POWER-CONSUMPTION-ORIENTED CHECKABILITY FOR FPGA-BASED COMPONENTS OF SAFETY-RELATED SYSTEMS

Oleksandr Drozd [1)], Viktor Antoniuk [1)], Miroslav Drozd [1)], Volodymyr Karpinskyi [2)], Pavlo Bykovyy [3)]

[1)] Odessa National Polytechnic University, 1, Shevchenko Ave., 65044, Odessa, Ukraine
drozd@ukr.net, viktor.v.antoniuk@gmail.com, miroslav_dr@mail.ru
[2)] Rolls-Royce plc., Watnall Road, Hucknall, NG15 6EU, UK
vkarpinskyi@gmail.com
[3)] Ternopil National Economic University, 3 Peremohy Square, Ternopil, Ukraine, 46020,
pb@tneu.edu.ua

1. INTRODUCTION

A checkability of the digital circuit is its suitability for monitoring the presence of a fault in it. The importance of this indicator increases with the expansion of the area of critical information technology applications that underlie instrumentation and control safety-related systems. These systems manage high-risk objects, including transportation infrastructures, power grids and power plants, as well as other areas relevant to people's livelihoods. Safety-related systems are focused on ensuring safety of the control object. Solving this problem requires ensuring functional safety also for the control system itself.

The amount of critical applications is increasing. Their complexity and power growth creates the prerequisites for increasing the risk of accidents.

Safety, which becomes the main argument in the prevention of man-made disasters, is based on the use of fault tolerant solutions.

The main threat to their effectiveness comes from the hidden processes that can lead to the accumulation of many hidden faults. The amount of these faults may exceed the possibilities of fault-tolerant solutions for their parrying. Such circumstances appear because of insufficient checkability of the circuits in the components of safety-related systems.

Therefore, ensuring of safety requires improvement in the circuit checkability, which can be significantly reduced with the growing complexity of the circuits themselves. Fault-tolerant solutions become effective in ensuring the safety of safety-related systems only when performing a condition of the system's checkability, which begins with the checkability of its components.

2. RELATED WORKS, GOAL AND STRUCTURE OF THE PAPER

Requirements for safety-related systems are regulated by international standards that define safety and measures to ensure it for the system and for the control object to prevent accidents and reduce the consequences if they occur.

Safety-related systems can be considered as the development of computer systems with the division of the operating mode into two modes: normal and emergency, which have significant differences. The normal mode is the longest and can be considered as waiting in relation to the emergency mode. Emergency mode is the most responsible and least studied. In these modes, digital circuits can receive various input data, for example, they can operate in normal mode at the noise level and receive useful signals only when the emergency mode starts.

The limited set of input data makes the digital circuit structurally redundant. This reduces the checkability of the circuit.

As a rule, safety is supported by fault-tolerant solutions based on configurable units, correcting codes, majority structures and multi-version technologies. Multi-version solutions allow to resist to common cause failures that may occur, for example, due to design errors.

Fault-tolerant circuit solutions significantly complicate the digital components of safety-related systems, repeatedly increasing their structural redundancy and complexity.

Generally, the checkability of a digital circuit is defined as its suitability for performing logical checking, which is considered as the possibility of detecting a fault, using for this the error of the result calculated at the output of this circuit in testing or operating mode.

Logical checkability is best known as testability, i.e., suitability to test development for detecting faults in the process of testing of the circuit. Testability is the simplest form of logical checkability. It depends only on the structure of the circuit, and, therefore, is called structural checkability.

In on-line testing, the logical checkability of the digital circuit becomes structurally-functional, since it depends not only on the structure of the circuit, but also on the input data processed in an operating mode. The possibilities of on-line testing of the digital circuits are completely limited by its structurally-functional checkability.

Safety-related systems, as well as other cyber-physical systems, including IoT, receive input data from sensors. These data are measurement results, i.e., they refer to approximate data, which is usually processed in floating-point formats.

Performing operations in floating-point arithmetic greatly complicates circuit design solutions both in terms of organizing main calculations and in checking them. Mantissa processing is most efficiently performed by using the truncated operations. These operations retain a single accuracy of computations, however, they significantly complicate checking schemes, including residue checking, which is the main method of on-line testing the arithmetic nodes.

The complication of the circuits in the main and checking operations reduces their logical checkability.

The logical checkability gained development in the theory and practice of creation of the totally self-checking circuits. Self-checking of these circuits increases structurally-functional checkability in error detection schemes when the self-testing condition is met.

However, in safety-related systems, structurally-functional checkability becomes dual-mode, i.e., different for a normal and emergency modes due to different input data. This difference creates a problem of the hidden faults that can be accumulated over the course of a long-term normal mode and manifest themselves in reducing the fault tolerance of the circuits in most critical emergency modes.

The main approach to a solution of the hidden fault problem is the use of the imitation modes which recreate emergencies and more than once brought to them as a result of unauthorized activation of the emergency mode by a person or a fault.

The use of hazardous imitation modes aimed at improving the checkability of safety-related systems indicates a lack of confidence in the effectiveness of the fault-tolerant solutions and the lack of checkability to support this effectiveness.

We can distinguish two groups of methods of the logical checkability improvement for solving the problem of hidden faults without use of the imitation modes. The first group of methods is aimed at improving the structurally-functional checkability of circuits in normal mode to counteract the accumulation of hidden faults.

Another group of methods aligns the structurally-functional checkability of the normal and emergency modes in order to remain the hidden faults of the normal mode in the emergency mode and to detect the faults of the emergency mode during the long-term normal mode.

Both groups of methods are focused on the implementation of digital components on FPGA (Field Programmable Gate Array) using modern CAD (Computer-Aided Design) systems. This feature makes them attractive for safety-related systems, which receive a number of advantages when designing on FPGA.

However, these methods are significantly limited by the complexity of modern circuits, a number of requirements imposed by standards to safety-related systems and opportunities of the logical checkability which is in certain dependence on the faults arising in chains of the common signals, such as signals of reset and synchronization.

Thus, ensuring the checkability of circuits for safety-related systems is an important and urgent task that requires its solution without the use of the dangerous imitation modes. Ensuring logical checkability faces the considerable complexity of modern circuit solutions both in the building of fault-tolerant components and the limitations of the standards, governing their development for safety-related systems. These arguments stimulate the search for new solutions, including those outside the logical form of checkability.

The goal of this article is to develop a new form of checkability as the suitability of a circuit for checking based on an assessment of its power consumption which allows detecting faults in chains of the common signals. Major scientific contribution is made to solving the hidden fault problem concerning common signals on the basis of assessment and the use of checkability associated with power consumption of FPGA components in safety-related systems.

Section 3 defines power-consumption-oriented checkability (power-checkability) and gives its analytical evaluation for the circuits designed on FPGA. Section 4 describes experiments with FPGA projects to evaluate their power-checkability and analyzes the results of these experiments.

3. POWER-CHECKABILITY DEFINITION

The circuit checkability can be estimated by the ratio of the P_F volume of ranges of impossible power consumption values, which uniquely characterizes the circuit as faulty, to the P_T volume of a whole range of power consumption values, $P_T = P_F + P_C$, where P_C is the volume of a range of possible power consumption values.

The R_C range of possible values of power consumption allocates two ranges of impossible values in the entire R_T range: upper R_U and lower R_L, for which their volumes P_U and P_L make up the volume $P_F = P_U + P_L$. Volumes P_U and P_L, referred to the entire volume of P_T, determine the upper and lower checkability of the circuit, respectively.

Upper checkability determines the detection of faults that significantly increase power consumption, for example, in the event of a short circuit.

Lower checkability is focused on faults that significantly reduce power consumption. This reduction of power consumption occurs in its dynamic component, which is proportional to the number of transitions switching signals in the circuit. A significant reduction in the number of transitions is caused by faults that violate common signal circuits, such as, for example, reset and synchronization signals.

Faults in common signals pose a significant threat to safety-related systems, as they can be hidden from logical checking due to its blocking in a state that indicates the absence of a fault.

Thus, logical checkability does not cover a set of faults arising in common signal circuits. For their detection, it is necessary to develop alternative forms of checkability, including power-oriented checkability. Further, we consider the lower checkability, which is important for detection of faults in chains of the common signals.

Taking into account the constant value of the supply voltage, the values of consumed power are replaced in the assessment of checkability with the values of current consumption. Lower checkability, which takes into account the influence of only the dynamic component of the power consumption, is accordingly determined using the dynamic component of the current consumption as follows:

$$C_{P.L} = I_{D\,MIN} / I_{D\,MAX},$$

where $I_{D\,MIN}$ and $I_{D\,MAX}$ – the minimum and maximum values of dynamic component of the current consumption, respectively.

Power-checkability $C_{P.L}$ essentially depends on the conditions of the circuit designing. We are reviewing Quartus Prime 17.1 Lite Edition (Intel FPGA), which estimates power consumption using its PowerPlay Power Analyzer utility.

Similar utilities, for example, XPower Analyzer, are also used in other recognized CAD systems, in this case in Xilinx ISE.

It should be noted that Intel FPGA (former Altera) and Xilinx are world leaders in FPGA design and produce 38% and 49% of products in this market, respectively.

Power monitoring of the circuit can be performed in its operating mode by measuring the current consumption. We can judge the dynamic component I_D by subtracting its static component I_S from the measured I_T current consumption, which can be estimated previously by means of the PowerPlay Power Analyzer utility.

We can assess checkability using simulation and measurement results taking into account their errors.

The minimum $I_{D\,MIN}$ value of the dynamic current consumption component can be estimated as follows:

$$I_{D\,MIN} = I_T - I_S - \Delta I_T - \Delta I_S, \qquad (1)$$

where ΔI_T and ΔI_S – an absolute value of the error of current consumption I_T and its static component I_S, respectively.

Formula (1), taking into account the equality $I_T - I_S = I_D$, is converted to the following form:

$$I_{D\,MIN} = I_D - \Delta I_T - \Delta I_S, \qquad (2)$$

The maximum $I_{D\,MAX}$ value of the dynamic component of current consumption can be received similarly taking into account the increasing errors and possible increase in activity of signals at circuit inputs:

$$I_{D\,MAX} = I_D^* + \Delta I_T^* + \Delta I_S^*, \qquad (3)$$

where I_D*, ΔI_T*, ΔI_S* – the dynamic component of current consumption, an absolute value of the error of current consumption and its static component for a case of the increased activity of input signals.

Then the lower power-oriented checkability is evaluated with regard to (2) and (3) by the following formula:

$$C_{P.L} = (I_D - \Delta I_T - \Delta I_S) / (I_D^* + \Delta I_T^* + \Delta I_S^*). \quad (4)$$

The PowerPlay Power Analyzer utility estimates the current consumption of I_T, as well as its dynamic I_D and static I_S components with an error of $\Delta = \pm 2.5\%$. Sensors for measuring current consumption work with the same error.

Then, formula (4), taking into account $\Delta I_T = \Delta I_S = 2.5\%$ and $\Delta I_T^* = \Delta I_S^* = 2{,}5\%$, takes the following form:

$$C_{P.L} = (I_D - 0.025\, I_T - 0.025\, I_S) / (1.025\, I_D).$$

The parameters I_D, I_S and I_T of power- checkability $C_{P.L}$ can change their values under the influence of the activity of signals that are fed to the inputs of the circuit. Therefore, the power-checkability $C_{P.L}$ should be investigated with different input signal activity. The final result is the smallest power-checkability $C_{P.L}$.

The assessment methodology contains the following sequence of steps:

– Designing in Quartus Prime a project of a multiplier of a given range.

– Compiling a project in Quartus Prime that results in determining the allowed synchronization frequency for the project.

– Setting up time parameters (frequency) in the utility Time Quest Timer Analyzer.

– Re-compiling the project with the established time parameters.

– Setting up in the Power Play Power Analyzer utility a given value for the activity of informational (input / output and internal) signals of the project as a percentage of the clock signal activity (frequency).

– Running a simulation in Power Play Power Analyzer, which determines the total current consumption of the core I_T and its static I_S and dynamic I_D components.

– Calculating by formula (4) the checkability value for the given multiplier design and given informational signals activity.

4. EXPERIMENTAL ASSESMENT OF LOW POWER-CHECKABILITY

Power-checkability $C_{P.L}$ is determined for iterative array multiplier circuits of binary numbers based on simulation results that were run on Intel Max 10 10M50DAF672I7G FPGA containing 288 9-bit multiplication blocks with input and output buffer registers.

The multiplication blocks in Quartus Prime are designed on the basis of the LPM_MULT multiplier from the Intellectual Property Core (IP-Core) of the Library of Parameterized modules (LPM), which is a part of Quartus Prime. In the course of the experiments, FPGA projects of iterative array multipliers with the size of operands n = 16, 32, 48 and 64 were implemented. The input signals activity A_I was set using the PowerPlay Power Analyzer utility in the range from 0% to 100% in relation to the synchronization signal of the multiplier registers with increments of 12.5%.

The simulation results which are the parameters I_D, I_S and I_T for a core of FPGA chip are shown in Tables 1-4 for n from 16 to 64 bits, respectively.

Table 1. Experiment results for n = 16

A_I, %	I_D, mA	I_S, mA	I_T, mA
0	7.76	11.75	19.51
12.5	8.61	11.76	20.36
25	9.46	11.76	21.22
37.5	10.31	11.76	22.08
50	11.16	11.77	22.93
62.5	12.02	11.77	23.79
75	12.87	11.78	24.64
87.5	13.72	11.78	25.50
100	14.57	11.79	26.36

Table 2. Experiment results for $n = 32$

A_I, %	I_D, mA	I_S, mA	I_T, mA
0	16.28	11.93	28.21
12.5	19.25	11.94	31.19
25	22.22	11.95	34.17
37.5	25.20	11.96	37.16
50	28.17	11.97	40.14
62.5	31.14	11.99	43.13
75	34.11	12.00	46.11
87.5	37.08	12.01	49.09
100	40.06	12.02	52.08

Table 3. Experiment results for $n = 48$

A_I, %	I_D, mA	I_S, mA	I_T, mA
0	34.07	12.11	46.18
12.5	39.61	12.13	51.74
25	45.15	12.15	57.30
37.5	50.69	12.17	62.87
50	56.23	12.19	68.43
62.5	61.77	12.22	73.99
75	67.31	12.24	79.55
87.5	72.85	12.26	85.11
100	78.39	12.28	90.67

Table 4. Experiment results for $n = 64$

A_I, %	I_D, mA	I_S, mA	I_T, mA
0	60.23	12.32	72.55
12.5	70.05	12.35	82.40
25	79.87	12.39	92.26
37.5	89.69	12.42	102.11
50	99.51	12.45	111.97
62.5	109.33	12.49	121.82
75	119.15	12.52	131.68
87.5	128.97	12.56	141.53
100	138.79	12.59	151.39

Power-checkability $C_{P.L}$ is calculated for $I_{D\,MIN}$ which is estimated at zero activity of input signals, and $I_{D\,MAX}$ received in case of an increase in activity A_I of input signals for value $\Delta A_I = 12.5\%$ from 0 to 100%.

Results of power-checkability assessment represented as a percentage are shown in Table 5.

Table 5. Assessment of Power-checkability

A_I, %	$n = 16$	$n = 32$	$n = 48$	$n = 64$
0	81.70	88.39	91.80	93.19
12.5	74.14	75.15	79.14	80.24
25	67.85	65.36	69.56	70.45
37.5	62.55	57.80	62.04	62.78
50	58.02	51.83	55.99	56.62
62.5	54.06	46.98	51.02	51.57
75	50.64	42.96	46.85	47.34
87.5	47.63	39.57	43.32	43.75
100	44.95	36.67	40.28	40.67

The graphics show the monotonous nature of change in the checkability, which raises with decrease in possible change of activity of the input signals.

For 16-, 32-, 48-, 64-bit multipliers, the greatest power-checkability values are reached at the minimum changes in activity of the input signals: 81.70%, 88.39%, 91.80%, 93.19% and 74.14%, 75.15%, 79.14%, 80.24% in cases $A_I = 0$ and $A_I = 12.5\%$, respectively.

Changes in activity of the input signals over a wide range reduce power-checkability: 58.02%, 51.83%, 55.99%, 56.62% and 54.06%, 46.98%, 51.02%, 51.57% in cases $A_I = 50\%$ and $A_I = 62.5\%$, respectively.

At the same time, even in an exceptional case of $A_I = 100\%$, power-checkability shows values from 36.67% to 44.95% which keep the considerable range of values of a dynamic component in the current consumption for detection of faults in chains of the common signals.

It should be noted that Power-checkability, as a rule, grows with increase in operand size of multipliers. The exception makes only operand size 16 for $\Delta A_I \geq 50\%$.

5. CONCLUSION

The checkability of the circuit plays a pivotal role in providing the effectiveness of fault-tolerant solutions used in safety-related systems to ensure the safety of the system itself and the control objects.

Understanding the logical checkability of the circuits was developed from testability to structurally-functional and dual-mode structurally-functional models, which allowed to determine the problem of the hidden faults and ways to solve it without using dangerous imitation modes.

However, the possibilities of improving logical checkability are limited by the growing complexity of modern circuit solutions.

In addition, the logical checkability and decisions developed in its framework, including methods of its improvement and on-line testing methods, are limited in detection of faults which arise in chains of the common signals playing an important role in functioning of the digital circuits. These faults can block the check circuits and the error detection results.

The development of circuit checkability by estimating its power consumption, that has been proposed, is provided by the necessary tools of evaluation in modern systems of digital component design on FPGA.

Power-checkability allows to detect faults in the circuits of common signals in reducing the dynamic component of power consumption.

Analytical assessment of power-checkability is based on the current consumption and its dynamic and static components, which reflect the power consumption at a constant supply voltage.

Experiments for power-checkability evaluations based on the dynamic component of the consumed current were performed on Quartus Prime 17.1 Lite Edition (Intel FPGA) CAD software using an intelligent LPM_MULT module for a range of iterative array multipliers sizes and activity levels of the input circuit signals.

The experiments that have been carried out showed a high level of power-checkability, which raises with the decrease in change of activity of the input signals and, as a rule, grows with increase in complexity of circuits.

In the most widespread cases if a change in activity of the input signals does not exceed 25% and 50%, power-checkability exceeds 50% and 65%, respectively. Thus, more than a half of range of values in a dynamic component of the current consumption lies in the area of impossible values which allow detecting faults in chains of the common signals.

Complication of iterative array multipliers while increasing the size of operands from 32 to 64 bits raises power-checkability of their circuits unlike a logical checkability which decreases with the growth of circuit complexity.