approach," IEEE Trans. Comput., vol.56, no.9, pp.1255–1268, Aug. 2007. DOI: 10.1109/TC.2007.1070

[13] M. Fazeli, S. Miremadi, A. Ejlali, and A. Patooghy, "Low Energy Single Event Upset / Single Event Transient-Tolerant Latch for Deep Submicron Technologies," IET Comput. Digit. Tech., vol.3, no.3, pp.289–303, May 2009. DOI: 10.1049/iet-cdt.2008.0099

[14] H. Nan and K. Choi, "High Performance, Low Cost, and Robust Soft Error Tolerant Latch Designs for Nanoscale CMOS Technology," IEEE Trans. Circuits Syst. I, Reg. Papers, vol.59, no.7, pp.1445–1457, July 2012. DOI: 10.1109/TCSI.2011.2177135

[15] H. Liang, Z. Wang, Z. Huang, and A. Yan, "Design of a Radiation Hardened Latch for Low-Power Circuits," Proc. IEEE Asian Test Symp., pp.19–24, Dec. 2014. DOI: 10.1109/ATS.2014.16
[16] M. Omana, D. Rossi, and C. Metra, "High-Performance Robust Latches," IEEE Trans. Comput., vol.59, no.11, pp.1455–1465, Nov. 2010. DOI: 10.1109/TC.2010.24
[17] J. Furuta, K. Kobayashi, and H. Onodera, "An Area/Delay Efficient Dual-Modular Flip-Flop with Higher SEU/SET Immunity," IEICE Trans. Electron., vol.E93-C, no.2, pp.340–346, March 2010. DOI:10.1587/transele.E93.C.340
[18] Y. Lu, F. Lombardi, S. Pontarelli, and M. Ottavi, "Design and Analysis of Single-Event Tolerant Slave Latches for Enhanced Scan Delay Testing," IEEE Trans. Device Mater. Rel., vol.14, no.1, pp.333–343, March 2014. DOI: 10.1109/TDMR.2013.2266543
[19] Y. Komatsu, Y. Arima, and K. Ishibashi, "Soft Error Hardened Latch Scheme with Forward Body Bias in a 90-nm Technology and Beyond," IEICE Trans. Electron., vol.E89-C, no.3, pp.384–391, March 2006. DOI: 10.1093/ietele/e89-c.3.384
[20] L. Wang, C. Wu, and X. Wen, "VLSI Test Principles and Architectures," Morgan Kaufmann, San Francisco, July 2006.
[21] S. Holst, R. Ma, and X. Wen, "The Impact of Production Defects on the Soft-Error Tolerance of Hardened Latches," Proc. IEEE Euro. Test Symp., Paper 7A-1, May 2018. DOI: 10.1109/ETS.2018.8400694
[22] A. Yan, Y. Hu, J. Cui, Z. Chen, Z. Huang, T. Ni, P. Girard, and X. Wen, "Information Assurance Through Redundant Design: A Novel TNU Error-Resilient Latch for Harsh Radiation Environment," IEEE Trans. Comput., vol.69, no.6, pp.789–799, June 2020. DOI: 10.1109/TC.2020.2966200
[23] A. Jee and F. Ferguson, "Carafe: An Inductive Fault Analysis Tool for CMOS VLSI Circuits," Proc. IEEE VLSI Test Symp., pp.92–98, April 1993. DOI: 10.1109/VTEST.1993.313302
[24] F. Hapke, W. Redemund, J. Schloeffel, R. Krenz-Baath, A. Glowatz, M. Wittke, H. Hashempour, and S. Eichenberger, "Defect-Oriented Cell-Internal Testing," Proc. IEEE Int'l Test Conf., pp.285–294, Nov. 2010. DOI: 10.1109/TEST.2010.5699229
[25] V. Sar-Dessai and D. Walker, "Resistive Bridge Fault Modeling, Simulation and Test Generation," Proc. IEEE Int'l Test Conf., pp.596–605, Sept. 1999. DOI: 10.1109/TEST.1999.805784
[26] S. Eichenberger, J. Geuzebroek, C. Hora, B. Kruseman, and A. Majhi, "Towards A World Without Test Escapes: the Use of Volume Diagnosis to Improve Test Quality," Proc. IEEE Int'l Test Conf., Paper 21-1, Oct. 2008. DOI: 10.1109/TEST.2008.4700604
[27] M. Zhang and N. Shanbhag, "Soft-Error-Rate-Analysis (SERA) Methodology," IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol.25, no.10, pp.2140–2155, Oct. 2006. DOI: 10.1109/ICCAD.2004.1382553
[28] Predictive Technology Model for Spice, [Online]. http://ptm.asu.edu/
[29] C. Qi, L. Xiao, J. Guo, and T. Wang, "Low Cost and Highly Reliable Radiation Hardened Latch Design in 65 nm CMOS Technology," Microelectronics Reliab., vol.55, no.6, pp.863–872, May 2015. DOI: 10.1016/j.microrel.2015.03.014
[30] A. Goel, S. Bhunia, H. Mahmoodi, and K. Roy, "Low-Overhead Design of Soft-Error-Tolerant Scan Flip-Flops with Enhanced-Scan Capability," Proc. IEEE Asia and South Pacific Design Automation Conf., pp.665–670, Jan. 2006. DOI: 10.1109/ASPDAC.2006.1594762
[31] K. Namba, T. Ikeda, and H. Ito, "Construction of SEU Tolerant Flip-Flops Allowing Enhanced Scan Delay Fault Testing," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol.18, no.9, pp.1265–1276, Sept. 2010. DOI: 10.1109/TVLSI.2009.2022083
[32] T. Heijmen, D. Giot, and P. Roche, "Factors That Impact the Critical Charge of Memory Elements," Proc. IEEE Int'l On-Line Testing Symp., Paper 3-2, July 2006. DOI: 10.1109/IOLTS.2006.35
[33] R. Ma, S. Holst, X. Wen, A. Yan, and H. Xu, "STAHL: A Novel Scan-Test-Aware Hardened Latch Design," Proc. IEEE Euro. Test Symp., Paper 4B-2, May 2019. DOI: 10.1109/ETS.2019.8791544
[34] R. Helinski and J. Plusquellic, "Measuring Power Distribution System Resistance Variations," IEEE Trans. Semicond. Manuf., vol.21, no.3, pp.444–453, Aug. 2008. DOI: 10.1109/TSM.2008.2001222

Ruijun Ma received an M.E. degree in Electric Engineering from Anhui University of Science and Technology, China, in 2017. He is currently pursuing a Ph.D. degree in the Department of Creative Informatics at Kyushu Institute of Technology, Japan. His research interests include soft-error tolerance and design-for-test.

Stefan Holst received his PhD in 2012 from University of Stuttgart (Germany). In 2013, he joined Kyushu Institute of Technology (Japan) where he is now an associate professor in the Department of Computer Science and Networks. He published about 50 works in journals, at international conferences, and peer-reviewed workshops and received two best paper awards (ETS2007, ATS2015). His research interests include reliability of AI hardware, VLSI simulation and diagnosis, soft-error tolerance as well as power-aware test.

Xiaoqing Wen received a Ph.D. degree from Osaka University, Japan, in 1993. He was an Assistant Professor with Akita University, Japan, from 1993 to 1997, and a Visiting Researcher with the University of Wisconsin–Madison, USA, from Oct. 1995 to Mar. 1996. He joined SynTest Technologies Inc., USA, in 1998, and served as its Vice President and Chief Technology Officer until 2003. He joined Kyushu Institute of Technology, Japan, in 2003, where he is currently a Professor of the Department of Computer Science and Networks. He is a Co-Founder and Co-Chair of Technical Activity Committee on Power-Aware Testing under Test Technology Technical Council (TTTC) of IEEE Computer Society. He served as an Associate Editor for IEEE Transactions on Computer-Aided Design (TCAD) and is currently serving as an Associate Editor for IEEE Transactions on Very Large Scale Integration Systems (TVLSI). He co-authored and co-edited two popular books, VLSI Test Principles and Architectures: Design for Testability (2006) and Power-Aware Testing and Test Strategies for Low Power Devices (2009). His research interests include design, test, and diagnosis of VLSI circuits. He published more than 200 peer-reviewed papers and conducted 19 tutorials on low-power VLSI testing. He holds 43 U.S. Patents and 14 Japan Patents. He received the 2008 Society Best Paper Award from the Information Systems Society (ISS) of the Institute of Electronics, Information and Communication Engineers (IEICE). He is a Fellow of IEEE, a Senior Member of Information Processing Society of Japan (IPSJ), and a Senior Member of IEICE.

Aibin Yan received a Ph.D. degree in Computer Application Technology from Hefei University of Technology, China. He joined Anhui University, Hefei, in 2016. From 2018 to 2019, he visited the WEN Lab, Kyushu Institute of Technology, Japan, under the support of China Scholarship Council (CSC), and under the supervision of Prof. Xiaoqing WEN, an IEEE Fellow, for one year time. Currently, he is an associate professor at Anhui University. He has published about 50 papers including IEEE TC, IEEE TCASI, IEEE TCASII, IEEE TETC, IEEE TAES, IEEE TRel, IEEE TVLSI, etc. His research interests mainly include radiation hardening by design for nano-scale CMOS ICs such as latches, flip-flops, and memory cells.

Hui Xu received a Ph.D. degree from School of Computer and Information Engineering, Hefei University of Technology, China, in 2013. He is currently working as an associate professor of the College of Computer Science and Engineering, Anhui University of Science and Technology. From 2017 to 2018, he was a visiting scholar at the Computer Science Department of the University of Texas at Austin, USA. His current research interests include VLSI design and testing, reliable systems, and artificial intelligence.