Hidden-Delay-Fault Sensor for Test, Reliability and Security

Giorgio Di Natale, Elena Ioana Vatajelu, Kalpana Senthamarai Kannan, Lorena Anghel
Univ. Grenoble Alpes, CNRS, Grenoble INP, TIMA,*
Grenoble, France

***Abstract*— In this paper we present a novel hidden-delay-fault sensor design and a preliminary analysis of its circuit integration and applicability. In our proposed method, the delay sensing is achieved by sampling data on both rising and falling clock edges and using a variable duty cycle to control the length of the path to be tested. The main advantage of our proposed method is that it works at nominal frequency, it can detect hidden-delay-faults on short paths and it is versatile in its applicability. It can be used (i) during testing to perform user-defined hidden-delay-fault test, (ii) for reliability degradation estimation due to process, environmental variations and ageing, and (iii) in security to detect the insertion of Trojan horses that alter the path delay.**

***Keywords*— hidden-delay-fault, monitor, test, reliability, security**

I. Introduction

Process, voltage, and temperature variations in digital designs cause performance degradation, which has become critical in nanometer-technology nodes. Moreover, transistor-aging effects, such as bias temperature instability (BTI), hot carrier injection (HCI), or time-dependent dielectric breakdown (TDDB) degrade the performance of a design with time. All these issues can manifest as delay faults, i.e., cause transition delays larger than the manufacturing specification. A delay fault larger than the slack of a propagation path is detectable by at-speed testing and by timing-violation monitors. A delay fault, which is smaller than the slack of the propagation path, it is called hidden delay fault (HDF) and cannot be detected by any of the previously mentioned methods. For detecting such faults, Faster-than-At-speed Test (FAST) is proposed [1, 2], where the clock frequency is increased until the slack of the propagation path becomes smaller than the HDF so the fault can be detected. In addition to testing for delay faults, timing errors can also be predicted my monitoring the timing slack of a design. Various types of monitors have been proposed in the literature and they can be largely classified as follows:

- Ring oscillators [3] or Replica Path [4] that aim at replicating the timing behavior of the circuit in which they are placed. These sensors are well suited for monitoring the effect of global variations on circuit performance; however, they fail to capture the effect of local variations caused by random manufacturing effects and by circuit aging.
- In-Situ Monitors (ISM) can be directly linked to the circuit path delays, and are well suited to capture the effect of local variations caused by random manufacturing effects and by circuit aging. Among a large choice of ISM, we find error-detection monitors embedded in techniques called Razor-like [5], or Double-sampling with Time Borrowing (DSTB) introduced in [6]. These monitors only detect errors. An additional operation of correction through rollback, for example, is needed to prevent eventual failures in case of error propagation. Another drawback consists in tedious error-detection implementation due to the multiple clock signals, which is not appropriate for safety critical applications, and the large complexity of the error recovery mechanism.
- Issues related to the error recovery scheme implementation are avoided by a circuit failure prediction approach [6], i.e. detecting a pre-error before the appearance of any error in system data and state. In-line with this approach, in [7] a stability checker circuit was proposed which detects transitions close to the clock edge due to an additional delay element in the clock path. Another approach called Canary Flip-Flop [8], consists in sensing a given propagation path prolonged by a delay element. A pre-error signal is raised when the value in the data-path Flip-Flop differs from the value in the Canary Flip-Flop, as an indicator of any speed violation due to aging or local variation within the die.

In this paper we present a novel in-situ delay monitor, that is adapted to detect small delay faults, including hidden delay faults, and it is adaptable to operation conditions. Moreover, a single sensor can be used to measure the delay of more than one path, thus minimizing the area overhead due to monitor insertion. The rest of the paper is structured as follows. The second section presents our proposed sensor design and underlines its main benefits over state-of-the-art solutions. The third section lists the applications for which the proposed sensor is suited and how it should be used. The fourth section discusses the main challenges posed by the deployment of the proposed sensor and future envisioned research directions.

II. Hidden-Delay-Fault Sensor Design

In-situ delay monitors such as DSTB or Canary Flip-Flop use double sampling of signals coming from the combinational logic. At a given circuit endpoint, the signal is sampled twice within a small timing window (dictated either by a delay of the clock signal, or by a delay of the data signal) [9]. If the two samples have different values, an alarm signal is raised signaling a potential error on the monitored path. The precision of such sensor is given by the size of the timing window (i.e., precise timing of the delay element). Previous published solutions consider for the size of the timing window, i.e., the

*Institute of Engineering Univ. Grenoble Alpes

978-3-9819263-2-3/DATE19/©2019 EDAA

timing difference between the two sampling steps, is thoroughly computed at design time, considering many parameters such as fan-outs, process variability, temperature influence, and workload dependence. It mostly targets the critical and close-to-critical paths; therefore, it does not detect the hidden-delay-faults on short paths (as shown in the upper part of Fig. 1).

In this paper we propose a different sampling technique that allows the detection of timing violations which occur on small paths. The proposed monitor is placed at the endpoint of the targeted paths, i.e., with the functional Flip-Flop (FF). It uses double sampling but, compared to existing solutions, the delay between the two samplings can be programmed according to the length of the path being monitored. The key idea of this proposal is that the signal coming from the combinational logic is sampled first at the falling and then at the rising edges of a clock signal with a programmable duty cycle (as shown in the bottom part of Fig. 1). Thus, the pulse width of the clock signal determines the length of the path to be monitored. The use of a programmable duty cycle clock generator allows us to use the same monitor for multiple path lengths. Therefore, with a single sensor we are able to detect all delay faults occurring on the small paths (within the range of the programmable duty cycle) belonging to the fan-in of that FF, as shown in Fig. 2.

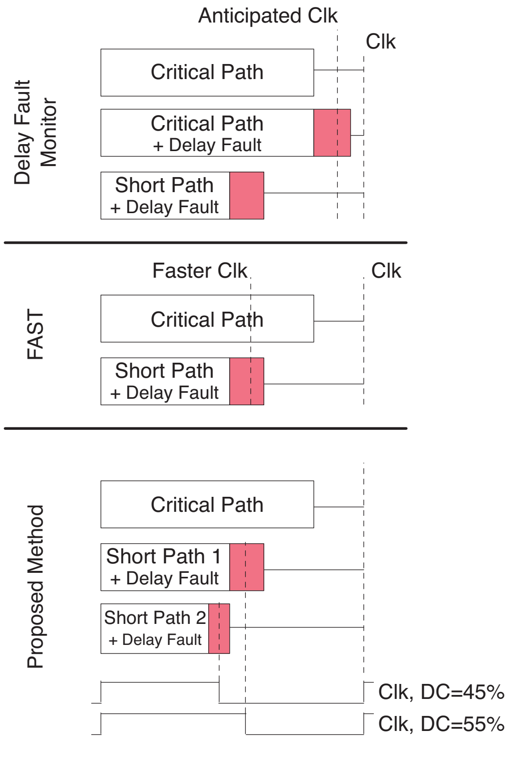

Fig. 1. Techniques for delay-fault detection

Our proposed monitor has the same advantages as the FAST technique, i.e., it is able to detect delay faults on smaller-than-critical paths (as shown in the middle part of Fig. 1). However, using the proposed monitor we are able to detect delay faults without affecting the nominal frequency of the circuit, due to the use of variable clock Duty Cycle. The proposed monitor can be used for on-line and off-line testing, either to replace FAST or to complement it, as it will be discussed in the third section of the paper.

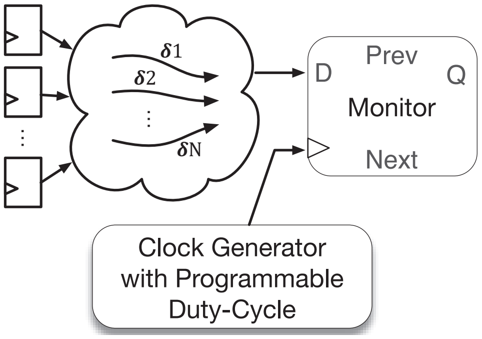

Fig. 2. High level architecture of the proposed hidden delay-fault (HDF) monitor

Figure 3 shows an example of the usage and benefits of the proposed delay fault monitor. For illustration purpose only, let us consider a small circuit composed of 3 logic gates, with different Propagation Delays (PDs) and one flip flop (FF) at the output of the path. The proposed monitor is composed of this functional FF and an additional check FF, called *shadow FF*, which is active on the falling edge of the clock. Let us consider the following two scenarios: (i) the inputs *a* and *b* are set to *0*, while the input *c* has a rising transition, and (ii) the inputs *a* and *b* have a rising transition while the input *c* is set to 0. In the first scenario, the PD from the inputs to the output *s* is of *4ns*, while in the second scenario the PD is of *8ns*. The goal of the proposed sensor is to detect timing violations in both paths. This is achieved thanks to the programmable duty cycle of the clock signal, which allows sampling the *s* signal depending on the path that is sensitized at a given moment. In particular, knowing the nominal path delays of the combinational network, the duty cycle can be correctly adjusted such that for a certain input transition, the pulse width of the clock equals the expected delay of the targeted path. In these conditions, the data is sampled first on the falling edge of the clock (*shadow FF*) and then on the rising edge of the clock (functional FF). If these two samples have different values, an HDF is detected. The red lines in fig. 3 correspond to faulty transitions (i.e., the path suffers from HDF). In this particular example, with one sensor, at nominal frequency, with two different settings of the duty cycle, the presence of HDFs is detected on both paths. This method can be applied for large fan-ins (as shown in Fig. 2) and the monitor can detect HDFs on all paths within the limits of the duty cycle.

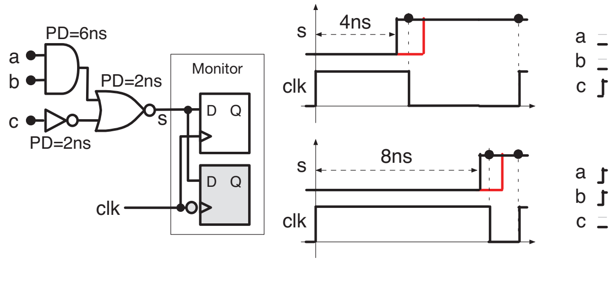

Fig. 3. Example of the HDF detection method

We propose the implementation of such a monitor as shown in Fig. 4. As previously explain, the monitor operates by signal double-sampling: on the falling and rising edge of the clock. The two samples are compared in an XOR gate and the result is memorized in the *shadow FF* on the following falling edge of the clock. During the subsequent clock cycles the results are collected and transmitted either to an external tester on an internal controller. To that end, we propose to collect data from all inserted monitors by using classic scan chain. The collected and transmitted results could be used to detect/evaluate the manufacturing defects, circuit aging or the presence of Trojan Horses. The possible applications of the proposed sensor will be discussed in more detail in the next section of the paper.

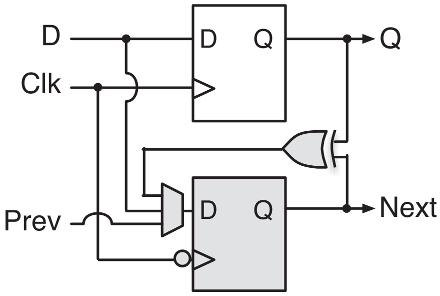

Fig. 4. Implementation of the proposed hidden-delay fault monitor

One of the main challenges posed by the proposed sensor consists in the interpretation of the results. Since all FFs are controlled by the same clock signal, the same duty cycle is seen by all paths in the combinational logic. Assuming multiple sensors are distributed in the circuit, part of the collected responses will be wrong, due to the fact that some of the *shadow FFs* will be inevitably placed on longer paths, with duration longer than the pulse width of the clock. For this reason, the results of sample comparison have to be taken as valid only for the input patters for which the duty cycle setting was chosen.

The main limitation of our proposed method is related to the flexibility of the clock duty cycle. State-of-the-art designs demonstrate a programmability of the duty cycle from 30% to 70% [10-11]. This means that our monitor can be used on short paths only. Moreover, the minimum size of detected fault is strongly dependent on the clock signal jitter and skew, especially for high-speed circuits.

Our proposed method of sensing hidden delay faults has several main advantages when compared to state-of the art methods, such as:

- The proposed method does not require the use of a second clock generator, the acceleration of the nominal clock, nor the use of a delay element; it has a smaller area footprint and a simpler design.
- In state-of-the art solutions the sensor location is chosen at design time depending on the estimated workload and process variation additional margins that need to be compensated. Once placed in circuit, it can only detect delay faults occurring on the path on which it is placed and only within the limits allowed by design (timing window, i.e., delay element). Therefore, it can only sense the predicted delays. In contrast, our proposed sensing method has the advantage of adaptability. Even if its location is also chosen at design time, this sensor can monitor various points of the Flip-Flop fan-in by simply modifying the input vectors and the clock duty cycle.
- Traditional sensors, designed with a fixed timing window (delay) may be inaccurate due to process variations of the delay element, resulting in false positive and false negatives; they can also become inefficient in frequency scaling scenarios. In contrast, the proposed sensor is less sensitive to process variations, and clock changes due to dynamic voltage-frequency scaling (DVFS) do not affect its efficiency.

III. Applications

We have identified three main application fields in which the proposed delay fault monitor could be used: test, reliability and security.

A. Test

For manufacturing test purposes, a modified ATPG (similar to the one proposed in [12]) can be used to generate test vectors, which will activate the targeted paths and simultaneously, for each vector, will generate the duty cycle that will allow the detection of HDF on the excited paths. For each test-vector/duty-cycle pair, the ATPG should compute the unknown responses (Xs) for the *shadow FFs* that are placed on longer paths than the pulse width of the clock. After each test vector, the ATE should extract the monitored outputs from the scan chain of the *shadow FFs* and verify if they are correct.

Our proposed method can be seen as complementary to the FAST method. The FAST method can be used to test for the HDF on the longer paths and place our monitors only on the shorter paths, thus reducing the strain caused by overly-accelerated clock.

B. Reliability

The proposed delay fault monitor can be used during the lifetime of the circuit in order to identify timing violations in short paths due to reliability degradation. The proposed monitor can be used in an off-line BIST scheme (similarly to the technique presented in [13]), where instead of varying the clock frequency for each input vector, the duty cycle will be controlled. In addition, this monitor can also be used in an on-line/concurrent BIST scheme. Indeed, the frequency of the clock is never modified; therefore the functional FFs will sample the responses of the circuit within the correct timing. This solution requires a smart test controller (not described in this paper), which should identify the useful shadow FFs, for a pair of input data and used duty cycle.

Moreover, the proposed delay fault monitor can be combined with powerful static and dynamic voltage and frequency scaling (DVFS). In such a setup, it is possible to directly access the embedded monitors through the scan chain, allowing both the monitor flags and the DVFS control signals to be directly connected to the system without the need of a special access mechanism. This way, the system is able to monitor its own reliability induced alerts and autonomously adapt its Operating Points represented by VDD and Frequency, in case multiple Operating Points are known and validated at signoff. This adaptation requires a complete rewrite of the control loop and careful validation of the functionality and timing.

C. Security

The proposed monitor can be also used for trust and security to detect the insertion of Trojan horses that alter the path delay.

A Hardware Trojan Horse is a malicious modification of an IC that can be done during the design or the fabrication steps. The insertion of an HT in a non-trusted foundry was initially considered the most likely threat [14]. Trojans inserted at silicon level cause changes in path delays due to capacitive loading effects. These changes are not considered during test vector generation, due to the fact that their presence is not intended by the designer. In [15], the authors propose the use of delay fault testing in order to detect such Trojans, even in presence of variability. In [16] the authors propose a complex sensor that resorts to a time-to-digital converter to measure the path delay. However, this design incurs large area overhead.

Since our proposed monitor detects time violation on small paths, it can be also used to detect the presence of Trojan Horses. In this situation, a delay fault detected by our proposed monitor could be caused an HDF or a Trojan horse. In order to differentiate between the two, several circuits coming from different dies and wafers should be tested. If a systematic behavior is observed, then there is a high probability that a Trojan is inserted on the tested small path, as presented in [15].

IV. Future Work

With this proposal, many issues are still open, in particular:

- The implementation of the delay fault monitor. Similar to previously proposed sensors, this monitor can be implemented as a standard cell in order to reduce its area overhead and facilitate its integration in a standard design flow.
- Define a strategy to identify the number of required monitors and their placement in the circuit depending on the application.
- Evaluate the efficiency and scalability of the monitor with respect to the testability of the circuit, by estimating the maximum number of HDF.
- Evaluate the effect of variability on the clock generator with variable duty cycle, but also on the delay of paths. Estimate and possibly mitigate this effect on the efficiency of the proposed sensor.
- Evaluate the cost and efficiency of the proposed monitoring infrastructure. Compare with state-of-the-art solutions.
- Develop an on-line testing strategy suitable for reliability degradation estimation. Moreover, voltage and frequency scaling can be combined with delay monitor insertion for overall system fault free operation.

References

[1] H. Yan, A. D. Singh, "Experiments at Detecting Delay Faults using Multiple Higher Frequency Clocks and Results from Neighboring Die", Proc. IEEE Int. Test Conf. (ITC'03), pp. 105-111, Sep.-Oct. 2003.

[2] S. Chakravarty et al., "Silicon evaluation of faster than at-speed transition delay tests," 2012 IEEE 30th VLSI Test Symposium (VTS), Hyatt Maui, HI, 2012, pp. 80-85. doi: 10.1109/VTS.2012.6231084

[3] T. D. Burd, T. A. Pering, A. J. Stratakos and R. W. Brodersen, "A dynamic voltage scaled microprocessor system," IEEE Journal of Solid-State Circuits, vol. 35, pp. 1571-1580, 11 2000.

[4] T. Kuroda, K. Suzuki, S. Mita, T. Fujita, F. Yamane, F. Sano, A. Chiba, Y. Watanabe, K. Matsuda, T. Maeda, T. Sakurai and T. Furuyama, "Variable supply-voltage scheme for low-power high-speed CMOS digital design," IEEE Journal of Solid-State Circuits, vol. 33, pp. 454-462, 3 1998.

[5] S. Das, C. Tokunaga, S. Pant, W. H. Ma, S. Kalaiselvan, K. Lai, D. M. Bull and D. T. Blaauw, "RazorII: In Situ Error Detection and Correction for PVT and SER Tolerance," IEEE Journal of Solid-State Circuits, vol. 44, pp. 32-48, 1 2009.

[6] M. Nicolaidis, "Time redundancy based soft-error tolerant circuits to rescue very deep submicron," in 17th IEEE VLSI Test Symposium, 1999.

[7] L. Lai, V. Chandra, R. C. Aitken and P. Gupta, "SlackProbe: A Flexible and Efficient In Situ Timing Slack Monitoring Methodology," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 33, pp. 1168-1179, 8 2014.

[8] M. Wirnshofer, L. Heiß, A. N. Kakade, N. P. Aryan, G. Georgakos and D. Schmitt-Landsiedel, "Adaptive voltage scaling by in-situ delay monitoring for an image processing circuit," in 2012 IEEE 15th International Symposium on Design and Diagnostics of Electronic Circuits Systems (DDECS), 2012.

[9] L. Anghel and M. Nicolaidis, "Cost reduction and evaluation of a temporary faults detecting technique," Proceedings Design, Automation and Test in Europe Conference and Exhibition 2000 (Cat. No. PR00537), Paris, France, 2000, pp. 591-598.

[10] R. Tajizadegan and A. Abrishamifar, "A duty-cycle control circuit with high input-output duty-cycle range," *2008 15th International Conference on Mixed Design of Integrated Circuits and Systems*, Poznan, Poland, 2008, pp. 169-171

[11] J. Su, T. Liao and C. Hung, "All-Digital Fast-Locking Pulsewidth-Control Circuit With Programmable Duty Cycle," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 21, no. 6, pp. 1154-1164, June 2013

[12] M. Kampmann, M. A. Kochte, E. Schneider, T. Indlekofer, S. Hellebrand and H. Wunderlich, "Optimized Selection of Frequencies for Faster-Than-at-Speed Test," 2015 IEEE 24th Asian Test Symposium (ATS), Mumbai, 2015, pp. 109-114.

[13] S. Hellebrand, T. Indlekofer, M. Kampmann, M. A. Kochte, C. Liu and H. Wunderlich, "FAST-BIST: Faster-than-at-Speed BIST targeting hidden delay defects," 2014 International Test Conference, Seattle, WA, 2014, pp. 1-8

[14] Yier Jin and Y. Makris, "Hardware Trojan detection using path delay fingerprint," 2008 IEEE International Workshop on Hardware-Oriented Security and Trust, Anaheim, CA, 2008, pp. 51-57, doi: 10.1109/HST.2008.4559049

[15] R. S. Chakraborty, S. Narasimhan, and S. Bhunia, "Hardware Trojan: Threats and emerging solutions," in Proc. IEEE Int. High Level Des. Validation Test Workshop, 2009, pp. 166–171.

[16] D. Ismari, J. Plusquellic, C. Lamech, S. Bhunia and F. Saqib, "On detecting delay anomalies introduced by hardware Trojans," 2016 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), Austin, TX, 2016, pp. 1-7.