Safety-Related Instrumentation and Control Systems and a Problem of the Hidden Faults

M. Drozd, A. Drozd
Institute of Computer Systems
Odessa National Polytechnic University
Odessa, Ukraine
miroslav_dr@mail.ru, drozd@ukr.net

Abstract—**This paper is dedicated to a problem of the hidden faults associated with development of the computer systems in form of their transformation into safety-related instrumentation and control systems. The hidden faults do not allow ensuring functional safety by construction of fault tolerant digital component without consideration of their checkability. Increase of checkability by imitation of accident is exposed to an unacceptable risk of transition into an emergency mode. The approaches to solving the problem during operational time using the methods for improvement of checkability in a normal mode and with analysis of both normal and emergency modes are offered.**

Keywords— safety-related instrumentation and control system; normal and emergency modes; functional safety; digital component; hidden fault; checkability

I. INTRODUCTION

The objects with raised risk in power systems, transport, space and defensive areas have become an integral part of human environment. A whole number of last years emergency connected with cascade cut of power grids, stopping the power plants, derailments, air crashes, unsuccessful launching of the spaceships focuses attention on maintaining the objects with raised risk by the safety-related Instrumentation and Control Systems (I&CS). They are aimed at both forestalling transition of control object in hazardous state and minimization of threats in case of such transition [1, 2].

The high demands regulated by international standards are made to I&CS [3, 4]. One of the most important is requirement in ensuring functional safety considered like a part of the overall safety of control object I&CS including construction of the fault safe digital components (DC) based on fault tolerance achieved for their circuits by the methods and means of on-line testing with use of correcting code, various kinds of reservation and reconfiguration, majority and multi-version structures [5, 6].

However fault tolerance of DC does not solve a problem of the hidden faults. A hidden fault of the one channel of the majority DC can be repeated keeping hidden nature in other channels. The hidden faults violate ensuring functional safety of I&CS as well as they can be shown only in condition of accident breaking I&CS functionality at the most critical moment. Traditionally detection of the hidden faults is executed by testing with imitation of accident in condition of blocking preventive protection. It multiple resulted in initiation of an imitation mode by faults, for example, with imitation of the rocket attacks between opposing countries bringing the world to the brink of war [7]. Violation of the preventive protection was one of Chernobyl disaster reason [8].

Safe decision of hidden faults problem demands maximal refusal of using the imitation modes in I&CS that is possible due improvement of DC checkability shown during the main operational time.

In Section 2 a problem of hidden faults from a position of diversification of the DC checkability in I&CS is considered. Both objective and subjective reasons of inadequate checkability of DC are analyzed. In Section 3 the approaches to solving the problem of the hidden faults are examined. The methods for leveling of DC checkability in normal and emergency modes and also the methods for detection and elimination of the potentially hazardous points in the circuits of DC are offered.

II. A PROBLEM OF THE HIDDEN FAULTS

A. Definition of Problem

The safety-related I&CS are the next stage in development of computer systems like the target resources [9]. This stage is characterized by diversification of an operating mode with division of it into normal and emergency modes. These modes are essentially difference in role which they play in life-cycle of I&CS: the safety-related systems are developed for forestalling and maintenance of an emergency mode, but the main time run in a normal one. The problem of the hidden faults follows from diversification of an operating mode of I&CS. Process of diversification is extended over DC checkability which become difference in a normal and an emergency modes variously referring the faults to hidden and detectable [10].

A concept of checkability has formed in testing for estimation in complexity of test generation aimed at fault detection in pause of an operating mode. Estimation of checkability is executed for the points of a digital circuit by calculating controllability, observability and their product [11, 12]. Checkability is increased by design for testability using the

methods of scan and self-testing. These methods are supported by IEEE standards [13, 14]. However use of these methods in safety-related systems is connected with the risk of transition in an emergency mode in case of initiation of an imitation mode by the faults. It shows long-felt need to solve the problem of the hidden faults in an operating mode by the methods and means of on-line testing for detection of all faults which reduce functional safety of I&CS.

First of all checkability is important for I&CS from a position of maintaining fault tolerance of their DC in an emergency mode. Diversification determines checkability like both functional and dual-mode forming essential dependence not only from structure of a circuit but also from particularities of input data in normal and emergency modes [15, 16].

B. Reasons of Inadequate Dual-Mode Checkability

In order to define the ways for solving the problem of the hidden faults it is necessary to consider objective and subjective reasons of inadequate dual-mode checkability of the safety-related systems.

Objective reasons are determined by the particularities of safety-related I&CS. The structure redundancy of fault tolerant DC is the first reason. Requirements to functional safety cannot be satisfied without using fault tolerant structure as well as fault tolerance cannot be achieved without structure redundancy. However structure redundancy of the digital circuits is the main factor of reducing their checkability [17, 18].

The second reason follows from design of I&CS for functioning in two modes in which DC processes different limited sets of input data. Limitation in input data increases structure redundancy of the digital circuits additionally reducing their checkability and promoting accumulation of the hidden faults during long time of I&CS work in a normal mode. The accumulated faults can be shown at the input data of an emergency mode in amount which exceeds possibilities of DC to forestall the faults breaking functional safety of I&CS and objects with raised risk.

Subject reasons amenable to eliminate are determined by particularities of I&CS construction oriented on achieving high, but not always founded rates, for example a high stability of the amplitude of signals at the output of sensors of the measured parameters. Signals are digitized with transformation into binary codes, which are changed at low noise level only in low-order bits. It occurs over a long period of time in a normal mode. In addition, unreasonably high ratio “signal / noise” is determined using DC with many thousands states to distinguish only two modes: a normal and an emergency. All these redundant solutions further reduce the checkability of digital circuits. But most of all it is limited by the processing of data in parallel codes on simultaneous devices with a large-scale parallelism, which became traditional for I&CS to ensure a high level of performance for DC.

Considered subjective reasons allow developing the methods for solving the problem of hidden faults to the limits determined by the objective reasons.

III. Approaches to Solving a Problem of the Hidden Faults

A. Definition of Approaches

Analysis of objective and subjective reasons of dual-mode checkability which is inadequate for I&CS notes its diversification and limitation in a normal mode. This leads to appearance of potentially hazardous points in the circuits of DC. Hidden faults can be accumulated in these points during a normal mode and can be active in an emergency mode, reducing the level of fault tolerance and safety of I&CS.

It defines two basic approaches to solving the problem of hidden faults:

1) to ensure maximum checkability in a normal mode of I&CS for maximum elimination of hidden faults;

2) to improve the ratio of DC checkability in normal and emergency modes from a position of eliminating the hidden faults which reduces tolerance of I&CS in accidents.

Marked objective reasons do not allow implementing the first approach to the full extent. You can only get close to the full level of checkability of the DC in a normal mode. It is shown that in on-line testing the calculations performed by the DC during the operating mode, observability coincides with checkability, and controllability is their top border. The methods for increasing the checkability in a normal mode to the top border, and methods to improve the top border have been developed [19, 20].

The first approach is implemented with diversification of the methods and means of on-line testing, adding to them one’s directly aimed at the detection of hidden faults in a normal mode. New opportunities of diversification in the methods and means of on-line testing are opened with the development of circuit engineering to the level of preparing the results [21]. Essence of these methods consists in the organization of choice not only for the current results of a normal mode, but also the results, which are typical for an emergency mode of the I&CS work with the aim of checking their validity.

The second approach requires consideration of a model of the DC, which characterizes it as an object of on-line testing from a position of the dual-mode checkability. This model must consider both normal and emergency modes of I&CS operation, i.e. to be the following:

$$M(I_N, I_E, D),$$

where I_N – the input data of the DC in a normal mode;
I_E – the input data of the DC in an emergency mode;
D – circuit description of the DC.

The second approach can be implemented using two ways:

- to make the checkability which is the same for both modes of I&CS for keeping the hidden faults of a normal mode like hidden also in an emergency mode;
- to identify potentially hazardous points of the DC circuits and eliminate those that pose a real threat to the safety of the I&CS.

B. The Methods for Realization of the First Way

The analysis of the DC model shows the possibilities of implementing the first way with encoding of the input data when the parameters I_N and I_E become identical. Examples of this encoding can be attributed to the use of the serial codes and dual-rail codes.

Traditionally, the DC is built like simultaneous for processing parallel code, justifying the use of such DC by their high performance. The result of the operation is calculated in every clock unit at the new input word. The multitude of input sequences becomes a set of words which is substantially limited in a normal mode of the DC operation. All bits of the parallel codes are simultaneously available to perform the operation. However, this does not lead to their simultaneous processing, because the significant bits of numbers are usually calculated using the low-order bits.

Iterative array multiplier with most quick circuits performs the operation for $2n - 2$ delays of full adders, i.e. $2n - 2$ full adders are series-connected [22]. Each of full adders is used only on small, $1 / (2n - 2)$ part of multiplication time. For $n = 32$ the full adders are involved only 1.6%, i.e. idle 98.4% of the execution time of operation. Iterative array multiplier contains almost n^2 full adders (10^3 full adders for $n = 32$). The usage of the elements is twice deteriorated with the transition to 64-bit platform. High percentage of idle elements is essential delimiter of checkability for points of simultaneous DC circuits.

The transition to the processing of data in sequential code allows to raise the controllability of the DC in the first approach, and to implement to the full extent the first way of the second approach, comprising I_N and I_E with the same words, which are the values of zero and one. Operation in serial code can be executed on a bit-serial pipeline. The required productivity can be achieved when many such pipelines are used in the DC. It also reduces the cost of equipment in comparison with iterative array units.

Dual-rail or multi-rail coding allows to ensure the controllability and observability for each channel of data. The use of dual-rail logic is extremely important to align dual-mode checkability of the DC working only in an emergency mode. For example, digital delay matching time stages of protections inclusion in an emergency mode refers to such of the DC. In a normal mode, this DC does not in use. Dual-rail or multi-rail encoding allows to align the checkability of digital delay in normal and emergency operation by encoding both on and off states.

C. The Methods for Realization of the Second Way

Implementation of the second way is based on the methods of detection and elimination of potentially hazardous points in the circuits of DC. A method for the detection of potentially hazardous points estimates the controllability and observability of the circuit at the input data I_N and I_E for both normal and emergency modes. The point is potentially hazardous in the conditions described by the following formula [23]:

$$((C_N + C_E = 3) \vee (O_N < O_E) \vee (O_N = 0)) \wedge (O_E > 0),$$

where C_N and C_E – controllability of a point in a normal and an emergency modes; controllability is equal to 1, 2, or 3, if the point is 1, 0, or both, respectively;
O_N and O_E – observability of a point in normal and emergency modes; observability is equal to 0, 1, 2 or 3, if the point is not broadcasting changing the value to the output of the circuit, passes, taking the value 1, 2 or both values, respectively.

Limitation of observability by controllability allows simplifying the formula to a disjunction of two conditions:

$$(C_N + C_E = 3) \wedge (O_E > 0) \ \vee \ ((O_N < 3) \wedge (O_E = 3)).$$

The first condition is executed only for one value of the constant fault ‘0’ or ‘1’. The second condition describes potentially hazardous points for both values of the hidden fault. Dual-mode checkability can be estimated by percentage of the circuit points which is not potentially hazardous taking into account execution of the first condition only for half of constant fault values. Then the dual-mode checkability is determined by the following formula:

$$C_F = 1 - (Q_{PH\,0\vee1} / 2 + Q_{PH\,0\wedge1}) / Q,$$

where $Q_{PH\,0\vee1}$ and $Q_{PH\,0\wedge1}$ – amount of potentially hazardous points identified by the first and second conditions accordingly; Q – total amount of the circuit points.

Values of the checkability C for iterative array multiplier of normalized mantissas in a normal mode and dual-mode checkability C_F received talking into account both modes are shown in Table 1.

Table 1: Checkability in a normal and both modes

S	10^2	20^2	30^2	40^2	50^2	60^2	70^2	80^2
S, %	0.6	2.4	5.5	9.8	15.3	22.0	29.9	39.1
C, %	64.5	73.3	75.3	80.2	81.2	81.7	86.6	87.1
C_F, %	87.5	93.2	93.4	93.4	93.4	93.9	99.1	100

Checkability is estimated using a program model of 8-bit multiplier for 8 various sets of input words. These sets are determined by range of operands binary codes in a normal mode from minimal value 128. The range is changed with step 10 from initial value up to 80. It determines the sets S of input words from 10^2 up to 80^2, i.e. from 0.6% to 39.1%. The threshold separating an operating mode into a normal and an emergency is setting at the level of 210. The results of simulation show that $C_F >> C$, and checkability C_F (unlike C) can be increased up to 100%.

Methods of elimination of the potentially hazardous points are aimed at violation of even one of the conditions relating these points to potentially hazardous. Such methods based on changing the controllability or observability for points of the DC circuits. Controllability can be changed in the DC circuit by the implementation of the several versions in execution of the operation. These versions can be created using self-dual logic function or various representations of binary codes which ensure a receipt of the same operation results. For example, the arithmetic operations can be performed in two’s complement

code with changing signs of operands and results: addition of numbers with a simultaneous change of signs of the summands and amount, multiplication or division with a simultaneous change of signs of the operands or one operand and the result. The change of sign in the two's complement code of odd binary numbers inverts all its bits except the lowest, which is controllable as a rule. Interleaving the versions of operation execution at input data changed in a limited range increases controllability of the DC circuit violating the first condition of a potentially hazardous point.

Values of the checkability for iterative array multiplier of mantissas in the two's complement code C, C_F and their values C^*, C_F^* improved by changing the operands signs are shown in Table 2 for the sets S from 1^2 to 8^2.

Table 2: Increase of the checkability

S	1^2	2^2	3^2	4^2	5^2	6^2	7^2	8^2
C, %	45,5	59,5	61,8	63,6	66,1	66,3	67,5	68,5
C_F, %	70,8	91,4	92,8	93,4	93,8	93,8	94,2	94,6
C^*, %	55,9	88,3	88,3	88,9	89,1	89,1	89,3	89,5
C_F^*, %	97,1	99,9	100	100	100	100	100	100

Received results show maximal efficiency of the method in increase of the checkability C_F.

IV. CONCLUSION

The problem of hidden faults associated with the transformation of the computer systems in critical-related I&CS for maintaining objects with raised risk. In these conditions, functional safety of I&CS ceases to be met only by its fault tolerance. Diversification of an operating mode leads to the diversification of checkability of the DC reducing the fault tolerance of I&CS in an emergency mode.

Two approaches are considered for solving the problem of hidden faults. The first approach aims to improve checkability in a normal mode. The second approach is implemented taking into account both modes by aligning checkability in a normal and an emergency mode or by exclusion of the potentially hazardous points in the DC circuits. The first way is implemented in the methods based on the encoding of the input data using serial or dual-rail codes. The second way involves the detection and elimination of potentially hazardous points violating the conditions which identify these points like potentially hazardous. Violation of these conditions is provided by the methods based on implementation of multiple versions of the operation in the DC circuit.

REFERENCES

[1] M. A. Yastrebenetsky, V. N. Vasilchenko, S. V. Vinogradskay e. a., *Safety of Nuclear Power Plants*: Instrumentation and Control Systems, M. A. Yastrebenetsky (Edit.), Ukraine, Kyiv: Technika, 472 p., 2004.

[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, 188 p., 2008.

[3] IEC 61508:2000. Safety of electrical, electronic and programmable systems important to safety. – Geneva: International Electrotechnical Commission, 2000.

[4] IEC 61513:2001. Nuclear power plants – Instrumentation and control systems important to safety – General requirements for systems. – Geneva: International Electrotechnical Commission, 2001.

[5] P. Kubalik, P. Fisher, H. Kubatova, "Fault tolerant system design method based on self-checking circuits," *Proc. 12th IEEE International On-Line Testing Symposium*, Como (Italy), pp. 185 – 186, 2006..

[6] V. Kharchenko, V. Sklyar, E. Bahmach, A. Siora, V. Tokarev, V. Golovir, A. Herasimenko, "*Multi-version FPGA-based NPP Instrumentation and Control Systems: Automata Models, Implementations and Operation Results*," Proceedings of IEEE East-West Design & Test Symposium (EWDTS'07), Yerevan, Armenia, Sept. 7–10, pp. 396 – 400, 2007.

[7] http://www.popmech.ru/article/2642-ballisticheskie-prizraki/

[8] http://chornobyl.ru/ru/chnpp/12-accident/28-chnpp-accident.html

[9] J. Drozd, A. Drozd, "Models, Methods and Means as Resources for Solving Challenges in Co-Design and Testing of Computer Systems and their Components," *The Ninth International Conference on Digital Technologies 2013*, Zhilina, Slovak Republic, 29 – 31 May, pp. 225 – 230, 2013.

[10] A. Drozd, V. Kharchenko, S. Antoshchuk, J. Drozd, M. Lobachev, J. Sulima, "The use of natural resources for increasing a checkability of the digital components in safety-critical systems," *Proc. IEEE East-West Design & Test Symposium*, Kharkiv, Ukraine, 14 – 17 Sept. – pp. 327 – 332, 2012.

[11] H. Goldstein, "Controllability/Observability Analysis of Digital Circuits," *IEEE Trans. on Circuits and Systems,* Vol. CAS-26, No. 9, pp. 685-693, September, 1979.

[12] P. G. Kovijanic, "Computer Aided Testability Analysis," *Proc. IEEE Automatic Test Conf.,* pp. 292 – 294, 1979.

[13] IEEE Standard 1149.1-1990. IEEE Standard Test Access Port and Boundary Scan Architecture. IEEE Standards Board, October, 44 p., 1993.

[14] IEEE Std 1500-2005 IEEE Standard Testability Method for Embedded Core-based Integrated Circuits, Volume, Issue, DOI 10.1109/IEEESTD.2005. 96465, 2005.

[15] 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, 11 – 13 May, pp. 139 – 147, 2011.

[16] A. Drozd, V. Kharchenko, S. Antoshchuk, M. Drozd, "Checkability of safety-critical I&C system components in normal and emergency modes," *Journal of Information, Control and Management Systems*, Vol. 10, No. 1, pp. 56 – 63,. 2012.

[17] I. M. Ratiu, A. Sangiovanni-Vincentelli, and D. O. Peterson, "VICTOR: A Fast VLSI Testability Analysis Program," *Proc. Intn'l Test Conf.,* pp. 397-401, November, 1982.

[18] N. S. Shcherbakov, *Reliability of digital devices operation*, Moskow: Mashinostroenie, 224 p., 1989.

[19] J. V. Drozd, O. V. Drozd, J. J. Sulima, "Features of Development of the Models and Methods in Co-Design and Testing of Computer Systems and their Components," *6-th International Conference "Advanced Computer Systems and Networks: Design and Application"*, Lviv, Ukraine, 16 – 18 Sept., pp. 29 – 31, 2013.

[20] A. Drozd, V. Kharchenko, S. Antoshchuk, J. Sulima, M. Drozd, "Checkability of the digital components in safety-critical systems: problems and solutions," *Proc. IEEE East-West Design & Test Symposium*, Sevastopol, Ukraine, 9 – 12 Sept., pp. 411 – 416, 2011.

[21] A. V. Drozd, M. V. Lobachev, J. V. Drozd, *Dedicated Architectures of Computers*, Learning aid, Odessa: Science and technique, 120 p., 2004.

[22] A. O. Melnik, *Architecture of computer*. Science publishing, Lutsk, Ukraine: Volinska oblastna drukarnya, 470 p., 2008.

[23] A. Drozd, V. Kharchenko, S. Antoshchuk, J. Drozd, M. Drozd, J Sulima, *On line testing of the safe instrumentation and control systems*, A. Drozd and V. Kharchenko (Edits), National Aerospace University named after N.E. Zhukovsky "KhAI", 614 p., 2012.