Evolution of a Problem of the Hidden Faults in the Digital Components of Safety-Related Systems

A. Drozd, M. Kuznietsov, S. Antoshchuk, A. Martynyuk, M. Drozd, J. Sulima
Odessa National Polytechnic University, Odessa, Ukraine,
drozd@ukr.net, koliaodessa@ukr.net, svetlana_onpu@mail.ru, anmartynyuk@ukr.net,
miroslav_dr@mail.ru, mr_lemur@mail.ru

1. Introduction

The human surrounds himself with objects of the increased risk to which power networks, power blocks of power plants, high-speed railway transport, flying technique and many other things belong. The risk is estimated as the product of an accident probability on the cost of its consequences. The cost of consequences permanently increases together with growth of complexity, power and number of objects with the increased risk. Control of risks requires lowering of probability in origin of accidents and it is based on enhancement of the information technologies implemented in the instrumentation and control safety-related systems. Development and maintenance of these systems is regulated by the international standards aimed at providing of the functional safety of both system and a control object for accident prevention and lowering of their consequences if accident happens.

The functional safety of system and control object is based on the use of fault-tolerant decisions in which an important role is played by methods and means of on-line testing. They give operational evaluation in state of system and its components by assessment of trustworthiness of the calculated results.

However, possibilities of on-line testing and fault-tolerant decisions in general are restricted by a checkability of circuits of the digital components. The circuit checkability in the test mode, i.e. a testability, is structural since it depends only on structure of the circuit. The checkability of circuits in an operating mode is structurally functional as depends on both structure of the circuit and input data.

On a number of the objective and subjective reasons, the circuit checkability of digital components in structure of the safety-related systems is low.

We can select two such objective reasons:

- designing of the safety-related systems for operation in two modes: normal and emergency;
- structural redundancy of circuits in fault-tolerant decisions.

The objectivity of these reasons is caused by features of safety-related systems as they cannot work only in one mode and shall resist to faults for support of the functional safety.

Features in designing of the safety-related systems and their components are the subjective reasons.

As a first approximation, the low checkability of circuits caused by the objective reasons becomes insuperable restriction in development of on-line testing methods and fault-tolerant decisions for the safety-related systems. The danger of such restriction is shown, first of all, in a problem of the hidden faults.

This problem consists in accumulation of faults of the circuit throughout a continuous normal mode in the conditions of absence of the input words showing them. Accumulated faults are shown in lowering of fault tolerance of circuits and the functional safety of systems on other input words in the most responsible emergency mode.

The problem of the hidden faults is known not on the hidden faults which remained hidden, but on abortive attempts of their detection with the use of the imitative modes.

These modes consist in reconstruction of emergencies which often require switch-off of abnormal protection. Such approach led to alert conditions more than once. An example of switch-off of abnormal protection is the Chernobyl catastrophe.

The use of the dangerous imitative modes shows complete mistrust to fault-tolerant decisions and the functional safety of safety-related systems and requires other solutions of the hidden faults problem.

Such decisions follow from reviewing of this problem with the use of resource-based approach.

Section 2 considers provisions of resource-based approach in relation to the problem of the hidden faults and identifies it as a problem in development of resources.

Section 3 shows solutions by increase in the level of resource development. Solutions with the use of the multi-version program code of the FPGA projects with the LUT-oriented architecture are suggested (LUT – Look-Up Table).

2. Identification of a problem of the hidden faults

An essence of the problem of the hidden faults and ways of its decision can be defined with the use of resource-based approach.

Resource-based approach analyzes models, methods and means, component resources, from a line item of their development in a way of integration into the natural world. Process of integration consists in structuring resources under features of the natural world. Development of the computer world showed most two features: parallelism and fuzziness.

Structuring is executed by a solution of problems in assessment and reduction of a mismatch between resources and the natural world. The solution is reached with a certain throughput for execution of all amount of works for limited time, sufficient trustworthiness of the received results and the resource turnover.

Resource-based approach selects three levels in development of resources: replication, diversification and autonomy.

Replication is the bottom level in development of resources. Integration into the natural world is carried out at the expense of throughput and its growth in the conditions of open resource niches: ecological, technological, market, etc. Replication is characterized by high resource intensity.

The modern computer world shows domination of the bottom level in development of resources. Digital components contain array structures which are stamped from the unified elements.

The resource intensity of array structures can be shown on the example of the iterative array multiplier which executes a key operation of approximate calculations as multiplication is present at the representation of numbers in floating-point formats). The iterative array multiplier of n-bit numbers contains n^2 of operational elements, $2n - 2$ of which are connected sequentially. The operation is executed for one clock cycle, but each operational element is used in a clock cycle during its small part $(2n - 2)^{-1}$ (0,8% for an operand size $n = 64$).

The big sizes of array structure determine the considerable static component of energy consumption. Waves of the parasitic transitions caused by a Glitch-problem make the main part of a dynamic component of energy consumption.

The software is also stamped. Programs consist of ready excess modules at the expense of resource niches of throughput and memory size of computer systems. The limited niche of energy consumption hinders with replication of programs and hardware decisions in mobile devices. Filling of resource niches stimulates transition to diversification level when clones survive, developing features, i.e. they become individuals, and the unified elements – versions. Integration into the natural world happens due to an increase in trustworthiness which includes safety.

It is necessary to mark that the trustworthiness of the results cannot be provided at the level of replication. The majority system is fault-tolerant as stamped channels are different due to many types of natural diversity.

The safety-related systems are development of computer systems with diversification of an operating mode by its division on normal and emergency. Diversification of an operating mode is inherited by a structurally functional checkability which becomes different in normal and emergency mode owing to different input data. Failure is also diversified, creating a set of the hidden faults which can be accumulated in normal and be shown in emergency mode.

It is important to note that the computer systems working only in an operating mode have no problem of the hidden faults as these faults are never shown. Therefore, the usual computers which are traditionally designed on the basis of array structures hide one more feature of these structures which consists in the low structurally functional checkability considerably decreasing with abbreviation of a set of input data.

Thus, the problem of the hidden faults is a problem in development of computer systems when they reach diversification level in support of the functional safety of objects with the increased risk.

However, these systems continue to be projected as usual computers on the basis of array structures which treat replication level, i.e. the bottom level of the resource development.

This output not only identifies the problem of the hidden faults, but also defines ways of its decision on the basis of an increase in the level of resource development for designing of the digital components in the safety-related systems.

3. Multi-version programming of the FPGA projects

An increase in the level of resource development in designing can be reached by different methods. The most cardinal method is transition to pipeline parallelism which reflects diversification level. The modern systems are built like pipeline. But their sections are single-cycle array nodes for data processing in parallel codes.

The maximum abbreviation of array structures in sections to one operational element will transform system to the bitwise pipeline for data processing in serial codes which do not leave the place for the hidden faults.

Implementation of a cardinal way is complicated by powerful infrastructure which was created in support of array decisions for several decades. Some other opportunities of an increase in the level of the resource development can be implemented by the use of a version redundancy. The important direction in development of resources is connected with designing of the digital components on FPGA. This direction gained recognition in development of the digital components for the safety-related systems. Designing of the digital components on FPGA creates version redundancy of a program code for the circuits with the LUT-oriented architecture.

Couple of LUT units in which the output of the first LUT is connected to an address input of the second LUT can function in two versions respectively by transmission of direct or inverse values of a signal between LUT units. The inverse value is provided with inverse of all bits of memory of the first LUT of couple and compensated by swap of bits in memory of the second LUT. The choice of the version of a code for one couple of LUT units does not superimpose any restrictions for others couple. This version redundancy is already used in two solutions of the hidden faults problem.

The first decision allows to select versions with the greatest checkability of LUT memory from a normal mode and the maximum trustworthiness of results from emergency operation for faults like shorts between adjacent address inputs of LUT. The combination of a high circuit checkability and result trustworthiness in one version is reached due to change of places which happens to sets of the input data showing and masking a fault of short on direct and inverse values of a signal.

The second decision allows to interchange the position of the LUT memory bits used in an emergency and normal mode in case of the serial use of several versions. It allows to use in a normal mode all bits of the LUT memory addressed in an emergency mode.

Both decisions use a version redundancy regarding relocation of bits in the second LUT of couple. At the same time, the version redundancy of a program code can be also used regarding inverting of bits in memory of the first LUT of couple.

The suggested method considers sets M_{0N}, M_{1N}, M_{0E}, M_{1E} of bits in memory of the first LUT which accept zero and unit values in normal N and emergency E mode, respectively. The method is directed to an increase in a checkability of the LUT memory and trustworthiness of results respectively in a normal and emergency mode for the dominating fault like stuck-at unit or zero in bit of the LUT memory.

The checkability of the LUT memory in a normal mode can be evaluated taking into account the bits in which the faults can be shown. The trustworthiness of results in an emergency mode can be estimated, in view of bits in which the faults are masked. In case of the dominating faults like stuck-at unit, the method selects for each couple the version with sets of $M_{0N} \geq M_{1N}$ and $M_{0E} \leq M_{1E}$. The checkability of the LUT memory and trustworthiness of results are determined in the appropriate modes by formulas $C_N = M_{0N} / M$ and $T_E = M_{1E} / M$ where M – the number of bits in the LUT memory.

The choice of the version provides the largest checkability $C_N \geq 0.5$ of the LUT memory and trustworthiness $T_E \geq 0.5$ of result. For example, let bits 0 ÷ 15 memories of 4-address LUT memory form the following sets: $M_{0N}\{5, 7\}$, $M_{1N}\{0 \div 4, 6, 8 \div 10\}$, $M_{0E}\{5, 7, 11 \div 15\}$, $M_{1E}\{6, 8 \div 10\}$.

In this case LUT memory is evaluated in checkability and trustworthiness as $C_N = 2 / 16$ and $T_E = 4 / 16$, respectively.

Transition to the inverse version interchanges the position of sets M_{0N} and M_{1N}, M_{0E} and M_{1E}, raising a checkability of the LUT memory and trustworthiness of results to values $C_N = 9 / 16$ and $T_E = 7 / 16$, i.e. by 4.5 and 1.75 times, respectively. The method can be used together with the second decision.

4. Conclusions

Support of the functional safety of safety-related systems and objects of the increased risk faces a problem of the hidden faults which calls into question a fault tolerance of the digital components in an emergency mode.

The problem of the hidden faults is solved in practice with the use of the dangerous imitative modes which led to emergency consequences more than once.

Important step to a safe solution of the problem of the hidden faults is its identification with the use of resource-based approach which defines it as a problem in development of resources. The safety-related systems are development of computer systems to the diversification level of an operating mode in support of the functional safety of objects with the increased risk. At the same time, the safety-related systems continue to be projected as usual computer systems on the basis of the array structures reflecting the bottom level in development of resources – replication.

Identification of the problem of the hidden faults as a problem in development of resources determines ways of its decision by enhancement of models, methods and design tools to diversification level.

A number of such decisions gives the use of version redundancy of a program code of the FPGA projects with the LUT-oriented architecture.

The suggested method of a choice of the version in the program LUT code allows to use the version with the raised checkability of the LUT memory in a normal mode and trustworthiness of results in emergency mode. It promotes the best detection and masking of faults in a normal and emergency mode, respectively.