УДК 004.056(274) Doi: https://doi.org/10.32918/nrs.2020.2(86).07

Application of the FPGA Technology for the Development of Multi-Version Safety-Critical NPP Instrumentation and Control Systems

■ **Perepelitsyn A.**
National Aerospace University «KhAI», Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-5463-7889

■ **Illiashenko O.**
National Aerospace University «KhAI», Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-4672-6400

■ **Duzhyi V.**
National Aerospace University «KhAI», Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-3383-1893

■ **Kharchenko V.**
National Aerospace University «KhAI», Kharkiv, Ukraine
Research and Production Corporation «Radiy», Kropyvnytskyi, Ukraine
ORCID: https://orcid.org/0000-0001-5352-077X

The paper overviews the requirements of international standards on application of diversity in safety-critical NPP instrumentation and control (I&C) systems. The NUREG 7007 classification of version redundancy and the method for diversity assessment are described. The paper presents results from the analysis of instruments and design tools for FPGA-based embedded digital devices from leading manufacturers of programmable logics using the Xilinx and Altera (Intel) chips, which are used in NPP I&C systems, as an example. The most effective integrated development environments are analyzed and the results of comparing the functions and capabilities of using the Xilinx and Altera (Intel) tools are described. The analysis of single failures and fault tolerance using diversity in chip designs based on the SRAM technology is presented. The results from assessment of diversity metrics for RadICS platform-based multi-version I&C systems are discussed.

Keywords: FPGA, diversity, safety, instrumentation and control system.

Introduction

Programmable logic devices (PLD) have proved to be among the few semiconductor technologies whose demand is virtually independent of how the sales of the end-product manufacturers are successful. Even in times of economic instability, the growth rate of field programmable gate arrays (FPGA) on the PLD market remains high. Manufacturers such as Xilinx, Intel (Altera), Microsemi, Lattice and others provide a wide range of FPGA chips. Intel and Xilinx mainly produce FPGA PLDs that are manufactured using energy-dependent SRAM technology. As the production of circuits with SRAM technology is becoming more complicated, their sensitivity to single failures (single-event upsets (SEUs)) due to high-energy particles generated by cosmic rays increases.

Diversity is a common approach used to provide various reliability attributes of information and control systems using FPGA as an embedded digital system; in particular, functional safety and cybersecurity. The use of diversity for information and control systems is recommended by international standards for various critical areas (nuclear – NUREG/CR-7007 [1], IEEE Std 7-4.3.2-2016 [2], IAEA SSR-2/1:2016 [3], IAEA NP-T-3.17:2016 [4]; automotive industry – ISO 26262-10: 2011 [5]; critical systems in general – IEC 61508: 2010 [6] etc.).

SSTC NRS ДЕРЖАВНЕ ПІДПРИЄМСТВО ДЕРЖАВНИЙ НАУКОВО-ТЕХНІЧНИЙ ЦЕНТР З ЯДЕРНОЇ ТА РАДІАЦІЙНОЇ БЕЗПЕКИ

The need for the diversity of the information and control (I&C) system architecture for NPPs is determined by in-depth defense analysis and diversity analysis (D3 analysis). Such a method is set forth in NUREG/CR-6303 [7], where it is concluded that diversity is necessary to adequately address the common cause failure (CCF) vulnerability associated with a functional safety feature. CCF is defined as "failure of two or more structures, systems or components due to a single specific event or cause" [8, 9]. Different types of diversity are used to minimize the CCF risk based on their classification [1]. The authors of the paper were involved in the R&D activities related to safety and security assessment of the RadICS platform, which is a set of general-purpose building blocks that can be configured and used to implement application-specific functions and systems for NPP I&C safety functions. It is composed of various standardized modules, each being based on the use of FPGA chips as computational engines. One of the crucial architectural decisions used in development of the RadICS platform was the implementation of diversity principle [10].

To eliminate the design defects that occur in the development of embedded digital systems and deal with the imperfection of integrated development environment systems, it is necessary to use the redundancy version.

Thus, the goal of this study is to analyze the use of the embedded systems, in which two channels with the same functionality are used to perform the functions of NPP I&C systems based on Altera and Xilinx chips. The paper analyzes integrated development environments from leading FPGA manufacturers, results from comparison of the potential use of Xilinx and Altera tools, and diversity metrics that can be assured using the FPGA-based RadICS platform.

Analysis of standard requirements for diversity

Appendix A of NUREG 7007/CR "Evaluating diversity in system designs" defines seven diversity attributes and related diversity criteria. These attributes and related criteria are:

design: different technologies; different approaches within a technology; different architectures;

equipment manufacturer: different manufacturers of fundamentally different equipment designs; same manufacturer of fundamentally different equipment designs; different manufacturers of the same equipment design; same manufacturer of different versions of the same equipment design;

logic processing equipment: different logic processing architectures; different logic processing versions in the same architecture; different component integration architectures; different data flow architectures;

function: different underlying mechanisms to accomplish safety function; different purpose, function, control logic, or actuation means of the same underlying mechanism; different response time scale;

life-cycle: different design organizations/companies; different management teams within the same company; different designers, engineers, and/or programmers; different implementation/validation teams (testers, installers, or certification personnel);

signal: different parameters sensed by different physical effects; different parameters sensed by the same physical effects; same parameter sensed by a different redundant set of similar sensors;

logic: different algorithms, logic, and program architecture; different timing or order of execution; different runtime environments; different functional representations.

NUREG 7007/CR does not provide detailed algorithms on diversity assessment, so it can be used as an umbrella standard for developing our own methods. Diversity issues were raised by several international standards issued after NUREG/CR 7007. These standards cover different critical domains like automotive and nuclear.

Standard IEC 61508:2 [6] emphasizes the need for diversity application in the design of hardware. Diverse hardware is not required if validation and extensive operational experience prove that the hardware is sufficiently free from design faults and sufficiently protected against common cause failures to fulfill the target failure measures. IEC 61508:3 also contains requirements for software diversity. For the selection of appropriate techniques and measures to meet the requirements of software architecture design, the following properties of the software architecture design should be considered: completeness with respect to the specification of software safety requirements; correctness with respect to the specification of software safety requirements; freedom from intrinsic design faults; simplicity and understandability; predictability of behavior; verifiable and testable design; fault tolerance; defense against common cause failure from external events.

The following architecture and design features should be targeted: diverse monitor techniques (with independence between the monitor and the monitored function in the same computer and separation between the monitor computer and the monitored computer as well); diverse redundancy (implementation of the same software safety requirement specification); functionally diverse redundancy (implementation of different software safety requirement specification).

Annex B of IEEE Std 7-4.3.2-2016 [2] provides determination of diversity requirements. It also specifies requirements and recommendations for the diversity of manual controls and displays, as well as requirements for automatic controls. The document states that safety-related instrumentation and control systems shall have adequate defense in depth and diversity (D3) to

compensate for credible common cause failure (CCF). If digital components have sufficient diversity, then CCF can be categorized as not credible between these components. The following cautions regarding diversity are determined in this document:

the justification for the level of diversity of equipment, or of related system software such as a real-time operating system, shall extend to the equipment's components to ensure that actual diversity exists;

with respect to software diversity, experience indicates that independence of failure modes may not be achieved in cases where multiple versions of software are developed to the same software requirements.

It is determined that manual operator action may be credited as backup to safety functions disabled by postulated CCF, if the manual action can be performed reliably in a period when the plant response remains bounded by the acceptance criteria for radiation release. Diverse automation may be credited as backup to safety functions disabled by a postulated CCF. The automation shall be provided by equipment that is not affected by the same postulated safety system CCF. This equipment may be digital or non-digital.

Table A.7 of ISO 26262-10 [5] states that hardware faults, development faults, stresses due to specific situations like wear and ageing, and even environmental factors can be addressed by measures such as diversity.

IAEA SSR-2/1 [3] specifies that diversity shall be considered for I&C systems performing safety functions, as well as for support service systems, communication systems etc. It is stated that functional diversity and diversity in component design and in concepts of operation shall be used to the extent practicable to prevent the loss of a safety function.

IAEA NP-T-3.17:2016 [4] states that the FPGA technology could constitute a viable option for diversity between primary and redundant safety functions. It is also stated that redundant microprocessor and FPGA-based systems must, as a minimum, meet the following diversity criteria: design diversity (different technologies and architecture); equipment diversity; functional diversity (different ways to achieve the same result); software diversity (different programming languages, design methodologies and software architecture). Section 3.1.7 summarizes utilization of FPGA features to provide diversity, in particular, within the FPGA-based system itself.

Considering all mentioned above, it can be concluded that all the standards are not devoted to diversity only, like NUREG 7007/CR, and do not provide any details on diversity evaluation and assurance. The standards do not provide recommendations for determination of diversity metrics, weights of diversity attributes and choice of version redundancy. These limitations were studied in [11, 12]. Besides, important issues of FPGA application in NPP I&C systems are assessment and assurance of security including diversity aspects [13, 14]. Review of other characteristics and features of application Altera and Xilinx FPGA chips in safety-critical systems including NPP I&C systems is presented in [15-18].

Analysis of the boundary diversity level of Altera and Xilinx FPGA technologies

Many embedded systems implemented using PLDs require not only a high level of reliability but also the security that can be achieved, including the application of the diversity principle. With regard to FPGA, diversity primarily involves the use of products from different manufacturers, which also include tools and development process in addition to the circuits themselves.

For example, the Radiy Company [10] uses Altera (Intel) products for the design of I&C platforms. One of the paramount criteria is the reliability of FPGA chips under given conditions. This requirement is met by Microsemi (Actel) products, which could be a version alternative to the products used. However, at large scales of production, significant risks are associated with providing the required volume of units in hardware components that may arise when the production of a particular family of FPGA chips is termination. This situation is not excluded for the Microsemi and Altera products. Given these risks, as well as being a world leader in programmable logic, Xilinx products are a worthy alternative to Intel's FPGA. In addition to programmable chips, companies release software for the development of FPGA software for Windows and Linux. The development environment for Intel products is Quartus and ModelSim. ISE and Vivado are the development environments for Xilinx products.

In order to justify the use of multiple versions with the same functionality, it is necessary to evaluate the maximum achievable version using different products (embedded digital system projects). In what follows, we will consider an example of two-version (diverse) embedded digital systems, in which the same functionality is implemented on two Intel and Xilinx systems. Each channel (version) is not limited to FPGA chips, but includes different IDE systems, project description methods, standard library sets, development techniques, etc.

The features peculiar to stages of system development, which can be conditionally divided into software and hardware ones, can serve as indicators for comparison of the Xilinx and Intel technologies. The first group includes everything related to the creation of FPGA implementable code: IDE, a set of libraries, a method of description (as well as the description language or processor cores) and the use of different design techniques (patterns). If different libraries are used in the development of the IDE itself, it could also serve as an additional factor of versatility.

The second group includes everything that is directly related to the FPGA chips and their integration

SSTC NRS ДЕРЖАВНЕ ПІДПРИЄМСТВО ДЕРЖАВНИЙ НАУКОВО-ТЕХНІЧНИЙ ЦЕНТР З ЯДЕРНОЇ ТА РАДІАЦІЙНОЇ БЕЗПЕКИ

into the system: implementation technology, series and family, model and type of housing within the family and mounting on the board. The characteristic values of the listed features for manufacturers are shown in Table 1.

The unique capability of the multi-version embedded digital system design is provided by modern IDE packages designed for the development of embedded digital systems, like SDAccel and Vitis for high-level description and Quartus or Vivado for chip-level prototyping. Their resources enable the development of embedded digital systems by introducing a schematic diagram, depicted graphically, using a library of standard elements, as well as by describing the logic of operation in one of the input languages such as AHDL, VHDL, Verilog HDL, System Verilog, OpenCL, C and C++.

These languages are high-level modular languages describing the operation of digital circuits that support the creation of digital finite state machines, truth tables, etc.

In practice, not all of these options are convenient for use. For example, the use of VHDL and Verilog is most likely, the use of AHDL and JHDL may be limiting and the use of AHDL and JHDL may introduce restrictions and may require additional costs. Similarly, FPGAs are the most likely choice, which means that the number of possible series of chips to choose from will decrease. An important criterion for comparing FPGA chips of different manufacturers can be the production process. Table 2 shows a comparison of some popular Altera and Xilinx FPGA families, combined by the process of 65 nm.

Table 1 – Possible sources of Intel and Xilinx dual-channel embedded digital system versions

Attribute	Intel	Xilinx
IDE	Quartus (Prime) (Windows)	ISE, Vivado (Windows)
	Quartus (Linux)	ISE, Vivado, SDAccel, Vitis (Linux)
Method of description	Circuitry solutions	Circuitry solutions
	VHDL, Verilog, AHDL	VHDL, Verilog, JHDL, OpenCL
	Microprocessor core Nios II	Microprocessor core MicroBlaze
Set of libraries	Standard and extraneous	Standard and extraneous
Description technique	Constructions, paradigms	Constructions, paradigms
Technology	FPGA, CPLD, ASIC	FPGA, CPLD
FPGA series	Stratix, Arria, Cyclone, MAX	Virtex, Spartan, Kintex, Artix, CoolRunner, XC9500, Ultrascale
Printed circuit board	Production company, method of installation	Production company, method of installation

Table 2 – Comparison of FPGA families of Altera and Xilinx companies with the 65 nm process

Attribute	Altera			Xilinx
Technological process 65 nm	Cyclone III	Stratix III L	Stratix III E	Virtex-5
Number of logical elements	119088	338000	254400	331776
Clock speed(max), MHz	260	550	550	550
Supply voltage, V	1.2	1.2 (0.9/1.1)	1.2	3.3, 2.5, 1.8, 1.2
Maximum RAM, kbps	3888	17876	14688	11664 (10368)
Number of I/O pins in maximum RAM configuration	531	1104	960	960 (1200)
Maximum speed of external exchanges per transmission channel	875 Mbps	up to 1.25 Gbps	up to 1.25 Gbps	up to 1.25 Gbps
Ability to connect processor cores (not counting the cores of I/O devices)	synthesizing ARM 32-bit Cortex-M1, 32-bit NiosII	synthesizing 32-bit NiosII	synthesizing 32-bit NiosII	DSP-48E hardware

Comparable FPGA chips from Altera and Xilinx are implemented using energy-dependent technology and require external flash memory. SRAM-based FPGAs, the bulk of Altera and Xilinx products, require constant power to maintain their programmed status. In addition, boot ROM may require an additional external component to manage the system configuration, as the FPGA cannot take over these functions until it reads its own configuration.

The main element of the Altera and Xilinx FPGA contains a table of correspondence with four inputs (Lookup Table (LUT)), a trigger and some additional scheme, called a logic element in Altera and a logic cell in Xilinx. Logical cells refer to logic elements as 1.125:1, despite the similar functionality. Altera and Xilinx also offer their own tabular comparison for the resources of many equivalent FPGA families of their production, but their comparison is only for a number of chips and does not carry versatility.

Analysis of the effect from single failure and fault tolerance using redundancy on the chip

SRAM is a technology that has the advantage of multiple FPG reprogramming. The disadvantages of SRAM implementation include the need to load the configuration each time the power is turned on, which requires placement of an additional loader on the board. Many of Altera's FPGAs are manufactured using the SRAM technology, the FPGA configuration being stored in SRAM during operation. Since the SRAM configuration is energy dependent, it must be downloaded each time after power is turned on. This increases the cost of the end device and is an additional source of cyber security threats to the embedded digital systems and the overall I&C system. As the technological process of manufacturing integrated circuits is becoming more complicated, their sensitivity to single-event upset increases due to high-energy particles generated by cosmic rays, background radiation or the body of the chip itself and the silicon substrate.

Since the latter two sources are directly within the device itself, no external shielding can protect the charged particles. When these particles penetrate the silicon substrates of the integrated circuits, they leave a trail of ionization, which can lead to a charge capable of altering the state of the logical memory element on complementary metal-oxide-semiconductor structures such as SRAM. This change in status is called a single-event upset.

Since such violations are temporary and disappear when you next record or reset the SRAM memory, it is justified to use redundancy inside the chip to prevent failure of intersecting cells within each cycle of the device. The sensitivity of memory circuits to SEU increases with each new generation of devices due to a decrease in the supply voltage and a decrease in the logic element threshold capacity. What used to be a concern only in space applications is now topical even at ground level and is a problem for any project with high reliability requirements, especially for NPPs. Such controls are not only sensitive to the natural background, but must also operate in the radiation environment of NPPs.

As the FPGA failure rate increases, the likelihood of the backup channel of the digital device decreases; as the number of bus discharges, the operating time, and the number of soldering connections increase, the probability of failure of the built-in digital system increases. One of the options for improving fault tolerance is the use of on-chip redundancy. Single physical defects of the FPGA chip and associated faults must be parried by redundancy within the chip (duplication or majority). Majority errors and one-time faults occurring with some combinations of input signals and design defects are eliminated using redundancy. Active and passive redundancy methods are used for reserving inside the chip. For reserving inside the chip, internal chip blocks can be in the «loaded» or «light» reserve.

FPGA fault tolerance is greatly influenced by the geometric (spatial) location of the project on the chip. To ensure the independent nature of project failures, they must be located in different areas of the internal structure of the FPGA chip and have no common logical cell. To reduce the likelihood of simultaneous failure of several internal backup channels due to their spatial proximity, a reserve should be placed in different parts of the FPGA chip.

Analysis of reconfiguration features has shown that dependent FPGA faults can be tolerated by external duplication or n out k methods. Versioned redundancy, which is introduced through the use of various combinations of company versions, development and testing tools, functions of the integrated digital system at intra- and non-chip levels, as well as the implementation of backup channels on the FPGA, provides fault tolerance not only to physical defects but also design flaws.

The method of dynamic reconfiguration, which is implemented by loading the configuration files in the FPGA according to the received information about the failures in the internal structure of the chip or loading the configuration only for certain sections of the chip, is promising. This configuration approach has been already implemented in some chips of the latest families of leading manufacturers, including Ultrascale from Xilinx.

Analysis of the lifetime of FPGA chips

For each type of FPGA chip of any family, Altera and Xilinx produce tests, whose results are published in a regularly updated document such as «Reliability Report»

SSTC NRS ДЕРЖАВНЕ ПІДПРИЄМСТВО ДЕРЖАВНИЙ НАУКОВО-ТЕХНІЧНИЙ ЦЕНТР З ЯДЕРНОЇ ТА РАДІАЦІЙНОЇ БЕЗПЕКИ

and «Device Reliability Report», respectively, which can be found at the official websites of Intel and Xilinx. The results of the durability tests are given by product family. For families produced with different substrate technologies, the results are reported separately for each production technology. Within the same family, the same logic elements, macros, and programmable interconnects are used. Only does the number of devices (3 to 10) in a particular family that differs in the number of macros or logic elements change.

It is most convenient to follow the order of tests and find the necessary characteristics on the example of popular chips, such as EP1C12, EP1C20 and EP2C70. The EP1C12 and EP1C20 (Cyclone) devices are manufactured using 130 nm technology with a rated voltage of 1.5 V. and the EP2C70 (Cyclone II) devices are manufactured using 90 nanometer technology with a voltage of 1.2 V. Durability tests for Cyclone devices were performed at 100 °C and a supply voltage of 1.8 V (20 % overvoltage) and those for Cyclone II devices at 125 °C and a supply voltage of 1.44 V (20 % overvoltage). The company performs high-speed load testing in a closed, stainless steel chamber, which allows the temperature and humidity tests under pressure. The ambient conditions and humidity are set to eliminate condensation on the pins of the test devices. Altera performs these tests at 130 °C and 85 % humidity, which provides at least 10x acceleration tests, compared to 85 °C and 85 % humidity. Thermocycling accelerates the effect of temperature change on integrated circuits. The change in temperature causes the various materials used in the integrated circuits to expand and contract with different intensities since they have different coefficients of expansion. Extreme temperatures during thermal cycling lead to mechanical stresses caused by different coefficients of expansion. These loads are most detrimental to dimensional devices.

Intel uses two high- and low-temperature cameras to move batches of devices. They are moved within seconds. The devices reach a specific temperature in the chamber within 5 minutes, after which they remain at this temperature for at least 5 minutes. Temperatures from military standard 883 ranging from -55 °C to + 125 °C are used for thermal cycling. Devices are inspected after 500, 700 and 1000 cycles. JESD47F qualification requires 700 cycles. The company tests the EP1C12, EP1C20 and EP2C70 device family on a sample of 24, 77 and 25 chips and claims that all devices in the sample have been tested with failure rates 5.68E+06 and 1.10E+06.

Xilinx performs tests for all chips, including Spartan, Virtex, Zynq, UltraScale and UltraScale+ devices. The tests also include overvoltage, different current of long load and temperature.

Intel releases ROMs of sequential configuration that support different configuration modes. Both programmable and reprogrammable ROM configurations are available. Reprogrammable configurators can be stitched directly on the board of the target device through the serial interface. The EPC4 and EPC16 circuits are included in the Enhanced Configurator family, which also supports Fast Passive Parallel and Active Serial mode in addition to Passive Serial mode. They are reprogrammable and can be programmed directly into the target device via the JTAG interface. The company performs high-temperature storage testing at 150 °C or higher temperature. These conditions allow one to detect disruption of connections across all device families and data storage failures in nonvolatile memory elements. EPCS4 and EPCS16 devices are manufactured on STMicroelectronics using the 110-nanometer CMOS technology. All devices in the sample were tested. Rated power supply was 3.3 V. They are available in 8-pin SO enclosure.

The ability of non-volatile memory cells to hold a charge is critical to reliability. The loss of charge on a floating shutter of a nonvolatile element of such configuration can be detected by the parametric method supported by Intel.

Assessment of diversity on application FPGA Altera and Xilinx

The RadICS platform is a SIL3-certified FPGA (Altera)-based automation platform [9]. At different certification phases, different designs of the RadICS platform were provided. These designs differ in hardware and software parts and, therefore, can be used as diverse solutions for the implementation of NPP I&C systems.

To perform analysis of RadICS platform-based I&C systems, an approach that considers NUREG 7007/CR and other standards mentioned in the previous section of the paper (so-called post NUREG/CR 7007 approach) was developed. In application of this approach, the following attributes of diversity were considered [13]:

design diversity as a result of applying different approaches, including both software and hardware to solve the same or similar problems;

equipment manufacturer diversity as a result of using different vendors, manufactures, etc.;

logic processing equipment diversity as a result of different logic processing architectures, logic processing versions in the same architecture, component integration architecture, data-flow architecture;

functional diversity as a result of treating two systems as functionally diverse ones if they perform different physical functions;

life-cycle diversity as a result of having different specialists involved in the design, development, installation, operation, and maintenance of I&C systems;

logic diversity as a result of differential features between systems in terms of algorithms, logic, program architecture, timing and/or order of

execution, runtime environment, etc.;

signal diversity as differences in sensed parameters to initiate safety output signal of I&C.

The described approach uses a double-level classification of diversity, including the types and subtypes (attributes and criteria, respectively).

The experts distinguish diversity types DTi and subtypes DSTij (using "Yes" or "No" values) by documentation analysis employing a set of special tools. The weight of the i-th diversity of type WDi depends on the rate of application in I&C. The values of MDi metrics are calculated considering PRij priorities (degree of importance in the decrease of common cause failure, while j = {1,…, NDi}, where NDi is the number of diversity subtypes) of diversity subtypes:

$$MD_i\left(PR_{ij}\right)=\frac{j}{\left(1+2+\ldots+ND_i\right)}, \quad (1)$$

where j is the number of priority.

The general metric of diversity is

$$GMD = \sum_{i=1}^{ND} WD_i MD_i. \quad (2)$$

If there are a few diversity subtypes DSTij

$$MD_i = \sum_{j=1}^{ND_i} B_{ij} MD_{ij}, \quad (3)$$

where Bij is a Boolean value which is equal to 0 if subtype DSTij is not applied, and is equal to 1 if vice versa.

This technique does not facilitate the calculation of diversity that considers more detailed classifications involving three or more attribute levels. Besides, GMD determines a maximum value because application of any DSSTijk sub-subtypes for DSTij diversity subtype postulates the MDi value.

The process of diversity assessment in this case is based on application of a two-level checklist filled by the experts. The experts should determine and mark all diversity attributes and criteria presented in I&C systems and mark them in the checklist using 'Yes' or 'No' values. If some criterion is applicable in the project (marked 'Yes'), the expert also marks INT = intentional (x). Filling the checklist with particular diversity criteria can automatically give rise to corresponding diversity criteria, which either the expert or the tool marks as INH = inherent (i). The weight of attribute depends on the rate at which the diversity type is applied in I&C. In the calculation of diversity metrics, both marks ('x' and 'i') are processed identically. When particular diversity types/subtypes are filled into the checklist, the respective ones can be revealed automatically (note: expert marks INH = inherent (i) against them). After the checklist is filled in, the diversity metrics are calculated as the sum of the weighted values of diversity types/subtypes (attributes and criteria). The diversity metric obtained after calculation is not normalized and can take any values in the range {0 – 1.76}. In this method, the diversity metric of 1.0 is considered to be acceptable for two-version I&C.

The presented NUREG-A technique was enhanced taking into account more detailed specification of hardware diversity classification as follows: extension of the subtypes sets (increasing NDi). In this case, the MDi calculation procedure is the same and reprioritization of diversity subtypes is required [19].

A special spreadsheet-based Diversity Assessment Tool implementing the mentioned checklist was developed to support the described approach. The proposed technique was applied for the RadICS FPGA-based platform. The examples of the results obtained are shown in Table 3.

The developed tool allows automating all steps that are presented in the previous section. We can conclude that application of the RadICS platform to develop a two-version system assures the accepted level of diversity 1.01 by diversifying the process and product decisions. In case of applying the Xilinx-based platform for diverse subsystem, the metrics of diversity can be increased to 1.10. In case of applying the RadICS platform to design the main and diverse systems, a compromise is achieved according to the safety-cost criteria, because such a system meets standard requirements for diversity and minimizes risks and cost of maintenance [11-13].

Conclusions

A sabotage channel with a maximum diversion index present in systems important for safety, in which PLDs like FPGA are used, increases the level of security peculiar to such a system by reducing the likelihood of CCF. As part of the study, some features of using two versions of the digital systems manufactured by Altera and Xilinx for the implementation of embedded digital systems have been analyzed. It has been revealed that the size of the process is the main criterion for comparing FPGA chips from different manufacturers.

It has been found that in-chip reservation to combat the SEU effect is effective for the Altera and Xilinx FPGAs. The analysis conducted in this paper shows that there is a strong need for the development of new regulatory procedures to cover application of diversity

SSTC NRS ДЕРЖАВНЕ ПІДПРИЄМСТВО ДЕРЖАВНИЙ НАУКОВО-ТЕХНІЧНИЙ ЦЕНТР З ЯДЕРНОЇ ТА РАДІАЦІЙНОЇ БЕЗПЕКИ

Table 3 – Diversity assessment tool spreadsheet

	Attribute criteria			RadICS Platform		
		Rank	DCE WT	INT	INH	Score
DESIGN	**Design**					
	Different technologies	1	0,500			0,000
	Different approaches within a technology	2	0,333			0,000
	Different architectures	3	0,167			0,000
	DAE weight and subtotals		1,000		0,000	0,000
EQUIP.MANUF.	**Equipment Manufacturer**					
	Different manufacturers of fundamentally different equipment designs	1	0,400			0,000
	Same manufacturer of fundamentally different equipment designs	2	0,300			0,000
	Different manufacturers of same equipment design	3	0,200			0,000
	Same manufacturer of different versions of the same equipment design	4	0,100			0,000
	DAE weight and subtotals		0,250		0,000	0,000
LOGIC PROC.EQUIP.	**Logic Processing Equipment**					
	Different logic processing architectures	1	0,400			0,000
	Different logic processing versions in same architecture	2	0,300			0,000
	Different component integration architectures	3	0,200	x		0,200
	Different data flow architectures	4	0,100			0,000
	DAE weight and subtotals		0,644		0,129	0,200
FUNCTION	**Function**					
	Different underlying mechanisms to accomplish safety function	1	0,500	x		0,500
	Different purpose, function, control logic, or actuation means of same underlying mechanism	2	0,333	x		0,333
	Different response time scale	3	0,167	x		0,167
	DAE weight and subtotals		0,600		0,600	1,000
LIFE-CYCLE	**Life-Cycle**					
	Different design companies	1	0,400			0,000
	Different management teams within the same company	2	0,300	x		0,300
	Different designers, engineers, and/or programmers	3	0,200	x		0,200
	Different implementation/validation teams	4	0,100	x		0,100
	DAE weight and subtotals		0,683		0,410	0,600
SIGNAL	**Signal**					
	Different reactor or process parameters sensed by different physical effect	1	0,500	x		0,500
	Different reactor or process parameters sensed by the same physical effect	2	0,333	x		0,333
	The same process parameter sensed by a different redundant set of similar sensors	3	0,167	x		0,167
	DAE weight and subtotals		0,867		0,867	1,000
LOGIC	**Logic**					
	Different algorithms, logic, and program architecture	1	0,400	x		0,400
	Different timing or order of execution	2	0,300		i	0,300
	Different runtime environments	3	0,200		i	0,200
	Different functional representations	4	0,100		i	0,100
	DAE weight and subtotals		0,733		0,733	1,000
Score(*100)				274		
Normalized score				1,01		
Basis for normalizing		271				

considering new FPGA-based technologies and their interconnections. The existing regulatory framework that governs diversification should be enhanced in three areas such as scope, depth and rigor to provide more detailed descriptions of potential applied techniques and tools for quantitative assessment of diversity.

The analysis performed with the specified approach shows that diversity attributes provided for different certified design revisions of the RadICS platform comply with NUREG 7007/CR requirements.

Acknowledgment

This research is supported by the STARC project (Methodology of SusTAinable Development and InfoRmation Technologies of Green Computing and Communication) funded by the Ministry of Education and Science of Ukraine.

References

1. NUREG/CR 7007-2009. Diversity strategies for nuclear power plant instrumentation and control systems. ONL, Oak Ridge, USA.

2. IEEE Std 7-4.3.2-2016. IEEE standard criteria for programmable digital devices in safety systems of nuclear power generating stations, USA.

3. IAEA Safety Standards Series No. SSR-2/1. (2016). Safety of nuclear power plants: Design. Specific safety requirements. International Atomic Energy Agency, Vienna.

4. IAEA Nuclear Energy Series No. NP-T-3.17. (2016). Application of field programmable gate arrays in instrumentation and control systems of nuclear power plants. International Atomic Energy Agency, Vienna.

5. ISO 26262:2011. Road vehicles – Functional safety.

6. IEC 61508:2010 Ed.2. Functional safety of electrical / electronic / programmable electronic safety-related systems.

7. United States Nuclear Regulatory Commission. (1994). Method for performing diversity and defense-in-depth analyses of reactor protection systems. NUREG/CR-6303, Office of Nuclear Regulatory Research.

8. International Electrotechnical Commission. (2008). Instrumentation and control systems important to safety. Requirements to cope with common cause failure (CCF). IEC 62340, Geneva, Switzerland.

9. Kharchenko, V., Siora, O., Duzhyi, V., Rusin, D. (2014). Standard analysis and tool-based assessment technique of NPP I&C systems diversity. Proceedings of the 22nd International Conference on Nuclear Engineering ICONE 22, July 7 – 11, 2014, Prague, Czech Republic, 7 p.

10. RadICS Platform description. Retrieved from http://www.radiy.com/en/nuclear/products/radics-platform.html.

11. Duzhyi, V., Kharchenko, V. Panarin, A., Rusin, D. (2018). Diversity metric evaluation considering extended NUREG-7007 Diversity Classification. Proceedings of 9th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT 2018 24-27 May 2018, Kyiv, Ukraine, pp. 56-61.

12. Andrashov, A., Bakhmach, I., Leontiiev, K., Kharchenko, V., Babeshko, E., Kovalenko, A. (2019). Diversity in FPGA-based platform and platform based I&C applications: strategy and implementation. Proceedings of the 11th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, NPIC & HMIT 2019, 9-14 February 2019, Orlando, Florida, USA, pp. 174-182.

13. Illiashenko, O., Kharchenko, V., Kovalenko, A., Sklyar, V., Boyarchuk, A. (2014). Security informed safety assessment of NPP I&C systems. Gap-IMECA technique. Proceedings of the 22nd International Conference on Nuclear Engineering ICONE 22, July 7 – 11, 2014, Prague, Czech Republic, 9 p.

14. Illiashenko, O., Kharchenko, V., Brezhniev, E., Boyarchuk, A., Golovanevskiy, V. (2014). Security informed safety assessment of industrial FPGA-based systems. Proceedings of Probabilistic Safety Assessment and Management Conference PSAM 12, 24-27 June 2014, Honolulu, Hawaii, USA, 11 p.

15. Georgescu, C. (2017). Use of FPGA technology in a (UK) nuclear protection system. Demanding regulatory regime (IEC 61226, 61513, IEC 60880, TAG 46). Horizon Nuclear Power, 25 p.

16. Owais, A. (2018). Latest FPGA in the market. Technical Report. COEN 6501, Digital Design and Synthesis, 22 p.

17. Ranta, J. (2012). The current state of FPGA technology in the nuclear domain. VTT Technical Research Centre of Finland, Espoo, Finland, 67 p.

18. Roy, S., Biswas, A., Pradhan, S. (2015). Use of FPGA and CPLD in nuclear reactor safety systems and its regulatory review requirements for reactor safety. Proceedings of CANDU Safety Association for Sustainability and New Horizons in Nuclear Reactor Thermal-Hydraulics and Safety, CANDU&NHNRTHS 2015, Anushaktinagar, Mumbai, India, pp. 2-8.

19. Illiashenko, O., Kharchenko, V., Kor, A., Panarin, A., Sklyar, V. (2017). Hardware diversity and modified NUREG/CR-7007 based assessment of NPP I&C safety. 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Bucharest, 2017, pp. 907-911.

Використання FPGA технології для розроблення багатоверсійних інформаційно-керуючих систем АЕС, критичних для безпеки

Перепелицин А. Є.[1], Ілляшенко О. О.[1], Дужий В. І.[1], Харченко В. С.[1, 2]

[1] Національний аерокосмічний університет імені М. Є. Жуковського «ХАІ», м. Харків, Україна

[2] Науково-виробниче підприємство «Радій», м. Кропивницький, Україна

У статті наведено огляд вимог міжнародних стандартів щодо використання принципу диверсності в інформаційно-керуючих системах (ІКС)

критичного застосування для АЕС, зокрема, IEC 61508 [6], IEEE Std 7-4.3.2-2016 [2] та ін. Описано методики оцінювання диверсності та класифікацію версійної надмірності, запропоновані у стандарті NUREG 7007 [1] та відомих публікаціях. Класифікація диверсності описується дворівневою ієрархією, на першому рівні якої використовується різноманітність виробників, апаратних засобів, програмного забезпечення, архітектури тощо. Наведено результати аналізу інструментів і засобів проєктування для вбудованих цифрових систем на базі FPGA від провідних виробників програмовної логіки. Аналіз надано на прикладі мікросхем Xilinx і Altera (Intel), які використовуються в ІКС АЕС. Проаналізовано найбільш ефективні середовища розроблення та описано результати порівняльного аналізу функцій і можливостей застосування інструментів компаній Xilinx і Altera (Intel). Представлено аналіз сімейств FPGA, виконаних за технологією 65nm, життєвого циклу їх використання. Проаналізовано особливості впровадження та засоби забезпечення принципу одиничної відмови й відмовостійкості завдяки застосуванню варіантів диверсності у проєктах на кристалі, які використовують SRAM технологію. Ознаками видів диверсності визначено типи IDE, методи опису проєктів, множини бібліотек, серії FPGA, технології виготовлення друкованих плат. Проаналізовано діапазони рівнів диверсності, які забезпечуються за умов використання при побудові основної та диверсної систем мікросхем Xilinx і Altera (Intel). Обговорюються результати оцінювання метрик диверсності для багатоверсійних ІКС, заснованих на платформі RadICS. Показано, що використання цієї платформи, яка побудована на базі кристалів Altera, для розроблення основної та диверсної систем, може забезпечити необхідний рівень диверсності відповідно до вимог стандарту NUREG 7007 [1] завдяки іншим видам процесно-продуктної версійної надмірності.

Ключові слова: FPGA, безпека, диверсність, інформаційно-керуючі системи.

Отримано 17.03.2020.