УДК 004.056, 004.75

Andriy Kovalenko, Oleg Rudenko

andriy_kovalenko@yahoo.com, *ro590@yahoo.de*

Simon Kuznets Kharkiv National University of Economics, Kharkiv

GAP-AND-IMECA-BASED APPROACH TO ASSESSMENT OF COMPLEX I&C SYSTEMS CYBER SECURITY

Complex instrumentation and control (I&C) systems are complex systems that consist of both hardware and software components, which continuously interact with each other in order to perform their intended functions. One of the development and operation problems of modern I&C systems for critical application is the reliable assessment and assurance of the two main system attributes, namely safety and cyber security. The assessment of cyber security, which also influences the safety of I&C systems and other controlled applications, is a very important, complicated, and challenging problem. During the assessment, it is necessary to take into account a set of various features and factors, their interrelations and interactions. Modern realities require improving I&C systems security, both in terms of requirements and their implementation. Moreover, assurance of cyber security for critical I&C systems is a requirement of national and international regulatory documents, as well as actual practice in safety engineering [1].

The Field Programmable Gate Arrays (FPGA) technology is now being widely used worldwide in process industries, and increasingly in I&C systems for various safety and security critical domains, such as Nuclear Power Plants (NPPs), on-board computer-based systems, electronic medical systems, etc. [2,3]. The application of FPGA technology allows developers to implement the required functions in a convenient and reliable way.

Nowadays the problem of cyber security assessment and assurance for FPGA technology as a whole, and application of the technology in I&C systems in particular, is not comprehensively solved due to several reasons, which are discussed.

Various aspects and challenges of I&C systems are analyzed in terms of cyber security, on the basis of existing regulations (including drafts), which cover various aspects of I&C systems development and operation (including safety-related applications), FPGA technology implementation, and cyber security assessment and assurance in context of safety as a whole. Such analysis revealed that the requirements in all the three categories do not completely cover all the aspects of FPGA technology application in I&C systems, as well as, in particular, the requirements do not consider all the possible security-related challenges of FPGA technology.

It is proposed an approach that can be used during FPGA-based I&C systems cyber security assessment. Such approach covers life cycle processes, products, and appropriate requirements; it is based on FPGA technology and FPGA-based I&C systems vulnerabilities assessment thorough the whole life cycle. Proposed approach requires that each of revealed possible vulnerabilities for FPGA technology should be assessed using GAP-analysis on the basis of Intrusion Modes, Effect and Criticality Analysis (IMECA) technique and Security Block Diagram .

IMECA is a modification to standardized FMECA technique, which takes into account a set of possible intrusions to a system and can be applied for determining both the weakest parts of such system, in terms of cyber security, and the required countermeasures.

The results are represented by IMECA table, which covers all the security aspects of the whole life cycle in a convenient and clear way. It is also possible to develop security criticality matrix on the basis of IMECA table; such table along with the matrix represents a case of FPGA-based I&C system cyber security assessment in order to further cyber security assurance in context of the whole I&C system via appropriate prevention measures.

Application of the proposed approach for assessment of FPGA-based I&C system is described.

References

1. *IEC 61508:2010 (2010) Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems*

2. *NUREG/CR-7006 (2010) "Review Guidelines for Field-Programmable Gate Arrays in Nu-clear Power Plant Safety Systems," U.S. Nuclear Regulatory Commission, February 2010*

3. *Kharchenko V, Sklyar V (Edits) (2008) FPGA-based NPP Instrumentation and Control Systems: Development and Safety Assessment, Research and Production Corporation "Radiy", National Aerospace University named after N.E. Zhukovsky "KhAI", State Scientific Technical Center on Nuclear and Radiation Safety, 2008, 188 p*