Checkability of the Digital Components in Safety-Critical Systems: Problems and Solutions

A. Drozd [1], V. Kharchenko [2,3], S. Antoshchuk [1], J. Sulima [1], M. Drozd [1],
[1]*Odessa National Technical University*
[2]*National Aerospace University named after N.E. Zhukovsky "KhAI"*
[3]*Centre for Safety Infrastructure-Oriented Research and Analysis, RPC "Radiy"*
[1]*drozd@ukr.net* [2,3]*V.Kharchenko@khai.edu,*
[1]*svetlana_onpu@mail.ru,* [1]*mr_lemur@mail.ru*

Abstract

Particularities of on-line testing for digital components in safety-critical Instrumentation and Control systems (I&CS) are analyzed. A problem of on-line testing associated with insufficient checkability of the digital components in safety-critical I&CS (reactor trip system) is considered. A method of checkability estimation is offered. An example of comparator checkability assessment is shown. An approach to increase checkability of the digital components is proposed.

1. Introduction

Design of safety-critical I&CS is based on a component approach which constitutes the use of components developed formerly and commonly employed in commercial and critical applications, including the components of one's own design [1, 2].

One of the most important problems is the ensuring and maintaining the functional safety of digital components and I&CS as a whole, which is solved by use development of the fault-tolerant structures [3].

The fault-tolerant systems are developed basing on a set of approaches, such as use of correction codes, majority structures, various kinds of redundancy and reconfiguration, and multi-version technologies [4, 5].

Requirements to operative detection and toleration of the faults in safety-critical I&CS determines the important role of the methods and means of on-line testing in maintenance of fault tolerance [6].

It is necessary to note, that fault tolerance is not end in itself, and only means to increase trustworthiness of calculated results and formed signals. These means basically are directed against the errors caused by many time repeated transient faults and rare failures.

On-line testing also is directed on maintenance of trustworthiness of results, carrying out its checking during performance of the main operations on operating sequences of the input data [7].

Opportunities of on-line testing essentially depend not only on an analyzed digital component, but also on operating sequence of input words which influences on checkability of points of the digital circuit.

Particularities of safety-critical I&CS impose restrictions on formation of input operating sequence for digital components, reducing checkability of the digital circuit (and available input points). It causes a problem of the limited opportunities of on-line testing in safety-critical I&CS [8].

In this paper we propose approach to assessment and increasing of component checkability for I&CS.

Structure of the paper is the following. Particularities of safety-critical I&CS are considered in section 2 in context of checkability. Section 3 is dedicated to the problem of the checking trustworthiness of results by the methods of on-line testing. Definitions of checkability and conditions of its maintenance in safety-critical I&CS are considered in section 4. The approach to increase checkability of digital components is offered and the example of checkability-oriented designing of the comparator is shown in section 5. Last section 6 concludes discussion.

2. Particularities of safety-critical I&CS

The safety-critical I&CS can be related to two kinds:

- I&CS like Reactor-Trip Systems (RTS) for Nuclear Power Plants (NPPs);
- I&CS like Reactor Power Control and Limitation System (RPCLS) for NPPs or other specialized computing systems [1, 9, 10].

Block diagrams of these kinds of safety-critical I&CS are shown in Figure 1 a and b, accordingly.

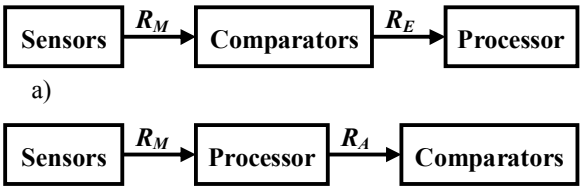


Figure 1: Kinds of safety-critical I&CS

Both block diagrams contain sensors, comparators and processor. The sensors form the results of measurements, giving out them as binary codes.

In first block diagram the results of measurements move on inputs of comparators, which compare them to threshold values. The results of comparison accepting values "Yes" or "No" (Is the threshold exceeded or not?), are the exact data. The processor obtains exact data from comparators and calculates the exact results.

In second block diagram the results of measurements being the approximate data, move on inputs of the processor, which on them calculates the approximated results. These results are compared on comparators to threshold values.

Thus processors in the first and second block diagrams differ by kind of operated data: exact and approximate ones accordingly.

To the particularities describing all safety-critical I&CS, it is necessary to relate, first of all, two basic operating modes: normal and emergency.

For most of operating time, the safety-critical I&CS runs in the normal mode. The emergency one, for which the safety-critical I&CS is designed, is a rare event as a rule and at best way never occur.

Both in the normal and emergency modes, the safety-critical I&CS and its components operate with different sets of input data.

For example, sensors of reactors in a normal mode form poorly varying levels of signals, which after numbering become a binary constant or the binary code varying in small limits. In emergency mode the level of signals changes, and components of the safety-critical I&CS operate on the other set of the input data.

Similarly, sensors of other systems form noise level and a useful signal in normal and emergency modes accordingly. On noise level the processor basically operates with low bits of the data, and the high bits are included in processing at a useful signal, i.e. in emergency operation.

The limited change of the input data creates a problem of low digital components checkability, which leads to accumulation of the latent constant faults in a normal mode. These faults can break functionality of digital components of safety-critical I&CS in emergency mode.

3. Problem of the checking the trustworthiness of results in safety-critical I&CS

Trustworthiness of results calculated in the safety-critical I&CS it is necessary to provide in emergency mode, using for this purpose opportunities of a normal mode. It is possible to assume that the normal mode proceeds so for a long time, that there can be transient faults (errors) and permanent faults (failures). In fault-tolerant system the influence of transient faults and single permanent faults on trustworthiness of results is excluded under condition of detection and elimination of one permanent fault before occurrence of the following one. Emergency mode, as a rule, proceeds not for long and can be accompanied by natural transient faults, and also the permanent faults caused by an emergency. The fault-tolerant system should be developed taking into account expected rate of such permanent faults, excepting inheritance of permanent faults from a normal mode.

Thus, for calculation of trustworthy results in both normal and emergency modes it is necessary:

- to provide the checking of trustworthiness of the erroneous results;
- to exclude accumulation of the latent faults in a normal mode.

This problem is defined for on-line testing of the digital components of the safety-critical I&CS in view of calculation of the exact and approximated results.

The basic development of on-line testing proceeded within the framework of the theory of self-checked circuits for processing the exact data [11, 12]. The exact data contain only integers by the nature, i.e. numbers of elements of sets. Such numbered data are used in definitions of fault-secure, self-testing and totally self-checking circuits as code words. According to these definitions, the purpose of on-line testing is the estimation of serviceability of the digital circuit by detection of its faults from the given set. On-line testing methods should satisfy to the requirement of fault detection by the first error. For the exact data the declared purpose of on-line testing coincides with the actual purpose to check trustworthiness of results as the detected error concurrently shows that he circuit contains a fault and calculated result is non-trustworthy. It follows from identity of erroneous and trustworthy result in case of the exact data.

An approximate result has exact most significant bits (MSB) and non-exact least significant bits (LSB).

The error produced by a fault of the computing circuit considered in MSB and LSB as essential or inessential for trustworthiness of the result, accordingly.

Trustworthiness of erroneous result is estimated as $D = 1 - P_E$ where P_E is probability of an essential error, i.e. probability of that the having place error is essential.

Trustworthiness of the erroneous result checking is estimated by the following formula [13]:

$$D_C = P_E P_D + (1 - P_E)(1 - P_D), \quad (1)$$

where P_D is an error detection probability.

According to (1), use of totally self-checking circuits, providing probability $P_D = 1$ for given set of faults, determines trustworthiness of the erroneous result checking as $D_C = P_E$.

Probability P_E characterizes object of on-line testing. In case of the exact data probability $P_E = 1$ and accordingly $D_C = 1$. Thus, on-line testing of the digital components calculating exact results can be carried out with high trustworthiness D_C by designing the totally self-checking circuits.

The approximate data, as a rule, are represented and processed in floating point formats with use of operation of multiplication in the record of number. Therefore multiplication is present at all operations with mantissas [14]. The result of two-operand complete operation with mantissas has the double word size. According to the error theory, the approximated result contains MSB no more, than in an operand. The low half of complete operation result contains non-exact LSB which, as a rule, are rejected, twice reducing probability P_E. Only the truncated arithmetic operations with mantissas reduce probability P_E to a lesser degree. However denormalization and normalization of mantissas additionally reduce the probability P_E in results of all previous and following operations accordingly.

Thus the use of the totally self-checking circuits for on-line testing of the digital components, calculating the approximated results of complete operations, determines low trustworthiness $D_C = P_E < 0{,}5$.

To increase the trustworthiness D_C of the on-line testing methods, following three ways can be used:

- an increase of the probability P_E;
- a decrease of the probability P_D;
- the detection of the essential and unessential errors with different probabilities P_{De} and P_{Dn}, where $P_{De} > P_{De}$.

The first way is realized for the truncated arithmetic operations with the high probability P_E using the residue checking methods with the high probability P_D [15].

The second way can be executed in case of keeping a given set of detected faults [16, 17]:

- using natural information redundancy of the arithmetic operations results;
- checking the approximated result by simplified operation on a limited set of input words.

The third way is used in on-line testing methods, which estimate value of result and its error, as the following methods [18 – 20]:

- logarithm checking;
- checking by inequalities;
- checking by segments.

For counteraction for accumulation of the latent fault it is necessary to consider checkability of digital components in the safety-critical I&CS.

4. Checkability of digital components and a condition of its maintenance in the safety-critical I&CS

Checkability of the digital component in safety-critical I&CS can be estimated using checkability of the separated points of a digital circuit component in both normal and emergency modes.

Description of the digital circuit should illustrate its embodiment by means of the specific elements. For instance, the description of the digital circuit embodied on FPGA with use of logic cells LE ALTERA should contain the list of points of two types:

- internal points, i.e. bits of memory LUT;
- external points which include all other points like bits of LUT address or its output.

The digital circuit points to which the error detection circuit is connected are referred to as the *check points*. The set of check points includes all output points of the result.

Definition 1. The digital circuit point is referred to as the *checkable* one if any error caused in this point by a fault belonging to the set F can be detected by the checking circuit on the assigned limited set of input words. Otherwise, this point is referred to as the *non-checkable*.

Checkability of the points can be considered in terms of controllability and observability for the set F of the single constant faults stuck-at '0' and '1'.

Definition 2. An internal point of the digital circuit is *a controllable* one if the limited set of input words contains at least one word, on which this point is chosen in its LUT i.e. the address of this point appears on the inputs of LUT. Otherwise, the internal point is a non-controllable one.

Definition 3. An external point of the digital circuit is *a partially controllable* one (0-*controllable* point or 1-*controllable* point) if this point takes only a value '0' or only a value '1' on the limited set of input words. Otherwise, the external point is *a controllable* one.

Definition 4. A point of the digital circuit is *a partially observable* one (0-*observable* point or 1-

observable point) if a path from this point up to a check point is activated on the limited set of input words only for one value '0' or '1'. In case the path is activated for both values '0' and '1' the point is *observable* one. Otherwise the point is a non-observable one. The path is activated if a change of value of the given point is transferred to a check point.

Statement 1. The point is a *checkable* one if it is controllable and observable on the same input words belonging to the limited set of ones. Otherwise, the point is *a non-checkable* one.

Indeed, the *checkable* point when being controllable while correct operation of the circuit on the set of input words can take any error value caused by the fault of the set *F*. Besides, the circuit can transfer to the check point the change caused by the error in the given point as soon this point is observable. Thus, the error in the point, which is controllable and observable on the same input words, is detected by the checking circuit on the limited set of input words.

Statement 2. The observable internal point is also a controllable and, hence, a *checkable* one.

Indeed, to activate the path from the internal point it has to be chosen by feeding a corresponding address to the input of LUT. Then this point, according to definition 3, is a controllable and, according to the statement 1, a *checkable* one.

Statement 3. For the assigned input word the result is determined only by the values of points of the circuit, which are observable ones.

Indeed, if the point is unobservable on the assigned input word then a change of its value does not reach the checkpoints, and, therefore, do not render any influence upon the result which is read out from the checkpoints.

We offer a method of checkability estimation based on analysis of controllability and observability of the digital component points in both normal end emergency modes.

Availability of a digital component to calculate the trustworthy results becomes non-checkable under coincidence of two events [21]:

- possibility of the latent fault occurrence in the normal mode;
- possibility of this fault appearance in the emergency mode.

Statement 4. In the normal mode, the latent stuck-at fault can appear in two cases:

- if the point is a non-controllable one and a value in it coincides with a value defined by the stuck-at fault;
- if the point is a non-observable one.

Indeed, in the first case the non-controllable point takes constant value, which in due course can become a value of the stuck-at fault. In the second case any changes of a point value including that under influence of fault are not observed in any way in the checkpoints of the circuit, i.e. hidden from the on-line testing.

Statement 5. In the emergency mode the stuck-at fault also appears in two cases:

- if the point is an observable and non-controllable and its value as a value of the non-controllable point is distinct from the value defined by the stuck-at fault;
- if the point is a checkable one.

Indeed, in the first case the stuck-at fault changes the value of the non-controllable point, which is observed in the check points of the circuit and, according to the statement 3, may distort the result. In the second case, the stuck-at fault will appear at the change of the point value as soon as it is a controllable one. This change will be transferred to the check, points while taking into account that this point is an observable one.

Controllability C can equal 3 values: 0, 1, 2 or 1, 2, 3 for an internal and external point, accordingly. Values 0, 1, 2 and 3 distinguish cases of non-controlled, 1-controlled, 0-controlled and controlled point, accordingly.

Observability O of an external point can equal 4 values: 0, 1, 2 and 3 in cases of non-observable, 1-observable, 0-observable and observable point, accordingly. Observability of an internal point can accept only values 0, 1 and 2.

Controllability and observability of a point can accept various values: C_N and O_N in a normal mode and also C_E and O_E in emergency mode, accordingly.

The latent fault can be saved up in a normal mode and deform value of an external point in emergency mode in three cases:

- $C_N + C_E = 3$;
- $O_N + C_E = 3$;
- $O_N = 0$.

Such distortion transports an error in result in case $O_E > 0$.

Thus, the external point is dangerous to an emergency mode under the following condition:

$$((C_N + C_E = 3) \text{ or } (O_N + C_E = 3) \text{ or } (O_N = 0)) \text{ and } (O_E > 0).$$

The latent fault can be saved up in a normal mode and can deform result in emergency mode if the internal point is not observable and observable in normal and emergency modes, accordingly. Thus, the internal point is dangerous to an emergency mode under the following condition:

$$(O_N = 0)) \text{ and } (O_E > 0).$$

Checkability of a digital component can be evaluated by the following formula:

$$K = 1 - N_E / N_T,$$

where N_E is amount of dangerous points;

N_T is total of the circuit points.

5. Increase in checkability of digital components in the safety-critical I&CS

The analysis of a problem shows, that checkability of digital circuit points is reduced with restriction of a set of input data, represented and processed in parallel codes.

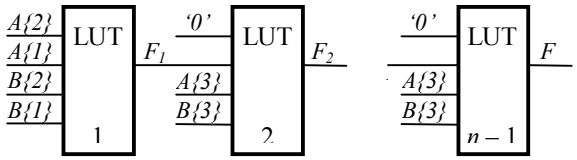
To solve this problem the transition from traditionally developed processing parallel codes to data processing in a serial code is offered.

In a serial code only constants from all "0" or from all "1" can hide constant permanent fault. The same constants arise in case the fault is in a circuit point through which the serial code follows. Therefore such constants are expedient for excluding from use and to relate to the forbidden codes.

Formation of result during several steps allows to code also it so that its serial code accepted both values '0' and '1'.

As an example, we may consider the comparator which compares the code $A = A\{n\} \ldots A\{2\}\, A\{1\}_2$ with a threshold $B = B\{n\} \ldots B\{2\}\, B\{1\}_2$ and calculates a result $F = 0$ if $A < B$, and $F = 1$ otherwise, where $n = 3 \ldots 16$.

In case of processing of parallel codes the comparator is built using $n - 1$ LUT in the circuit shown in Figure 2.



LUT 1

A{2} \ B{2} B{1}	11	10	01	00
00	0	0	0	1
01	0	0	1	1
10	o	1	1	1
11	1	1	1	1

LUT 2 .. n – 1

'0' \ A{3} B{3}	11	10	01	00
00	0	1	0	0
01	1	1	0	1
10	0	1	0	0
11	1	1	0	1

Figure 2: Comparator for parallel code processing

In the normal mode the code A takes A^*+1 values: $A = 0 \ldots A^*$. The threshold B takes the same value in both modes. In the emergency mode $A = B$.

The example is considered for various values $A^* = 0 \ldots B - 1$ and $B = 1 \ldots 2^{n-1}$. The output F is the check point. The comparator contains $3n - 1$ external and $16(n - 1)$ external points.

The results of simulation shows that checkability K of the comparator is reduced with growing of n from 38% up to 34% for external points, for internal points $K = 94\%$.

In case of processing of serial codes the comparator is built using two LUT 1, 2 and two flip-flops 3, 4 in the circuit shown in Figure 3 (for $n = 9 \ldots 16$).

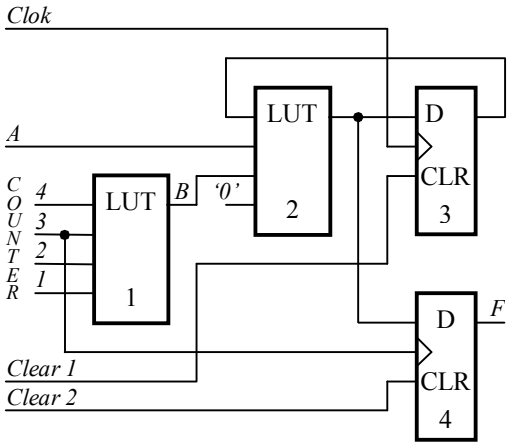


Figure 3: Comparator for serial code processing

The threshold B is stored in LUT 1 and is read under control of the counter. The difference of the serial code A and B is calculated in two's complement code using the LUT 2 and flip-flop 3. The signs of the differences of all and of the first 8 low bits of the compared codes A and B are stored in flip-flop 4 under control of the inverse value of the counter third bit. The output of the flip-flop 4 takes the value F at the first 8 clock units in a time interval of comparison. The following $n - 8$ clock units the output of the flip-flop 4 takes the value of sign which can be not equal to F. The comparator contains 11 external and 32 external points.

The results of simulation show increasing of comparator checkability K up to 96% for external points and 100% for internal points.

Serial processing of the data is carried out more slowly parallel processing. It can be not critical for the safety-critical I&CS of the reactor of nuclear station. Otherwise the methods of decrease in time of serial processing of data can be applied, such as follows:

- overlapping processes of reception, processing and delivery of the data;
- series-parallel performance of operations;
- parallel-serial performance of operations.

Conclusion

This paper particularities of on-line testing application were analyzed for the digital components of safety-critical I&CS.

As the digital components are designed to operate in normal and emergency modes it causes a problem of ineffective checkability of the digital circuits associated with the limited sets of input words in these modes. Offered method of checkability estimation shows it on example of the parallel comparator. The second reason of low checkability is connected with modern technology of data processing based on use of the parallel codes of numbers.

We offer an approach to increase checkability of the digital components by using of processing the serial codes. Considered example shows significant increase of checkability in the comparator designed for operation with the serial codes.

The directions for further research include development of the serial-operating digital components with high checkability and increase of their productivity without essential lowering of checkability.

References

[1] M.A. Yastrebenetsky (edit.) *NPP I&Cs: Problems of Safety*, Ukraine, Kyiv: Technika, 2004. – 472 p. (translated in USA by NPC, 2007)

[2] V.S. Kharchenko, V.V. Sklyar (edits). *FPGA-based NPP I&C Systems: Development and Safety Assessment*, RPC Radiy, National Aerospace University "KhAI", SSTC on Nuclear and Radiation Safety, 2008. – 188 p.

[3] A.A. Siora. V.A. Krasnobaev, V.S. Kharchenko. *Fault Tolerant Systems with Version-Information Redundancy* // National Aerospace University "KhAI, 2009. – 321 p.

[4] A. Drozd, M. Lobachev. *Multi-version computer systems with use of strongly connected versions* // in Monographs of System Dependability. Dependability of Networks. – Wroclaw (Poland) – 2010. – P. 39 – 51.

[5] V. Kharchenko. *Multy-version Systems: Models, Reliability, Design Technologies* // 10th European Conference on Safety and Reliability. – Munich (Germany). – 1999, V. 1. – P. 73 – 77.

[6] M. Nicolaidis, Y. Zorian. *On-Line Testing for VLSI – a Compendium of Approaches* // Electronic Testing: Theory and Application (JETTA). – 1998. – V. 12. – P. 7 – 20.

[7] A. Drozd, S. Antoshchuk, A. Rucinski, J. Drozd. *Increase in reliability of the on-line testing methods using features of approximate data processing* // 1th International Conference on Waterside Security. – Copenhagen (Denmark). – 2008. – P. 137 – 140.

[8] A. Drozd, V. Kharchenko, A. Siora, V. Sklyar. *Component-based safety-oriented on-line testing of digital systems // IEEE East-West Design & Test Symposium*. – Sankt-Petersburg, Russia. – 2010. – P.135 – 140 .

[9] www.globalsecurity.org/wmd/world/russia/pill_box.htm

[10] www.popmech.ru/article/4954-vosmoe-chudo-sveta

[11] W. Carter, P. Schneider. *Design of Dynamically Checked Computers* // Proc. IFIP Congress 68. – Edinburgh (Scotland). – 1968. – P. 878 – 883.

[12] C. Metra , L. Schiano, M. Favalli, B. Ricco. Self-*Checking Scheme for the on-Line Testing of Power Supply Noise* // Proc. Design, Automation and Test in Europe Conf. Paris (France). – 2002. – P. 832 – 836.

[13] A. Drozd, M. Lobachev, J. Drozd. *The problem of on-line testing methods in approximate data processing // 12th IEEE International On-Line Testing Symposium*). – Como (Italy). – 2006). – 251-256.

[14] ANSI/IEEE Std 754-1985. IEEE Standard for Binary Floating-Point Arithmetic. IEEE, New York, USA, 1985.

[15] A.V. Drozd, M.V. Lobachev. *Efficient On-line Testing Method for Floating-Point Adder* // Proc.. Design, Automation and Test in Europe. Conference and Exhibition 2001 (DATE 2001). – Munich (Germany). – 2001. – P. 307 – 311.

[16] A.V. Drozd. *Efficient Method of Failure Detection in Iterative Array Multiplier* // Proc. Design, Automation and Test in Europe. Conference and Exhibition 2000 (DATE 2000). – Paris (France). – 2000. – P. 764.

[17] M. Said, M. Lobachev, O. Drozd. *A New On-Line Testing Method to Increase the Reliability of Checking Approximated Results* // 4-th international Conference "Advanced Computer Systems and Networks: Design and Application". – Lviv (Ukraine). – 2009. – P. 166 – 168.

[18] A. Drozd, R. Al-Azzeh, J. Drozd, M. Lobachev. *The logarithmic checking method for on-line testing of computing circuits for processing of the approximated data* // Proc. of Euromicro Symposium on Digital System Design. – Rennes, France. – 2004. – P. 416 – 423.

[19] A. Drozd, O. Oginska. *Checking by inequalities of floating-point multiplier of mantissas* // Visnik NTUU 'KPI'. – Kiev. – 2002. – V. 38. – P. 34 – 40.

[20] A. Drozd, M. Lobachev, R. Kolahi. *Effectiveness of on-line testing methods in approximate data processing* // Proc. IEEE East-West Design & Test Conference. – Odessa (Ukraine). – 2005. – P. 62 – 65.

[21] A. Drozd, V. Kharchenko, S. Antoshchuk, M. Drozd. *On-line testing of safety-critical I&C systems in normal and emergency modes: Problems and solutions* // First International Workshop 'Critical Infrastructure Safety and Security' (CrISS-DESSERT'11). – Kirovograd (Ukraine). – 2011. – P. 139 – 147.