# The Use of Natural Resources for Increasing a Checkability of the Digital Components in Safety-Critical Systems

A. Drozd[1], V. Kharchenko[2,3], S. Antoshchuk[1], J. Drozd[1], M. Lobachev[4], J. Sulima[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"*
[4]*Odessa National Mechnikov University*
[1]*drozd@ukr.net,* [2,3]*V.Kharchenko@khai.edu,*[1]*svetlana_onpu@mail.ru,* [1]*mr_lemur@mail.ru*

## Abstract

*Influence of safety-critical Instrumentation and Control systems (I&CS) particularities on checkability of their digital components are examined. The natural resources which can be used for increasing checkability of the digital components are analyzed. Natural resources of digital components developed as multi-version system with strongly connected versions are considered. The checkability-oriented designing of simultaneous fault tolerant digital components is offered.*

## 1. Introduction

Design of safety-critical I&CS based as a rule on a component approach is associated with a problem of the ensuring and maintaining the functional safety of digital components for obtaining the reliable results of data processing [1].

Traditionally this problem is solved by use development of the fault-tolerant systems based on a set of approaches such as employ of correction codes, majority structures, various kinds of redundancy and reconfiguration [2]. Last time the fault-tolerant digital components are developed with use of the multi-version technologies which opposite to failure due to common cause failure [3].

Requirements to operative detection and toleration of the faults in safety-critical I&CS determines the methods and means of on-line testing as the basic in maintenance of fault tolerance [4].

In commercial applications fault tolerance of digital components as a rule guarantees their functional safety. However particularities of safety-critical I&CS cause a problem of low checkability of digital component which limits opportunities of on-line testing including fault-tolerant structures.

The main particularities of safety-critical I&CS are their design for operation in two modes: normal and emergency and also a role of these modes in live cycle. For most of operating time, the safety-critical I&CS run in the normal mode. The emergency one, for which these systems are designed, is a rare event and at best way never occurs. The digital components work in both modes on the different limited sets of input words [5].

What influence do these particularities render on the checkability of the digital components? And why the digital component checkability is so important for safety-critical I&CS? For the answer to these questions it is necessary to be addressed to definition of the checkability. The checkability traditionally concerns to area of testing, where bears the name of testability, and it is determined by their opportunity to carrying out of testing [6].

Non-checkable digital components can accumulate the latent constant faults. In commercial applications the components work in one mode. Therefore the accumulated faults remain latent during all operating time without damage of functional safety.

Accumulation of the latent constant faults in a normal operating mode is the uncontrollable process proceeding in safety-critical I&CS during long time. The amount of the latent faults which have been accumulated in a normal mode can exceed a threshold for which fault tolerance of digital components is designed. It can lead to violation of the functional safety in emergency mode of safety-critical I&CS. That is why in safety-critical I&CS it is necessary to use digital components with high checkability.

However the analysis of safety-critical I&CS digital components has shown their low checkability. In particular the checkability of the digital comparators being the most widespread component of safety-critical I&CS does not exceed 50% [7].

In this paper we propose approach to increasing of component checkability for safety-critical I&CS using their natural resources and resources of their digital components.

Structure of the paper is the following. Influence of safety-critical I&CS particularities on checkability of their digital components are considered in section 2. Section 3 is dedicated to the resources which can be use for increasing checkability of the digital components. Natural resources of digital components developed as multi-version system with strongly connected versions are considered in section 4. The approach to increase checkability of simultaneous fault tolerant digital components is offered and the example of checkability-oriented designing of the iterative array multiplier is shown in section 5. Last section 6 concludes discussion.

## 2. Influence of safety-critical I&CS particularities on digital components checkability

In testing the checkability of digital components is estimated in a context of the verifying their technical condition that is considered as the independent task which has been not connected to calculations on real operating sequences of input words [8]. At the same time, on-line testing aimed at the checking reliability of calculated results is limited in the opportunities to the checkability of digital components in not smaller degree, than testing.

In on-line testing non-self-checking circuit containing one output can be examined as an example of the digital component with low checkability. Really this output is not suitable to be tested or checked for estimating technical condition of circuit or reliability of result accordingly [9].

Checkability (testability) of digital component is estimated on its controllability and observability [10]. Controllability is determined by an opportunity of installation of a digital component in any condition by submission on its inputs of some input sequences, and observability is an opportunity of revealing, in what condition there was a digital component under the analysis of its input - output sequence for final number of steps.

As it is known, uncontrollability and non-observability of the digital circuit are determined, first of all, by its structural redundancy inherent in fault tolerant structures [6].

Work of the safety-critical I&CS in two modes increases dependence of on-line testing efficiency and functional safety of fault- tolerant digital components from their checkability.

The limited set of the input words used in a normal mode, is the reason of low controllability and observability of points in circuit of the digital component. Really, the functions calculated in internal and output points of the circuit, are not completely determined on the limited set of input words. This makes the circuit redundant for work in a normal mode. Such additionally created structural redundancy becomes the reason of occurrence of uncontrollable and non-observable points. It promotes decrease of checkability in digital components and leads to accumulation of the latent faults.

For estimating checkability of a digital component in on-line testing it is expedient to use definitions of a controlled and observable point of its circuit.

The point of the circuit is controlled if it accepts all possible values on set of input words. Further values of zero and unit are considered.

The point of the circuit is observable if changes of each of its values results on set of input words in change at least a check point. The circuit points to which the error detection circuit is connected are referred to as the check points.

If the point is both controlled and observable it is said to be checkable. Otherwise the point is non-checkable.

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

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

where $N_E$ is amount of non-checkable points;

$N_T$ is total of the circuit points.

Non-checkable points suppose accumulation in them of constant faults. The checkable points exclude such opportunity.

The estimation of safety-critical I&CS digital components shows a low level of checkability in a normal mode, and demands development of approaches to its increase.

## 3. Resources for increasing checkability of safety-critical I&CS digital components

For solving the tasks including such as the safety-critical I&CS development, design of digital components and increase of their checkability it is necessary to attract some resources - models, methods and means. They belong to targeted resources as are selected to reach an objective.

At the same time they are accompanied with natural resources which as a rule are not planned but are attached to target resources naturally by virtue of particularities of the accepted decision.

Natural character of these resources consists that they should not be entered (as they already are present) and accordingly to pay for them. On the contrary, their use can essentially simplify target resources and improve parameters of the received solution.

Two natural resources are widely known only: natural information and natural time redundancy [11, 12]. Actually set of natural resources is infinite as particularities of target resources concern to them. These particularities are shown in the organization and functioning of target resources where they act accordingly as system of elements and an element of system.

All target resources are elements of the Universe and inherit its particularities (natural resources of organization) to be parallel and approximate. Target resources receive such development by their choice and the creation encouraged with gifts as natural resources applied to them.

Natural resources can be in an active or passive condition, demanding their activation. Among target resources the methods differ by an active position in the decision of tasks, using models, determining means and activating the natural resources.

The methods can be divided into two groups: the methods of analysis and synthesis which for natural resources are the methods of their revealing and activation accordingly.

To methods of revealing of the natural resources it is possible to relate a method of classification which separates particularities of target resources, carrying it to a subclass of some class [13]. Thus the methods of activation of the natural resources, directed on the account of the revealed particularities, receive development from universal methods to ones dedicated on a subclass of target resources.

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

- I&CS like Reactor-Trip Systems for Nuclear Power Plants (NPPs) [14];
- I&CS like Reactor Power Control and Limitation System for NPPs or other specialized computing systems [15].

Such classification allows separating the particularities of these I&CS kinds.

The first kind of I&CS mainly process exact data obtained from comparators. Except some certain degree of inertia of the controllable objects in comparison with that of high-rate digital components creates natural time redundancy.

This natural resource allows designing the digital components for processing data in serial code. It leads to multiple use of every point in circuit of the digital components during execution of the operation. Due to this feature all points of the circuit become controlled.

Points which thus did not become observable are included in set of checkpoints of the circuit. In such way all points become also observable and the digital component become checkable [16].

The second kind of I&CS mainly process approximate data obtained from sensors and their development answer to requirements of providing a high productivity. Such data processing as a rule is carried out in floating-point format using pipeline processor containing simultaneous digital components for execution of the arithmetic operations [17].

Simultaneous digital components are characterized by unitary use of points of the circuit during operation and by such natural resource, as uniformity of elements and a regularity of connections between them.

Unitary use of points causes low checkability of simultaneous digital components of the safety-critical I&CS on the limited set of input words. For example, the iterative array multiplier achieves 100% of checkability only at use of 39% of input words [18].

In order to increase checkability of simultaneous digital components it is expedient to include not only own natural resources, but also the natural resources being particularities of obligatory target resources of the safety-critical I&CS. Target resources which provide fault tolerance of digital components concern to them, for example, the digital components with use of multi-version technologies.

However multi-version structures possess significant redundancy [19]. The structural redundancy reduces checkability of the circuits. The increase in amount of versions, as a rule, only complicates a digital component and increases amount of non-checkable points in its circuit.

For activation of the natural resources raising checkability of digital components, multi-version systems which become simpler at increase in quantity of versions can be used.

## 4. Digital components developed as system with strongly connected versions and their natural resources

Multi-version system with strongly connected versions (SVS) are developed proceed from maximal versions connectivity which ensure protection from failure due to common reason [20].

Basis for development of SVS are computer systems (CS) which contain sets of identical elements. Versions can be created, increasing the structure of the initial CS by introducing of additional identical elements. While defining a SVS structure, identical elements of initial CS are united in identical sections, which, in particular, can also consist of one element.

Let CS consist of identical elements divided into $K$ sections. Then use of one additional section forms SVS, which will consist of $K + 1$ various versions (of initial CS) received by removal of one section. A minimum quantity of versions in a SVS is three.

The SVS becomes protected from failure due to the common reason using two groups of target resources:

- a set of versions, that contains at least one true version;
- means of a choice of the true version.

Development of SVS has been prepared by previous perfection of CS by a way of execution of parallel calculations inheriting parallelism of Universe as its natural resource. In this process we've obtained such natural resource as structure of CS with array of identical elements. This resource has been activated for generation of versions in SVS.

Besides, the parallelism of Universe has stimulated development of functions for selection of results calculated on parallel branches of computing process.

Therefore the SVS and the CS become related not only by identical elements, but also by performance of choice functions, which can be subdivided into operational and specific functions. Operational functions of choice are used in initial CS for a choice of results from parallel branches of calculations. These functions are common for SVS and initial CS. Specific functions of choice are used for a choice of the true version in SVS. Choice executed with use of both operational and specific functions is a natural resource which can be activated by their sharing for simplifying the target resources of SVS.

On a circuit level the simultaneous digital components, such as parallel combinational adders and shifters, iterative array multipliers and dividers, also memory blocks create basis for SVS. They, as a rule, contain identical elements and regular connections between them.

The following units concern to identical elements:

- multiplexor choosing a bit of result in parallel shifter;
- full adder in parallel adder of numbers;
- row of operation elements in iterative array multiplier and divider.

These identical elements can be incorporated into sections.

## 5. Case-study: checkability-oriented designing of the iterative array multiplier

The digital component containing $N$ sections can be transformed into SVS by the following steps.

1. The additional section is built into circuit of the digital component, not disrupting its regular structure.
2. The circuit will be transformed into ring structure by joining the last and first sections using regular connections.
3. Each pair of the next sections is supplemented with units of disconnection of the ring. The first of these sections is excluded from calculations, and the second section becomes the first section of CS. Exclusion of one section creates one of $N + 1$ versions of the computing circuit. These units relate to means of a choice of the true version.
4. Besides, the choice of the true version demands embedding the units of receiving operands and outputting the results (depending on the number of the version), the counter keeping the number of the current version and the circuit of on-line testing for changing of the version number before removal of detected error.

The true version is searched for by consecutive exception of sections, which are additions to versions.

Increase of checkability can be shown by the example of the iterative array multiplier of $n$-bit operands which structure will consist of $n^2$ cells and is shown for $n = 4$ on figure 1 [21].

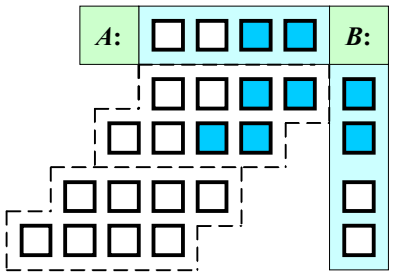


Figure 1: Structure of iterative array multiplier

If in a normal mode the operands change in $r$ low bits the multiplier contains only $r^2$ cells with the changing data. They are allocated by dark color on fig. 1 for $r = 2$. Points of circuits of these cells are controlled. They are connected to points of result, i.e. check points, by means of the full adders included in cells. Functions of carry and the sum of full adders are self-dual, that ranks controlled points also to observable points and, hence, to checkable. Other cells (not allocated by color) are non-checkable.

The multiplier is divided into two sections with two rows as identical elements and transformed to the SVS containing three sections. The system forms three versions by cyclic shift of operand $B$ (with step 2) added with two zero positions. At consecutive exception of section 1, 2 and 3 the versions contain section 2 and 3, 3 and 1, 1 and 2, accordingly.

Use of sections, containing $N \leq r$ identical elements, provides checkability of $r$ low cells in all rows of the multiplier as it is shown for $N = r$ and $r = 2$ on figure 2.

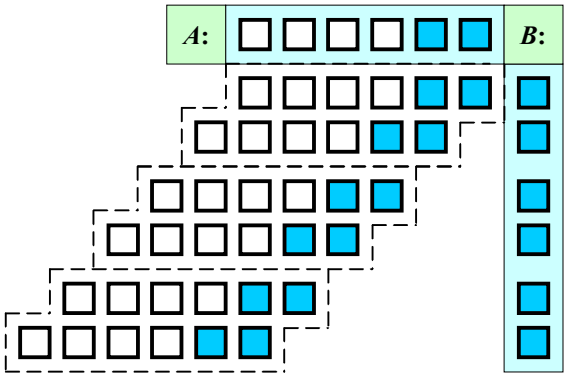


Figure 2: The iterative array multiplier as SVS

Additional generation of versions by cyclic shift of operand $A$ makes all cells of the multiplier checkable as it is shown on figure 3.

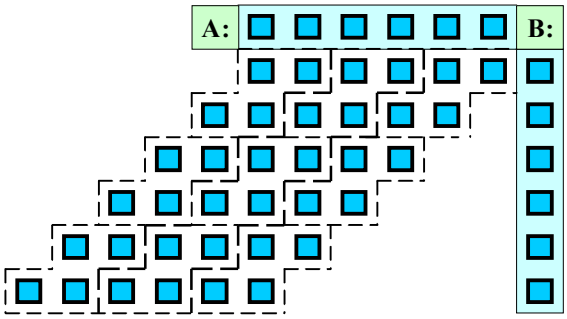


Figure 3: The checkable iterative array multiplier

## Conclusion

Safety-critical I&CS and their digital components are developed as fault-tolerant ones. However it does not guarantee their functional safety. The reason is low checkability of simultaneous digital components used most frequently. Such checkability is caused by particularities of safety-critical I&CS including their work in a normal mode on the limited set of input words. It results in additional structural redundancy of digital circuits in a normal mode. Structural redundancy of circuits of digital components becomes the reason of their low checkability which creates conditions for accumulation of the latent faults. These faults cause additional risks of unsafe behaviour of safety-critical I&CS in an emergency mode.

In order to increase checkability the natural resources which are activated in the simultaneous digital components developed with use of multi-version technology are used. The simultaneous digital component containing, as a rule, sections of identical elements, are transformed to SVS which uses change of versions for both search of the true version and increase of checkability.

## References


[1] 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.

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

[3] Sklyar V., Kharchenko V., Bahmach E., e.o. *Multi-version FPGA-based NPP Instrumentation and Control Systems: Automata models, Implementation and operation Results* // Proc. IEEE East-West Design & Test Symposium. – Yerevan (Armenia). – 2007. – P. 396–400

[4]. 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.

[5] 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* // Proc. First International Workshop 'Critical Infrastructure Safety and Security' (CrISS-DESSERT'11). – Kirovograd (Ukraine). – 2011. – P. 139 – 147.

[6] N. S. Shcherbakov. *Reliability of work of the digital devices*. – Moskow: Mashinostroenie.– 1989. – 224 p.

[7] A. Drozd, V Kharchenko., S.Antoshchuk, M. Drozd. *Checkability of safety-critical I&Cc system components in normal and emergency modes* // Journal of Information, Control and Management Systems. – 2011. – Vol. 1, No. 1. – P. 56 – 63.

[8] V. M. Lokazuk, J. G. Savchenko. *Reliability, checking, Diagnostic and modernization of PC*. – Kiev: Publishing house 'Academy'. – 2004. – 376 p.

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

[10] R. Bennets. Co-design of testable logic circuits. – Moskow: Radio i Svyaz. – 1990. – 180 p.

[11] J. G. Savchenko. Digital devices fault tolerant to element. – Moscow: Sov. Radio. – 1977. – 176 p.

[12] A. M. Romankevich, V. N. Valuyskiy, V. A. Ostafin. *Structural-time redundancy in control circuits*. – Kiev: 'Vishcha shkola'. – 1979. – 160 p.

[13] J. Drozd. A. Drozd. *Natural resources of co-design and diagnostic of computer systems and their components* // Tp. 13*th* International Conference 'Modern information and electronic technology'. – Odessa (Ukraine). – 2012. – P. 92.

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

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

[16] 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). – 2011. – P. 411 – 416.

[17] E. Tanenbaum. *Architecture of Computers*. – Petersburg: Piter. – 2003. – 698 p.

[18] A. Drozd, V. Kharchenko, S. Antoshchuk, M. Drozd, J.Sulima. *Assessment in checkability of safety-critical embedded systems components* // Electronic and Computer Systens. – 2012. – No 6 (58). – P. 184 – 190.

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

[20] 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.

[21] A. Drozd, M. Lobachev, R. Kolahi, J. Drozd. *Iterative array multiplier with on-line repair of its functions* // Proc. IEEE East-West Design & Test Conference. – Sochi (Russia). – 2006. – P. 93 – 94.

**Authors:**

**ALEXANDR DROZD**, Professor, PhD (1982), Dr. Sci. Eng. (2003), Professor with the Department of Computer Systems and Networks of Odessa National Polytechnic University. He has published more than 300 papers dealing with problems of On-line Testing.

**VYACHESLAV KHARCHENKO** Professor, PhD (1981), Dr. Sci. Eng. (1995), Head of the Department of Computer Systems and Networks, National Aerospace University "KhAI", and the Centre for Safety Infrastructure-Oriented Research and Analysis, RPC "Radiy". He has published more than 200 papers and 12 books dealing with problems of computer-based safety and fault-tolerance.

**SVETLANA ANTOSHCHUK**, Professor, PhD (1997), Dr. Sci. Eng. (2005) Head of Computer Systems Institute and Head of Information Systems Department of Odessa National Polytechnic University. She has published more than 130 papers.

**JULIA DROZD**, Associate Professor, PhD (2000), Associate Professor of Information Systems Department of Odessa National Polytechnic University. She has published more than 70 papers.

**MICHAIL LOBACHEV**, Associate Professor PhD (1997), Associate Professor, Odessa National Mechnikov University. He has published more than 50 papers

**JULIAN SULIMA**, Master of Computer Systems and Networks (2008) Postgraduate student of Information Systems Department of Odessa National Polytechnic University.