Security Informed Safety Assessment of Industrial FPGA-Based Systems

Vyacheslav Kharchenko*[a,b], Oleg Illiashenko[a], Eugene Brezhnev[a,b], Artem Boyarchuk[a], Vladimir Golovanevskiy[c]

[a] National Aerospace University KhAI, Kharkiv, Ukraine

[b] Centre for Safety Infrastructure Oriented Research and Analysis, Kharkiv, Ukraine

[c] Western Australian School of Mines, Curtin University, Australia

Abstract: The strong interconnection and interrelation of safety and security properties of industrial system which are based on programmable logic (field programmable gate arrays, FPGA) is reviewed. Information security, i.e. system's ability to protect the information and data from unauthorized access and modification, is a subordinate property with respect to safety of many instrumentation and control systems (I&Cs), primarily to the NPP reactor trip systems. Such subordination may be taken into account by implementation of security informed safety (SIS) approach. The methodology for safety assessment of FPGA-based systems which are widely used in industrial critical systems is described. It is based on joint using of security analysis techniques (GAP-analysis and intrusion modes, effects and criticality IMECA analysis) and also their reflection on the final safety assessment picture of the system with two channels. This methodology forms so called security informed safety approach. Additional aspects of safety assessment of diverse instrumentation and control FPGA-based systems for safety-critical application are described.

Keywords: Safety, Security, Security Informed Safety, FPGA, Assessment

1. INTRODUCTION

The program logic devices and Field Programmable Gate Arrays (FPGA) particularly are widely used for development and implementation of safety-critical industrial I&Cs. FPGA-based systems have irrefutable advantages relatively microprocessor (software)-based ones confirmed by their application in critical domains such as NPP I&Cs, aerospace equipment, etc.

However, the use of FPGA in industrial I&Cs causes specific risks for ensuring of safety. I&C projects on FPGA are complex solutions which include both software and hardware components. Overall and precise safety assessment of modern FPGA-based industrial I&Cs is impossible without taking into account its security properties.

The goal of the paper is the presentation of the technique and tool for of SIS-based assessment of the industrial FI&Cs. The structure of the article is as follows: section 2 describes integration of safety and security into overall safety assessment of the FPGA-based I&Cs, the influence of security on system's safety is given. Main stages of GAP-IMECA analysis and concepts of security informed safety approach are given in section 3. Section 4 contains methodology and case study of proposed security informed safety approach for assessment of diverse FPGA-based industrial I&Cs. The description of the tool for automation of GAP and IMECA analysis stages is presented. Finally paper contains conclusions and directions of future research.

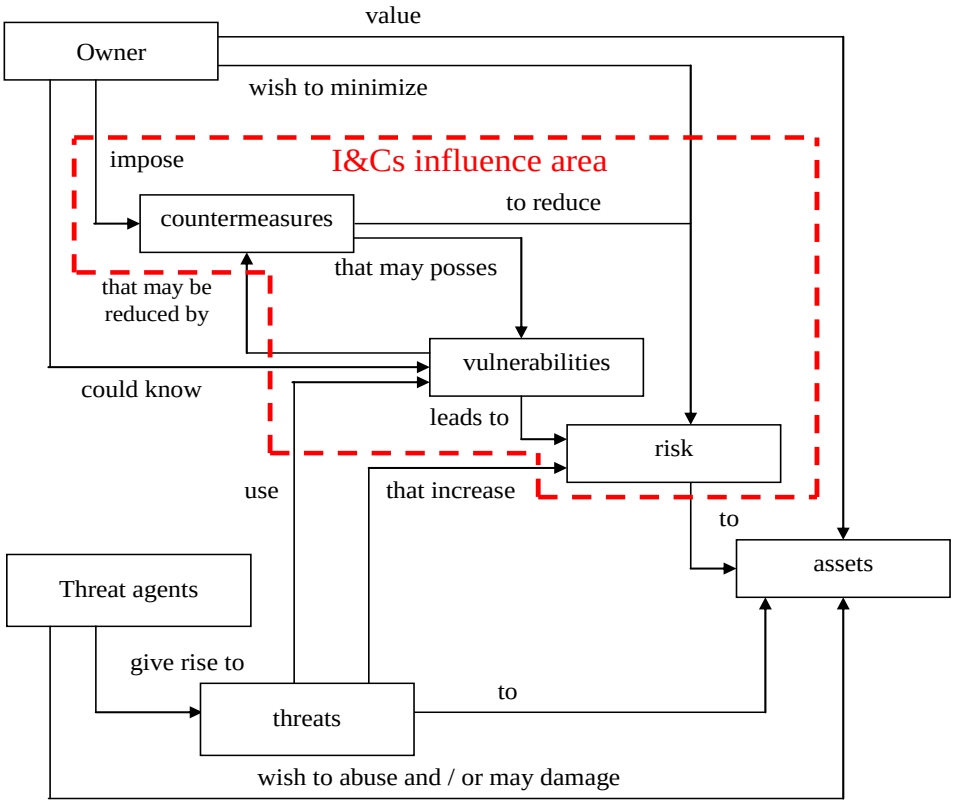
2. SAFETY AND SECURITY INTERRELATION

2.1. The principle of unity of safety and security assessment

Presently there are no integrated approaches for assessment of functional safety (further "safety") and information security (further "security") of complex industrial I&Cs. The overall methodological apparatus in the area of safety and security would allow to assess and

ensure the safety if I&Cs. It should be based not only on traditional approaches and experience of experts (separated analysis of safety and security) but, primarily considering the allocation of general and private features both for safety and security.
According to well-known international standard ISO/IEC 15408 [1] security is connected with defense of assets from threats, where threats are classified based on abuse potential securable assets. All kinds of threats should take into account, especially those associated with human actions, malicious or otherwise. Figure 1 shows high-level security concepts and their relationships, the security model taking from ISO/IEC 15408 standard series. The area of notions in which influence of I&Cs is occurred is dotted with red color.

Figure 1: Security concepts and relationships according to ISO/IEC 15480 series



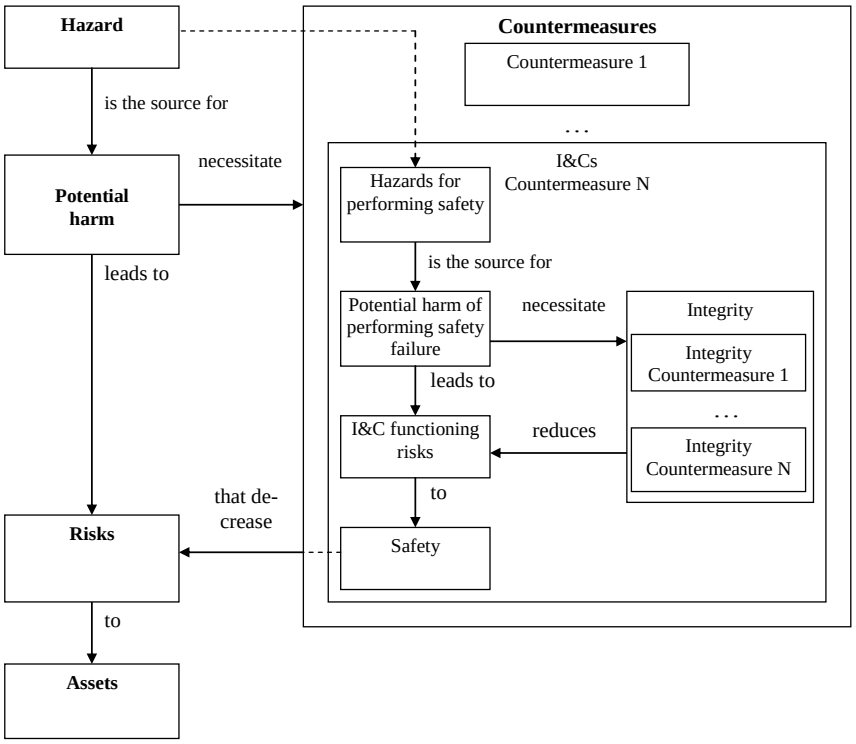
This area is specific for industrial I&Cs in frame of assessment and assurance of its security. It encompasses the following entities [2]:

- countermeasures for risk reduction (because some I&Cs could be one of the such countermeasures, e.g. I&Cs important to safety),
- vulnerabilities (because from the one side I&Cs aimed at vulnerabilities elimination and from the other they could have vulnerabilities itself),
- risks (from the one side I&Cs, as countermeasures itself, aimed to decreasing the risks, and from another they could produce additional risks to the system).

The difference between security analysis and safety analysis is lying in the assets for which the analysis is performed (safety analysis – for critical objects of control and management (OCM), security analysis – for information assets).The appropriate representation of this interrelation is shown on figure 2. Depending on I&Cs assets and safety functions that are performed the "flow" of functional safety into information security and vice versa is taken place. For information assets security is taken into account and in this case safety aimed at

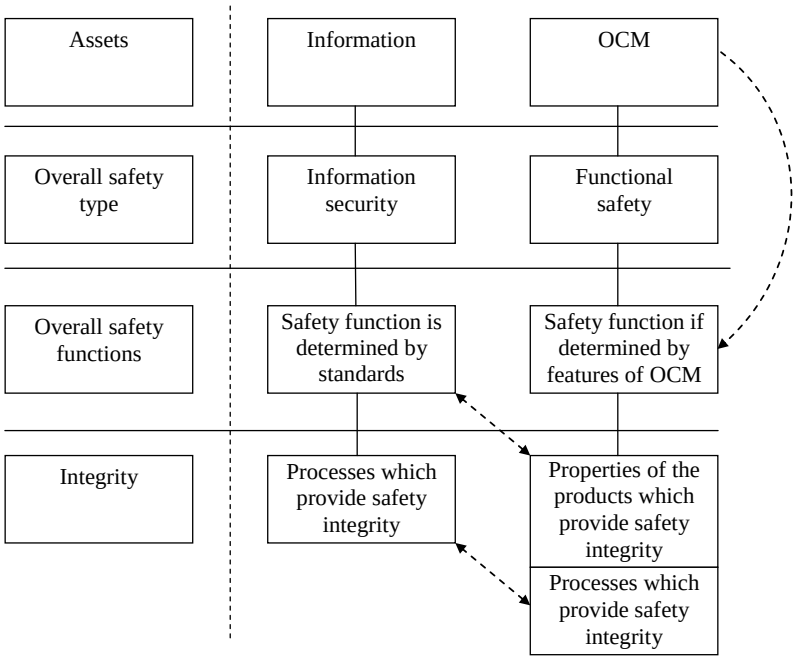
ensuring of safety integrity. It should be noted that for information assets safety functions and processes which ensure security integrity are determined in series of ISO/IEC 15408 standards. For OCMs safety functions are determined by specific features of object and they should be regulated by industry standards.

Figure 2: The structure of objects which are used during safety analysis: integration of level of assets and I&Cs



The interrelation of safety and security is presented on figure 3.

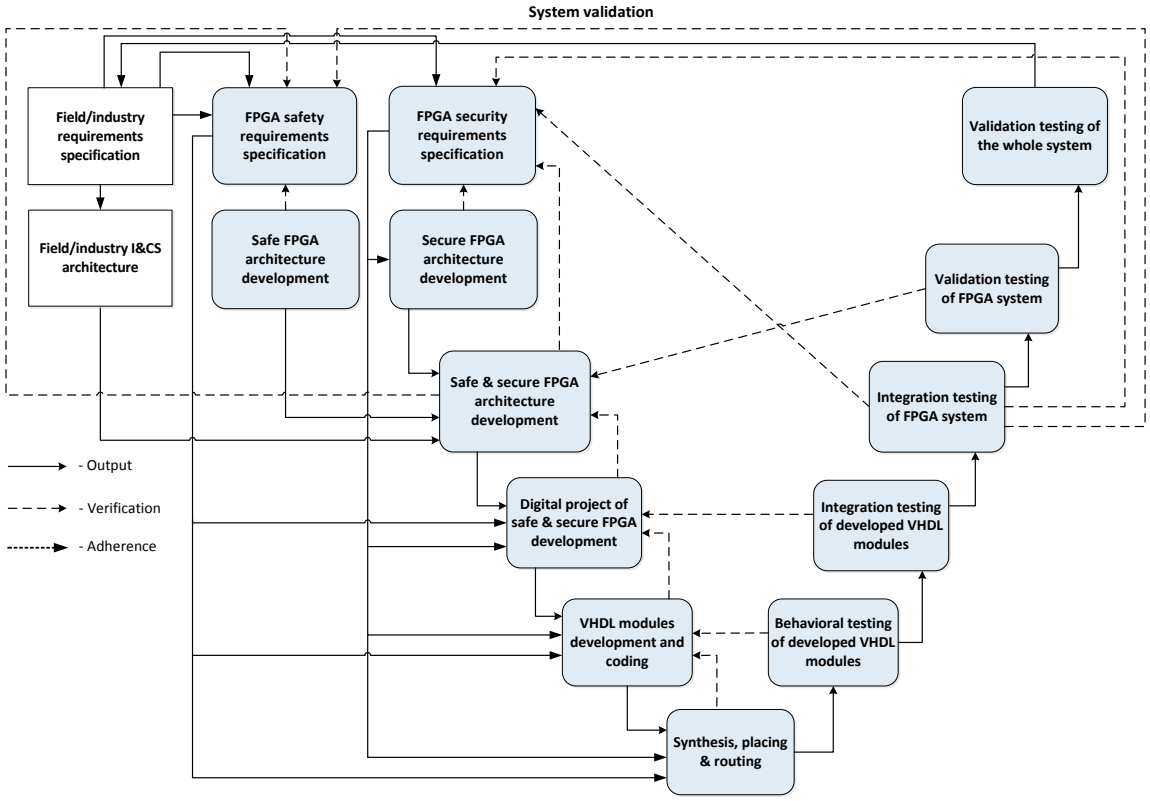
Figure 3: Safety and security cross influence



2.2. Safety and security lifecycle model of FPGA-based I&Cs

To assess security of critical FPGA-based I&Cs (FI&Cs) it is needed to refine the life cycle (LC) model and the strategy for reporting about development process, including control of environment and development tools. LC model is a structured and systematic model covering the development and operation phase of a system. Ideally, it shall be possible to verify the output of each stage of development LC, which should be the successful implementation of the considered input stages. Taking into account I&Cs safety and security needs, general safety life cycle model based on the model of application-specific integrated circuit development lifecycle (standard IEC 61508 [3]) and security LC model (based on standards IEC 15408 [1], IEC 62645 [4]), the joint security and safety LC model for FI&Cs, taking into account features of FPGA technology, is proposed.

Figure 4: Safety and security lifecycle model of FPGA-based I&Cs



In figure 4 two rectangles depict activities that are not directly related to the project based on FPGA development LC, but they play regulatory role during the development of such systems. Rectangles with rounded corners depict the activities related exactly to the stages of development LC. The arrows of different types are shown the relationships between the above LC activities. Adherence of safety and security depicts with a dotted line.

One of the important challenges is balance between safety and security requirements in critical systems and cost for providing safe and/or secure architecture of critical I&Cs. The weak spot hides in specification of clear and precise safety and security requirements for I&CSs under development to avoid the situations when these requirements will contradict with each other and also to examine the system in accident regimes when safety and security requirements could conflict with each other in order to guarantee that the system will operate in an appropriate way in such situations.

3. GAP-IMECA SECURITY ASSESSMENT TECHNIQUE

3.1. GAP-analysis technique

Key principle in the security assessment is the use of process-product approach, which consists in determination of the possible problems and discrepancies in the final product and product development process. One of the fundamental concepts behind the idea of the approach is the concept of GAP, which is determined as a set of discrepancies of any single process within the lifecycle of I&C system that can introduce some anomalies (e.g. vulnerabilities) in a product and/or cannot reveal (and eliminate) existing anomalies in a product.

Depending on FI&Cs under consideration, each GAP is represented in a form which determines all discrepancies. The formal description should be made for a set of discrepancies identified within the GAP. GAP-analysis technique and used notions is described in detail in [7,8].

3.2. IMECA-analysis technique.

The IMECA analysis is actual refinement of FMECA-analysis (Failure modes, effects and criticality analysis) applied to security (analysis of modes and effects of intrusion to the system). Each identified GAP could be represented by a single local IMECA table and each discrepancy inside the GAP can be represented by a single row in that local IMECA table taking into consideration process-product features of the FPGA and FI&Cs itself. For each GAP, a separate table that contains all the vulnerabilities identified in the GAP analysis is created. All separated tables are combined into general IMECA table. IMECA-analysis technique with all supporting theoretical material is presented in detail in [7,8].

3.3 Criticality matrix

Each row (vulnerability and effect of intrusion) of the general IMECA table is represented by the cell of criticality matrix according with its probability and severity in context of FI&C safety. The integrated metric is calculated using criticality matrix. If any of the vulnerability parameters is not included in the allowed range, a corresponding countermeasure should be implemented.

3.4 Security informed safety approach

Safety systems operate in an open environment and they need to be secure in order to be safe. Both security and safety are sophisticated engineering cultures that emphasize the need for good process, the importance of risk analysis and the need for assurance and justification. Besides, security informed safety (SIS) approach was described in [5,6] in wide context for critical infrastructure safety assessment. This approach is based on the use of structured safety cases.

The problems of assessment and assurance of FPGA-based I&Cs safety and security were earlier researched: [2, 6-9]

- consideration of possible vulnerabilities that may occur in the components due to any anomalies in the earlier phases of the life cycle;
- development of the product security threat models;
- ranging of identified vulnerabilities in accordance with their criticality and severity;

- determination of both sufficient and cost-effective countermeasures either to eliminate identified (or even possible) attacks, vulnerabilities and threats or make them difficult (or even impossible) to exploit by an attacker.

4. SIS ASSESSMENT OF DIVERSE FPGA-BASED I&Cs: CASE STUDY

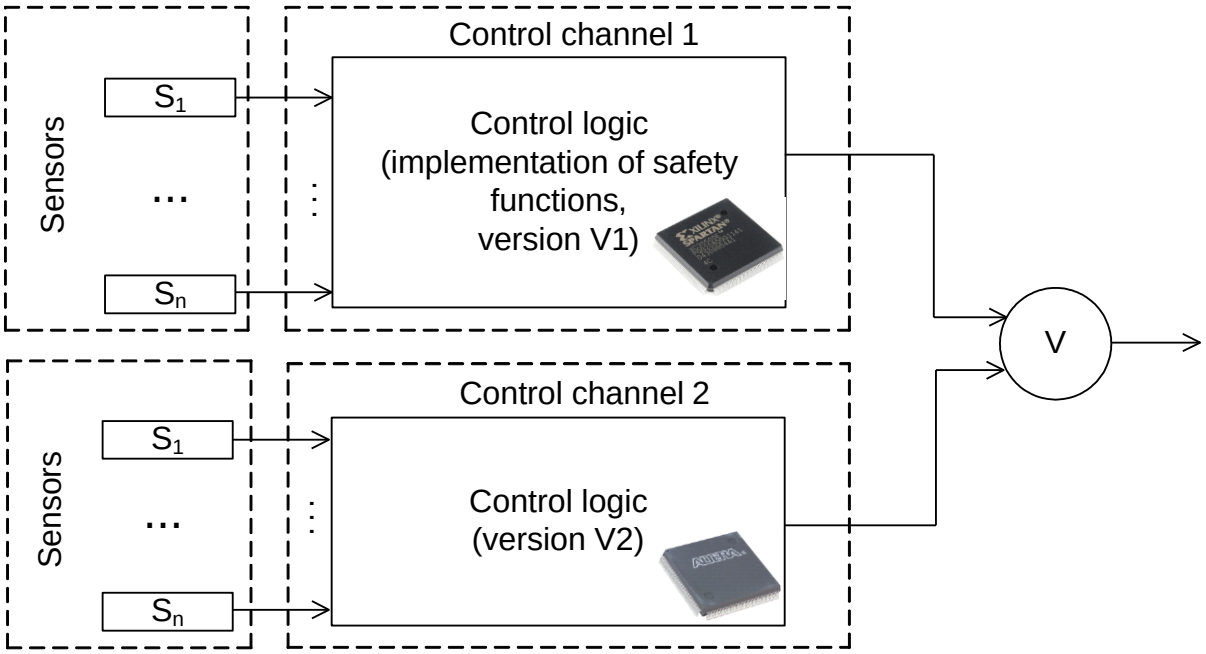
4.1 Version redundancy principle

To provide reliability and safety for I&Cs the principle of version redundancy or diversity is widely used ("is there an appropriate element of redundancy against each failure condition for which one is required?"). Using version redundancy it is possible to increase the reliability and ensure functional safety of I&Cs [10]. It assumes performance of the same problem with two or more methods (versions), processing the data obtained for the control, selection or formation of a final or intermediate results [11,12]. Need to use of the version redundancy principle is due to a fact that only when it is applied it is possible to confront the most dangerous in terms of their consequences for redundant structures (or redundant processes) mean failures, so-called common cause failures (CCF) [13]. Version redundancy principle is widely used for industrial I&Cs protection [14]. Due to this failure there exists a defect (error), which causes losses of operability of all channels of the system (or causes negative results of processes performed) independently from the number of reserved channels (redundant processes).

4.2 Diverse FI&Cs SIS assessment technique

The example that follows illustrates the problem in general. It describes simplified architecture of 2-channel platform RadICS™, which composed of multiple type of modules, based on the use of FPGA-chips as computational, processing and system-internal control engine for each of the modules [15]. RadICS™ is used for installation and implementation of the biggest ESFAS systems on-line for VVER-1000 type reactors with full "hot" redundancy and double diversion (figure 5). Safety controller of RadICS is based on FPGA.

Figure 5:Diverse system with two channels



Let us also suppose the architecture is such that for an accident to happen it is necessary that both channels exhibit failures (erroneous behaviour) that would cause an accident if that channel were the whole FPGA-based controller (critical channel failures). That is, the system is safe as long as at least one channel's behaviour satisfies a safety condition. If one out of two channels fails then the remaining channel is able to detect the failure and trigger a transition to a failsafe state. In the mentioned example for implementation of safety functions of safety controller in control channels 1 and 2 different types of FPGA are used (e.g. produced by Xilinx and Altera vendors). The type and number of sensors are the same, so they didn't take into account. It is assumed that voting unit is absolutely safe and reliable (it will not fail and works properly).

Based on the analysis of possible FPGA vulnerabilities for both vendors it is possible to choose several types of intrusions (attacks), among which the brute force will reviewed. Good brute force attack is time and resource consuming and hackers are likely to pass this attack type, but it's is good applicable for the example of analysis provided.

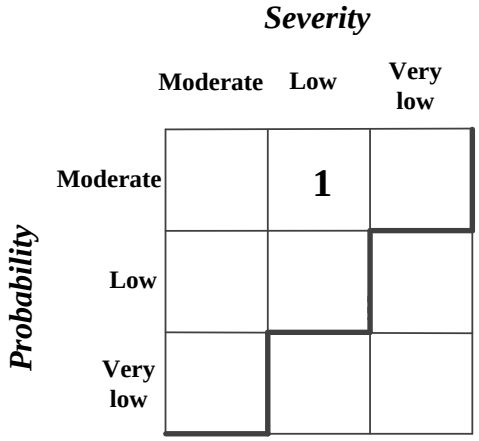
Table 1 shows application of IMECA technique for analysis of abovementioned intrusion (brute force attack) with possible countermeasures which are based on the experience of FPGA use and some recommendations derived from [16]. It describes a regulatory position that promotes a defensive strategy consisting of a defensive architecture and a set of cyber security controls based on standards provided in documents that are based on well-understood threats, risks, and vulnerabilities, coupled with equally well-understood countermeasures and protective techniques [17, 18]. As an example of gap that could lead to successful implementation of brute force attack could be in violation of (C.3.7, Appendix C to RG 5.71, Page C-7: "…Employing hardware access controls (e.g., hardwired switches), where technically feasible, to prevent unauthorized software changes…") requirement from [16]. Going back to the safety and security lifecycle model of FPGA-based I&Cs it is possible to state that this attacks (intrusion) could be mitigated if the appropriate preventive actions would take place during the stage "FPGA safe and secure architecture design".

Table 1: Result of IMECA analysis for brute force attack

Gap №	Attack mode	Attack nature	Attack cause	Occurrence probability	Effect severity	Type of effects	Countermeasures
1	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	Low	Moderate	Leak of undesirable information	• Detecting and documenting unauthorized changes to software and information

This type of attack could be applicable to both channels of FI&Cs and both FPGAs. And as soon as both channels performs the same logic, criticality matrixes will be the same (figure 6). The number inside of the matrix represents an appropriate row number of IMECA table.

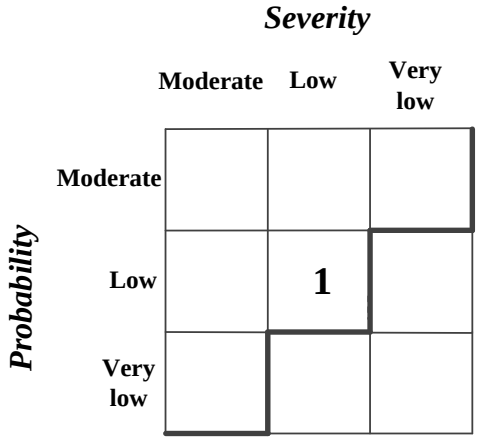
Figure 6: Criticality matrix of brute force attack



From security assurance point of view, the possible way of risk reduction is in decreasing of attacks' occurrence probability, since related damage is constant. Such decreasing of the probability can be achieved, for example, by implementation of certain process countermeasures.

The next important step is transformation of security-oriented criticality matrix that was received during GAP-IMECA-analysis into safety-oriented criticality matrix, which means the reevaluation of potential risk for the system. New, safety-oriented criticality matrix is shown on figure 7.

Figure 7: Criticality matrix of brute force attack



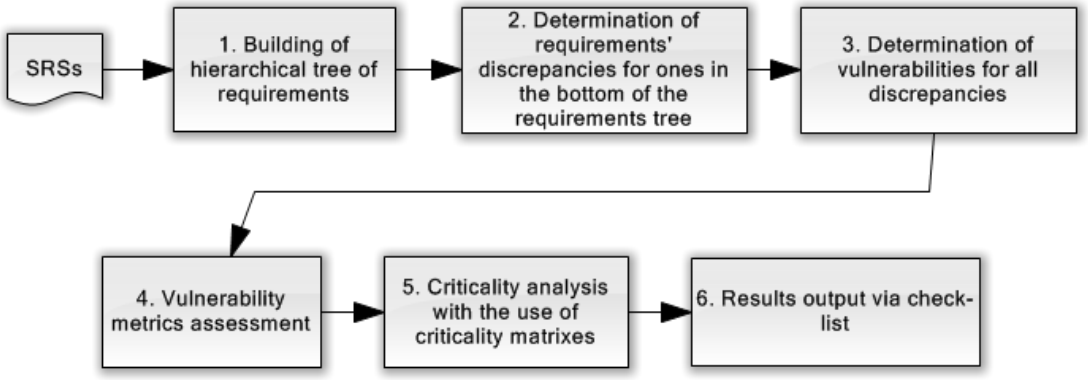
The probability (likelihood) of successful attack of the same type which is implemented into one of the channels was considered in this section.
Taking into account diversity of the control logic functions the following statements are true:

- the probability of successful attack of the same type decreased if resources of attacker is fixed,
- the probability of successful attack of the same type which is applied for both channels decreased if resources of attacker is fixed,
- during analysis of system both vulnerabilities of channels separately and of system (as combination of diverse channels) should be taken into account.

4.3 SIS-GAP-IMECA diversity analyzer tool

To decrease the risk of manual errors, the tool for the SIS-oriented assessment automation is described. The tool is based on joint use of abovementioned models and techniques, is proposed. The tool allows conducting the joint use of the following analysis techniques: GAP and IMECA. The block-scheme of main stages of analysis is shown on figure 8.

Figure 8: The general scheme of analysis process



The ideal system is represented by requirements profile (SRS), which contains all elements of the system of process on the different levels of decomposition.

Input data is requirements profile. Requirements could be divided into different levels hierarchically. After determination of quantity of requirements levels the list of requirements for each level is composed. Levels of requirements are filled alternately from top to bottom. When filling one level, for each requirement of the current level the requirements on the lower level, which expand, clarify or detail it, are created. As a result, the requirement at one level can meet one or more requirements of the level below (Step 1 and Step 2).

After input of requirements their analysis at the lowest level is conducted. It is assumed that requirement could be violated, i.e. GAP is introduced artificially and detailed further. During the analysis of the requirement, the specific violations that may possibly occur depending on the nature of requirement are pointed out. In such way GAP is represented as a set of violations of a certain requirement, which could take place in the critical FPGA-based I&Cs under consideration. At this stage the IMECA-tables are formed for each discrepancy (Step 3, Step 4). It could also be defined more options, which could be determined by expert assessment or additional methods of analysis. One of the required parameters is the likelihood and critical impact on the system. The additional parameters also could be defined with the help of expert assessment or with the use of additional methods of analysis. Above the parameters under assessment are the likelihood and impact on the criticality of the system. Quantitative parameters can be determined by peer review or other auxiliary tools and techniques.

For each GAP, a separate table that contains all the vulnerabilities identified in the GAP analysis is created. Each vulnerability is determined by the criticality matrix. With the help of criticality matrix on the basis of vulnerability parameters the metric should be calculated and resulting conclusion for vulnerability shall be made. For the criticality matrix the set of valid parameters is defined.

If any of the parameters of the vulnerability are not included in the allowed range, a decision that the vulnerability is present in the system and requires fixing is made (Step 5).

The presence of discrepancy is determined on the basis of criticality matrix. Check-list is formed from the requirements and a conclusion about their implementation (Step 6). Example of check-list is shown on figure 5.

5. CONCLUSION

Ensuring security and safety of industrial FI&Cs must be done with a special care, because their development is under the strict constraints related to resources and cost. It should be done iteratively, rather than the disposable decision.

Features of project development with the use of FPGA technology are represented in safety and security LC model. Based on FPGA technology a set of safety and security assurance processes is formed. This set of processes allows further implementation of process-product approach to assessment and to optimize choice of countermeasures

Thus it was described the proposed security informed safety approach for safety assessment of diverse industrial FPGA-based instrumentation and control systems. It may be used to provide security analysis and safety related risks. Future research will be dedicated to formalization of assessment procedure and description of different types of attacks effects (effect for 1 channel, effect for the whole system) depending on the attacker's resources, quantity of vulnerabilities, ways of successful attacks on them and quantity of attackers, and extension of tool for the tasks of countermeasures choice. Developed tool could be expanded for GAP-xMECA analysis.

References

[1] ISO/IEC 15408:2009, *"Information technology – Security techniques – Evaluation criteria for IT security"*, 2009.

[2] V. Kharchenko, V. Sklyar, E. Brezhniev, *"Safety of information and control systems and infrastructures"*, Palmarium Academic Publishing, 2013.

[3] IEC 61508:2010, *"Functional Safety of Electrical /Electronic/Programmable Electronic Safety-related Systems"*, 2010.

[4] IEC 62645:2013, *"Nuclear power plants - Instrumentation and control systems - Requirements for security programmes for computer-based systems"*, 2013.

[5] R. Bloomfield, K. Netkachova, R. Stroud, *"Security-Informed Safety: If It's Not Secure, It's Not Safe"*, Software engineering for resilient systems, Springer, pp. 17-32, 2013.

[6] O. Illiashenko, V. Kharchenko, G. Jervan, *"Security of industrial FPGA-based I&C systems: normative base and SIS approach"*, Radioelectronic and computer systems Scientific and technical magazine №3(62), National Aerospace University KhAI, pp.86-91, 2013.

[7] V. Kharchenko, A. Kovalenko, A. Andrashov, A. Siora *"Gap-and-IMECA-based Assessment of I&C Systems Cyber Security"* Complex Systems and Dependability, Advances in Intelligent and Soft Computing, pp. 149-164, 2012.

[8] O. Illiashenko, V. Kharchenko, A. Kovalenko, "*Cyber Security Lifecycle and Assessment Technique for FPGA-based I&C Systems"*, EWDTS-2012 (East-West Design and Test Symposium 2012), Proceedings of IEEE East-West Design & Test Symposium (EWDTS 2012), pp. 432-436, 2012.

[9] V. Sklyar, *"Cyber Security of Safety-Critical Infrastructures: a Case Study for Nuclear Facilities, Information & Security"* An international Journal, Vol. 28, No.1, pp. 98-117, 2012.

[10] V. Akimov, V. Lapin, V. Popov, V. Puchkov, V. Tomakov, M. Faleev, "Reliability of technical systems and technogenic risk", Business Express, 2002.

[11] V. Kharchenko, V. Sklyar, A. Siora, "*Multi-Version FPGA-Based Nuclear Power Plant I&C Systems: Evolution of Safety Ensuring"* Nuclear Power: Control, Reliability and Human Factors, INTECH, 2011.
[12] V. Kharchenko, V. Duzhyi, V. Sklyar, A. Volkoviy, *"Diversity assessment of multi-version NPP I&C Systems: NUREG7007 and CLB-BASED techniques"*, East-West Design and Test Symposium proceedings, pp. 1-5, (2013).
[13] R. Wood, R. Belles, M. Cetiner, D. Holcomb, K. Korsah, "*Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems"*: NUREG/CR–7007 ORNL/TM–2009/302. – U.S. Nuclear Regulatory Commission, Oak Ridge National Laboratory, pp. 251, 2010.
[14] B. Littlewood, P. Popov, L. Strigini, *"DISPO project: A Summary of CSR Work on Modelling of Diversity"*, Centre for Software Reliability, City University, London, UK, 2006.
[15] http://www.radiy.com/eng/products/fpga_based_systems/fpga_based_platform/
[16] Regulatory Guide 5.71, *"Cyber security programs for nuclear facilities"*, U.S. Nuclear regulatory commission, 2010, 105 pp.
[17] NIST SP 800-52, *"Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations Computer Security"*, National Institute of Standards and Technology Special Publication 800-52, 2005, 33 pp.
[18] NIST SP 800-53, *"Information Security, Security and Privacy Controls for Federal Information Systems and Organizations"*, National Institute of Standards and Technology Special Publication 800-53 Revision 4, 2012, 375 pp.