Design techniques for safe, reliable, and trustworthy analog circuits

by

Matthew Strong

A dissertation submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Major: Electrical Engineering (Very Large Scale Integration)

Program of Study Committee:
Degang Chen, Major Professor
Randall Geiger
Nathan Neihart
Ratnesh Kumar
Zhengdao Wang

The student author, whose presentation of the scholarship herein was approved by the program of study committee, is solely responsible for the content of this dissertation. The Graduate College will ensure this dissertation is globally accessible and will not permit alterations after a degree is conferred.

Iowa State University

Ames, Iowa

2023

Copyright © Matthew Strong, 2023. All rights reserved.

TABLE OF CONTENTS

Page

LIST OF FIGURES iv

LIST OF TABLES vi

ACKNOWLEDGMENTS vii

ABSTRACT viii

CHAPTER 1. INTRODUCTION 1
- Background and Motivation 2
- Research Overview 3
- Organization of Dissertation 4

CHAPTER 2. INTEGRATING AMS CIRCUIT TESTS IN ON-CHIP SYSTEMS 6
- Defect-Oriented Testing 8
- Analog & Mixed-Signal Design-for-Test (DfT) 10
- PCB Demonstration & Measurements of Analog DfT Circuits 14
- Handling Defects in Test Circuit Components 24
- Summary 27

CHAPTER 3. MONITORING AGING WITH ONLINE MEASUREMENTS 29
- Bias & Temperature Instability 29
- Simulating and Measuring BTI 32
- Monitor for In-Field Statistical Characterization of BTI 36
  - Sizing the Transistors of the Monitor 40
  - Aging-Related Errors from Other Components 43
  - **ΔVT** Comparison and Data Conversion 45
  - Sampling BTI from Multiple Devices 48
- Discussion 49
- Summary 50

CHAPTER 4. HARDWARE TROJAN THREATS TO ANALOG CIRCUITS 51
- Threat Model 52
- Trojan Taxonomies & Detection Methods 53
- Analog Hardware Trojans 56
- PAAST Trojan Classification 59
- Summary 66

CHAPTER 5. TRIGGERING A PAAST TROJAN 67
- Coupled Oscillator Applications 67
- The Trojan Design 70
- Measurements of Trojan Activation 75
- Discussion 79

CHAPTER 6. CONCLUSIONS 81

REFERENCES 83

LIST OF FIGURES

Page

Figure 1.1. Multi-faceted research thrust for safe and reliable analog circuit function. 4

Figure 2.1. Typical failure rate of a part population after fabrication. 7

Figure 2.2. Modeling hard defects in MOSFETs. 10

Figure 2.3 Analog test PCB and FPGA board for injecting analog faults and validating BISTs. 15

Figure 2.4 Kuijk bandgap reference with window comparator for testing. 17

Figure 2.5 DfT LDO in test mode. 18

Figure 2.6 PGA schematic(a) and the amplifier's transfer curve(b). 20

Figure 2.7 Concurrent sampling method using unary data. 23

Figure 2.8 High-resolution concurrent sampling method. 23

Figure 2.9 Bandgap reference circuit with window comparator observer. 24

Figure 2.10 Gate modification that prevents observer defects from loading the circuit. 25

Figure 2.11 Switch architectures with varying resiliency to faults. 27

Figure 3.1 Threshold voltage difference circuit. 38

Figure 3.2 Proposed BTI Monitor. 39

Figure 3.3 Comparator input stage with power-disabling capability. 47

Figure 3.4 An array of aged devices compared to a reference device. 49

Figure 4.1 Production flow and points of Trojan insertion. 53

Figure 4.2 Summary of existing hardware Trojan taxonomies. 54

Figure 4.3 Widlar current reference with Trojan equilibrium. 61

Figure 4.4 Coupled ring oscillator with Trojan equilibria or Trojan limit cycle. 62

Figure 4.5 Active filter that is not input-to-state stable but has a globally stable equilibrium. 64

Figure 4.6 Jump resonance in the active filter. The blue curve plots gain for the sweep in the increasing direction and the orange curve plots gain for the decreasing direction. 64

Figure 4.7 Stability characteristics for PAAST Trojans. 66

Figure 5.1 The coupled oscillator architecture to be designed with a PAAST Trojan. 69

Figure 5.2 The coupled oscillator's feedback loops. 72

Figure 5.3 Coupled oscillator's output phase difference vs. VDD mismatch. 73

Figure 5.4 Modeling power bus delay to create trigger the Trojan. 74

Figure 5.5 A localized power supply glitch triggering the PAAST Trojan. 74

Figure 5.6 Free-running frequency vs. control voltage for the normal and Trojan limit cycles. 78

LIST OF TABLES

Page

Table 2.1 LDO input voltage measurements. 18

Table 2.2 LDO IOI test results. 18

Table 2.3 Truth table for PGA test when the input voltage requires a gain of 16. 22

Table 5.1 Measurements of the frequency and phase difference for the oscillator's nominal and Trojan function. 76

Table 5.2 Summary of if the trigger successfully activated the Trojan. 76

Table 5.3 Summary of if Trojan deactivation was successful. 78

ACKNOWLEDGMENTS

I would first like to thank my major professor, Dr. Degang Chen. His thoughtful advice and careful guidance through the years have been invaluable in my research and studies, and he helped me get the most out of my time at Iowa State. I consider myself lucky to have had such a dedicated mentor helping me make this experience one of the most rewarding of my life.

I would also like to thank Dr. Randall Geiger for his help and direction. As principal investigator in my first research project, he taught me many of the fundamental skills required in academic research. His advice as one of my committee members has been immensely helpful as well.

Thank you to my other committee members, Dr. Nathan Neihart, Dr. Ratnesh Kumar, and Dr. Zhengdao Wang. Each provided unique insights that helped me maintain perspective in my work.

The Electrical and Computer Engineering department has a wonderful and extremely helpful staff, and I want to thank them for their dedication to the students.

I was very fortunate to work with many gifted students during my journey. Our discussions and exchange of ideas have been tremendously helpful, and I am extremely grateful to my past and present colleagues.

Finally, none of this would have been possible without the support of my family who I love very much.

ABSTRACT

Rapid developments in communication, automation, and smart technologies continue to drive the trend of increasingly large-scale integration of electronics. The number of ICs embedded in various systems continues to rise to realize more sophisticated functions and capabilities, and as a result we rely more and more on the smooth, safe, and secure operation of ICs. Quality assurance of ICs is of paramount importance in critical missions because faults can incur heavy consequences. To ensure reliability, IC designs undergo a thorough verification process prior to fabrication and comprehensive testing and measurements before distribution. These steps provide confidence in parts shortly after their deployment into operation. Many critical ICs also embed functions to detect abnormal or faulty behavior in the field and add another layer of safety to the operation. The methodology for creating these built-in self-tests (BISTs) for digital circuits is fairly mature, yet analog and mixed signal (AMS) circuits still present a significant challenge for verification and testing.

The development of in-field tests for AMS circuits is relatively new. Part of the difficulty is the many constraints that define satisfactory function. Complicated signal generators and observers are usually required to stimulate the circuit and measure its response in order to accurately determine if it meets specifications. These are available in a production test environment in the form of external equipment, but the amount of hardware, power, and other resources required for these tests make it impractical for in-field operation. To address this issue, some simple, low-resource test circuits have been developed to test some fundamental AMS blocks. The test results allow one to infer faulty behavior of circuit rather than explicitly confirming specifications are not met, which makes the design of test inputs and observers significantly easier. These test circuits use simple analog-digital interfaces which aid the

integration of the designs into existing digital test architectures. The AMS test circuits were implemented on a PCB to demonstrate their feasibility.

For ICs targeting high reliability, the parts are designed such that the probability of a fault occurring is extremely low, at least for a time. BISTs for in-field testing are intended to detect faults originating from a single source because of a defect or some other unpredictable event. But every IC will reach a time when devices start to fail independently of each other because of normal wear from use. The physical mechanisms causing transistor degradation, called transistor aging, have a predictable trend for a given history of use. On-chip monitors that track device aging over the life of a part can provide warnings before widespread failure occurs and allow confident operation of IC right up to its effective end of life (EOL). A bias and temperature instability (BTI) monitor was designed to estimate the evolving probability of BTI degradation in a device or devices during its operation.

In addition to the chance of random failures in critical ICs, designers and customers must also concern themselves with intentionally induced failures. The important role these parts play in their respective systems makes them potential targets of attack by third parties whose goal is contrary to the parts' primary missions. One potential class of threats is the hardware Trojan horse, a hidden and malicious function physically embedded in the design. These are high-risk/high-reward attacks because insertion of the Trojan is generally considered difficult but successful activation is potentially devastating. Much research and resources have been dedicated to developing threat models, identifying potential means of insertion and operation, and detection of Trojans during production tests. However, these efforts are almost entirely focused on the security of digital circuits while threats to AMS circuits have been ignored. One of the main reasons for this is the inherent sensitivity of AMS circuits, which leads to the

assumption that any tampering would be obvious. This assumption falls short when a well-known problem in AMS circuit design is considered: multi-stable operation. A definitive taxonomy of this sub-class of hardware Trojans was constructed to complement existing definitions and efforts on Trojan classification. An example of an AMS circuit with such a Trojan is provided to validate the threat this class of Trojans poses.

CHAPTER 1. INTRODUCTION

Continued progress in circuit integration techniques has allowed increasingly sophisticated electronic products to be developed for use in a wide range of systems. Many systems rely on integrated circuits to perform critical functions, meaning that a failure of the IC would cause system-wide failure. With automation and smart technologies advancing, ICs are having a broader impact than ever before on day-to-day life. The growth rate of critical IC deployment makes it inevitable that faults will occur at inopportune times of operation. This is why it is necessary to add safeguards to designs that facilitate graceful failure of a system, such as a safe shutdown or giving time for manual intervention.

These ICs targeting functional safety and reliability need effective means of self-testing. The continually increasing variety of applications and scale of integration has resulted in very diverse testing methodologies and growing amount of data that must be processed to perform diagnostics. This is spurring efforts for efficient test data collection and transmission. Expansive test architectures are being integrated into designs to optimize this process, and newly developed built-in self-tests need to be compatible with these architectures to maintain a continuously high level of functionality and safety.

In addition to creating reliable ICs, designers must ensure their parts remain safe from a security standpoint. Due to the critical role that these ICs play in some systems, they may be targeted for attack by adversaries who wish to sabotage the larger system and/or compromise its mission. One avenue of attack is the hardware Trojan, a secret function within an IC that forces it to act contrary to its intended use. To offset this vulnerability, researchers have proposed potential architectures and methods on how a hardware Trojan may be realized, as well as many testing strategies to identify the presence of a hardware Trojan within a part. By continuously

anticipating different forms of security breaches, companies can continue developing defenses to stay a step ahead of attackers.

The onset of a fault and the activation of a hardware Trojan both result in a sudden and undesirable change in system behavior. The steps to prevent either, or at least reduce the harm they cause, are also similar: meticulous design, rigorous verification and testing, and the inclusion of detectors and controllers that correct failures or allow the system to fail safely. With these similarities, it is appropriate to discuss hardware security and reliability within the same setting as concepts and solutions from one topic often apply to the other.

Background and Motivation

Research and development of tests and functional safety measures is an ongoing process for both analog and digital circuits, but the progression of digital circuit solutions has far outpaced that of analog circuits. A report published in 2014 compared the number AMS ICs and digital ICs returned due to faults escaping testing and found that, at best, the defective parts per million of the AMS ICs were 10 times higher than the digital ICs[1]. This represents a significant gap in the effectiveness of AMS testing. Since this report, there has been a massive overhaul of how AMS ICs are tested and how the test methods are validated, including more efficient BIST simulation and standardized models for defect-oriented testing[2], [3]. There have also been a growing number of proposed BIST solutions to improve the testability and functional safety of AMS designs, with widely varying levels of sophistication. With the increase in testing options and the fact that analog tests are typically costly in terms of resources, the efficiency and coverage of these tests must be carefully considered.

Producing and testing safe and reliable ICs for mission-critical applications is expensive, a motivating reason to try and extend the lifetime of the chip for as long as possible. As feature sizes grow smaller, on-chip components have become more sensitive to aging effects that impede

the goal of long IC lives[4]. Continued efforts to measure, characterize, and model aging effects have increased the reliability of ICs as they approach their end. In a similar manner to in-field BISTs, aging sensors and monitors have been suggested to personally track chip-specific aging to provide closer estimations of the time-to-failure. Like the AMS BISTs, the online sensors need to efficient with their resources to be attractive inclusions.

Like AMS testing, the hardware security field's progress on anticipating attacks to analog circuits has lagged the development of digital circuit countermeasures. Examples of potential analog hardware attacks continue to be sparse, and the cases that have been presented often cannot be adequately defended against with existing methods[5]. Efforts in this field cannot be allowed to stagnate, otherwise it is only a matter of time before adversarial efforts overcome the existing safeguards and a viable attack is conceived.

Research Overview

This dissertation presents a multi-faceted outlook on the challenges involved in integrating an analog circuit into a large-scale mission-critical system and the considerations that must be made for continued safe and reliable operations. Fig. 1.1 illustrates the three-pronged approach taken in this research. The three different factors shown primarily take place at different points of an IC's life. Most steps that need to be taken to secure the circuit happen at the design phase or during production testing. In-field testing using BISTs continuously or periodically scans for randomly occurring faults in the circuit throughout its life. Finally, aging prediction provides data needed for the system to prepare for shutdown at the end of its life. The combination of these approaches effectively supervises the development and function of the circuit from conception to decommissioning.

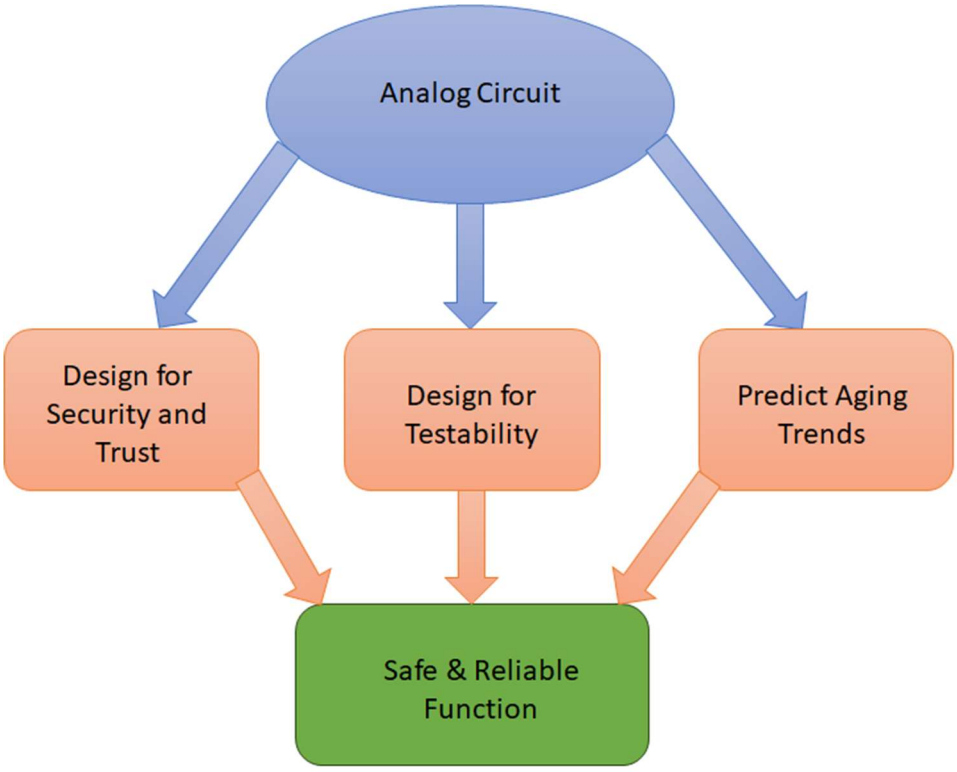

Figure 1.1. Multi-faceted research thrust for safe and reliable analog circuit function.

Organization of Dissertation

Chapter 2 discusses in-field BIST architectures for AMS circuits and compares their defect coverage, complexity, and relative cost. A PCB capable of injecting faults to test a set of efficient BISTs is presented. Measurements show integration of the simple and efficient analog BISTs into digital test architectures can be done with relative ease. The testability and reliability of circuit additions enabling test are discussed as well as how these modifications to the circuit under test can be improved to continue safe operations.

Chapter 3 reviews the effects of transistor aging and how they reduce reliability of a circuit. The methods for measuring and characterizing bias and temperature instability (BTI) are covered, and the challenges involved with accurately modeling and predicting BTI are discussed. An integrated in-field BTI monitor design and its benefits are presented[6].

Chapter 4 investigates the limitations of existing hardware Trojan classifications and detection methods with respect to security breaches in analog circuits. A survey of analog hardware Trojans to date has been conducted. PAAST Trojans are formally defined and classified to fit within existing hardware Trojan taxonomies. The challenges of analyzing and detecting PAAST Trojans is discussed.

Chapter 5 presents a case study of a PAAST Trojan in a coupled oscillator circuit. The numerous applications of coupled oscillators are reviewed. Details of the oscillator design and the Trojan design are covered. A practical trigger mechanism for this and other PAAST Trojans is discussed. Measurements of the fabricated PAAST Trojan are reported and the implications of the measurements and Trojan effectiveness are analyzed.

Chapter 6 summarizes the contributions and concludes the dissertation.

CHAPTER 2. INTEGRATING AMS CIRCUIT TESTS IN ON-CHIP SYSTEMS

Mass production of ICs inevitably results in a few parts being produced with faults. These parts are filtered out of the population during production testing leaving only the functional parts to be sold to customers. These parts will eventually fail too as normal use causes wear on the components within the part. Due to variations in the fabrication process, some parts will contain components that are closer to failure than others. Recording the failures-in-time of a typical part population, the failure rate curve with respect to time will resemble the curve in Fig. 2.1. The relatively high failure rate shortly after production is attributed to latent defects within the parts, where individual component parameters only marginally pass specification. To be clear, the latent defects do not necessarily result in marginal function of the whole part, so the parts with latent defects may not be identified during the production tests. When the parts in question are critical to a mission demanding high reliability, additional tests are performed to weed out latent defects. Burn-in tests typically involve running a part at temperatures and voltages higher than the nominal range for which the part was designed and ran with inputs and functional operations that engineers know will cause maximal degradation at the component level. The purpose of these tests is to cause enough wear on the parts with latent defects such that they fail and can be detected by testing the parts' functions.

Removing the parts with latent defects from the population effectively changes the curve in Fig. 2.1 so that the failure rate of active parts is at its minimum when they are first put to use. The failure rate will steeply increase after a time referred to as the End of Life (EoL) for the part, and this will be discussed further in the next chapter. The period of time between initial deployment to EoL has a low and relatively constant failure rate for the population. In some applications, even infrequent failure of parts can have dire consequences, and further steps must

be taken to mitigate failures. To this end, testing must continue throughout a reliable part's lifetime so that faulty behaviors can be identified and corrected. Sometimes this is done manually by experienced technicians. In power plants, technicians perform periodic maintenance to test and recalibrate the electronic systems that monitor and regulate plant operations. Power plants also employ operators that continuously monitor plant parameters and are trained to identify faults shortly after they occur and take action to keep the plant in the safest condition possible. Typically, there is an on-call staff of technicians available to start repairs on faulty systems when operators identify them as well. This approach requires many man-hours be spent supervising the electronics, and it is not feasible for every application. An additional concern is that some faults cause reactions in the system that are too fast for any person to respond. Quick and catastrophic failures require an automated response to minimize casualties and damage.

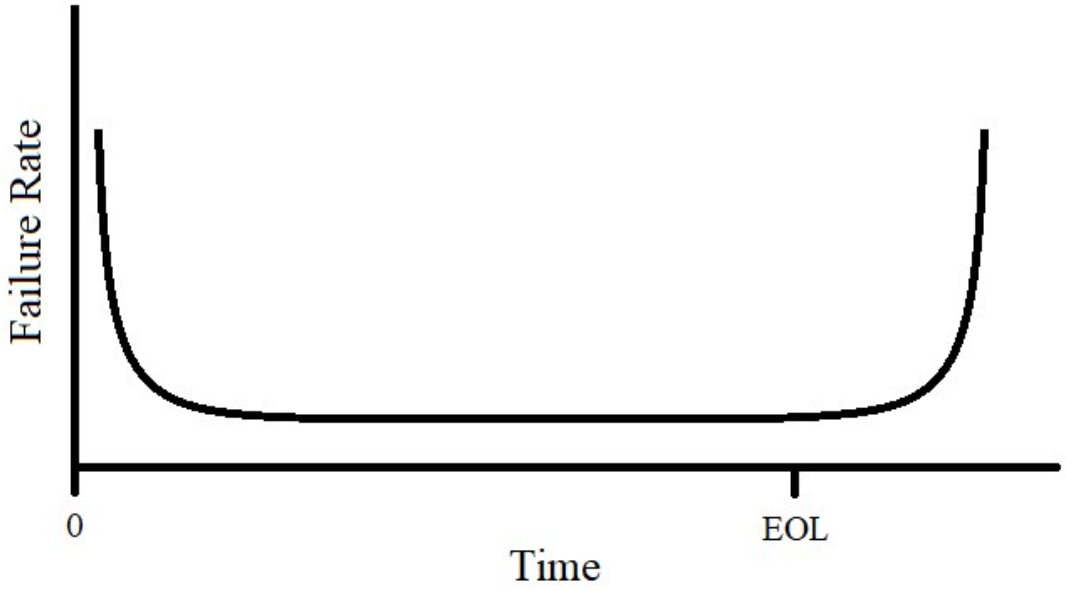

Figure 2.1. Typical failure rate of a part population after fabrication.

To initiate an automated response to failure, a system needs a way to diagnose internal faults through self-testing to determine proper operation. The challenge in designing BISTs is the limited resources available to generate test stimuli and sample outputs, especially if the testing method is fully integrated into a single part. To meet budgets for area, power, and other IC resources, designers must create tests that efficiently use measurements from the circuit under test to evaluate its performance.

Defect-Oriented Testing

Since direct measurement of a particular circuit specification is often impractical for a BIST, the tests must instead create responses from which a fault may be inferred. Such tests must be validated to confirm the designer's assumptions about the faulty behavior of the circuit by defining specifications for the BIST. Defect-oriented testing is a validation method used to standardize specifications on a BIST's effectiveness across many test scenarios and circuit types. The basic concept of defect-oriented testing is that the cause of a fault can be isolated to a single defective component in the circuit, and if a circuit with a defect causes a test's results to differ from those of the nominal circuit then the resulting fault can be detected. The definitions of a defect have varied among articles published by members of academia and industry. A proposal for a standard definition of defects and faults as they relate to analog testing was described in [3]: "… a defect is defined as an unexpected permanent change in a circuit element or connection that is not within fabrication specifications for the element; a fault is an unexpected (temporary or permanent) change in a primitive circuit or circuit module that causes it to fail one of its specifications." Companies create a library of likely defects for the defect-oriented testing, then they simulate a test's response to each defect within the library to obtain a metric called the defect coverage, the percentage of defects detected by the test.

Defects that result in a change in a circuit connection by open- or short-circuit are often termed hard defects. Many different hard defects are possible in ICs, like a metal bridge forming between interconnects or pinholes in the dielectric of a MOS transistor. The similarity in effects allows these defects to be collectively modeled by simple schematic changes in a component cell. For example, a popular method for modeling defects in the 3-terminal MOSFET is shown in Fig. 2.2. The open-circuit defects use a high resistance looking into the terminal while the short-circuit defects use a low resistance to connect two terminals. Modeling the defects using schematic changes like in Fig. 2.2 allows for efficient changes to a circuit netlist so that many simulations of the self-test may be run[3], [7], [8]. The defect coverage obtained from the simulation results determines the effectiveness of the test. Some circuits must also consider a parametric defect, which is a defect that changes one or more process parameters of a circuit element[3]. These defects can also be efficiently modeled in a schematic by modifying component cells.

The type of defects included in a library for defect-oriented testing will vary based on the circuit application. For many digital applications that are robust to parametric variations, simulating parametric defects would give unnecessary or redundant information about the self-test. On the other hand, some AMS circuits are extremely sensitive to variations and the simulation of parametric defects is important to validating the test. Ultimately, the goal of defect-oriented testing is to validate a test method using every defect that is likely to cause a fault in a circuit and achieve a high defect coverage. A high defect coverage means the test will detect most faults and improve the reliability and functional safety of the circuit.

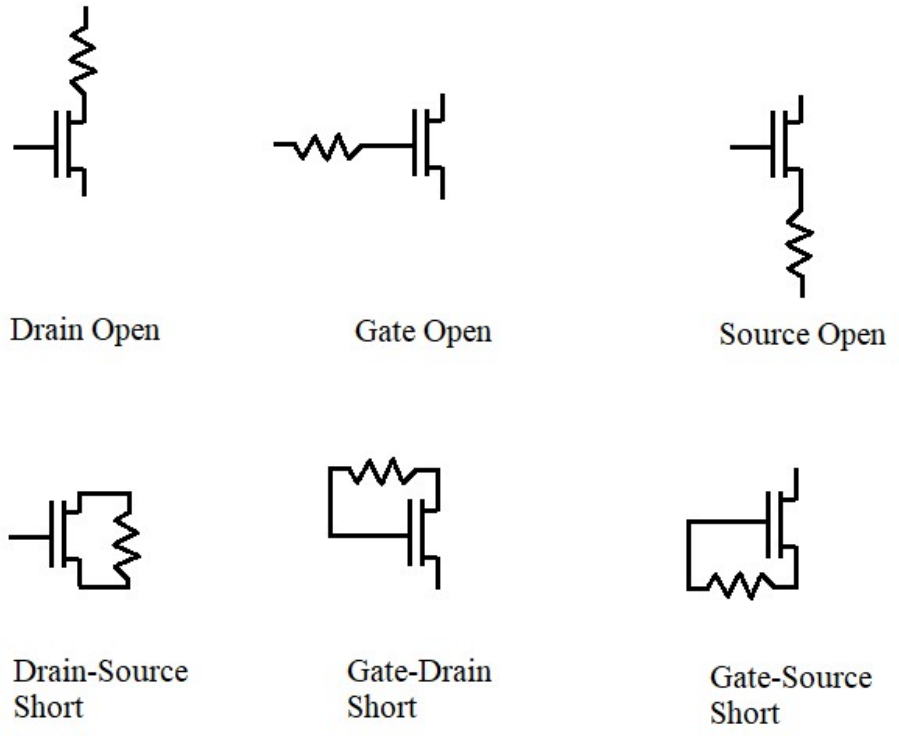

Figure 2.2. Modeling hard defects in MOSFETs.

Analog & Mixed-Signal Design-for-Test (DfT)

Digital signals offer many advantages over analog signals in terms of maintaining the integrity of the information and flexibility in processing. Analog BISTs should have a means to translate the analog signals measured by the tests into a digital format. This is a relatively simple task for DC reference circuits since the most important specification, the static output, can be measured passively by routing the output to an ADC. Other circuits require an input-output response which may require more extensive modifications to the initial architecture to make the circuit testable. In order to select analog blocks to test, a method of digital control should be available in the test to exercise the circuit by a central control unit. The use of digital control signals and simple data converters is essential in analog circuits designed for testability.

DC voltage measurements of circuit nodes give information on how a circuit is biased. Most reference circuits use high-gain feedback to regulate their output to the desired value, and hard defects within the circuit have dramatic effects. For these cases, a low-resolution measurement of the sensitive node conserves a chip's resources while still providing a lot of information about the circuit. A single comparator can be used to indicate if a signal is higher or lower than the reference signal. An even simpler solution would be an inverter whose switching threshold is set at design by its physical size and the supply voltage. Similar approaches are already used for sequencing power management circuits to indicate when the supply voltage is sufficiently high to power the next device, and the method is readily adoptable for power-on testing.

Low-resolution sampling may not be enough to detect parametric defects, though, and tracking the subtle changes in a bias voltage may give clues to impending failure. A more accurate data conversion is required for these cases. Since the cost of in-field testing must remain practical, a test design should use a limited number of high-resolution data converters capable of measuring multiple analog nodes. The legacy method, the Analog Test Bus (ATB), routes analog voltages to a high-resolution ADC to perform the data conversion, and an analog multiplexer addresses which analog signal on the ATB is converted. Reference [9] discussed some of the limitations to this approach, including signal degradation that occurs on long routing paths and the bottleneck of using a multiplexer for conversions, and proposed a different solution. Their concurrent sampling method uses a global ramp reference signal to be compared with various analog node voltages using comparators at each node. The analog measurement is taken when the comparator transitions; noting the time of transition relative to the reference ramp quantifies the measurement, and the number of times the comparator is evaluated during the

ramp signal sets the resolution. The highlight of [9] is the efficiency of test data collection. The sampling resolution is tailored for each analog node to eliminate extraneous data, and the simultaneous measurements combined with compatibility to existing test architectures (IJTAG boundary scan chain) mean that determinations of faults can be made quickly. As was noted previously, reaction time is critical for functional safety.

Another aspect to consider when designing BISTs is the time until availability. For circuits that require a test stimulus and response, the test mode prevents the circuit from performing its normal function. If the circuit under test is the sole signal channel for the system and the system requires its continuous operation, this restricts the available testing time to directly after startup, in which case the test time must be included in the budget for acceptable startup time. Even if the system has redundant channels allowing one channel to be taken offline for testing, the testing time should be limited in case a fault occurs on an operational channel and a quick switchover becomes necessary. A motivating example is a comparison of test methods for evaluating an operational amplifier. The oscillation test method of [10] takes an analog circuit that would normally have a stable equilibrium and introduces feedback components to force oscillation. The defect-free circuit will oscillate at a frequency related to its pole frequencies, so defects will either cause a deviation in oscillation frequency or prevent oscillation altogether. This method has been used to test opamps, active filter, and ADCs with a high coverage for both hard and parametric defects. Generally, frequency measurements on-chip are done by counting the number of cycles in a fixed time interval. This test requires a test time interval dependent on the nominal oscillation frequency and the necessary resolution of the measurement, with higher resolution frequency measurements needing a longer time interval.

Now the oscillation test method for opamps is compared to the intentional offset injection (IOI) test of [11]. The IOI test uses the fact that an operational amplifier has a high gain and only requires a small input magnitude to cause output saturation, and then assumes that many defects will diminish the gain of the amplifier or otherwise fundamentally alter its performance. The example in [11] changes the input-referred offset voltage by effectively skewing the size ratio of the differential input pair through a switched parallel branch, which in turn causes the output to either a high or low voltage depending on the sign of the offset voltage when the differential input voltage is 0 V. The output is converted to a digital signal using a CMOS inverter and produces two bits of information, one bit for the positive offset injection and one for the negative offset injection. Deviation from the nominal truth table indicates a defect. For each half of the IOI test, the maximum time required for testing is the most conservative estimate for how long the defect-free opamp will take to slew from supply rail to the other.

For a given opamp, the IOI test takes significantly less time than oscillation test method. The IOI test also has superior test data consolidation compared to all but the coarsest frequency measurements using the oscillation test method. However, comparisons between the simulations of [10] and [11] indicate that the oscillation test method has a higher defect coverage. The IOI simulations still report a high defect coverage, 95% of the hard defects simulated, and it could be argued that the difference in coverage is negligible compared to the time-savings. But some missions may require the additional confidence provided by the oscillation test method. A possible compromise is to integrate both test methods for the opamp (at the cost of more area) but run the oscillation test less frequently than the IOI test since the majority of defects can be detected by either method.

A similar comparison can be made for two types of low dropout regulator (LDO) BISTs. The use of pseudorandom bit sequences (PRBS) has recently been gaining popularity to infer the impulse response of dynamic systems. The PRBS is used to manipulate voltages or currents in an analog circuit to create an input similar to white noise, then the output of the system is sampled and correlated to the PRBS for the test. This test was used in [12] to find the load-dependent phase margin of a LDO, and it was used in [13] as a defect-oriented test for a LDO. The input bit sequence must be made longer and/or more samples of the output must be taken to improve the accuracy of parameter estimations in this test, which increases both the duration of the test and the amount of data that must be processed. Like the oscillating test method, designers must carefully consider the tradeoff between more information versus shorter test times. The IOI test was used to test a LDO in [14], where the feedback loop was disconnected during testing to achieve the desired open-loop response, and achieved a high coverage of 97.5% for the hard defects considered. Reference [13] reported a higher defect coverage than [14], but the latter report has significant test time savings and needs only two test stimuli and two corresponding output samples for the test, each signal only requiring one digital bit.

BISTs require efficient operation to be a worthwhile inclusion to a system. Designers must consider the likelihood of a fault escaping detection during testing and the consequences of an escape, but overdesigning a BIST also has consequences like limiting a systems performance, and even its safety if resources are diverted from other circuits requiring testing. With this in mind, simple DfT architectures that still have a high defect coverage such as the one used for the IOI test are the best solution for most applications to ensure reliable and safe function.

PCB Demonstration & Measurements of Analog DfT Circuits

A proof of concept for digitally controlled analog BISTs was implemented on a PCB using commercial components and means to inject faults in the circuit. The main portion of the

circuits consists of an LDO, a programmable gain amplifier (PGA), and a DAC. The procedure for this experiment is a testing sequence of the analog blocks directly after power-on of the system. An Altera DE2-115 board with the Cyclone IV FPGA was used to send test control signals and read the results of the analog tests.

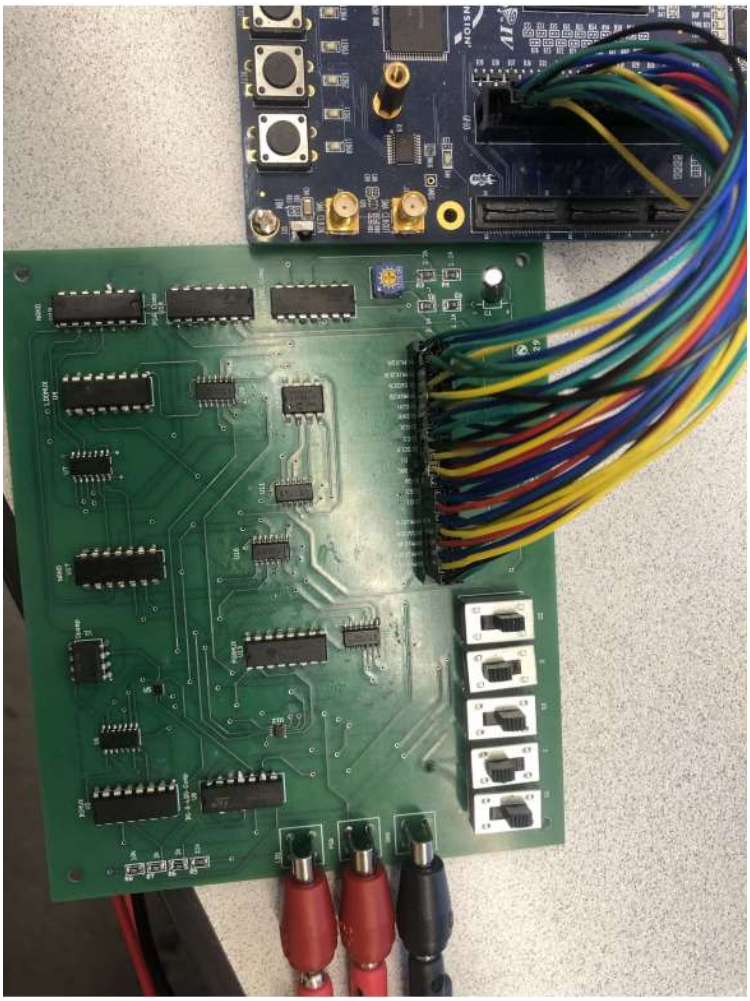

Figure 2.3 Analog test PCB and FPGA board for injecting analog faults and validating BISTs.

BISTs assume the power supply of the circuit is within a valid range so that the test results are valid. To meet this requirement for subsequent tests, the LDO must be tested before the circuit it powers (the DAC and PGA) can be tested. The LDO output voltage is regulated to a factor of its input reference voltage which also must be verified. The input voltage is usually

generated by a bandgap voltage reference so that the input voltage is invariant to temperature changes. The DAC's output cannot be verified before the reference voltage, so a high-resolution sample using the concurrent sampling method of [9] is not possible. However, hard defects disrupt the high-gain feedback paths in reference circuits and often cause significant changes in their outputs. Simulations of the Kuijk bandgap reference in Fig. 2.4 showed that the output voltage deviated from the nominal 1.2 V when hard defects were present, either to a high voltage near the positive supply voltage or to a low voltage near ground. A low-resolution sample of the output using a window comparator is sufficient to test the reference voltage. The comparison window needs to include the nominal output voltage and be sufficiently narrow to exclude voltages that would appear if a defect were present, but the edges of the comparison window do not need to be precisely set to a particular voltage. This relaxes the accuracy requirements of the comparator to the point where the switching thresholds can be set by sizing CMOS logic gates, which eliminates the need for an accurate voltage reference to test the other voltage reference.

Once the input reference voltage is confirmed, the LDO can be tested using the IOI method. The IOI test requires an open-loop response of the opamp, so the feedback path must be broken for testing. The opamp's input must also be set so that its common mode input voltage is within the design range of the circuit and its differential input voltage set to 0 V. The former requirement is met if the bandgap reference voltage is functional as confirmed by the window comparator. The differential input voltage is set to 0 V by closing a switch to connect the inverting and non-inverting input. The response is observed at the output of the LDO. The output is expected to drop to a low voltage near ground when offset forces the opamp output to a high voltage and turns off the pMOS pass transistor. The opposite offset injection is expected to

set the LDO output to a high voltage. The binary response of the test makes a simple CMOS inverter a suitable choice for an observer.

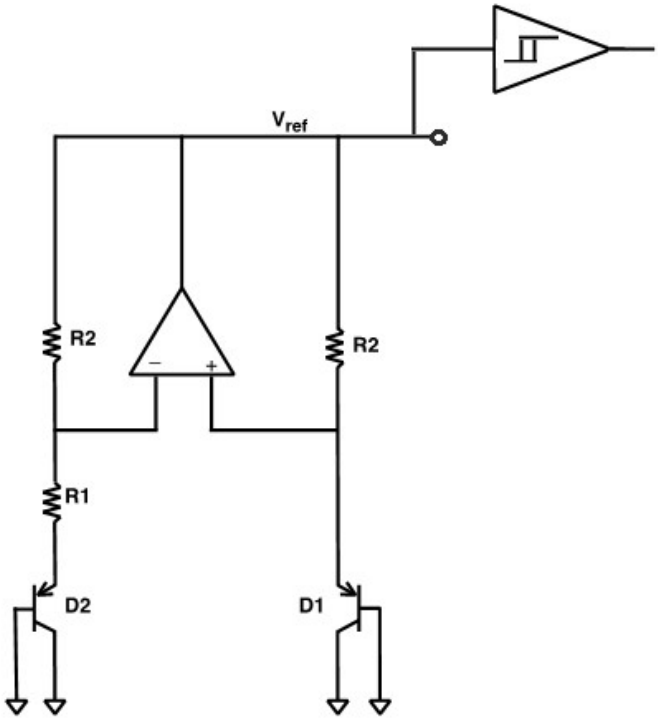

Figure 2.4 Kuijk bandgap reference with window comparator for testing.

A simplified schematic of the LDO configured in test mode is shown in Fig. 2.5. The switches setting the opamp input voltage and disconnecting the feedback loop are digitally controlled by the FPGA board. A select set of faults were manually injected into the voltage reference and LDO circuits by through switches on the FPGA board and mounted on the PCB, then the test response was measured to determine if the faults were detected. The transistor defect models of Fig. 2.2 were considered for the pMOS pass FET. For the bandgap reference, the fault effects were consolidated to three possible outcomes based on where the reference voltage is with respect to the comparison window. The opamp faults were also consolidated to three possible outcomes: normal operation, the output stuck at a high voltage (not responding to

the input), and the output stuck at a low voltage. Tables 2.1 and 2.2 summarize the results of the test.

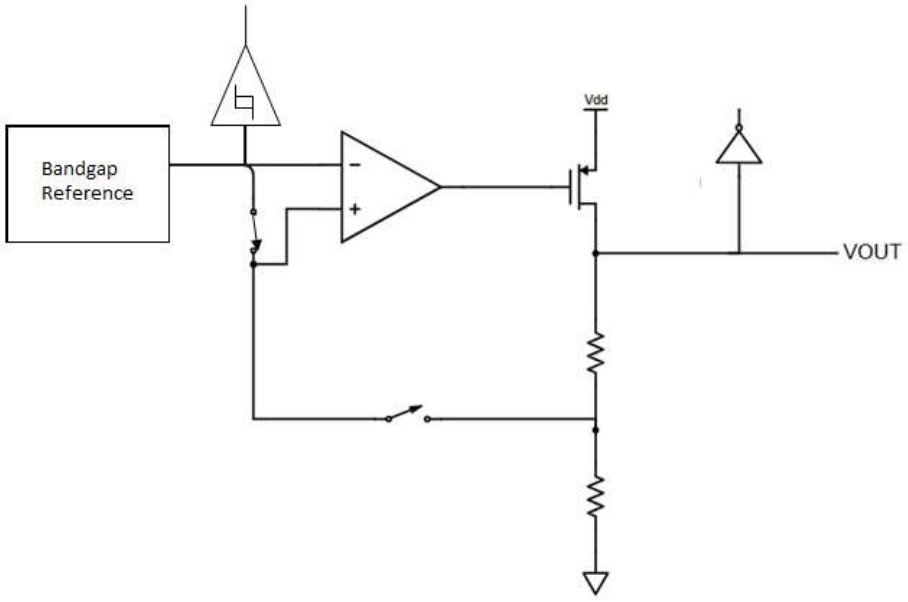

Figure 2.5 DfT LDO in test mode.

Table 2.1 LDO input voltage measurements.

	Expected	Observed
< 1.0 V	0	0
> 1.4 V	0	0
1.2 V	1	1

Table 2.2 LDO IOI test results.

	Negative Offset Injection	Positive Offset Injection
No fault	0	1
Opamp stuck high	1	1
Opamp stuck low	0	0
Pass FET gate open	1	1

Table 2.2 Continued

	Negative Offset Injection	Positive Offset Injection
Pass FET drain open	1	1
Pass FET source open	1	1
Pass FET drain-gate short	1	1
Pass FET source-gate short	1	1
Pass FET drain-source short	0	0

After the LDO and voltage reference are verified functional, the other analog circuits powered and biased by these can be tested. The PGA is next in the sequence of analog tests. The experiment scenario uses the PGA to amplify incoming signals within a desired envelope for sampling and data conversion. This preamplifier increases the sampling resolution for small signals while also preventing amplifier saturation from larger input signals by adjusting the gain of the amplifier. A simplified schematic of the PGA as well as an example of the transfer curve with gain-folding is shown in Fig. 2.6. The gain of the amplifier is adjusted by making parallel resistor connections to the input resistor using digitally controlled switches. Referencing the amplifier's input voltage to the opamp's reference voltage,

$$V_{IN} = V_{REF} + V_{SIGNAL},$$

(2.1)

the output voltage of the amplifier is related to the input voltage by

$$V_{OUT} = V_{REF} - V_{SIGNAL}\frac{R_{FB}}{R_{IN}}.$$

(2.2)

The input resistance is actually the equivalent resistance of *n* parallelly connected resistors of equal resistance to the feedback resistor,

$$R_{IN} = \frac{1}{\frac{1}{R_{FB}} + \cdots + \frac{1}{R_{FB}}} = \frac{R_{FB}}{n}.$$

(2.3)

Substituting (2.3) into (2.2) yields

$$V_{OUT} = V_{REF} - nV_{SIGNAL}.$$

(2.4)

The value of *n* is set by a 3-bit binary code. The code 000 is reserved for disabling the amplifier by disconnecting the input voltage to the amplifier. The remaining codes follow the pattern of one code increment resulting in a doubling of the gain, where code 001 relates to *n*=1 and 111 to *n*=64.

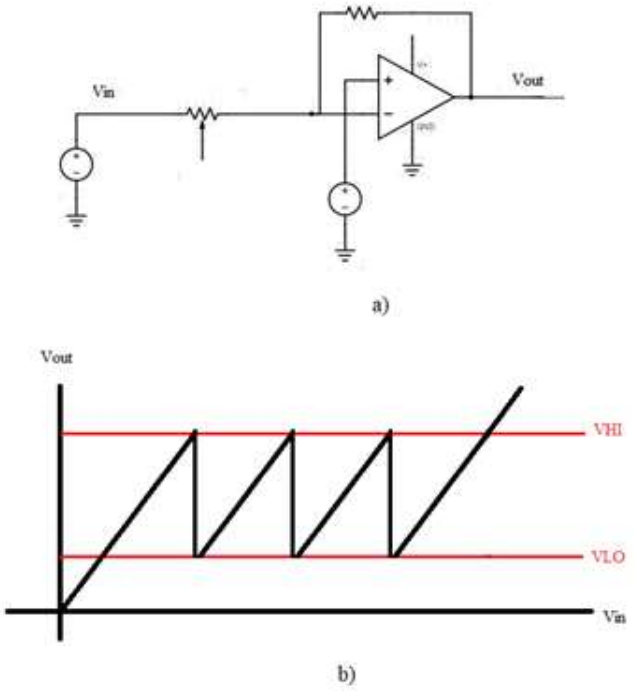

Figure 2.6 PGA schematic(a) and the amplifier's transfer curve(b).

The PGA needs a way to detect when the output voltage leaves the desired envelope so that the gain can be automatically adjusted. This can be accomplished with a pair of window comparators, one with a narrow window and one with a wide window. The narrow window comparator determines when the output is too small and the gain must be increased, and the wide window comparator detects when the output is too large and the gain must be decreased. These window comparators' outputs along with the gain control code can be used to diagnose faults in the PGA. A given input voltage to the amplifier will have only one gain setting that will appropriately set the output voltage within the desired envelope. If a known input voltage is applied to the amplifier and the digital feedback from the window comparators is disconnected, the response of the PGA can be tested by setting the gain through independent signals and observing the gain adjustment signals.

For example, suppose the appropriate gain setting for the input voltage was n=16. The gain-too-high signal (labeled G2H) sends a logic 1 when the output is outside the wide window indicating the gain should be decreased while the gain-too-low signal (labeled G2L) sends a logic 1 when the output is inside the narrow window indicating the gain should be increased. The fault-free performance of the PGA in this case is described by the truth table of Table 2.3.

The PGA requires only a few input voltages as reference for the test. The valid input voltage range of this PGA includes the power supplies, so the DfT architecture includes a 4-to-1 multiplexer to select 1 of 3 voltages (positive supply, negative supply, or opamp reference voltage) for testing or the input voltage for normal function. Like the IOI test, the PGA BIST completes its tests quickly allowing for faster fault detection and return to service.

Table 2.3 Truth table for PGA test when the input voltage requires a gain of 16.

n	A	B	C	G2H	G2L
OFF	0	0	0	0	1
1	0	0	1	0	1
2	0	1	0	0	1
4	0	1	1	0	1
8	1	0	0	0	1
16	1	0	1	0	0
32	1	1	0	1	0
64	1	1	1	1	0

At the satisfactory conclusion of the PGA test, the analog system can be placed into normal service and background testing can commence. The PCB includes a DAC controlled by the FPGA to generate a ramp signal used for concurrent sampling. Three analog voltages derived from LDO were sampled during the testing to demonstrate the method. The authors of [9] use a unary data format for the concurrent sampling method that is illustrated in Fig. 2.7. The authors note that this method becomes inefficient when the DC node sampled requires a higher resolution. Fortunately, most applications will have only a few nodes needing this level of accuracy. This experiment shows an alternative sampling approach that can be used in conjunction with the original method described in [9]. At a given analog node, the comparator output transitions from logic 0 to logic 1 when the reference ramp signal reaches the switching threshold. The rising edge of the comparator output sends an interrupt signal to the clock that increments the digital ramp into the DAC and loads the input code into a register addressed to the analog node. Once the DAC input code is loaded, the ramp recommences. This temporary

interruption is transparent to the sampling operation of the other nodes making it possible for a combination of low- and high-resolution samples to be taken concurrently with only a small additional delay of data to the processor. This alternative sampling method is illustrated in Fig. 2.8.

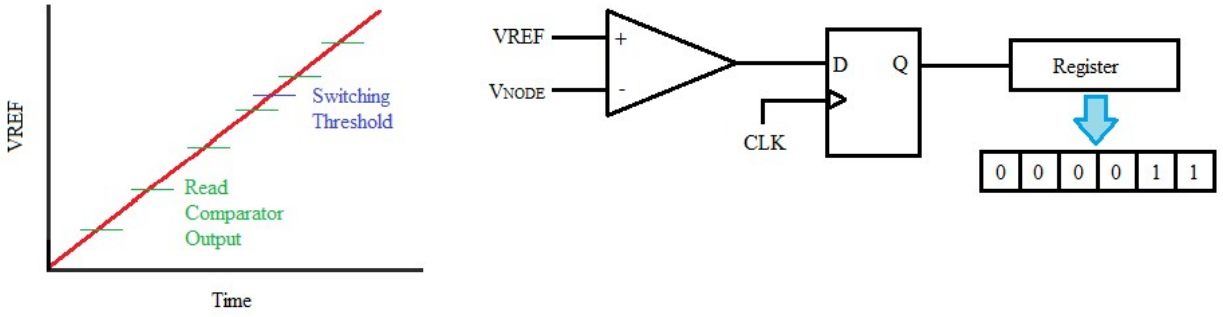

Figure 2.7 Concurrent sampling method using unary data.

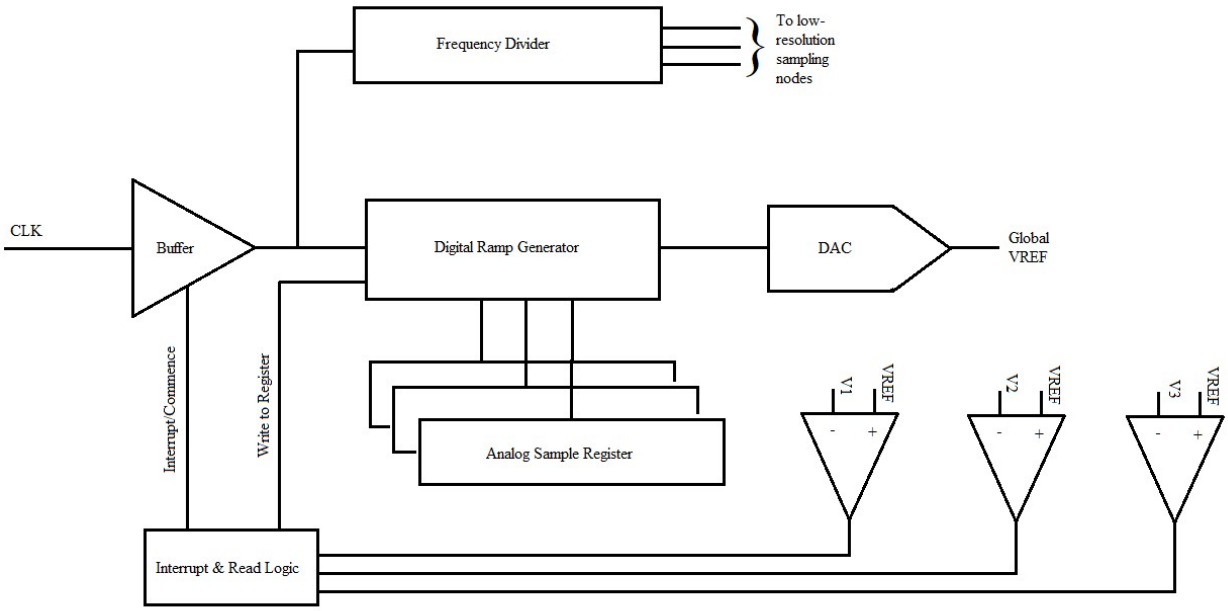

Figure 2.8 High-resolution concurrent sampling method.

The analog BISTs and DfT architectures implemented on this board demonstrate that digitally controlled test stimuli and local digitization of analog signals offers a great deal of

flexibility and function for testing the AMS circuits. The simplicity of the tests performed in this experiment makes it easier to integrate these tests into the large test architectures already deployed in digital systems.

Handling Defects in Test Circuit Components

The inclusion of test input points and observers increases the testability of a circuit, but it also increases the probability of a fault occurring. It is possible for defects to manifest in the components used to test a circuit, such as the switches and comparators described in the previous sections, which can lead to either a misdiagnosis of the condition of the circuit under test or an actual fault in the circuit. Fortunately, there are some simple techniques that can be used to make a circuit hardy to defects in the test components.

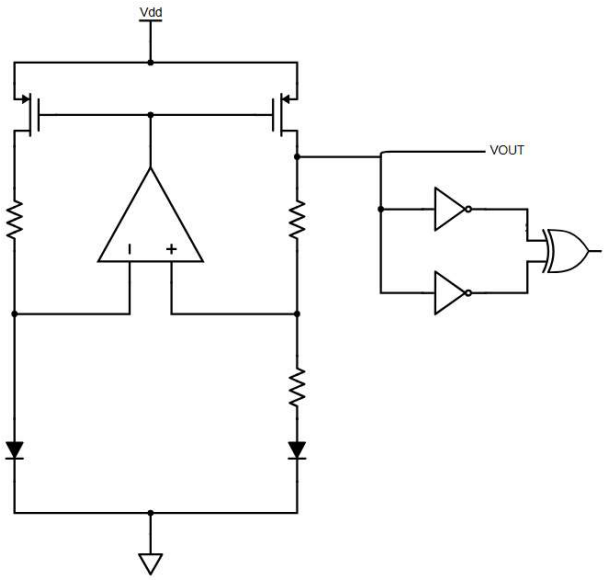

Figure 2.9 Bandgap reference circuit with window comparator observer.

Consider the bandgap reference in Fig. 2.9 that uses a window comparator to quantize the output voltage. The nominal output voltage of the reference is 1.22 V and the window edges are set at approximately 1.0 V and 1.4 V. When the reference is operating normally, the window

comparator's output is logic 1. The window comparator consists of two inverters and an XOR gate that adds 16 transistors to the circuit. Assuming 6 possible hard defects per transistor, the window comparator has 96 defects that must be considered. Simulations of the circuit after injecting defects into the window comparator only revealed that 8 defects caused faults in the bandgap reference, specifically shorts in the inverters' gates caused the output voltage to deviate. The influence these defects have on the reference can be eliminated by modifying the inverters to be enabled only during testing. Fig. 2.10 shows the inverter modification where the top and bottom transistors enable operation only when the signal TEST is logic 1. The circuit was simulated again with the inverters disabled and no single defect in the window comparator affected the reference's output voltage.

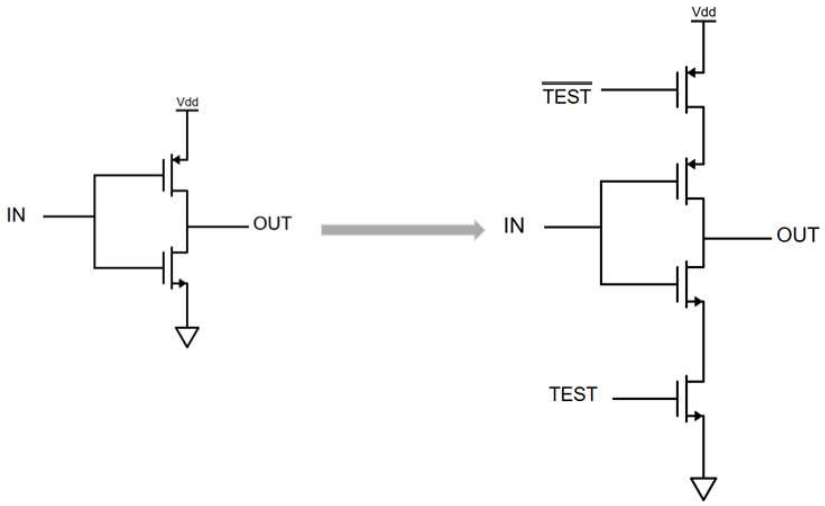

Figure 2.10 Gate modification that prevents observer defects from loading the circuit.

This solution only prevents circuit faults when the observer is disabled, but the circuit becomes vulnerable to observer defects again when the observer is enabled to sample the reference's output. There is also the issue of observer defects that do not affect the circuit under test but misdiagnose its status. Both problems can be addressed with redundancy techniques

widely used in digital self-tests. Logic gates with complementary outputs have two valid output combinations: “0 1” or “1 0”. Many transistor defects in logic gates cause a gate output to either be stuck high or stuck low, and it is a common practice for defect-oriented tests to only consider these two defects for each logic gate. In a gate with complementary outputs, the stuck high or stuck low defect on one output can result in a forbidden output state of “0 0” or “1 1”. Observing one of these forbidden outputs indicates a defect is present, and this principle was used as the self-checking capability for the family of logic gates proposed in [15]. A similar approach can be taken to include defect coverage of the observers used in analog BISTs. The conversion of a single analog voltage to a digital signal requires some of the digital outputs in the observer to be single ended rather than complementary. Defects early in the signal chain where the digital outputs are single ended can cause output errors even when complementary outputs are used later in the signal chain. The use of multiple observers and majority voting can be used to determine which of the observers have valid outputs. Looking back at Fig. 2.9, three window comparators can be connected to the reference’s output instead of one for a 2 of 3 voting method. If a defect in one of the window comparators causes its output to be contrary to the circuit under test’s condition, its output will differ from the other two window comparators. With majority voting, the two observers that agree are considered functional while the remaining observer is assumed to have a defect. Majority voting further improves the defect coverage of the observers. The redundant observers also solve the issue of a fault occurring when a defective observer is enabled. Activating and sampling the window comparator outputs one at a time ensures the defective comparator is disabled and cannot cause a fault in the circuit under test while the other comparators are performing their evaluations.

Using redundant components can also benefit the reliability of the test input circuitry. The analog test inputs used to stimulate a circuit under test are enabled using digitally controlled switches. For this discussion, an analog switch is modeled as a single throw switch shown in Fig. 2.11a. This model has two possible defects, stuck ON and stuck OFF. Either of these defects makes a change to the circuit structure that can prevent testing or prevent normal function. The series-parallel connection of multiple component switches to form a single composite switch can ensure continuity of function in the presence of a single defect. In Fig. 2.11b, the composite switch can still be turned OFF even when one of the component switches is stuck ON. In Fig. 2.11c, the composite switch can be turned ON even when one of the component switches is stuck OFF. The composite switch in Fig. 2.11d combines the advantages of Figs. 2.11b and 2.11c and can be turned ON or OFF even when a single defect is present. This method improves the fault resilience of the circuit containing the switch.

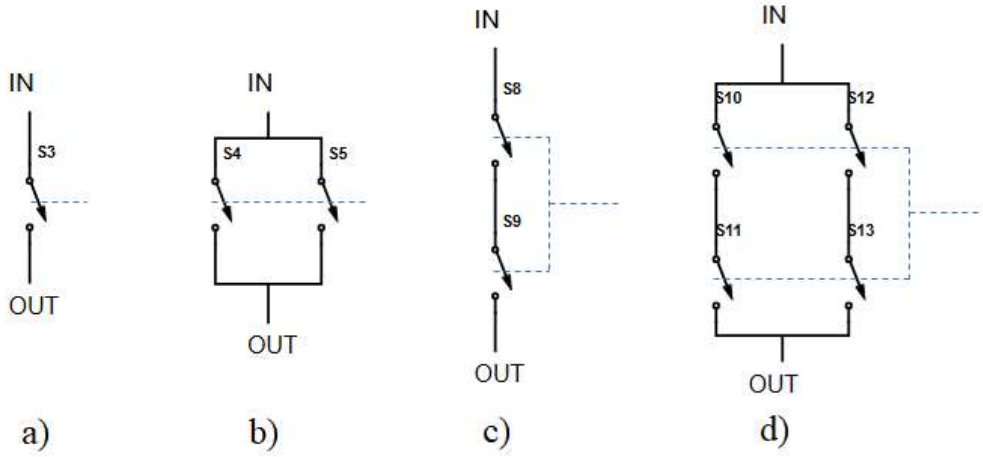

Figure 2.11 Switch architectures with varying resiliency to faults.

Summary

In-field AMS testing methods are vital to a mission of safer and more reliable parts. The efficient tests described in this chapter infer proper circuit operations with simple test signals and

sampling techniques that reduce the overhead of expensive precision circuits normally required to test analog systems. Autonomous diagnostics allows fast fault response and system correction for safer and more reliable designs, a critically important feature considering the IC market growth in safety-centric industries. The concept of defect-oriented testing standardizes the benchmarks and goals of BISTs. Handling test coverage at lower levels of abstraction like the opamps, amplifiers, reference circuits, etc. enables many of the test strategies to be transferred to different circuit topologies and process technologies; the agreement between PCB measurements of the analog tests with simulations in different semiconductor technologies effectively demonstrates the transferability.

CHAPTER 3. MONITORING AGING WITH ONLINE MEASUREMENTS

Over the course of part's use, component aging creates parametric defects that increase the probability of failure. The most likely cause of a fault after a part has reached it EoL (the time when failure rate dramatically increases, Fig. 2.2) is from aging; unlike defects that occur at the beginning or middle of a part's life, aging defects have a degree of predictability. Estimating how aging defects evolve and when they will cause a fault is critical to long-term mission planning. Functional safety applications also require a method of detecting faults in order to place the system in a safe condition. Ideally, a system would take action shortly before a fault occurs to prevent system damage. Sensors that track aging and predict trends are needed to determine imminent failure and enact precautionary measures. Among the different aging effects for silicon MOSFETs, bias and temperature instability (BTI) is generally considered the most severe. This chapter covers the cause and effects of BTI and techniques to measure and respond to BTI in integrated circuits.

Bias & Temperature Instability

BTI is the decrease in transconductance of a MOSFET over time caused by strong gate bias voltages and exacerbated by temperature. The decrease in transconductance is attributed to the accumulation of charge carriers in the gate dielectric creating an electric field that opposes channel formation. The most common way of quantifying BTI is through a change in a transistor's threshold voltage, though the mechanism also degrades charge carrier mobility and gate capacitance. The effect is most prominent in pMOS transistors with a largely negative gate bias (NBTI). Early experiments of NBTI dynamics in silicon MOSFETs show a trend consistent with the rate of molecular diffusion in a solid, specifically hydrogen[16]–[18]. Hydrogen is used during fabrication to improve charge carrier mobility in the channel. The interface between the

body of a transistor and its gate dielectric marks an abrupt change in crystalline structure, and the body silicon at the interface is left with “dangling” bonds. The mobility of charge carriers interacting with the dangling bonds is significantly lower compared with the rest of the channel, effectively trapping the charge carriers, so hydrogen is used to passivate the bonds. However, a strong electric field can cause channel holes to displace the hydrogen and the hole becomes trapped. The concentration of free hydrogen at the interface increases as this reaction continues at other sites. At a high enough concentration, hydrogen near the interface will begin to react in the reverse direction and reform some of the passivation bonds. The back reaction limits the net rate of hole trapping. Over time, the hydrogen diffuses away from the dielectric-body interface to equalize the concentration throughout the dielectric. The diffusion process lowers the interface concentration allowing the hole-trapping reaction to continue. The back reaction of hydrogen to passivate traps means that recovery of the threshold voltage is also possible. The hole-trapping rate is also a function of the electric field strength drawing in carriers from the channel. If the gate bias is reduced or removed altogether, the back reaction rate will overcome the hole-trapping rate causing the threshold voltage trend to reverse direction. The reduced hydrogen concentration from the back reaction also causes hydrogen located further in the dielectric to diffuse back towards the interface.

The Reaction-Diffusion model cannot entirely predict NBTI. Fast measurements of NBTI recovery have shown recovery rates faster than a diffusion-based limit on reaction rates[19]. The widely accepted theory for this fast recovery is the existence of permanent defects in the dielectric that trap holes[20], [21]. The interface traps are formed by the displacement of hydrogen by a channel hole, so the trap is immediately occupied after it is formed. In contrast, permanent traps can either be occupied or vacant leading to very different NBTI and recovery

rates as holes are captured or emitted. The implications of fast NBTI recovery by hole emission from permanent traps is that the degradation of threshold voltage is also more significant than the diffusion model prediction for a given interval of time and bias voltage. Permanent traps can originate from flaws in the fabrication process, but it has also been theorized that traps can form from chemical reactions of hydrogen with the dielectric material[22], [23]. These secondary reactions further compound the complexity in accurately predicting NBTI.

BTI can also occur in nMOS transistors with large positive gate bias voltages, which is called PBTI. The nMOS transistor is less sensitive to PBTI than the pMOS is to NBTI, and PBTI has been considered a negligible effect for older processes. Newer processes with smaller feature sizes have exhibited enough PBTI to be significant and worth modeling. The mechanism for PBTI is believed to be similar to NBTI except electrons are the contributing charge carrier. Processes using high-κ metal oxides have been reported to show more significant PBTI, and the suspected cause is a higher number of permanent defects in the metal oxide during fabrication compared to other dielectric materials[24], [25].

Timing faults are usually the primary concern for BTI defects. Reductions in transconductance of switching transistors reduces the current that charges the load capacitors, which lengthens the transitions time. The shift in threshold voltage also means the transistors turn on later with respect to a transitioning input, which increases the propagation delay. This can lead to hold time violations in latches and memory circuits. In addition to the sensitivity of switching circuits to BTI-induced delays, the transistors in these circuits generally degrade faster as well. The charge trapping reaction is related to the strength of the electric field in the dielectric. Switches and digital circuits use the full supply voltage to either turn on or turn off the switch, whereas transistors in analog circuits typically have a much smaller gate bias voltage.

The combination of effects makes high-speed digital communications and memory the most vulnerable circuits for BTI-related faults.

Simulating and Measuring BTI

The rate of BTI varies for different process technologies, feature size, and biasing voltages. Measurements of BTI are necessary to characterize aging in a given process, but the effects of aging usually take years to create a fault when a part is operated within its design constraints. The aging process is accelerated by operating devices at elevated voltages and temperatures so that relevant measurements can be taken in a matter of hours. There are several commonly used measurement techniques to determine the shift in threshold voltage caused by BTI. During the accelerated aging process, measurements of a transistor's drain current while regulating the terminal voltages constant can be used to track the decrease in transconductance. Alternatively, a transistor can be connected such that its gate-source voltage is a function of its drain current and threshold voltage and the drain current is held constant, called a gate-diode connection[26]. The results of these experiments have been used to derive predictive models for BTI using process constants found empirically to fit the theorized equations. Reference [18] found a concise equation to fit experimental results for the generation of interface traps using the Reaction-Diffusion model. This equation was used as the basis for compact equations in [27] to calculate the change in threshold voltage from the trap generation equation.

Compact models like these are commonly used in industry to simulate BTI and other aging effects in their circuits to see if they will reach a target EoL. Compact aging models fail to capture aging behavior for every scenario, though. For example, the equations in [27] used to calculate the threshold voltage are derived from interface trap generation and does not account for the fast capture/emission of charge carriers in permanent traps. Another detail that is often neglected in aging models is the random aspect of the physical process. Theoretical mechanisms

supported by experimental measurements show the charge trap formation and charge capture/emission to be stochastic processes creating a variability for BTI[28]–[30].

Companies will typically defer to the simpler deterministic models for simulation, which is understandable considering the complexity of the circuits that require simulation and the multiple combinations of process and operating corners that must be simulated just to see if the circuit will work when it is new. ICs are often conservatively designed with respect to aging so that only a few worst-case scenarios need to be considered. This strategy errs on the side of caution, but there is usually a significant overlap of mission-critical parts and parts that need aging estimates. The mission-critical parts are usually expensive because of the amount of time it takes to thoroughly test them as well as the additional BISTs that need to be integrated into the design for functional safety. Discarding these parts at a conservative estimate of their EoL means that most of the parts are decommissioned long before an aging fault would have occurred, and this is an additional cost to the mission.

Integrated sensors that measure aging in the field can provide a more realistic estimate of when an aging fault will occur for a single part and allow the part to be utilized to its full extent. Instead of directly testing circuit functions like what was described in the last chapter, separate monitors measuring representative devices' aging have been proposed to serve as a type of odometer for the chip. The devices in the monitors are assumed to age similarly to devices in the rest of the circuit, and specifications for warnings or failures are set by the amount of degradation in a critical device (change in threshold voltage for BTI) will cause a fault. Aging sensors may also provide data used to recalibrate systems and extend their life. Many designs have proposed reducing their operating frequency to avoid timing errors caused by BTI. Another

approach is to adjust the body voltage of the pMOS transistors to change their threshold voltages and compensate for NBTI[31], [32].

Most BTI monitors' operations are concisely described by the phrase "stress-measure-stress." During stress, the devices in the monitor are biased to cause the desired aging scenario. Measurement requires the monitor to be reconfigured to take measurements determining the amount of BTI incurred. The device bias is usually much less during measurement than it is during stress, so the device will begin to recover from BTI. Most BTI monitors are designed for very short measurement intervals to minimize device recovery, especially from fast charge carrier emissions from permanent traps, to prevent overly optimistic estimates of BTI.

A popular architecture for integrated BTI sensors is an enabled ring oscillator. The enabled ring oscillator using CMOS inverters has alternating stages with low input voltages, which causes NBTI in those stage's pMOS transistors. NBTI causes the running frequency of the oscillator to decrease when it is enabled. Measuring the oscillator's frequency can be accomplished relatively quickly provided it has a high enough running frequency, which makes them attractive choices for measuring BTI before there has been a significant amount of recovery. Reference [33] used a sensor for accelerated aging measurements that compares the frequencies of an aged oscillator and an unaged oscillator. The unaged oscillator is used as a reference to account for variations in frequency due to voltage, temperature, and process parameters, but it also allows for fine measurements of the frequency using the beat frequency produced by the two oscillators. This architecture can be modified for in-field measurements by power gating the reference oscillator to prevent aging, but there are several limitations to this type of sensor.

In processes where PBTI is significant, the nMOS transistor aging will also contribute to the decreasing frequency of the aged oscillator making an NBTI measurement overly pessimistic. Modified ring oscillators that use inter-stage switches to force each inverter input to a low voltage while the oscillator is disabled were described [34] to prevent nMOS PBTI. A similar switch connection was used in [4] to separately analyze the effects of NBTI, hot carrier injection (HCI), and time-dependent dielectric breakdown (TDDB). An alternative approach to reduce the oscillator's sensitivity to PBTI was reported in [35]. Instead of not gates, the oscillator uses alternating NAND and NOR gates as the delay stages. The series connection of pMOS transistors and parallel connection of nMOS transistors in the NOR gate cause an increased delay for a given amount of NBTI and a reduced sensitivity to PBTI. Conversely the NAND gates are more sensitive to PBTI and less sensitive to NBTI. The authors of [35] used different oscillator configurations to separately measure NBTI and PBTI.

Another consideration for accurate BTI measurements is the biasing history. If the aging of transistors in the sensor must closely match the aging of a transistor in a critical path, then the bias conditions should closely match. The enabled ring oscillator just described use the supply voltage to cause aging in the oscillator stages; this is the worst-case bias condition for BTI and can lead to overly pessimistic estimates of aging. This issue was addressed in [36] and [37] by using current-starved ring oscillators. A single transistor with arbitrary gate bias ages similarly to a critical transistor in the circuit, then its BTI decreases the current (and frequency) of the oscillator over time. Reference [37] used a single oscillator whose frequency is first measured when current is supplied by an unaged transistor and then is measured when current is supplied by the aged transistor. This comparison allows frequency deviation from temperature, voltage, and process parameter variations to be considered.

Along with the bias history dependence, the random component of BTI must be accounted for in the sensor design as well. Sampling of the NBTI distribution for experiments in these references show how the standard deviation of the threshold voltage increases with its mean. The simple enabled ring oscillator sensor averages these variations when measuring the frequency and does not provide information on the likely range of BTI that could occur in critical transistor. The current-starved ring oscillator sensors of [36] and [37] have a single aged transistor determining the output, so it is possible to create multiple copies of at least portion of the sensor to sample the BTI distribution.

Sampling the trend of a BTI distribution for part-specific operating conditions improves the estimate of when a fault is likely to occur, but it requires multiple identical devices that are identically biased to perform this measurement. BTI sensors should be compact to facilitate sampling, which was recognized in [37] and [38]. The next section describes a proposed BTI sensor meeting these requirements; additionally, the measurement is more closely related to a transistor's threshold voltage than the frequency measurements previously described.

Monitor for In-Field Statistical Characterization of BTI

The principles of this monitor's operation are as follows. Consider the circuit of Fig. 3.1; the two transistors are of identical size and type and are biased with equal currents, and both are assumed to be in strong inversion and saturated. The square-law model uses the drain current equation

$$I = \frac{1}{2}\beta(V_{SG} + V_T)^2, \tag{3.1}$$

where the threshold voltage is a negative quantity. Rearranging (3.1) to solve for the source voltage with respect to ground yields

$$V_S = \sqrt{\frac{2I}{\beta}} + V_G - V_T. \tag{3.2}$$

Now assume that the voltage V_{FORCE} in Fig. 3.1 is set such that the source voltages of the two transistors are equal. Substituting the appropriate gate voltages for each transistor in (3.2) and equating the source voltages produces the relationship

$$\sqrt{\frac{2I_1}{\beta_1}} - V_{T1} = \sqrt{\frac{2I_2}{\beta_2}} + V_{FORCE} - V_{T2}. \tag{3.3}$$

Since the transistors are of identical type and size (identical β) and the bias currents are equal, (3.3) can be simplified and rearranged to

$$V_{FORCE} = V_{T2} - V_{T1} = \Delta V_T. \tag{3.4}$$

If V_{T2} remains constant while V_{T1} decreases due to NBTI then the quantity ΔV_T is the amount of NBTI in M1 of Fig. 3.1. Therefore, V_{FORCE} is equal to the NBTI in M1 when the source voltages are equal.

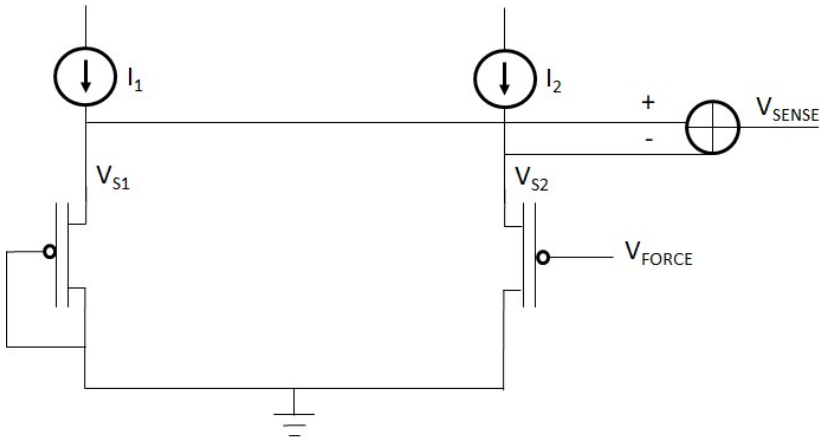

Figure 3.1 Threshold voltage difference circuit.

A simplified schematic of the proposed monitor measuring NBTI is shown in Fig. 3.2. The monitor uses the stress-measure-stress type of operation which temporarily interrupts the aging bias using switches to measure BTI. During the stress phase, M5 and M6 act as OFF switches preventing current from flowing in either of the branches. The transistors M1 and M2 operate in strong inversion saturation during the measurement and in the linear region during the stress phase with an almost zero drain-source voltage. This means that the sources of M3 and M4 will be nearly VDD during the stress phase. M4 is diode connected during the stress phase by turning M7 ON and M8 OFF with almost zero current flowing from drain to source, so it will be operating in deep subthreshold with almost zero gate-source voltage. This will mean that M4 will experience no NBTI during the stress phase. M3's gate voltage will be whatever desired stressing voltage the designer chooses, static or dynamic. The architecture allows a designer to choose how various devices under test are biased during stress to best represent devices of interest in the system. During the measurement phase, M5 and M6 are turned ON to allow current to flow in each branch. M3's gate is biased with a static reference voltage such that is operating in strong inversion saturation. M4's gate is biased with the voltage output of a DAC. The measurement operation occurs by searching for the DAC code that will cause the source

voltages of M3 and M4 to be matched. This is done by evaluating the comparator output in a successive approximation algorithm. When the source voltages of M3 and M4 are equal, M1 and M2 will have identical gate-source and drain-source voltages. If M1 and M2 are perfectly matched, then the currents in the M3 and M4 will be identical. At this point, all assumptions required for (3.4) to be valid are met with the DAC's output voltage being V_{FORCE}. The monitor effectively acts as an aging-to-digital converter where the DAC code is sent off to be processed at the completion of the algorithm.

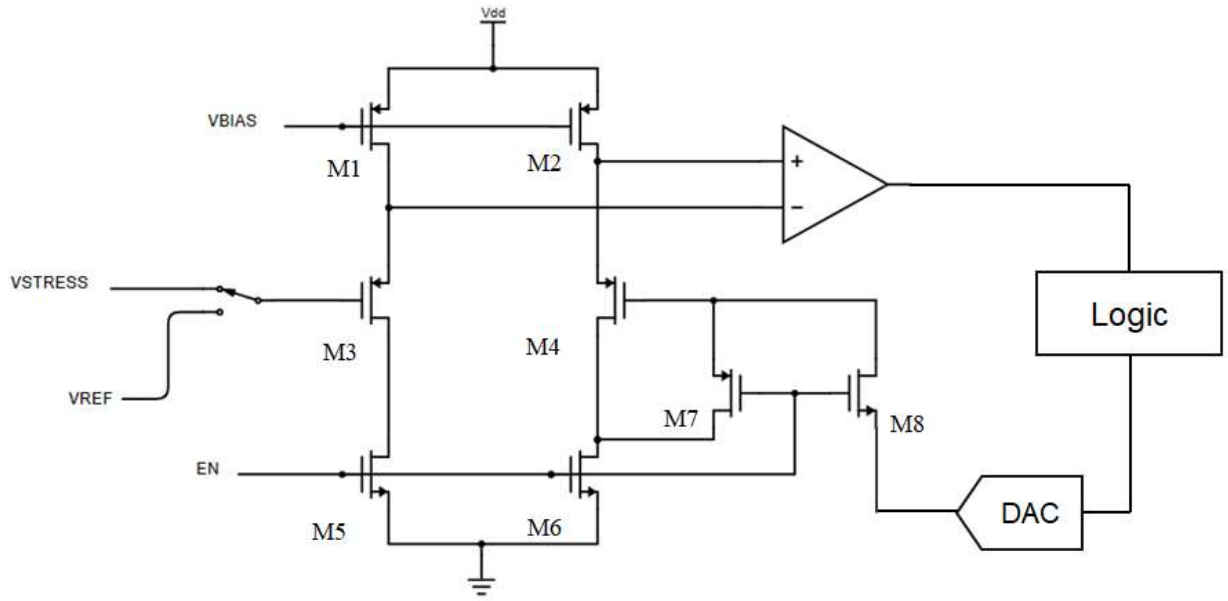

Figure 3.2 Proposed BTI Monitor.

Fig. 3.2 shows a monitor for measuring NBTI in pMOS transistors, but it is simply modified if it is desired to measure PBTI in nMOS transistors instead. The aged device and unaged device are replaced with the representative nMOS transistors, the current cutoff switches remain on the drain side of the devices being measured, and the current sources remain on the source side of these device with nMOS transistors sinking current instead. Equations similar to

(3.1)-(3.4) exist for the nMOS version of the monitor making the relationship of the DAC's output voltage to BTI the same.

Sizing the Transistors of the Monitor

Referencing the device numbers of Fig. 3.2, the design flow for the monitor is described next. The transistors M3 and M4 are chosen so they are the same size and type of devices as a critical transistor within the circuit that is likely the first to fail due to BTI. M3 and M4 should be in strong inversion during the measurement to improve the signal to noise ratio. The gate-source voltage of M3 is set by its bias current and threshold voltage, so the bias current should be chosen large enough that M3's gate-source voltage exceeds its threshold voltage for the maximum amount of BTI to measured. The current is supplied by M1 and M2, both of which should be biased with a low overdrive voltage to avoid NBTI; otherwise, a random time-varying offset could develop in the monitor. Sizing M1 and M2 with larger aspect ratios lowers their overdrive voltage for a given current, and using more area for the transistors improves their matching. During the measurement phase, M1 and M2 should be in saturation. This is a relatively easy requirement to meet provided the designed overdrive voltage of M3 and reference voltage are not too large. The maximum source voltage of M3/M4 is determined by the maximum aging measured before the part is decommissioned,

$$V_{S(Max)} = V_{REF} + V_{OD,M3/M4} - V_{T(Aged)},$$

(3.5)

where

$$V_{OD} = \sqrt{\frac{2I}{\beta}}.$$

(3.6)

The requirement to maintain M1/M2 in saturation is

$$V_{D,M1/M2} \leq VDD - V_{OD,M1/M2}.$$

(3.7)

Substituting (3.5) into (3.7) and rearranging the inequality yields

$$V_{REF} + V_{OD,M3/M4} \leq VDD - V_{OD,M1/M2} + V_{T(Aged)}.$$

(3.8)

Process engineers design the nominal threshold voltage to be several times less than the supply voltage, and a 20% change in the threshold voltage is considered an extreme case of aging. With this in mind, satisfying (3.8) is not anticipated to be difficult.

The switches M5 and M6 enable the biasing current to flow during measurement. M3 and M4 need to be in saturation during measurement, so the ON resistances of M5 and M6 should not be so large as to have a voltage drop pushing M3 and M4 into the linear region. The inequality that must be true for M3 and M4 to be in saturation is

$$IR_{ON} \leq V_{REF} - V_{T,M3},$$

(3.9)

where R_{ON} is the ON resistance of M5/M6. The right-hand side of (3.9) is at its minimum when M3 is unaged, so satisfying the saturation requirements for the fresh design is sufficient. The ON resistance should not be made too small because it also results in a decrease in the OFF resistance, which increases leakage current when the monitor is operating in the stress phase. Since this monitor is intended to support multiple device sampling and the monitor spends the majority of its life in the stress phase, the leakage current through the switches is a major contributor to the power consumption of the monitor.

The purpose of M7 is to equalize the gate, drain, and source voltages of M4 during the stress phase to prevent M4 from aging; ideally it passes no static current, so its ON resistance is essentially trivial. The OFF resistance of M7 should be very high to prevent much current being injected into the monitor branch from the DAC. M8 should also have a high OFF resistance to prevent the DAC voltage from increasing M4's source-gate voltage during stress and potentially causing aging. The minimum ON resistance of M8 depends on how fast the BTI measurements must be taken; the gate voltage M4 should be settled by the time the comparator output is evaluated and a large ON resistance will slow the charging of the gate. It is unlikely that the size of M8 will be the limiting factor on the data conversion speed since M4 will most commonly be a copy of a transistor used in high-speed digital communications, which are often designed for GHz switching frequencies.

The reference voltage biasing M3 during measurements is added to the final DAC voltage when the measurement algorithm is complete,

$$V_{DAC} = V_{REF} + \Delta V_T. \tag{3.10}$$

If the reference voltage is known, then it can be subtracted from the measurement to obtain the BTI measurement. If the voltage is not known exactly but is constant, the BTI can still be determined by referencing every measurement to a chosen measurement. For example, a measurement during production testing before aging has occurred can act as the reference for subsequent measurements. The negative power supply voltage is a convenient choice as reference voltage that is both known and constant, but this presents problems when this reference is also used by the DAC. Good matching cannot be guaranteed between M3 and M4 since their active area is not a free design variable. For BTI measurements, it is common to lump the

mismatched parameters into an initial difference in the threshold voltage. If the M3's threshold voltage is initially lower than M4's and the minimum DAC voltage is equal to the reference voltage, then the measurement can only indicate the initial ΔV_T is less than or equal to 0 V. Aging will eventually cause the ΔV_T to become positive and measurable, but valuable data on the BTI trend is lost until this occurs. Choosing a reference voltage that is statistically likely to have a larger magnitude than the initial ΔV_T eliminates this issue, though the reference voltage should not be made so high that it is difficult to satisfy the inequalities guaranteeing M1-M4 operate in saturation.

Aging-Related Errors from Other Components

The monitor's measurements should be solely influenced by BTI on M3. To prevent other device aging from affecting the measurement, steps are taken to either minimize the other transistors' aging or to reduce the monitor's sensitivity to their aging. The measurement phase of the monitor is very short compared to the stress phase and it is assumed no aging occurs during this brief time interval. Besides BTI, HCI and TDDB are the most prevalent aging mechanisms for MOSFETs and their effects should be considered in the monitor. TDDB is also caused by large gate biases, but the effect is an increased leakage current through the gate instead of a change in threshold voltage. HCI occurs when an inversion layer is formed in a transistor and a large drain-source voltage causes energetic charge carriers to enter the dielectric; this results in a change in threshold voltage. Most of the transistors in the monitor do not conduct current during the stress phase, so HCI is less of a concern than BTI and TDDB.

It is most important to prevent M4 from aging because it provides the reference threshold voltage, and aging is prevented by maintaining its gate-source and drain-source voltages at 0 V during the stress phase. M1 and M2 must remain in strong inversion during stress to set the

source voltages of M3 and M4 to VDD. They are biased for a low overdrive voltage to minimize BTI-related mismatch between the branch currents. The low overdrive voltage also means M1 and M2 are not at risk for TDDB. The switches M5 and M6 are OFF during the stress phase (no inversion layer), so they do not degrade from BTI or TDDB. M7 is ON during stress and will have the worst-case bias conditions for BTI. This may cause significant increases in its ON resistance. This is not an issue, however, because the switch does not conduct sustained current meaning there is no voltage drop across the switch while it is ON. M8 is OFF during the stress phase and the terminal connected to the gate of M4 is biased with VDD, making it the drain of M8. Depending on the DAC voltage, the gate-source voltage of M8 is less than or equal to 0 V. M8 will not degrade from PBTI, but there has been some study of opposite-signed bias on transistors (NBTI in nMOS and PBTI in pMOS) that show an effect on the threshold voltage. Experimental evidence of NBTI in nMOS suggest a minute decrease in the ON/OFF resistance[39], making this aging effect a non-issue.

The switching circuit that selects either the reference voltage or stressing bias to M3's gate is purposefully not defined at the transistor level in Fig. 3.2 because its architecture depends on the choice of reference and stress voltages. If the stress voltage is static, the switching circuit can probably be realized by a single transistor for each switch path. Dynamic stress signals likely require at least a transmission gate to preserve the signal's amplitude through the switch, and fast signals may need a high-speed buffer to prevent rise/fall time degradation of the signal to M3's gate. In either case, changes to the switch resistance in the path leading to the reference voltage will not affect the accuracy of measurements because the lack of current in the path means there is no voltage across the switch, just like M8. The same is true for the stress voltage switch if the stressing bias is DC. For scenarios with dynamic stress signals, the switch/buffer is

probably vulnerable to BTI, HCI, and TDDB. The best solution for this is to oversize the transistors in the switch/buffer to compensate for the eventual increase in ON resistance from aging.

Regarding the components sensitive to TDDB, the impact on the monitor depends on the magnitude of stress-induced leakage current (SILC). Experimental evidence of TDDB reports the degradation rate to be extremely nonlinear, with the breakdown initially happening gradually and then abruptly speeding up. This makes SILC measurements appear to have an abrupt jump on a linear time scale (generally from pA to μA for constant voltage stress)[40]. The SILC before the jump will be low enough to have negligible effects on the monitor's operation, but the effects after a rapid breakdown are akin to a hard defect. A hard defect will cause the monitor to fail and diminish the diagnostic capabilities of the system, but hard breakdown of M3 can also cause unwanted loading effects on the source of the stressing bias. The inclusion of a buffer, even for DC stress voltages, can practically eliminate this concern. A hard dielectric breakdown in the transistors of the monitor will cause dramatic shifts in the source voltages during measurement for most cases, and this will appear as an anomaly in the measurement trend making the condition somewhat detectable. Additional information to predict the time-to-breakdown and probable SILC may be obtained from other compact aging monitors, like the one presented in [41], and the combination of BTI and TDDB monitors will improve the long-term reliability of a system.

ΔV_T Comparison and Data Conversion

The proposed monitor uses multiple evaluations of a comparator in a successive approximation algorithm to force the source voltage of M4 equal to that M3. Most BTI measurements reported do not exceed mV accuracy, and this sufficient for the monitor application considering the variance of the BTI distribution can be much larger than this[28],

[29], [42]. This sets the gain requirement of the comparator. Regarding the input offset of the comparator, an offset is already expected from mismatch between M3 and M4, and the comparator's unknown offset can be removed from the BTI measurement using the method previously described as long as the offset is constant. Aging of transistors in the comparator can create a time-varying offset voltage, though, which is not calibratable. The major contributors to input offset are the differential input pair, so it is imperative to minimize their aging. One potential solution in processes with almost no nMOS PBTI is to use an nMOS input pair. A more reliable and widely applicable method is to instead make sure the input pair is not stressed for the majority of its lifetime. The NBTI monitor's comparator inputs will be the VDD voltage during the stress phase, so forcing the input pair's source and drain voltages to VDD during this phase and prevent aging just like the method used for M4. This can be accomplished by adding a power-disabling circuit to the comparator's input stage like what is shown in Fig. 3.3. BTI in the comparator is also a concern when taking measurements. Measurement errors from BTI in SAR ADCs have been reported, caused by a short-term offset voltage from the fast charge trapping at permanent sites in the input pair. Offset cancellation techniques[43] and stress equalization[44] have been proposed to correct these errors.

The speed of the comparator depends on the desired conversion speed of the monitor, a decision influenced by the recovery rate of BTI. If fast measurements are desired to find the peak threshold voltage, the measurement of a device must be completed within microseconds after removing the stressing bias[19], [20]. This pushes the limits of most SAR ADC's sampling rates. The amount of BTI recovery in M3 depends on its overdrive voltage and how long it is in the measurement mode. Since the overdrive voltage of M3 is set by the choice of biasing current, it is possible to limit the amount of BTI recovery provided the inequalities for M1-M4 in

saturation remain satisfied. This makes the monitor's operation closer to on-the-fly measurements (stress not removed) than the stress-measure-stress technique and it could potentially increase the slack time for data conversion.

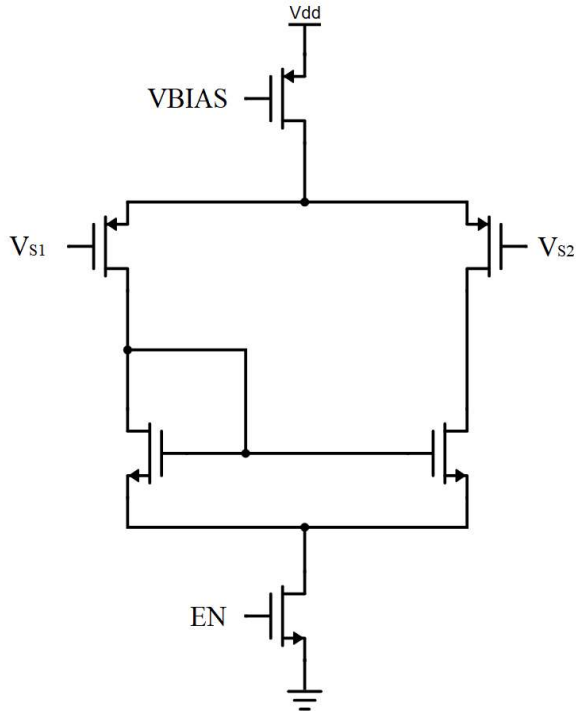

Figure 3.3 Comparator input stage with power-disabling capability.

This monitor uses mixed-signal feedback to bias the gate of M4, but an analog feedback signal could be used instead through simple modifications of the monitor's core. The comparator can be replaced with an opamp whose output is connected directly to M8, and an ADC with sample and hold circuits can take the BTI measurements. Issues may arise with this approach if the ADC is located far away from the rest of the monitor(s) due to issues with routing analog signals, as was mentioned in the previous chapter when discussing the analog test bus.

Sampling BTI from Multiple Devices

Estimations of the mean and variance of the BTI distribution are made by measuring multiple copies of identically stressed transistors. The devices in this array are representative of a transistor that is concerned to cause a fault at the part's EoL, so the array of devices must age similarly to this critical device. BTI depends on process parameters, biasing, and temperature; the device array should be placed close to the critical device to minimize aging variation from process and temperature gradients. The unaged device should be placed close to the aging array to minimize errors from unequal overdrive voltage terms from (3.3). Identical stressing of the array requires the signal source to have enough driving strength to bias the array. Buffers can increase the driving strength to sections of the array, and multiple buffers should be used to section the array instead of one large buffer so that a hard breakdown of one device from TDDB does not compromise the entire array. Local random mismatch between the array devices and the reference device will result in an initial distribution of threshold voltages. This is not a concern for subsequent BTI measurements as it has been shown from experimental measurements that the initial threshold voltage distribution and aging are uncorrelated[20], [29], and an appropriate choice of reference voltage to the devices under test prevents a loss of data used for determining BTI trends. An example of a random-access array of devices for the monitor is shown in Fig. 3.4.

Each monitor is meant to model one critical transistor in the circuit. Designers define the amount of BTI degradation that can occur in a transistor before a fault occurs prior to fabrication using simulation data. However, the transistor with the lowest initial margin to failure will not necessarily fail first. It is prudent to select a set of critical devices and insert monitors on chip for each device.

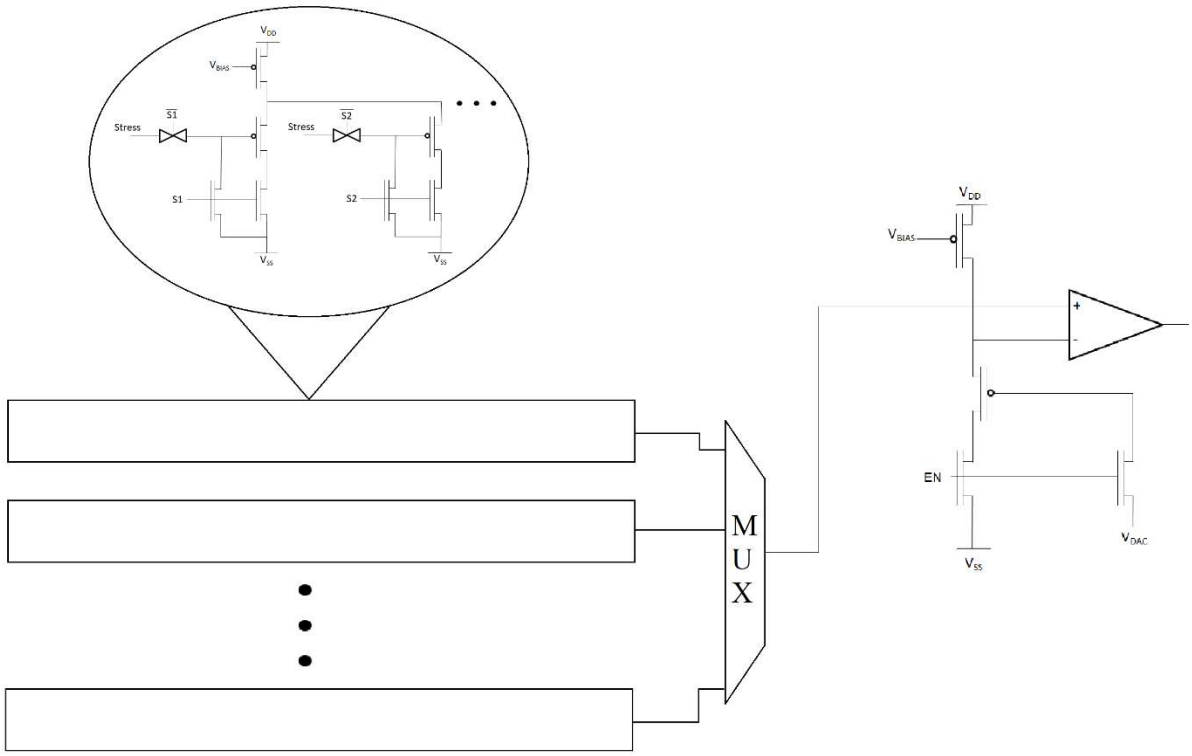

Figure 3.4 An array of aged devices compared to a reference device.

Discussion

This monitor is used to find the probability of a given amount of BTI degradation. This data can reduce the probability of fault occurrence by shutting down the system once a BTI measurement exceeds the specification threshold with the desired confidence. There is no simple procedure for determining the minimum number of devices in the sample set to get an accurate picture of the distribution. This is due in large part to the uncertainty of operating conditions and the uncertainty of the predictive models themselves. It has been shown experimentally that the σ^2 of the ΔV_T is linearly proportional to the mean, and hence increases over time. Initial implementations of the BTI monitor can choose their sample sizes based on predictions of the worst-case stress scenario to give more than enough data to accurately estimate the distribution and continue to enable functional safety measures for the system. Over time, it is expected that

data from the monitor will aid in refining the predictive models, especially for rate operating conditions, so that more precise procedures and engineering thumb rules can be developed to optimize the monitor.

Summary

Aging monitors are valuable inclusions in integrated systems. Providing part-relevant data of device degradation allows parts to be operated right up to a point just prior to failure maximizing the part's useful lifetime. Tracking aging as it occurs is anticipated to give foresight into a part's gradual degradation and help with planning its safe decommissioning as it nears its end. These motivating factors must overcome the initial investment costs of including aging monitors in a design, especially when the goal is obtaining statistical data. In this regard, the metrics of a good aging monitor design are the same as the BIST architectures discussed in the last chapter: compact area, efficient data generation, and low resource consumption.

The proposed BTI monitor has a small area/sample ratio to promote larger array sizes and better estimations of the BTI distribution. Like the monitors based on an enabled ring oscillator, the only significant power consumption is during the measurement phase which is assumed to be brief. The mixed-signal feedback loop results in direct conversion of the BTI measurement data into a digital signal for efficient and robust communications and processing. The presented monitor also has a much more straightforward measurement relationship to the threshold voltage compared to other monitor designs. The simplicity of the measurement relationship improves the efficiency of data processing which in turn improves applications of functional safety and reliability.

CHAPTER 4. HARDWARE TROJAN THREATS TO ANALOG CIRCUITS

The last two chapters covered the testing and detection of defects that randomly occur during the life of a part. The BISTs discussed are employed in ICs performing critical functions within the system, which justifies the cost of the additional hardware needed for testing. The importance of these parts makes them vulnerable to a different type of failure, one that is caused by deliberate action from an adversarial party. The potential motivations for these attacks are broad, ranging from simple monetary gain to grand ideological goals. Knowing that components of a system may be targeted for sabotage, the hardware must be made secure.

Valuable electronics are safeguarded against manual attempts to alter the system. Even if an adversary gains physical access to the system, integrated circuits have a natural defense against tampering. The small feature size of devices and the limited number of pins in an IC package makes it difficult to manipulate a finished product without completely destroying the part. One way to circumvent the challenges of unauthorized access to an IC is through a hardware Trojan.

Hardware Trojans are hidden, malicious function physically embedded within a system. Trojans are designed to cause system failure, though the type of failure may not be a complete breakdown of function. The failure may be in more abstract specifications, like the assumption that data cannot be read. Other cases are more like the defect-related faults already discussed, like alterations causing complete breakdown of a system's functions. The characteristic differentiating Trojans from random faults is the precise timing of the induced failure; Trojans are activated at the most opportune time for the adversary (or the most inopportune time for the customer). The meticulous coordination of attack for maximum damage means BISTs used for

functional safety, which only force action after a failure has occurred, are insufficient countermeasures for Trojan activation.

Threat Model

The physical embedment of hardware Trojans makes it nearly impossible to remove or insert them into an already fabricated design. The insertion point must be before fabrication of the circuit. The knowledge, resources, and cost involved in fabricating ICs limits the number of people capable of creating a hardware Trojan in an IC. There has been speculation of companies including kill switches and back doors into their designs on behalf of a government for electronic warfare and espionage[45]. An alternative scenario is an employee or small group of employees are influenced to act out an external organization's agenda unbeknownst to the company. This case requires any inclusion of a hardware Trojan to evade detection during the verification and testing of a product.

IC production has several stages where a Trojan can be inserted, with the general production flow illustrated in Fig. 4.1. Early production stages have the most flexibility for Trojan design and insertion since the system is not fully defined yet, but they also must pass the most reviews, simulations, and testing. Insertions at the fabrication facility can potentially be very difficult to detect, especially if only a small set of parts are modified. Potential threats as subtle as modifying doping levels and as brazen as adding entire circuits to a design have been suggested[45], [46]. However, expertise in multiple disciplines is required to stealthily modify designs this late in the production flow and likely requires a larger number of members in the conspiracy. Fabrication is the last stage where a Trojan can be inserted by an IC, but the production test phase also poses a security concern. Collaborated efforts between a Trojan designer and test engineer can conceal the fact that the part has been compromised.

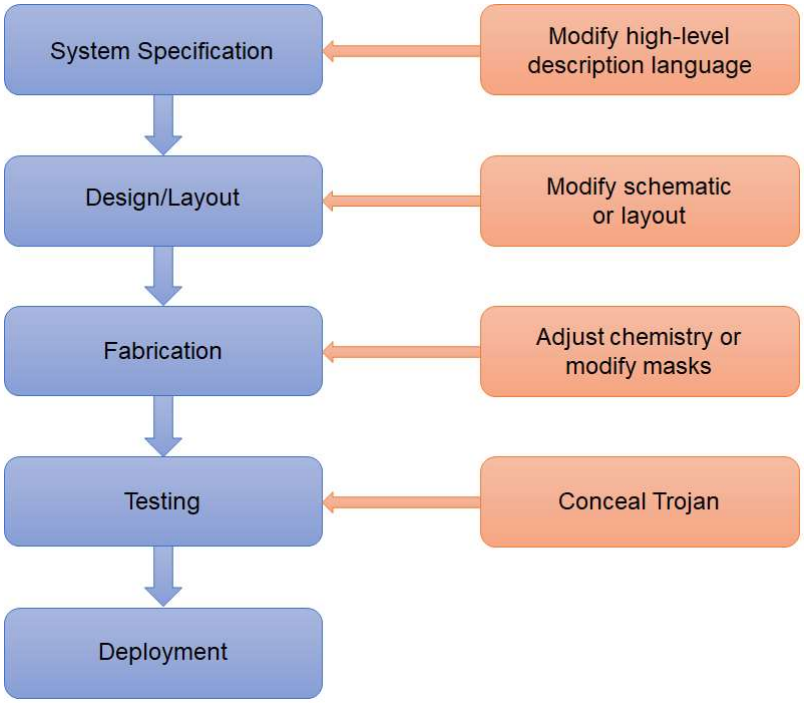

Figure 4.1 Production flow and points of Trojan insertion.

Techniques for detection have been proposed at each stage, where production tests are the final chance to detect a Trojan in an IC before it is handed off to a customer. Security-conscious testing requires foreknowledge of likely targets and a Trojan's characteristics/effects. To this end, numerous taxonomies attempting to comprehensively classify hardware Trojans have been proposed.

Trojan Taxonomies & Detection Methods

The taxonomy described in [47], [48] defines three attributes of a Trojan: the physical characteristics, triggering mechanism, and effect (payload). The categories of physical characteristics assume an alteration from some nominal circuit, which is often referred to as the golden model or golden die/chip. The authors distinguish additions/omissions of components, which they call functional changes to the system, from parametric changes to the system. The parametric changes consider modifications of geometry or another parameter of a component or

wire. Most hardware Trojans conceived to date target and are embedded within digital circuits. The large scale of these systems hides the presence of a Trojan with physical characteristics that cause a functional change. If a golden model is available, some comparisons can be made to authenticate a part. The insertion of a Trojan can result in visually distinguishable changes to the layout, for example, that can be used as a point of comparison. Golden models take different forms for each stage of production. A comparison of netlists can be performed if the Trojan is inserted in the design phase, while insertions at the foundry require die images for visual comparisons. The importance of model abstraction was recognized in [46], [49], and their taxonomy includes attributes of the phase of insertion, the abstraction level, and the general circuit type within which the Trojan is embedded. Searching for architectural modifications cannot be the only method of detection since Trojans have extremely small footprints, and parametric Trojans inserted at the foundry would be completely missed.

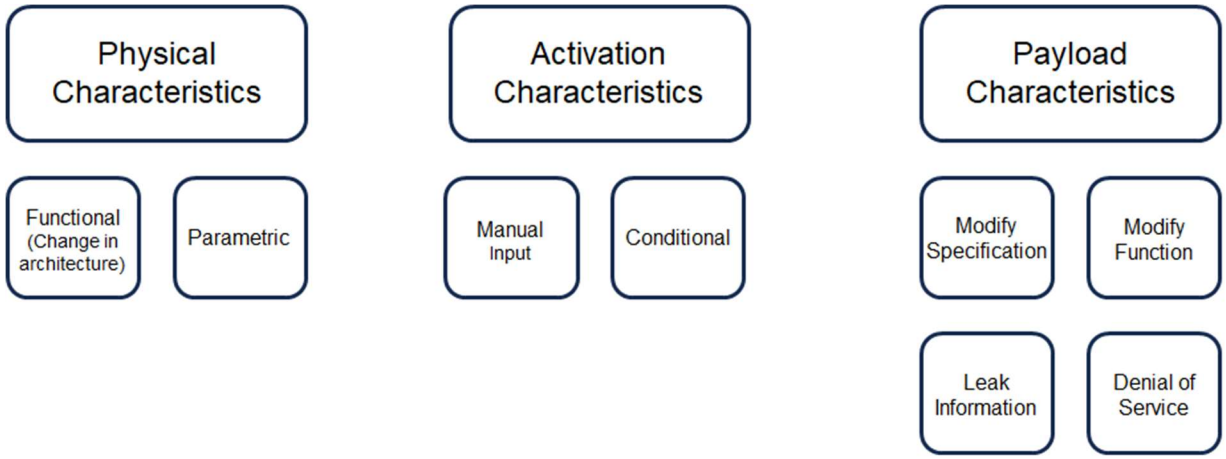

Figure 4.2 Summary of existing hardware Trojan taxonomies.

A stealthy Trojan that is inactive will have at most a minute effect on the system, motivating the specially designed tests for detection. Since most Trojans are embedded within digital systems, the outputs are naturally robust to these variations and simple evaluations of the

output states will not detect the insertion. Tests instead measure the side-channels, which are either the analog system signals (power, biasing) or the system's digital signals analyzed in an analog context (timing, amplitude). Changes in power consumption, delay, noise, and electromagnetic spectrum have all been used to find Trojans. However, unless a design violates a specification, a golden model is needed to determine normal function. Obtaining a golden model may prove difficult. Some security philosophies presume a Trojan insertion in the design carries on to every fabricated part, in which case the part does not possess a golden model. Companies often reuse individual circuits across different parts allowing at least a partial point of comparison, but otherwise a part must be reverse engineered to determine it's free of Trojans. In light of this, some tests attempt to trigger hardware Trojans to detect their presence and effect.

Tests to trigger hardware Trojans use the attributes of the trigger mechanism and the payload of the Trojan. In fact, the taxonomy of [50], [51] only consider these two attributes relevant to classifying the threat. Activations can be triggered directly by an adversary or automatically when a set of conditions are met. The former method requires the adversary to have some access to inputs of the system; the latter method does not require input from the adversary but requires some forethought to what operating condition the Trojan activation will be most advantageous. Detection methods attempting to trigger a Trojan involve applying many combinations of inputs into the system. Since the Trojan must be stealthy, conditional activation must occur only in a rare scenario so there is no accidental activation during functional tests in production. Testing for rare operating scenarios or input patterns helps reduce the number of plausible input combinations to trigger the Trojan.

In some cases, the effects of the Trojan can be subtle even after activation. Activation-based testing can be improved through awareness of probable payloads so that observations of a

system's operation can be focused when looking for a change in performance. The taxonomies of [47], [48] generalize payloads into three categories, a change in specification, a change in function, or leaking information. The change in specification category is used to classify parametric Trojans that degrade normal performance or reduce the lifetime. Another payload category is distinguished in [46], [49]–[51], "denial of service", which simply disables a system function.

Analog Hardware Trojans

Previous attempts to classify hardware Trojans do not consider the possibility of attacks on or embedment in analog circuits. Some of the examples from which the taxonomies were derived do have analog circuits playing a role in the attack, but it is in the context of either a means to trigger the Trojan or to describe the degrading or destructive effects of parametric Trojans in a system. The omission of analog circuits from the list of threatened systems makes it difficult to classify recently proposed analog hardware Trojans. The primary purpose of classifying hardware Trojans is to aid in the conception of test and detection methods, so incomplete taxonomies imply a potential gap in security and Design for Trust.

Analog circuits are not integrated on the same scale as digital circuits. They are not automatically synthesized by standard cells and their design is done by manual placement and sizing of components at both the schematic and layout level. This makes it difficult to conceal architecture modifications and Trojan insertions. Additionally, many analog circuits are quite sensitive to loading, interference, and noise. Comparing the changes in performance from additional hardware insertions between analog and digital systems, the deviations in the analog system are much more significant. This means that functional hardware Trojans targeting analog performances must be much more subtle.

There have been some recently proposed hardware Trojans targeting wireless communications. These Trojans are realized with extremely simple modifications to the nominal architecture making it more plausible for them to be included at the fabrication phase, hence avoiding the issue of architecture reviews. A hardware Trojan used to leak information from an RF transmitter was proposed in [52]. The authors modified the power of the output signal so that a receiver could distinguish between transmitted "1's" and "0's". Two methods of attack were studied; one used a double throw switch whose position was linked to the binary level of the transmitted data to alter the input impedance to a power amplifier. The logic 0 output positioned the switch to an impedance that caused more reflected power and less transmitted power while the logic 1 output caused the impedance to have less reflection. The second method of attack followed the same strategy with less power transmitted for logic 0 than for logic 1, but the Trojan was housed in variable gain amplifiers to alter the gain which in turn altered the signal's amplitude. A very similar Trojan was provided as an example in [53], where the power amplifier of a transmitter was modified to include a switch that alternatively enabled and disabled the amplifier depending on the logic level. While it is doubtful that this type of Trojan was considered while developing the taxonomies of Trojans previously presented, the attack on the transmitter can be classified within these attributes: its physical attributes are a functional change to the circuit, its payload is the leakage of information, and the choice of trigger mechanism is flexible.

Interestingly, the addition of BISTs to enable the testability of analog circuits is also a vulnerability to security. Hardware Trojans inserted in the digital circuitry can control the configuration of DfT analog circuits to either operate normally or in a test mode[54], [55]. The analog circuit architecture and test connections remain unchanged, meaning inspections of the

analog circuit schematic and performance tests will not detect this Trojan. This also presents many new possibilities in the form of payloads. Several hardware Trojan attacks on a LDO were considered in [54]. The test stimulus points were located in the bandgap reference that biased the LDO and the opamp in the LDO's regulating loop. Some forced test configurations caused complete failure of the LDO to regulate the output voltage while others only diminished the regulating capability. These changes to the power management circuit do not necessarily cause faults in the circuits it powers, but they almost certainly cause parametric changes in their performance. Attacks on a SAR ADC were presented in [55] with several inappropriate test mode activations. These Trojans either resulted in errors in the data conversion or the ADC's output being independent of its input. The changes in power supply voltage and data conversion errors most closely resemble the change in specification payload, but the underlying cause is fundamentally different from the cases considered when developing the taxonomies. Unlike the parametric Trojans previously mentioned, these analog hardware attacks are not necessarily destructive, nor are their effects permanent. The hardware Trojans that manipulate test modes can conceivably be disabled just as easily as they are triggered, making their effects temporary and more difficult to detect using side-channel analyses.

Another type of hardware Trojan, distinct enough to warrant its own class, exploits alternate stable modes of operation in a system. Stability used to be discussed solely due to concerns about reliability. Non-global stability of operating points is a well-known problem in analog reference circuit designs. It is not uncommon for engineers to observe a reference circuit converging to an undesired stable mode of operation after power-on, earning the phenomena the name "start-up problems". The standard solution is to add a start-up circuit to the design, a circuit that globally stabilizes the system. In their approach to verify the effectiveness of start-up

circuits in DC references, the authors of [56] referred to alternate modes as stable Trojan states because they are undesired, hidden equilibria of the systems. This concept was further explored for an analog hardware Trojan in an Inverse Widlar current reference[57]. This type of Trojan does not make any changes to a circuit's architecture, nor does it cause any change in system performance from the nominal case when the circuit is not operating in Trojan state. This makes the presence of the Trojan transparent to architectural review and side-channel analysis, and the class of Trojan came to be known as Power, Area, Architecture, and Signature Transparent (PAAST)[58], [59]. PAAST Trojans are not restricted to DC circuits; several examples of dynamic PAAST Trojans were presented in [60], and a case study of a coupled ring oscillator was presented in [59] where a power supply voltage glitch triggered a change in the oscillator's phase.

PAAST Trojans cannot be classified within the taxonomies discussed so far. The activation mechanism attributes still apply to these Trojans, but the physical characteristics and payload types previously defined are inadequate to describe this threat. The PAAST Trojan does modify nominal circuit architectures but terming it a parametric Trojan is not appropriate either since stable Trojan state(s) are not necessarily able to be inserted/removed through parametric adjustments only. This also raises an issue on the assumption of Trojan insertion. The alternate modes of operation are inherent to a circuit architecture, and adversarial designers do not insert the Trojan as much as they tune parameters to achieve the desired activation characteristics and payload[57]. The next section provides definitions for the PAAST Trojans so their classification can be incorporated into the existing taxonomies.

PAAST Trojan Classification

Before proceeding to definitions for different PAAST Trojans, some assumptions must be made to distinguish these threats from reliability issues and normal circuit functions. The

existence of multiple stable modes in a circuit does not necessarily indicate a PAAST Trojan. A latch, for example, is a fundamental building block and its bistable operation is its key feature. The stability traits of the circuit must be different from the circuit's desired operation to qualify. Another necessary assumption comes from the fundamental property of a hardware Trojan: it is an attack on the system defined by malicious intent. As previously mentioned, start-up problems have long been studied because of their imposition on system reliability. Hardware Trojans must be analyzed separately from random failures because the function is intentionally executed for maximum effect. Finally, the function must be tailor-made for a system to be considered a PAAST Trojan. Since a circuit can have undesired stability traits simply for the fact that it was missed during production, it is possible that an adversary becomes aware of the vulnerability and exploits it. This kind of attack is a valid security concern, but the type of function and extent of damage is mostly outside the control of the adversary. The designation of PAAST Trojan should be reserved for cases where the function is specifically designed for a malicious purpose.

A PAAST Trojan is defined with reference to the desired stability of a system. The first type of PAAST Trojan is an undesired stable equilibrium. As an example, consider the current reference circuit studied in [57] and shown in Fig. 4.3. The desired case is the circuit having a globally stable equilibrium. The circuit can instead have three equilibria, one unstable and two stable. With two stable equilibria, the Trojan designer must make sure that one equilibrium corresponds to the nominal function of the circuit and meets all specifications while the other equilibrium corresponds to the Trojan function. This task requires some expertise because the two modes' functions are linked by the same set of design variables. The authors of [57] showed that the existence of the Trojan equilibrium could be ensured for certain ranges of temperature, a range that can be selected by appropriate sizing of the transistors.

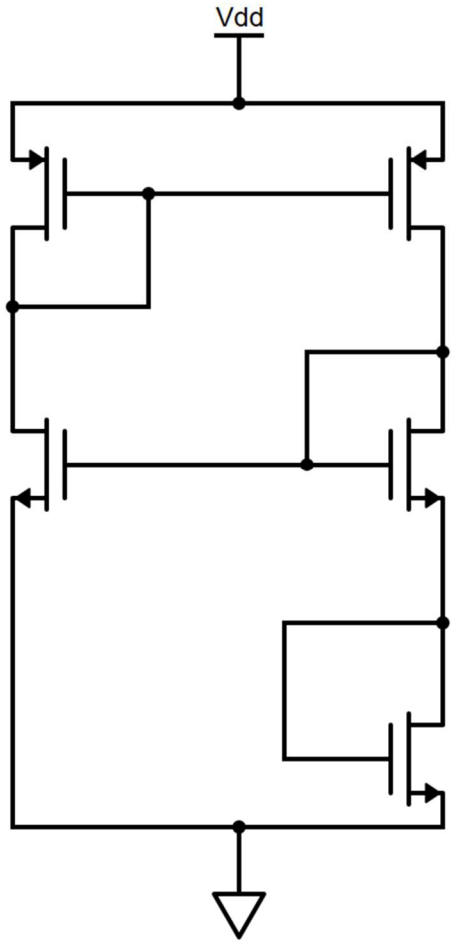

Figure 4.3 Widlar current reference with Trojan equilibrium.

The second type of PAAST Trojan is an undesired stable limit cycle. A limit cycle is a sequence of states that results in a periodic waveform. Several examples of oscillators and filters with Trojan limit cycles, which were confirmed with simulations, were presented in [60]. An interesting case study on designing for the existence of a Trojan limit cycle was presented for a coupled ring oscillator circuit in [61], and the circuit is shown in Fig. 4.4. The coupled oscillator consists of two ring oscillators connected by a set of inverters to synchronize the frequency and phase of the output. The desired stability of this circuit is one stable limit cycle and no stable equilibria. The authors of [61] simulated several cases of varying coupling strength (controlled by different sizes of coupling inverters) and found four different scenarios. One of the scenarios

did not have a stable limit cycle but did have stable equilibria. This is not a case that an adversary would use since the circuit cannot operate in the nominal mode. Another scenario had a single stable limit cycle, the desired characteristic of the circuit. The other two scenarios were candidates for a PAAST Trojan, one with a stable limit cycle and stable equilibria and the other with two stable limit cycles. This shows that Trojan equilibria can be designed in dynamic circuits, and the opposite case is also possible with a Trojan limit cycle designed in a static circuit.

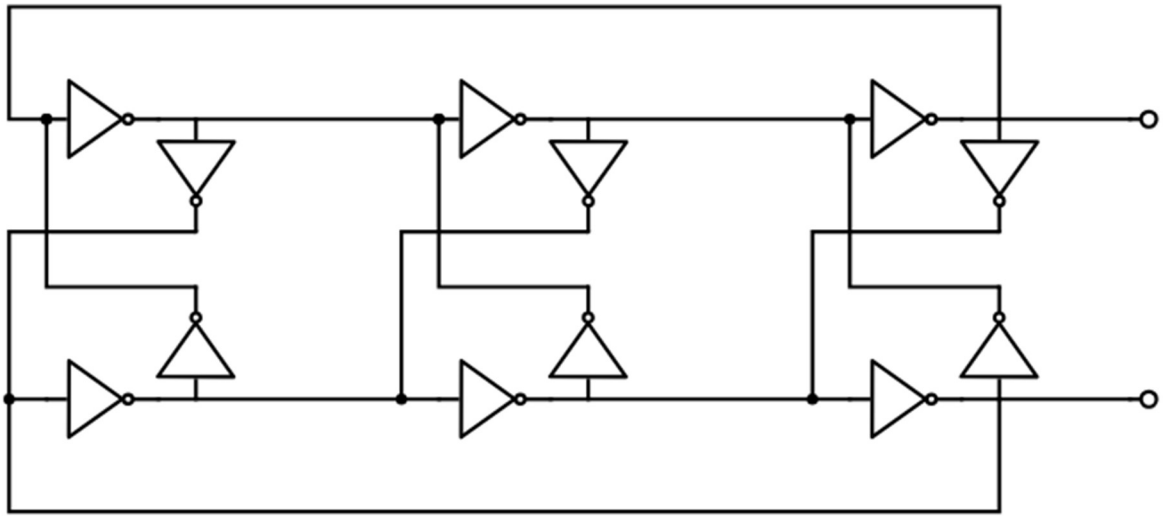

Figure 4.4 Coupled ring oscillator with Trojan equilibria or Trojan limit cycle.

The circuits in Figs. 4.3 and 4.4 are normally modeled as autonomous systems, meaning the output solution to which the system converges is dependent only on the initial conditions of the circuit. In reality, circuits will experience perturbations component noise, power supply transients, capacitive coupling, etc. If a perturbation is large enough, then it can force the system from its nominal equilibrium or limit cycle to the Trojan state(s). The authors of [62] transmitted pulses through the parasitic coupling of adjacent wires to cause a bit flip on an otherwise inaccessible wire, a technique they used to disable a cryptographic core and leak information. A

similar approach can be used to activate PAAST Trojans in reference circuits lacking other inputs for stimuli.

Circuits that do have designated inputs (nonautonomous systems) are modeled in systems analysis by defining a zero-input condition. A static input value is chosen as a reference for the zero-input condition, and the system model becomes equivalent to an autonomous system while the input remains at this value. The nonautonomous system's equilibria and limit cycles are defined with respect to the zero-input condition. These circuits can also have Trojan equilibria or Trojan limit cycles, such as the Trojan limit cycle shown in an active filter in [63], and the designated input provides an additional path from which the Trojan can be activated.

There is a third type of PAAST Trojan that applies only to nonautonomous systems. This is an undesired stability property where the circuit has a globally stable equilibrium but is not input-to-state stable. A system that is input-to-state stable has the property that its output, regardless of initial conditions, will eventually converge to a unique solution (static or dynamic) that is a function of its input. Input-to-state stability is a stronger property than a globally stable equilibrium, meaning if the system is the former then the latter is also true. An example of this type of Trojan is maliciously designed jump resonance in an active filter. Consider the filter in Fig. 4.5, where the desired property is input-to-state stability. Simulations were performed using a single-tone sinusoidal input to the filter, with a bidirectional sweep of input frequency while maintaining the amplitude constant. The resulting Bode plot of Fig. 4.6 shows a range of input frequencies where the output is not unique.

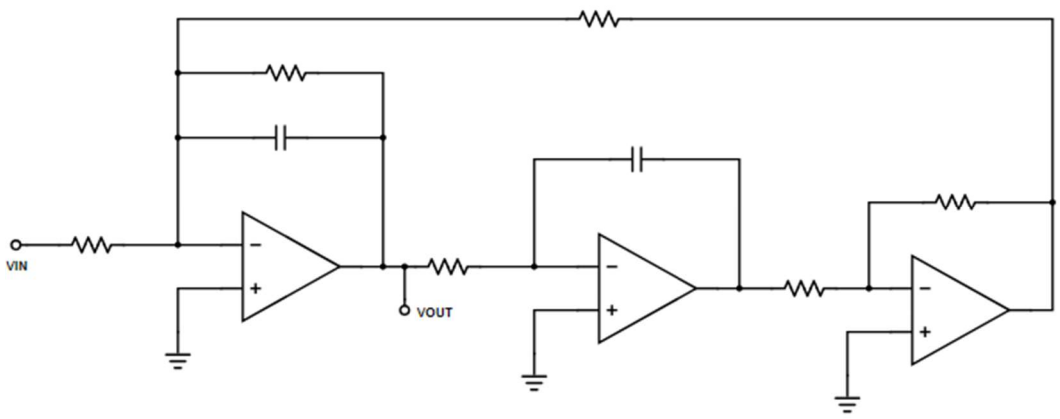

Figure 4.5 Active filter that is not input-to-state stable but has a globally stable equilibrium.

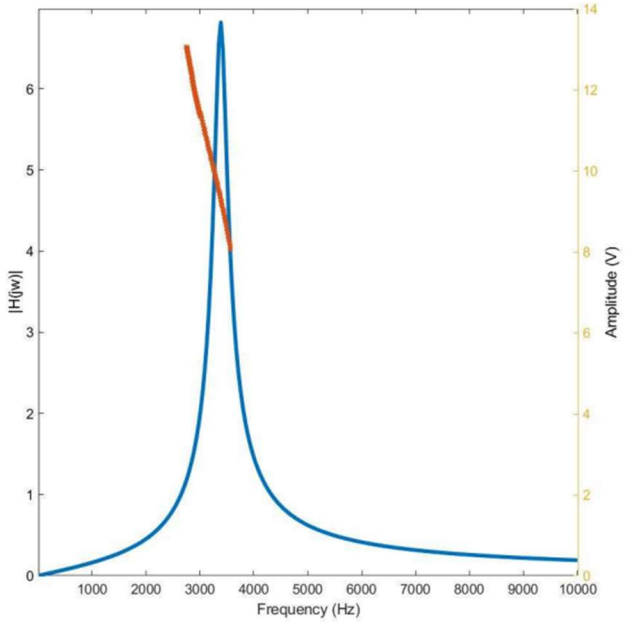

Figure 4.6 Jump resonance in the active filter. The blue curve plots gain for the sweep in the increasing direction and the orange curve plots gain for the decreasing direction.

Reconsidering the taxonomy presented in the previous sections, the PAAST Trojan does not require the activation characteristics attribute to be modified, and the payload types only need a broader interpretation of how analog circuits modify system specifications. Since the physical characteristics list does not adequately describe PAAST Trojans, a new characteristic based on the type of stability problem must be included to classify the Trojans. A circuit that is

input-to-state stable does not have a PAAST Trojan. The two major categories for the stability characteristics are the circuit does or does not have a globally stable equilibrium. The first category is used to classify the third type of PAAST Trojan discussed, where the circuit is not input-to-state stable but has a globally stable equilibrium. The other category covers the Trojan equilibrium and Trojan limit cycle. As for the phase of Trojan "insertion", sometimes the undesired stability trait is already present in the design. However, this classification of PAAST Trojans requires intentional inclusion and tailoring of the function which requires deliberate action from an adversary. The phase of production where the PAAST Trojan is tuned/verified can be used as an interchange of the phrase "inserted" used for the other Trojan types.

Unlike other hardware Trojans, there is no golden model that can be used to find the PAAST Trojan; the adversary does not conceal the presence of this Trojan in the same manner as others and it is likely the PAAST Trojan is hiding in plain sight. Informing designers about this threat is the most important step to preventing the attack. The only type of tests that are effective to detect these Trojans are those attempting intentional activation. There has been some headway in detecting Trojan equilibria, including software to automatically perform break-loop homotopy analysis using circuit simulators[56], [64]–[66]. Analyzing circuits to detect Trojan limit cycles is a more difficult prospect, and the typical approaches are ad hoc methods specific to a circuit architecture[60], [63], [67]. Determining input-to-state stability is even more challenging, though there are some models for predicting jump resonance[68], [69]. The numerous difficulties associated with detecting PAAST Trojans makes it all the more important that the threat is classified so that more verification and testing methods can be developed to detect them.

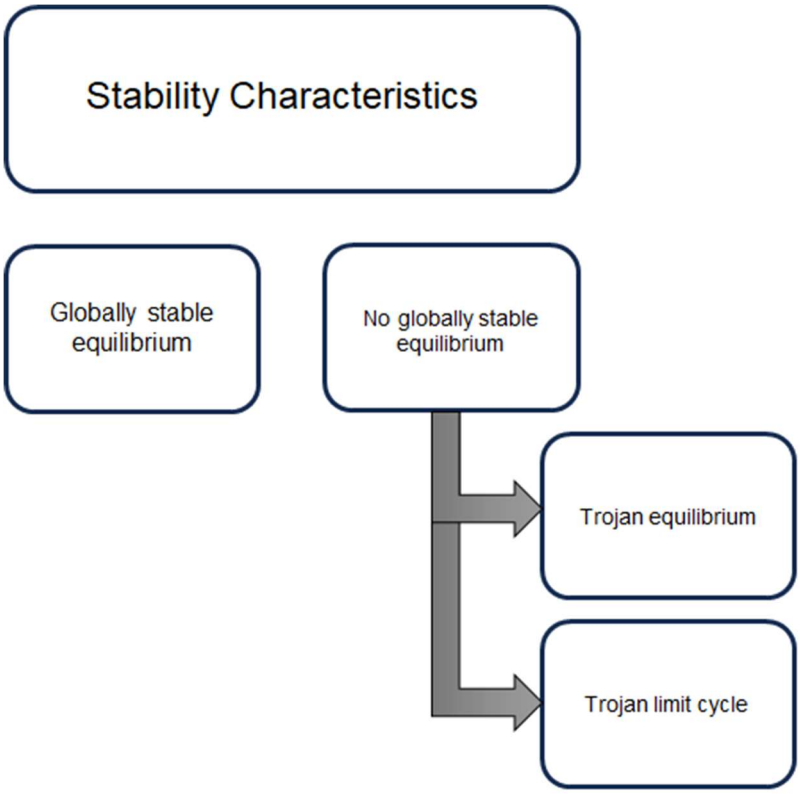

Figure 4.7 Stability characteristics for PAAST Trojans.

Summary

The review of hardware Trojan classification and detection methods considered in this chapter makes it clear that many of the assumptions about the Trojan threat need to be updated to include analog design security. Based on the recent drive to improve functional safety and testability of analog systems, it is expected that analog systems will soon be a critical topic in the security community as well. The summary and classification of PAAST Trojans that was presented fills a gap in the list of plausible avenues of attack and is an important step in the continued development and improvement of Trojan detection methods. A case study of a PAAST Trojan is presented in the next chapter to provide further details on how these Trojans are designed and activated.

CHAPTER 5. TRIGGERING A PAAST TROJAN

The previous chapter describes the different types of PAAST Trojans using a stability characteristics-based classification. This chapter covers the design and measurement of a circuit with a PAAST Trojan in a coupled ring oscillator, which is desired to have one stable limit cycle. The type of Trojan designed in this study is an undesired limit cycle. In order to trigger the Trojan, a practical and stealthy method to create a voltage glitch on the power supply was devised.

Coupled Oscillator Applications

A coupled oscillator circuit consists of multiple oscillators connected together to synchronize their frequencies and create a specific phase relationship between their outputs. These circuits are used in many different applications including signal modulation in RF communications, clock and data recovery systems, and clock synthesis. Coupled oscillators can offer an advantage in power supply noise immunity compared to a single oscillator[67], [70], [71], and they have been used phase- and delay-locked loops for low-jitter applications[72], [73]. These structures are also beneficial when multiple outputs are needed with evenly separated phases, such as modulation in wireless communications[74], [75], and clock and data recovery using phase interpolation[73]. Unfortunately, the multitude of feedback paths often results in undesired equilibria and/or limit cycles in these circuits.

One issue with coupled oscillators is ensuring that they start up. When power is applied, the circuit should begin oscillating with the output amplitude growing to the desired level. However, if the current injected into the oscillators by the coupling network is too large then a stable equilibrium is possible. A conceptual explanation for this is coupled ring oscillators typically have feedback paths that form loops resembling latches. References [61] and [76] both

present cases where the inverting delay cells of the coupling network are too large relative to the delay cells in the oscillators and result in the circuit having stable equilibria. On the other hand, the coupling strength cannot be too weak, or the oscillators will not effectively injection-lock and the benefits of the coupled oscillator will be diminished. Therefore, designers must choose the strength of the coupling network within a range that optimizes performance but also ensures proper start-up.

Undesired stable limit cycles are fairly well-documented for coupled oscillators, though usually it is discussed as a matter of reliability rather than a security concern. Reference [70] analyzes quadrature LC oscillators with the multiple stable limit cycles. It was observed that the output of one oscillator was able to either lead or lag the other output by 90^{o}, what the authors of [70] called phase ambiguity. They also noted that the free-running frequency of the oscillators changed depending on which phase mode the oscillator operated, termed frequency ambiguity. Phase and frequency ambiguity also appear in coupled ring oscillator circuits, a common alternative to LC oscillators due to their compact area in integrated circuits. Time-domain waveforms of the coupled ring oscillator reported in [61] and [77], and shown in Fig. 5.1, show two possible phase modes for a given coupling strength, one where the outputs are in phase and one where the outputs are 180^{o} out of phase. The cyclic-coupled ring oscillator in [71] showed possible alternate phase relationships for their oscillators' outputs, though this was irrelevant to their application since they only required the phase difference between stages to be equal and the frequency regulated to extract a harmonic of the coupled oscillator's running frequency. Another coupled ring oscillator circuit designed for quadrature phase outputs was reported to have a stable harmonic oscillation. In addition to their contributions on start-up verification of the

quadrature ring oscillator[78], a case was presented in [79] where the oscillator ran at a frequency that was the third harmonic of the desired running frequency.

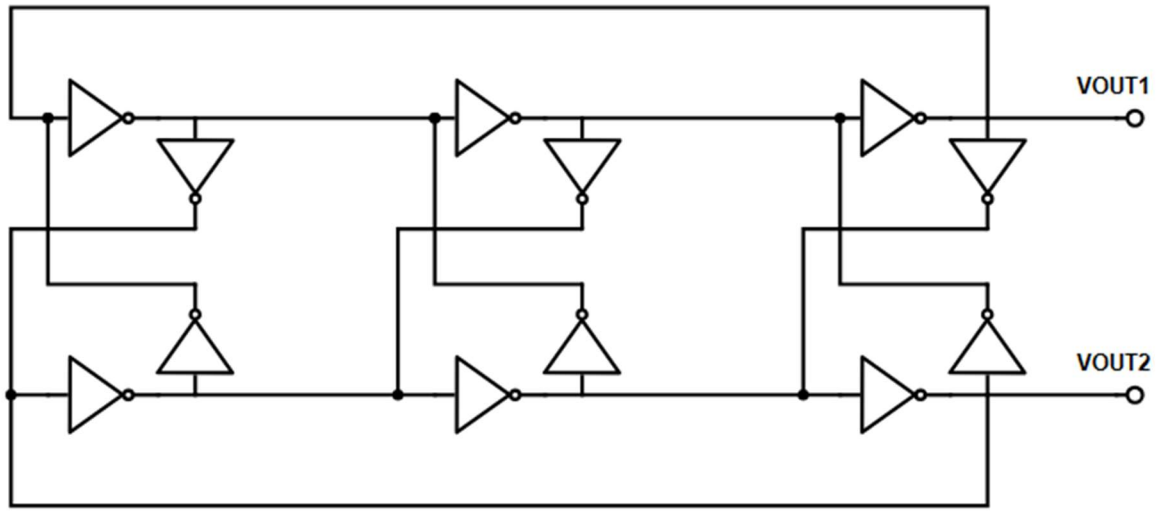

Figure 5.1 The coupled oscillator architecture to be designed with a PAAST Trojan.

With these numerous examples, it is clear that coupled oscillator architectures are very vulnerable to PAAST Trojans, but a means to activate the Trojan is still required for it to be a concern. Oscillators are autonomous systems, meaning their output(s) are determined only by nominally invariant parameters like the power supply and bias voltages/currents, and the initial conditions of the circuit. The lack of user inputs into the circuit means that any perturbation of the system that could activate a Trojan must come through a side channel. A potential means of perturbing the system is interference through parasitic components in the circuit. An attack using intentional capacitive crosstalk to gain an encryption key was described in [80], where pulses on traces running parallel to traces in the cryptographic core caused a bit change that prematurely ended in the encryption algorithm and allowed the key to be deciphered. Another attack option is through the supposedly invariant supply or bias voltages into the circuit. Reference [81] presented circuits with Trojan limit cycles, including the oscillator in Fig. 5.1,

and showed that a single pulse on the power supply with sufficient width and amplitude could trigger the Trojan.

Although hardware Trojans provide much more access to the internal functions of integrated circuits, adversaries still need to gain enough access to the victim part to trigger the Trojan. Considering the power supply attack of [81], one must ask how access to this vital system has been gained. Previous studies of attacks using power supply glitches have used specialized external equipment, like pulse generators, as evidence that such an attack can induce faults[82]. These manipulations have a global effect on the power supply and affect every circuit in an IC. Many hardware Trojans aim to modify a single function, so they rely on the rest of the system operating normally. Means of injecting glitches only at specific points through ionizing radiation and body bias injection have been proposed, though both methods require removing the package of the part[83], [84]. This level of access implies that a hardware Trojan is not needed for the attack. A more realistic trigger scenario is that the adversary has access to another less critical channel into the part through which they may indirectly and temporarily influence the power supply. This is similar to the scenario presented in [80], where the adversary has permission to input data to be encrypted and uses those inputs to indirectly corrupt the encryption process. The next section will describe the design of the coupled oscillator of Fig. 5.1 so that it possesses a Trojan stable limit cycle and may be activated by a temporary perturbation on the local supply voltage of the oscillators.

The Trojan Design

In this design, the desired operation of the oscillator is defined as a single stable limit cycle and no stable equilibria. More specifically, the two outputs of the oscillator should have a phase difference of 0 radians. The purpose of the Trojan is to cause the output phase relationship of the oscillator to change. The output phase relationship is dependent on the phase shift of the

delay cells and the phase shift of the coupling cells. Like the analysis in [71], the loop formed by the delay cells in the ring oscillators is considered separately from the loop formed by coupling cells to find the possible phase shifts. Consider Fig. 5.2; when the inverters in the ring oscillators are identical, each stage has an equal phase shift during steady-state. The same is true for the other loop if each coupling inverter is identical. The sum of the phase shift around each respective loop will be an integer multiple of 2π,

$$3\theta = 2n\pi \tag{5.1}$$

for the ring oscillators' cell phase shift and

$$6\varphi = 2m\pi \tag{5.2}$$

for the coupling inverters' phases shift. Since the cells are inverters, it is assumed that the phase shift must be greater than π. The upper and lower bounds for each cell's phase shift are

$$\pi < \theta, \varphi < 2\pi. \tag{5.3}$$

There is only one solution that satisfies (5.1) and (5.3), n=2 and θ=$4\pi/3$. There are two solutions that satisfy (5.2) and (5.3): m=4 and φ=$4\pi/3$, or m=5 and φ=$5\pi/3$. In the loop formed by the coupling inverters, there are three stages between the two outputs of the circuit. This means the former case of coupling inverter phase shift results in an output phase difference of 4π, the desired phase relationship, and the latter case results in a difference of 5π, which will act as the PAAST Trojan.

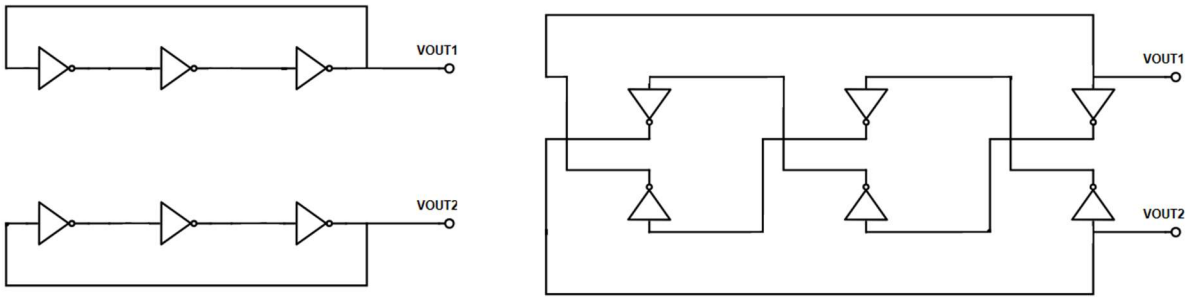

Figure 5.2 The coupled oscillator's feedback loops.

The existence of the Trojan limit cycle is ensured by setting the coupling strength in the coupled oscillator. The coupling strength was described as a ratio of peak current supplied by the inverters of the ring oscillator to the peak current supplied by the coupling inverters in [71]. The peak currents are a function of the inverters' sizes. This design chooses a unit length for the transistors and defines a unit inverter size, where the pMOS and nMOS transistor widths are sized with a ratio to deliver approximately the same magnitude peak current. The inverters in the ring oscillators are designed to be an integer factor times larger than the coupling inverters. Such a scenario was described in [61] to show that the size ratios are a bifurcation parameter determining the existence of a Trojan limit cycle. This design chooses the ring oscillators' inverters to be 8 times larger than the coupling inverters.

The method to trigger the Trojan is inspired by the regulation of a phase-locked loop. A PLL locks the output of a voltage-controlled oscillator (VCO) to the phase of reference signal by making small adjustments to the VCO's running frequency. If the VCO's phase lags the reference, its frequency is temporarily increased to "catch up" to the reference phase. In this oscillator, the frequency of the two ring oscillators cannot be independently controlled because of the coupling network, however the phase relationship can still be modified through separate control of the power supply voltage. Experiments with simulations were performed where each

ring oscillator had an independent supply voltage and the supply voltage of the coupling network was linked to one of the ring oscillators'. The coupled oscillator was initialized in the desired mode of operation and the difference in supply voltage was swept. It was observed that the steady-state outputs' phase difference increased with the difference in supply voltage, shown in Fig. 5.3. This curve has a sharp transition to a phase shift of π, and further increases in the supply voltage difference cause little change in the phase. Furthermore, if the coupled oscillator initially operates in the saturated portion of the curve, then a step in ΔVDD to 0 V will settle into the Trojan limit cycle. The trigger creates a temporary mismatch between the ring oscillators' power supplies to activate the PAAST Trojan.

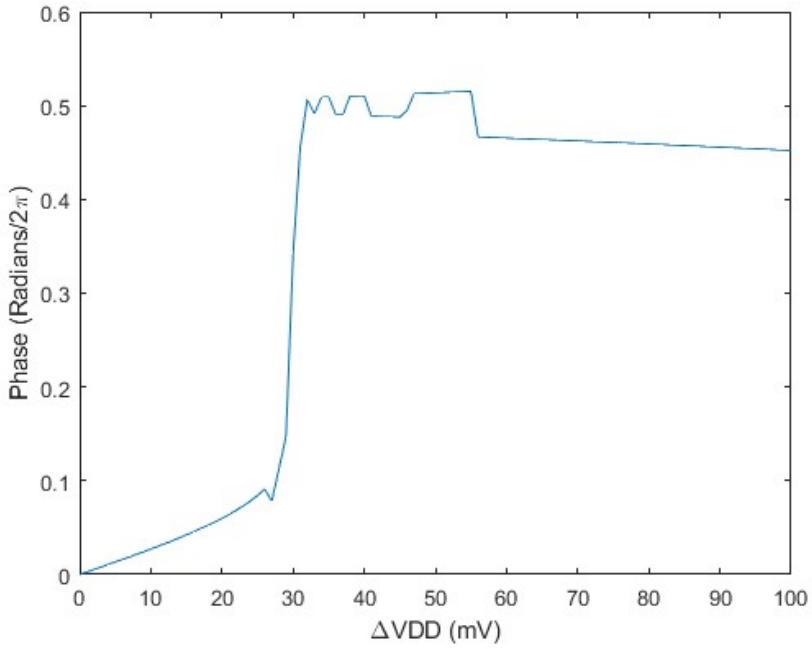

Figure 5.3 Coupled oscillator's output phase difference vs. VDD mismatch.

The power bus for the coupled oscillator is not broken to create the mismatch. Instead, a glitch is introduced to the local supply voltage of one the ring oscillators by suddenly drawing current from the power bus near the ring oscillator. By strategically activating a load in the

vicinity of the oscillator, the voltage on that section of the power bus dips while the other ring oscillator's supply remains constant due to the delay on the power bus. This transient causes the momentary ΔVDD necessary to trigger the Trojan, shown in Fig. 5.5.

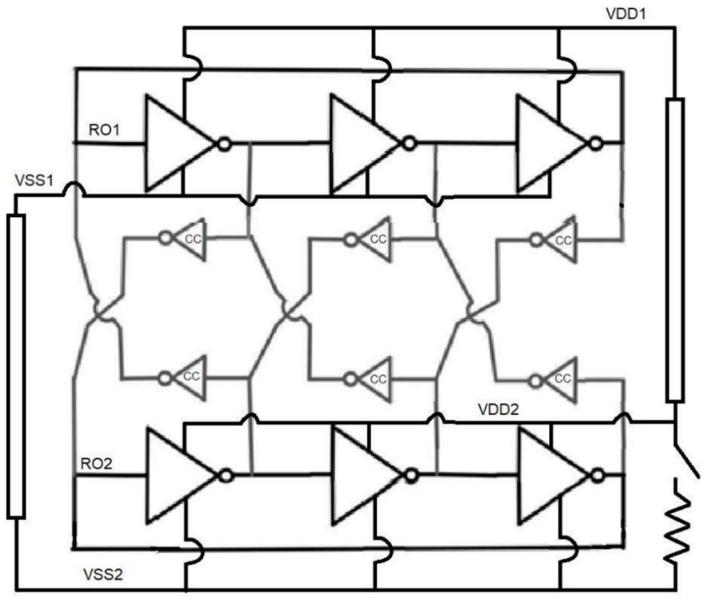

Figure 5.4 Modeling power bus delay to create trigger the Trojan.

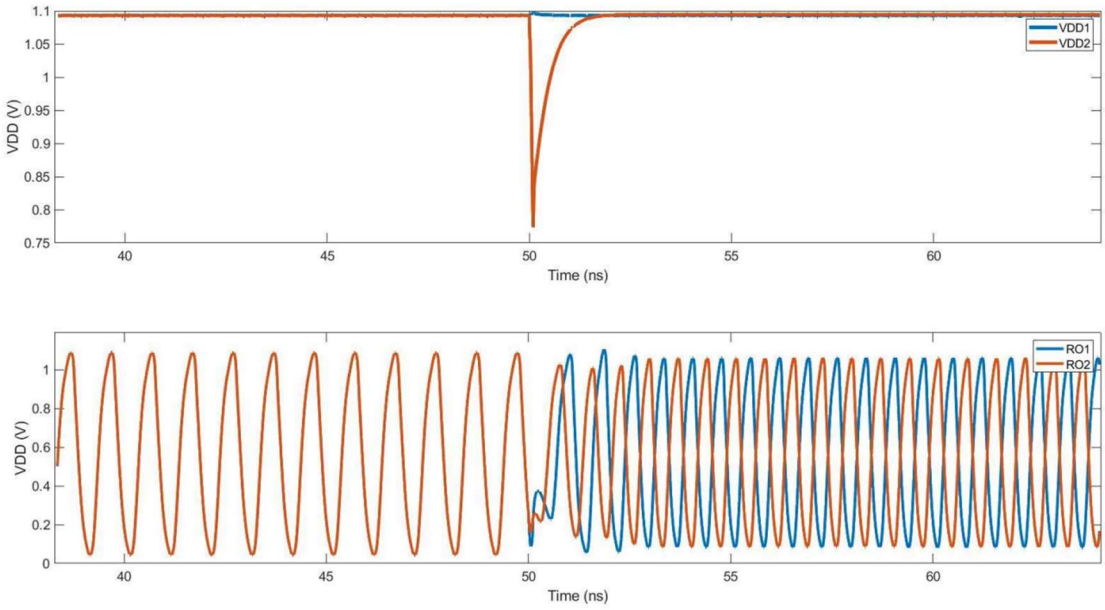

Figure 5.5 A localized power supply glitch triggering the PAAST Trojan.

The magnitude of the load transient needed to trigger the Trojan depends on the delay in the power bus and where the load is located with respect to the oscillator. The adversarial designer must have at least an approximate knowledge of the floorplan for the chip. From there, the adversary can tune the design based on estimates of the bus delay to find what magnitude of current is needed for the Trojan. The load change can be either conditional or from input to the chip, such as an operation that causes increased switching activity of circuits near the oscillator. This design uses a pad driver, a circuit designed for a high driving strength to pass signals to the large capacitive load of a pin pad, as the sudden load caused by a signal switch.

Measurements of Trojan Activation

The coupled oscillator with the PAAST Trojan was fabricated in a 65 nm process. The design was simulated with layout-extracted parasitics to run in the desired mode at a frequency of 800 MHz at 25 ˚C with a supply voltage of 1.1 V. The outputs of the coupled oscillator are buffered on-chip to prevent the measurement equipment from influencing the operation. The fabricated oscillator was measured for both the desired operation and the Trojan function at the same operating conditions as the simulations, where the Trojan was activated by a bit-flip at the input of the pad driver causing the load transient. The measured frequency and phase difference is provided in Table 5.1. The measured results of the nominal operation's frequency is slightly lower than that simulated, possibly due to inaccurate modeling of the pin pads' parasistics. Note also that this coupled oscillator has the frequency ambiguity described in the first section of the chapter. Simulations and measurements confirm the Trojan limit cycle has a higher frequency than the desired limit cycle. The change in phase difference was the primary goal of the Trojan, but a change in the free-running frequency can have consequences to a system's performance even there is a regulating input to control the oscillator's frequency.

Table 5.1 Measurements of the frequency and phase difference for the oscillator's nominal and Trojan function.

	Normal Mode	Trojan Mode
Frequency (MHz)	660	920
Phase Difference (Radians)	0	π

Attempts to activate the Trojan were made for several combinations of operating conditions. The circuit was triggered at different temperatures in the range of 0-70 ˚C at 10 ˚C intervals. At each of these temperatures, attempts were made to activate the Trojan for different supply voltages: 0.8 V, 0.9 V, 1.0 V, and 1.1 V. These experiments were performed to account for cases when the coupled oscillator has its frequency regulated by controlling its supply voltage. Success or failure of the trigger to activate the Trojan is shown in Table 5.2.

Table 5.2 Summary of if the trigger successfully activated the Trojan.

	0 ˚C	10 ˚C	20 ˚C	30 ˚C	40 ˚C	50 ˚C	60 ˚C	70 ˚C
0.8 V	YES	YES	YES	YES	YES	YES	YES	YES
0.9 V	NO	NO	NO	NO	YES	YES	YES	YES
1.0 V	YES	YES	NO	NO	NO	NO	NO	NO
1.1 V	YES	YES	YES	YES	YES	YES	NO	NO

Viewing Table 5.2, there is a clear trend of successful activation with respect to voltage and temperature. This trend is believed to be variable depending on the form of the load transient, because it was confirmed that the Trojan exists for every combination. In cases where the Trojan failed to be triggered, the supply voltage was changed to a case where the Trojan

activation was successful. Then the Trojan was activated, and the supply voltage was adjusted back to the case where the trigger was unsuccessful. The out-of-phase relationship that characterizes the Trojan limit cycle was maintained despite variations in the supply voltage within the defined range. This behavior validates the threat of this Trojan even when the oscillator's frequency is regulated.

Fig. 5.6 plots the frequency of both the normal and Trojan modes with respect to supply voltage at 30 ˚C. The Trojan limit cycle has a higher free-running frequency than the desired limit cycle, and both frequencies increase with supply voltage. For this case, the lower end of the control voltage range results in a Trojan running frequency of 604 MHz and the upper end of the control voltage range has a normal running frequency of 641 MHz. What this implies for the Trojan in a system that regulates the oscillator frequency is there is potentially a range of frequencies where the required control voltages for the normal and Trojan modes both lie within the tunable range of the loop. Going back to the example of phase-locked loop, the activation of the Trojan will cause the oscillator's frequency to initially be too high, so the controlling voltage will start to lower. The oscillator's output eventually returns to the correct frequency, but now with the Trojan phase relationship instead of the desired relationship. Without additional means of observation or regulation, the Trojan function can continue undetected indefinitely.

An unexpected characteristic of the Trojan was observed during measurements that makes this attack more dangerous to systems. There was an interest during the Trojan design to include the ability to deactivate it, meaning forcing the oscillator from the Trojan limit cycle back to the desired limit cycle. Simulations suggested that load transient used to activate the Trojan would almost never successfully force the system back to its original operation, and successful cases happened when the trigger corresponded to a very small range of an output's

instantaneous phase. However, experiments on the fabricated oscillator had several operating conditions where the Trojan could be deactivated, and with an almost 100% success rate. The results of this experiment are shown in Table 5.3. This shows that the Trojan can be toggled ON and OFF, which could make it even more difficult to detect.

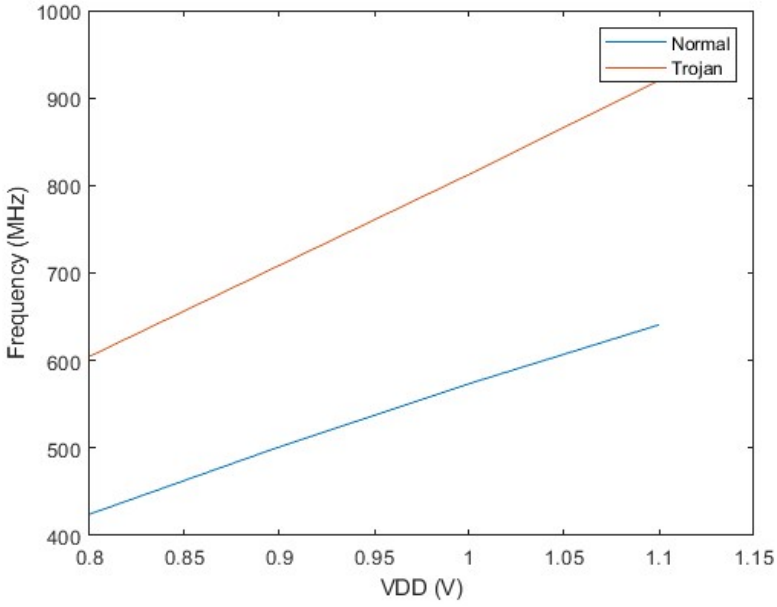

Figure 5.6 Free-running frequency vs. control voltage for the normal and Trojan limit cycles.

Table 5.3 Summary of if Trojan deactivation was successful.

	0 ˚C	10 ˚C	20 ˚C	30 ˚C	40 ˚C	50 ˚C	60 ˚C	70 ˚C
0.8 V	YES	YES	YES	NO	YES	YES	NO	NO
0.9 V	YES	YES	YES	YES	NO	NO	NO	NO
1.0 V	YES	YES	YES	YES	YES	YES	YES	YES
1.1 V	NO	NO	NO	YES	YES	YES	YES	YES

Discussion

With many possible applications for coupled oscillators in analog and mixed-signal systems, this Trojan has the potential for many different functions. The simplest scenario is that the change in phase difference between the outputs causes a fault in the system, in which case the Trojan function is a Denial of Service. Even if the phase relationship is not critical to the normal function, this Trojan can still have adverse effects to the system's performance. In applications where the oscillator's frequency is regulated, it was shown that the system could remain in the Trojan mode while the frequency is adjusted. Integrated oscillators are also very sensitive to temperature changes, which affects their free-running frequency and requires compensation from a control voltage. The other components in a regulating loop can also be sensitive to temperature, which factors into the loop gain of the regulator. Designers have to make sure that the ability to control the oscillator tracks with environmental conditions. When the Trojan is active, this also requires compensation by the control signal. The control signal required to compensate for the Trojan is unlikely to be an optimal choice with respect to the loop gain and the current environmental conditions, which can cause a degradation in performance similar to the Change of Specification type of Trojan function.

Without prior knowledge of the stability issues for coupled oscillators, the only way to detect it at the design phase is to activate the Trojan and observe the relevant signals. This can be challenging depending on how the load transient is realized. Presumably, the adversary will design the trigger so that a rare set of inputs can overtax the system and cause the voltage glitch on the supply bus. As for detecting the Trojan in the field, the ability to deactivate the Trojan makes it extremely difficult to pinpoint the source of the problem, even if the Trojan function has dramatic results. Toggling the Trojan has an effect similar to an intermittent fault, a type of fault that is notoriously difficult to troubleshoot because it requires recreating the exact conditions that

instigated the fault. Without the key information of the Trojan's trigger, it is unlikely that troubleshooting efforts would be able to find the Trojan through in-field testing.

CHAPTER 6. CONCLUSIONS

Industries continue to take advantage of the enhanced functionality that comes with the large-scale integration of circuits. Recent demands for mass data collection and sensing have led to a significant increase in the number of analog circuits deployed in safety-critical systems. This motivates the continued development of techniques that improve the reliability and security of analog circuits, as well as methods to improve these circuits' testability for operational self-diagnostics. The research presented here has shown how the existing practices used to make reliable, safe, and secure designs can be modified or improved to better reach those goals for analog circuits.

Various BISTs used for on-line testing of AMS circuits were reviewed. The defect-coverages, test times, and data collection methods for different BIST architectures testing the same type of circuit were compared, and the efficiency of the test methods were discussed. The importance of a BIST's portability between parts and its compatibility with digital testing architectures was covered, and several BIST's for analog circuits were implemented on a PCB to prove their test efficiency and compatibility. Potential faults in the analog-digital interfaces used to test analog circuits were considered, and methods to improve the system's fault tolerance and detection capabilities were proposed.

To improve the reliability of parts when they reach a time where aging-related faults become likely, an integrated sensor for monitoring BTI was presented. The flexibility of the design in choosing the type of transistor to test and the type of signal used to induce aging makes the architecture applicable for monitoring BTI in both digital and analog designs. The ability to measure BTI of a single device along with the compact area of the monitor makes it better-suited for probability-based estimates of BTI than other in-field BTI monitors. The stochastic

characterization of BTI improves the likelihood that a system can be shut down or recalibrated before a fault can occur, hence increasing the reliability and safety of the system.

The threat of hardware Trojans attacking analog circuits was discussed. It was concluded that the existing taxonomies for hardware Trojans, which are the foundation for conceiving Trojan detection methods, failed to classify many of the analog Trojan attacks. A new set of classifying attributes was defined to describe PAAST Trojans and complement the existing taxonomies.

A case study of a PAAST Trojan was also presented, and measurements demonstrated that this class of Trojan can be robust and reliably activated. The prevalence of coupled oscillators in mixed-signal systems was discussed to emphasize the range of potential functions the Trojan could deliver. The innovative trigger mechanism used to create the voltage glitch shows how this Trojan, and many other Trojan architectures, can be indirectly controlled by an adversary.

In conclusion, the results found in each of these related areas collectively contribute to the improved safety of analog integrated circuits, which improves the overall safety of an IC. By considering security defenses against attacks, testability for random fault detection, and sensing for aging prediction, high-quality ICs can be operated confidently in safety-critical applications.

REFERENCES

[1] G. Gielen, W. Dobbelaere, R. Vanhooren, A. Coyette, and B. Esen, "Design and test of analog circuits towards sub-ppm level," in *2014 International Test Conference*, Oct. 2014, pp. 1–2. doi: 10.1109/TEST.2014.7035330.

[2] S. Sunter and P. Sarson, "A/MS benchmark circuits for comparing fault simulation, DFT, and test generation methods," in *2017 IEEE International Test Conference (ITC)*, Oct. 2017, pp. 1–7. doi: 10.1109/TEST.2017.8242079.

[3] S. Sunter, "Analog Fault Simulation - a Hot Topic!," in *2020 IEEE European Test Symposium (ETS)*, May 2020, pp. 1–5. doi: 10.1109/ETS48528.2020.9131581.

[4] J. Keane, D. Persaud, and C. H. Kim, "An all-in-one silicon Odometer for separately monitoring HCI, BTI, and TDDB," in *2009 Symposium on VLSI Circuits*, Jun. 2009, pp. 108–109.

[5] A. Antonopoulos, C. Kapatsori, and Y. Makris, "Security and trust in the analog/mixed-signal/RF domain: A survey and a perspective," in *2017 22nd IEEE European Test Symposium (ETS)*, May 2017, pp. 1–10. doi: 10.1109/ETS.2017.7968235.

[6] M. Strong, K. Bhatheja, R. Yang, and D. Chen, "A Simple Monitor for Tracking NBTI in Integrated Systems," in *2021 IEEE International Midwest Symposium on Circuits and Systems (MWSCAS)*, Aug. 2021, pp. 1112–1115. doi: 10.1109/MWSCAS47672.2021.9531715.

[7] B. Kruseman *et al.*, "Defect Oriented Testing for Analog/Mixed-Signal Designs," *IEEE Des. Test Comput.*, vol. 29, no. 5, pp. 72–80, Oct. 2012, doi: 10.1109/MDT.2012.2210852.

[8] S. Sunter, K. Jurga, and A. Laidler, "Using Mixed-Signal Defect Simulation to Close the Loop Between Design and Test," *IEEE Trans. Circuits Syst. Regul. Pap.*, vol. 63, no. 12, pp. 2313–2322, Dec. 2016, doi: 10.1109/TCSI.2016.2616159.

[9] N. Liu, S. K. Chaganti, Z. Liu, D. Chen, and A. Majumdar, "Concurrent Sampling with Local Digitization — An Alternative to Analog Test Bus," in *2018 IEEE International Symposium on Circuits and Systems (ISCAS)*, May 2018, pp. 1–5. doi: 10.1109/ISCAS.2018.8351555.

[10] K. Arabi and B. Kaminska, "Testing analog and mixed-signal integrated circuits using oscillation-test method," *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, vol. 16, no. 7, pp. 745–753, Jul. 1997, doi: 10.1109/43.644035.

[11] M. Saikiran, M. Ganji, and D. Chen, "Robust DfT Techniques for Built-in Fault Detection in Operational Amplifiers with High Coverage," in *2020 IEEE International Test Conference (ITC)*, Nov. 2020, pp. 1–10. doi: 10.1109/ITC44778.2020.9325226.

[12] J. W. Jeong, E. Yilmaz, L. Winemberg, and S. Ozev, “Built-in self-test for stability measurement of low dropout regulator,” in *2017 IEEE International Test Conference (ITC)*, Oct. 2017, pp. 1–9. doi: 10.1109/TEST.2017.8242033.

[13] M. Ince and S. Ozev, “Digital Defect Based Built-in Self-Test for Low Dropout Voltage Regulators,” in *2020 IEEE European Test Symposium (ETS)*, May 2020, pp. 1–2. doi: 10.1109/ETS48528.2020.9131577.

[14] M. Saikiran, M. Ganji, and D. Chen, “Robust Built-in Defect-Detection for Low Drop-Out Regulators using Digital Mismatch Injection,” in *2022 IEEE International Symposium on Circuits and Systems (ISCAS)*, May 2022, pp. 1580–1584. doi: 10.1109/ISCAS48785.2022.9937644.

[15] M. Taheri, S. Sheikhpour, A. Mahani, and M. Jenihhin, “A Novel Fault-Tolerant Logic Style with Self-Checking Capability,” in *2022 IEEE 28th International Symposium on On-Line Testing and Robust System Design (IOLTS)*, Sep. 2022, pp. 1–6. doi: 10.1109/IOLTS56730.2022.9897818.

[16] F. Faggin, D. D. Forsythe, and T. Klein, “Room Temperature Instabilities Observed on Silicon Gate Devices,” in *8th Reliability Physics Symposium*, Apr. 1970, pp. 35–41. doi: 10.1109/IRPS.1970.362431.

[17] C. E. Blat, E. H. Nicollian, and E. H. Poindexter, “Mechanism of negative-bias-temperature instability,” *J. Appl. Phys.*, vol. 69, no. 3, pp. 1712–1720, Feb. 1991, doi: 10.1063/1.347217.

[18] S. Mahapatra, P. B. Kumar, and M. A. Alam, “Investigation and modeling of interface and bulk trap generation during negative bias temperature instability of p-MOSFETs,” *IEEE Trans. Electron Devices*, vol. 51, no. 9, pp. 1371–1379, Sep. 2004, doi: 10.1109/TED.2004.833592.

[19] H. Reisinger, O. Blank, W. Heinrigs, A. Muhlhoff, W. Gustin, and C. Schlunder, “Analysis of NBTI Degradation- and Recovery-Behavior Based on Ultra Fast VT-Measurements,” in *2006 IEEE International Reliability Physics Symposium Proceedings*, Mar. 2006, pp. 448–453. doi: 10.1109/RELPHY.2006.251260.

[20] S. Mahapatra *et al.*, “A Comparative Study of Different Physics-Based NBTI Models,” *IEEE Trans. Electron Devices*, vol. 60, no. 3, pp. 901–916, Mar. 2013, doi: 10.1109/TED.2013.2238237.

[21] S. Mukhopadhyay and S. Mahapatra, “An Experimental Perspective of Trap Generation Under BTI Stress,” *IEEE Trans. Electron Devices*, vol. 62, no. 7, pp. 2092–2097, Jul. 2015, doi: 10.1109/TED.2015.2434955.

[22] T. Aichinger, S. Puchner, M. Nelhiebel, T. Grasser, and H. Hutter, “Impact of hydrogen on recoverable and permanent damage following negative bias temperature stress,” in *2010 IEEE International Reliability Physics Symposium*, May 2010, pp. 1063–1068. doi: 10.1109/IRPS.2010.5488672.

[23] T. Grasser *et al.*, “Gate-sided hydrogen release as the origin of ‘permanent’ NBTI degradation: From single defects to lifetimes,” in *2015 IEEE International Electron Devices Meeting (IEDM)*, Dec. 2015, p. 20.1.1-20.1.4. doi: 10.1109/IEDM.2015.7409739.

[24] S. Pae, J. Maiz, C. Prasad, and B. Woolery, “Effect of BTI Degradation on Transistor Variability in Advanced Semiconductor Technologies,” *IEEE Trans. Device Mater. Reliab.*, vol. 8, no. 3, pp. 519–525, Sep. 2008, doi: 10.1109/TDMR.2008.2002351.

[25] D. Heh, C. D. Young, and G. Bersuker, “Experimental Evidence of the Fast and Slow Charge Trapping/Detrapping Processes in High- k Dielectrics Subjected to PBTI Stress,” *IEEE Electron Device Lett.*, vol. 29, no. 2, pp. 180–182, Feb. 2008, doi: 10.1109/LED.2007.914088.

[26] T. Sato, T. Kozaki, T. Uezono, H. Tsutsui, and H. Ochi, “A device array for efficient bias-temperature instability measurements,” in *2011 Proceedings of the European Solid-State Device Research Conference (ESSDERC)*, Sep. 2011, pp. 143–146. doi: 10.1109/ESSDERC.2011.6044214.

[27] W. Wang, V. Reddy, A. T. Krishnan, R. Vattikonda, S. Krishnan, and Y. Cao, “Compact Modeling and Simulation of Circuit Reliability for 65-nm CMOS Technology,” *IEEE Trans. Device Mater. Reliab.*, vol. 7, no. 4, pp. 509–517, Dec. 2007, doi: 10.1109/TDMR.2007.910130.

[28] S. E. Rauch, “Review and Reexamination of Reliability Effects Related to NBTI-Induced Statistical Variations,” *IEEE Trans. Device Mater. Reliab.*, vol. 7, no. 4, pp. 524–530, Dec. 2007, doi: 10.1109/TDMR.2007.910437.

[29] B. Kaczer *et al.*, “Origin of NBTI variability in deeply scaled pFETs,” in *2010 IEEE International Reliability Physics Symposium*, May 2010, pp. 26–32. doi: 10.1109/IRPS.2010.5488856.

[30] S. Kumar, R. Anandkrishnan, N. Parihar, and S. Mahapatra, “A Stochastic Framework for the Time Kinetics of Interface and Bulk Oxide Traps for BTI, SILC, and TDDB in MOSFETs,” *IEEE Trans. Electron Devices*, vol. 67, no. 11, pp. 4741–4748, Nov. 2020, doi: 10.1109/TED.2020.3020533.

[31] H. Mostafa, M. Anis, and M. Elmasry, “NBTI and Process Variations Compensation Circuits Using Adaptive Body Bias,” *IEEE Trans. Semicond. Manuf.*, vol. 25, no. 3, pp. 460–467, Aug. 2012, doi: 10.1109/TSM.2012.2192143.

[32] A. P. Shah, N. Yadav, A. Beohar, and S. K. Vishvakarma, "On-Chip Adaptive Body Bias for Reducing the Impact of NBTI on 6T SRAM Cells," *IEEE Trans. Semicond. Manuf.*, vol. 31, no. 2, pp. 242–249, May 2018, doi: 10.1109/TSM.2018.2804944.

[33] T.-H. Kim, R. Persaud, and C. H. Kim, "Silicon Odometer: An On-Chip Reliability Monitor for Measuring Frequency Degradation of Digital Circuits," in *2007 IEEE Symposium on VLSI Circuits*, Jun. 2007, pp. 122–123. doi: 10.1109/VLSIC.2007.4342682.

[34] P.-F. Lu, K. A. Jenkins, K. P. Muller, and R. Schaufler, "Long-term data for BTI degradation in 32nm IBM microprocessor using HKMG technology," in *2015 IEEE International Reliability Physics Symposium*, Apr. 2015, p. 6A.2.1-6A.2.5. doi: 10.1109/IRPS.2015.7112756.

[35] M. Igarashi, Y. Takazawa, Y. Tsukamoto, K. Takeuchi, and K. Shibutani, "NBTI/PBTI separated BTI monitor with 4.2x sensitivity by standard cell based unbalanced ring oscillator," in *2017 IEEE Asian Solid-State Circuits Conference (A-SSCC)*, Nov. 2017, pp. 201–204. doi: 10.1109/ASSCC.2017.8240251.

[36] J. Keane, T.-H. Kim, and C. H. Kim, "An On-Chip NBTI Sensor for Measuring pMOS Threshold Voltage Degradation," *IEEE Trans. Very Large Scale Integr. VLSI Syst.*, vol. 18, no. 6, pp. 947–956, Jun. 2010, doi: 10.1109/TVLSI.2009.2017751.

[37] P. Singh, E. Karl, D. Blaauw, and D. Sylvester, "Compact Degradation Sensors for Monitoring NBTI and Oxide Degradation," *IEEE Trans. Very Large Scale Integr. VLSI Syst.*, vol. 20, no. 9, pp. 1645–1655, Sep. 2012, doi: 10.1109/TVLSI.2011.2161784.

[38] J. Keane, W. Zhang, and C. H. Kim, "An Array-Based Odometer System for Statistically Significant Circuit Aging Characterization," *IEEE J. Solid-State Circuits*, vol. 46, no. 10, pp. 2374–2385, Oct. 2011, doi: 10.1109/JSSC.2011.2160813.

[39] G. Park, H. Yu, M. Kim, and C. H. Kim, "An All BTI (N-PBTI, N-NBTI, P-PBTI, P-NBTI) Odometer based on a Dual Power Rail Ring Oscillator Array," in *2021 IEEE International Reliability Physics Symposium (IRPS)*, Mar. 2021, pp. 1–5. doi: 10.1109/IRPS46558.2021.9405181.

[40] Y.-L. Wu, S.-T. Lin, and C.-P. Lee, "Time-to-Breakdown Weibull Distribution of Thin Gate Oxide Subjected to Nanoscaled Constant-Voltage and Constant-Current Stresses," *IEEE Trans. Device Mater. Reliab.*, vol. 8, no. 2, pp. 352–357, Jun. 2008, doi: 10.1109/TDMR.2008.918987.

[41] K. Bhatheja, X. Jin, M. Strong, and D. Chen, "Fast Gate Leakage Current Monitor With Large Dynamic Range," *IEEE Trans. Circuits Syst. II Express Briefs*, vol. 68, no. 5, pp. 1690–1694, May 2021, doi: 10.1109/TCSII.2021.3068628.

[42] N. Ayala, J. Martin-Martinez, R. Rodriguez, M. Nafria, and X. Aymerich, "Unified characterization of RTN and BTI for circuit performance and variability simulation," in *2012 Proceedings of the European Solid-State Device Research Conference (ESSDERC)*, Sep. 2012, pp. 266–269. doi: 10.1109/ESSDERC.2012.6343384.

[43] C. Yilmaz, L. Heiß, C. Werner, and D. Schmitt-Landsiedel, "Modeling of NBTI-recovery effects in analog CMOS circuits," in *2013 IEEE International Reliability Physics Symposium (IRPS)*, Apr. 2013, p. 2A.4.1-2A.4.4. doi: 10.1109/IRPS.2013.6531944.

[44] W. H. Choi, H. Kim, and C. H. Kim, "Circuit techniques for mitigating short-term vth instability issues in successive approximation register (SAR) ADCs," in *2015 IEEE Custom Integrated Circuits Conference (CICC)*, Sep. 2015, pp. 1–4. doi: 10.1109/CICC.2015.7338417.

[45] S. Adee, "The Hunt For The Kill Switch," *IEEE Spectr.*, vol. 45, no. 5, pp. 34–39, May 2008, doi: 10.1109/MSPEC.2008.4505310.

[46] R. Karri, J. Rajendran, K. Rosenfeld, and M. Tehranipoor, "Trustworthy Hardware: Identifying and Classifying Hardware Trojans," *Computer*, vol. 43, no. 10, pp. 39–46, Oct. 2010, doi: 10.1109/MC.2010.299.

[47] X. Wang, M. Tehranipoor, and J. Plusquellic, "Detecting malicious inclusions in secure hardware: Challenges and solutions," in *2008 IEEE International Workshop on Hardware-Oriented Security and Trust*, Jun. 2008, pp. 15–19. doi: 10.1109/HST.2008.4559039.

[48] M. Tehranipoor and F. Koushanfar, "A Survey of Hardware Trojan Taxonomy and Detection," *IEEE Des. Test Comput.*, vol. 27, no. 1, pp. 10–25, Jan. 2010, doi: 10.1109/MDT.2010.7.

[49] J. Rajendran, E. Gavas, J. Jimenez, V. Padman, and R. Karri, "Towards a comprehensive and systematic classification of hardware Trojans," in *Proceedings of 2010 IEEE International Symposium on Circuits and Systems*, May 2010, pp. 1871–1874. doi: 10.1109/ISCAS.2010.5537869.

[50] R. S. Chakraborty, S. Narasimhan, and S. Bhunia, "Hardware Trojan: Threats and emerging solutions," in *2009 IEEE International High Level Design Validation and Test Workshop*, Nov. 2009, pp. 166–171. doi: 10.1109/HLDVT.2009.5340158.

[51] S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, "Hardware Trojan Attacks: Threat Analysis and Countermeasures," *Proc. IEEE*, vol. 102, no. 8, pp. 1229–1247, Aug. 2014, doi: 10.1109/JPROC.2014.2334493.

[52] K. S. Subramani, N. Helal, A. Antonopoulos, A. Nosratinia, and Y. Makris, "Amplitude-Modulating Analog/RF Hardware Trojans in Wireless Networks: Risks and Remedies," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 3497–3510, 2020, doi: 10.1109/TIFS.2020.2990792.

[53] J. Kan, Y. Shen, J. Xu, E. Chen, J. Zhu, and V. Chen, "RF Analog Hardware Trojan Detection Through Electromagnetic Side-Channel," *IEEE Open J. Circuits Syst.*, vol. 3, pp. 237–251, 2022, doi: 10.1109/OJCAS.2022.3210163.

[54] M. Elshamy *et al.*, "Digital-to-Analog Hardware Trojan Attacks," *IEEE Trans. Circuits Syst. Regul. Pap.*, vol. 69, no. 2, pp. 573–586, Feb. 2022, doi: 10.1109/TCSI.2021.3116806.

[55] A. Pavlidis, E. Faehn, M.-M. Louërat, and H.-G. Stratigopoulos, "Run-Time Hardware Trojan Detection in Analog and Mixed-Signal ICs," in *2022 IEEE 40th VLSI Test Symposium (VTS)*, Apr. 2022, pp. 1–8. doi: 10.1109/VTS52500.2021.9794208.

[56] Y. Wang, D. Chen, and R. L. Geiger, "Practical methods for verifying removal of Trojan stable operating points," in *2013 IEEE International Symposium on Circuits and Systems (ISCAS)*, May 2013, pp. 2658–2661. doi: 10.1109/ISCAS.2013.6572425.

[57] X. Cao, Q. Wang, R. L. Geiger, and D. J. Chen, "A hardware Trojan embedded in the Inverse Widlar reference generator," in *2015 IEEE 58th International Midwest Symposium on Circuits and Systems (MWSCAS)*, Aug. 2015, pp. 1–4. doi: 10.1109/MWSCAS.2015.7282131.

[58] Y.-T. Wang, Q. Wang, D. Chen, and R. L. Geiger, "Hardware trojan state detection for analog circuits and systems," in *NAECON 2014 - IEEE National Aerospace and Electronics Conference*, Jun. 2014, pp. 364–367. doi: 10.1109/NAECON.2014.7045837.

[59] Q. Wang, D. Chen, and Randall. L. Geiger, "Transparent side channel trigger mechanism on analog circuits with PAAST hardware Trojans," in *2018 IEEE International Symposium on Circuits and Systems (ISCAS)*, May 2018, pp. 1–4. doi: 10.1109/ISCAS.2018.8351233.

[60] Q. Wang, R. L. Geiger, and D. Chen, "Hardware Trojans embedded in the dynamic operation of analog and mixed-signal circuits," in *2015 National Aerospace and Electronics Conference (NAECON)*, Jun. 2015, pp. 155–158. doi: 10.1109/NAECON.2015.7443059.

[61] S. Youn, J. Kim, and M. Horowitz, "Global convergence analysis of mixed-signal systems," in *2011 48th ACM/EDAC/IEEE Design Automation Conference (DAC)*, Jun. 2011, pp. 498–503.

[62] C. Kison, O. M. Awad, M. Fyrbiak, and C. Paar, "Security Implications of Intentional Capacitive Crosstalk," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 12, pp. 3246–3258, Dec. 2019, doi: 10.1109/TIFS.2019.2900914.

[63] K. O. Banahene, M. R. Strong, B. Gadogbe, D. Chen, and R. L. Geiger, "Hardware Security Vulnerability in Analog Signal Chain Filters," in *2022 IEEE International Symposium on Circuits and Systems (ISCAS)*, May 2022, pp. 667–671. doi: 10.1109/ISCAS48785.2022.9937611.

[64] Y.-T. Wang, C. Zhao, R. Geiger, D. Chen, and S.-C. Huang, "Performance verification of start-up circuits in reference generators," in *2012 IEEE 55th International Midwest Symposium on Circuits and Systems (MWSCAS)*, Aug. 2012, pp. 518–521. doi: 10.1109/MWSCAS.2012.6292071.

[65] S. Liu, R. L. Geiger, and D. Chen, "A graphical method for identifying positive feedback loops automatically in self-biasing circuit for determining the uniqueness of operating points," in *NAECON 2014 - IEEE National Aerospace and Electronics Conference*, Jun. 2014, pp. 384–390. doi: 10.1109/NAECON.2014.7045841.

[66] Z. Liu, Y. Li, R. L. Geiger, and D. Chen, "Auto-identification of positive feedback loops in multi-state vulnerable circuits," in *2014 IEEE 32nd VLSI Test Symposium (VTS)*, Apr. 2014, pp. 1–5. doi: 10.1109/VTS.2014.6818794.

[67] A. Mirzaei, M. E. Heidari, R. Bagheri, S. Chehrazi, and A. A. Abidi, "The Quadrature LC Oscillator: A Complete Portrait Based on Injection Locking," *IEEE J. Solid-State Circuits*, vol. 42, no. 9, pp. 1916–1932, Sep. 2007, doi: 10.1109/JSSC.2007.903047.

[68] A. Fukuma and M. Matsubara, "Jump resonance criteria of nonlinear control systems," *IEEE Trans. Autom. Control*, vol. 11, no. 4, pp. 699–706, Oct. 1966, doi: 10.1109/TAC.1966.1098453.

[69] C. D. Salthouse and R. Sarpeshkar, "Jump resonance: a feedback viewpoint and adaptive circuit solution for low-power active analog filters," *IEEE Trans. Circuits Syst. Regul. Pap.*, vol. 53, no. 8, pp. 1712–1725, Aug. 2006, doi: 10.1109/TCSI.2006.879050.

[70] Shenggao Li, I. Kipnis, and M. Ismail, "A 10-GHz CMOS quadrature LC-VCO for multirate optical applications," *IEEE J. Solid-State Circuits*, vol. 38, no. 10, pp. 1626–1634, Oct. 2003, doi: 10.1109/JSSC.2003.817258.

[71] M. M. Abdul-Latif and E. Sanchez-Sinencio, "Low Phase Noise Wide Tuning Range N-Push Cyclic-Coupled Ring Oscillators," *IEEE J. Solid-State Circuits*, vol. 47, no. 6, pp. 1278–1294, Jun. 2012, doi: 10.1109/JSSC.2012.2188564.

[72] T. Lee, Y.-H. Kim, and L.-S. Kim, "A 5-Gb/s Digital Clock and Data Recovery Circuit With Reduced DCO Supply Noise Sensitivity Utilizing Coupling Network," *IEEE Trans. Very Large Scale Integr. VLSI Syst.*, vol. 25, no. 1, pp. 380–384, Jan. 2017, doi: 10.1109/TVLSI.2016.2566927.

[73] S. Song *et al.*, "A 2-to-20 GHz Multi-Phase Clock Generator with Phase Interpolators Using Injection-Locked Oscillation Buffers for High-Speed IOs in 16nm FinFET," in *2019 IEEE Custom Integrated Circuits Conference (CICC)*, Apr. 2019, pp. 1–4. doi: 10.1109/CICC.2019.8780177.

[74] M. S. Mehrjoo and J. F. Buckwalter, “A Differential Oscillator Injection Locking Technique for an 8 GHz Outphasing Modulator With 22.7% Modulation Efficiency,” *IEEE J. Solid-State Circuits*, vol. 51, no. 12, pp. 3093–3102, Dec. 2016, doi: 10.1109/JSSC.2016.2600860.

[75] T. Sowlati *et al.*, “A 60GHz 144-element phased-array transceiver with 51dBm maximum EIRP and ±60° beam steering for backhaul application,” in *2018 IEEE International Solid - State Circuits Conference - (ISSCC)*, Feb. 2018, pp. 66–68. doi: 10.1109/ISSCC.2018.8310186.

[76] C. Yan and M. Greenstreet, “Oscillator verification with probability one,” in *2012 Formal Methods in Computer-Aided Design (FMCAD)*, Oct. 2012, pp. 165–172.

[77] Q. Wang, R. L. Geiger, and D. Chen, “Hardware Trojans embedded in the dynamic operation of analog and mixed-signal circuits,” in *2015 National Aerospace and Electronics Conference (NAECON)*, Jun. 2015, pp. 155–158. doi: 10.1109/NAECON.2015.7443059.

[78] C. Yan and M. Greenstreet, “Oscillator verification with probability one,” in *2012 Formal Methods in Computer-Aided Design (FMCAD)*, Oct. 2012, pp. 165–172.

[79] C. Yan, M. R. Greenstreet, and S. Yang, “Verifying global start-up for a Möbius ring-oscillator,” *Form. Methods Syst. Des.*, vol. 45, no. 2, pp. 246–272, Oct. 2014, doi: 10.1007/s10703-013-0204-6.

[80] C. Kison, O. M. Awad, M. Fyrbiak, and C. Paar, “Security Implications of Intentional Capacitive Crosstalk,” *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 12, pp. 3246–3258, Dec. 2019, doi: 10.1109/TIFS.2019.2900914.

[81] Q. Wang, D. Chen, and R. L. Geiger, “Transparent side channel trigger mechanism on analog circuits with PAAST hardware Trojans,” in *2018 IEEE International Symposium on Circuits and Systems (ISCAS)*, May 2018, pp. 1–4. doi: 10.1109/ISCAS.2018.8351233.

[82] L. Zussa, J.-M. Dutertre, J. Clédière, and A. Tria, “Power supply glitch induced faults on FPGA: An in-depth analysis of the injection mechanism,” in *2013 IEEE 19th International On-Line Testing Symposium (IOLTS)*, Jul. 2013, pp. 110–115. doi: 10.1109/IOLTS.2013.6604060.

[83] S. P. Skorobogatov and R. J. Anderson, “Optical Fault Induction Attacks,” in *Cryptographic Hardware and Embedded Systems - CHES 2002*, B. S. Kaliski, çetin K. Koç, and C. Paar, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 2–12.

[84] N. Beringuier-Boher, M. Lacruche, D. El-Baze, J.-M. Dutertre, J.-B. Rigaud, and P. Maurine, “Body Biasing Injection Attacks in Practice,” in *Proceedings of the Third Workshop on Cryptography and Security in Computing Systems*, Prague Czech Republic: ACM, Jan. 2016, pp. 49–54. doi: 10.1145/2858930.2858940.