Test Escapes of Stuck-Open Faults Caused by Parasitic Capacitances and Leakage Currents

Daniel Arumí, Rosa Rodríguez-Montañés, and Joan Figueras, Member, IEEE

Abstract—Intragate open defects are responsible for a significant percentage of defects in present technologies. A majority of these defects cause the logic gate to become stuck open, and this is why they are traditionally modeled as stuck-open faults (SOFs). The classical approach to detect the SOFs is based on a two-vector sequence, and has been proved effective for a wide range of technologies. However, factors typically neglected in past technologies have become a major concern in nanometer technologies, i.e., leakage currents and downstream parasitic capacitances. Some recent works have examined the influence of leakage currents. However, to the best of our knowledge, no one has considered the influence of downstream parasitic capacitances. In this paper, the influence of both factors is investigated and experimentally measured with a test chip built on a 65-nm technology. An analysis based on the electrical simulations is performed to quantify the number of test escapes in the presence of SOFs. Test recommendations are derived from the analysis results to maximize the detectability of these faults in present and future technologies.

Index Terms—Integrated circuit (IC) testing, leakage currents, parasitic capacitances, stuck-open faults (SOFs), test escapes.

I. INTRODUCTION

The aggressive scaling of technology and the increasing number of transistor counts pose a major challenge for keeping the integrated circuit (IC) quality under control. This is especially critical in automotive and medical applications among others, where approximately ten defective parts per million (DPPM) is demanded. Because of the increasing number of contacts and vias [1], the open defects are currently one of the most common yield killer defects affecting present ICs. An open defect consists in undesired partial or total breaking of electrical connection between two points, which should be connected by design. Opens may appear both in the interconnect structures and the logic structures, opening connections to the source and the drain terminals of transistors. In the latter case, opens have traditionally been modeled as stuck-open faults (SOFs) [2].

Since the SOF model was first proposed in [2], intensive research effort has been devoted to improving the characterization [3], testing [4]–[6], and diagnosis [9]–[12] of this class of faults. These studies have demonstrated its efficiency for a wide spectrum of technologies, including the deep submicrometer domain. Today, 30 years after its proposal, the complexity of this fault’s behavior still attracts the interest of the research community [13]–[16]. In fact, new paradigms have arisen which appeal for the revision of the classical model to extend the detectability of these faults in nanometer technologies. In this direction, the works in [17] and [18] demonstrate the influence of leakage on the behavior of the faulty cells affected by the SOFs. Downstream parasitic capacitances related to the faulty node, which were considered a second-order factor in past technologies, also arise as a nonnegligible factor. These capacitances generate a pull-up/down, influencing the behavior of the faulty nodes. If the leakage currents and the downstream parasitic capacitances are not properly addressed, SOFs may become an important source of test escapes, causing unacceptable DPPM levels, especially in applications where high test quality and low escape rates are required.

In this paper, the impact of downstream parasitic capacitances on SOF behavior is analyzed. It is demonstrated how these capacitances may become the major contributor to test escapes for at-speed testing, even greater than the leakage currents. A test IC was designed and built on 65-nm technology to experimentally demonstrate this influence. This paper is organized as follows. The classical SOF model is briefly reviewed in Section II. In Section III, a simple analysis is carried out to demonstrate the influence of downstream parasitic capacitances on nanometer technologies. In Section IV, the SOF model including leakage currents and downstream parasitic capacitances is proposed. The experimental results obtained with the test IC are shown in Section V. Section VI presents the results from electrical simulations of circuits with SOFs for several technology nodes. Section VII provides recommendations to improve SOF detectability. Finally, the conclusions are drawn in Section VIII.

II. CLASSICAL STUCK-OPEN FAULT MODEL

An SOF is a failure mechanism modeled as a loss of charge transfer in one transistor of the defective gate in such a way that the output is set to a high impedance state for at least one logic state [2]. In this situation, the output voltage depends on the previously applied state. Throughout this paper, the SOFs are assumed to be caused by opens at the drain terminals of transistors.Opens at the source terminals are almost equivalent to those affecting the drain terminals in terms of the charge transfer path. Therefore, they are also covered by this paper.
Without loss of generality, consider the example in Fig. 1(a), which illustrates a two-input NAND gate with an SOF at the drain terminal of the pMOS transistor driven by B. The truth table for this faulty gate is displayed in Fig. 1(b). Note that how the output node remains in a high impedance state for the input combination (A B) = (1 0). Thus, if the previously applied vector were (A B) = (1 1), the output (Z) would be interpreted as a logic 0. For the input combinations (0 0) and (0 1), Z would be interpreted as a logic 1. Since an SOF induces a sequential behavior, a two-vector sequence is required. The first vector initializes the faulty node and the second one excites the fault.

III. DOWNSTREAM PARASITIC CAPACITANCE CONDITIONS TO GENERATE A TEST ESCAPE

A simple analysis is presented to demonstrate that downstream parasitic capacitances may influence the behavior of the faulty circuits affected by SOFs. For simplicity, the impact of leakage currents is neglected. Consider the example in Fig. 2. An SOF disconnects the pMOS transistor from the output (Z). The capacitances influencing the faulty node are the gate-to-drain \( C_{gd(n)} \) and drain-to-bulk \( C_{db(n)} \) capacitances of the nMOS transistor and the downstream capacitances related to Z. These downstream capacitances, which summarize the parasitic capacitances to neighboring lines and transistor capacitances of downstream gates, are denoted by \( C_{ft} \), \( C_{ft} \), \( C_{n} \), and \( C_{1} \). In fact, \( C_{ft} \) \( (C_{0}) \) represents the part of the downstream capacitances undergoing a rising (falling) transition and \( C_{0} \) \( (C_{1}) \) the part remaining constant at a logic 0 (1) value.

During the application of the two-vector sequence, the inverter output is first discharged to GND. Subsequently, the transition is generated at the inverter input. Z remains in a high impedance state and cannot be charged to \( V_{DD} \). The parasitic capacitances induce a pull-up/down on Z. To derive the exact voltage variation, it must be considered that node A undergoes a falling transition, the substrate remains constant and the influence of the downstream parasitic capacitances depends on the test sequence applied. The faulty node voltage can be obtained by applying the charge conservation law derived in (1)

\[
V_{Z} = \frac{C_{ft} - C_{ft} - C_{gd(n)}}{C_{TD} + C_{gd(n)} + C_{db(n)}} V_{DD}
\]

where \( C_{TD} \) represents the total downstream parasitic capacitances, as follows:

\[
C_{TD} = C_{ft} + C_{ft} + C_{0} + C_{1}.
\]

A positive or a negative voltage variation is due to the influence of the downstream parasitic capacitances. In this example, a drop helps to detect the fault whereas a positive variation may generate a test escape. Assuming the fault is not detected as long as the faulty node voltage is equal to or higher than \( V_{DD}/2 \), from (1) and by rearranging the inequality, we have

\[
C_{ft} - C_{ft} \geq \frac{1}{2} (C_{TD} + 3C_{gd(n)} + C_{db(n)}). \tag{3}
\]

This inequality describes the relationship between \( C_{ft} \) and \( C_{ft} \) as a function of \( C_{TD} \) and the inverter transistor parasitic capacitances \( C_{gd(n)} \) and \( C_{db(n)} \) in order to generate a test escape. For long lines, around hundred of micrometers, transistor capacitances become negligible and it is expected that the high number of neighbors induces similar values for \( C_{ft} \) and \( C_{ft} \). Hence, the probability of accomplishing (3) may be low. On the contrary, transistor capacitances are important for short lines. If \( 1/2 [C_{TD} + 3C_{gd(n)} + C_{db(n)}] \) is higher than \( C_{TD} \), (3) cannot be fulfilled and no test escape can be generated.

A minimum faulty line length, with the corresponding \( C_{TD} \) value, is required to enable a test escape. \( L_{min} \) refers to this length and was predicted for different technology nodes, as shown in Fig. 3. A minimum distance between adjacent lines was assumed for coupling purposes. Observe that \( L_{min} \) values are low, around a few micrometers. What is more, \( L_{min} \) decreases for every technology node since the relative importance of the downstream parasitic capacitances increases with technology shrinking. The similar results would be obtained if the corresponding analysis were carried out for different faulty gates.
IV. STUCK-OPEN FAULT MODEL IN NANOMETER TECHNOLOGIES

The output voltage of a faulty gate affected by an SOF has traditionally been considered to remain constant during the high impedance state. However, the transistor leakages and downstream parasitic capacitances invalidate this assumption. The classical model must, therefore, be reviewed to comprise both factors, which are described in Sections IV-A–IV-C.

A. Influence of Leakage Currents

The two major leakage contributors in the presence of an SOF are subthreshold leakage and gate leakage. Subthreshold leakage [19] is the current between the source and drain terminals of a transistor when it operates in the weak inversion region. For ultrathin silicon oxide layers and low electric fields, gate leakage current [19] becomes nonnegligible and is mainly caused by the direct tunneling mechanisms.

An example of the influence of leakage currents is shown in Fig. 4. The output of the NAND gate (Z) is disconnected from the drain terminal of one of the pMOS transistors. The faulty cell is in turn driving an inverter and is cross-coupled with i neighboring lines. For ease of simplicity, the dashed line omits some of the neighbors from Fig. 4. In the high impedance state [(A B) = (1 0)], leakage currents influence the behavior of Z. These leakage currents are made up of the subthreshold leakage and gate leakage components from the affected transistors, namely, the subthreshold current [I_{sub(pA)}] and the gate-to-drain current [I_{gd(pA)}] from the pMOS transistor driven by A, the subthreshold current [I_{sub(pB)}] and the gate-to-drain current [I_{gd(pB)}] from the nMOS transistor driven by B, and the gate-to-drain [I_{gd(az)} and I_{gd(pz)}] and gate-to-source [I_{gs(az)} and I_{gs(pz)}] current from the nMOS and pMOS transistors of the downstream inverter.

A circuit like that in Fig. 4 was simulated to show the influence of leakage currents. The faulty line was cross-coupled with 20 neighbors, deriving a total downstream parasitic capacitance equal to 6 fF. All the neighbors remained constant during the application of the vector sequence to excite the SOF. The simulation results showing the evolution of Z in the high impedance state using 16-nm predictive technology model (PTM), low power (LP), and high performance (HP) model [20]–[21] are summarized in Fig. 5. Note that how the leakage currents generate a charge flow. Its voltage increases with time until the steady state is reached, that is, once the sum of all current components flowing into and out of Z is null. At this point, any small deviation (caused by noise, interference, and so on) may be decisive for the logic interpretation of Z. It must be pointed out that the LP technology reports a large time constant, in the order of microsecond, a time constant several orders of magnitude higher than the one reported by HP technology, which is of a few tens of nanosecond. The exact behavior depends on the technology and the faulty circuit topology, i.e., the faulty gate, the particular fault location, the downstream parasitic capacitances, and the downstream gates.

B. Influence of Downstream Parasitic Capacitances

The faulty node is cross-coupled with the parasitic capacitances. These capacitances are related to neighboring lines [C_{N1}, C_{N2}, ..., C_{Ni} in Fig. 4], the transistor parasitic capacitances of the faulty gate [C_{gd(pA)}, C_{gb(pA)}, C_{gd(nB)}, and C_{gb(nB)}] and the transistor parasitic capacitances of the downstream gate [C_{gd(pZ)}, C_{gb(pZ)}, C_{gd(nZ)}, and C_{gb(nZ)}]. When applying a test sequence, the parasitic capacitances undergoing a rising (falling) transition may generate a pull-up (down) of the faulty node. The exact influence depends on the relationship between the capacitances undergoing a rising (falling) transition or remaining at a constant value. The faulty node behaves similar to an interconnect line affected by a full open [22]–[25]. The difference lies in that the faulty node is in a high impedance state for some specific excitations whereas the interconnect line affected by a full open always remains disconnected from the driver.

Increasing the parasitic capacitances undergoing a rising (falling) transition leads to higher positive (negative) voltage
variations induced in the faulty node. This is demonstrated in the results from Fig. 6. The simulated circuit was composed of the faulty NAND gate like the one in Fig. 4, but cross-coupled with a single neighboring capacitance. It is assumed that neighboring line is cross-coupled along all the line at the minimum distance allowed by the technology. A falling transition is applied at the faulty input of the NAND gate and a rising transition (RT) at the neighboring line. A positive voltage variation is thus generated due to the influence of the neighboring line. Fig. 6 shows $\Delta V_Z$, the induced voltage variation, for different cross-coupling lengths between the faulty line and the neighboring line ($L_c$). For lengths longer than 5 $\mu$m, a variation higher than $V_{DD}/2$ is already induced.

C. Stuck-Open Fault Behavior in Nanometer Technologies

An electrical model including the leakage currents and the downstream parasitic capacitances is required to accurately describe the SOF behavior. Simulations were carried out with the same circuit used to obtain the results in Fig. 5, but in this case applying test vectors causing the neighboring lines to undergo transitions as these vectors were applied. The simulations results are given in Fig. 7(a) and (b), where 16-nm PTM, LP, and HP models are considered, respectively. The plots report the transient evolution of the faulty nodes upon application of the same ten sets of two-vector sequences with a test period of 100 ns. The first vector of the sequence initialized the faulty node (Z) and the second one excited the fault. Every test sequence induced different excitation conditions on the neighboring lines. Black vertical lines and gray dotted vertical lines represent the moments where the first and the second vector of the sequence were applied, respectively.

From the plots in Fig. 7, observe how when the first vector is applied, $V_Z = 0 \text{ V}$. Every time the second vector of the sequence is applied, a pull-up/down up to several tenths of volts is induced due to the downstream parasitic capacitances. This influence is clearly observable in both technologies.

Charge flow then occurs due to the leakage currents in a similar manner as shown in Fig. 5. However, this influence is limited in time by the test period, since when the first vector of the next sequence is applied, $V_Z = 0 \text{ V}$. The impact of leakage currents is negligible for LP model [Fig. 7(a)]. This is due to the fact that the induced time constant is a few orders of magnitude higher than the test period (100 ns).

By contrast, the influence of leakage currents is significant for HP model, where $V_Z$ increases with time until the next vector is applied [Fig. 7(b)]. These results are consistent with those in Fig. 5. The HP model circuits are expected to work for shorter periods than 100 ns. For higher working frequencies, the influence of leakage currents may be similar to the LP model case. By contrast, the parasitic capacitances induce voltage variations up to several tenths of volts, which become of concern irrespective of test frequency.

V. EXPERIMENTAL BEHAVIOR

A design based on STMicroelectronics CMOS 65-nm technology was sent to fabrication to corroborate the impact of parasitic capacitances and leakage currents on defective circuit behavior. The layout of the design is shown in Fig. 8 and the picture of one of the devices is shown in Fig. 9. It is a multiproject IC where the design area and its corresponding pads occupies part of the bottom left area of the die. Apart from the power supply pads, the circuit comprises five digital pads, four inputs, and one output. The rest of pads pinpointed in Fig. 9 are devoted to another circuit. The design inputs and the output are enumerated as follows.

1) $\text{TIN}$: test input.
2) $\text{SE}$: scan enable.
3) $\text{CLK1}$: scan in/out clock.
4) $\text{CLK2}$: launch clock.
5) $\text{TO}$: test output.
A simplified schematic is shown in Fig. 10. It comprises random logic with open defects intentionally injected affecting the pMOS and nMOS networks of inverters (IV), NAND and NOR gates. These defective topologies were generated realistically according to the cell layout by including open contacts in the affected gates. Neighboring lines were routed to derive different topologies of the parasitic capacitances. Table I summarizes the topology information. Length refers to the defective line length, $C_{TD}$ to the total downstream parasitic capacitances reported by the layout extractor, and $C_N$ to the percentage of $C_{TD}$ corresponding to downstream neighboring coupling capacitances. The inputs of the defective gates and the neighboring lines are fully controllable, i.e., any possible state can be induced in the circuit. Two registers are used for this purpose: 1) the scan register shifts in the input vectors ($TIN$) and 2) the launch register maintains the state of the system between the application of the first vector and the load of the second one. Each register is managed by its own clock signal. The scan and launch registers are managed by CLK1 and CLK2, respectively. Once the response is captured, the scan register shifts out the results through TO, activating the scan enable signal (SE). The power supply voltage is 1.2 V, the clock period 100 ns, and the delay between the launch and capture 50 ns.

An automatic test equipment (ATE) was used to perform the measurements. A set of tests was applied to experimentally determine the defect detectability under different excitations of the neighboring lines and the leakage currents. The tests induced different proportions of the neighboring coupling capacitances undergoing a rising transition, a falling transition, and remaining at a constant value. The faulty gates were also excited to derive the different leakage current conditions. Table II summarizes the experimental results when considering the influence of neighboring parasitic capacitances. Among all range of neighboring lines excitations applied to the circuit, $C_{TD\text{ CRIT}}$ stands for the minimum percentage of $C_{TD}$ undergoing the same transition as the defective node inducing a test escape. Hence, for SOFs affecting a pMOS (nMOS) network, $C_{TD\text{ CRIT}}$ represents the minimum percentage of $C_{TD}$ undergoing a rising (falling) transition which induces a test escape. Observe that $C_{TD\text{ CRIT}}$ ranges between 51% and 64%, depending on the topology. The percentage required by the inverters is higher since their topologies have the lower parasitic neighboring capacitances, as reported in Table I.

Experiments were also conducted to demonstrate the influence of leakage currents. Figs. 11 and 12 show these results for gates with defective nMOS and pMOS networks, respectively. The plots represent the time required by the leakage to generate a change in the logic interpretation of the defective gate for different $\Delta V_{CN}$ values, where $\Delta V_{CN}$ stands for pulls up/down induced by the neighboring lines. This voltage variation was obtained from the electrical simulations of the same conditions used for the ATE. Neglecting transistor capacitances, $\Delta V_{CN}$ can be approximated by

$$\Delta V_{CN} = \frac{C_N - C_R}{C_{TD}} V_{DD}.$$ 

\(\Delta V_{CN} = 0\) V accounts for the reference case, where the measured delay is maximum, in the order of hundreds/thousands of microsecond. The delay decreases for the higher $\Delta V_{CN}$ values until an excitation already inducing a different logic interpretation of the defective gate is applied. In this case, the delay becomes null. Observe how the

---

**Table I**

<table>
<thead>
<tr>
<th>Defective topology</th>
<th>IV</th>
<th>NAND</th>
<th>NOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length (µm)</td>
<td>28.5</td>
<td>72.0</td>
<td>72.5</td>
</tr>
<tr>
<td>$C_{TD\text{ FF}}$</td>
<td>6.7</td>
<td>19.1</td>
<td>19.2</td>
</tr>
<tr>
<td>$C_N$ (%)</td>
<td>72</td>
<td>82</td>
<td>83</td>
</tr>
</tbody>
</table>

**Table II**

<table>
<thead>
<tr>
<th>Defective topology</th>
<th>pMOS</th>
<th>nMOS</th>
<th>pMOS</th>
<th>nMOS</th>
<th>pMOS</th>
<th>nMOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C_{TD\text{ crit}}$</td>
<td>64</td>
<td>62</td>
<td>59</td>
<td>51</td>
<td>59</td>
<td>57</td>
</tr>
</tbody>
</table>
topology with the lowest delay and $\Delta V_{CN}$ value is reported for the inverters. This is again expected because they have the lowest node capacitances and the highest ratio between the transistor and the neighboring parasitic capacitances.

The experimental results demonstrate the influence of leakage currents and neighboring parasitic capacitances. As the former derive high time constants, the latter is expected to become the most important contributor to test escapes for at-speed-testing.

VI. ANALYSIS OF TEST ESCAPES DUE TO STUCK-OPEN FAULTS

This section presents the analysis of HSPICE simulations carried out with the faulty circuits affected by SOFs. The source of the analysis was an industrial design in a 90-nm technology, although the same circuits were subsequently scaled-down to other technology nodes. A set of SOFs was intentionally injected to affect the four transistor network configurations, as shown in Fig. 13. These four networks summarize the topology of any open affecting the source or drain terminals of transistor(s), considering simple faulty parallel and serial networks for the pMOS and nMOS transistors.

The subcircuit comprising the faulty gate, the extracted neighboring parasitic capacitances, and the downstream gates was considered during the simulations to speed up the analysis. The parasitic capacitances were extracted from the design exchange format (.def) file. A recreation of a pattern file consisting of 250 pairs of test vectors was made. Thousand SOFs were randomly injected in every fault topology. The whole set of 250 pairs of vectors was considered for the evaluation of faulty circuit responses. In case any of the downstream gates propagated a faulty logic value for any two-vector sequence, the fault was detected; otherwise, a test escape was generated. The extracted circuits were scaled down to the 32- and 16-nm technology [20], and also to the 16-nm FinFET technology (PTM-MG model) [26]. It must be pointed out that the equivalent model, such as the one in Fig. 4, can be easily derived for a FinFET technology. The main difference for FinFET devices lies in that gate leakage components are small compared with the subthreshold ones. The LP and HP applications are considered for every technology node. The working period during electrical simulation was 100 ns for the LP circuits and 1 ns for the HP counterparts. In fact, 100 ns is the test period of the 90-nm technology design in the real test environment.

Information about test escapes obtained from postprocessing of the electrical simulation results is given in Table III. The number of test escapes rises with technology shrinking irrespective of fault topology. This increase is more abrupt for the LP technologies than for the HP technologies, except for the FinFET technology. This tendency is mainly due to differences in scalability of transistor physical dimensions and power supply voltage. It is also worth noting that the FinFET circuits have more test escapes than the MOS counterparts. As transistor capacitances are lower in the FinFET technologies, the downstream parasitic capacitance effect becomes preponderant.

Leakage currents have a slight influence considering a test period of 1 ns. For this reason, the same simulations are repeated for the HP circuits over a longer test period; that is, the same post-processing analysis is performed while increasing the test period to 10 and 100 ns. The downstream parasitic capacitances have the same logic influence irrespective of the test period since the applied patterns are the same. However,
the increasing test period implies increasing the time the faulty node is in the high impedance state. Hence, the leakage currents have more time to generate a charge flow and modify the voltage of the faulty node. Differences in the results can thus be justified only by the influence of these leakage currents. The results are summarized in Table IV. Note the small influence for the 32- and 16-nm PTM models when the test period is 10 ns. However, the influence becomes more noticeable for 100 ns. The 16-nm PTM-MG model simulations undergo leakage influence for 10 ns, mainly because of the lower transistor capacitances and dimension scalability due to the discrete width of the transistor fins.

When an SOF affects a serial network configuration, the leakage influence is dominated by the subthreshold current of the fault free transistor network connected to the gate output, which pulls the node to the faulty voltage value. For this reason, the number of test escapes decreases for longer test periods, irrespective of the technology. In fact, the number of test escapes is almost null for the 16-nm PTM-MG model for 100 ns. By contrast, when the SOF affects a parallel network, there is a fight between the p-network and the n-network connected to the output. An intermediate voltage value which may be interpreted either as 0 or 1, depending on the exact topology of the faulty and downstream gates, is thus induced.

A tendency to interpret these intermediate voltages as 0 is reported for the technologies used in this paper. For this reason, the leakage currents induce an increase in the number of test escapes for SOFs affecting parallel n-networks and a decrease for the faulty parallel p-networks. Observe that 14.780% of test escapes are reported for SOFs affecting parallel n-networks for the 16-nm PTM HP model over a test period of 100 ns. This percentage increases dramatically in PTM-MG, reaching up to 95.745% of test escapes. This is partially justified by logic threshold variations resulting from downscaling of this technology and the discrete width of transistor fins. On the contrary, the number of test escapes is extremely low for the faulty parallel p-networks.

The results show that the influence of leakage currents is not noticeable at the working frequency whereas it is highly significant at lower test frequencies. In this context, the leakage currents help detect the SOFs affecting serial networks. For parallel networks, they can help detect or mask the fault, depending on the faulty circuit topology. For the configurations in this paper, leakage currents help detect SOFs affecting parallel p-networks but increase the number of test escapes when SOFs affect parallel n-networks.

The results in Table III lead to the question whether these escape rates are critical. Assuming that the most probable cause of an SOF is an open contact, it is possible to derive DPPM according to

$$
\text{DPPM} = N_{\text{contacts}} \cdot \text{POF}_{\text{contact}} \cdot P_{\text{escape}}
$$

where \(N_{\text{contacts}}\) is the number of contacts prone to SOFs, \(\text{POF}_{\text{contact}}\) the probability of failure of a single contact and \(P_{\text{escape}}\) the escape probability of an SOF. Considering a medium-sized circuit with \(2 \times 10^7\) contacts and according to the results in Tables III and IV, a representative escape probability \(P_{\text{escape}} = 0.01\) is assumed. The relationship between DPPM and \(\text{POF}_{\text{contact}}\) can be derived from (6), as shown in Fig. 14. DPPM reaches nonnegligible values when \(\text{POF}_{\text{contact}}\) ranges between \(10^{-11}\) and \(10^{-10}\). These DPPM values due to SOFs may be unacceptable for a single fault class, even for noncritical applications. This is, however, a pessimistic scenario since every SOF is assumed to be tested only once.
The results presented in this paper show that the number of test escapes due to SOFs is of concern in nanometer technologies. Hence, the test strategy must be refined to improve test robustness. For this purpose and without loss of generality, consider the example in Fig. 15, where an SOF is affecting an nMOS transistor of an AO gate. The faulty gate is in turn driving a NAND and a NOR gate and the faulty is affecting an nMOS transistor of an AO gate. The faulty gate is propagated through the NOR gate, then G is set to 0.

According to the work in [18], some recommendations can be followed when configuring the faulty gate and the corresponding downstream gates to minimize the influence of leakage currents. In the above example, three combinations for inputs (B C) can be used to propagate the fault. Among them, (0 0), (0 1), and (1 0), the most appropriate one is (0 0) since it minimizes the leakage through the stack of the two serial nMOS transistors. Regarding the downstream two-vector sequence, an rising transition is applied at A to excite the fault. Assuming the output of the faulty gate is propagated through the NOR gate, then G is set to 0.

According to the work in [18], some recommendations can be followed when configuring the faulty gate and the corresponding downstream gates to minimize the influence of leakage currents. In the above example, three combinations for inputs (B C) can be used to propagate the fault. Among them, (0 0), (0 1), and (1 0), the most appropriate one is (0 0) since it minimizes the leakage through the stack of the two serial nMOS transistors. Regarding the downstream two-vector sequence, an rising transition is applied at A to excite the fault. Assuming the output of the faulty gate is propagated through the NOR gate, then G is set to 0.

In a general configuration with multiple neighbors, the state of the entire neighborhood should be considered to determine fault detectability, as already considered for interconnect full open faults [24], [27], [28]. The problem is similar to that about crosstalk in [29] and [30], but with more relaxed conditions. In fact, it is not feasible to set the best test scenario for every possible fault. Instead, a different approach should be taken to minimize the risk of test escapes while avoiding increasing test complexity. The use of N-detect appears as a valid option for this purpose [31], [32]. As this strategy excites the same fault multiple times by generating different neighboring excitations, it should increase the probability of inducing at least one proper configuration to detect the SOF. Although successful in some contexts, N-detect improves detectability at the expense of increasing the number of test vectors. If the criterion for pattern generation is not deterministically based on optimizing the neighboring conditions, its application may not be feasible.

An alternative approach consists in a previous analysis of faulty topologies prone to the test escapes and the subsequent modification or even addition of some test vectors. This process is expected to be time consuming but must be done once for every design, with no implications on product development time. The diagram flow in Fig. 16 shows an example of the process steps. The first one consists in extracting the parasitic information between coupling lines, i.e., from a .def file. Based on this information, the subset of potential candidates to undergo a test escape is selected. For every possible SOF affecting the selected nodes, the two-vector sequences exciting the fault are obtained from the pattern file. Subsequently, the neighboring state is analyzed for the vector pairs exciting the fault. If any induces a robust test scenario, the SOF is considered as covered. Otherwise, these vectors should be revisited to modify the don’t care bits in order to generate a robust test scenario. If no appropriate conditions are derived, a new vector sequence must be added to cover this fault.

It must be pointed out that if multiple two-vector sequences excite the same fault, finding a single case with a robust test scenario is sufficient, making it unnecessary to analyze the rest of vectors. The analysis to check the possible occurrence of test escapes is based on (3), which specifies the conditions for every fault topology. At the end of this process, the pattern file obtained is optimized to cover the maximum number of SOFs.

### TABLE V

<table>
<thead>
<tr>
<th>Test sequence</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>rt</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

### VII. TEST RECOMMENDATIONS

**Best Test Scenario to Minimize Leakage**

<table>
<thead>
<tr>
<th>Test Scenario</th>
<th>A</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Good</td>
<td>rt</td>
<td>0</td>
</tr>
<tr>
<td>Good</td>
<td>rt</td>
<td>1</td>
</tr>
<tr>
<td>Worst</td>
<td>rt</td>
<td>1,5</td>
</tr>
<tr>
<td>Best</td>
<td>rt</td>
<td>rt</td>
</tr>
</tbody>
</table>

In Table V, the most robust test condition to detect this SOF is obtained.

In a general configuration with multiple neighbors, the state of the entire neighborhood should be considered to determine fault detectability, as already considered for interconnect full open faults [24], [27], [28]. The problem is similar to that about crosstalk in [29] and [30], but with more relaxed conditions. In fact, it is not feasible to set the best test scenario for every possible fault. Instead, a different approach should be taken to minimize the risk of test escapes while avoiding increasing test complexity. The use of N-detect appears as a valid option for this purpose [31], [32]. As this strategy excites the same fault multiple times by generating different neighboring excitations, it should increase the probability of inducing at least one proper configuration to detect the SOF. Although successful in some contexts, N-detect improves detectability at the expense of increasing the number of test vectors. If the criterion for pattern generation is not deterministically based on optimizing the neighboring conditions, its application may not be feasible.
The continuous demand for better products requires high-quality tests and low escape rates, especially for safety critical applications. In present technologies, the intragate opens are an important source of defects, most of which can be modeled as SOFs. The classical approach to the SOF detection, based on a two-pattern sequence, has proved to be effective for a wide range of technologies. However, this paper demonstrated that SOF detectability decreases with technology shrinking because of the influence of leakage currents and downstream parasitic capacitances. These induce a nonnegligible number of test escapes, which increase with technology shrinking. The obtained escape ratios may be unaffordable, especially for critical applications where the low DPPM values are demanded. Although the influence of leakage currents is demonstrated to be insignificant for at-speed testing, their impact becomes preponderant if the frequency is reduced at least one order of magnitude. This fact may be of interest in those cases where an increase of total test time is affordable.

Test strategy of the SOFs must be reviewed to extend their detectability in present and future technologies. In this direction, a proposal for the analysis of SOFs prone to the generation of test escapes was proposed. In critical cases, modification of the don’t care bits or even addition of new patterns is required to assure the detectability of these SOFs.

**ACKNOWLEDGMENT**

The authors would like to thank NXP Semiconductors, The Netherlands, for providing the 90-nm technology and the industrial circuit used as a basis for its scaled down versions.

**REFERENCES**


Daniel Arumí received the M.S. degree in industrial engineering and the Ph.D. degree in electronic engineering from the Universitat Politècnica de Catalunya (UPC), Barcelona, Spain, in 2003 and 2008, respectively.

He is currently an Assistant Professor with the Department of Electronic Engineering, UPC. His current research interests include defect-based testing, fault modeling, defect diagnosis, and security in ICs.

Rosa Rodríguez-Montañés received the M.S. degree in physics from the Universitat de Barcelona, Barcelona, Spain, in 1988, and the Ph.D. degree in physical science from the Universitat Politècnica de Catalunya (UPC), Barcelona, in 1992.

She has been an Associate Professor with the Department of Electronic Engineering, UPC, since 1994. She spent her sabbatical leave with the Test Group, Philips Research, Eindhoven, The Netherlands, in 2002. She is currently involved in fault models, defect characterization, and defect diagnosis of digital nanometric CMOS technologies.

Joan Figueras (M’88) received the M.Sc. and Ph.D. degrees from the University of Michigan, Ann Arbor, MI, USA, and the Ph.D. degree from the Universitat Politècnica de Catalunya (UPC), Barcelona, Spain.

He is currently with the Department of Electronics Engineering, UPC, where he has research and teaching responsibilities in the areas of electronics and digital- and mixed-signal design and test.

He has an extensive publication record, and has presented seminars and tutorials in professional meetings and NATO seminars on topics related to low-power design and quality in electronics. His current research interests include emerging topics in low-power design and advanced test of electronic circuits and systems.

Dr. Figueras was an Associate Editor of the IEEE TRANSACTIONS ON COMPUTER-AIDED DESIGN OF INTEGRATED CIRCUITS AND SYSTEMS, and is an Editor of the Journal of Electronic Testing: Theory and Applications, and a member of the Steering and Program Committee of several Test and Low Power Design Conferences.