Problems due to open faults in the interconnections of self-checking data paths

M. Favalli
DI - University of Ferrara - Italy
44100 Ferrara - Italy

C. Metra
DEIS - University of Bologna - Italy
40136 Bologna - Italy

Abstract

In this work, the problem of open faults affecting the interconnections of SC circuits composed by data-path and control is analyzed. In particular, it is shown that, in case opens affect control signals, some problems may arise even if both control and data-path signals are concurrently checked. In particular, wrong codewords may be generated at the outputs of multiplexers and registers. To address this problem, new registers and multiplexers are proposed which allow the design data-paths which are TSC with respect to opens (and resistive opens). These components are also TSC with respect to stuck-at, transistor and gross delay faults. They present a good testability with respect to resistive bridgings.

1 Introduction

Recent works in the field of failure analysis and testing have evidenced the relevance of open (break) faults in Deep Submicron (DSM) ICs [1]. These faults may affect wires as well as vias [2, 3] and they are due to production failures or stress occurring during normal circuit operations,

In the case of Self-Checking (SC) systems [4], these faults can be accounted in the design of self-checking functional blocks inside a data-path. The same holds in the case of self-checking FSMs used to the purposes of control.

Conversely, in this paper, we show that some problems arise in the case of opens affecting the wires[1] bringing the control signals to the data-path. Therefore, this paper will focus on the interface between the data-path and the control circuitry of SC systems.

In particular, in case of open faults affecting the selection signals of multiplexers or the write-enable signals of registers, wrong codewords may propagate inside the data-path, thus leading to errors which are undetectable by the most of the commonly used kind of error detecting codes. This may occur if the open affects a control signals either in all the bits of a word or in a subset of them.

As it will be shown, the problem cannot be solved by generating a two-railed version of control signals and by separately checking them. This approach, in fact, can be used to detect single stuck-at faults [5], but not opens affecting the wires in an unpredictable position. Of course, the problem could also be solved by duplicating the data-path or by introducing some protection at higher levels (such as the algorithmic one). It is rather evident, however, that the considered problem does not justify the higher costs of duplication or the design complexity required by such approaches.

To solve this problem, we propose a simple design methodology which is based on the duplication of data-path control signals and on a new design of multiplexers and registers which are totally self-checking (TSC) with respect to single open faults affecting their control signals. In the presence of an open fault on a control signal, in fact, either the correct codeword or a non-codeword is given at the output of the considered component, thus verifying the fault secure (FS) property [4]. In case the multiplexer are not redundant, at least a codeword exists which exposes the effects of such a fault thus verifying the self-testing (ST) property [4].

These properties have been verified also in the cases of: a) resistive opens [3] which may result in both slow-to-rise and slow-to-fall failures; b) of opens resulting in intermediate voltages of the affected signal.

In addition, the resulting registers and multiplexers are totally self-checking with respect to internal faults such as stuck-at faults, transistor faults and gross delay faults. The proposed circuits present also a good testability with respect to resistive bridging faults.

Therefore, this kind of components can be conveniently used in the design of SC systems based on a design paradigm where the control and the data-path are separately checked.

This paper is organized as follows. The problem of opens in SC circuits is discussed in Section 2. Section 3 presents the basic idea for the design of SC multiplexers and registers in the presence of ideal opens. The possible implementations in the CMOS technology of such components is analyzed in Section 4. Section 5, instead, discusses the behavior of the proposed schemes in the presence of opens whose behavior is not ideal. The SC capabilities of the proposed multiplexers and registers are analyzed in Section 6 with respect to internal faults, while conclusions are drawn in Section 7.

2 The problem

Let us consider a portion of a self-checking data-path and control (Fig. 1). We suppose that the information flow in the

[1] Notice that these wires may be typically longer than other signals inside the circuit, thus presenting a relevant probability of opens.

data path is encoded by means of an error detecting code, and that the components along the data-path are code-disjoint [4]. This latter hypothesis allows to use only a single checker connected to the data-path output with consequent savings in area occupation. It should be noticed, however, that even if all the signals in the data-path are separately checked, the problems described here would be still in order.

In the remainder of this section, we will suppose that both the functional units (FU_1 and FU_2) in Fig. 1 produce data encoded by means of an error detecting code checked by C_{dp}. At this regard, we will suppose to use all or partial unidirectional error detecting codes such as the Berger one. The same considerations may be also made in case of residue codes. In fact, self-checking data-paths have been designed for the Berger code [6, 7], or the residue codes [8]. The proposed approach, instead, is not well suited for the case of parity codes [9], since, as it will be seen, it exploits the unidirectional error detection capabilities of the considered codes. The control unit is also supposed to be self-checking with a checker (C_c) which verifies its output signals and its state variables.

The kind of fault considered here is the (single) wire open (break), which in CMOS logic insulates the logic driving a signal from the inputs of all or a fraction of the CMOS blocks fed by such a signal [4]. Modeling the behavior of the floating part of the wire may be rather complex. In fact, it depends on its capacitive and resistive couplings with other signals in the circuit. For the sake of readability, we make the simplest hypothesis about the induced faulty behavior by supposing that its floating part remains at a given logic value along a clock period.

This stuck-at like behavior does not directly account for capacitive couplings with on-(off)-chip noise sources, which may make the floating signal change value along a clock period (notice, that the possibility for the floating wire to assume intermediate voltage values should also be accounted). In addition, in case of resistive opens, it is also possible that the affected signal has an additional delay, but a correct final value. In section 5, we will show that the proposed approach can take into account also these possible behaviors.

In the presence of opens (for instance, **open1** in Fig. 1) affecting a control signal, two possible cases are in order depending on whether the open has a location making its effects affect the C_c inputs or not.

In the first case, the open is easily detectable, in the second case, some problems may arise. Suppose, in fact, that: a) the open occurs in the location indicated in the figure; b) because of such a fault, all the signal branches insulated from the signal source have a wrong logic value. In such a case, the wrong data is selected by the multiplexer. Such data, however, still constitute a valid codeword and it will not be detected by the data-path checker (C_{dp}).

The same behavior may be in order also if the open affects only a fraction of the two-way multiplexers. This case is instantiated in Fig. 2, where only 4 two-way multiplexers are affected by the break. If their control signal has a value different from the fault-free one, the word 1010 is propagated, instead of 1100, thus resulting in a non unidirectional error.

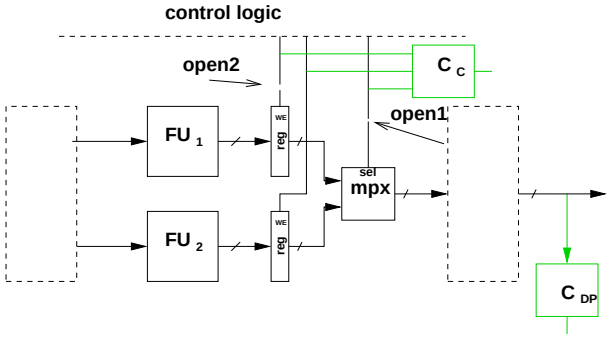

Figure 1. Example of a SC system where the control unit and the data-path outputs are separately checked by the checkers C_c and C_{dp}, respectively.

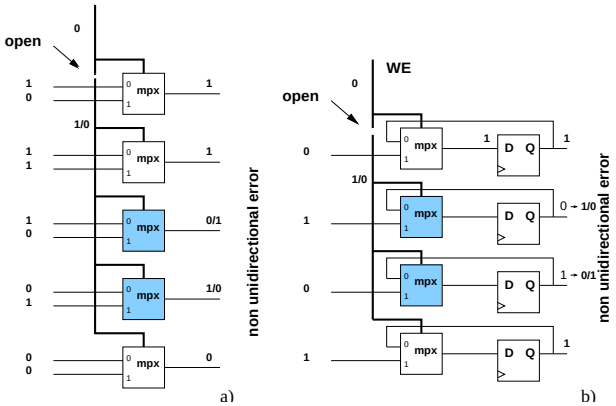

Figure 2. Because of an open fault, 4 single bit multiplexers (a) have a wrong selection value (1 instead of 0, 1/0). Therefore, two multiplexers (the shaded ones) produce a non unidirectional error which cannot be detected by a large fraction of the mostly used error detecting codes. For the same reason, the two shaded flip-flops (b) receive a write signal instead of an hold command, thus producing a non unidirectional error.

If the break affects the WE signal of a register (**open2**), the same kind of problems is in order. In this case, depending on the kind of error, either the previous codeword is wrongly retained, or a new codeword is erroneously written in the register. In both cases, the error cannot be detected by C_{dp}.

Also in this case, the problem may be in order even if only a fraction of flip-flops is affected by the fault (Fig. 2b).

3 Basic idea

In order to avoid the problem described in the previous section, we propose a scheme where the control signals are duplicated (this is possible since the control unit is typically smaller than the data-path) and subsequently exploited in or-

der to make open faults result in a non codeword at the output of the controlled multiplexers or registers. If the logic in the fan-out of such blocks is code-disjoint (CD), then such an error indication may be propagated to C_{dp}.

Conversely, if the considered signals are individually checked, the errors are immediately recognized.

The key block of the proposed method is very similar to a two-way multiplexer controlled by the selection signal and its complement, thus matching with the case where the control unit is implemented by using a two rail approach.

The idea is to produce an error indication if the two signals are not two-railed because one of them is faulty.

Working with unidirectional error detecting codes, a first approach minimizing the latency of errors could provide always an unidirectional error in the presence of an error affecting the two control signals. Unfortunately, by using this approach, it is very difficult to design the multiplexer to be ST with respect to internal faults.

As an alternative, the multiplexer can be designed in such a way (Fig. 3a) that, in the presence of an error on one of the selection signals (p, n), either the correct output is produced, or an error is produced. Such an error is univoquely determined by the kind of errors affecting the selection signals (i.e. it is independent from the multiplexer data inputs). This latter property ensures that, if all (or a fraction) of bit level multiplexers are affected by the same fault on their control signals, then either a correct word is produced or a non codeword is produced (with the used kind of codes).

Fig. 3b illustrates this kind of behavior on a Karnaugh map. In particular, when the two railed selection signals have the 00 logic values, all the affected multiplexers have the output at 0 independently of the data inputs. If the error produces a 11 value, two cases may be in order: a) data inputs have the same value; b) data inputs have different values. In case a), the correct output is produced. In case b), a logic 1 is always produced. Therefore, the correct value is produced if the signal selected in the fault-free circuit is at logic 1, otherwise, an error is produced.

By considering more than one multiplexer, it can be noticed that, for a given behavior of the faulty signal, the errors are always unidirectional, thus never resulting in a wrong codeword and ensuring the FS property. Conversely, if both selections are possible with data inputs at different values, the ST property is ensured (this may not be ensured in case of strong correlations between control and data values).

The same approach can be used to design the multiplexer which selects between data writing/retention in registers. The proposed scheme is that illustrated in Fig. 4a, where WE and WD are the two-railed version of the write enable.

Also in this case, either the correct word is written inside the register or a non codeword is written. This holds true if a whole register or only a subset of its flip-flops are affected by an error on one of the two railed selection signals. Therefore, the registers are FS with respect to such kind of faults.

As it can be seen from Figs. 4b-c, the ST property is ensured if the following sequences can be applied to the register:

$$dat, WE, WD = <110, 101>, \\ <---, 110>, <110, 010>, <010, 101> \quad (1)$$

Therefore, the TSC property is verified.

4 Implementation dependent considerations

In the CMOS technology, multiplexers can be implemented in ways different from their mapping on elementary logic gates (NAND/NOR). As it can be seen in Figs.5, this hold true also for the proposed methodology, which can be easily implemented by using pass-transistors logic (Fig. 5a) or a FCMOS macro-gate (Fig. 5b). Unfortunately, these structures match the logic behavior outlined in the previous section only under fault free conditions. Both of them present a high impedance state of the node x in the presence of an open resulting in a wrong logic 0 on one control signal. This may lead to the retention of previous output values and to consequent bidirectional errors.

Therefore, it is more convenient to use a direct mapping of the multiplexer logic function of CMOS gates (Fig. 5c).

5 Opens with non ideal behavior

In the previous section, we have considered an ideal behavior of open faults. This behavior occurs if: a) the floating part of the signal presents leakages toward the power supply or the ground; b) it has a capacitive coupling with another signal. The AC and DC couplings, however, may not verify these hypotheses, giving rise to a more complex behavior. For instance, the floating part of the wire may be coupled with more than one signal. Conversely, the open may be only partial, thus giving rise to a resistive open. Therefore, the proposed design technique has to be validated also in the presence of such non ideal behaviors.

5.1 Resistive opens

In the case of resistive opens, the faulty line has a slow to switch (rise and fall) behavior. Depending on the size of the resulting additional delay and on the slack on the multiplexer output with respect to the clock sampling instant, this kind of behavior may or may not result in some data-path register sampling a wrong logic value.

Therefore, the detection of this kind of faults strongly depends on the logic blocks placed between the multiplexer output and the flip-flops sampling the signals which may be affected by the additional delay.

To analyze the detectability of these faults in a self-checking system, some hypothesis should be made regarding the kind of sampled errors. At this regard, accordingly to the hypothesis made in the previous section, we will suppose that the logic belonging to the multiplexer fan-out let allow

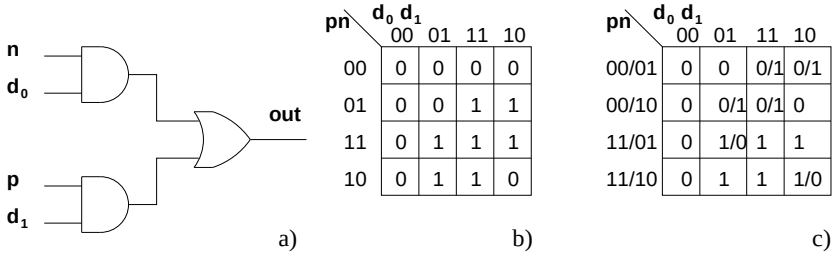

Figure 3. Proposed multiplexer scheme for on-line detection of open faults affecting the selection signals a). Its true table b) and its behavior in the presence of a fault on one selection signal c).

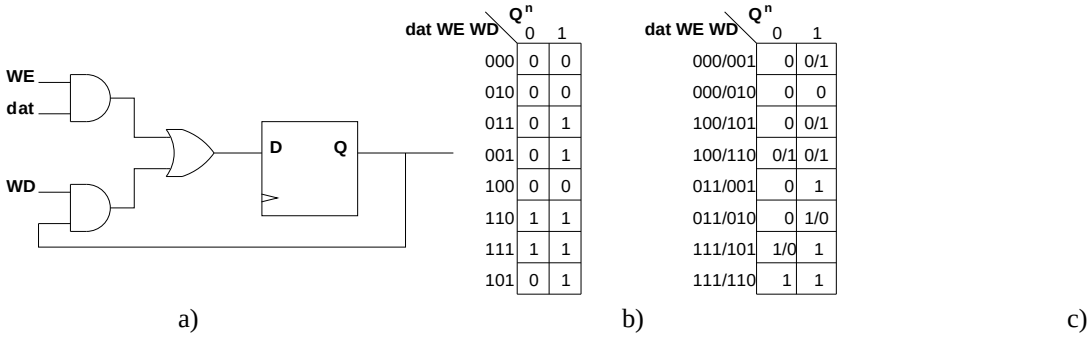

Figure 4. Proposed register cell scheme for on-line detection of open faults affecting the selection signal a). State transition table of the corresponding FSM b). State transition table in the presence of an error one of the two selection signals c). The table rows show the faulty values of dat, WE, WD and their fault-free values exciting the fault. The table entries show the faulty/fault-free values of Q^{n+1}.

the transitions at its inputs to propagate through paths with the same parity of inversions.

In order to guarantee the FS property also with respect to this kind of faults, we have to show that it is not possible that both a rising and a falling transition occurring at different multiplexer's outputs are delayed, thus resulting in the sampling of bidirectional errors.

Let us first consider the case where the transition is originated by a transition of the multiplexer control signals only (Fig. 6). In such a case, the multiplexer data inputs have different values that do not change in the two considered periods. In case one of the two selection signals is affected by a resistive open, its rising and falling transition will be affected by an additional delay. In the first case, the intermediate configuration 00 will be present at the multiplexer (selection) inputs, while in the second one, the configuration 11 will be present. In the first case, all the affected multiplexers may have a 0 sampled instead of a 1, and in the second case, they have a logic 1 instead of a 0. In both cases, no bidirectional error can be produced.

The case where both the data inputs and the selection signals switch, instead, is slightly more complex because a dynamic hazard can be generated. It can be verified, however, that also in these cases, it is not possible to generate a bidirectional error if the transitions of data signals are not affected themselves (as a consequence of a multiple fault) by a timing violation. In fact, a delayed 1 to 0 (0 to 1) transition may result in the sampling of a wrong final logic value only if the two control signals traverse the 11 (00) configuration.

Therefore, also in the case of resistive opens, the FS property is verified. Notice that this holds true even if only a fraction (or none) of the paths connecting the affected multiplexers with the sampling elements has a timing which results in the sampling of wrong logic values. If the additional delay is large enough, also the ST property will be verified. Otherwise, the TSC property is not verified (this of course is normal in the case of parametric faults) and the SFS property should be analyzed. This property, however, is complex because it involves sequences of faults.

5.2 Opens leading to intermediate voltages

The insulated part of the affected wire may have an intermediate voltage because of the coupling with other signals and/or of leakage currents. From the point of view of steady state conditions, the FS property is ensured because none of the possibilities in order may lead to a wrong codeword at the output of the multiplexer.

This case, instead, is very dangerous under dynamic conditions: let us suppose that the fault-free value of the signal is 1, while its faulty voltage is interpreted as a high but degraded voltage. Suppose also that the affected signal control two multiplexers which present two opposite transitions at the data input which is selected under fault-free conditions.

Depending on the multiplexers' way to interpret such

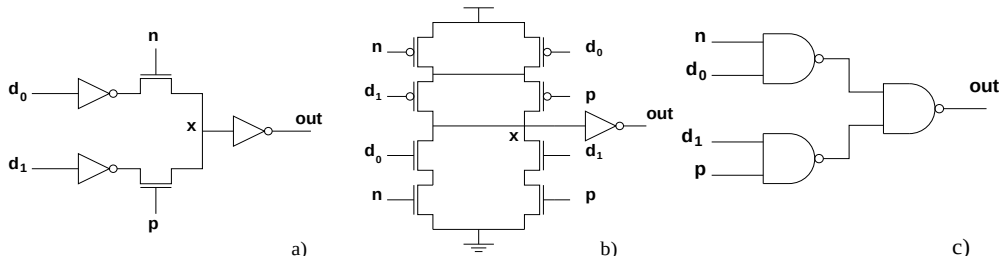

Figure 5. Different possible implementations of the logic scheme of Fig. 3.

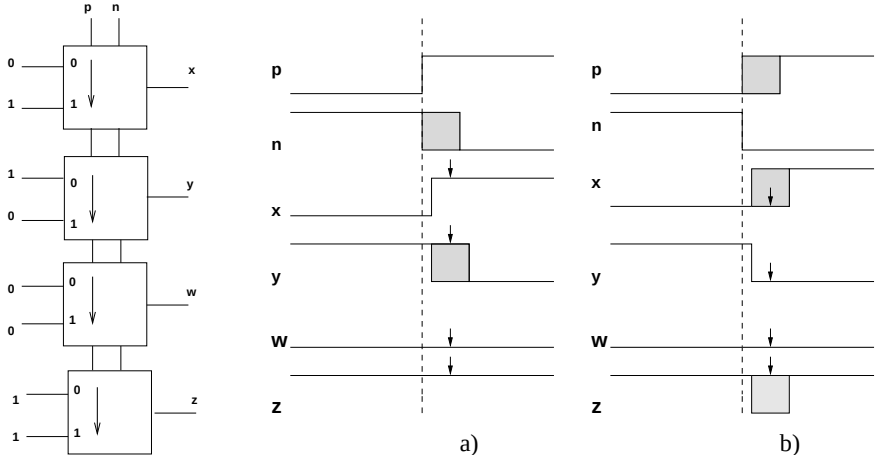

Figure 6. Effects of resistive opens on control signals. The arrows denote the instant in which the multiplexers outputs are sampled. In the considered example, the control signals switch while the data inputs are kept constant. In case a), the signal n is faulty. Because of the delay, the multiplexers receive the value 11 of p and n, that result in a wrong 1 if the two data inputs have different value. Hence, only 01 transitions are affected. In case b), p is faulty and the multiplexers receive the configuration 00 which may affect only 01 transitions or steady 1 values.

voltages, it is possible that both transitions are delayed, thus possibly giving rise to a bidirectional error. At this regard, it is worth mentioning that the NAND gate implementation does not suffer from this problem. In fact, an intermediate voltage on a control signal may delay only the pull-down path of NAND gate. Therefore, only rising transitions of data inputs can be delayed and no bidirectional error may be produced. The same does not hold true for the pass-transistor implementation.

6 TSC property with respect to internal faults

In this section, we will analyze the TSC properties of the considered multiplexers and registers with respect to internal faults. In particular, we will first consider stuck-at, transistors and gross delay (i.e. transition) faults at the logic level. Then, we will suppose a CMOS implementation of the multiplexer and we will analyze resistive bridging faults.

Notice that, a part from the case of bridgings, the effects of the considered faults affect only an output signal of the whole block. At the word level, such faults will result in a single bit error, thus verifying the FS property.

6.1 Stuck-at faults

The proposed multiplexer, for which we have considered the gate level structure of Fig. 3, has been verified to be ST with respect to stuck-at faults. In particular, the tests

$$n,d_0,p,d_1 = <110->,<0110>,<1001>,<0-11> \quad (2)$$

are sufficient to test for all the multiplexer stuck-ats.

The register cell is also ST with respect to stuck-ats. In such a case, the tests for the input multiplexer are given by:

$$dat,WE,WD,Q = <110->, \\ <1010>,<0101>,<-011> \quad (3)$$

which need the application of the following test pairs:

$$dat,WE,WD = <---,110>, \\ <010,101>,<110,010>,<110,-01> \ . \quad (4)$$

which have been verified to test also all the stuck-at faults inside the multiplexer.

6.2 Gross delay faults

A gross delay fault is an additional delay in a gate output transition which is characterized by a size which is large enough to result in the sampling of a wrong logic value independently of the actual signal and circuit timing. In practice, the behavior induced by such a kind of faults is often handled by using the transition fault model.

The gross delay faults affecting the two AND gates and the output OR gate in the scheme of Fig. 3 are all detectable

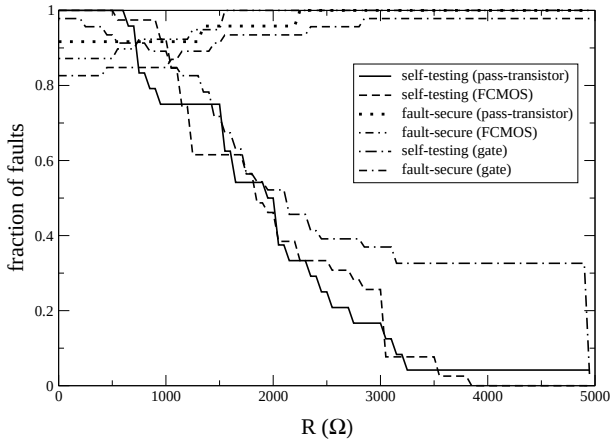

Figure 7. Fraction of resistive bridging faults satisfying the ST and the FS properties as a function of the bridging resistance.

by applying input codewords to the considered multiplexer. Therefore, the ST property is verified.

6.3 Transistor faults

It has been verified that the CMOS gate level implementation of the proposed multiplexer (Fig. 5c) is testable with respect to all transistor stuck-open and on faults. The same does not hold for the two alternate implementations.

6.4 Bridging faults

In the case of bridging faults, we have considered the three circuits of Fig. 5. The circuits of Fig.5a and b are considered only to the purpose of comparison. In such circuits, we will suppose that data, control and multiplexer output drivers have the same transistor sizing.

The choice of the fault set, of course, requires the knowledge of the actual IC's layout and the use of inductive fault analysis [10] based tools. To be independent from it, we will consider all the possible resistive bridgings [11] between: a) the nodes belonging to a multiplexer (including its input and output nodes); b) the internal nodes of a multiplexer; c) the input/output signals of another multiplexer.

For each fault, the circuit (constituted by two multiplexers, data and control drivers) has been simulated at the electrical level for 100 random vectors under dynamic conditions. The results achieved are shown in Fig. 7 as a function of the bridging resistance.

As can be seen, the ST property is verified for a good fraction of resistive bridging faults. Unfortunately, there is a fraction (18%) of faults which do not verify the FS property. These faults are due to resistive bridgings between control signals and ground or power supplies. If these faults give rise to intermediate voltage values on the affected signal, there is the same problem discussed in Sect. 5.2 in the case of opens originating intermediate voltages. This is mainly due to the use of symmetric gates (with equal driving strength and logic thresholds close to $V_{DD}/2$). The problem can be avoided by using strong drivers for the control signals.

7 Conclusions

This paper addresses the problem of open faults in self-checking circuits composed by control and data-path. In particular, it is shown that, in case the control and the data-path are separately checked, open faults affecting the control signals of multiplexers and registers may result in undetected errors. These faults cannot be neglected because of control wires are typically long thus exposing a large critical area to breaks and opens. Differently from the stuck-at faults case, a separate checking of control signals may be not effective for several fault locations.

In order to approach this problem, a new 2-way multiplexer design is proposed which allows to design word level multiplexers and registers which are TSC with respect to open faults affecting the interconnections.

The proposed circuits have been shown to maintain such properties even if the open faults exhibit a non-ideal behavior. In addition, they are TSC with respect to stuck-ats and transistor faults. While they have good ST properties with respect to resistive bridging faults.

References

[1] E. McCluskey and C.-W. Tseng, "Stuck-fault tests vs. actual defects," in *Proc. of Int. Test Conf.*, pp. 336 – 343, 2000.

[2] W. Needham, C. Prunthy, and E. Yeoh, "High volume microprocessor test escapes an analysis of defects our tests are missing," in *Proc. of Int. Test Conf.*, pp. 25 – 34, 1998.

[3] Baker and et. al., "Defect-based delay testing of resistive vias-contacts," in *Proc. of Int. Test Conf.*, pp. 467 – 476, 1999.

[4] P. Lala, *Self-Checking and Fault Tolerant Digital Design*. Academic Press, 2001.

[5] A. Kakaroudas and et al., "Hardware and power requireents of self-checking circuits," in *Int. Conf. on Electronic, Circuits and Systems*, pp. 1655 – 1658, 1999.

[6] J.-C. Lo, S. Thanawastien, T. R. N. Rao, and M. Nicolaidis, "An SFS Berger Check Prediction ALU and Its Application to Self-Checking Processor Designs," *IEEE Transactions on CAD*, vol. 11, pp. 525 – 540, April 1992.

[7] S. Gorshe and B. Bose, "A self-checking ALU design with efficient codes," in *Proc. of IEEE VLSI Test Symp.*, pp. 157 – 161, 1996.

[8] I. Noufal and M. Nicolaidis, "A CAD framework for generating self-checking multipliers based on residue codes," in *Design Aut. and Test in Europe - DATE*, pp. 122 – 129, 1999.

[9] M. Nicolaidis, "Efficient implementations of self-checking adders and ALUs," in *Proc. of Int. Symp. Fault-Tolerant Comput.*, pp. 586 – 595, 1993.

[10] J. Shen, W. Maly, and F. Ferguson, "Inductive Fault Analysis of MOS Integrated Circuits," *IEEE Design & Test*, pp. 33 – 26, Dec. 1985.

[11] H. Hao and E. McCluskey, ""Resistive Shorts" within CMOS Gates," in *Proc. of Int. Test Conf.*, pp. 292 – 301, 1991.