DOI: https://doi.org/10.32836/2521-6643-2018-1-56-5
УДК 004.315

В. В. Антонюк, старший викладач кафедри комп'ютерних інтелектуальних систем та мереж Одеського національного політехнічного університету
М. О. Дрозд, кандидат технічних наук, старший викладач кафедри інформаційних систем Одеського національного політехнічного університету
О. В. Дрозд, доктор технічних наук, професор кафедри комп'ютерних інтелектуальних систем та мереж Одеського національного політехнічного університету
Л. В. Кабак, кандидат технічних наук, доцент кафедри інформаційних систем та технологій Університету митної справи та фінансів

КОНТРОЛЕПРИДАТНІСТЬ FPGA-ПРОЕКТІВ ЗА РОЗСІЮВАНОЮ ПОТУЖНІСТЮ

Розглянуто розвиток контролепридатності схем для цифрових компонентів систем критичного застосування. Наголошено на важливості контролепридатності для забезпечення функціональної безпеки систем та їхніх компонентів у частині критичних додатків. Аргументовано потребу подальшого розвитку контролепридатності за межі логічної форми. Запропоновано розвиток контролепридатності цифрових компонентів за ознакою розсіюваної потужності. Отримано формулу для оцінювання контролепридатності схем за розсіюваною потужністю для FPGA-проектів. Проведено експерименти, виконано розрахунки контролепридатності схем за розсіюваною потужністю для матричних помножувачів, що імплементовані в FPGA-проекти.

Ключові слова: *система критичного застосування; цифровий компонент; FPGA-проект; загальний сигнал; прихована несправність; контролепридатність; розсіювана потужність.*

Рассмотрено развитие контролепригодности схем для цифровых компонентов систем критического применения. Отмечено важность контролепригодности для обеспечения функциональной безопасности систем и их компонентов в области критических приложений. Аргументована необхо-

димость дальнейшего развития контролепригодности за пределы логической формы. Предлагается развитие контролепригодности цифровых компонентов по признаку рассеиваемой мощности. Получена формула для оценки контролепригодности схем по рассеиваемой мощности для FPGA-проектов. Проведены эксперименты и выполнены расчеты контролепригодности схем по рассеиваемой мощности для матричных умножителей, имплементированных в FPGA проекты.

Ключевые слова: *система критического применения; цифровой компонент; FPGA-проект; общий сигнал; скрытая неисправность; контролепригодность; рассеиваемая мощность.*

The issue is devoted to development of a checkability of the circuits for digital components of instrumentation and control safety-related systems, which operate objects of the increased risk, such as power grids and power plants, high-speed transport and aircraft. Importance of a checkability of the circuits for ensuring functional safety of systems and their components in the field of critical applications where the operating mode is divided into normal and an emergency is noted. In these conditions, there is a problem of the hidden faults which can be accumulated throughout the long normal mode and reduce fault tolerance of schemes in the most responsible emergency operation. The most studied logical form of a checkability of the digital circuits determines efficiency of on-line testing of the digital components. Need of further development of a checkability of the circuits out of limits of its logical form as it does not solve a problem of the common signals, such as signals of reset and synchronization signals is shown. The faults arising in chains of the common signals can remain hidden, by blocking schemes of on-line testing is able which demonstrates the correct functioning of on-line testing means. For the solution of this problem, development of a checkability of the digital components on the basis of the power-dissipation is offered. The formula for analytical assessment of a checkability of the circuits by the power-dissipation for FPGA projects is received. The experiments directed to studying of a checkability of the digital circuits by the power-dissipation for the iterative array multipliers implemented in FPGA projects with the help of a CAD of Quartus Prime 17.1 Lite Edition (Intel of FPGA) are made. By means of the PowerPlay Power Analyzer utility, values of the power-dissipation for all FPGA project and for its input/output system and also dynamic and static components of the power-dissipation in core are received. On these data obtained at various activity of the input signals, calculations of a checkability of the circuits for the power-dissipation of iterative array multipliers with various word size from 16 to 64 bits are executed.

Key words: *critical application system; digital component; FPGA-project; common signal; hidden fault; checkability; power-dissipation.*

Постановка проблеми. Системи критичного застосування – це розвиток комп'ютерних систем у напрямі керування об'єктами підвищеного ризику, до яких належать енергомережі, електростанції, швидкісний наземний і повітряний транспорт тощо [1; 2]. Керування спрямоване на забезпечення функціональної безпеки та системи, а також об'єкта для запобігання виникненню аварій і зниження їхніх наслідків. Удосконалення об'єктів за потужністю спричиняє їхнє ускладнення, а зростання потужності разом зі складністю та кількістю підвищують критичність очікуваних наслідків аварій. За таких обставин стримування ризиків потребує зниження ймовірності виникнення аварій, що стосується насамперед виконання вимог міжнародних стандартів щодо систем критичного застосування.

За цими стандартами основою в забезпеченні функціональної безпеки систем критичного застосування визначається використання відмовостійких рішень, що поширюються і на систему, і на її компоненти. Утім, на практиці використання відмовостійких рішень не дає повної впевненості щодо забезпечення функціональної безпеки, це засвідчує наявність імітаційних режимів, які для перевірки системи відтворюють умови аварії, що не раз призводили до аварійних наслідків.

Дійсно, системи критичного застосування не гарантують і не можуть гарантувати функціональну безпеку ані власну, ані об'єктів керування лише за рахунок відмовостійких рішень. Такі рішення стають достатніми тільки для контролепридатних систем та їхніх компонентів, оскільки за браку контролепридатності кількість відмов завжди може перевищити закладену відмовостійкість рішення. Використання небезпечних імітаційних режимів вказує на наявність проблеми недостатньої контролепридатності систем критичного застосування та їхніх компонентів і потребу проведення досліджень у напрямі її підвищення.

Аналіз останніх досліджень і публікацій. Особливістю систем критичного застосування є їхня дворежимність: вони проектуються для роботи в нормальному й аварійному режимах. Вимоги до функціональної безпеки систем критичного застосування регламентуються стандартом IEC 61508 щодо електричних, електронних і програмованих компонентів [3]. Він є базовим для стандартів з функціональної безпеки у різних галузях, зокрема EN 50126 для залізничного транспорту й IEC 61513 для атомних електростанцій [4; 5].

Зазвичай контролепридатність розуміють як її логічну форму, тобто придатність до виявлення несправностей за помилками результату. Контролепридатність цифрових схем у тестовому режимі – тестопридатність, тобто придатність схем до написання для них тестів з виявлення несправностей. Вона структурна, бо повністю визначається самою схемою. В робочому режимі контролепридатність стає структурно-функціональною, оскільки залежить також від вхідних даних. У системах критичного застосування цифрові

компоненти працюють у нормальному та аварійному режимах зазвичай на різних вхідних даних. Це робить структурно-функціональну контролепридатність також дворежимною, тобто різною в нормальному та аварійному режимах [6]. Як наслідок, виникає проблема прихованих несправностей, що можуть накопичуватись упродовж довготривалого нормального режиму та виявлятись в аварійному режимі зниженням відмовостійкості схемних рішень [7].

На практиці проблема прихованих несправностей розв'язується шляхом використання небезпечних імітаційних режимів, що вже мають певну історію несанкціонованого втручання людського фактора, та несправністю [8]. Імітація аварійних умов, як правило, потребує блокування засобів аварійного захисту, що стало однією з причин Чорнобильської катастрофи.

Для розв'язання проблеми прихованих несправностей запропоновано методи підвищення контролепридатності цифрових компонентів у нормальному режимі та вирівнювання контролепридатності обох режимів, що має певні наслідки [9]. Водночас обмеження розвитку контролепридатності схем тільки її логічною формою стикається з проблемами робочого діагностування, можливості якого вона визначає. До таких проблем належить проблема загальних сигналів, зокрема сигналів скидання та синхронізації. Загальні сигнали можуть блокувати не тільки роботу цифрових компонентів, але й засобів робочого діагностування, причому у стані, що ідентифікує правильне функціонування схем. Ці несправності також можна зарахувати до множини прихованих, однак їхньою особливістю є прихованість у виявленому стані.

На контролепридатність схем також суттєво впливають особливості цифрових компонентів. Високі технології, що задіяні в критичних ділянках застосування, визначають для їхньої розробки сучасні системи проектування, зокрема проектування на FPGA (Field Programmable Gate Array) [10; 11].

Мета статті – розвиток контролепридатності компонентів за межі її логічної форми на підставі можливостей, які надаються FPGA-проектуванням і можуть слугувати для оцінювання придатності схеми до контролю за розсіюваною потужністю. Запропоновано низку експериментів з FPGA-проектами щодо визначення їхньої контролепридатності за потужністю, що має ними розсіюватися за правильного функціонування.

Виклад основного матеріалу. Контролепридатність схеми за розсіюваною потужністю можна визначити відношенням обсягів діапазонів значень розсіюваної потужності за межами можливого за умов правильного функціонування до загального обсягу, що включає можливі та неможливі значення. Діапазон можливих значень виокремлює в загальному діапазоні два діапазони неможливих значень: нижній (від нуля до мінімального можливого значення) та верхній (від максимального можливого значення до межі вимірювання). Для цих діапазонів неможливих значень відповідно визначається нижня та верхня контролепридатність схеми.

Нижня контролепридатність корисна для виявлення несправностей, що значно зменшують розсіювану потужність, наприклад, призводять до блокування тактових сигналів, а верхня контролепридатність – навпаки, суттєво збільшує розсіювану потужність, що може трапитись за умови короткого замикання.

Далі розглядається нижня контролепридатність, яка дає можливість виявляти несправності, що спотворюють загальні сигнали, внаслідок чого зменшується динамічний складник розсіюваної потужності. Тому нижню контролепридатність можна визначити за мінімальним відношенням обсягів діапазонів мінімального $N_{\mathrm{D\,MIN}}$ і максимального $N_{\mathrm{D\,MAX}}$ значень динамічного складника розсіюваної потужності, тобто за такою формулою: $K_H = \mathrm{MIN}(N_{\mathrm{D\,MIN}} / N_{\mathrm{D\,MAX}})$.

Контролепридатність K_H схеми залежить від умов її проектування. Розглянуто систему автоматизованого проектування Quartus Prime 17.1 Lite Edition від Intel FPGA [12].

Для моделювання параметрів енергоспоживання та розсіюваної потужності використовується утиліта PowerPlay Power Analyzer, що входить до складу Quartus Prime [13].

Контролепридатність K_H визначається для схем матричних помножувачів двійкових чисел за результатами моделювання, що проводилось на FPGA Intel Max 10 10M50DAF672I7G. У цій програмованій логічній інтегральній схемі (ПЛІС) розміщено 288 9-бітних апаратних блоків множення, котрі, крім власних помножувачів, містять буферні вхідні регістри операндів і вихідний регістр результату [14].

Апаратні блоки множення в Quartus Prime проектуються на основі інтелектуального модуля (Intellectual Property Core – IP-Core) помножувача LPM_MULT із бібліотеки параметризованих модулів (Library of Parameterized modules – LPM), що постачається разом із Quartus Prime [15].

Під час введення IP-Core до проекту майстер налаштування дає можливість задати основні характеристики помножувача (розрядність операндів, знакова або беззнакова операція, наявність або брак буферизації операндів і результату), що відповідають характеристикам убудованих блоків множення.

У результаті моделювання оцінюються значення загальної розсіюваної потужності ПЛІС N, системи введення/виведення N_{IO}, а також динамічного N_{D} і статичного N_{S} складників ядра ПЛІС.

Оскільки контролепридатність визначається через посередників, слід зважати на похибки вимірювання й оцінювання. Для утиліти PowerPlay Power Analyzer похибки оцінювання становлять 5 % в один бік зменшення, або збільшення – 2,5 %. Теплові датчики також працюють на рівні похибки 5 %. Тоді мінімальне значення знаходимо за формулою:

$$N_{\mathrm{D\,MIN}} = N_{\mathrm{D}} - 0.025\, N_{\mathrm{D}}.$$

Максимальне значення $N_{\text{D MAX}}$ визначається за вимірюванням N загальної розсіюваної потужності ПЛІС під час розрахунку оцінених значень розсіюваної потужності системи введення/виведення N_{IO}, а також статичного складника ядра N_{S} та їхніх похибок за формулою:

$$N_{\text{D MAX}} = N - N_{\text{I/O}} - N_{\text{S}} + 0.025\,N + 0.025\,N_{\text{I/O}} + 0.025\,N_{\text{S}},$$

або за умови, що $N - N_{\text{I/O}} - N_{\text{S}} = N_{\text{D}}$,

$$N_{\text{D MAX}} = N_{\text{D}} + 0.025\,N + 0.025\,N_{\text{I/O}} + 0.025\,N_{\text{S}}.$$

Для знаходження мінімального значення MIN($N_{\text{D MIN}}$ /$N_{\text{D MAX}}$) необхідно зважати на коливання значень $N_{\text{D MIN}}$ і $N_{\text{D MAX}}$ залежно від активності сигналів, які подаються на входи до схеми, тобто моделювання слід виконувати за різної активності вхідних сигналів і далі обрати результати з мінімальним значенням обчисленої контролепридатності.

У ході експериментів було реалізовано FPGA-проекти знакових помножувачів із регістрами операндів і результату та розрядністю n = 16, 32, 48, 64. За допомогою утиліти PowerPlay Power Analyzer активність A вхідних сигналів задавалася від 0 до 100 % щодо сигналу синхронізації регістрів помножувача з кроком збільшення на 12,5 %.

Результати моделювання та розрахунку контролепридатності помножувачів подано в табл. 1–4 відповідно, якщо n – від 16 до 64 бітів.

Таблиця 1

Результати оцінювання контролепридатності помножувача, n = 16

A, %	N_D, mW	N_S, mW	N_{IO}, mW	N, mW	K_H, %
0	7,62	89,94	73,07	170,63	46,55
12,5	8,46	89,95	74,42	172,83	48.84
25	9,31	89,95	75,76	175,02	50.91
37,5	10,15	89,96	77,11	177,22	52.76
50	10,99	89,96	78,46	179,41	54.43
62,5	11,83	89,97	79,81	181,61	55.95
75	12,67	89,98	81,16	183,80	57.34
87,5	13,51	89,98	82,50	186,00	58.62
100	14,36	89,99	83,85	188,19	59.81

Таблиця 2

Результати оцінювання контролепридатності помножувача, n = 32

A, %	N_D, mW	N_S, mW	N_{IO}, mW	N, mW	K_H, %
0	15,83	90,17	153,70	259,71	54,31
12,5	19,04	90,19	156,40	265,63	58.29
25	22,25	90,21	159,10	271,55	61.51
37,5	25,45	90,22	161,79	277,47	64.14
50	28,66	90,24	164,49	283,38	66.35
62,5	31,86	90,25	167,18	289,30	68.23
75	35,07	90,27	169,88	295,22	69.85
87,5	38,27	90,28	172,58	301,14	71.25
100	41,48	90,30	175,27	307,05	72.48

Таблиця 3

Результати оцінювання контролепридатності помножувача, n = 48

A, %	N_D, mW	N_S, mW	N_{IO}, mW	N, mW	K_H, %
0	35,38	90,42	225,95	351,75	66,23
12,5	41,49	90,45	230,00	361,93	69.09
25	47,59	90,47	234,04	372,11	71.38
37,5	53,70	90,50	238,08	382,29	73.26
50	59,81	90,53	242,13	392,47	74.82
62,5	65,91	90,56	246,17	402,64	76.15
75	72,02	90,58	250,22	412,82	77.28
87,5	78,13	90,61	254,26	423,00	78.27
100	84,23	90,64	258,31	433,18	79.13

Таблиця 4

Результати оцінювання контролепридатності помножувача, n = 64

A, %	N_D, mW	N_S, mW	N_{IO}, mW	N, mW	K_H, %
0	64,97	90,69	297,99	453,66	73,63
12,5	76,04	90,74	303,38	470,16	75.93
25	87,10	90,78	308,77	486,66	77.73
37,5	98,16	90,83	314,17	503,16	79.18
50	109,23	90,87	319,56	519,66	80.39
62,5	120,29	90,92	324,95	536,16	81.40
75	131,35	90,96	330,34	552,66	82.25
87,5	142,41	91,01	335,74	569,16	82.99
100	153,48	91,05	341,13	585,66	83.63

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. Контролепридатність цифрових компонентів систем критичного застосування – необхідний складник для забезпечення функціональної безпеки не тільки системи, але й об'єкта управління.

Розвиток моделей контролепридатності в її логічній формі від тестопридатності до структурно-функціональної та дворежимної сприяв усвідомленню проблеми прихованих несправностей і визначенню шляхів її розв'язання, покращивши ефективність робочого діагностування цифрових схем.

Водночас логічна форма контролепридатності обмежена у виявленні несправностей загальних сигналів, що можуть блокувати роботу засобів робочого діагностування у стані індикації правильного функціонування. Це потребує розвитку контролепридатності схем в інших формах, зокрема енергетичного складника, за яким найбільш забезпечені засоби (температурні датчики) – це придатність до контролю тепловиділення шляхом вимірювання розсіюваної потужності.

Оцінювання контролепридатності схем за розсіюваною потужністю, проведене для FPGA-проектів з урахуванням сучасних викликів, мають подальший розвиток щодо елементної бази ПЛІС у розробці цифрових компонентів систем критичного застосування.

Експерименти з оцінювання контролепридатності схем за розсіюваною потужністю здійснено на системі автоматизованого проектування Quartus Prime 17.1 Lite Edition (Intel FPGA) з використанням інтелектуального модуля LPM_MULT для низки значень розрядності матричних помножувачів і рівнів активності вхідних сигналів схеми.

Результати моделювання визначили вихідні дані для розрахунку контролепридатності, а саме: значення загальної розсіюваної потужності ПЛІС, її системи введення/виведення та динамічного N_D і статичного N_S складників ядра.

За отриманими результатами контролепридатність схеми оцінюється за мінімальним відношенням мінімального та максимального значень динамічного складника розсіюваної потужності ПЛІС, що визначаються, зважаючи на похибки вимірювання та оцінювання вихідних даних для різних рівнів активності вхідних сигналів.

Обчислені оцінки контролепридатності засвідчують досить високий рівень, який зростає зі збільшенням розрядності помножувачів та активності вхідних сигналів, тобто мінімальні значення контролепридатності відповідають найменшій (нульовій) активності вхідних сигналів, що для розрядності 16, 32, 48 і 64 становить відповідно 46,55 %, 54,31 %, 66,23 % та

73,63 %. Рекомендований рівень активності вхідних сигналів 12,5 % створює для вказаної розрядності матричних помножувачів резерв контролепридатності у 2,29 %, 3,98 %, 2,86 % та 2,30 % відповідно.

Подальші дослідження доцільно спрямувати на розвиток і використання нових форм контролепридатності схем з метою підвищення функціональної безпеки систем критичного застосування.

Список використаних джерел:

1. *Kharchenko V., Gorbenko A., Sklyar V., Phillips C.* Green Computing and Communications in Critical Application Domains: Challenges and Solutions // Digital Technologies: Proceedings of the 9th International Conference, Zhilina, Slovak Republic. 2013. P. 191–197.

2. *Brezhnev E., Kharchenko V.* Approach for formalization of influences in critical infrastructure // Critical Infrastructure Safety and Security (CrISSDESSERT): proceedings of I Int. Workshop, Kirovograd (Ukraine), 10–11 May. 2011. Kirovograd. 2011. P. 216–226.

3. IEC 61508-1:2010. Functional safety of electrical / electronic / programmable electronic safety related systems. Part 1: General requirements. Geneva: International Electrotechnical Commission. 2010.

4. EN 50126 / IEC 62278. Quick Guide to safety Management based on EN 50126 / IEC 62278 // Blogspot. 2008. URL: http://en50126.blogspot.com

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

6. *Drozd M., Drozd A., Kharchenko V., Antoshchuk S., Sulima J.* Checkability of the digital components in safety-critical systems: problems and solutions // IEEE East-West Design & Test: Proceedings of the IEEE Symposium, Sevastopol, Ukraine. 2011. P. 411–416.

7. *Drozd M., Drozd A.* Safety-Related Instrumentation and Control Systems and a Problem of the Hidden Faults // Digital Technologies : Proceedings of the 10th International Conference, Zhilina, Slovak Republic. 2014. P. 137–140.

8. *Gillis D.* The apocalypses that might have been // DAMN Interesting. 2007. № 298. URL: http://www.popmech.ru/go.php?url=http%3A%2F%2Fwww.damninteresting.com%2F%3Fp%3D913

9. Evolution of a Problem of the Hidden Faults in the Digital Components of Safety-Related Systems / *Drozd A., Kuznietsov M., Antoshchuk S., Martynyuk A., Drozd M., Sulima J.* // East-West Design & Test : Proceedings of the 16th IEEE Symposium. P. 1–5. 2018. DOI: 10.1109/EWDTS. 2018.8524806.

10. *Kharchenko V. S., Sklyar V. V. (edits)* FPGA-based NPP I&C Systems: Development and Safety Assessment. Kharkiv. RPC Radiy, National Aerospace University “KhAI”, SSTC on Nuclear and Radiation Safety. 2008. 188 p.

11. *Kharchenko V. S., Siora A. A., Bakhmach E. S.* Diversity-Scalable Decisions for FPGA-based Safety-Critical I&Cs: from Theory to Implementation // Sixth ANS International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies (NPI–HMIT 2009) April 5–9. 2009. Knoxville, Tennessee, USA.

12. Intel Quartus Prime Standard Edition User Guide: Getting Started. URL: https://www.intel.com/content/www/us/en/programmable/documentation/yoq 1529444104707.html

13. Intel Quartus Prime Standard Edition User Guide: Power Analysis and Optimization. URL: https://www.intel.com/content/www/us/en/programmable/ documentation/xhv1529966780595.html

14. MAX 10 FPGA Device Architecture. URL: https://www.intel.com/ content/ www/us/en/programmable/documentation/sss139743990 8414.html

15. Intel FPGA Integer Arithmetic IP Cores User Guide. URL: https://www.intel.com/content/www/us/en/programmable/documentation/sam139 5330298052.html

References:

1. Kharchenko V., Gorbenko A., Sklyar V. and Phillips C. (2013), “Green Computing and Communications in Critical Application Domains: Challenges and Solutions” // Digital Technologies: Proceedings of the 9th International Conference, Zhilina, pp. 191–197 [Slovak Republic].

2. Brezhnev E. and Kharchenko V. (2011), Approach for formalization of influences in critical infrastructure // Critical Infrastructure Safety and Security (CrISSDESSERT): proceedings of I Int. Workshop, Kirovograd, 10–11 May, Kirovograd, pp. 216–226 [Ukraine].

3. IEC 61508-1:2010 (2010), Functional safety of electrical / electronic / programmable electronic safety related systems. Part 1: General requirements. Geneva: International Electrotechnical Commission.

4. EN 50126 / IEC 62278 (2008), Quick Guide to safety Management based on EN 50126 / IEC 62278 // Blogspot, available at: http://en50126.blogspot.com

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

6. Drozd M., Drozd A., Kharchenko V., Antoshchuk S. and Sulima J. (2011), “Checkability of the digital components in safety-critical systems: prob-

lems and solutions" // IEEE East-West Design & Test: Proceedings of the IEEE Symposium, Sevastopol, pp. 411–416 [Ukraine].

7. Drozd M. and Drozd A. (2014), "Safety–Related Instrumentation and Control Systems and a Problem of the Hidden Faults" // Digital Technologies: Proceedings of the 10th International Conference, Zhilina, pp. 137–140 [Slovak Republic].

8. Gillis D. (2007), The apocalypses that might have been // DAMN Interesting, vol. 298, available at: http://www.popmech.ru/go.php?url=http%3A%2F%2Fwww.damninteresting.com%2F%3Fp%3D913

9. Drozd A., Kuznietsov M., Antoshchuk S., Martynyuk A., Drozd M. and Sulima J. (2018), "Evolution of a Problem of the Hidden Faults in the Digital Components of Safety-Related Systems" // East–West Design & Test: Proceedings of the 16th IEEE Symposium, pp. 1–5, DOI: 10.1109/EWDTS. 2018. 8524806

10. Kharchenko V. S., Sklyar V. V. (edits) (2008), FPGA-based NPP I&C Systems: Development and Safety Assessment. RPC Radiy, National Aerospace University "KhAI", SSTC on Nuclear and Radiation Safety, Kharkiv, 188 p. [Ukraine].

11. Kharchenko V. S., Siora A. A. and Bakhmach E. S. (2009), "Diversity-Scalable Decisions for FPGA-based Safety-Critical I&Cs: from Theory to Implementation" // Sixth ANS International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies (NPI–HMIT 2009) April 5–9, Knoxville, Tennessee [USA].

12. Intel Quartus Prime Standard Edition User Guide: Getting Started, available at: https://www.intel.com/content/www/us/en/programmable/ documentation/yoq1529444104707.html

13. Intel Quartus Prime Standard Edition User Guide: Power Analysis and Optimization, available at: https://www.intel.com/ content/www/us/en/programmable/ documentation/xhv1529966780595.html

14. MAX 10 FPGA Device Architecture, available at: https://www.intel.com/ content/www/us/en/programmable/documentation /sss1397439908414.html

15. Intel FPGA Integer Arithmetic IP Cores User Guide, available at: https://www.intel.com/content/www/us/en/programmable/documentation/ sam1395330298052.html