Diversity for security: case assessment for FPGA-based safety-critical systems

Vyacheslav Kharchenko[1,2], Oleg Illiashenko[1,a]

[1]*National Aerospace University "KhAI", 61070 Kharkiv, Ukraine*
[2]*Centre for Safety Infrastructure Oriented Research and Analysis, 61085 Kharkiv, Ukraine*

Abstract. Industrial safety critical instrumentation and control systems (I&Cs) are facing more with information (in general and cyber, in particular) security threats and attacks. The application of programmable logic, first of all, field programmable gate arrays (FPGA) in critical systems causes specific safety deficits. Security assessment techniques for such systems are based on heuristic knowledges and the expert judgment. Main challenge is how to take into account features of FPGA technology for safety critical I&Cs including systems in which are applied diversity approach to minimize risks of common cause failure. Such systems are called multi-version (MV) systems. The goal of the paper is in description of the technique and tool for case-based security assessment of MV FPGA-based I&Cs.

1 Introduction

1.1 Four challenges for I&C safety assessment and assurance

Industrial safety critical instrumentation and control systems (I&Cs) such as reactor trip systems, on-board aviation systems, railway blocking and signaling systems, etc. are facing more with information (in general and cyber, in particular) security threats and attacks. It concerns most sensitive in point of view safety nuclear domain [1]. Nowadays there is a gap in understanding how to assess safety of industrial I&Cs considering the following:

- firstly, the security issues; security related threats are more and more challengeable for safety critical application. As a result security informed safety conception is intensively developed the last years, in particular for NPP I&Cs [2];
- secondly, the features of FPGA technology and FPGA-based systems as a specific target for intruders. Security aspects for FPGA design and implementation are analyzed in [3-5]. These works allow to systemize different vulnerabilities and threats, and better to understand which of them should be taken into account to assure security;
- thirdly, an application of diversity approach as a mean of minimizing common cause failure risks. In this case two (or more) channels are used in different combinations for obtaining the needed functionality and ensuring of required level of safety. Techniques of development and safety assessment of FPGA-based multi-version industrial systems (MVI&Cs) are researched in [6-8]. However, it is required to analyze influence and features of diversity application in point of view security;
- fourthly, using of case-based proved paradigm. Really, to assure trustworthiness of security assessment for such extremely complex systems, more formalized (and independent in sense of expert errors and uncertainties) techniques are required.

1.2 Researched domains. Goal of the paper

The paper represents research results in the domains of safety, security, diversity and FPGA with representation of methodology of cybersecurity assessment based on cases. The figure 1 shows research fields and the targeted area encircled by red line. Additionally, dashed line describes area of case-based approach application to assessment of safety and security.

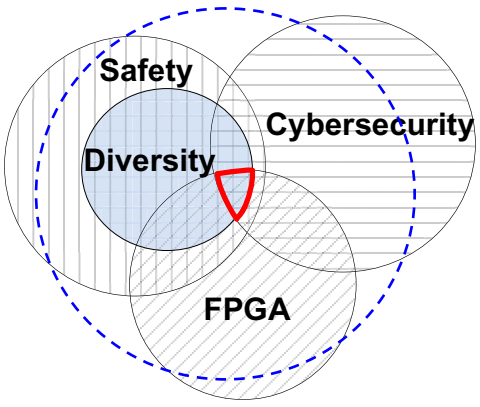

Figure 1. Targeted area of research

[a] Corresponding author: o.illiashenko@csn.khai.edu

Another research aspect is providing effective risk mitigation strategy by use of countermeasures (see Figure 2 where area of countermeasures for FPGA-based MV I&C systems is encircled by red as well, and dashed line describes area of case-based approach application to choice and prove effectiveness of countermeasures).

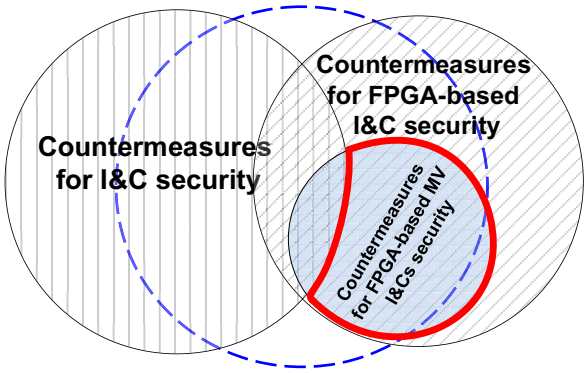

Figure 2. Targeted area for countermeasures.

Thus, goal of the paper is to suggest technique and tool for case-based security assessment of FPGA-based MVI&Cs. Structure of the paper is following.

Second section describes normative base (ISO, IEC and IAEA standards), classification and analysis of application of diffrent diversity kinds for safety and security assessment and assurance for FPGA-based I&Cs.

Third section is dedicated to case development and descridiscusses an example of ASAC application for security analysis and assessment.

The last section concludes the paper and presents directions of future researches.

2 Diversity for safety and security of FPGA-based I&Cs

Diversity is a part of more general principle D3 (Defense-in-Depth&Diversity) [8] applied to provide trusted, fault- and intrusion-tolerant design and operation of I&Cs. Defense-in-Depth is a horizontal/sequential echelon of defense, diversity is a vertical/parallel part of once [11].

2.1 Diversity related standards for safety and security

There are a lot of international standards and national guides containing requirements for implementation and assessment of diversity. Among them are:

a) IEC standards:

- IEC 61513:2001. NPPs - I&Cs important to safety – general requirements for systems;
- IEC 60880 2006. NPPs - I&Cs important to safety - SW aspects for computer-based systems performing category A functions;
- IEC 61508 :2011. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems;

b) IAEA standards :

- IAEA NS-G-1.1:2001. Software for Computer Based Systems Important to Safety in NPPs;
- IAEA NS-G-1.3:2002. I&Cs important to safety in NPPs;
- IAEA NP-T-1.5:2009. Protecting against CCFs in Digital I&C Systems of NPPs ;

c) IEEE and NUREG (USA) standards :

- IEEE std.7-4.3.2:2003. IEEE standard criteria for digital computers in safety systems of NPPs;
- NUREG/CR-7007:2009. Diversity Strategies for NPP I&C Systems, NUREG/CR-7007 ORNL/TM-2009/302.

d) National guides and norms :

- DI&C-ISG-02, Diversity and Defense-in-Depth Issues, Interim Staff Guidance (USA);

BTP 7-19, Guidance for Evaluation of D&DiD In Digital I&C Systems (USA);

- NP 306.5.02/3.035. Requirement on nuclear and radiation safety for I&Cs important to safety in NPPs (Ukraine), etc.

There are standards for other critical domains where diversity as an approach is postulated or requirements to its application are described. For example, requirements to diversity for automotive systems are determined by standard IEC 26262. This standard contains requirements regarding application of software and hardware diversity for on-board vehicle systems.

Generally, the standards are not enough detailed to make all necessary decisions concerning diversity: type of diversity selection and combining, process and product diversity volume assessing and grounding, etc. It is very importanty that they do not take into account two issues :

- features of FPGA technology what complicates their application and
- security issues for safety assessment.

2.2 Assessment of safety and security of FPGA-based I&Cs

2.2.1 Comparison of diversity for SW- and FPGA-based I&Cs

FPGA-based technology provides new possibilities for implementation of diversity principle and additional options [7, 8]. The features of FPGA technology increase a number of diversity kinds and enlarge a set of possible diversity-oriented decisions.

General diversity classification scheme was presented by "cube of diversity" with three coordinates: “stage of the life cycle” – “level of project decisions” and “type of version redundancy” [8]. Using this classification we can analyse safety and security issues for FPGA-based systems and traditional SW-based I&Cs, first of all, for NPPs.

Table 1 summarizes variety of diversity attributes from NUREG-CR/7007:2009 for NPP I&Cs and their accordance with kinds of version redundancy of FPGA-based systems.

Table 1. Diversity attributes and correspondent FNI&Cs version redundancy kinds.

DIVERSITY ATTRIBUTES (NUREG-CR/7007:2009)	KINDS OF VERSION REDUNDANCY (FPGA-BASED I&Ss)
Design	**Diversity of electronic elements (EE)**
Different technologies	Different manufacturers of EEs; Different technologies of EEs production
Different approaches within a technology	Different technologies of EEs production
Different architectures within a technology	Different families of EEs
Equipment Manufacturer	**Diversity of electronic elements (EE)**
Different manufacturers of fundamentally different equipment designs	Different manufacturers of EEs
Same manufacturer of fundamentally different equipment designs	Different families of EEs
Different manufacturers of same equipment design	Different manufacturers of EEs
Same manufacturer of different versions of the same equipment design	Different EEs of the same family
Logic Processing Equipment	**Diversity of project development languages**
Different logic processing architectures	
Different logic processing versions in same architecture	
Different component integration architectures	Joint use of graphical scheme language and hardware description language (HDL)
Different data flow architectures	Joint use of graphical scheme language and HDL
Function	**Diversity of CASE-tools**
Different underlying mechanisms to accomplish safety function	Combination of couples of diverse CASE tools and SSs
Different purpose, function, control logic, or actuation means of same underlying mechanism	Different SSs
Different response time scale	
Life-Cycle	**Diversity of CASE-tools**
Different design companies	Combination of couples of diverse CASE-tools and HDLs
Different management teams within the same company	Combination of diverse CASE-tools and HDLs
Different designers, engineers, and/or programmers	Different HDLs
Different implementation/validation teams	
Signal	**Diversity of CASE-tools, Diversity of scheme specification (SS)**
Different reactor or process parameters sensed by different physical effect	Combination of couples of diverse CASE tools and SSs
Different reactor or process parameters sensed by the same physical effect	
The same process parameter sensed by a different redundant set of similar sensors	
Logic	**Diversity of CASE-tools, Diversity of scheme specification (SS)**
Different algorithms, logic, and program architecture	Combination of couples of diverse CASE-tools and HDLs
Different timing or order of execution	Different CASE tools configurations
Different runtime environments	Different CASE tools
Different functional representations	Different HDLs

2.2.2 Diversity and security

Table 2 shows results of research on diversity attributes from NUREG-CR/7007 which could be applied to mitigate CCF in diverse SW- and HW/FPGA-based systems with the same vulnerabilities in both versions. Different vulnerabilities in both versions have four grades: VH – very high, H –high, M – medium, L – low.

Gradation is based on risk reduction after appliance of a certain diversity attribute. In this case diversity is considered as a countermeasure for elimination of harmful consequences after successful attacks.

2.3 Diversity as a countermeasure

Table 3 summarizes some attacks on FPGA-based I&Cs and results of security assessment using IMECA-analysis [2,8]. Countermeasures are employed to thwart such tampering attacks. The table contains countermeasures strategies which could be applied as a requirements from Regulatory Guide 5.71:2010 (Cyber Security Programs For Nuclear Facilities, U.S. NRC) to eliminate the attack causes and, moreover, FPGA-based MV I&Cs diversity kind and its attributes as a countermeasures.

Thus diversity of FPGA-based MV I&Cs is reviewed as a countermeasure and mitigation strategy for ensuring of security and safety of systems. Criticality matrix (see Fig.3) shows how application of different FPGA-based I&Cs diversity kinds and its attributes will decrease the level of overall risk.

3 Security case development

3.1 Advanced security assurance case

The idea of cybersecurity case for evaluation of security of MV I&Cs lays in appliying of Advanced Security Assurance Case ASAC proposed by [9] which is built taking into account requirements to version kinds of systems.

Table 2. Diversity attributes as a countermeasure.

DIVERSITY ATTRIBUTES (NUREG-CR/7007:2009)	VULNERABILITIES			
	Software		Hardware	
	common vulnerability	different vulnerabilities	common vulnerability	different vulnerabilities
Design				
Different technologies	H	H	H	H
Different approaches within a technology	M	M	M	M
Different architectures within a technology	L	L	L	L
Equipment Manufacturer				
Different manufacturers of fundamentally different equipment designs	H	H	H	H
Same manufacturer of fundamentally different equipment designs	HM	HM	HM	HM
Different manufacturers of same equipment design	M	M	M	M
Same manufacturer of different versions of the same equipment design	L	L	L	L
Logic Processing Equipment				
Different logic processing architectures	H	H	H	H
Different logic processing versions in same architecture	HM	HM	HM	HM
Different component integration architectures	M	M	M	M
Different data flow architectures	L	L	L	L
Function				
Different underlying mechanisms to accomplish safety function	H	H	H	H
Different purpose, function, control logic, or actuation means of same underlying mechanism	M	M	M	M
Different response time scale	L	L	L	L
Life-Cycle				
Different design companies	H	H	H	H
Different management teams within the same company	HM	HM	HM	HM
Different designers, engineers, and/or programmers	M	M	M	M
Different implementation/validation teams	L	L	L	L
Signal				
Different reactor or process parameters sensed by different physical effect	H	H	H	H
Different reactor or process parameters sensed by the same physical effect	M	M	M	M
The same process parameter sensed by a different redundant set of similar sensors	L	L	L	L
Logic				
Different algorithms, logic, and program architecture	H	H	H	H
Different timing or order of execution	HM	HM	HM	HM
Different runtime environments	M	M	M	M
Different functional representations	L	L	L	L

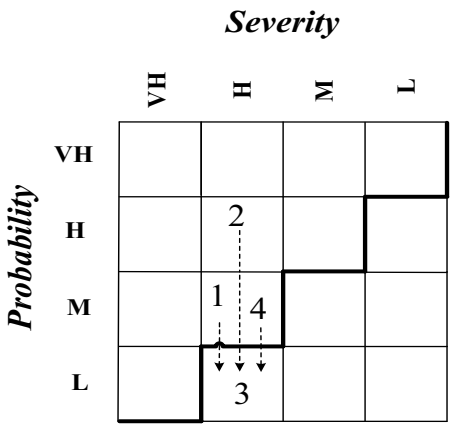

Figure 3. Criticality matrix.

DRAKON was used as a graphical modeling language for representation of cybersecurity case based on ASAC. It was developed from former USSR space program Buran (analogue of Space Shuttle). DRAKON, stands for "friendly algorithmic language that provides clarity." Initially DRAKON was developed for capturing requirements and building software that controls spacecraft [10]. As a language of requirements modeling was chosen IDEF0 notation. Notation IDEF0 allows to show the steps of the evaluation unambiguously (in the form of a directed graph), for each step to determine the evaluated property and evidences necessary for the evaluation, the subjects of assessment, and standards.

If the assessment is subject to a complex (composite) requirement, so each step (or block of IDEF0-diagram) can be decomposed for a detailed description of sub-properties evaluation procedure.

Table 3. IMECA-analysis of attacks on FPGA-based I&Cs.

No	Attack mode	Attack nature	Attack cause	Occurrence probability	Effect severity	Type of effects	Countermeasures (including RG 5.71)	FPGA-based I&C diversity kinds and its attributes
1	Readback	Active	Absence of chip security bit and/or availability of physical access to chip interface (e.g., JTAG)	M	H	Obtaining of secret information by adversary	• The use of security bit; • Application of physical security controls; (B.1.18 Insecure and Rogue Connections, Appendix B to RG 5.71, Page B-6)	Diversity of (EE): •Different technologies of EEs production
2	Cloning	Active	Storing of decoded configuration	H	H	Obtaining of configuration data by adversary	• Checking of chip's internal ID before powering up an electronic design; • Encoding of configuration file; • Storing of configuration file within FPGA chip (requires internal power source)	Diversity of EE: •Different technologies of EEs production; •Different element kinds of EE families
3	Brute force	Active	• Search for a valid output attempting all possible key values; • Exhaustion of all possible logic inputs to a device in order; • Gradual variation of the voltage input and other environmental conditions	L	M	Leak of undesirable information	Detecting and documenting unauthorized changes to software and information, (C.3.7, Appendix C to RG 5.71, Page C-7)	Diversity of project development languages •Combination of couples of diverse CASE-tools and HDLs
4	Fault injection (glitch)	Active	•Altering the input clock; •Creating momentary over- or under-shoots to the supplied voltage	M	H	•Device to execute an incorrect operation •Device left in a compromising state •Leak of secret information	•Making sure all states are defined and at the implementation level, verifying that glitches cannot affect the order of operations; •Detection of voltage tampering from within the device; •Clock supervisory circuits to detect glitches	Diversity of EE: •Different manufacturers of EEs; •Different technologies of EEs production; Diversity of SS •Different SSs; •Combination of diverse CASE tools and SSs

3.2 Building of ASAC

The result of the analysis of requirements of assurance class "Vulnerability analysis" AVA_VAN.3 from International Standard ISO/IEC 15408 is presented in the form of ontological graph (see Fig. 4). The graph accurately and unambiguously (in the accepted notation) describes the subject area (i.e. basic notions/concepts and relations between them). It contains diversity requirements for ensuring of cybersecurity of I&Cs (as countermeasures, Table 3) marked in light-blue fillings.

Completeness of scope of assessment is ensured by using ontological graphs of two kinds of object-oriented and process-oriented ontology. Requirements of assurance class "Vulnerability analysis" AVA_VAN.3 from IEC 15408 are depicted in form of properties (Fig. 5), evidences (Fig. 6) and corresponding actions of an

expert (Fig. 7) as results of ontological analysis of diversity requirements for secure I&Cs (marked with blue and dark-blue) and represented in established ASAC form on figure.

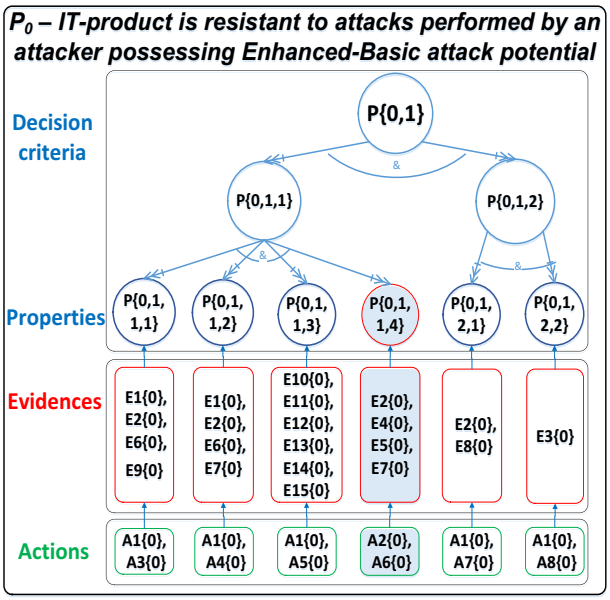

Figure 4. Ontological model in form of graph.

P{J}	PROPERTIES
P{0}	Resistant of the TOE to attacks performed by an attacker possessing Basic attack potential
P{0,1}	Readiness of the TOE for testing
P{0,1,1}	Consistent of the TOE with ST
P{0,1,1,1}	Conformity of the TOE reference with the CM capabilities (ALC_CMC) sub-activities and ST introduction
P{0,1,1,2}	Consistent of the all TOE configurations with ST
P{0,1,1,3}	Conformity of the testing environment to the security objectives for the operational environment described in the ST
P{0,1,1,4}	Conformity of the TOE to diversity requirements
P{0,1,2}	Accuracy of the TOE installing
P{0,1,2,1}	Successfulness completion of the AGD_PRE.1
P{0,1,2,2}	Successfulness of the TOE install and start up, using the supplied guidance only

Figure 5. Properties of ASAC represented in tabular form.

Ei{J}	EVIDENCES
E1{0}	TOE is suitable for testing
E2{0}	Security Target
E3{0}	Guidance documentation
E4{0}	Information is publicly available to support the identification of potential vulnerabilities
E5{0}	Current information regarding potential vulnerabilities (e.g. from an evaluation authority)
E6{0}	Basic functional specification
E7{0}	Security architecture description
E8{0}	Implementation representation of the TSF
E9{0}	Basic modular design
E10{0}	Applicability of different technologies of EEs production
E11{0}	Applicability of different element kinds of EE families
E12{0}	Applicability of different manufacturers of EEs
E13{0}	Applicability of different SSs
E14{0}	Applicability of combination of diverse CASE tools and SSs
E15{0}	Applicability of combination of couples of diverse CASE-tools and HDLs

Figure 6. Evidences of ASAC represented in tabular form.

Ai{J}	ACTIONS
A1{0}	Obtain the evidences
A2{0}	Obtain the diversity applicability evidences
A3{0}	Check the conformity of the TOE reference with the CM capabilities (ALC_CMC) sub-activities and ST introduction
A4{0}	Check the consistent of the all TOE configurations with ST
A5{0}	Check the conformity of the testing environment to the security objectives for the operational environment described in the ST
A6{0}	Check the conformity of the TOE to diversity requirements
A7{0}	Check the successfulness completion of the AGD_PRE.1
A8{0}	Check the successfulness of the TOE install and start up, using the supplied guidance only

Figure 7. Actions of ASAC represented in tabular form.

4 Conclusions

The paper describes cybersecurity assurance technique of multi-version FPGA-based I&Cs. Requirements profile is formulated using the best practices from the following international regulations. The paper summarizes research results on using of security informed safety assessment of FPGA-based MV I&Cs by development of security case based on ASAC. This case considers requirements from Common Criteria and added requirements for diversity as a countermeasure and CCF risk reduction strategy.

Security assurance case tends to reducing of uncertainty of safety assessment taking into account influence of security (cybersecurity) to safety.

It is characterized by introduction of technique of decision making, which is easy to scale, modify, it's in compliance with standards requirements to the

Future steps of research and development will be connected with creation integrative intsrumentation tool to assess secuirty and safety at the all life cycle stages considering features of FPGA-based industrial I&Cs where application of diversity is defined by standard requirements. Other direction of future work is concerned to improve and completely assure computer-based implementation of ASAC-based technique.

References

1. V. Sklyar, Cyber Security of Safety-Critical Infrastructures: A Case Study for Nuclear Facilities, Information & Security An international Journal, **28**, 1 (2012)
2. V. Kharchenko, O. Illiashenko, A. Kovalenko, et. al. Security Informed Safety Assessment of NPP I&C Systems: GAP-IMECA Technique, ICONE 22, Prague, Czech Republic (2014)
3. B. Badrignans, J. Danger, V. Fischer, G. Gogniat, L. Torres, *Security Trends for FPGAs* (Springer, 2011)
4. T. Huffmire, C. Irvine, T. Nguyen, T. Levin, R. Kastner, T. Sherwood, *Handbook of FPGA Design Security* (Springer, 2010)
5. M. Tehranipoor, C. Wang (edits), *Introduction to Hardware Security and Trust* (Springer, 2012)
6. NUREG/CR-7007 ORNL/TM-2009/302 (2009)
7. V. Kharchenko, V. Sklyar (edits). *FPGA-based NPP Instrumentation and Control Systems: Development and Safety Assessment*, (KhAI , 2008)

8. M. Yastrebenetsky, V. Kharchenko (edits). *NPP I&S for Safety and Security*, (IGI-Global, USA, 2014)
9. O. Illiashenko, O. Potii, D. Komin. Advanced security assurance case based on ISO/IEC 15408, DepCoS-RELCOMEX, Brunów, Poland (2015)
10. V. Parondzhanov*, How to improve the work of your mind* (Delo, Russia, 2001)
11. N. G. Bardis, N. Doukas, O. P. Markovski. Burst Error Correction Using Binary Multiplication without Carry, MILCOM 2011 Military Communications Conference, Baltimore, MD (2011)