SECURE ENVIRONMENT ESTABLISHMENT FOR FPGA-BASED SAFETY-CRITICAL SYSTEMS: QUALITY MANAGEMENT SYSTEM CONTEXT

Vyacheslav Kharchenko, Andriy Kovalenko
Centre for Safety Infrastructure-Oriented Research and Analysis
37 Astronomicheskaya str., Kharkiv, 61085, Ukraine
v.kharchenko@csn.khai.edu; andriy_kovalenko@yahoo.com

Ievgen Brezhniev
Radics LLC
29 Geroyev Stalingrada str., Kropyvnytskyi, 25009, Ukraine
milestone@list.ru

Kostyantyn Leontiiev
Research and Production Corporation Radiy
29 Geroyev Stalingrada str., Kropyvnytskyi, 25009, Ukraine
ksleontiev@gmail.com

ABSTRACT

The paper discusses importance of secure development and operational environment establishment process, its particular stages, including security-oriented analysis and assessment of safety-critical instrumentation and control (I&C) systems. Two particular aspects are covered – security assessment and security assurance related to processes established by Quality Management System (QMS).

One of the underlying ideas for the security assessment approach is in performance of gap analysis. Such analysis considers influence of all different factors within I&C system development process, and further application of Intrusion Modes and Effect Criticality Analysis (IMECA) technique. It makes the approach applicable to various safety-critical systems, considering underlying technologies (for example, Field-Programmable Gate Arrays (FPGA).

Nowadays FPGA technology is often used in wide spectrum of hardware devices – from personal devices to complex I&C systems for Nuclear Power Plants (NPPs). The problem of cyber security assessment and assurance for FPGA technology in general and its application in safety-critical I&C systems in particular is not completely solved due to several reasons that cover regulations, QMS processes, implementation of development and verification activities, etc.

The paper overviews existing regulations, which cover various aspects of NPP I&C systems development and operation, FPGA technology implementation, and secure development and operational environment establishment and assurance. The paper also emphasizes that complex approach should be used to identify and mitigate all specific vulnerabilities thorough the whole life cycle on the basis on Intrusion Modes, Effect and Criticality Analysis technique.

The paper also proposes approach to the development of safety-critical I&C systems in the scope of cyber security assurance process at developer site. Secure development environment is described as a key factor during the development process and the paper also discusses establishment and maintenance of such environment as a part of company's Nuclear Quality Assurance's QMS.

Key Words: I&C, system, QMS, secure, environment

1 INTRODUCTION

The aspect of cyber security in the development of industrial systems used for production management or sophisticated process control becomes more and more interesting. Partly, this fact is explained by the increasing number of cyber attacks on systems of SCADA type.

Analysis of modern trends shows the strong growth of attacks aimed at industrial and other I&C systems, starting from 2010 (just after Stuxnet case). Thus, in particular, in February 2011, it was successfully implemented "Night Dragon" massive attack aimed at five petroleum-refining companies. During 2012, a number of major companies, operating in a banking area of Syria, Lebanon and Sudan, detected a spyware ("Flame" worm). The example shows obviously growing trend for a number of cyber attacks on various industrial and other safety-critical I&C systems, and such a trend will continue its rapid strengthening.

The developers of industrial and safety-critical systems, including those based on Field Programmable Gates Array technology, try to improve their protection against attacks, reduce risks and potential cyber vulnerabilities. During implementation of security requirements for such systems, designers are trying to develop a safe product. A set of applicable security requirements covers regulatory requirements, customer requirements and others. However, very often a general set of requirements is not consistent and not harmonized. For the developers of a software and FPGA design for NPP Instrumentation and Control systems, one of the initial problems is security informed safety analysis, requirements assessment and identification of the priorities. [1]

Results of such analysis can be used for development of practical approaches aimed at compliance with the complete set of relevant requirements. It should be noted that requirements analysis and development of approaches are not separate tasks. It is typical to deal with a variety of interrelated problems, which inputs and outputs are interconnected. At the same time, about 74% of the organizations implement their mechanisms for verifying compliance with the product/process security requirements mostly using manual methods and tools, which demonstrate the lack of satisfactory solutions in 37% of cases. [2]

Thus, we can talk about the necessity in such design processes, which can assure security properties for the product and ensure further automation and software support. Such a process is, in fact, one of the critical business processes of the company, aimed at achieving both customer satisfaction and required properties of the final product, including those related to security. Development of an effective security assurance process for the product can be based on the use of approaches to business processes engineering. [3]

During development of security assurance process, the following aspects should be taken into account: company's available resources, the level of personnel training, requirements to the products, the maturity of the technologies used, etc. An important basis for the design process is the company's Quality Management System, which is an essential component of business management system. It contains a description of all company's business processes that guarantee for the manufacture of quality products.

The purpose of the paper is to analyze joint issues of security assurance processes and QMS in the context of requirements of US Nuclear Regulatory Commission (US NRC), and to describe QMS-based security assurance process.

2 PROCESS-BASED APPROACH TO SECURITY ASSURANCE

2.1 Analysis of Security Requirements

NPP I&C system is an example of safety-critical systems with strict requirements to functional safety and security. In particular, in the United States, US NRC actively applies a set of regulations and, from our point of view, in terms of security, the most important are the following:

– 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants";

– 10 CFR 73.54, "Protection of digital computer and communication systems and networks";

– NQA-1a-2009, "Quality Assurance Requirements for Nuclear Facility Applications";

– Regulatory Guide (RG) 1.152-2011, Revision 3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants";

– IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations";

– IEEE Std 603-1991, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations";

– DI&C-ISG-01, Revision 0, "Cyber Security Associated with Digital Instrumentation and Controls";

– DI&C-ISG-06, Revision 1, "Licensing Process";

– RG 5.71, "Cyber Security Programs for Nuclear Facilities";

– IEEE Std 1074-2006, "IEEE Standard for Developing a Software Project Life Cycle Process";

– NUREG/CR-7117, "Secure Network Design";

– NIRMA TG-16;

– Branch Technical Position (BTP) 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems".

Such regulations govern many aspects, covering most of product's life cycle (LC) stages starting from creating Secure Development Environment (SDE) and finishing with assurance of security properties of the final product. However, problems related to integration of security-related activities into product's LC model, are still challenging and unresolved. In terms of safety-critical systems, cyber security, first of all, is related to security controls intended to protect from malicious acts critical assets and I&C systems under development at developer's site, as well as I&C systems during operation at the customer's site.

IEEE Std 603-1991 is focused on importance of administrative controls for protection of NPP I&C systems hardware, as well as necessity in combined controls (for example, physical and electronic) for protective actions to provide access to critical systems and data for authorized personnel only. Moreover, such administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof. [4]

10 CFR Part 50, Appendix B and 10 CFR 73.54 are generic regulations in the area of licensing the production and utilization facilities within the US market. [5, 6]

Security and cyber security aspects are mainly covered by RG 1.152-2011 "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants" [7] and RG 5.71-2010 "Cyber Security Programs for Nuclear Facilities" [8]. First of them describes a method that the US NRC considers acceptable to

implement licensing process with regard to the use of computers in safety systems of NPPs; it provides regulatory criteria on the establishment of a Secure Development and Operational Environment (SDOE) for digital I&C systems via appropriate physical, logical and programmatic controls during development phases and appropriate physical, logical and administrative controls during operation phase. The second is a direct guidance for activities implementation under 10 CFR 73.54 "Protection of digital computer and communication systems and networks", based on international and federal standards. It describes methods and security activities for the operation and maintenance of NPPs, including appropriate I&C systems. Therefore, cyber security features should be designed and implemented during the development phase of the I&C system, before its installation. Security audits are essential part of security assurance process to establish, implement and maintain SDOE.

BTP 7-14 "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems" is a guideline BTP 7-14 "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems" on evaluating software LC processes for digital computer-based I&C systems. It contains main definitions related to security in terms of management and functional characteristics related to software planning , as well as a set of requirements to project planning documents, each of those contains security requirements. [9]

In this way, today there are many security requirements for safety-critical systems. Compliance with such requirements can be achieved while implementation one of the most important company's business processes – SA. It should be developed considering interrelations with other company's processes. Then security assurance process becomes an integral part of company's QMS.

2.2 Comparative Analysis of QMSs Considering Requirements to Security Assurance Process

In general, cyber security assurance process for I&C systems can be implemented in the scope of two QMS types: commercial and special (nuclear).

Traditionally, companies operating in the information technology industry under commercial QMS, and producing non-certified product in terms of cyber security requirements, do not use all the possibilities of the QMS. Often QMS considers only a product-related component of cyber security. This approach is focused on the security testing process to ensure sufficient quality of the product. Representatives of the verification teams include representatives of company's quality management.

ISO standard of 9001 series, which describes QMS model, was developed to assist different organizations to comply with the requirements and expectations of their clients and other parties concerned. In the scope of ISO, there is a set of requirements, which can be indirectly treated as cyber security requirements. Thus, for example, requirements to document control include necessity in assurance of appropriate controls for the following aspects:

– Inappropriate information security (confidentiality loss, integrity loss, etc.);

– Document management (access control, reliable storage, change control, version control);

– Storage life and disposal methods (protection from unintended changes).

Hence, in the scope of ISO series standards, there is only a small set of requirements to documents security and their protection from unauthorized and unintended changes.

Special QMS, though, is more strict in terms of cyber security requirements. The focus of such QMS is not customer satisfaction, but safety/security of the final product. Most attention is given to business processes, which are the most important from the point of view of security functions performed by the product. Thus, for example, in the USA, a company that plans to sell its product on the nuclear market, or to become a supplier to the NPP, shall have a specific 10 CFR Part 50 Appendix B based QMS.

Nuclear Quality Assurance (NQA) standard is a generic industrial standard, which provides 18 criteria (including requirements to the development of all the processes that are important to safety), which, in its turn, meets the criteria of 10 CFR 50 Appendix B.

Nuclear QMS focuses more on aspects of cyber security for safety-important and safety-critical I&C systems. The aspect of the cyber security for the final product is considered throughout the entire LC for the software.

3 QMS-BASED SECURITY ASSURANCE PROCESS FOR PRODUCTS

3.1 Main Elements of a Security Assurance Process

As part of security assurance process development, which is based on QMS, it is appropriate to establish:

– Quality procedures and working instructions;

– The company's policy aimed at the development of safe/secure products;

– Training programs for company's personnel and subcontractors.

Quality procedures describe the processes of secure products development. Their aim is to provide guidance for the design in order to minimize all possible vulnerabilities, which can lead to safety functions failure. This type of quality document also describes the methodology to meet the requirements to reliability, functional safety, quality of the software and SDOE establishment and assurance. In this way, the document describes measures that help develop SDE for the product and assure protection against undocumented and unwanted modifications. It also helps reduce reliability risks and increase operational safety.

Working instructions, in turn, are supplementary, lower-level type of document. They contain a more detailed explanation, if it is necessary, for the methodology described in the appropriate quality procedure.

3.2 Approach to Implementation of a SDOE

SDE is defined as the condition of having appropriate physical, logical and programmatic controls during the system development phases to ensure that unwanted, unneeded and undocumented functionality (e.g., superfluous code) is not introduced into digital safety-critical systems. Secure Operational Environment is defined as the condition of having appropriate physical, logical and administrative controls within a facility to ensure that the reliable operation of I&C systems is not degraded by undesirable behavior of connected systems and events initiated by inadvertent access to the I&C system [7].

For both environments, in a generic case, the main types of components are the following:

– Hardware (including equipment for operation and securing the infrastructure of development and operational environments, equipment used in implementation of development and operation activities);

– Software (including software used in implementation of development and operation activities, as well as software directly related to appropriate infrastructures);

– Data networks (related to development and operational environments);

– Personnel;

– Final product (I&C system during development and operation).

In addition to these types of components, an important aspect is their configuration, which includes a number of factors, covering their physical, logical and behavioral interactions. The configuration depends mostly on the quality and completeness of QMS implementation in both environments, personnel qualifications and quality of used software and hardware components.

The establishment of a SDOE in the context of US NRC's RG 1.152-2011, refers to the following aspects:

– Measures and controls used to establish a secure environment for development of safety I&C systems against undocumented, unneeded and unwanted modifications;

– Protective actions taken against a predictable set of undesirable acts that could challenge the integrity, reliability, or functionality of I&C systems during operations.

Phases of the waterfall LC model form a framework for describing specific guidance(s) for the protection of digital safety systems and the establishing a SDOE via identification and mitigation of potential weaknesses or vulnerabilities in each of the phases that may degrade the SDOE or degrade the reliability of the system.

Security audits are essential part of security assurance process to establish, implement and maintain SDOE. Such audits are implemented on the following basis:

– SDE audit: is conducted after development infrastructure is established and I&C system design/development project is ready to start;

– Periodic SDE audits: are conducted before each of the LC development phases begins.

The purpose of SDE audit is to assess "basic" security level of the development environment. Mainly, appropriate security controls are implemented by hardware (network components, physical protection devices, etc.) Periodic SDE audits are to assess additional specific security controls required during implementation of each LC development phases. Each of the periodic SDE audits includes the following stages:

– Auditing additional specific security controls for certain development phase (i.e. what exactly implemented and how it is implemented);

– Auditing compliance with company's proprietary standards, procedures and instructions, related to SDE (i.e. performance-based assessment of the fact that the personnel activities are in compliance with the requirements of QMS).

The input for a security audit is SDOE audit plan (and, if it is required, a set of documents, related to certain aspects of development infrastructure organization or workflow implementation), and the output is SDOE report, which documents audit results.

Fig. 1 below represents detailed activities on SDOE assurance during different phases of FPGA-based safety-critical systems LC model, including Concept, Requirements, Implementation and Test phases. Such activities are grouped into two categories, related to:

– Assurance of SOE: what features and controls shall be implemented and then tested in the scope of the product to assure its safe operation;

– Assurance of SDE: what generic and phase-specific controls shall be implemented within the development facility to ensure that unwanted, unneeded and undocumented functionality is not introduced into the product during its design, development and testing.

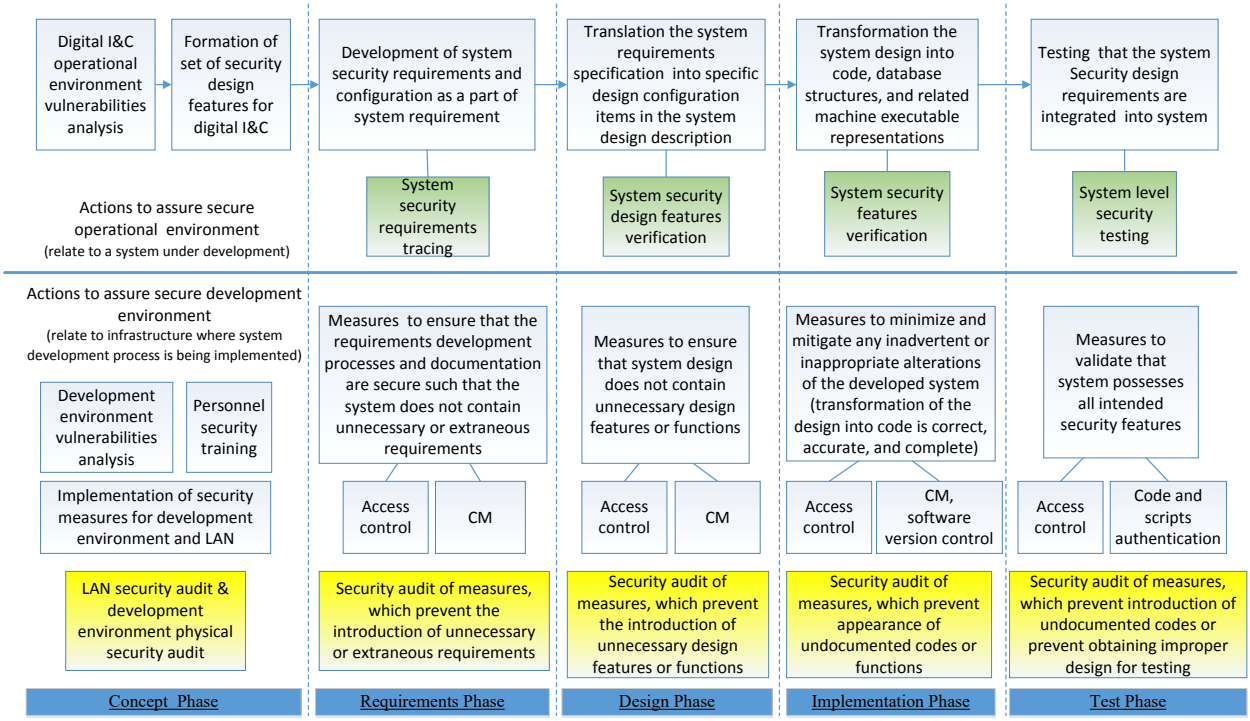

Figure 1. Detailed activities on SDOE assurance.

4 CONCLUSIONS

Cyber security assurance is an important business process of the company. The development of such process should be carried out taking into account the specifics of the company, its resources and technologies. The output of this process is a product that meets the customer's quality requirements and complies with the regulations. Security assurance process shall be implemented within the company's QMS. One of the important stages during design process is establishing the SDE, which can be based on nuclear QMS and its inherent principles.

Security specialists have to work together with quality specialists, paying attention to the problems of product's security, access control, management of records and documents. The company must employ quality specialists who understand the importance of cyber security risks. QMS should focus on cyber security and security team should focus on quality.

An important aspect is to make the process of establishment and monitoring a SDE an integral part of the QMS. To assess the security level of product development environment the Advanced Security Assurance Case (ASAC) approach can be used. The approach is described in [2]. Visualization of estimation algorithm allows to uniquely assess the level of security for development process (and the final product), as well as to conduct an external security audit by a third party. Such approaches and processes are implemented by RPC Radiy and RadICS LLC during the development of NPP I&C systems based on RadICS platform.

5 REFERENCES

1. V. Kharchenko, A. Kovalenko, V. Sklyar, O. Siora, "Security Assessment of FPGA-based Safety-Critical Systems: US NRC Requirements Context," *Proceedings of the International Conference on Information and Digital Technologies (IDT 2015)*, Žilina, Slovakia, IEEE, July 7-9 2015, pp. 117-123. (2015)

2. O. Illiashenko, O. Potii, D Komin, “Advanced Security Assurance Case Based on ISO/IEC 15408,” *Proceedings of the 10th International Conference on Dependability and Complex Systems DepCoS-RELCOMEX*, Brunów, Poland, June 29 – July 3 2015. Advances in Intelligent Systems and Computing, vol. 365, Springer International Publishing, pp. 391-401. (2015)
3. M. Yastrebenetsky, V. Kharchenko, *Nuclear Power Plant Instrumentation and Control Systems for Safety and Security. Advances in Environmental Engineering and Green Technologies (AEEGT) Book Series*, Hershey, Pennsylvania, United States of America, IGI Global. 470 p. (2014).
4. IEEE Std 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” http://ieeexplore.ieee.org/document/159411/ (1991).
5. 10 CFR 50, Appendix B, “Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plant,” U.S. Nuclear Regulatory Commission, http://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-appb.html (2015).
6. 10 CFR 73.54, “Protection of digital computer and communication systems and networks,” U.S. Nuclear Regulatory Commission, http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html (2015).
7. Regulatory Guide 1.152, Revision 3, “Criteria for use of computers in safety systems of nuclear power plants,” Office of nuclear regulatory research, U.S. Nuclear Regulatory Commission, 13 p. (2009).
8. Regulatory Guide 5.71, “Cyber security programs for nuclear facilities,” Office of nuclear regulatory research, U.S. Nuclear Regulatory Commission, 105 p. (2010).
9. BTP 7-14, “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems,” https://www.nrc.gov/docs/ML0706/ML070670183.pdf (2007).