https://doi.org/10.32362/2500-316X-2019-7-4-60-70

UDC 621.3.049.774

Design for Testability of Integrated Circuits and Project Protection Difficulties

Evgeny Ph. Pevtsov@,
Tatiana A. Demenkova,
Alexander A. Shnyakin

MIREA – Russian Technological University, Moscow 119454, Russia
@Corresponding author e-mail: pevtsov@mirea.ru

Design solutions of domestic VLSI were obtained as a result of the application of computer-aided design tools of a foreign supplier (CAD Synopsys, Cadence Design Systems and Mentor Graphics), based on standard libraries of PDK elements (Project Design KIT) of factories and IC-modules also supplied mainly by foreign companies. As a rule, the developer does not have its own production facilities, using the services provided by foreign factories (fabless-companies). Due to this fact, relevant are the studies aimed at the development of a complex of measures, excluding the possibility of unauthorized changes into IC, i.e. protection of projects against intentional hardware and technology violations made during the formation of the control information for handing it over to the production facility and/or in case of IC manufacture at the factory. This paper considers this task from the standpoint of the analysis of the methodology of design for testability (DFT), i.e., a complex of measures that provide obtaining solutions at the design stage. The solutions include the verification of the correct performance of the manufactured chip by means of external tests and/or self-testing procedures. It was proposed, inter alia: 1) to analyze the libraries of standard elements used in the project with full disclosure of their specifications; 2) to create nodes with the physical non-cloning function in the projects on the basis of the libraries of standard elements in models and analysis programs; 3) to analyze IP modules used in the project with the maximum disclosure of structure, methods and algorithms for providing test coverings; 4) to provide for the development in projects of special test kits and methods of their generation at the design stage of functions in order to detect malicious nodes and programs both within SoC cores and at the level of system buses; 5) to develop at the design stage and to apply during tests a technique of special hardware measurements of parameters of the manufactured circuits and analysis of their results, inter alia, according to measurements of delays in distribution of signals and/or buses current consumption.

Keywords: design for testability, instrument bugs/Trojans, IC project verification, test coverings, self-testing units, design for security.

Тестопригодное проектирование интегральных схем и проблемы защиты проектов

Е.Ф. Певцов@,
Т.А. Деменкова,
А.А. Шнякин

МИРЭА – Российский технологический университет, Москва 119454, Россия
@Автор для переписки, e-mail: pevtsov@mirea.ru

Проектные решения отечественных СБИС получены в результате применения инструментов автоматизированного проектирования зарубежного поставщика (САПР Synopsys, Cadence Design Systems и Mentor Graphics) на основе библиотек стандартных элементов PDK (Project Design KIT) фабрик и IP-модулей, поставщиками которых также являются в основном зарубежные компании. Как правило, компания-разработчик не имеет собственных производственных мощностей, пользуясь услугами иностранных фабрик (fabless-компании). В этой связи актуальными являются исследования по созданию комплекса мер, исключающих возможности внесения несанкционированных изменений в интегральные схемы (ИС), т. е. защиты проектов от намеренных аппаратных и технологических нарушений, вносимых при формировании управляющей информации для передачи на производство и/или при изготовлении ИС на фабрике. В данной работе эта проблема рассматривается с позиций анализа методологии тестопригодного проектирования (DFT), т.е. комплекса мер, предусматривающих на этапе проектирования получение решений, в которых заложены проверки правильного функционирования изготовленной микросхемы с помощью внешних тестов и/или процедуры самотестирования. Предложено, в частности: 1) проводить анализ применяемых в проекте библиотек стандартных элементов с полным раскрытием их спецификации; 2) на основе библиотек стандартных элементов моделей и программ анализа создавать в проектах узлы с функцией физического неклонирования; 3) проводить анализ применяемых в проекте IP-модулей с максимальным раскрытием структуры, методов и алгоритмов обеспечения тестового покрытия; 4) предусматривать в проектах разработку специальных тестовых наборов и методов их генерации на этапе проектирования функций с целью обнаружения вредоносных узлов и программ как внутри ядер СнК, так и на уровне системных шин; 5) разрабатывать на этапе проектирования и применять при тестах методики специальных аппаратных измерений параметров изготовленных схем и анализа их результатов, в частности, по данным измерений задержек распространения сигналов и/или токов потребления шин.

Ключевые слова: тестопригодное проектирование, аппаратные закладки/трояны, верификация проекта ИС, тестовые покрытия, узлы самотестирования.

Introduction

Despite numerous procedures of verification of an IC project, chips that have already been manufactured may contain defects that disrupt its performance. A breach of functional specifications may be due to both objective factors, such as defects in raw materials or fluctuations in technological modes, and to subjective ones, intentional changes (hardware

Trojans). Verification of IC after its manufacture is a complex and expensive procedure that requires the solution of a whole range of engineering tasks. The contemporary approach to IC design is based on the concept of embedding additional components into the project. They are specifically designed to check VLSI for defects. Such design methodology with the possibility of testing or designing for the implementation of controllability (Design for Testability, DFT) is currently an integral part of all commercial integrated circuit projects, such as microprocessors, systems on chip or systems in package [1–3].

Design for testability methods

Any DFT project is based on two components: 1) implementation of the necessary links (connections or circuits) inside the IC to ensure complex effective testing and 2) application of test templates (test vectors), which are specially designed sets of effects on IC inputs and the adequate expected sets of signals at the outputs.

According to the generally accepted classification, performance tests of the finished ICs are divided into: 1) diagnostic, when the developer performs a targeted search for a defective node; 2) functional, determining compliance with the specification stated in the technical specification; 3) parametric, designed to test certain parameters. These parameters can be, inter alia, maximum clock-rate, immunity to noise, temperature, etc. An integral part of testing is specialized automated testing equipment, the cost of which is rather high.

While implementing DFT strategy, one should consider that the test covering, which provides for the enumeration of all possible combinations of input signals, considering VLSI of the microprocessor as a serial device with a set of output statuses determined by the inputs and internal statuses (Mealy machine) is almost impossible, as it will require resources impractical from the technical point of view. The following two circumstances provide guiding ideas for the process of the combinatorial circuit tests design: 1) optimization of the test covering volume at the level of 95–99%, and 2) the impact of one defect can manifest in the whole range of input signals, so one test pattern is enough to identify a specific defect, while all the others detecting the same failure are redundant.

When testing the sequential circuits, the number of required input test vectors increases significantly due to the fact that before applying a particular effect, firstly, it is necessary to bring circuits to a certain initial condition, and secondly, to ensure the transfer of the circuit response to these patterns to one of the outputs. Accordingly, while implementing the DFT concept, it is necessary to analyze the controllability and observability of specific project components.

Since the number of internal statuses of a circuit can be very large, the number of input vectors required to test only one specific sequential circuit error becomes unacceptably large. As a result, the original (special, ad hoc) methods can be applied in the design process. The following are typical examples:

1) Introduction of additional hardware into the circuit. This facilitates the testing, but produces no effect on the functional features of the circuit.

2) Introduction of additional inputs and outputs and adding test points into the circuit. They serve for the testing process implementation.

3) Partitioning of large finite state automation.

4) Introduction of special test buses.

In any case, the effectiveness of such methods depends on the subjective properties of the developer, inter alia, his qualifications and experience, which cannot be taken into account in

the design automation process. Therefore, the following two common unified methods (e.g., see [3]) are integrated and applied in contemporary VLSI CAD systems:

1) Testing based on scanning (boundary scan), when the feedback loops break in the process of testing, and the sequential circuit is converted into a combinatorial one, and peripheral scanning of the circuit is being performed.

2) Built-in self-test (BIST), when modules are embedded into the integrated circuit, providing the self-test opportunity without the application of external templates or with a minimum number of them (the self-control concept).

The contemporary design implementation with a sequential scanning for the first time assumes that the circuit registers are modified so that, in addition to the normal operation mode in the test mode, they are sequentially connected and form a sequential shift register. A simple example illustrating this approach is shown in Fig. 1.

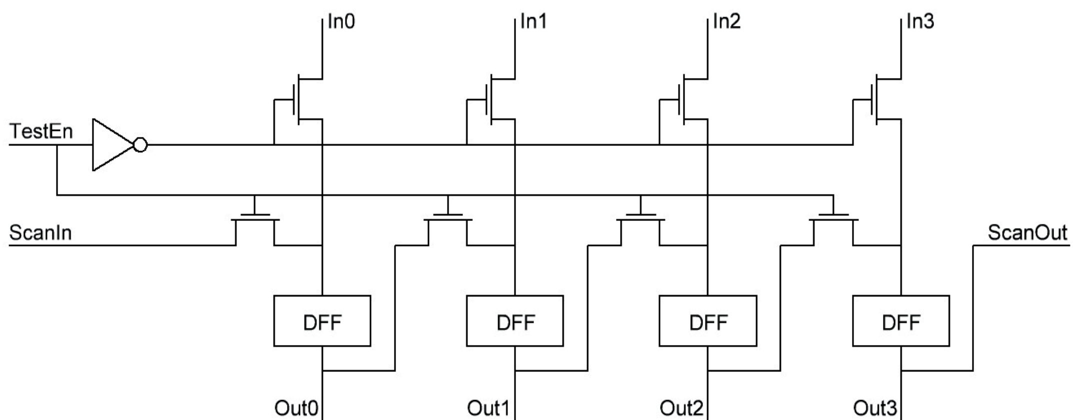

Fig. 1. Diagram of a 4-bit register with a sequential scan chain.

When the «Test» signal level is low, the circuit is in the normal operation mode. In the test mode, «ScanIn» input is activated, and the registers are connected into the scan chain so that the 4-bit register output is connected to the output branching logic and is duplicated at «ScanOut»output, which is in turn connected to «ScanIn» input of the adjacent register.

The most common and technically complete solution of the sequential scanning is the status scan method (Level-Sensitive Scan Design – LSSD), the main idea of which is to use the shift register latch (SRL), the operation of which is shown in Fig. 2.

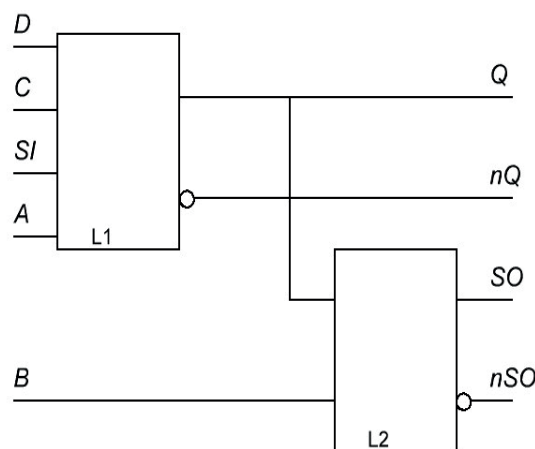

Fig. 2. Shift Register Latch.

The circuit consists of two latches, and the second one is used only when scanning. In the normal mode, A and B inputs are at low level and D, C and Q signals form data inputs, clocking and output, respectively. In the scan mode, the clock signal is generated by the low C level, SI is the input, and SO is the output, while A and B operate as two-phase clock signals of the test mode.

LSSD method is widely applied in the test automation programs. IEEE 1149 standard is currently the regulatory document for the organization of scanning systems.

The self-control methodology is an alternative to scanning, which is increasingly applied in the automation of VLSI and ICS design. In this case, the circuit itself generates tests and checks their results. Tests can be exhaustive, i.e., detecting all possible failures, which requires a lot of resources. In practice, a random subset is formed from the whole range of possible input signals.

Analysis and model description of possible circuit faults always comes before the automated development of test codes. In the most critical cases, the standard models of short-circuit defects such as stuck-at-zero (sa0) and stuck-at-one (sa1) can be added to the fault models of such types as «permanently open transistor» or «open circuit» (stuck-at-open) and stuck-at-short. However, the addition of these faults requires proper justification, as it leads to a significant complication in the process of generating test codes, while many faults of this type can be replaced by sa1 or sa0.

In the process of automatic generation of test codes, a minimum amount of test vectors is set. It is usually assigned on a random basis, but covering most of the errors in the circuit. Determining the minimum amount of test vectors is based on the accepted fault model and special algorithms and is a complex technical task, which belongs to one of the intensive areas of development in the field of computer-aided design and is solved by CAD developers in a different manner. As a standard example illustrating the research nature of such activities one can mention the work [4] performed by the MIREA – Russian Technological University. During the work, inter alia, a software tool for automating the methods of the test systems building was developed on the basis of the proposed methods of dynamic verification of system exchange modules and universal verification technology. This allowed more than 30% reduction of the labor costs for the development of test systems for dynamic verification of system exchange modules in the course of development of the domestic microprocessors of a new generation [5].

The example of a pseudorandom generator of a subset of input signals is the circuit of N sequentially connected one-bit registers with an EXCLUSIVE OR element connected to two of them, the output of which is supplied to the input of the first register. Thus, Linear Feedback Shift Register – LFSR is formed, which runs through $2^N–1$ statuses, which is a pseudorandom sequence, and the initial register loading determines which pseudorandom sequence will be formed.

The response analyzer is a compare circuit with possible statuses, the sets of which are stored inside the circuit memory. To reduce service costs a response compression method is applied before comparison. This approach is called a signature analysis, because in this case the response analyzer consists of the output dynamic compression circuit of the tested circuit and the comparator. The simplest single-bit stream signature generator counting the number of transitions from zero to one and from one to zero is presented in Fig. 3.

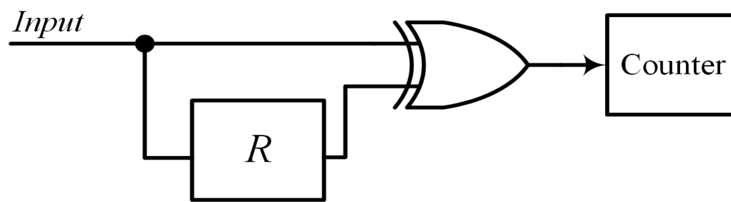

Fig. 3. Example of the circuit signature generator.

Matching of the received signature with the predetermined one can be considered as a successful passing of the test, since the probability of obtaining a signature match with an erroneous sequence of transitions is small.

The circuit combining the modules of test code generation and signature analysis is a modification of the self-testing methodology. In this case, the EXCLUSIVE OR operation is applied to the output word and LFSR content, forming a test signature at the end of the test sequence. In case of such activation, by means of the actuating signals the circuit can be switched from the test configuration to the shift register or to the scanning shift register. This method is called the built-in logic block observation – BILBO. The three-bit BILBO controller circuit is shown in table and Fig. 4.

Three-bit BILBO controller operating modes

B0	B1	State
1	1	Normal Operation
0	0	Scan
1	0	Pattern Generation or Analysis
0	1	Reset

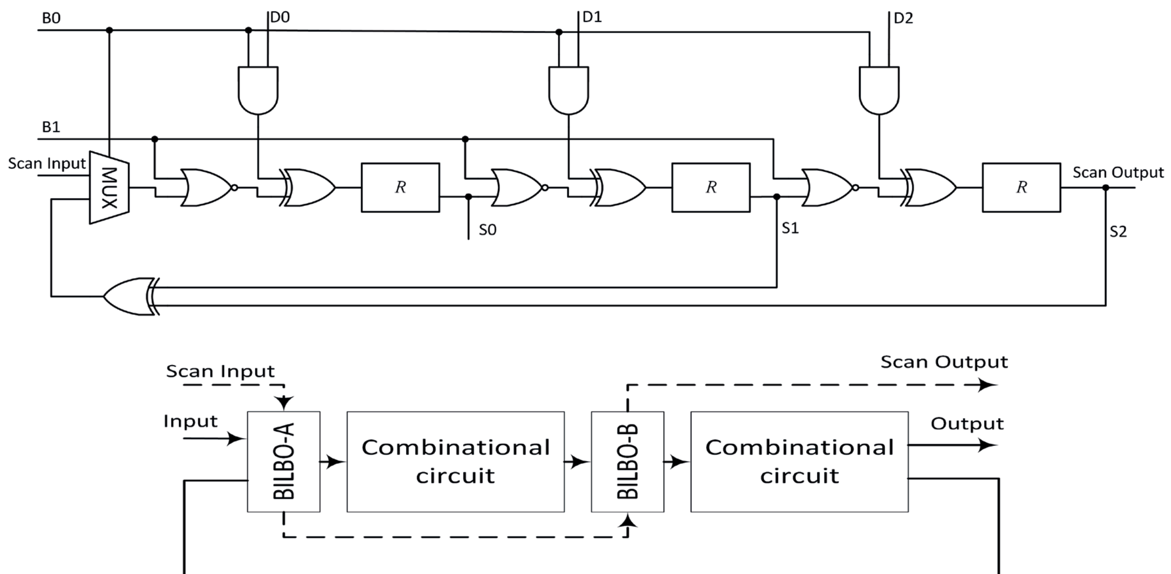

Fig. 4. Three-bit BILBO controller circuit and its operating modes.

Before the test some number is loaded into the register A of the circuit that initializes the register B. The register A operates in the mode of generating pseudorandom codes, while the register B, in the signature analysis mode. The signature is read from B upon the completion of the test sequence transfer.

Difficulties of determining the project malfunctions

Contemporary VLSI can not only be systems on chip (SoC), but also systems in package (SiP). In this case, due to the fact that each chip can have its own testing system, the entire assembly test can only be performed using a built-in self-test. ICS test concept involves the inclusion of test modules into the configurable interface nodes connecting the chips and providing synchronization and data exchange. Development of ICS design and verification ideology is, inter alia, represented through an increase in the level of project abstraction aimed at the application of higher-level languages in CAD [6].

Despite numerous procedures of IC project verification, chips that have already been manufactured may contain defects that disrupt its performance. A breach of functional specifications may be due to both objective factors, such as defects in raw materials or fluctuations in technological modes, and subjective ones, intentional changes (hardware Trojans). Verification of IC after its manufacture is a complex and expensive procedure that requires the solution of a whole range of engineering tasks. The detailed analysis of possible threats caused by the violation of functions of the executed projects is represented in the monograph [7].

Protection of integrated circuits and systems based on them, which is aimed at identifying and eliminating unnecessary interventions into the design solutions, should be implemented through various methods. In particular: 1) at the level of standard project library elements testing; 2) by means of IC boundary scan systems; 3) by means of an appropriate upgrade of vulnerable software. Detailed studies of this task and analysis of their results show that the development of trusted intelligent data processing systems is a complex scientific and technical task that requires thorough analysis and research to develop grounded technical solutions at all the design stages. In the microelectronics CAD market, the testing solutions are mainly represented by major DFT suppliers in the field (Cadence Design Systems, Mentor Graphics, Synopsys). These packages vary significantly in terms of technology, design overhead costs, design rules, and ease of use.

It is obligatory for the structure of contemporary CAD to contain 1) modules for checking the implementation of design rules (design Rules Check, DRC) set by the manufacturer and 2) modules for checking the compliance of the pattern of the obtained topology and functional diagram of the device (Layout Versus Schematic, LVS). The correct application of the rules and LVS tools in principle provides for conducting the analysis of intentional or unintentional errors in the chip topology after its manufacture. The set of standard library elements (valves, logic cells, triggers, etc.) serves the basis of any project. Thus, conformance testing of the behavioral description and the results of the designed operations is the necessary stage of IC. Such testing is carried out by modeling in specialized tools of different CAD manufacturers (Cadence Design Systems, Synopsys and Mentor Graphics) and comparative analysis of the results. The developed method of conformance testing of topology and the electrical circuit was checked using test chips. The method consists of the following procedures: recognizing circuit elements by a topological pattern; restoring links between the elements; forming chains of connection (net list) matching the real electric circuit; comparing the extracted net list with the original one.

Recognition of circuit elements by topological pattern is based on the preliminary geometric processing of the topology pattern for layer-by-layer coding of the contours of all elements of the

topology and subsequent application of logical operations with the figures in order to identify transistors, interconnects and other circuit elements. E.g.: «polysilicon layer» – AND operation – «diffusion layer» = «transistor channel»; «diffusion layer» – AND operation – «metal layer»– AND operation – «contact layer» = «transistor output».

Restoration of links between the elements is carried out by monitoring the routes of the identified interconnects connecting the outputs of the identified elements with subsequent conformance testing of the topology and the electric circuit. The method analysis demonstrated that it is more effective to compare the connections at the logical level, not at the level of transistors.

The report on testing results contains: information about the match of the output data of the Spectre and Verilog simulation; check for compliance with the design rules of the manufacturer; check for errors in LVS report. Contemporary CAD tools provide the opportunity for detailed research and analysis of a particular element operation. Cadence NC-Verilog simulator combined with SimVision visualization tool can serve as an example, as well as Spectre MDL and Cadence ViVA.

Special hardware protection modules built into IC, the control of which will allow the developer to identify possible bugs and breaches that can lead to operation failures and correct them, serve as an additional measure of protection of IC projects manufactured by foreign companies. The detailed development of such modules should be project-specific and is a subject of separate studies. IEEE Std 1500 standard is the basis of such methods, according to which each core of the designed system on chip should have a test harnessing. A detailed description of hardware and software methods to counter malicious inclusions into chips and design for IC security purposes is given in the papers [7, 8].

A significant addition to CAD tools providing for verification and even correction of the already manufactured chips is represented by the methods for analyzing IC topology. The methods are based on the technology of the ion beams preparation. Examples of such studies are presented in publications [9].

Thus, in terms of the analysis of possible breaches of project integrity and development of the requirement to the description and structure of models of standard digital circuits and complex functional modules, one can make the following conclusions.

Contemporary VLSI CAD applications provide for achieving the full covering of the project, but the resources required for this purpose can be non-optimal, both in terms of time required and the cost of test equipment. As a result the control of the functional integrity of the project is possible with some degree of probability.

The built-in self-testing units are usually generated automatically in the form of RTL code or part of a netlist and are difficult to distinguish from units also included in the project, but performing any other function, inter alia, a malicious one. The correctly implemented means of scan testing and built-in self-testing can confirm only the completeness of the project functionality, but not redundancy, especially if the redundant functions are not activated by digital signals of the circuit, or the results of its operation do not affect the basic functionality of the circuit.

The test circuits generating means, both scanning circuits and built-in self-testing can pose threats to information security, since VLSI CAD software products are proprietary, and their source code is closed, and control of the project changes made by the test generation programs is performed by these means.

It is essential that in the standard design flow, usually provided by the manufacturer in the form of PDK, standard testing tools are not designed to control the topological integrity of the

project. Formal verification of the project, both before and after the implementation of testing circuits, for the presence of changes in the functionality of the project itself may not reveal the breach done, especially if the formal verification is carried out by means of CAD of the same manufacturer as CAD for the testing circuits' generation.

As long as all contemporary developments of domestic VLSI are manufactured with varying degrees of the foreign companies involvement, a prerequisite for ensuring the reliable operation of these products is the development and implementation of special organizational and technical measures aimed at analysis, identification and elimination of possible distortion of projects in the form of software and/or instrument bugs directly at the design stage, inter alia, in the form of nodes complementing scanning and self-testing modules. Such measures, inter alia, are:

– Analysis of the libraries of standard elements used in the project with complete disclosure of their specifications, i.e., descriptions at the topology level, circuit diagrams and methods of checking design and verification rules.

– Creation on the basis of libraries of standard elements in models and programs of the analysis of special nodes with a function of physical non-cloning, serving as standards for comparison with results of tests and the manufactured chip.

– Analysis of IP modules used in the project with the maximum disclosure of the internal structure, and especially the methods and algorithms for providing test covering and circuits for peripheral scanning and/or built-in self-testing nodes.

– Introduction of special modules (IP-infrastructure Security-IIPS [10]) into the project, which are complex functional units specifically designed to check for protection against possible bugs (hardware Trojans).

– Development of special test kits and methods of their generation at the function design stage to detect malicious nodes and programs both inside SoC cores and at the level of system buses.

– Development of methods for special hardware measurements of the manufactured circuits parameters and analysis of their results, inter alia, according to the measurement of delays in signal propagation and/or bus consumption currents.

Conclusions

Specific examples show that the protection of integrated circuits and systems based on them, the purpose of which is to identify and eliminate undesirable interference in design solutions, should be implemented by various methods: at the level of standard project library elements testing; by means of IC boundary scan systems and by means of appropriate upgrade of vulnerable software. Performed studies and analysis of their results show that development of trusted intelligent data processing systems is a complex scientific and technical task that requires thorough analysis and research to develop grounded technical solutions at all the design stages.

Acknowledgments

The work was carried out within the framework of the state order with the support of the Ministry of Science and Higher Education of the Russian Federation (project № 8.5098.2017/8.9).

Благодарности

Работа выполнена в рамках государственного заказа при поддержке Министерства науки и высшего образования Российской Федерации (проект № 8.5098.2017/8.9).

References:

1. Wong B.P., Mittal A., Starr G. Nano-CMOS circuit and physical design. Moscow: Tekhnosfera Publ., 2014. 432 p., (in Russ.).

2. Wang L.T., Chang Y.W., Cheng K.T.T. Electronic design automation: Synthesis, verification, and test. New York: Morgan Kaufmann, 2009. 971 p.

3. Rabai Jean M., Chandrakasan A., Nikolic B. Digital integrated circuits. Design methodology: 2nd ed. Moscow: Publishing House Williams, 2016. 912 p., (in Russ.).

4. Stotland I.A. An approach to simulation-based verification of interconnection modules of microprocessor computer systems. *Nauchno-tekhnicheskij vestnik Povolzh'ya* [Scientific and Technical Volga region Bulletin]. 2012; (4):191-196, (in Russ.).

5. Bobkov S.G. Development of high-performance trusted computing systems based on KOMDIV microprocessors. *Nanoindustiya* [Nanoindustry]. 2017; S(74):14-17, (in Russ.).

6. Gubarev V.A., Voronkov S.O., Antufeev G.V. System modeling of digital devices in the style of block design. *Voprosy radioelektroniki. Seriya «Elektronnaya vychislitel'naya tekhnika» (EVT)* [Issues of Radio Electronics. Series: Electronic Computing]. 2012; 2:138-146, (in Russ.).

7. Belous A.I., Solodukha V.A., Shvedov S.V. Software and hardware Trojans-ways of implementation and methods of counteraction. The first technical encyclopedia: in 2 v. Ed. A.I. Bilous. Moscow: Tekhnosfera Publ., 2018. 1318 p., (in Russ.).

8. IEEE 1500 Embedded Core Test. URL: http://grouper.ieee.org/groups/1500.

9. Shnyakin A.A., Pevtsov E.Ph., Demenkova T.A. Improving the functionality of the semiconductor matrix receiver of optical radiation. In: Proceed. VII Int. Conf. «Modern Technologies for Non-Destructive Testing» IOP Conf. Series: Materials Science and Engineering. IOP Publishing. 2018; 457: 012015. https://doi.org/10.1088/1757-899X/457/1/012015

Литература:

1. Вонг Б.П. Миттал А., Старр Г. Нано-КМОП-схемы и проектирование на физическом уровне. М.: Техносфера, 2014. 432 с.

2. Wang L.T., Chang Y.W., Cheng K.T.T. Electronic design automation: Synthesis, verification, and test.New York: Morgan Kaufmann, 2009. 971 p.

3. Рабаи Жан М., Чандракасан А., Николич Б. Цифровые интегральные схемы. Методология проектирования. 2-е изд.: Пер. с англ. М.: ООО «И.Д. Вильямс», 2016. 912 с.

4. Стотланд И.А. Метод динамической верификации модулей системного обмена микропроцессорных вычислительных комплексов // Научно-технический вестник Поволжья. 2012. № 4. С. 191–196.

5. Бобков С.Г. Создание высокопроизводительных доверенных систем на базе микропроцессоров с архитектурой КОМДИВ // Наноиндустрия. 2017. № S(74). С. 14–17.

6. Губарев В.А., Воронков С.О., Антюфеев Г.В. Системное моделирование цифровых устройств в стиле блочного проектирования СБИС СнК // Вопросы радиоэлектроники. Серия «Электронная вычислительная техника (ЭВТ)». 2012. Вып. 2. С. 138–146.

7. Белоус А.И., Солодуха В.А., Шведов С.В. Программные и аппаратные трояны – способы внедрения и методы противодействия. Первая техническая энциклопедия: в 2-х кн. / Под. общ. ред. А.И. Белоуса. М.: Техносфера, 2018. 1318 с.

8. IEEE 1500 Embedded Core Test. URL: http://grouper.ieee.org/groups/1500 (дата обращения 01.07.2019).

9. Shnyakin A.A., Pevtsov E.Ph., Demenkova T.A. Improving the functionality of the semiconductor matrix receiver of optical radiation // In: Proceed. VII Int. Conf. «Modern Technologies for Non-Destructive Testing» IOP Conf. Series: Materials Science and Engineering. IOP Publishing. 2018. V. 457. P. 012015. https://doi.org/10.1088/1757-899X/457/1/012015

About the authors:

Evgeny Ph. Pevtsov, Cand. of Sci. (Engineering), Associate Professor, Director of the Center for Design of Integrated Circuits, Devices of Nanoelectronics and Microsystems, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow 119454, Russia). Scopus Author ID 6602652601, ResearcherID M-2709-2016, https://orcid.org/0000-0001-6264-1231.

Tatiana A. Demenkova, Cand. of Sci. (Engineering), Associate Professor of the Chair of Computer Technology, Institute of Information Technologies, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow 119454, Russia). Scopus author ID 57192958412, https://orcid.org/ 0000-0003-3519-6683.

Alexander A. Shnyakin, Programmer of the Center for Design of Integrated Circuits, Devices of Nanoelectronics and Microsystems, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow 119454, Russia).

Об авторах:

Певцов Евгений Филиппович, кандидат технических наук, доцент, директор Центра проектирования интегральных схем, устройств наноэлектроники и микросистем ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). Scopus Author ID 6602652601, ResearcherID M-2709-2016, https://orcid.org/0000-0001-6264-1231.

Деменкова Татьяна Александровна, кандидат технических наук, доцент кафедры вычислительной техники Института информационных технологий ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). Scopus Author ID 57192958412, https://orcid.org/ 0000-0003-3519-6683.

Шнякин Александр Андреевич, программист Центра проектирования интегральных схем, устройств наноэлектроники и микросистем ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78).

For citation: Pevtsov E.Ph., Demenkova T.A., Shnyakin A.A. Design for testability of integrated circuits and project protection difficulties. *Rossiiskii tekhnologicheskii zhurnal* = Russian Technological Journal. 2019; 7(4):60-70, https://doi.org/10.32362/2500-316X-2019-7-4-60-70

Для цитирования: Pevtsov E.Ph., Demenkova T.A., Shnyakin A.A. Design for testability of integrated circuits and project protection difficulties // Российский технологический журнал. 2019. Т. 7. № 4. С. 60–70. https://doi.org/10.32362/2500-316X-2019-7-4-60-70