A Fault-Tolerant Combinational Circuit Design*

S. Ostanin, I. Kirienko, V. Lavrov
Tomsk State University
sergeiostanin@yandex.ru, irina.kirienko@sibmail.com, neverlva@gmail.com

Abstract

In this paper we have proposed a fault-tolerant scheme based on totally self-checking system with low overhead. The scheme has only one self-checking module and another one is simplex module (combinational circuit). The analysis of the reliability of proposed scheme is given.

1. Introduction

In modern military, space, medical, etc. computer systems requirements for hardware reliability are increased. One of approaches to increase of reliability of the system is fault tolerance. A fault-tolerant system is one that can continue the correct performance of its specified tasks in the presence of faults. Fault tolerance is assumed to add one of the redundancy: hardware redundancy, software redundancy, information redundancy or time redundancy.

One of the most common techniques providing the fault-tolerant property is triple modular redundancy (TMR) [1]. The basic idea of TMR is to triplicate the circuit and perform a majority vote to determine the output of the system. The main difficulties with TMR are the voter, if the voter fails, the complete system fails, and high area overhead.

A fault-tolerant system that is based on two replicas of a self-checking circuit and on error-masking interface has been suggested in [2]. They use two checkers and rather complicate error-masking interface containing flip-flops.

In the paper [3] is suggested a fault-tolerant combinational or sequential circuit design also based on two self-checking circuits. It includes two self-checking circuits, one self-testing checker and rather simpler error-masking interface than one in [2]. Such survivable scheme [4] preserves the correct behavior of a synchronous sequential (combinational) circuit for any permissible transient or intermittent fault.

In this paper we have proposed a fault-tolerant scheme based on totally self-checking system with low overhead comparison with architectures suggested in [2] and [3]. In difference from these schemes ours has only one self-checking module and another one is simplex module (combinational circuit). Such scheme implements the correct behavior of a combinational circuit when any permissible transient or intermittent fault occurs. The analysis of the reliability of proposed scheme is given.

This paper is structured as follows. In Section 2 basic definitions are introduced. Description of the fault-tolerant scheme are presented in Section 3. Section 4 gives the analysis of the fault-tolerant properties for suggested scheme. Comparison of reliability of different approaches is shown in Section 5. Finally, conclusions are drawn in Section 6.

2. Basic definitions

Let the fault-free function of a system F be denoted as $F(x, \varnothing)$ for an input x. Let X and Y be the set of input and output code words, respectively. Let V be a predefined fault set.

Definition 1. F is self-testing with respect to V if and only if, for $\forall v \in V$, there is at least one input code word during which v is detected.

Definition 2. F is fault-secure with respect to V if and only if $\forall x \in X$, $\forall v \in V$, $F(x, v) = F(x, \varnothing)$ or $F(x, v) \notin Y$.

Definition 3. F is code-disjoint if and only if $\forall x_1 \in X$, $F(x_1, \varnothing) \in Y$, and $\forall x_2 \notin X$, $F(x_2, \varnothing) \notin Y$.

Definition 4. F is totally self-checking (TSC) if it is self-testing and fault-secure.

Definition 5. F is a TSC checker if it is self-testing, fault-secure and code-disjoint.

Hypothesis 1.

1) Faults occur one at a time;

2) a next fault from V can appear only after a forgoing fault (both transient and intermittent) has disappeared.

*The reported study was partially supported by Russian Science Foundation, research project № 14-19-00218.
Participation in EWDTS2015 is partially supported within the "Program of increase of the international competitiveness of Tomsk State University for 2013-2020".

 978-1-4673-7776-8/15/$31.00 ©2015 IEEE

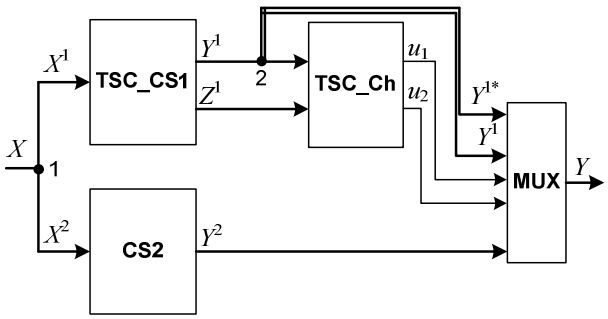


Figure 1. A fault-tolerant scheme based on self-checking circuit.

3. A fault-tolerant architecture based on self-checking circuit

We propose to implement a fault-tolerant system using the scheme shown in Fig. 1.

Here TSC_CS1 is totally self-checking circuit, for its realization we suggest to use one of the well-known techniques, for instance TSC circuits with parity checking [5, 6] or unidirectional error detection circuits [7, 8]. $X^1 = (x_1^1, x_2^1, ..., x_n^1)$ - inputs of TSC_CS1, $Y^1 = (y_1^1, y_2^1, ..., y_m^1)$ - primary outputs of TSC_CS1, $Z^1 = (y_{m+1}^1, y_{m+2}^1, ..., y_{m+s}^1)$ - additional outputs of TSC_CS1 providing a special code.

CS2 – combinational circuit realizing main functionality of the system. We suggest to use any low cost realization. For increasing reliability properties of the system it is possible using different synthesis methods for TSC_CS1 and CS2 (for example, TSC_CS1 uses OR-NOT gates, CS2 uses AND-NOT gates). Such approach to decrease a probability of appearing identical faults [9]. $X^2 = (x_1^2, x_2^2, ..., x_n^2)$ - inputs of CS2, $Y^2 = (y_1^2, y_2^2, ..., y_m^2)$ - primary outputs of CS2.

TSC_Ch – totally self-checking checker [10-12]. TSC checker detects erroneous code words on outputs of TSC_CS1 $(Y^1, Z^1) = (y_1^1, y_2^1, ..., y_m^1, y_{m+1}^1, y_{m+2}^1, ..., y_{m+s}^1)$. The checker has two outputs $U = (u_1, u_2)$ given in double-rail form, i.e., "01" or "10" if error-free, and "00" and "11" if an error is detected.

MUX – a multiplexor with inputs u_1, u_2, Y^2, Y^1 and Y^{1*}. On additional lines from branch point 2 to corresponding inputs of multiplexor (Y^1, Y^{1*}) the double-rail code is realized. The multiplexor connects outputs of TSC_CS1 $Y^1 = (y_1^1, y_2^1, ..., y_m^1)$ with primary outputs of fault-tolerant circuit $Y = (y_1, y_2, ..., y_m)$ when (u_1, u_2) take either (01) or (10) values and values $(y_1^1, y_2^1, ..., y_m^1) = (\overline{y}_1^{1*}, \overline{y}_2^{1*}, ..., \overline{y}_m^{1*})$. Otherwise the multiplexor connects outputs of CS2 $(y_1^2, y_2^2, ..., y_m^2)$ with outputs $(y_1, y_2, ..., y_m)$. Describe a multiplexer behavior for one data line *i* (Table 1).

Table 1. A multiplexer behavior for one data line *i*.

u_1	u_2	y_i^1	y_i^{1*}	y_i^2	y_i
0	1	0	0	--	y_i^2
0	1	1	1	--	y_i^2
0	1	1	0	--	1
0	1	0	1	--	0
1	0	0	0	--	y_i^2
1	0	1	1	--	y_i^2
1	0	1	0	--	1
1	0	0	1	--	0
0	0	--	--	--	y_i^2
1	1	--	--	--	y_i^2

4. Fault-tolerant property analysis

We consider any transient or intermittent faults from permissible set which don't contradict Hypothesis 1, i.e. faults occur one at a time and a next fault from permissible set can appear only after a forgoing fault has disappeared.

Notice as V_{cs1} a set of permissible faults of TSC_CS1 and single stuck-at faults on input lines from branch point 1 to inputs X_1 of TSC_CS1. In the presence of any fault from V_{cs1} the circuit TSC_CS1 may produce non-code word at the output (by totally self-checking properties) that will be detected by checker and multiplexer will use erroneous free output from CS2.

Let V_{Ch} be a set of permissible faults of a checker and single stuck-at faults on input lines from outputs of TSC_CS1 (Y^1, Z^1) to inputs of TSC_CS1. In the presence of any fault from V_{Ch} the checker will produce error indicator signals ("00", "11") at the

output (by totally self-checking properties) that drives multiplexer use erroneous free output from CS2.

Let V_{CS2} be a set of arbitrary faults of the circuit CS2 and single stuck-at faults on input lines from branch point 1 to inputs X^2 of CS2 and single stuck-at faults on output lines from outputs Y^2 to inputs of a multiplexor. In this case other parts of system are fault-free (by Hypothesis 1) and multiplexor uses erroneous free outputs from TSC_CS2.

Let V_{point2} be a set of single stuck-at faults on internal lines from branch point 2 to inputs of a multiplexor (Y^1, Y^{1*}). When the fault from V_{point2} appears the multiplexor connects fault-free outputs of CS2 $(y_1^2, y_2^2, ..., y_m^2)$ with outputs $(y_1, y_2, ..., y_m)$.

Let V_{MUX} be a set of permissible faults of the multiplexer. These faults can change connection of some lines from a set Y^1 for corresponding lines from a set Y^2.

Faults on primary inputs (x_1, x_2,…,x_n) and primary outputs $(y_1, y_2, ..., y_m)$ are not considered.

Notice $V = V_{CS1} \cup V_{Ch} \cup V_{CS2} \cup V_{point2} \cup V_{MUX}$.

Theorem 1. Any fault from V under Hypothesis 1 preserves the combinational circuit behavior.

5. System reliability evaluation

Let us discuss the reliability of the TMR scheme and the self-checking-based fault-tolerant systems one of them suggested us another one from [2].

Let us assume that TMR voter mechanism has a reliability R for a given mission time. Supposing that the simplex module is T times more complex than the voter, then the reliability of every module $R_{module} = R^T$. The behavior of the system degrades if either the voter fails, or at least two copies fail, then the reliability of TMR system is:

$$R_{TMR} = (3 \cdot R^{2T} - 2 \cdot R^{3T}) \cdot R. \quad (1)$$

As was assumed in [2] the interface for fault tolerance and the voter have the same reliability R. It was also assumed than the simplex module is T times more complex than the interface for fault tolerance and the corresponding self-checking module is δ times more complex than its simplex counterpart. The reliability of every self-checking module is defined as $R^{\delta T}$. The behavior of the whole self-checking system degrades either if the interface for fault tolerance fails or if two copies fail, then the self-checking system reliability is:

$$R_{SC1} = (2 \cdot R^{\delta T} - R^{2\delta T}) \cdot R. \quad (2)$$

In order to compute the reliability of our fault-tolerant system, let us use the same assumptions as in [2]. The behavior of the whole self-checking system degrades either if the interface for fault tolerance (MUX) fails or if the self-checking system (TSC_CS1+TSC_Ch) and the combinational circuit (CS2) fail, then the self-checking system reliability is:

$$R_{SC2} = (R^T + R^{\delta T} - R^{(\delta+1)T}) \cdot R. \quad (3)$$

In [13] shown that when transforming a complex circuit into a self-checking one a silicon surface overhead can be obtained in the range 10-84 percent. For comparing our approach with others in Fig. 2 the reliability for the simplex module (R module), the TMR (R tmr), the self-checking system from [2] (R sc1) and our self-checking system (R sc2) are plotted for R = 0.99, for δ ranging from 1.2 to 1.6 and for different module complexities T ($10 \le T \le 150$).

The diagrams show that the reliability of ours self-checking system is higher comparison with others. If δ = 1.8 the reliability of self-checking system from [2] is almost identical the TMR reliability.

6. Conclusion

The fault-tolerant scheme with low overhead based on a totally self-checking system is suggested. The scheme has only one self-checking module and another one is simplex module (combinational circuit). Such scheme implements the correct behavior of a combinational circuit when any permissible transient or intermittent fault occurs. The analysis of the reliability of proposed scheme shows that the reliability of our self-checking system is higher comparison with others.

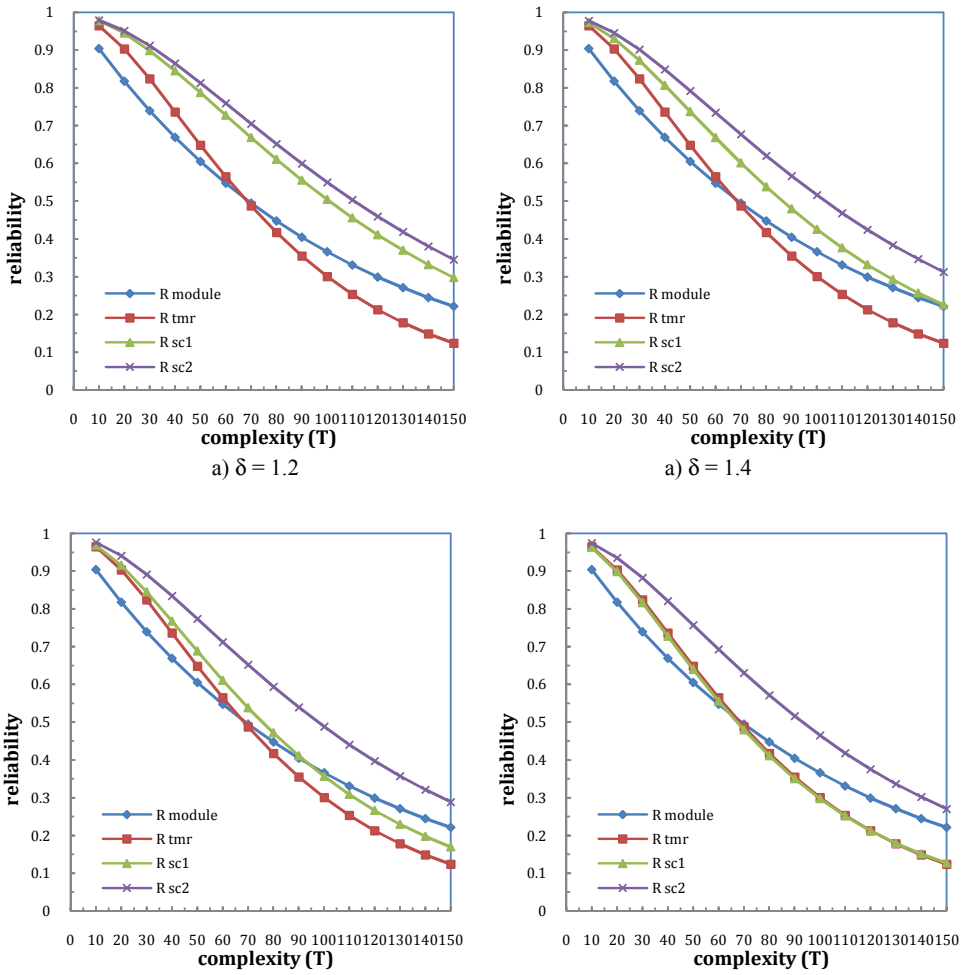
References

[1] J. Von Neumann, "Probabilistic logics and the synthesis of reliable from unreliable components", *Automata Studies*, Princeton Univ. Press, Princeton, NJ, 1958, pp. 43-98.

[2] M. Lubaszewski, B. Courtois, "A reliable fail-safe system", *IEEE Tran. On Comp.*, vol. 47, №2, 1998, pp. 236-241.

[3] A. Matrosova, V. Andreeva, Yu. Sedov, "Survivable discrete circuits design*", Proc. Of the 8 IEEE Int. On-Line Testing Workshop (IOLTW'02)*, Bendor, France, 2002, pp. 13-17.

[4] I. Levin, A. Matrosova, and S. Ostanin, "Survivable Self-checking Sequential Circuits", *Proc. of the IEEE Int. Symp. DFT'01*, San Francisco, USA, October 2001, pp. 395-402.



a) δ = 1.2 a) δ = 1.4

a) δ = 1.6 a) δ = 1.8

Figure 2. Reliability comparison

[5] F.F. Sellers Jr., M. Hsiao, L.W. Bearnson, "Error Detecting Logic for Digital Computers", *McGraw-Hill*, 1968.

[6] Vl.V. Saposhnikov, A. Dmitriev, M. Goessel, V.V. Saposhnikov, "Self-dual parity checking-A new method for on-line testing", *Proc. of IEEE 14th VLSI Test Symposium*, Princeton, NJ, 1996, pp. 162-168.

[7] F.Y. Busaba, P.K. Lala, "Self-Checking Combinational Circuit Design for Single and Unidirectional Multibit Errors", *JETTA*, №5, 1994, pp. 19-28.

[8] A. Yu. Matrosova, S.A. Ostanin, "Self-Checking Synchronous FSM network Design", *Proc. of the IEEE Int. On-Line Testing Workshop*, Capri, Italy, 1998, pp. 162-166.

[9] S. Mitra, N.R. Saxena and E.J. McCluskey, "A Design Diversity Metric and Analysis of Redundant Systems", *IEEE Trans. Computers*, Vol. 51, Issue 5, 2002, pp. 498-510.

[10] V.V. Dimakopoulos, G. Sourtziotis, A. Paschalis, D. Nikolos, "On TSC Checkers for m-out-of-n Codes", *IEEE Trans. Computers*, vol.44, issue 8, 1995, pp. 1055-1059.

[11] S.J. Piestrak, "Design of Self-Testing Checkers for Unidirectional Error Detecting Codes", *Scientific Papers of the Inst. of Techn. Cybern. of the Wroclaw Univ. of Technology*, vol. 92, №24, 1995, pp. 1-112.

[12] N. Butorina, "Self-Testing Checker Design for Incomplete m-out-of-n Codes", *Proc. of the IEEE East-West Design & Test Symposium (EWDTS)*, Kiev, Ukraine, 2014, pp. 1-4.

[13] M. Nicolaidis, "Efficient implementations of self-checking adders and ALUs", Proc. 23rd Int'l Symp. Fault-Tolerant Computing, Toulouse, France, 1993, pp. 586-595.