Defects in Hardened Latches: Analysis, Detection and Evaluation

著者	Ma Ruijun
その他のタイトル	耐ソフトエラーラッチにおける欠陥の分析、検出及び評価に関する研究
学位授与年度	令和4年度
学位授与番号	17104甲情工第371号
URL	http://doi.org/10.18997/00009010

Defects in Hardened Latches: Analysis, Detection and Evaluation

(耐ソフトエラーラッチにおける欠陥の分析、検出及び評価に関する研究)

MA RUIJUN

Abstract

The development of modern integrated circuits (ICs) has greatly changed the life of humankind. Nowadays, ICs are also indispensable to mission-critical applications, such as medical devices, autonomous cars, aircraft navigating systems, and satellites. The reliability of these mission-critical applications is a major concern.

A soft-error occurring in an IC is a severe threat to its reliability, especially for mission-critical applications. The continuous trend of shrinking technology feature sizes makes modern ICs more and more vulnerable to soft-errors. Soft-errors are caused by radiation particles striking an IC and generating current pulses to disturb its functionality. A soft-error can cause data corruption and may eventually lead to system failures. If a soft-error occurs in an operational medical device during surgery, it may cause a malfunction of this device and interrupt the surgery process. A soft-error may change the control data of an autonomous car, which may lead to an accident. A soft-error may corrupt the aircraft navigating systems. No one would take the chance to let it happen even though malfunctions caused by soft-errors can be solved by resetting these devices. Because reset takes time and severe results may happen during the resetting. If a soft-error causes a malfunction in the control system of a satellite, it may not be able to maintain its height and eventually burn up as it falls into the Earth's atmosphere. Hence, it is important to protect ICs from soft-errors.

Many soft-error tolerance methods have been proposed to protect ICs against soft-errors. In an IC, memory elements and storage elements (e.g., latches and flip-flops) are the most vulnerable to soft-errors, and data stored in them are crucial to the operation of a circuit. Error correction codes (ECCs) can be used to protect memories. Register-level soft-error tolerance methods can be used to detect soft-errors in latches by using parity-checking and correct them by resetting. Hardened designs protect latches against soft-errors by using redundant feedback loops to store the same input data and using a voter to select the correct output. The advantage of using hardened designs is that they can prevent soft-errors from reaching outputs while ECCs and register-level soft-error tolerance methods must detect soft-errors and then correct them by restoring the data. For protecting storage elements in mission-critical applications, hardened latch design is the best option because it has high reliability and can save the resetting time. Many state-of-the-art hardened latch designs have been proposed to tolerate soft-errors and they are believed to have good soft-error tolerability.

Defects (physical flaws due to imperfect production (production defects) and physical changes caused by aging effects after a long operation time (aging-related defects)) can also cause a malfunction of a circuit and cause a system failure eventually. Different from the temporal state change of a circuit caused by soft-errors, defects are permanent damages to a circuit and can disturb the behavior of a circuit from its desired manner. Defects in storage elements should be detected to make sure a system/device

operating correctly and stably. Scan test is a commonly used defect detection method, which connects reconfigured storage elements to form a shift register with external access and the internal states of these storage elements can be easily controlled and checked.

However, the impact of defects on existing state-of-the-art hardened latch design has not been considered. This impact requires consideration because added redundancy in hardened latch designs can not only mask soft-errors but also mask the effects of defects and it can lead to two serious problems:

Problem-1 (Low Testability)： Production defects in hardened latch designs are difficult to detect with conventional scan tests, in which the observability (an important metric to evaluate a circuit's testability) of defects in hardened latch designs can be greatly reduced. Therefore, existing state-of-the-art hardened latches have low observability and thus low testability. Furthermore, defects that escaped the production test (undetected defects) may become more and more serious and cause a system failure eventually.

Problem-2 (Low Soft-Error Tolerability)： Undetected defects and aging-related defects can make hardened latch designs vulnerable to soft-errors while defect-free ones do not. The soft-error tolerability of hardened latch designs may be compromised by undetected defects or aging-related defects.

This research is the first to consider **Problem-1** of low testability of hardened latches and **Problem-2** of defects reducing the reliability of hardened latches. Furthermore, this research is the first to propose a comprehensive solution to solve these two problems with the following five major contributions:

Contribution-1: A first-of-its-kind metric for quantifying the impact of defects on hardened latches, called Post-Test Vulnerability Factor (*PTVF*). It is used to analyze the residual soft-error tolerability of hardened latches after testing. **Problem-2** is solved by this first major contribution.

Contribution-2: A novel design called Scan-Test-Aware Hardened Latch (STAHL) that provides the highest defect coverage in comparison with all existing hardened latches. **Problem-1** is solved by using STAHL to build a scan cell to perform a scan test.

Contribution-3: A novel scan test procedure is proposed to solve **Problem-1** by fully testing the STAHL-based scan cell.

Contribution-4: A novel High-Performance Scan-Test-Aware Hardened Latch (HP-STAHL) design can also solve **Problem-1** and has similar defect coverage as STAHL but has lower power consumption and higher propagation speed.

Contribution-5: A novel scan test procedure is proposed to fully test the HP-STAHL-based scan cell to solve **Problem-1**.

Comprehensive simulation results demonstrate the accuracy of the *PTVF* metric

and the effectiveness of the STAHL-based scan test and HP-STAHL-based scan test. As the first comprehensive study bridging the gap between hardened latch designs and IC testing, the findings of this research are expected to significantly improve the soft-error-related reliability of IC designs for mission-critical applications. Furthermore, the two proposed hardened latches and the scan test procedures can not only be used to detect defects after production but also can be applied to detect aging-related defects in the field through performing built-in self-test (BIST).

In Chapter 1, an example is introduced to indicate **Problem-1** and **Problem-2**. Chapter 2 shows the background information of soft-errors and defects. Chapter 3 shows some typical soft-error mitigation methods and details of a scan test. Chapter 4 describes the detailed information of *PTVF* (**Contribution-1**). Chapter 5 shows the structure of STAHL (**Contribution-2**) and Chapter 6 shows the scan test procedure of testing the STAHL-based scan cell (**Contribution-3**). Chapter 7 shows the structure of HP-STAHL (**Contribution-4**) and Chapter 8 shows the scan test procedure of testing the HP-STAHL-based scan cell (**Contribution-5**). Chapter 9 shows the experimental results of comparing STAHL and HP-STAHL with state-of-the-art hardened latch designs. Chapter 10 concludes this thesis.

Contents

List of Tables

List of Figures

Abbreviations

IC	Integrated Circuit
CUT	Circuit Under Test
DUT	Device Under Test
VLSI	Very-Large-Scale-Integration
LSI	Large-Scale-Integration
FinFET	Fin Field-Effect Transistor
MOSFET	Metal-Oxide-Semiconductor Field-Effect Transistor
GND	Ground
VDD	Supply Voltage
DICE	Dual Interlocked Storage Cell
TMR	Triple Modular Redundancy
SPICE	Simulation Program with Integrated Circuit Emphasis
FL	Feedback Loop
DFT	Design-for-Test
PTVF	Post-Test Vulnerability Factor
STAHL	Scan-Test-Aware Hardened Latch
HP-STAHL	High Performance Scan-Test-Aware Hardened Latch
SER	Soft-Error Rate
SEB	Single-Event Burnout
SEL	Single-Event Latchup
SET	Single-Event Transient
SEU	Single-Event Upset
DDD	Displacement Damage Dose effect
TID	Total Ionizing Dose effect
SNU	Single-Node Upset
MNU	Multiple-Node Upset
TVF	Timing Vulnerability Factor
AVF	Architectural Vulnerability Factor
SEV	Soft-Error Vulnerability

LELE	Litho-Etch-Litho-Etch
I_{DDQ}	Quiescent Power Supply Current
DC	Defect Coverage
ECC	Error Correction Code
NAND	Not-AND gate
XOR	Exclusive-OR gate
CE	C-Element
SE	Scan-Enable
SA	Scan-Apply
CK	Clock
SI	Scan-In
SO	Scan-Out
SRAM	Static Random-Access Memory
TG	Transmission Gate
MUX	Multiplexer
PDP	Power-Delay Product
DPQP	DC-PTVF-Q_{crit} Product
BIST	Built-In Self-Test

1. Introduction

1.1. Problem Statement

The shrinking of transistor feature sizes continues for decades since the famous Moore's Law was released [1]. A smaller feature size allows for manufacturing a smaller transistor as well as the integration of more transistors on a chip to achieve more functionalities. For a given wafer size, a smaller technology feature size means more chips can be manufactured on a wafer and IC foundries can earn more profits since the whole wafer is processed in the same steps.

A smaller technology feature size usually comes with a smaller supply voltage. Because of the reduction of geometry sizes, a smaller supply voltage is enough to drive the gate of a transistor to form a propagation channel between source and drain. Due to this supply voltage reduction, the amount of charge (critical charge) that defines the state of a storage element becomes smaller, making a storage element more and more vulnerable to soft-errors, which raises a great threat to the reliability of modern circuits.

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 [2-7]. 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]. A fin field-effect transistor (FinFET) shows lower sensitivity to radiation-induced soft-errors than a planer metal-oxide-semiconductor field-effect transistor (MOSFET) because of its smaller radiation-sensitive volumes at drain junctions [10]. However, a FinFET is still vulnerable to radiation-induced soft-errors [10, 11].

Soft-errors impact not only systems in high-radiation environments, such as aerospace [5, 6, 12], but also systems or devices at the sea-level [13, 14]. Normally, the magnetosphere of earth can prevent most outer space radiation particles since 92% of them are protons and 6% of them are alpha particles [26]. The magnetosphere can make almost all of them fall into the poles of the earth. However, the activity of the sun (such as sunspots and solar flares) can bring a large amount of high energetic and accelerated plasmas to change the magnetosphere. As a result, a large number of radiation particles can enter the atmosphere of the earth and have interactions with the atoms in the atmosphere to generate cascade particles. These entering particles and the following generated cascade particles may hit operating devices or systems on earth or satellites in low earth orbit (LEO) [5, 6]. With the reduction of technology feature sizes and supply voltages, these radiation particles can easily change the state of a circuit and interrupt its

functional working. If a soft-error causes a malfunction of an electronic device like a personal computer, this malfunction can be solved by resetting this device since a soft-error will not cause permanent damage. However, if a soft-error causes a malfunction of mission-critical applications (such as medical devices, autonomous cars, the navigating systems of aircraft, and satellites), it may lead to a catastrophic result. Hence, it is important to protect chips in mission-critical applications against the impact of soft-errors to maintain high reliability.

Many soft-error tolerance approaches have been proposed to protect circuits from the impact of soft-errors. Error correction codes (ECCs) can be used to protect memory cells (such as SRAM and DRAM) [50-51]. A register-level soft-error tolerance approach can be used to detect soft-errors in latches [60]. Hardened designs [15-25] can be used to protect storage elements (such as latches or flip-flops) by adding redundancy. This research focuses on using hardened latch designs to tolerate soft-errors for the following three reasons:

(1) Sequential elements, such as latches and flip-flops, are the most susceptible to soft-errors in logic circuits [7].

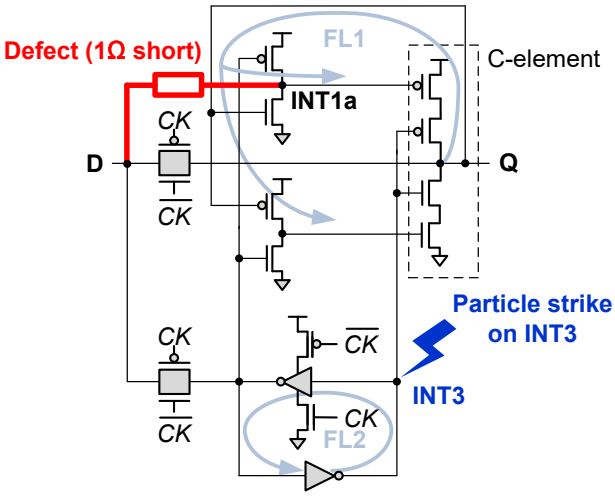
(2) A flip-flop is commonly constructed of two latches. Tolerating soft-errors in latches can reduce the soft-error vulnerability of flip-flops as well.

(3) Hardened latch design is an effective approach that can prevent soft-errors from reaching outputs by using redundant feedback loops to store the same input data and using a voter to select the correct output. Other existing soft-error tolerance methods must detect and then correct soft-errors while protecting sequential elements. For mission-critical applications, a hardened latch design is a good option to protect sequential elements while compared with other soft-error tolerance methods.

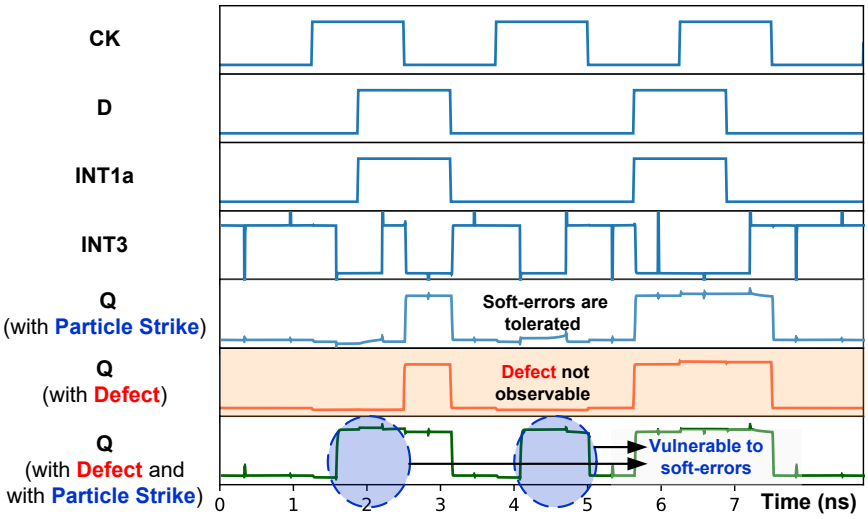
If a soft-error occurred in a latch and changes the internal state of this latch, this soft-error is called a single-event upset (SEU). To tolerate SEUs, many hardened latches [15-25] have been proposed by adding redundancy to their structures. The latch in [15] adds transistors at feedback loops to prevent SEUs from propagating. This latch has fewer transistors than most other hardened latches. The dual interlocked storage cell (DICE) [16] can tolerate soft-errors 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 [17-21] store logic values in multiple feedback loops and use a voter circuit (such as C-element) to select the correct output. The design in [22] can tolerate SEUs by its dual-modular structure. The design in [4] can be used to tolerate multiple-node upsets (MNUs). 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 low observability and thus low testability. Furthermore, undetected defects may become more and more serious and cause a system failure eventually.



(a) HiPeR [21] with a short defect



(b) SPICE simulation

Figure 1.1 The impact of defects.

Figure 1.1 illustrates this problem. Figure 1.1 (a) shows a typical hardened latch (HiPeR) [21], 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 Figure 1.1 (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): Undetected defects and aging-related defects can make hardened latch designs vulnerable to soft-errors while defect-free ones do not. If a defect exists in a hardened latch, the hardened latch's soft-error tolerability may be reduced, making it more vulnerable to SEUs.

Consider the hardened latch shown in Figure 1.1 (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 Figure 1.1 (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.

1.2. Research Objectives

This thesis focuses on improving the testability of hardened latch designs by addressing the above two problems (**Problem-1: Low Testability** and **Problem-2: Low Soft-Error Tolerability**) through the following five major contributions:

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

Contribution-2 (STAHL): To solve **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. **Problem-1** is solved by using STAHL to build a scan cell to perform a scan test.

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 to solve **Problem-1**.

Contribution-4 (HP-STAHL): To solve **Problem-1**, we also propose a novel High Performance Scan-Test-Aware Hardened Latch (HP-STAHL) design, which has similar defect coverage as the STAHL but costs lower power consumption and has a faster propagation speed by compromising part of its soft-error tolerability.

Contribution-5 (An HP-STAHL-based Scan Test): A novel scan test procedure is proposed to test HP-STAHLs to solve **Problem-1**.

1.3. Thesis Organization

The organization of this thesis is shown in Figure 1.2, which includes 10 chapters. The first chapter introduces the target problem and contributions of this research.

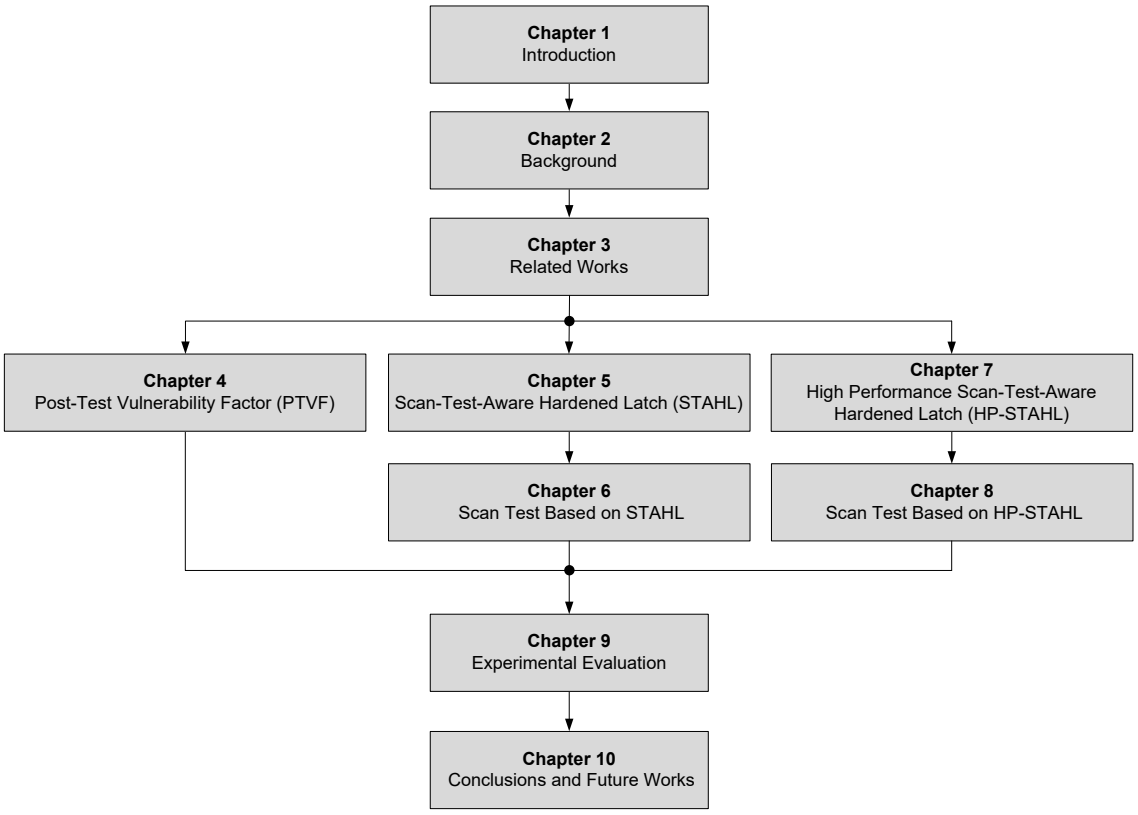


Figure 1.2 Thesis organization.

Chapter 2 describes the background of this research, such as soft-error, soft-error rate (SER), defects, fault models, and defect coverage. Chapter 3 describes the related works of soft-error mitigation and defect detection. The *PTVF* metric is introduced in Chapter 4 for evaluating the residual soft-error tolerability of hardened latch designs after manufacturing. The Scan-Test-Aware Hardened Latch (STAHL) design is described in Chapter 5, including its structure as well as its operation details in both shift and functional modes. Chapter 6 shows the scan chain structure based on STAHLs and a novel test procedure for fully testing the STAHLs. Chapter 7 shows the High Performance Scan-Test-Aware Hardened Latch (HP-STAHL) design along with its structure and operation details. The scan chain based on HP-STAHL and its test procedure is shown in Chapter 8. Chapter 9 shows evaluation results and Chapter 10 concludes this thesis.

1.4. Summary

This chapter introduces two problems that are caused by defects in hardened latches: **Problem-1: Low Testability** and **Problem-2: Low Soft-Error Tolerability**.

For solving these two problems, 5 major contributions are introduced in section 1.2. In **Contribution-1 (*PTVF*)**, This research is the first to find that defects can reduce the soft-error tolerability of hardened latch designs. A novel metric, called Post-Test Vulnerability Factor (*PTVF*), is proposed for quantifying the impact of defects on hardened latches. In **Contribution-2**, the first hardened latch design, Scan-Test-Aware Hardened Latch (STAHL), has high defect coverage and high soft-error tolerability. In **Contribution-3**, we propose a novel minimal-overhead scan design and a novel test procedure based on the STAHL-based scan chains to test STAHLs. In **Contribution-4**, a novel High Performance Scan-Test-Aware Hardened Latch (HP-STAHL) design is proposed. HP-STAHL has the same merits as STAHL but has lower power and delay. In **Contribution-5**, A novel scan test procedure is proposed to test HP-STAHLs.

Section 1.3 introduces the organization of this thesis.

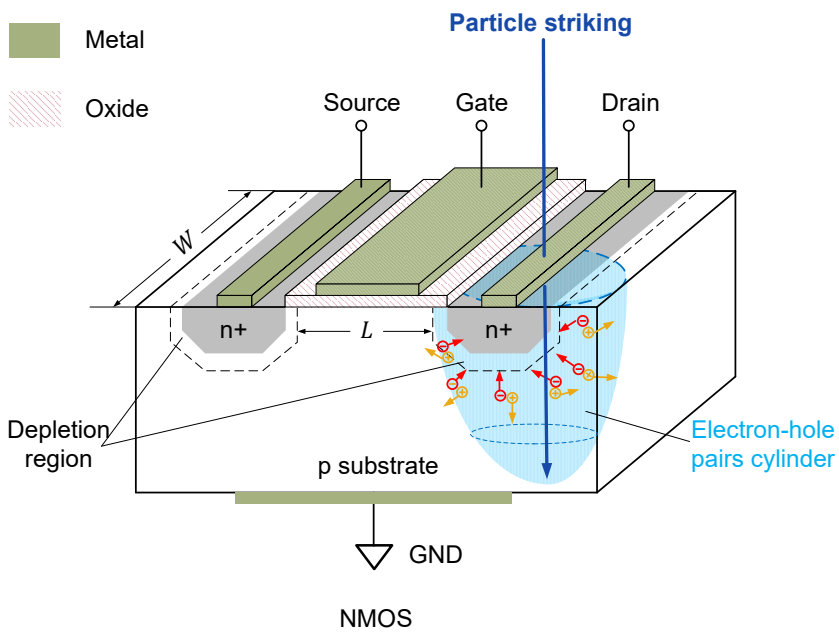
2. Background

2.1. Soft-Error

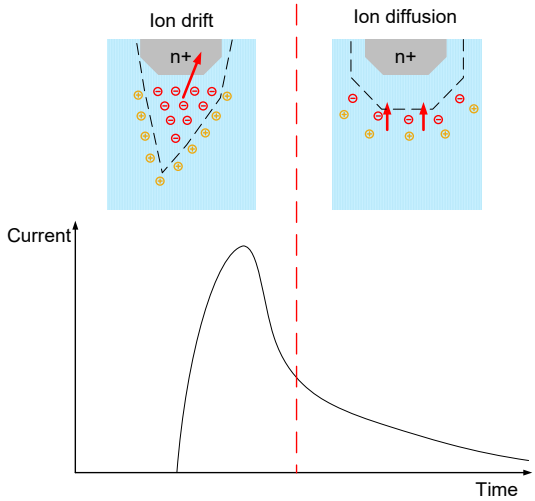
Soft-errors are caused by radiation particles striking ICs, which can temporally change the states of circuits but cause no physical damage. The following subsections show the basic knowledge of soft-errors.

2.1.1. Soft-Error Mechanism

A soft-error is caused by a particle striking an OFF transistor and generating a current pulse to disturb the output results. Figure 2.1 (a) shows an NMOS transistor with a particle striking on its drain side p-n junction. The p substrate of this NMOS connects with the ground (GND). When this NMOS is in an OFF state, there is no current from drain to source because there is no channel beneath the oxide. The electrical field in the two depletion regions can prevent electrons from free propagating. When a particle strikes on this NMOS, it generates a cylinder of electron-hole pairs in this drain side p-n junction along the striking track. These generated electrons can be accumulated by the electrical field to generate a current pulse at the drain. Generating a pair of electron-hole in bulk silicon requires energy of 3.6 eV (1 eV = 10^{-19}J) [47].



(a) Particle striking on an NMOS transistor.



(b) Particle striking generates a current pulse.

Figure 2.1 Soft-error mechanism.

Figure 2.1 (b) shows two phases of a particle striking: ion drift and ion diffusion. These generated electrons will be collected by the electrical field in the depletion region and then emerge from the drain to generate a current pulse. This is called ion drift and may last in the scale of picoseconds. Then, the electrical field in the drain side depletion region disappears when several electrons are collected. These residual ionized electrons and holes may temporally conduct the drain and GND, which features a temporary short between them. A diffusion process will follow the drift until all carriers diffuse away and the inner electrical field reestablish. This is called ion diffusion and it may last from a few picoseconds to hundreds of picoseconds [32].

This generated current pulse may disturb the state of a circuit to generate a soft-error [2]. If this soft-error changes the state of a latch during its latching phase, this latch will continue to output the corrupted data until a new datum arrives. Hence, it is very important to protect latches from the impact of soft-errors.

2.1.2. Sources of Radiation Particles

Radiation particles on the planet earth can be generally classified into two types: primary particles and secondary particles [26, 34]. Secondary particles are the major cause of soft-errors on earth or satellites in low earth orbit (LEO) [5-6] and are usually generated by the interaction between primary particles and the atoms (such as oxygen or nitrogen atoms) in the atmosphere.

One source of primary particles is galactic particles, which are generated by

supernova explosions, stellar flares, or pulsars in the galaxy. These generated high-energy particles can last about 200 million years and may enter the solar system and hit the earth during their life circle [26]. Another source of primary particles is the sun, which may enter an active period almost every 11 years. During an active period of the sun, solar flare creates high energetic and density solar particles, whose number is about two times its quiet period [26, 27]. Also, the high-energy solar wind may disturb the magnetosphere of the earth (which can deflect the outer-space particles) and increase the possibility of high energetic particles reaching the terrestrial.

The secondary particles are generated by the interaction of these primary particles and atoms in the atmosphere. When these primary particles escape from the magnetosphere of the earth and enter the atmosphere, they may hit the atmospheric atoms (such as oxygen or nitrogen atoms) to generate secondary particles, such as protons, alpha particles, neutrons, heavy ions, pions, muons, and so on [26]. These secondary particles are responsible for soft-errors in terrestrial devices and systems. Also, the radioactive isotope in the package and silicon wafer process materials may emit alpha particles and can cause soft-errors [28, 29]. However, these materials caused soft-errors can be solved by replacing them with low alpha materials [29].

2.1.3. Soft-Errors Induced Incidents

Soft-errors can cause serious consequences. In 2008, a soft-error occurred at the computer system of an Australian flight (Qantas flight 72). The soft-error corrupts the control data (angle of attack, AOA [66]) of the flight, which changes its gesture and made this flight abnormally pitched down two times during cruising over the Indian Ocean [35]. This incident caused more than 100 people (including passengers and crew members) injured because many of them had released their safety belts when this incident occurred. Due to this incident, European Aviation Safety Agency requires that aircraft computers should have the capability to tolerate soft-errors [36].

Another incident is the stuck accelerator pedals of Toyota cars in 2009 [37], which caused 89 people killed and 57 injured. According to the report [37], the suspect cause is that soft-errors occurred in the memories and caused a system malfunction.

In the study [79] reported in 1975, soft-errors changed the states of flip-flops of a satellite system and led to several anomalies.

In 2003, a soft-error in a voting machine adding 4096 extra votes to a candidate [38]. It is because all the votes are recorded by a binary number and a soft-error changes the 13th bit from 0 to 1, thus added $4096 = 2^{12}$ extra votes. Another interesting thing is that a soft-error in a video game helps the player directly skip to the next level [39]. As can be noticed that soft-errors can impact electronic devices on earth anywhere, anytime, these mission-critical applications should be protected against the impact of soft-errors.

2.1.4. Soft-Error Classification

Depending on the occurrence location of a soft-error in a circuit, it can be classified into single-event upset (SEU), which is occurred in a sequential circuit, and single-event transient (SET), which is occurred in a combinational circuit. An SEU can be divided into single-node upset (SNU) and multiple-node upset (MNU). If a particle striking only affects a p-n junction, it changes the logic value of a node. However, if a particle strikes multiple p-n junctions and may cause charge sharing, this particle striking changes the logic values of multiple nodes, thus flipping multiple bits. Due to the shrinking of technology sizes, MNUs are possible to occur in the storage elements. So far, there is no valid evidence to prove that MNUs may frequently occur in storage elements. On the contrary, the occurrence of SNUs can be proved by many valid data [61]. Therefore, tolerating SNUs in storage elements is more important than MNUs.

2.1.5. Soft-Error Rate (SER) Definition and Calculation

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 [63-65]. There are some SER calculation metrics for combinational logic and memories [40], as well as for latches [7, 30].

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 at a node of a latch results in erroneous output. In our previous research [41], 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: $\sum_{f \in F(c)} P_F(f)$. The particle set $F(c)$ and probabilities P_F are determined by the chosen soft-error model, e.g. [21]. 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.

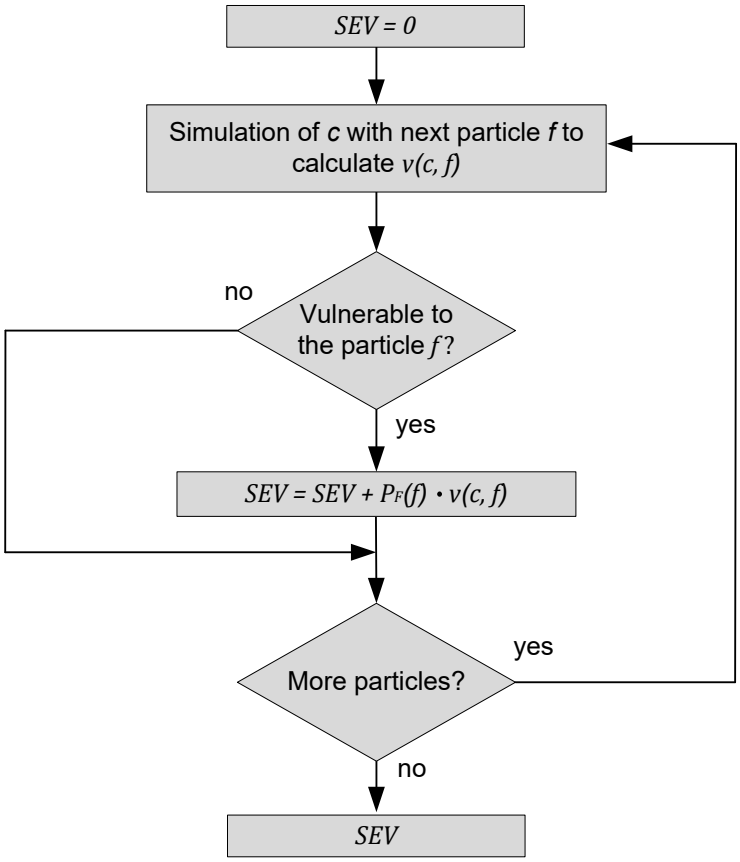


Figure 2.2 Soft-error vulnerability (SEV) calculation flow.

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:

$$SEV(c) = \sum_{f \in F(c)} P_F(f) \cdot v(c, f) \qquad (2.1)$$

The calculation flow of SEV is shown in Figure 2.2. After initialization of the variable $SEV = 0$ for accumulating the result, all particles $f \in F(c)$ are injected into the SPICE netlist of the cell c. For each particle f, $v(c, f)$ is calculated. If the cell c is vulnerable to a particle strike, $v(c, f)$ will be positive. SEV is increased by the combined probability of the particles occurring and the particle strike leading to an

erroneous output of the latch cell: $P_F(f) \cdot v(c, f)$.

These SER metrics are for the defect-free hardened latches. However, 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 defects on the soft-error vulnerability of these hardened latches.

2.2. Defect

Defects are physical flaws caused by imperfect production (production defects) and physical changes caused by aging effects (aging-related defects). High energy radiation particle striking can also cause physical damages of a circuit, which are radiation-induced defects. Defects may change the behavior of a circuit and make it deviate from its proper manner.

2.2.1. Production Defect

The manufacturing of chips contains a lot of repetitive physical and chemical process steps, including photoresist coating, lithography, etching, deposition, and ionization. An example of forming an n-well on p-type silicon (as shown in Figure 2.1 (a)) is introduced to show these processes. Some Group V dopants need to be doped into the exact location on the p-substrate to change it from p-type to n-type. Before defining the n-well location, a protective layer on the wafer is formed by a reaction with oxygen to form an oxide on its surface. Then, a photoresist coating will be spread on the oxide surface and the photoresist on the determined n-well location is then exposed to the ultraviolet light through a mask pattern. The area of photoresist exposed to the light becomes more soluble and can be easily removed to reveal the oxide. Hydrofluoric acid can be used to etch the oxide area and cause no damage to the photoresist protected area. Another acid called piranha acid is used to clean the residual photoresist and dopant ions are prepared to dope into the n-well location as well as the surface of the remaining oxide layer. The remaining oxide layer protects the p-substrate from the dopant ions. Finally, the hydrofluoric acid can be used to remove the oxide layer and the n-well is formed.

Manufacturing chips need repetitions of the above process to form transistors and metal layers. Any randomly occurred manufacturing imperfection (such as a weakly connected line bonding, impurities, improperly etched metal traces, shorts between lines or opens) or process variation (the channel length of a transistor, transistor threshold voltage, or metal line thickness and width) can cause a flaw on the chip, which may affect the behavior of a transistor, the conductivity of a metal line, or even worse a malfunction.

Along with the shrinking of the technology feature sizes, a lithography technology called multiple pattern technology helps to support 20nm and below. Multiple pattern technology is developed to enhance the resolution of lithography exposure [42]. The commonly used multiple pattern methods are litho-etch-litho-etch (LELE) process [43] and self-aligned double patterning (SADP) [44]. However, this technology increases the process steps as well as the risk of generating production defects.

2.2.2. Aging-Related Defect

Aging effects refer to the degradation of the parameters of ICs after a long time of stressful field operation. These parameter changes can affect the performance of ICs and cause permanent physical damage, called aging-related defects. Three typical aging effects may cause aging defects and they are electromigration (EM), negative bias temperature instability (NBTI), and hot carrier injection (HCI).

Electromigration (EM): It is a gradual movement of metal atoms pushed by the momentum of a high density of electrons. With the continuously shrinking of technology sizes, the risk of EM-caused ICs malfunction will increase because the density of both current and power increases [45]. EM can cause the movement of atoms in metal wire and cause two possible results. (1) It may make the wires thinner and eventually lead to open defects. (2) It may push atoms together to form a bumped knot, which may conduct with adjacent wires (short defects).

Negative Bias Temperature Instability (NBTI): It affects PMOS transistors by changing the threshold voltage. It is because the positive charges are trapped at the oxide, which increases the threshold voltage.

Hot Carrier Injection (HCI): Different from NBTI, HCI affects NMOS transistors. Due to high switching activity, hot electrons (energetic electrons) may enter the depletion region to permanently damage the activity of NMOS transistors or become trapped in the gate dielectric to change the threshold voltage.

2.2.3. Radiation-Induced Defect

A radiation-induced defect is also called a hard-error, which is permanently physical damage caused by the striking of radiation particles and will not disappear after resetting. Radiation-induced defects include single-event latch-up (SEL), single-event burnout (SEB), displacement damage effect (DDD), and total ionizing dose effect (TID). These hard-errors are not a big concern to the terrestrial electronic devices because most of arriving particles on the terrestrial are secondary particles that are not as energetic as the outer space particles. They are a big concern for outer space devices, such as satellites. There are two typical radiation-induced defects:

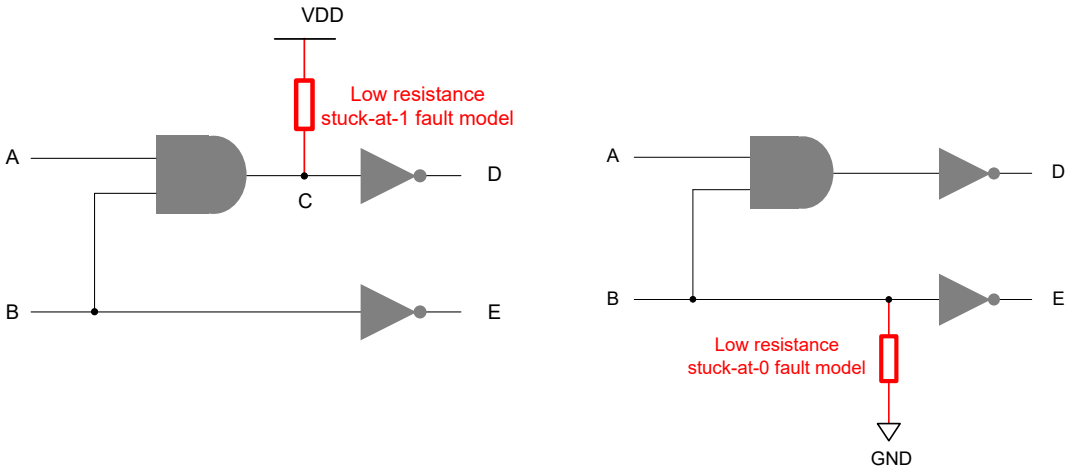
Single-Event Latchup (SEL): It is a type of short effect caused by particle striking. A particle strikes a transistor and causes permanent damage to it, which makes it continually conducting.

Single-Event Burnout (SEB): It is a type of single event caused by a high-energy particle striking and it induces localized high current damage that leads to a failure.

2.3. Fault Model

A fault is the logical level abstraction of the physical behavior of a defect. Fault models are a series of faults, which can precisely reflect the physical condition of defects. The probably occurred defects can be assumed according to the layout information. These assumed defects are represented by fault models, which can show their physical conditions and make the test pattern generation more easily. Using fault models can greatly reduce test time and increase test efficiency. A good fault model can accurately show the behavior of a defect and can be efficient for simulation and test pattern generation [67-69]. The commonly used fault models are stuck-at fault models, transistor fault models, wire open fault models, and wire short fault models.

Stuck-at faults refer to a signal line stuck at a constant logic value ("1" or "0"), which can represent a short defect that this signal line shorted with VDD or GND, respectively. The stuck-at fault models are widely used in combinational circuits. Figure 2.3 shows an example of stuck-at fault models. Figure 2.3 (a) shows a stuck-at-1 fault model to represent a short defect between VDD and node C. Figure 2.3 (b) shows a stuck-at-0 fault model to represent a short defect between GND and node B.



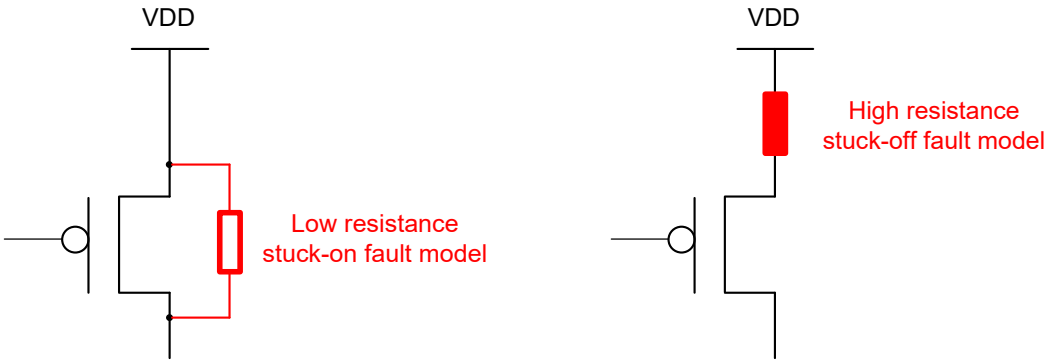
(a) Stuck-at-1 fault model (b) Stuck-at-0 fault model

Figure 2.3 Stuck-at fault models.

These stuck-at faults can be tested by using quiescent power supply current (I_{DDQ})

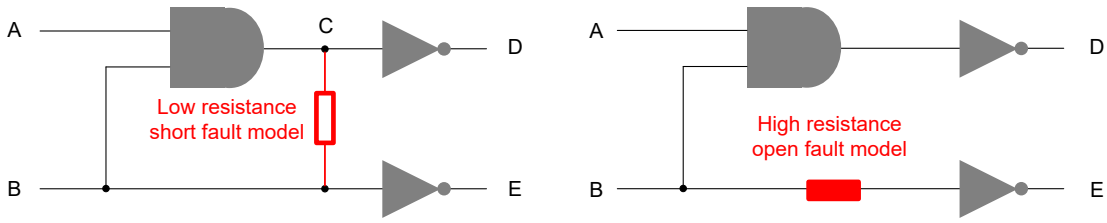
measurement [49].

Transistor faults refer to the stuck-on or stuck-off of a transistor. The stuck-on fault of a transistor represents a transistor short defect (such as gate oxide shorts, defective p-n junctions, and parasitic transistor leakage) that will turn ON this transistor. The stuck-off fault of a transistor represents a transistor open defect (such as gate oxide opens and defective p-n junctions) that will turn OFF this transistor. Figure 2.4 shows an example of transistor fault models. Figure 2.4 (a) shows a stuck-on fault model to represent a short defect between source and drain. Figure 2.4 (b) shows a stuck-off fault model to represent an open defect at the source of this transistor.



(a) Stuck-on fault model (b) Stuck-off fault model

Figure 2.4 Transistor fault models.



(a) Short fault model (b) Open fault model

Figure 2.5 Wire short and open fault models.

Short faults and open faults refer to short defects and open short defects in metal wires. Short faults represent shorts between two adjacent metals. Open faults represent opens in diffusion, poly, or metal due to process variation or production imperfection. Figure 2.5 (a) shows a wire short fault model to represent a short defect between wires C and B. Figure 2.5 (b) shows a wire open fault model to represent an open defect at the wire connecting node B and the input of an inverter.

2.4. Defect Coverage

For a given circuit under test (CUT), a series of fault models can be generated according to its layout information. After applying test patterns (according to the fault models) to the inputs of this CUT and observing the test responses from its outputs, this CUT can be tested. If all considered faults are observed, we can say that the defect coverage (fault coverage) of this CUT is 100%. If not, its defect coverage is defined as:

$$Defect\ Coverage = \frac{Number\ of\ Detected\ Faults}{Total\ Number\ of\ Faults} \qquad (2.2)$$

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 [75, 76, 78].

The defect coverage of a hardened latch cell is calculated by simulating a simple flush test with all possible 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 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: $\sum_{d \in D(c)} P_D(d)$. 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:

$$DC(c, t) = \sum_{d \in D(c)} P_D(d) \cdot (1 - t(c_d)) \qquad (2.3)$$

The calculation flow of defect coverage (DC) of a latch cell is shown in Figure 2.6. After initialization of the variable $DC = 0$ for accumulating the result, a 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. If the defect d is not observable, this defect escapes the test. After all considered defects are simulated and the DC can be calculated.

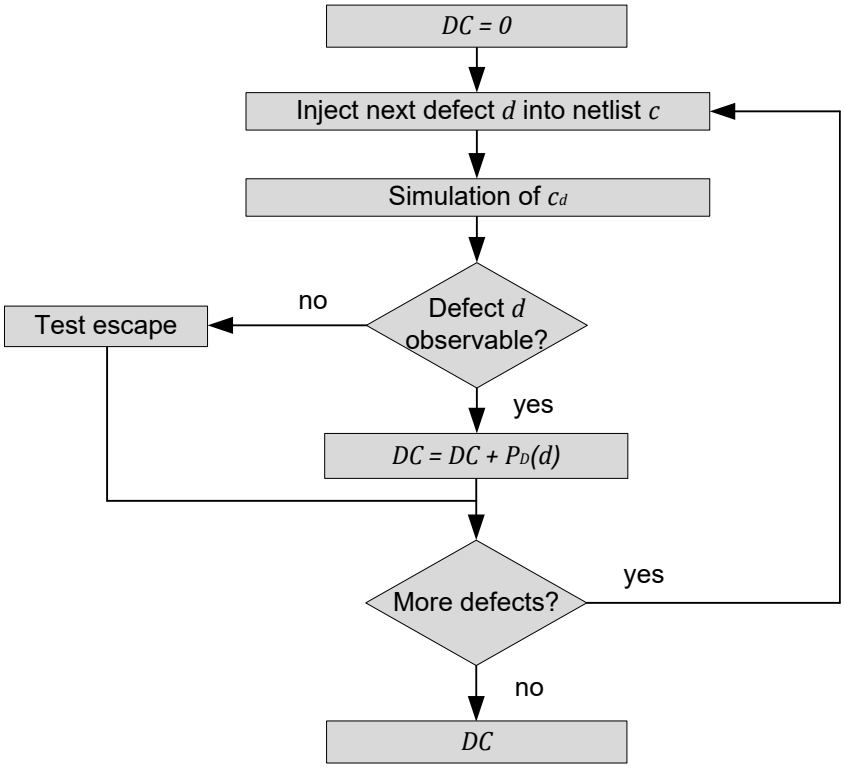


Figure 2.6 Defect coverage (DC) calculation flow.

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.

2.5. Summary

This chapter briefly introduces the basics of soft-errors, including the mechanism of soft-errors, sources of radiation particles, the impact of soft-errors, and soft-error classification. The introduced soft-error rate (SER) calculation metric (soft-error vulnerability, SEV) can be used to evaluate the soft-error tolerability of hardened latches. However, this SEV metric is only for defect-free hardened latches. This chapter also introduces the basics of defects (production defects, aging-related defects, and radiation-induced defects). For simplifying test generation for LSI circuits, fault models are provided to behave the physical condition of defects, which are located according to the layout information. At last, defect coverage is introduced.

3. Related Works

This chapter introduces some typical soft-error tolerance methods, including Error Correction Codes (ECCs) for protecting the memories, system-level soft-error mitigation, register-level soft-error mitigation, and hardened latch designs. Also, this chapter introduces some defect detection methods.

3.1. Soft-Error Mitigation

Due to the stochastic nature of radiation-induced soft-errors, various elements (such as memories and sequential elements) in modern chips may suffer from the impact of soft-errors. For mission-critical applications, protecting these soft-error vulnerable elements becomes especially important.

3.1.1. Error Correction Code

Error Correction Codes (ECCs) are widely applied to protect memories from the impact of soft-errors [50, 51]. The ECCs are performed by adding parity checking bits to check and correct soft-errors caused bit flips. These parity bits are computed into the code along with their write operations and can be decoded by the read operations. The encoding and decoding of these parity bits are performed by a specific circuitry. With the help of these added parity bits, corrupted data in memories can be checked and corrected. However, bigger memory requires more overhead for the parity bits. Also, the decoding process needs a lot of time when the parity bits scale is very large [52].

3.1.2. System-Level Mitigation

A system-level soft-error tolerance scheme [53] is applied in small satellites by combining hardware and software. It uses multiple cores to operate the same process and uses a software program to compare the results of these cores. If a core shows wrong results, the rest cores will continue with the majority of results and this corrupted core will roll back to a few clock cycles before continuing this process.

Another system-level soft-error tolerance scheme [54] is using a combination of soft-error tolerance techniques together to protect process cores, including hardened designs [55, 56], parity checking [57], and micro-architectural recovery [58, 59].

3.1.3. Register-Level Mitigation

A register-level soft-error detection and correction method was proposed in [60]. It uses latches, NAND, and XOR cells to form a parity tree and two of these parity trees can form an error detecting register. This method can locate the soft-error occurred register and be reapplied for both offline and online testing.

3.1.4. Hardened Latch Design

Hardened latch designs achieve soft-error tolerability by adding redundant feedback loops and using a voter to select the correct output. Some typical hardened latches will be introduced in this section. C-element is a commonly used voter, which is shown in Figure 3.1. Its truth table is shown in Table 3-1. If two inputs (input A and input B) of a C-element are the same logic value, the C-element works as an inverter, which inverts the input logic value. If two inputs of a C-element hold different logic values, the output of this C-element is at a high-impedance state.

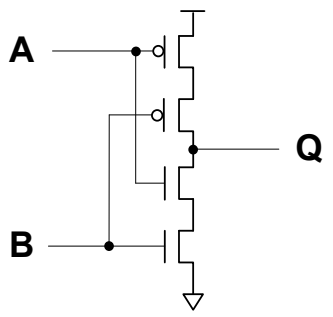


Figure 3.1 Structure of C-element.

Table 3-1 C-element truth table

A	B	Q
0	0	1
1	1	0
0	1	High-Impedance
1	0	High-Impedance

Figure 3.2 shows a triple modular redundancy (TMR) latch design, which uses three standard latches to store the same input data and uses a voter circuit to select the majority as its output. This latch can prevent the soft-errors from appearing at the output. However, it cannot correct the corrupted logic value until the arrival of a new datum.

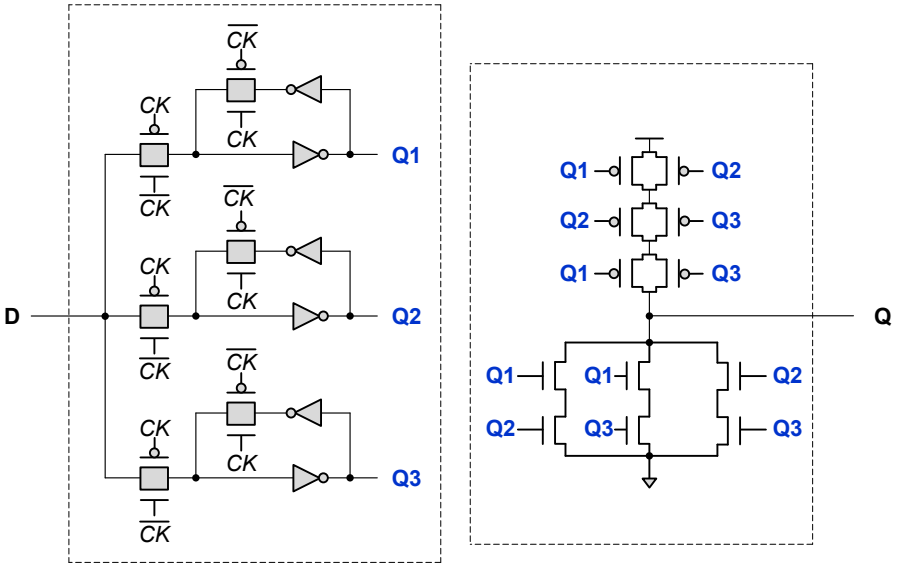


Figure 3.2 Triple modular redundancy (TMR) latch.

Figure 3.3 shows a feedback redundant hardened latch design (FERST) [18], which stores the same logic value in two feedback loops (FL0 and FL1) and uses a C-element (CE3) to prevent the soft-errors from outputting. Within each feedback loop, a C-element is applied to tolerate soft-errors. A weak keeper is at the output of CE3 to avoid the impact of the high-impedance state of CE3.

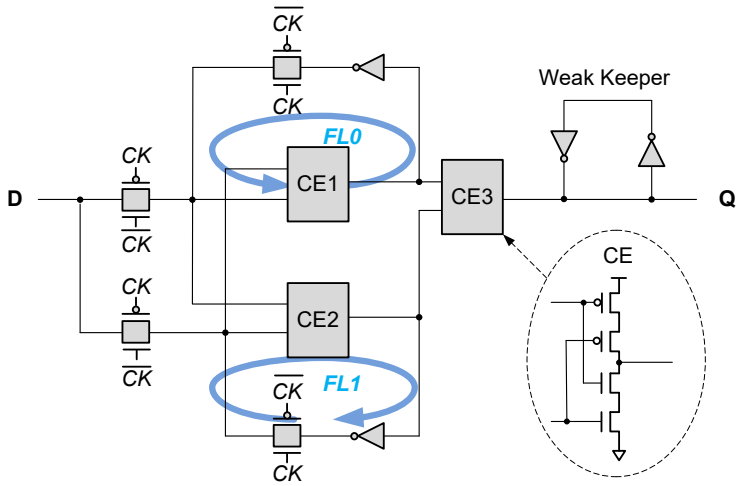


Figure 3.3 FERST [18] latch.

Figure 3.4 shows a hardened latch design (HLR) [19], which uses three transmission gates, two feedback loops (FL0 and FL1), and a clock-controlled C-element to form a hardened latch design.

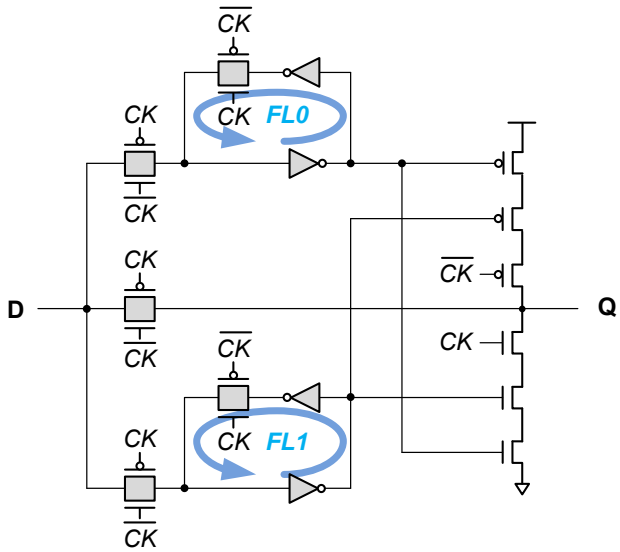


Figure 3.4 HLR [19] latch.

In transparent mode, the input signal propagates through three transmission gates and divides into three parts. Two feedback loops store the input signal, and the third part propagates directly to the output. During this transparent mode, the clock-controlled transistors in the C-element are in the OFF state and it can prevent the probable conflict at the output of this latch. In hold mode, the clock-controlled transistors in the C-element are in the ON state and two feedback loops will continually drive the clock-controlled C-element. Similar to the TMR latch, the HLR latch can prevent the soft-errors from appearing at the output, however, it cannot correct the corrupted logic value.

3.2. Defect Detection

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 [46].

3.2.1. Functional Test

Figure 3.5 shows an example of a sequential circuit with a combinational portion and three flip-flops. Using functional tests can detect defects in flip-flops. The test vectors are applied to the inputs of the combinational portion and the test results can be checked at the output of this circuit.

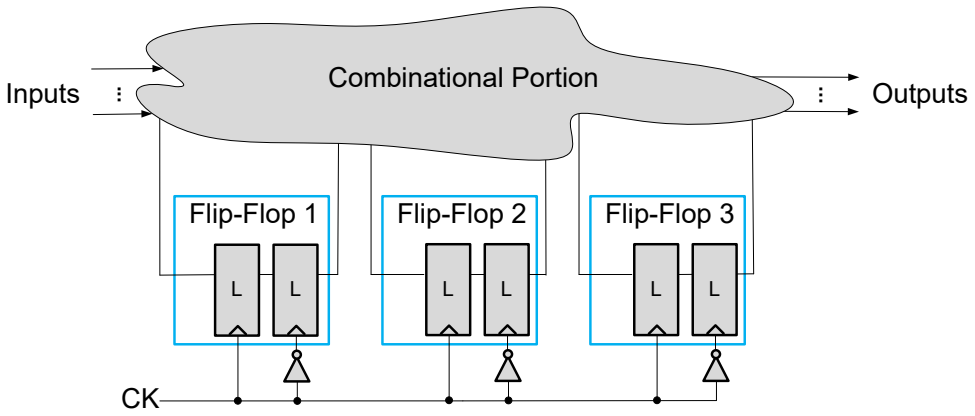


Figure 3.5 Functional test.

When the scale of the CUT is very small, it is an acceptable way to apply all possible test patterns to the inputs of the CUT to fully test it. However, this way meets problems when testing large-scale-integration (LSI) or very-large-scale-integration (VLSI) circuits and it is very difficult to check and control the internal states of numerous flip-flops. In the following section, a design-for-test (DFT) technique called scan design can be used to overcome this difficulty [70, 71].

3.2.2. Scan Design

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

Scan design is a commonly used DFT technique [46]. 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, which can greatly improve the testability.

3.2.3. Scan Test

Figure 3.6 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 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.

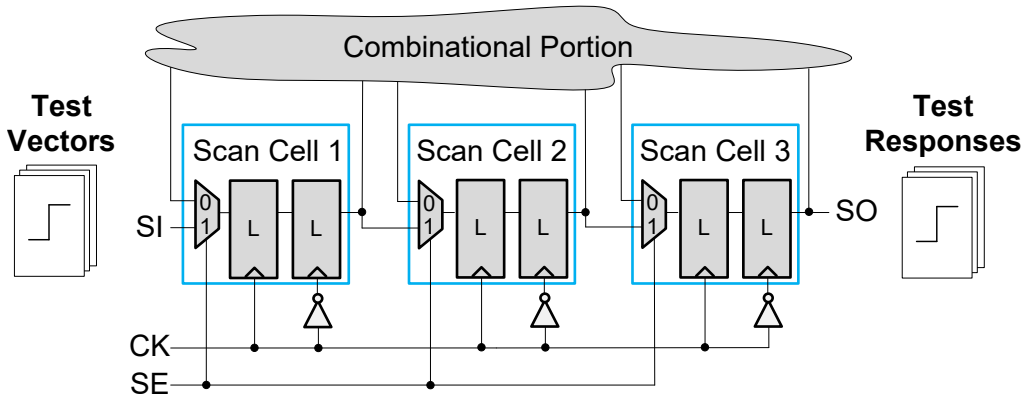


Figure 3.6 Scan chain example.

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” [46]) 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, Figure 3.6 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. Flush tests can be applied to detect the transition delay faults in scan cells. A good flush test pattern should provide four causes of transitions, including 0 - to - 0, 0 - to - 1, 1 - to - 0, and 1 - to - 1. Also, flush tests can be applied for diagnosis.

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

3.3. The Importance of This Research

With the continuously reduction of technology feature sizes and supply voltages, modern ICs become more and more vulnerable to soft-errors. Sequential elements (like latches and flip-flops) are the most vulnerable to soft-errors in a circuit. Hence, it is very important to protect them from the impact of soft-errors. A register-level soft-error mitigation method is available to detect soft-errors in latches [60]. However, it is not suitable to protecting mission-critical applications because it requires some time to process the roll-back operation to tolerate soft-errors. During this time interval, bad results may have already happened. Hardened latch designs can be used to protect sequential elements as well. The advantage of using hardened latch designs is that hardened latch designs can prevent soft-errors from reaching their outputs and do not need to sacrifice valuable time.

So far, many state-of-the-art hardened latch designs have been proposed to tolerate soft-errors and they are believed to have high reliability. However, the problem with the application of these hardened latch designs is that the impact of defects on the tolerability of hardened latches has not been considered. The soft-error tolerability of manufactured chips based on these hardened latch designs cannot be evaluated because defects can reduce the soft-error tolerability of hardened latch designs. Furthermore, redundancy in hardened latch designs may mask not only soft-errors but also the defect effects, which makes defects in hardened latches difficult to detect. This research is the first to find the impact of defects on the soft-error tolerability of hardened latches and the first to propose a novel metric to evaluate residual soft-error tolerability of hardened latches after production. Furthermore, this research proposes novel hardened latch designs with good defect detectability. It is the first research that bridges the hardened latch design field and defect detection field as well.

In this research, the impact of defects on the tolerability of hardened latches has been analyzed. This research proposed the first soft-error vulnerability metric, called post-test vulnerability factor (*PTVF*), that takes defects into account to evaluate the impact of defects (in Chapter 4). Furthermore, two new hardened latches (scan-test-aware hardened latch, STAHL, as shown in Chapter 5 and a novel high performance scan-test-aware hardened latch design, HP-STAHL, as shown in Chapter 7) with good defect detectability are proposed. A new test procedure for testing STAHLs is proposed in Chapter 6 and a new test procedure for testing HP-STAHLs is proposed in Chapter 8.

3.4. Summary

In this chapter, some typical soft-error tolerance methods are introduced. Error correction codes can be used to protect memories. A register-level soft-error tolerance method can be used to detect soft-errors in latches [60]. Hardened latches can be used to

protect latches from the impact of soft-errors. This research focuses on using hardened latches because hardened latches can prevent soft-errors from reaching their outputs.

Some defect detection methods are also introduced in this chapter. This research focuses on using scan chains and performing flush tests to detect defects in latches. Because scan design is a commonly used industry practice, it is easy to control and check the internal logic values stored in latches.

4. Post-Test Vulnerability Factor (*PTVF*)

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

4.1. 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: $v(c,f) \neq v(c_d,f)$. I define a novel metric called Post-Test Vulnerability Factor (*PTVF*) [48] that takes the probabilities of the test-escaping defects into account as follows:

$$PTVF(c,t) = \frac{\sum_{d \in D(c)} P_D(d) \cdot t(c_d) \cdot SEV(c_d)}{1 - DC(c,t)} \qquad (4.1)$$

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. (4.1) 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. (4.1) $\sum_{d \in D(c)} P_D(d) \cdot t(c_d) \cdot SEV(c_d)$ 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. (2.1). Assume that each calculated $SEV(c_{ud})$ is 30%. The numerator of Eq. (4.1) is then: $5 \times 1\% \times 30\% = 1.5\%$. The denominator of Eq. (4.1)

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.

4.2. 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 Figure1.1 (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 Figure 4.1. 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 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 simulation is rather quick since it lasts 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.

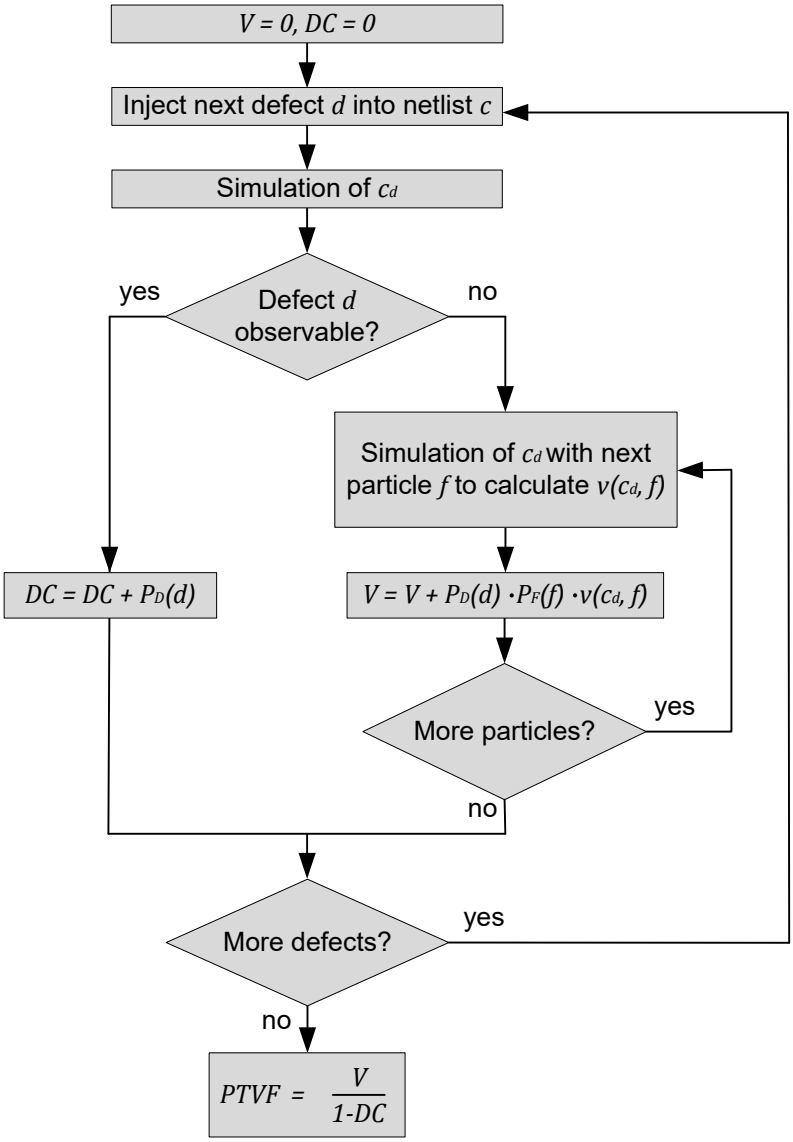


Figure 4.1 *PTVF* calculation flow.

4.3. Summary

Post-Test Vulnerability Factor (*PTVF*) is the first metric to evaluate the impact of defects on the soft-error tolerability of hardened latches. *PTVF* considers both the impact of defects and the impact of soft-errors on the defective hardened latches. It is an important metric to evaluate the reliability of hardened latch designs.

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

To overcome **Problem-1 (Low Testability)**, a novel scan-test-aware hardened latch (STAHL) design is proposed [77]. In this chapter, the structure of STAHL is introduced in Section 5.1. Both functional mode and shift mode of the STAHL are introduced in the following sections. The summary section concludes this chapter.

5.1. Structure of STAHL

The STAHL's structure is shown in Figure 5.1. 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 $\overline{CK}$ (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). $\overline{SE}$ 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).

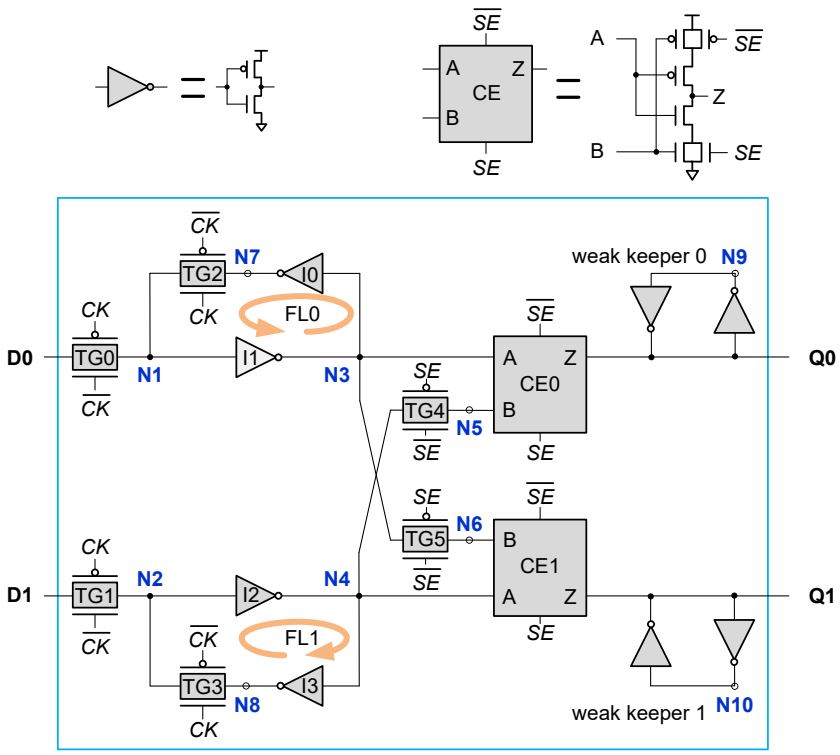


Figure 5.1 Structure of the proposed STAHL.

2 SE-signal-controlled transmission gates (TG4 and TG5) drive the inputs of 2 C-elements (CE0 and CE1). For each C-element, we add 2 SE-signal-controlled transistors (an $\overline{SE}$-controlled PMOS and an SE-controlled NMOS), which will be ON in shift mode and 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.

5.2. Functional (Hardened) Mode of STAHL

The STAHL is in functional mode when SE = 0. Figure 5.2 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.

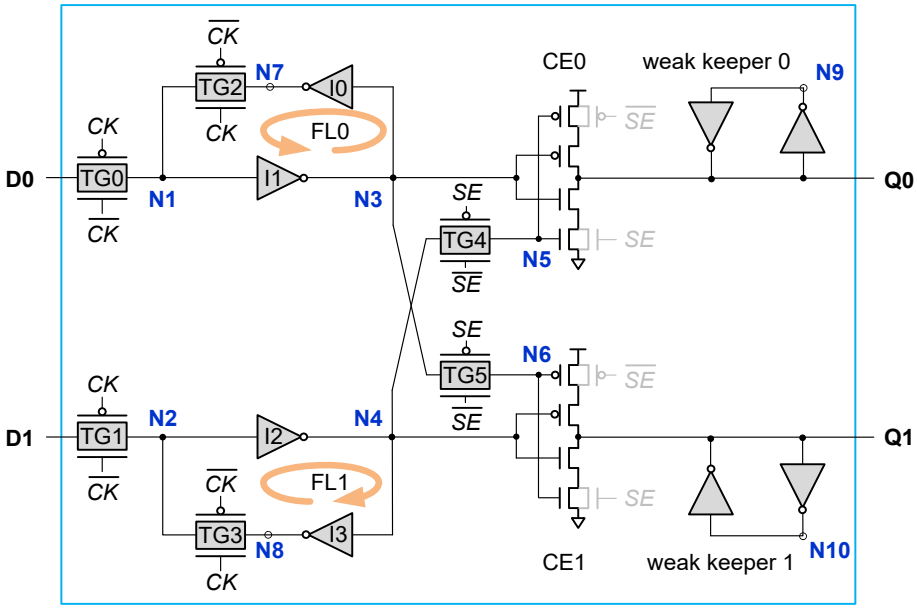


Figure 5.2 SE = 0: functional (hardened) mode.

In 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 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 a soft-error 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 soft-errors occurring on nodes N3, N5, and N7. Due to the symmetric nature of the STAHL, the same discussion holds for soft-errors occurring on nodes N2, N4, N6, and N8.

Suppose that node Q0 is affected by a soft-error 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.

Suppose that a soft-error temporally turns on a SE-signal-controlled transistor, it will not influence the outputs of the STAHL.

5.3. Shift Mode of STAHL

The STAHL is in shift mode when SE = 1. Figure 5.3 shows the circuit for this mode. The transistors shown in gray are OFF. Two 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).

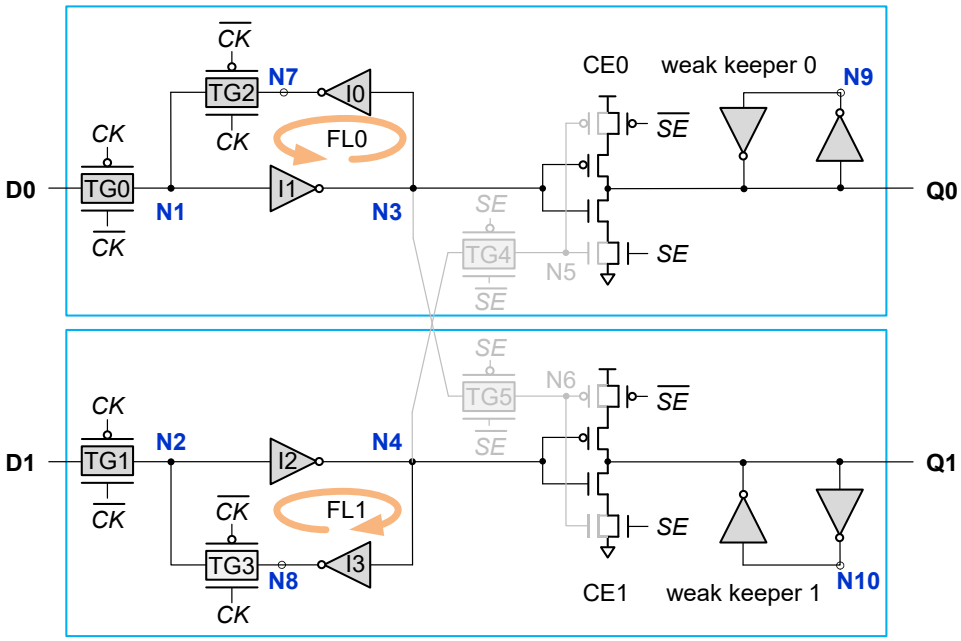


Figure 5.3 SE = 1: shift mode.

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 the 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.

5.4. Summary

Existing hardened latch designs focus on increasing their soft-error tolerability by adding redundant circuitry. However, the fact that added redundancy can mask the defect effect has not been considered during their design process, which makes defects in them difficult to detect. To overcome this difficulty, this research proposed a scan-test-aware hardened latch (STAHL) design, which is the first hardened latch design to achieve high soft-error tolerability and high defect detectability. It has two modes: shift and functional. In shift mode, defect effects will not be masked, and the STAHL can be tested efficiently. In functional mode, it can be applied to tolerate soft-errors.

6. 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 sections 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.

6.1. Scan Chain Structure Based on STAHL

Figure 6.1 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.

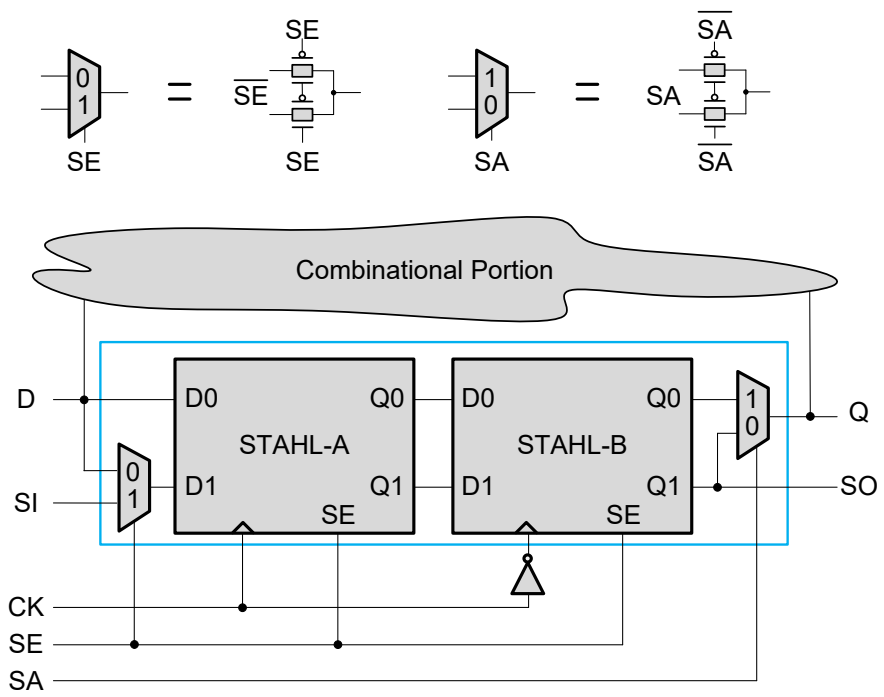


Figure 6.1 STAHL-based scan cell.

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 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 (Figure 5.1) 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 Subsection 6.5.

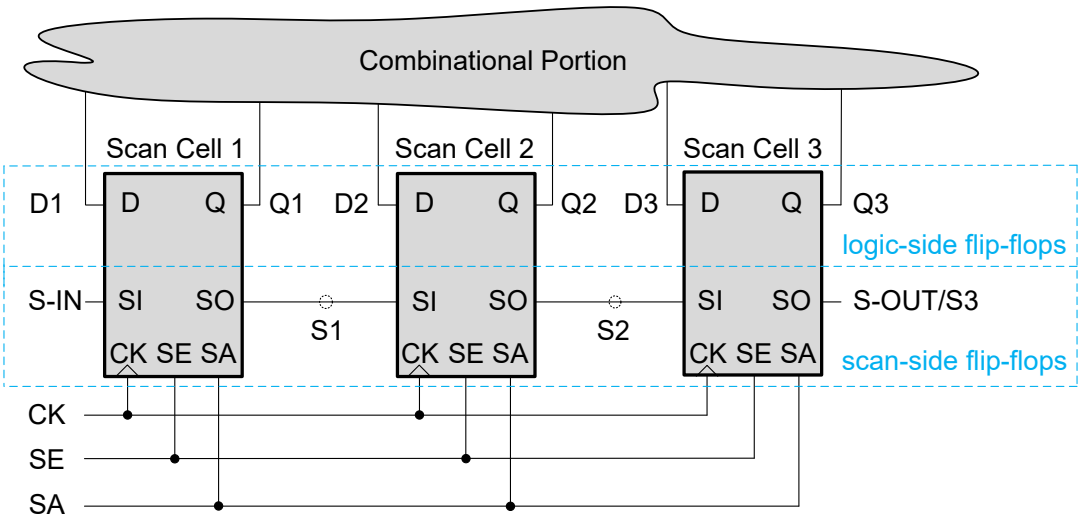


Figure 6.2 STAHL-based scan chain.

Figure 6.2 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.

6.2. Test Procedure Flow

The overall test procedure flow of an STAHL-based scan chain is shown in Figure 6.3 with three phases: Phase-A, Phase-B, and Phase-C. Flush tests are applied to detect defects in the scan-side flip-flops in Phase-A. In Phase-B, a scan-side capture is applied to detect defects in the combinational portion. In Phase-C, a logic-side capture is applied to detect 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.

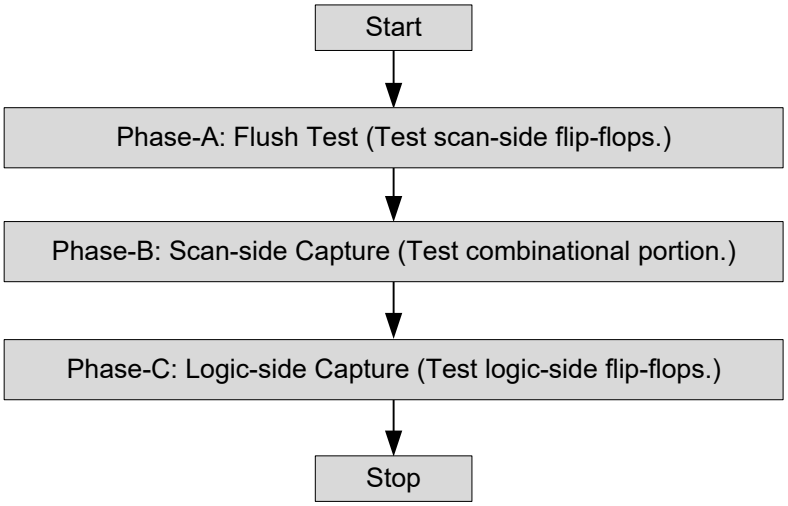


Figure 6.3 Test procedure flow.

In this thesis, 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 Figure 6.2 as an example to explain the details of the test procedure.

6.3. 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 (Figure 6.2) 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.

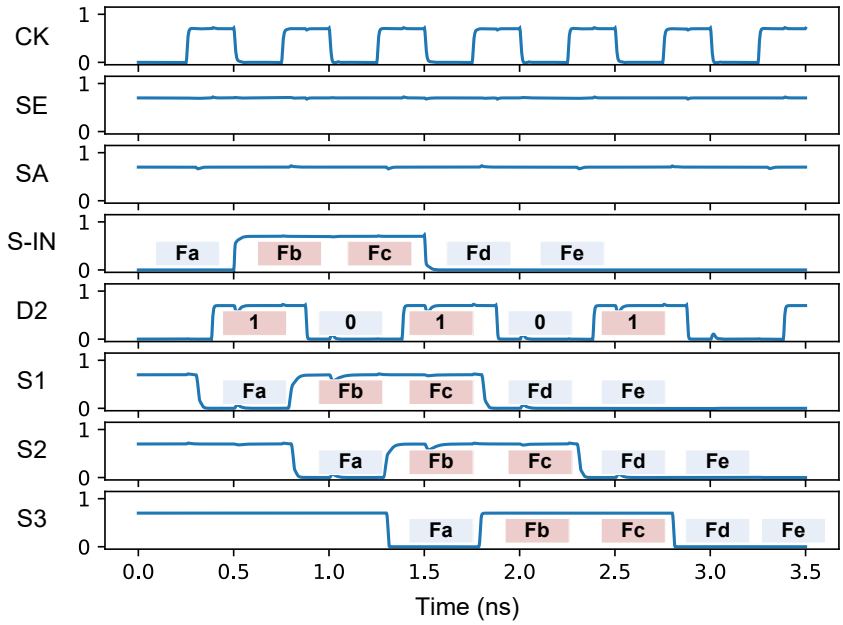


Figure 6.4 SE = 1 and SA = 1: a test pattern of FaFbFcFdFe = 01100 flushes through the scan-side flip-flops.

Figure 6.4 shows an example that 5 bits (FaFbFcFdFe = 01100) [46] 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 Figure 6.4, S1 (input of the Scan Cell 2 in Figure 6.2) 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.

6.4. 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 Figure 6.5. 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).

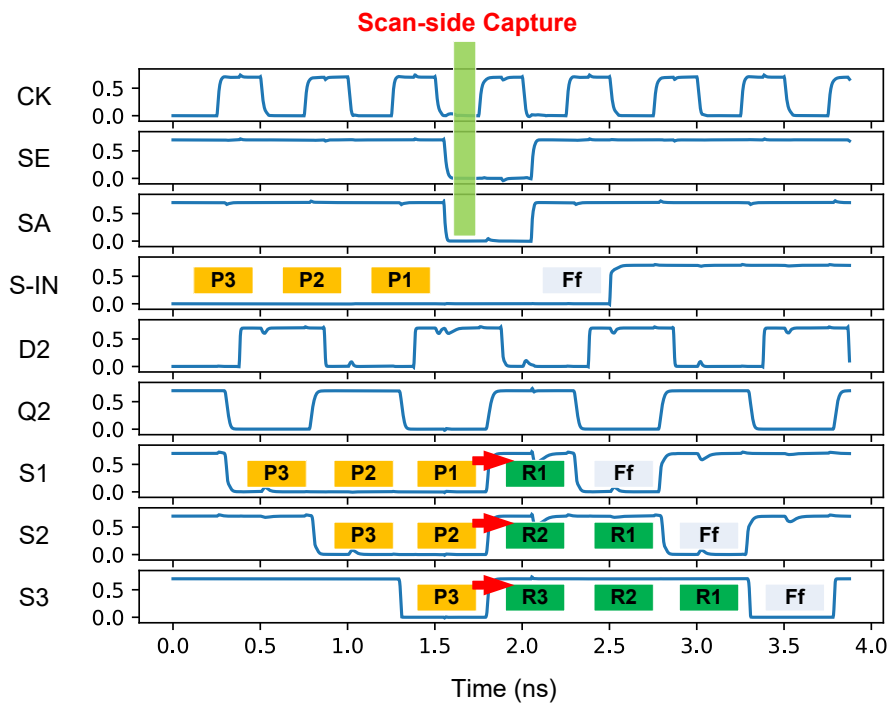


Figure 6.5 SE = 0 and SA = 0: the next rising clock captures R1R2R3 = 111 (test response of the pattern P1P2P3 = 000).

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 Figure 5.1) at the node Q1 of STAHL-B will keep the logic value.

6.5. 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.

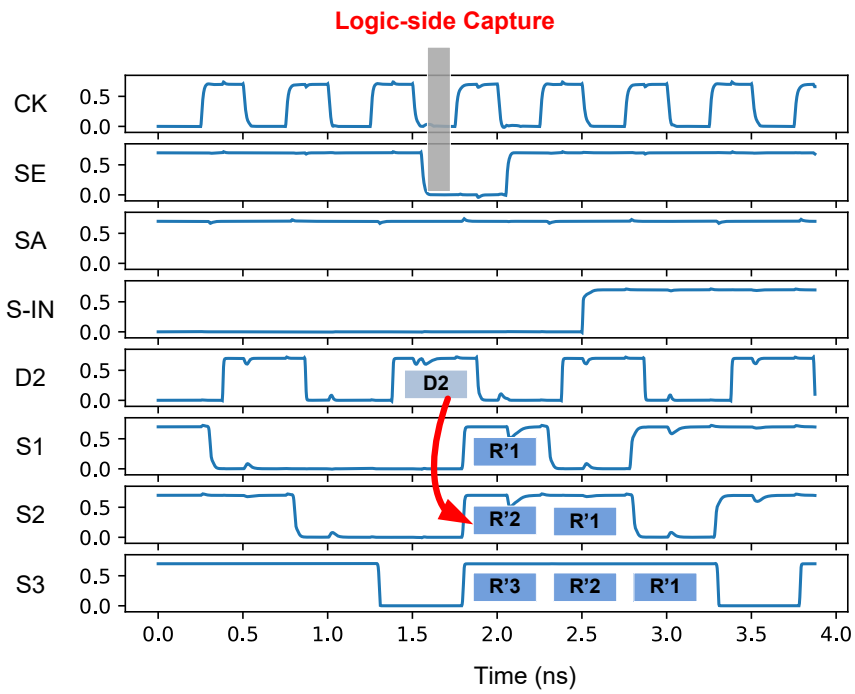


Figure 6.6 SE = 0 and SA = 1: the next rising clock captures D2 = 1 (test response to the value stored in the logic-side flip-flop of Scan Cell 2).

The logic-side capture example is shown in Figure 6.6. The logic value at D2 is 1 and is captured at S2 (R'2 = 1). It is the same for D1 and D3 in Figure 6.2. So, we have the test response (R'1R'2R'3 = 111).

6.6. Full Test Procedure

Figure 6.7 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 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).

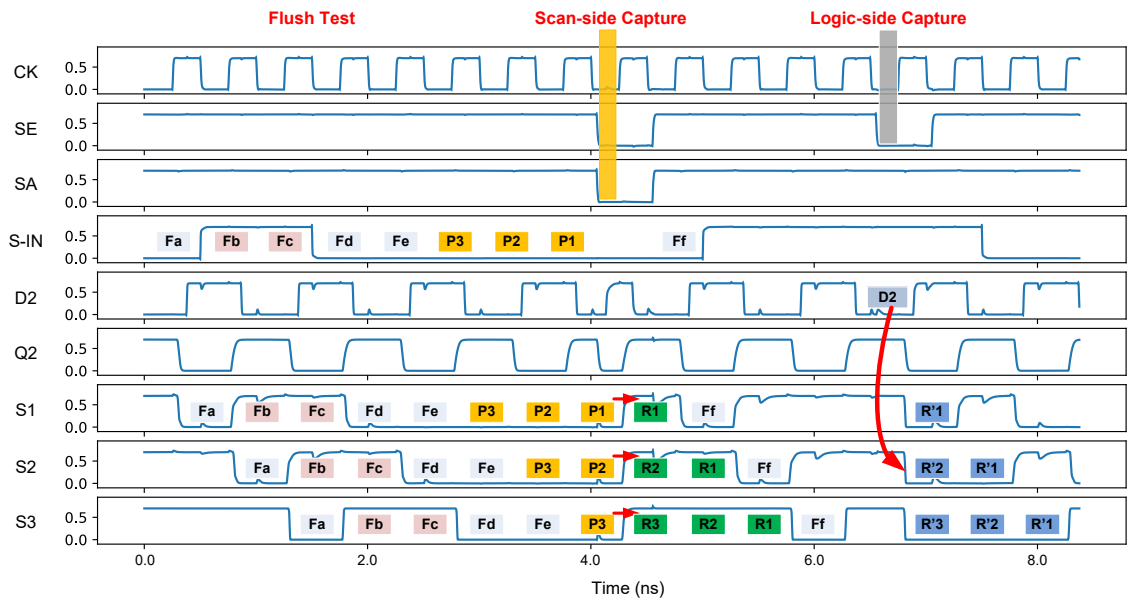


Figure 6.7 Test procedure of the STAHL-based scan chain.

6.7. Summary

In this chapter, the STAHL-based scan chain structure is introduced. Compared with a conventional scan chain, this STAHL-based scan chain has the same interface except for an additional control signal SA. The test procedure of this STAHL-based scan chain is also introduced in this chapter with three phases (Phase-A, Phase-B, and Phase-C). In Phase-A (flush test), the scan-side flip-flops can be tested by using flush tests. In Phase-B (scan-side capture), the combinational portion can be tested. In Phase-C (logic-side capture), the logic-side flip-flops can be tested. According to the proposed test procedure, STAHL-based scan cells can be effectively tested.

7. High Performance Scan-Test-Aware Hardened Latch (HP-STAHL)

In this chapter, a high-performance scan-test-aware hardened latch (HP-STAHL) [62] is introduced, including its structure and operation detail. Different from the STAHL, HP-STAHL sacrifices parts of its soft-error tolerability to achieve low power consumption and high propagation speed, as well as high defect coverage. HP-STAHL is an option for applications that require high performance.

7.1. Structure of HP-STAHL

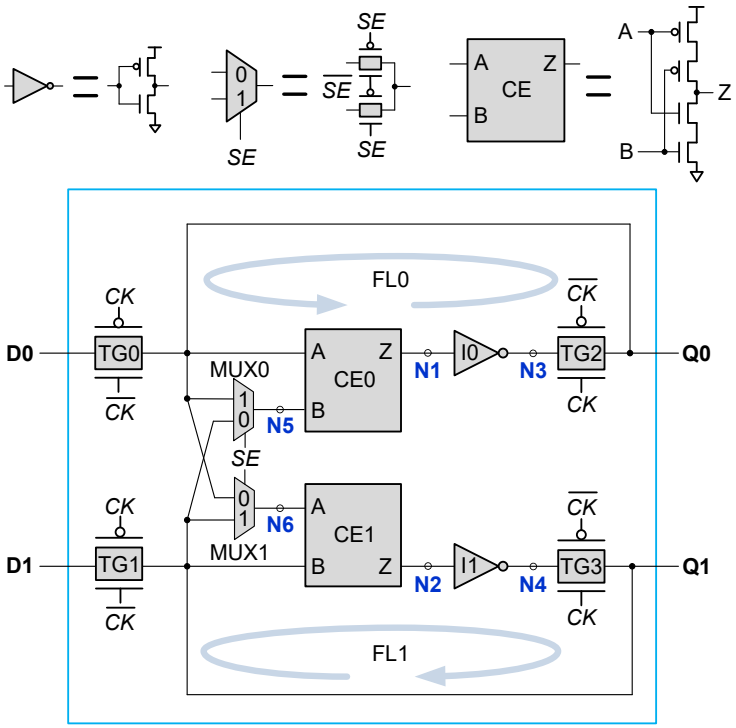


Figure 7.1 Structure of HP-STAHL.

HP-STAHL is shown in Figure 7.1 Same as the STAHL, HP-STAHL has two inputs (D0 and D1) as well as two corresponding outputs (Q0 and Q1). In addition to the normal clock signals CK and $\overline{CK}$ ($\overline{CK}$ is the inverse signal of CK), HP-STAHL has an additional control signal SE (scan enable) that switches between shift mode (SE = 1) and functional mode (SE = 0). $\overline{SE}$ is the inverse signal of SE. The HP-STAHL has two

independent feedback loops (FL0 and FL1) formed by 2 transmission gates (TG2 and TG3), 2 inverters (I0 and I1), and two C-elements (CE0 and CE1). The two C-elements prevent soft-errors from appearing at the outputs.

7.2. Functional (Hardened) Mode of HP-STAHL

HP-STAHL is in functional mode when SE = 0. Figure 7.2 shows an equivalent circuit for this mode.

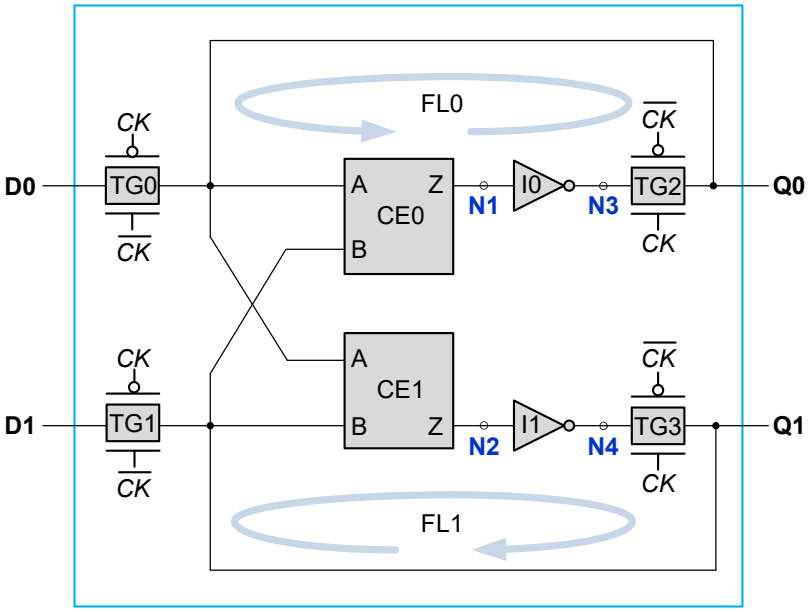


Figure 7.2 SE = 0: functional (hardened) mode.

During functional operations, the value to be stored in the latch needs to be applied to both inputs of D0 and D1.

In transparent phase (CK = 0), two transmission gates TG0 and TG1 are ON. The input value at D0 (D1) propagates to output Q0 (Q1).

In latching phase (CK = 1), two transmission gates TG0 and TG1 are OFF while TG2 and TG3 are ON. There are two feedback loops, FL0 and FL1. FL0 consists of C-element CE0, inverter I0, and transmission gate TG2. FL1 consists of C-element CE1, inverter I1, and transmission gate TG3. Particle strikes will be tolerated by HP-STAHL as follows. Both feedback loops FL0 and FL1 store the same value and each of the C-elements is connected to both feedback loops. If one feedback loop is affected by a particle strike, both C-elements will stop driving N1 and N2. The outputs of the C-elements will be in high-impedance.

Suppose that node N1 is affected by a soft-error and the logic value of N1 is temporally changed. Node N3 is influenced by this soft-error through inverter I0. Since nodes N3 and Q0 are equivalent, Q0 is influenced too. However, node Q1 is not influenced, leaving the outputs of C-elements in a high-impedance state. Similar analysis can be made for soft-errors occurring on nodes N3, N6, and Q0.

Suppose that a soft-error temporally turns on an OFF-state transistor in MUX0 (Figure 7.1), it will influence both of the inputs of CE0 and cause a wrong output. A similar analysis can be made for a soft-error at an OFF-state transistor in MUX1.

Due to the symmetric nature of HP-STAHL, the same discussion holds for a soft-error at nodes Q1, N2, N4, and N5.

7.3. Shift Mode of HP-STAHL

HP-STAHL is in shift mode when SE = 1. Figure 7.3 shows an equivalent circuit for this mode. In this mode, both feedback loops operate completely independently of each other, effectively forming two independent latches D0 - Q0 and D1 - Q1. In shift mode, both inputs of CE0 are connected to FL0 while both inputs of CE1 are connected to FL1. The two C-elements, therefore, act as simple inverters.

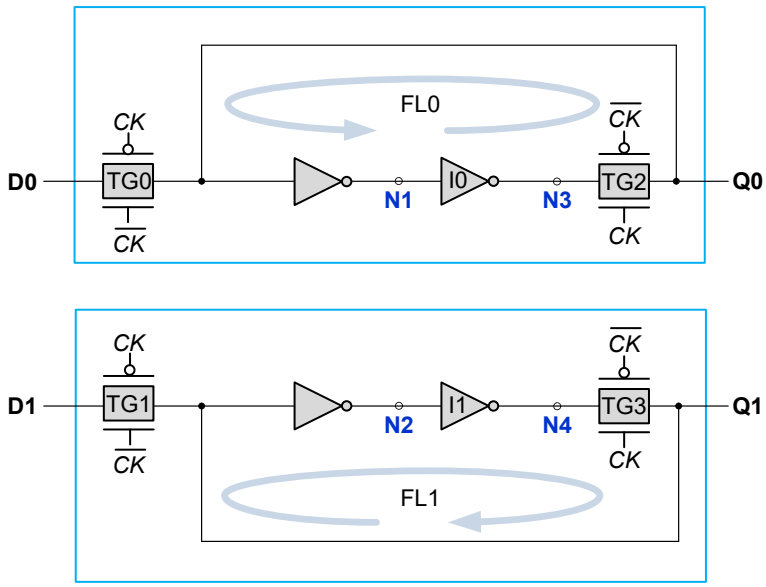


Figure 7.3 SE = 1: shift mode.

Both feedback loops can be tested in the same way as standard non-hardened latches. The only structures that cannot be completely tested in shift mode are the cross-connections from the FL0 to CE1 and FL1 to CE0. Still, the number of undetected defects that affect the soft-error hardness is significantly reduced.

7.4. Summary

In this chapter, the structure of HP-STAHL and its operation detail are introduced. Compared with the STAHL, the HP-STAHL has a lower transistor number and faster propagation speed. HP-STAHL sacrifices a part of its soft-error tolerability to achieve high propagation speed and high performance. Similar as the STHAL, the proposed HP-STAHL also has two modes: functional and shift. In functional mode, it can be applied to tolerate soft-errors. In shift mode, defect effects will not be masked. In the following chapter, the test procedure of HP-STAHL is introduced.

8. Scan Test Based on HP-STAHL

In this chapter, the structure of HP-STAHL-based scan cell and this scan cell-based scan chain structure are introduced. The following sections introduce the test procedure of testing this HP-STAHL-based scan chain.

8.1. Scan Chain Structure Based on HP-STAHL

Figure 8.1 shows a scan cell based on the HP-STAHL. Two HP-STAHLs are used to form a flip-flop and two additional multiplexers complete the scan cell. Different from the STAHL-based scan cell, this HP-STAHL-based scan cell only requires one control signal while the STAHL-based scan cell requires two. This HP-STAHL-based scan cell has the same interface as a commonly used scan cell.

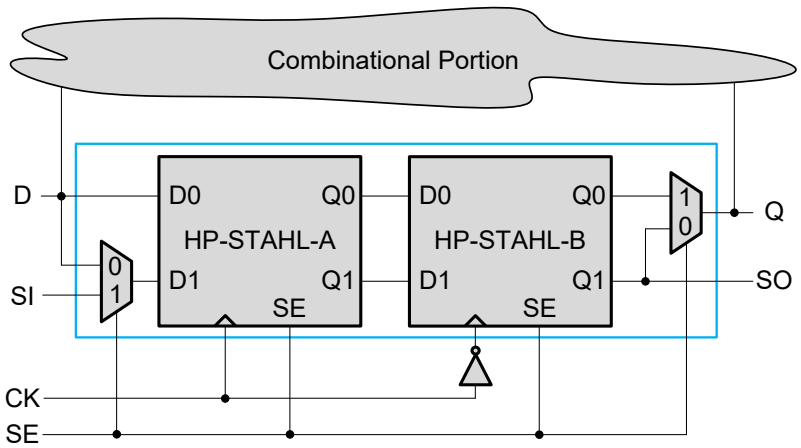


Figure 8.1 HP-STAHL-based scan cell.

When SE = 0, the scan cell operates as a flip-flop. Both HP-STAHLs are hardened against soft-errors. The input D is applied to both inputs of D0 and D1 of the master latch (HP-STAHL-A). The output Q of the scan cell is connected to the output Q1 of the slave latch (HP-STAHL-B). When SE = 1, the scan cell operates in shift mode. In shift mode, both HP-STAHLs operate as two independent flip-flops and can store two values simultaneously. The logic-side flip-flop D0 - Q0 is connected to D and Q of the scan cell, respectively. The scan-side flip-flop D1 - Q1 is connected to the SI (scan-in) and SO (scan-out) of the scan cell. Since both logic-side flip-flop and scan-side flip-flop operate independently, the combinational portion of the design will continue to operate just as in functional mode while test data are shifted from SI to SO.

An example of an HP-STAHL-based scan chain with three scan cells is shown in Figure 8.2. All connections between the scan cells are the same as a traditional scan design. The behavior of the HP-STAHL-based scan chain, however, is closer to the enhanced scan approach [30, 31] than a standard scan design-based scan chain.

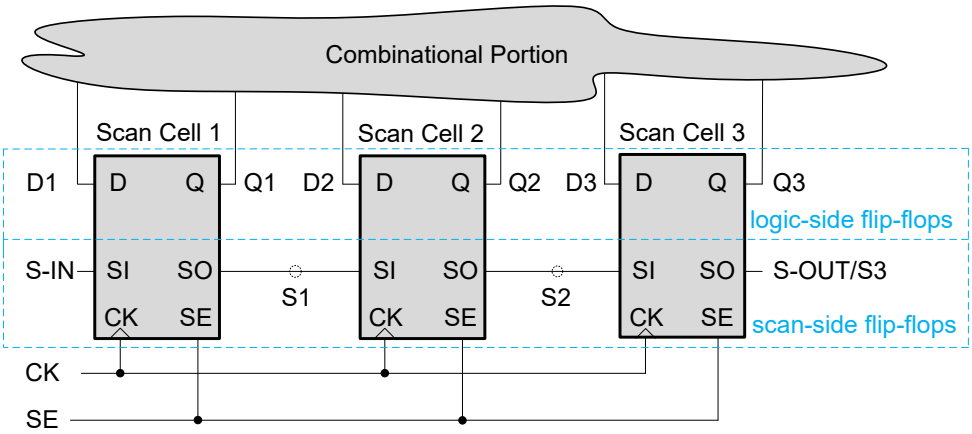


Figure 8.2 HP-STAHL-based scan chain.

8.2. Test Procedure Flow

The overall test procedure flow of an HP-STAHL-based scan chain is shown in Figure 8.3 with three phases: Phase-A, Phase-B, and Phase-C.

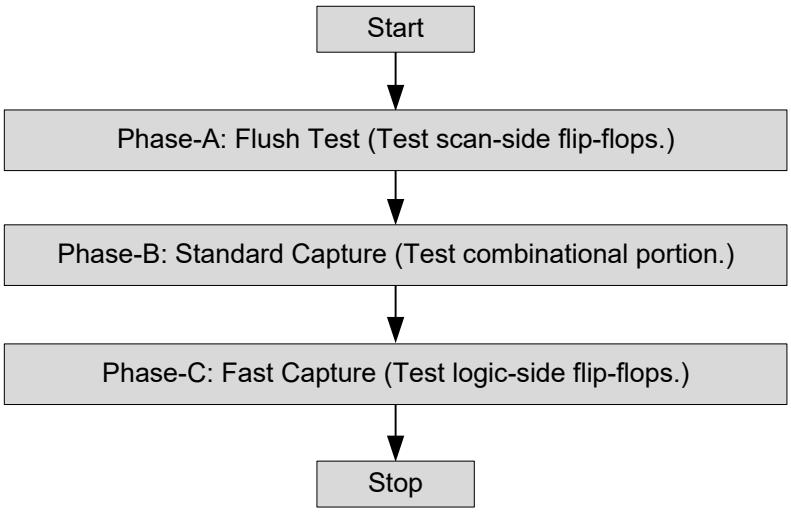


Figure 8.3 Test procedure flow.

Flush tests are applied to detect defects in the scan-side flip-flops in Phase-A. In Phase-B, a standard capture is applied to detect defects in the combinational portion. In Phase-C, a fast capture is applied to detect 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 thesis, the testing target is the HP-STAHL-based scan cell. We aim to prove that the HP-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 Figure 8.2 as an example to explain the detail of the test procedure.

8.3. Phase-A: Flush Test

During a flush test (SE = 1), test vectors can be shifted from S-IN to S-OUT via the scan-side flip-flops (Figure 8.2) 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 detected.

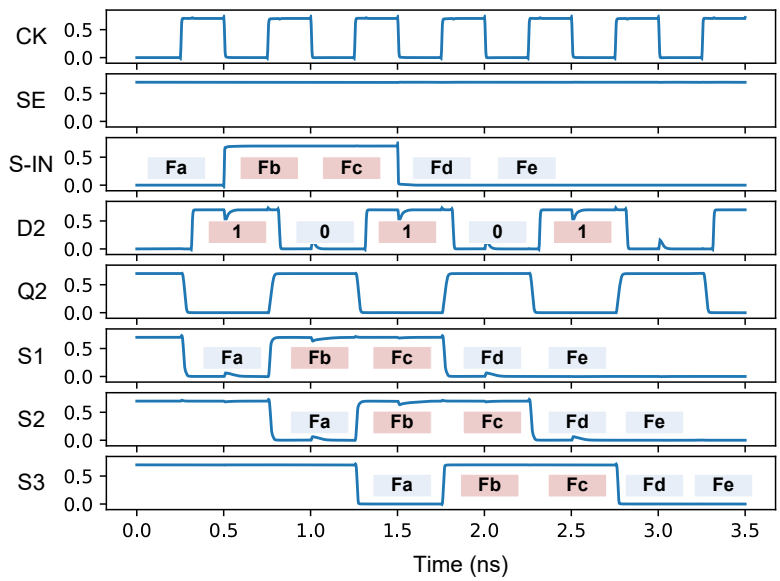


Figure 8.4 SE = 1: a test pattern of FaFbFcFdFe = 01100 flushes through the scan-side flip-flops.

Figure 8.4 shows an example that 5 bits (FaFbFcFdFe = 01100) [46] 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 Figure 8.4, S1 (input of the Scan Cell 2 in Figure 8.2) 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.

8.4. Phase-B: Standard Capture

A series of scan-side capture operations (SE = 0) is used to test the combinational portion. When a test pattern is completely shifted in, SE signal is set to 0 in preparation for the capture operation. With the falling edge of SE, the output Q of each scan cell switches to the values of the shifted-in test pattern, and 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.

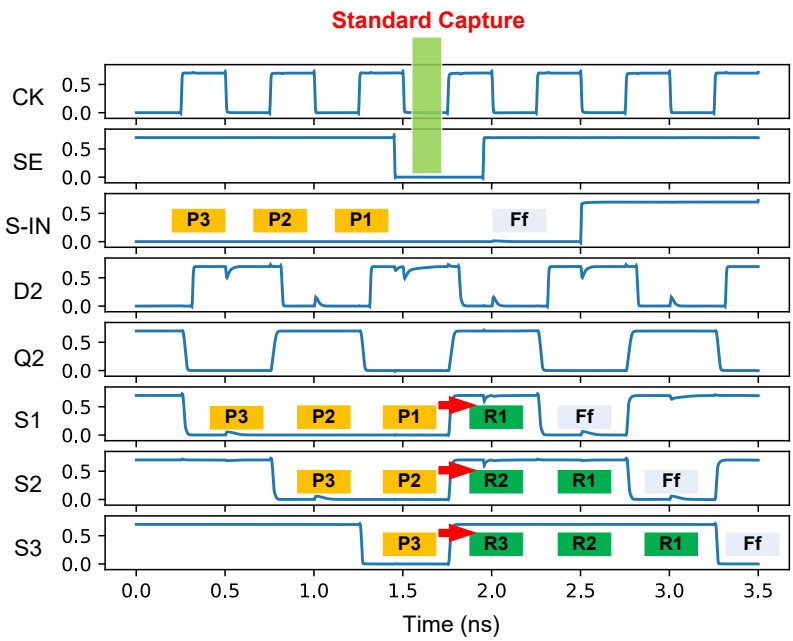


Figure 8.5 SE = 0: the next rising clock captures R1R2R3 = 111 (test response of the pattern P1P2P3 = 000).

The example is shown in Figure 8.5. The test pattern P1P2P3 = 000 is present at the outputs of the scan cells at the falling edge of SE. The pattern starts to propagate through the combinational portion of the DUT and arrives at the inputs of the scan cells. The next rising clock captures the test response (R1R2R3 = 111).

With the falling edge of SE, HP-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). A solution is to add a weak keeper after the output Q of this scan cell to keep the logic value.

8.5. Phase-C: Fast 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 fast capture cycle. By capturing and observing the corresponding responses to the values stored in the logic-side flip-flops, we can test them.

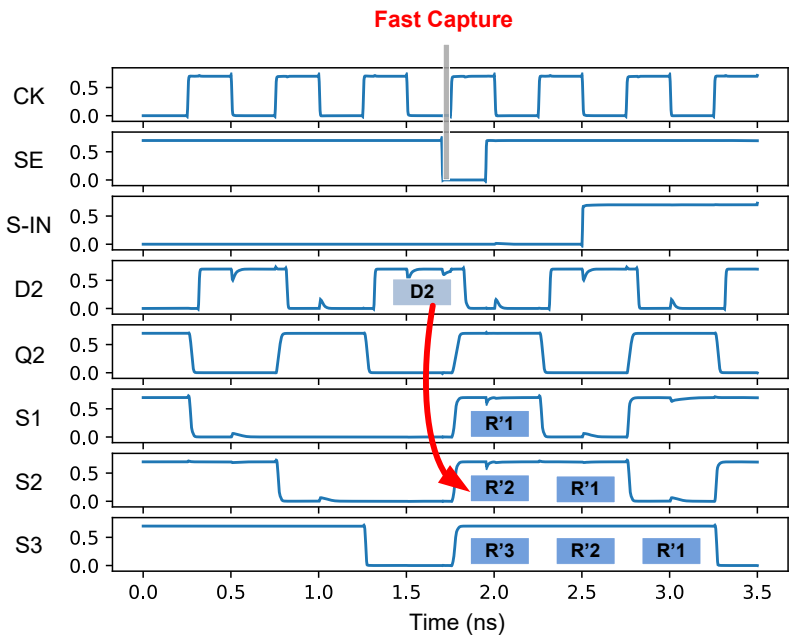


Figure 8.6 SE = 0: the next rising clock captures D2 = 1 (test response to the value stored in the logic-side flip-flop of Scan Cell 2).

For the fast capture, the falling edge of SE is placed right before the next rising edge of the clock. Before the fast capture cycle, the combinational logic has calculated the response to the state currently stored in the logic-side flip-flops of the scan cells.

The fast capture cycle will capture exactly this response because the test pattern that has been applied to the circuit with the falling edge of SE does not have enough time to propagate. If the combinational portion provides enough hold-time at each scan cell, the fast capture cycle will provide observability for the logic-side flip-flops and allows testing for defects in these parts. The logic-side capture example is shown in Figure 8.6. The logic value at D2 is 1 and is captured at S2 (R'2 = 1). It is the same for D1 and D3 in Figure 8.2. So, we have the test response (R'1R'2R'3 = 111).

8.6. Full Test Procedure

Figure 8.7 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 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 at 4.2ns. Third, a logic-side capture is applied to capture the corresponding data D2 = 0 at 6.2ns to load the current output of the combinational portion into the scan chain (R'1R'2R'3 = 000).

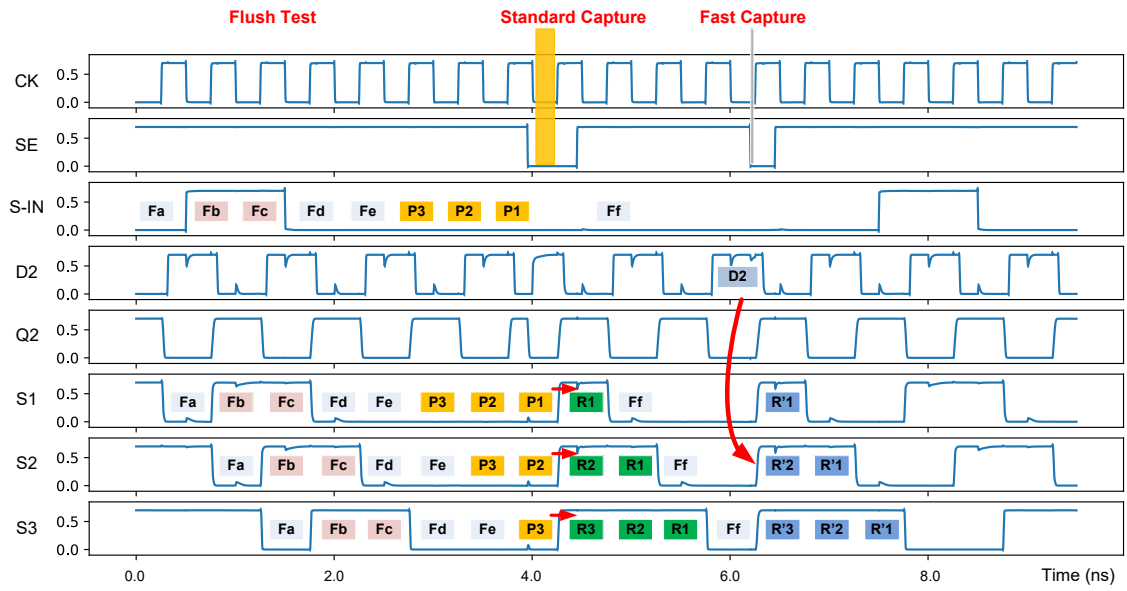


Figure 8.7 Test procedure of the HP-STAHL-based scan chain.

8.7. Summary

Different from the test procedure of STAHL-based scan chain with two control signals (SE and SA), this HP-STAHL-based scan chain test procedure only needs one control signal SE. This HP-STAHL-based scan chain has the same interface as a conventional scan chain, which means that this HP-STAHL-based scan chain can be used to replace a conventional scan chain directly.

However, it requires strict constraints on the timing between the rising edge of the clock (CK) and the falling edge of SE during the fast capture cycle. While the test procedure of the STAHL-based scan chain does not need to worry about this timing issue. There are two solutions available to test STAHLs and HP-STAHLs and the test infrastructures of the STAHL and the HP-STAHL can be exchangeable.

9. Experimental Evaluation

In this chapter, the experimental results of STAHL, HP-STAHL, and some existing hardened latches are compared. All latches were simulated using a 16nm predictive technology model [75] with a 0.7 V supply voltage and a clock frequency of 2GHz at room temperature.

For the STAHL, 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 the HP-STAHL, transistors aspect ratios were set as follows: W/L = 1 for both PMOS and NMOS transistors in inverters I0, I1, multiplexers MUX0 and MUX1, and transmission gates TG2 and TG3. W/L = 4 for the PMOS transistors and W/L = 2 for the NMOS transistors in 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 [19] in the SPICE simulation.

9.1. Basic Statistics of Latch Cells

Table 9-1 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 transistor number is relative to the area overhead of a latch design. Power-delay (average delay) product (PDP) shows the performance of a latch design.

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 supply voltage. Input buffer and output load are added to calculate their D - Q delay and CK - Q delay.

Setup time is the amount of time that the input of a flip-flop is required to be stable before a rising clock edge. The setup time represents the D - Q delay of the master latch

of a flip-flop. Hold time is the amount of time that the input data of a flip-flop becomes stable after a rising clock edge. This hold time represents the CK - Q delay of the slave latch of a flip-flop. The setup time of the STAHL and the HP-STAHL are 33.57ps and 6.72ps, respectively. The hold time of the STAHL and the HP-STAHL are 37.23ps and 9.40ps, respectively.

In the physical world, it is difficult to measure 1ps (picosecond). However, SPICE simulation tool does not have this difficulty, which is because SPICE is a simulator software. Different domains of parameters can be applied to solve the nonlinear differential equations in the simulator software [82, 83].

Dynamic power includes two portions: the power consumption of switching transistors and the power consumption of charging/discharging metal wire capacitances. For calculating the dynamic power of a latch, an input pattern of "01010101…" can be applied to change the stored logic value of a latch with the switching of clock cycles. Static power is due to the leakage current while a circuit is at its idle mode (no switching activity). For calculating the static power of a latch, the all-0 (all-1) pattern can be applied. For power consumption results shown in the table, dynamic power and static power are both considered by assuming an input pattern of "00110011…".

Table 9-1 Basic statistics of latch cells

Latch	#Tran.	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 [18]	28	63.16	76.93	70.05	0.58	40.63
HLR [19]	24	4.91	6.94	5.93	0.10	0.59
HLR-CG2 [19]	24	4.81	6.34	5.58	0.11	0.61
ISEHL [20]	24	9.65	12.91	11.28	0.33	3.72
HiPeR [21]	18	9.27	12.07	10.67	0.24	2.56
STAHL	40	33.57	37.23	35.40	0.41	14.51
HP-STAHL	28	6.72	9.40	8.06	0.16	1.28

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, thus TMR has the highest power consumption. The remaining 5 latches are state-of-the-art hardened latch designs. The STAHL and the HP-STAHL are the scan-test-aware latch designs. 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 speed, less area overhead, 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. HP-STAHL is proposed to achieve high propagation speed and high performance. The

proposed HP-STAHL has a much lower D - Q delay and CK - Q delay than the STAHL as well as a standard latch. The power consumption of HP-STAHL is a little higher than a standard latch but much less than the STAHL. The PDP result of HP-STAHL is similar to a standard latch. Hence, the HP-STAHL has high performance.

9.2. Soft-Error Tolerability Evaluation

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 impact on the output values, the internal sensitive nodes can be classified into three types [21]:

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 [21, 30-32].

$$I(t) = \frac{Q}{\tau_f - \tau_r}\left(e^{-\frac{t}{\tau_f}} - e^{-\frac{t}{\tau_r}}\right) \qquad (9.1)$$

In Eq. (9.1), $I(t)$ denotes transient current pulse; Q denotes the total deposited charge; τ_f denotes collection time constant, which is the falling time of the current pulse; τ_r denotes ion track establishment constant, which is the rising time of the current pulse. The parameters τ_f and τ_r depend on the technology [33]. In the following simulations, we use the values of $\tau_f = 20ps$ and $\tau_r = 5ps$ [32].

As shown in Figure 9.1, 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. Similar results for the nodes N9, N10, and Q1 can be obtained.

As shown in Figure 9.2, SEUs were injected into the internal node N1 of the STAHL. The logic value of N1 was changed. The SEUs at node N1 will not propagate to outputs Q0 and Q1. The Q0 and Q1 remain correct. Similar simulation results for the nodes N2, N3, N4, N5, N6, N7, and N8 can be obtained.

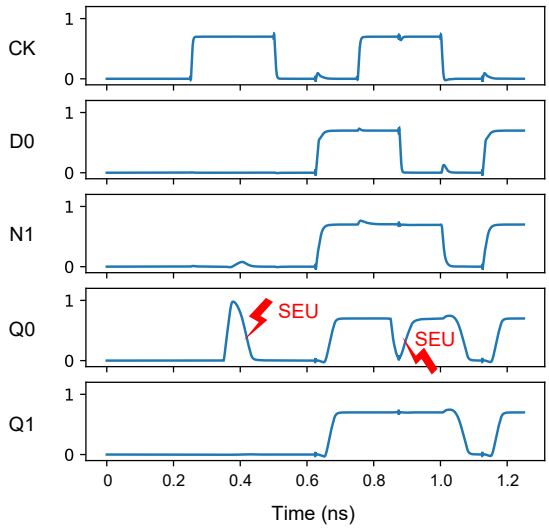


Figure 9.1 Impact of SEUs on Q0 of STAHL.

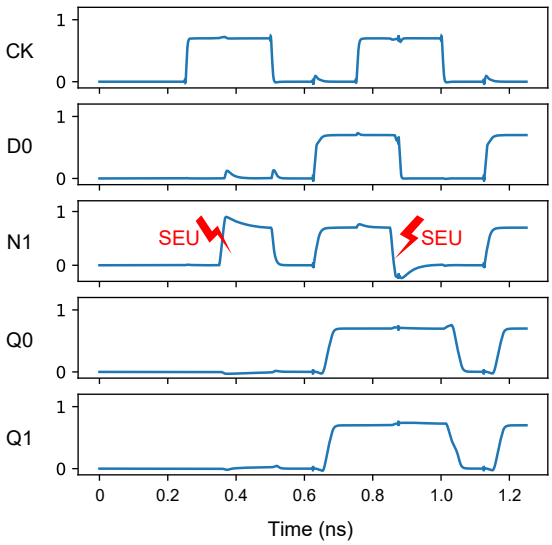


Figure 9.2 Impact of SEUs on N1 of STAHL.

As shown in Figure 9.3, SEUs were injected into the internal node N1 (output node of the C-element CE0) of the HP-STAHL. The logic value of N1 was changed and the SEUs at node N1 will propagate to output Q0. This feedback loop cannot correct this corrupted logic value because the corrupted logic at Q0 will keep the CE0 at a high-

impedance state and stop it from driving its output. Hence, node N1 is a Type-3 node, which means that it cannot be corrected once it is corrupted. There are two Type-3 nodes in the HP-STAHL and the other Type-3 node is node N2.

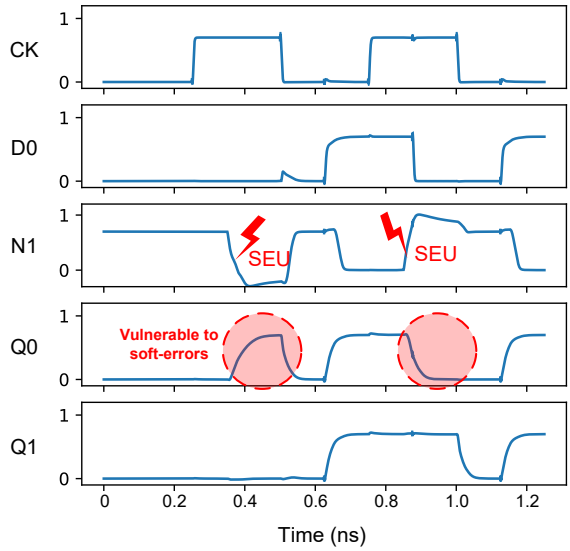


Figure 9.3 Impact of SEUs on N1 of HP-STAHL.

As shown in Figure 9.4, SEUs were injected into the internal node N3 of the HP-STAHL. The logic value of N3 is changed and the SEUs at node N3 will propagate to outputs Q0. However, this corrupted value at node N3 will be corrected eventually. Node N3 is a type-2 node, which means that it can correct the corrupted logic values. Similar simulation results for the nodes N3, N4, N5, N6, Q0, and Q1 can be obtained.

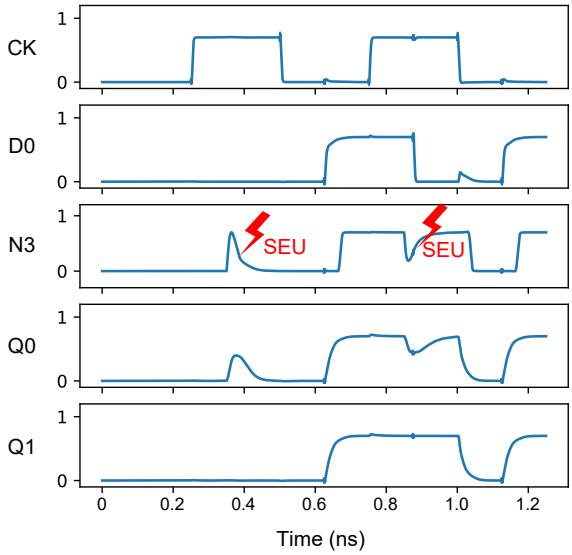


Figure 9.4 Impact of SEUs on N3 of HP-STAHL.

Table 9-2 shows the soft-error vulnerability (SEV) of all considered latches, their count of internal nodes, their count of Type-1, their count of Type-2, their count of Type-3, and their critical charge Q_{crit}, respectively.

Table 9-2 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 [18]	0.0	14	12	2	0	0.7
HLR [19]	0.0	13	12	1	0	0.5
HLR-CG2 [19]	0.0	16	15	1	0	0.5
ISEHL [20]	0.0	15	14	1	0	0.5
HiPeR [21]	0.0	9	8	1	0	0.4
STAHL	0.0	16	12	4	0	0.8
HP-STAHL	16.0	12	0	10	2	0.5

The standard latch shows a SEV of 60% because it is an unhardened latch and has 3 Type-3 nodes of all 5 nodes. The HP-STAHL shows a SEV of 16% because it has 2 Type-3 nodes of all 12 nodes. The HP-STAHL achieves high-performance and high testability by compromising part of its soft-error tolerability, which is the two Type-3 nodes and a critical charge of $Q_{crit} = 0.5$fC was estimated by SPICE simulation for such two nodes. For the proposed HP-STAHL, there are 10 Type-2 internal nodes, and its critical charge is higher than 0.5fC according to SPICE simulation. 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.

9.3. Defect Coverage and *PTVF* of Single Latches

This section compares the STAHL and the HP-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 [74] 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 defects includes 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 [75, 76]. 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 was classified into external and internal ones. For STAHL, external nets are D, GND, VDD, CK, $\overline{CK}$, SE, and $\overline{SE}$, while internal nets are the remaining nets as shown in the STAHL structure in Figure 5.1. As for the HP-STAHL, 28 transistor open defects were considered, and the short defects is the same as the STAHL. For HP-STAHL, external nets are D, GND, VDD, CK, $\overline{CK}$, SE, and $\overline{SE}$, while internal nets are the remaining nets as shown in the HP-STAHL structure in Figure 7.1.

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 [75], 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. As for the HP-STAHL, a total of 173 defects were considered, including 28 transistor open defects and 145 net short defects. The other latches were simulated in the same way. Table 9-3 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.

Table 9-3 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 [18]	5	14	184	60.3	13.8
HLR [19]	5	13	162	45.6	23.8
HLR-CG2 [19]	5	16	219	39.7	11.7
ISEHL [20]	5	15	199	50.7	19.1
HiPeR [21]	5	9	94	31.9	28.6
STAHL	7	16	271	85.6	9.2
HP-STAHL	7	10	173	81.5	22.1

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

its DC is a little lower than a standard latch.

Post-Test Vulnerability Factor (*PTVF*) is used to evaluate the soft-error vulnerability of test-escaped defective hardened latch 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. The *PTVF* of HP-STAHL is better than standard latch, HiPeR [21], and HLR [19], but worse than the rest considered latches.

9.4. Defect Coverage of Latch Based Scan Cells in Scan Test

This experiment was conducted to demonstrate the testability of an STAHL-based scan cell and an HP-STAHL-based scan cell in scan tests. A scan chain with three STAHL-based scan cells (see Figure 6.2) was simulated in SPICE simulation. Also, it is the same for a scan chain with three HP-STAHL-based scan cells (see Figure 8.2).

All possible open defects and short defects between internal nets were injected one by one into the second STAHL-based scan cell (Scan Cell 2 in Figure 6.2). It is the same setup for the second HP-STAHL-based scan cell (Scan Cell 2 in Figure 8.2). 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 Subsection 6.3, an open defect was modeled by a resistor of 1MΩ [75, 76] at the source of a transistor and a short defect was modeled by a resistor of 1Ω [75] between two nets.

For each defect in the second STAHL-based scan cell, the test procedure of a scan chain in Figure 6.7 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 in Figure 6.7 were correctly observed at S3.

For each defect in the second HP-STAHL-based scan cell, the test procedure of a scan chain in Figure 8.7 was executed and the scan-out signal was observed. For the HP-STAHL-based scan chain, the test was considered to pass if all response bits from Fa to R'1 in Figure 8.7 were correctly observed at S3.

For scan chains based on other latches, only the bits from Fa to Ff in Figure 8.7 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 9-4 shows the test results for scan chains based on standard latches, TMR latches, other hardened latches, and the proposed STAHLs, and the proposed HP-STAHLs.

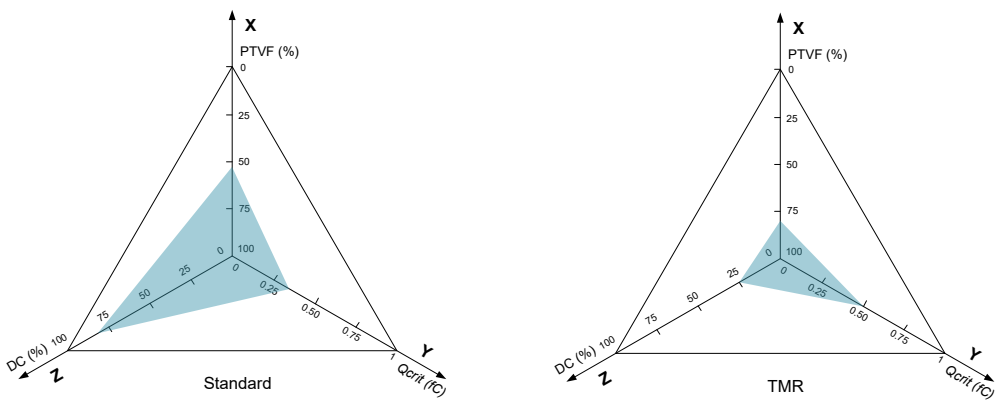
Table 9-4 Defect coverage (DC) of scan cells

Scan Cell	#Defect	#Detected	#Undetected	*DC* (%)
Standard-based	244	185	59	75.8
TMR-based	902	287	615	31.8
FERST [18]-based	807	456	351	56.5
HLR [19]-based	724	300	424	41.4
HLR-CG2 [19]-based	961	346	615	36.0
ISEHL [20]-based	878	380	498	43.3
HiPeR [21]-based	452	216	236	47.8
STAHL-based	1227	957	270	78.0
HP-STAHL-based	776	599	177	77.2

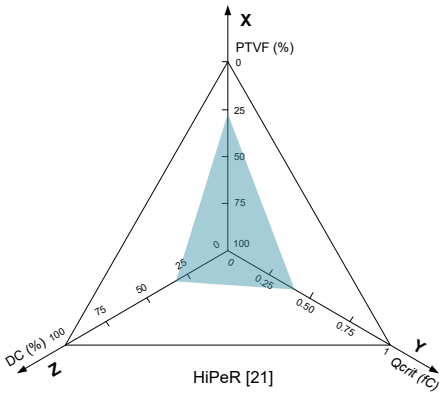
The standard-latch-based scan cell shows a DC of 75.8%. As expected, the DC of the TMR-latch-based scan cell is the lowest (31.8%). The STAHL-based scan cell achieves a DC of 78.0%, which is the best among all compared latch-based scan cells. The HP-STAHL-based scan cell achieves a defect coverage of 77.2%, which is the second best among all compared latch-based scan cells. Therefore, we can conclude that the STAHL-based scan cell and the HP-STAHL-based scan cell provide significantly better testability than any other hardened latch.

9.5. Overall Comparison

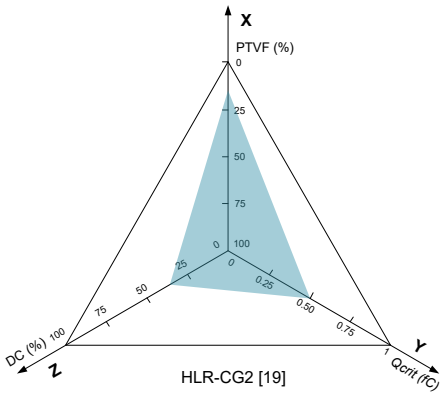
Figure 9.5 shows the overall comparison. The percentage of *PTVF* from 100% to 0% is shown on the X-axis. 100% of *PTVF* represents the worst value and 0% represents the best value. The critical charge (Q_{crit}) ranges from 0fC to 1fC on the Y-axis. A higher critical charge means that the Type-2 node is more robust. The Z-axis shows defect coverage (DC), which ranges from 0% to 100%. A higher DC value is better. The colored triangle shows the overall comparison result.



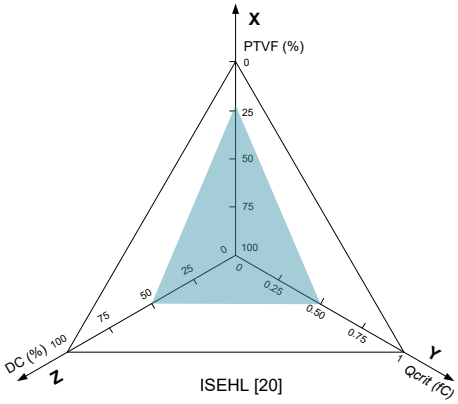
(a) (b)


X
PTVF (%)
0
25
50
75
100
0
25
50
75
100
DC (%)
Z
0
0.25
0.50
0.75
1
Y
Qcrit (fC)
HiPeR [21]

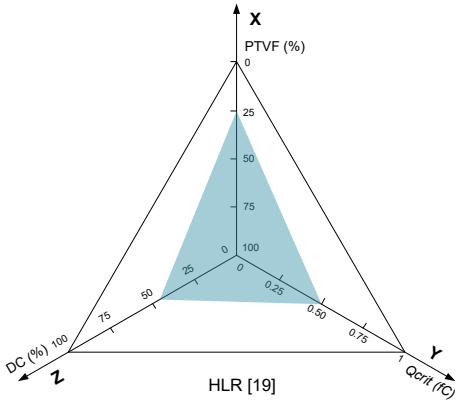
(c)


X
PTVF (%)
0
25
50
75
100
0
25
50
75
100
DC (%)
Z
0
0.25
0.50
0.75
1
Y
Qcrit (fC)
HLR-CG2 [19]

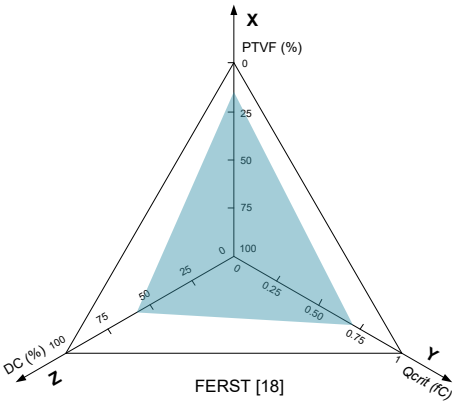
(d)


X
PTVF (%)
0
25
50
75
100
0
25
50
75
100
DC (%)
Z
0
0.25
0.50
0.75
1
Y
Qcrit (fC)
ISEHL [20]

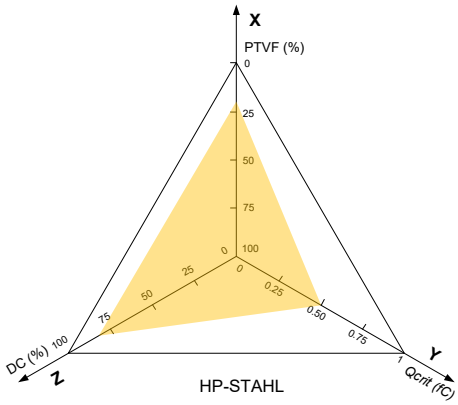
(e)


X
PTVF (%)
0
25
50
75
100
0
25
50
75
100
DC (%)
Z
0
0.25
0.50
0.75
1
Y
Qcrit (fC)
HLR [19]

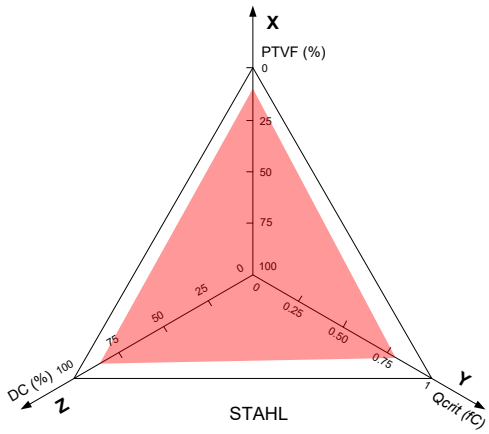
(f)


X
PTVF (%)
0
25
50
75
100
0
25
50
75
100
DC (%)
Z
0
0.25
0.50
0.75
1
Y
Qcrit (fC)
FERST [18]

(h)


X
PTVF (%)
0
25
50
75
100
0
25
50
75
100
DC (%)
Z
0
0.25
0.50
0.75
1
Y
Qcrit (fC)
HP-STAHL

(i)



(j)

Figure 9.5 Overall comparison of latch cells.

We introduce a DC-$PTVF$-Q_{crit} product (DPQP) to quantify the comparison results. Eq. (9.2) shows the DPQP equation.

$$DPQP = DC \cdot (1 - PTVF) \cdot Q_{crit} \qquad (9.2)$$

Table 9-5 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 STAHL shows the highest DPQP, which shows that the STAHL has the best overall comparison result. The FERST [18] latch shows the second-best DPQP. The HP-STAHL shows the third best of DPQP due to its compromising at the soft-error tolerability part. However, the delay and the power consumption of HP-STAHL are much less than the FERST [18] and STAHL. 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.

Table 9-5 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
HP-STAHL	317

9.6. Applicability Comparison

For the applicability comparison, we compare the STAHL and the HP-STAHL with the standard latch and the TMR latch. It is because the standard latch is widely used in conventional applications and the TMR latch is a commonly used hardened latch design in high radiation environments. Table 9-6 shows the comparison results, including the name of the latches, transistor numbers, an average delay (average of the D - Q delay and the CK - Q delay in Table 9-1), power consumption, power-delay (average delay) product (PDP), defect coverage (DC), and *PTVF*, respectively.

Table 9-6 Applicability comparison results

Latch	#Tran.	Average Delay (ps)	Power (μW)	PDP ($10^{-18}J$)	*DC* (%)	*PTVF* (%)
Standard	12	12.94	0.09	1.16	83.3	54.2
TMR	48	37.61	0.61	22.94	25.1	20.3
STAHL	40	35.40	0.41	14.51	85.6	9.2
HP-STAHL	28	8.06	0.16	1.28	81.5	22.1

Standard latch has the lowest transistor number, which is relative to its area overhead. At the same time, it has no cell-internal redundancy and has high defect coverage. If a soft-error causes a malfunction of a personal computer, this malfunction can be solved by rebooting this personal computer. Thus, the standard latch is widely applied in conventional applications, such as personal computers, video games, etc. However, it is a different story for mission-critical applications, such as medical devices, autonomous cars, and satellites. A soft-error-caused malfunction in these mission-critical applications may lead to a disaster. This is the reason that hardened latch design is widely applied in mission-critical applications.

The STAHL has the best defect coverage and *PTVF* results when compared with all considered latch designs, which shows that the STAHL has high reliability. The power consumption and the propagation delay of the STAHL are lower than a TMR latch. The disadvantage of the STAHL is that it has higher power consumption and propagation delay than a standard latch. The HP-STAHL can compensate for the disadvantage of the STAHL and the HP-STAHL has the lowest propagation delay. The HP-STAHL has similar PDP and DC results as a standard latch. The disadvantage of the HP-STAHL is that it has a higher *PTVF* result, which is similar to a TMR latch.

9.7. Summary

In this chapter, the experimental results of the STAHL, the HP-STAHL and some existing hardened latches are compared, including basic statistics, defect coverage, *PTVF*, soft-error tolerability, and applicability. The STAHL is better than the other

latches in defect coverage, soft-error tolerability, *PTVF,* and reliability. The HP-STAHL is better than the other latches in propagation delay. The defect coverage and the PDP of the HP-STAHL are similar to the standard latch. If an application requires high performance and soft-error tolerability, the HP-STAHL is a good option. If an application requires high reliability, the STAHL is a good option. The STAHL and the HP-STAHL both have good defect detectability due to their scan-test-aware design.

10. Conclusions and Future Works

10.1. Conclusions

This is the first research that bridges the hardened latch design research field and defect detection research field. This research is the first to observe that defects can impact the soft-error tolerability of hardened latch designs and it is the beginning of a brand-new research area.

In Chapter 1, an example is shown to indicate the impact of defects on hardened latches, which may cause two problems: **Problem-1** of low testability of hardened latches and **Problem-2** of defects reducing the reliability of hardened latches. Chapter 2 introduces the background of this research about soft-errors and defects and Chapter 3 shows the related works of soft-error tolerance methods and detection methods. In this research, these problems are solved by the following five major contributions:

Contribution-1: A first-of-its-kind metric for quantifying the impact of defects on hardened latches, called Post-Test Vulnerability Factor (*PTVF*). **Problem-2** is solved by this first major contribution. Chapter 4 shows this Post-Test Vulnerability Factor (*PTVF*), which helps to analyze the impact of defects on the soft-error tolerability of hardened latches. In this chapter, the flow of calculation *PTVF* is introduced.

Contribution-2: A novel design called Scan-Test-Aware Hardened Latch (STAHL) that provides the highest defect coverage in comparison with all existing hardened latches. **Problem-1** is solved by using STAHL to build a scan cell to perform a scan test. Chapter 5 shows a novel Scan-Test-Aware Hardened Latch (STAHL) design, which can tolerate SEUs and has high defect coverage. The 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 the defect coverage of STAHL 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.

Contribution-3: A novel scan test procedure is proposed to solve **Problem-1** by fully testing the STAHL-based scan cell. Chapter 6 shows the STAHL-based scan chain structure and the detailed test procedure for testing a STHAL-based scan chain.

Contribution-4: A novel High-Performance Scan-Test-Aware Hardened Latch (HP-STAHL) design can also solve **Problem-1** and has similar defect coverage as STAHL but has lower power consumption and higher propagation speed. Chapter 7 shows a novel High Performance Scan-Test-Aware Hardened Latch (HP-STAHL) design, which also can tolerate most SEUs and has high defect coverage. Same as the STAHL, HP-

STAHL also has two modes: functional and shift. In functional mode, it can tolerate most SEUs. In shift mode, most cell-internal production defects become detectable. Simulation results have shown that the defect coverage of HP-STAHL is 81.5%, which is a little lower than the STAHL but still much higher than all compared hardened latch designs. HP-STAHL has a low cost in propagation delay and power consumption. The $PTVF$ of HP-STAHL is 22.1%.

Contribution-5: A novel scan test procedure is proposed to fully test the HP-STAHL-based scan cell to solve **Problem-1**. Chapter 8 shows the HP-STAHL-based scan chain structure and the detailed test procedure for testing an HP-STHAL-based scan chain.

Chapter 9 shows the evaluation results, which show that both STAHL and HP-STAHL have high defect coverage and can be used to tolerate soft-errors.

10.2. Future Works

The used 16nm predictive technology model [75] is based on planar MOSFETs. Hence, soft-error injection models and fault models for defects are based on the planar MOSFETs. If the STAHL and the HP-STAHL are constructed by FinFETs, they can also achieve high soft-error tolerability and good defect detectability. It is because the basic idea of the STAHL and the HP-STAHL is independent of the transistor structure. For further evaluating the applicability of the STAHL and the HP-STAHL at FinFET technology nodes, I plan to use a FinFET-based predictive technology model, FinFET-based soft-error injection models, and FinFET-based fault models in the future.

Apart from the considered transistor open defects and short defects between internal nets in a latch, some other types of defects are also needed to be considered, including port open defects, fin-open defects (FinFET), gate-open defects (FinFET), and fin-short defects (FinFET) [80, 81].

Multiple-node upset (MNUs) in latches are also needed to be considered in the future [4]. Tolerating MNUs requires more redundancy, which will increase the difficulty to detect defects in them. At the same time, the added redundancy may reduce the impact of defects on the soft-error tolerability of hardened latches. It is important to achieve a balance between soft-error tolerability and detect detectability.

In future work, I plan to apply the two proposed hardened latch designs (the STAHL and the HP-STAHL) to detect aging-related defects by performing built-in self-test (BIST). For mission-critical applications, performing in-system BIST to detect aging-related defects is essential to maintain their reliability.

10.3. Summary

This chapter concludes this thesis and introduces future works. This research

bridges two different research fields: hardened latch design and defect detection research field. This research is the first research to analyze, detect, and evaluate defects in hardened latches and it is the beginning of a new research area. Comprehensive simulation results demonstrate the applicability of the STAHL and the HP-STAHL. The two proposed hardened latch designs can be applied in mission-critical applications, such as medical devices, autonomous cars, satellites, etc.

Bibliography

[1] G. Moore, "Cramming More Components onto Integrated Circuits," *Electronics,* vol. 38, no. 8, pp. 114-117, Apr. 1965.

[2] R. Baumann, "Soft Errors in Advanced Computer Systems," *IEEE Design & Test of Computers*, vol. 22, no. 3, pp. 258-266, May-Jun. 2005.

[3] 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.

[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 and Systems*, vol. 67, no. 12, pp. 4684-4695, Dec. 2020.

[5] H. Köksal,N. Demir, and A. Kilcik, "Analysis of the Cosmic Ray Effects on Sentinel-1 SAR Satellite Data," *Aerospace*, vol. 8, no. 3, pp. 62-73, Mar. 2021.

[6] N. Ya'acob, A. Zainudin, R. Magdugal, and N. Naim, "Mitigation of Space Radiation Effects on Satellites at Low Earth Orbit (LEO)," *Proc. IEEE International Conference on Control System, Computing and Engineering (ICCSCE),* Penang, Malaysia, pp. 56-61, Jun. 2016.

[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.

[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.

[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.

[10] G. Hubert, L. Artola, and D. Regis, "Impact of Scaling on the Soft Error Sensitivity of Bulk, FDSOI and FinFET Technologies Due to Atmospheric Radiation," *Elsevier Integration of the VLSI Journal*, vol. 50, pp. 39-47, Jan. 2015.

[11] J. Noh, V. Correas, S. Lee, J. Jeon, I. Nofal, J. Cerba, H. Belhaddad, D. Alexandrescu, Y. Lee, and S. Kwon, "Study of Neutron Soft Error Rate (SER) Sensitivity: Investigation of Upset Mechanisms by Comparative Simulation of FinFET and Planar MOSFET SRAMs," *IEEE Trans. Nucl. Sci.*, vol. 62, no. 4, pp. 1642-1649, Aug. 2015.

[12] 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.

[13] 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, Apr. 2009.

[14] 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.

[15] 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.

[16] 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.

[17] M. Omana, D. Rossi, and C. Metra, "Latch Susceptibility to Transient Faults and New Hardening Approach," *IEEE Trans. Computers*, vol. 56, no. 9, pp. 1255-1268, Aug. 2007.

[18] 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.

[19] H. Nan and K. Choi, "High Performance, Low Cost, and Robust Soft Error Tolerant Latch Designs for Nanoscale CMOS Technology," *IEEE Trans. Circuits and Syst. I: Reg. Papers*, vol. 59, no. 7, pp. 1445-1457, Jul. 2012.

[20] 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.

[21] M. Omana, D. Rossi, and C. Metra, "High-Performance Robust Latches," *IEEE Trans. Comput*ers, vol. 59, no. 11, pp. 1455-1465, Nov. 2010.

[22] J. Furuta, K. Kobayashi, and H. Onodera, "An Area/Delay Efficient Dual-Modular Flip-Flop with Higher SEU/SET Immunity," *IEICE Trans. Electronics*, vol. E93-C, no.2, pp. 340-346, Mar. 2010.

[23] 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 and Mater. Reliab.,* vol. 14, no. 1, pp. 333-343, Mar. 2014.

[24] 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. Electronics*, vol. E89C, no. 3, pp. 384-391, Mar. 2006.

[25] 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. Computers*, vol. 69, no. 6, pp. 789-799, Jun. 2020.

[26] J. Ziegler, "Terrestrial Cosmic Rays," *IBM Journal Research and Development* vol. 40, no. 1, pp.19-39, Jan. 1996.

[27] C. Schrijver and A. Title, "On the Formation of Polar Spots in Sun-like Stars," *The Astrophysical Journal*, vol. 551, no. 2, pp.1100-1100, Apr. 2002.

[28] A. Masuda, M. Ishikawa, M. Kohinata, M. Mashima, K. Tsuji, and T. Shinkawa, "Development of Immersion SN Plating Process for Low-Alpha Bump Formation," *Proc. Electron. Components Technol. Conf.,* pp. 1654-1658, May 2008.

[29] M. Gordon, K. Rodbell, H. Tang, P. Ronsheim, Z. Zhu, S. Rauch, B. McNally, and S. Coleman, "Ultra-Low Emissivity Alpha-Particle Detection," *IEEE Trans. Nucl. Sci.*, vol. 59, pp. 3101-3109, Dec. 2012.

[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.

[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 Int. Syst.*, vol. 18, no. 9, pp. 1265-1276, Sept. 2010.

[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, Jul. 2006.

[33] 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.

[34] L. Drury, "Origin of Cosmic Rays," *Astroparticle Physics*., vol. 39-40, no. 6, pp. 52-60, Dec. 2012.

[35] "In-flight upset, 154 km west of Learmonth, WA, 7 October 2008, VH-QPA, Airbus A330-303," Australian Transport Safety Bureau. 14th, Nov. 2008.

[36] A. Cloudberg, "Ghosts in the Code: The Near Crash of Qantas Flight 72," Web. 20th, Oct. 2019. https://admiralcloudberg.medium.com/ghosts-in-the-code-the-near-crash-of-qantas-flight-72-b4faebc90e27

[37] P. Koopman, "A Case Study of Toyota Unintended Acceleration and Software Safety." *Keynote*, 14th, Nov. 2014.

[38] F. Becky, "How Space Weather Can Influence Elections on Earth," Web. 18th, Feb. 2017. https://www.vice.com/en/article/9agbxd/space-weather-cosmic-rays-voting-aaas

[39] G. Burtt, "How an Ionizing Particle from Outer Space Helped a Mario Speed Runner Save Time," Web. 16th, Sep. 2020. https://www.thegamer.com/how-ionizing-particle-outer-space-helped-super-mario-64-speedrunner-save-time/

[40] M. Zhang and N. Shanbhag, "Soft-Error-Rate-Analysis (SERA) Methodology," *IEEE Trans. Comput.-Aided Design of Int. Circuits and Syst.*, vol. 25, no. 10, pp. 2140-2155, Oct. 2006.

[41] 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.

[42] C. Pan, R. Baert, I. Ciofi, Z. Tokei, and A. Naeemi, "System-Level Variation Analysis for Interconnection Networks at Sub-10-nm Technology Nodes Using Multiple Patterning Techniques," *IEEE Trans. Electron Devices*, vol. 62, no. 7, pp. 2071-2077, Jul. 2015.

[43] S. Demuynck, C. Huffman, M. Claes, S. Suhard, J. Versluijs, H. Volders, N. Heylen, K. Kellens, K. Croes, H. Struyf, G. Vereecke, and P. Verdonck, "Integration and Dielectric Reliability of 30 nm Half Pitch Structures in Aurora (R) LK HM," *Japanese Journal of Applied Physics*, vol. 49, no. 4, pp. 04DB01-04DB05, Jul. 2010.

[44] Y. Ma, J. Sweis, C. Bencher, H. Dai, Y. Chen, J. Cain, Y. Deng, J. Kye, and H. Levinson, "Decomposition Strategies for Self-Aligned Double Patterning," *Proc. Design for Manufacturability through Design-Process Integr. IV*, vol. 7641, pp. 76410T-1-76410T-13, Apr. 2010.

[45] J. Lienig and M. Thiele, "Fundamentals of Electromigration-Aware Integrated Circuit Design," Springer, 2018.

[46] L. Wang, C. Wu, and X. Wen, "VLSI Test Principles and Architectures," Morgan Kaufmann, San Francisco, Jul. 2006.

[47] M. Nicolaidis, "Soft Errors in Modern Electronic Systems," Springer New York Heidelberg Dordrecht London, 2011.

[48] 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.

[49] C. Hawkins, J. Soden, R. Fritzemeier, and L. Horning, "Quiescent Power Supply Current Measurement for CMOS IC Defect Detection," *IEEE Trans. Industrial Electronics*, vol. 36, no. 2, pp. 211-218, May 1989.

[50] C. Chen and M. Hsiao, "Error-Correcting Codes for Semiconductor Memory Applications: A State-of-the-Art Review," *IBM Journal Research Development.,* vol. 28, no. 2, pp. 124-134, Mar. 1984.

[51] S. Krishnan, R. Panigrahy, and S. Parthasarathy, "Error-Correcting Codes for Ternary Content Addressable Memories," *IEEE Trans. Computers,* vol. 58, no. 2, pp. 275-279, Feb. 2009.

[52] P. Reviriego, S. Liu, O. Rottenstreich, and F. Lombardi, "Two Bit Overlap: A Class of Double Error Correction One Step Majority Logic Decodable Codes," *IEEE Trans. Computers,* vol. 68, no. 5, pp. 789-803, May 2019.

[53] C. Fuchs, P. Chou, X. Wen, N. Murillo, G. Furano, S. Holst, A. Tavoularis, S.-K. Lu, A. Plaat, and K. Marinis, "A Fault-Tolerant MPSoC For CubeSats," *Proc. IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT),* Oct. 2019.

[54] E. Cheng, S. Mirkhani, L. Szafaryn, C. Cher, H. Cho, K. Skadron, M. Stan, K. Lilja, J. Abraham, P. Bose, and S. Mitra, "Tolerating Soft Errors in Processor Cores Using CLEAR (Cross-Layer Exploration for Architecting Resilience)," *IEEE Trans. Computer-Aided Design of Integrated Circuits and Systems,* vol. 37, no. 9, pp. 1839-1852, Sep. 2018.

[55] H. Lee, K. Lilja, M. Bounasser, P. Relangi, I. R. Linscott, U. S. Inan and S. Mitra, "LEAP: Layout Design through Error-Aware Transistor Positioning for Soft-Error Resilient Sequential Cell Design," *Proc. IEEE Reliability Physics Symposium (IRPS),* May 2010.

[56] K. Lilja, M. Bounasser, S. J. Wen, R. Wong, J. Holst, N. Gaspard, S. Jagannathan, D. Loveless and B. Bhuva, "Single-Event Performance and Layout Optimization of Flip-Flops in a 28-nm Bulk Technology," *IEEE Trans. Nuclear Science,* vol. 60, no. 4, pp. 2782-2788, Aug. 2013.

[57] L. Spainhower and T. Gregg, "IBM S/390 Parallel Enterprise Server G5 Fault Tolerance: A Historical Perspective," *IBM Journal of Research and Development,* vol. 43, no. 5.6, pp. 863-873, Sep. 1999.

[58] J. Lu, "Watchdog Processors and Structural Integrity Checking," *IEEE Trans. Computers,* vol. C-31, no. 7, pp. 681-685, Jul. 1982.

[59] A. Meixner, M. Bauer and D. Sorin, "Argus: Low-Cost, Comprehensive Error Detection in Simple Cores," *IEEE Micro.*, vol. 28, no. 1, pp. 52-59, Mar. 2008.

[60] M. Imhof, H. Wunderlich, and C. Zoellin, "Integrating Scan Design and Soft Error Correction in Low-Power Applications," *Proc. IEEE Int. On-Line Testing Symp*., pp. 59-64, 2008.

[61] A. Hwang, I. Stefanovici, and B. Schroeder, "Cosmic Rays Don't Strike Twice: Understanding the Nature of DRAM Errors and the Implications for System Design," *ACM SIGARCH Notices*, vol. 47, no. 4, pp. 111-122, Apr. 2012.

[62] Ruijun Ma, Stefan Holst, Xiaoqing Wen, Aibin Yan, and Hui Xu, "A Novel High Performance Scan-Test-Aware Hardened Latch Design," *Proc. IEEE Workshop on RTL and High Level Testing,*

Paper. 2.2, Nov. 2020.

[63] C. Savant, M. Roden, and G. Carpenter, "Electronic Design: Circuits and Systems," Benjamin-Cummings Pub. Co., 1991.

[64] N. Seifert, B. Gill, S. Jahinuzzaman, J. Basile, V. Ambrose, Q. Shi, R. Allmon and A. Bramnik, "Soft Error Susceptibilities of 22 nm Tri-Gate Devices," *IEEE Trans. Nucl. Sci.*, vol. 59, no. 6, pp. 2666- 2673, Dec 2012.

[65] B. Gill, N. Seifert and V. Zia, "Comparison of Alpha-Particle and Neutron Induced Combinational and Sequential Logic Error Rates at the 32nm Technology Node," *Proc. IEEE Int'l Reliability Physics Symposium*, Apr. 2009.

[66] A. Kermode, "Mechanics of Flight," (8th edition), Pitman Publishing Limited, London, 1972.

[67] A. Jee and F. Ferguson, "Carafe: An Inductive Fault Analysis Tool for CMOS VLSI Circuits," *Proc. IEEE VLSI Test Symp.*, pp. 92-98, Apr. 1993.

[68] 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.

[69] 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.

[70] M. Bushnell and V. Agrawal, "Essentials of Electronic Testing for Digital, Memory and Mixed-Signal VLSI Circuits," *Springer Science,* New York, 2000.

[71] N. Jha and S. Gupta, "Testing of Digital Systems," *Cambridge University Press,* London, 2002.

[72] C. L. Chen and M. Y. Hsiao, "Error-Correcting Codes for Semiconductor Memory Applications: A State-of-the-Art Review," *IBM Journal Research. Development*, vol. 28, pp. 124-134, Mar. 1984.

[73] T. Rao, "A Generalization of the Single B-Bit Byte Error Correcting and Double Bit Error Detecting Codes for High-Speed Memory Systems," *IEEE Trans. Computer*, vol. 45, pp. 508-511, Apr. 1996.

[74] R. Helinski and J. Plusquellic, "Measuring Power Distribution System Resistance Variations," *IEEE Trans. Semiconductor Manufacturing,* vol. 21, no.3, pp. 444-453, Aug. 2008.

[75] Predictive Technology Model for Spice, [Online]. http://ptm.asu.edu/

[76] 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.

[77] 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.

[78] 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.

[79] D. Binder, E. Smith, and A. Holman, "Satellite Anomalies from Galactic Cosmic Rays," *IEEE Trans. Nucl. Sci.*, vol. 22, no. 6, pp. 2675- 2680, Dec. 1975.

[80] F. Mesalles, H. Villacorta, M. Renovell, and V. Champac, "Behavior and Test of Open-Gate Defects in FinFET Based Cells," *Proc. IEEE Euro. Test Symp.*, May 2016.

[81] F. Forero, J. Galliere, M. Renovell, and V. Champac, "Analysis of Short Defects in FinFET Based Logic Cells," *Proc. IEEE Latin American Test Symp.*, Mar. 2017.

[82] S. Mandal, "Some Important Simulation Software Tools for a Student of Electronics Engineering," *Global Journal on Advancement in Engineering and Science (GJAES)*, vol. 3, no. 1, pp. 1-8, 2017.

[83] L. Nagel and D. Pederson, "SPICE (Simulation Program with Integrated Circuit Emphasis)," *Technical Report*, no. ERL-M382, Apr. 2017.

Acknowledgements

It is a great honor to gratitude all those people who helped me during my Ph. D. course.

First, I would like to give my deepest appreciation to Prof. Xiaoqing Wen at Kyushu Institute of Technology for providing me with a valuable opportunity as a Ph. D. student at his laboratory.

I would like to thank Prof. Xiaoqing Wen and Prof. Stefan Holst for their kind instructions and inspirational suggestions during my study. They offered me not only their knowledge, experiences, and a lot of opportunities to communicate with worldwide researchers but also a lot of help when I met problems and their patience when I made mistakes. Their detailed comments and insightful advice always lead me to move on. I have learned a lot of good qualities from them. I see a fine example of an excellent researcher and an enlightening educator. Furthermore, I would like to express my sincere thanks to Prof. Aibin Yan from Anhui University and Prof. Hui Xu from Anhui University of Science and Technology for their kind help during my research.

I would like to demonstrate my gratitude to the committee for their valuable time and kind help.

I also want to thank the lab members with that we spent a lot of good time together.

Last but not least, I would like to demonstrate my gratitude for the support from my family. They provide financial and spiritual supports so that I can finish my course.

List of Publications

The publications of my doctoral research are listed below.

International Conferences

- Stefan Holst, **Ruijun Ma**, and Xiaoqing Wen, "The Impact of Production Defects on the Soft-Error Tolerance of Hardened Latches," *Proc. IEEE Euro. Test Symp.*, Paper 7A-1, May 2018.
- **Ruijun Ma**, Stefan Holst, and Xiaoqing Wen, Aibin Yan, and Hui Xu, "STAHL: A Novel Scan-Test-Aware Hardened Latch Design," *Proc. IEEE Euro. Test Symp.,* Paper 4B-2, May 2019.
- **Ruijun Ma**, Stefan Holst, Xiaoqing Wen, Aibin Yan, and Hui Xu, "A Novel High Performance Scan-Test-Aware Hardened Latch Design," *Proc. of IEEE Workshop on RTL and High Level Testing*, Paper. 2.2, Penang, Malaysia, Nov. 2020.

Journals

- **Ruijun Ma**, Stefan Holst, and Xiaoqing Wen, Aibin Yan, and Hui Xu, "Evaluation and Test of Production Defects in Hardened Latches," *IEICE Trans. info. & syst.,* vol. E105-D, no.5, pp.996-1009, May 2022.