Andriy Kovalenko, Oleg Rudenko

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

Abstract. *This chapter presents an approach to cyber security assessment, which is based on Gap Analysis (GA) and Intrusion Modes and Effects Criticality Analysis (IMECA) techniques, applicable to complex Instrumentation and Control (I&C) systems, including safety-critical FPGA-based I&C systems. Elements of the GA-and-IMECA procedure of assessment are proposed. As an example, the proposed approach and technique are considered in the context of assessing the cyber security properties of FPGA-based I&C systems, taking into account vulnerabilities of products and discrepancies of appropriate processes.*
Keywords: *instrumentation, control, gap, FPGA, system, approach, IMECA, vulnerability, threat.*

Introduction

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]. The application of FPGA technology allows developers to implement the required functions in a convenient and reliable way.

There are several challenging problems in the area of cyber security assurance for complex FPGA-based I&C systems, including the following: consideration of all

possible vulnerabilities that can appear in the final product due to process discrepancies, which were present at earlier stages of the product life cycle, prioritization of such vulnerabilities according to their criticality and severity, determination of both sufficient and cost-effective countermeasures either to eliminate the identified (or potential) vulnerabilities or to make the vulnerabilities difficult to exploit by an adversary. In our opinion, the accurate evaluation of the actual level of the vulnerabilities' criticality and severity (and security of the system in whole) is one of the main challenges. Inaccurate estimation can cause additional efforts, costs and may present undesirable level of risk. In the framework of this chapter, I&C safety is considered as an attribute of high importance. Security is an attribute, which affects safety [3].

One of the possible ways to consider all possible security vulnerabilities for complex I&C systems is using a process-product approach. Such an approach requires performance assessments not only for products (components of the I&C system received at different life cycle stages), but for all the processes within the product life cycle. Application of process-product approach is inevitable in case of FPGA-based I&C systems, due to FPGA's dual nature: it consists of both hardware and software, with its inherent complexity. Such a process-product approach should also be considered in FPGA-specific regulatory documents that would address issues such as system safety assessment, design life cycle, verification and validation, configuration management, documentation requirements, etc. in order to identify all possible discrepancies. Each discrepancy can potentially lead to the introduction of security vulnerabilities (or breaches) into the final product, during the implementation of life cycle processes.

Analysis of related works

Modern authors describe security-related gaps, unique to commercial embedded system design only. Importance and uniqueness of the embedded security challenges, an enumeration of security requirements, concepts, and design challenges are presented. Though, the paper is limited to security processing requirements and architecture, illustrated with a popular secure sockets layer protocol, and processing workload example.

Some papers introduces the concepts of designing secure hardware in embedded systems. The major classes of attacks and the mindset of potential attackers are presented, as well as examples of previous hardware attacks are

discussed. Typical product development cycle and recommends ways to incorporate security, risk assessment, and policies into the process are presented.

Failure Mode, Effects and Criticality Analysis (FMECA) is an extension of standard formalized technique called Failure Mode and Effects Analysis initially intended for the systems reliability analysis devoted to the specification of failure modes, their sources, causes, criticality, and influence on system's operability. "Failure modes" means the ways, or modes, in which something within an I&C system might fail. Failures are any errors or defects in a form of deviations from normal operation, which can affect the user of I&C system, and can be potential (that can happen in future) or actual (that have already happened). "Effects analysis" refers to studying the consequences of those failures. In addition, FMECA extends FMEA (Failure Modes and Effects Analysis) by including a criticality analysis, which is used to chart the probability of failure modes against the severity of their consequences.

In the FMEA-technique, all possible failures are prioritized according to consequences severity, frequency and detectability. Such technique is used during design stages in order to avoid failures in a system being developed. During certain consequent stages it can also be used for the purpose of process control. The overall purpose of FMEA-techniques is to take actions to eliminate or reduce possible failures.

There are a lot of FMECA technique modifications related to various components, including software (SFMECA), to various levels of I&C hierarchy (HFMECA), to various processes, including design (DFMECA) and others. In general cases, Concept and Event Modes and Effect Criticality Analysis may be considered. These modifications are not used to assess I&C security.

IMECA (Intrusion Modes and Effects Criticality Analysis) is a modification to FMECA-technique that takes into account possible intrusions into the system [4]. During the assessment of I&C systems, IMECA can be used in addition to standardized FMECA for safety-related domains, because each vulnerability can become a failure in a case of intrusion into such systems [5].

The objectives of this chapter are to customize the IMECA-technique and to develop an applicable approach to assessment the level of I&C systems cyber security. The rest of the paper is structured as follows: sections below describe the underlying concepts of the gap-and-IMECA-based approach, as well as its application to assessment of safety-critical I&C systems and provide a

methodological-level interpretation of the proposed approach in the context of cyber security of FPGA-based I&C systems.

Conception of gap-and-IMECA-based approach

Here, as one of possible solutions for I&C systems assessment problem, we propose an approach, which is based on IMECA technique.

One of the fundamental concepts behind the idea of the approach is the concept of gap. Before providing a definition for gap, we propose the taxonomy of the main notions used in the chapter. Such taxonomy covers the notions of process, product, intrusion, discrepancy, gap, anomaly, vulnerability and attack (see Fig. 1). We outlined clearly some important attributes of a process, product and intrusion, as well as their interrelations. Also, the proposed taxonomy allows tracing a case of non-ideal process in product development along with possible consequences of process implementation.

The main notions in Fig. 1 are process, product, and intrusion. Processes are being implemented through the development stages of I&C system life cycle model in order to produce products, which can be vulnerable to intrusions of various types. Results of implementation of the processes can have effects on possible consequential changes in such processes. Each process comprises activities, and, in a case of "non-ideal" process, some of them can contain discrepancies.

So, now we can define gap as a set of discrepancies of any single process within the life cycle of I&C system that can introduce some anomalies in a product and/or cannot reveal (and eliminate) existing anomalies in a product. In particular, such anomalies can be caused by imperfection of product specification, implementation, verification, and/or other non-compliances.

In terms of cyber security, some of the anomalies can be vulnerabilities of the product. Vulnerabilities, in turn, can be exploited by an adversary during intrusion into the product to implement an attack in order to introduce some unintended functionality into the product.

Direct relation between vulnerabilities and unintended functionality in Fig. 1 denotes some possible situation, which is not covered by the scope of this chapter; such a situation may occur in the presence of hardware Trojans within the components of the product, and, hence, requires additional comprehensive analysis.

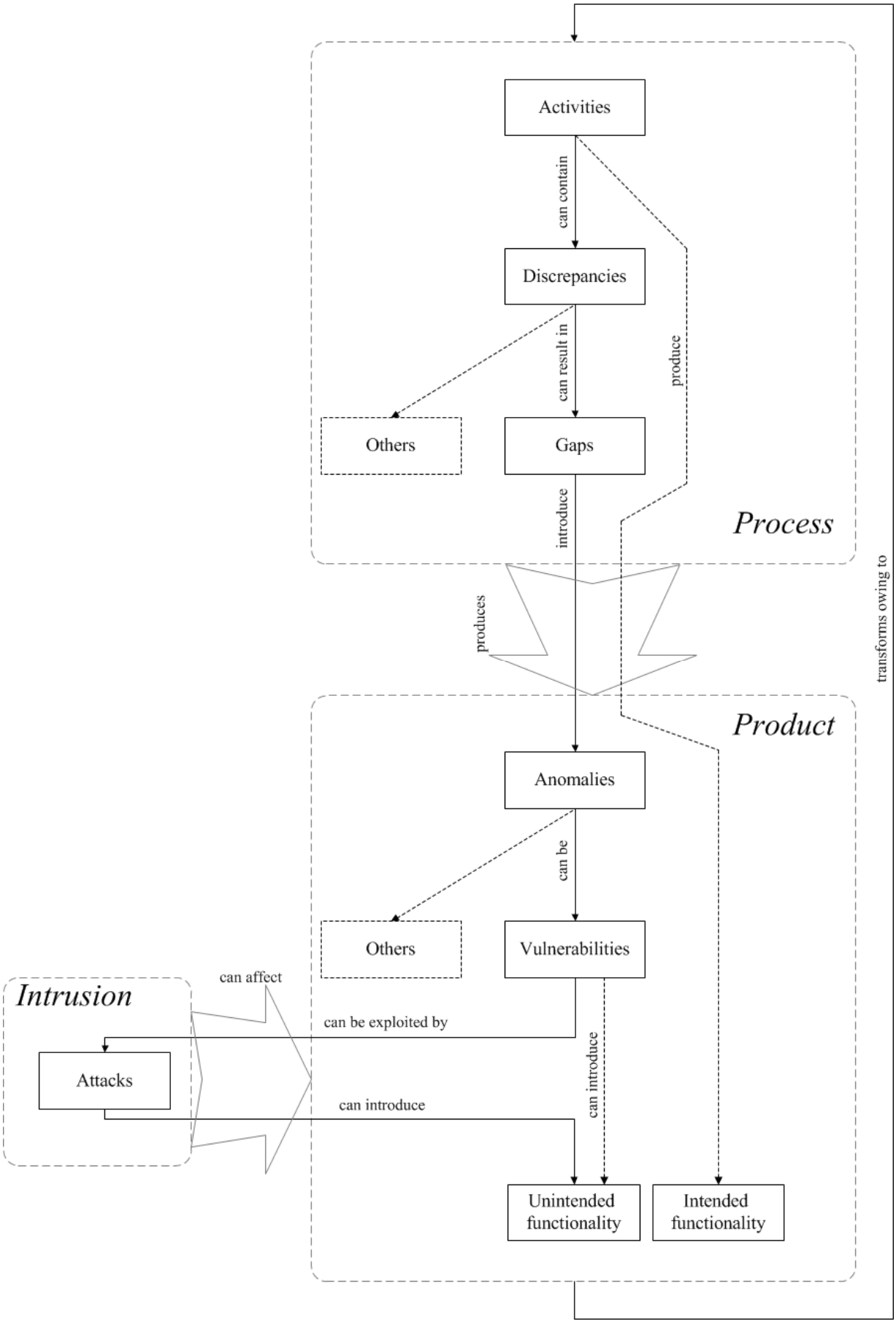

Figure 1. A taxonomy of used notions

Hence, we propose a process-based approach to GA, because “non-ideal” processes, which contain discrepancies, can produce various problems in the corresponding products, and the following statements are true:

1. Presence of gaps in $Process_j$ results in anomalies in $Product_i$ even if $Product_{i-1}$ is “ideal”.

2. Presence of anomalies within $Product_{i-1}$ can be eliminated by “ideal” $Process_j$ in many cases. This may be true in case of verification and validation processes, however, it does not apply to design processes. For example, anomaly in the technical specification is not eliminated by an “ideal” direct translation process (since it may not include verification).

As an illustrative example for the proposed definition of gap, let us consider a development process within the I&C system life cycle model, where the input of $Process_j$ is represented by $Product_{i-1}$, and the output (result of process implementation) – is $Product_i$. The transition from the previous product (i-1) to next one (i) is accomplished by the implementation of a prescribed process (j) by developers, using certain tools. This process can be represented as a set of sub-processes that are implemented in serial and/or parallel ways, and each of such sub-processes may contain problems (or discrepancies towards appropriate “ideal” sub-process) due to various reasons caused by either the developer or the tool. Therefore, the problems in sub-processes lead to problems in processes, which are implemented in order to produce a new product and can result in product anomalies.

The activities, required to implement the approach, comprise several consequent steps intended for a comprehensive analysis and assessment of I&C systems.

The key idea of assessment is in the application of the process-product approach. Therefore, the life cycle model of I&C systems should include detailed representation of life cycle processes and appropriate products. Then, it is possible to identify problems (or discrepancies) within the model, i.e. gaps. In general, such gaps may reflect various aspects of the I&C system, depending on what system properties are assessed (for example, safety and security).

Hence, depending on the I&C system aspects under assessment, each gap should be represented in a form of a formal description; such formal description should be made for a set of discrepancies identified within the gap. The IMECA technique is the most convenient, in our opinion, to perform such description: each identified gap can 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. In this way, complete traceability of life cycle processes, appropriate products and inherent properties of corresponding discrepancies can be achieved. As a result, the number of local IMECA tables would correspond to the number of identified gaps, and the number of rows within each local IMECA table would correspond to the number of identified discrepancies within the appropriate gap.

After completing the appropriate columns, for example on the basis of expert assessment, for all local IMECA tables, each gap being represented by a set of discrepancies with appropriate numerical values. Data within each row of local IMECA tables reveal, in explicit form, the weaknesses of the I&C system aspect under assessment: for example, in terms of safety – system faults and failures, in terms of security – intrusion probability and severity.

Further, in order to implement the approach, the following cases are possible, depending on the scope of the assessment:

1. Assessment of the I&C system as a whole. Then, a set of particular IMECA tables (which represent all the identified gaps by a set of discrepancies) should be integrated into the single global IMECA table that reflects the whole system. In this case, each row of the global IMECA table forms the basis for creating a global criticality matrix.

2. Assessment of particular (sub-)systems within the I&C system. In this case, it is possible to create an appropriate set of local criticality matrixes that correspond to certain (sub-)systems, based on a set of local IMECA tables.

Integration of local criticality matrixes into a global one is carried out in accordance with the following rule:

$$e_{yz}^{G} = \bigcup_{k=1}^{n} e_{yz}^{L_k} , \qquad (1)$$

where e^{G} is an element of the global criticality matrix, e^{L_k} is the corresponding element of the k-th local criticality matrix, and n is the total number of local criticality matrixes (equal to total number of gaps).

Moreover, the scales for the numerical values of a discrepancy (for example, its probability and severity) for local criticality matrixes can be set to the same value in order to eliminate the necessity of additional analysis during the creation of a global criticality matrix.

In both cases, the highest risk of the selected assessment aspect corresponds to the highest row in the criticality matrix. In a case of independent gaps and discrepancies, the total risk of R can be calculated using the following equation:

$$R = \sum_{i=1}^{n} \sum_{j=1}^{m} p_{ij} D_{ij} , \quad (2)$$

where n is the total number of gaps, m is the total number of rows in the IMECA table, p is the occurrence probability, and D is the corresponding damage.

Moreover, the criticality matrix can be extended to be K-dimensional (where K>2) that allows us to consider, for example, the amount of time required to implement the appropriate countermeasures for the assessed I&C system.

For example, during the assessment of security, the prioritization of vulnerabilities identified on the basis of process-product approach, should be performed according to their criticality and severity, representing their corresponding stages in the cyber security assurance of the given I&C system. The main goal of this step is to identify the most critical security problems within the given set. Prioritization may require the creation of a criticality matrix, where each vulnerability is represented within single rows. In such cases, it is possible to manage the security risks of the whole I&C system via changing the positions of the appropriate rows within the matrix (the smallest row number in the matrix corresponds to the smallest risk of occurrence).

During the performance of GA, the identification of discrepancies (and the corresponding vulnerabilities in case of security assessment), can be implemented via separate detection/analysis of problems caused by human factors, techniques and tools, taking into account the influence of the development environment.

Then, after all identified vulnerabilities are prioritized, it is possible to assure security of the I&C system by implementing of appropriate countermeasures. Such countermeasures should be selected on the basis of their effectiveness (also, in context of assured coverage), technical feasibility, and cost-effectiveness. But there is an inevitable trade-off between a set of identified vulnerabilities and a minimal number of appropriate countermeasures, which allows us to eliminate vulnerabilities or to make them difficult to be exploited by an adversary. The problem of choosing such appropriate countermeasures is an optimization problem and is still challenging.

Example of proposed approach application

As an illustrative example for the proposed approach, consider a typical development process for a VHDL code, implemented by a developer (see Fig. 2).

The input to the process is represented by a technical specification document (containing the comprehensive description of the object being developed), and the result is the VHDL code (development object). In such a case the possible discrepancies can be caused by design faults, developer's errors, and/or errors in appropriate procedures intended for the developer. Moreover, during the subsequent stages of the overall development process, existing problems in the product can be either eliminated or multiplied. Then, it is possible to represent the identified set of the process' discrepancies (or single gap) in a form of IMECA-based table, where each row corresponds to a discrepancy within the process.

Such a complex gap can be eliminated, for example, via the implementation of another development process (see Fig. 3), which includes three entities: technical specifications, an Event-B tool model (a form of technical specification representation in terms of a tool that is understandable to developer and can automatically be translated into a VHDL code), and the VHDL code itself.

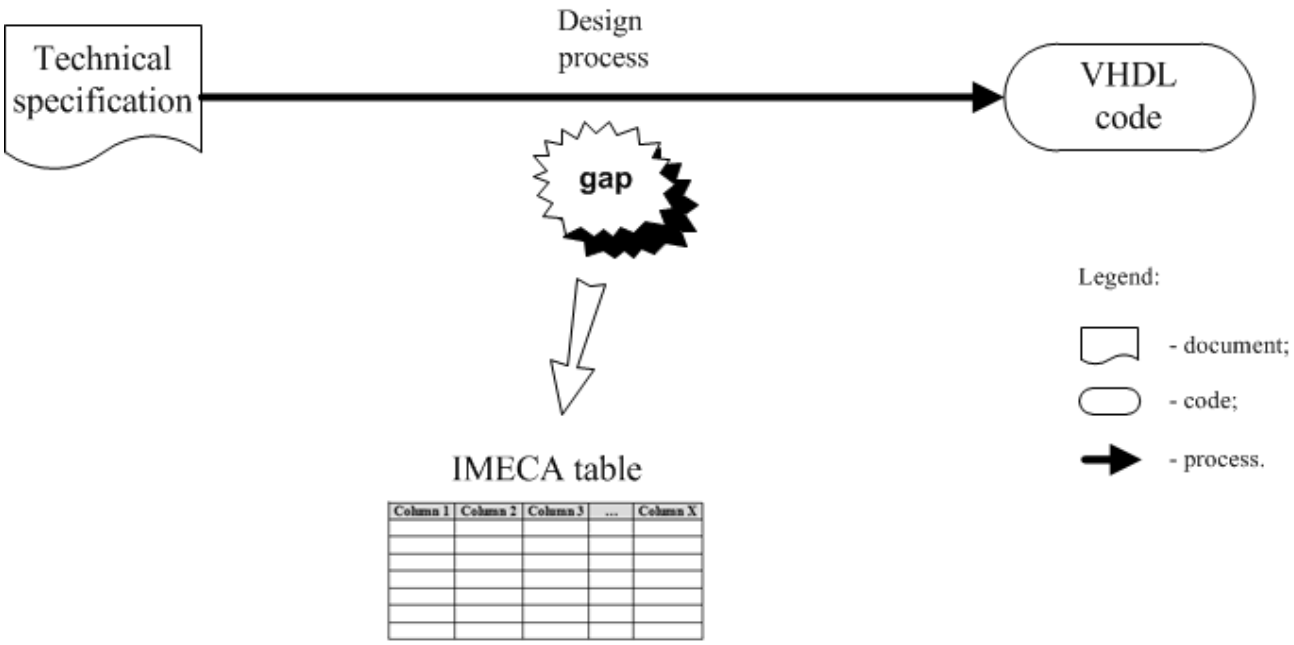

Figure 2. A typical development process for a VHDL code

Transitions from previous entities to the next are accomplished by the execution of certain processes, namely: formal notations development process (implemented by the developer, and consisting of translation of technical specifications into a model, in terms of internal instructions of the Event-B tool,

allowing the developer to mathematically prove the correctness of the resulting notation) and the translation process (implemented by special add-ons of the Event-B tool, and consisting of generating the final VHDL code on the basis of the derived model).

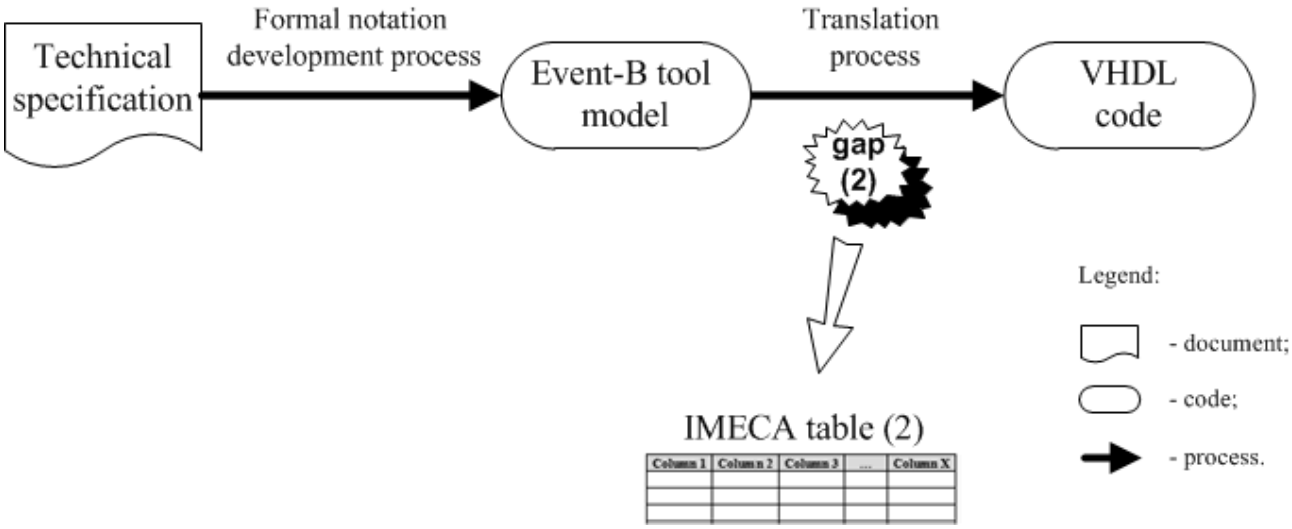

Figure 3. Development processes for VHDL code

Discrepancies in such processes can be caused by the applied tools only, since the formal notations development process is followed by the model in Event-B tool that is mathematically verifiable. Discrepancies of the translation process (or discrepancies of its sub-processes) can be caused by the Event-B tool, for example, in a case, when such tool is not fully tested or certified.

In this way, it is possible to state that we can identify the only existing gap. Moreover, such a gap can be eliminated if certified tools are applied. Thus, in the case given in Equation (2), the risk factor R is reduced due to the reductions in the values of parameters n (from 2 to 1), m, and p_{ij}.

Life cycle model of FPGA-based I&C system

Basis of modern critical I&C systems is usually formed by FPGA chips, which are used in various hardware components. Vulnerabilities of FPGA technology can unintentionally arise or can be introduced by an adversary during different stages of FPGA chip life cycle. A model of FPGA-based I&C system life cycle is depicted in Fig. 4, and includes:

1) stages implemented by FPGA chip vendor:

– a stage of FPGA chip design (Stage 1);

– a stage of FPGA chip manufacturing (Stage 2)

– a stage of FPGA chip packaging and testing (Stage 3);

2) stages implemented by I&C system developer:

– a stage of FPGA electronic design (which describes I&C system's logic) development for integration into FPGA chip (Stage 4);

– a stage of FPGA electronic design implementation and testing (Stage 5);

3) a stage implemented by user of I&C system:

– a stage of operation of FPGA-based I&C system at intended location (Stage 6).

There are factors that can contribute to intended or unintended introduction of vulnerabilities into FPGA-based I&C system during implementation of various processes for the following life cycle stages:

– use of malicious tools (EDA tools or CAD tools) during either FPGA chip designing by a vendor or during FPGA electronic design development by an I&C system developer;

– use of compromised devices during integration of developed FPGA electronic design into FPGA chip by an I&C system developer;

– use of IP-cores from third-party vendors during development of FPGA electronic design by an I&C system developer;

– the presence of adversaries (insiders) in development teams.

Some vendors of FPGA chips do not have own manufacturing capacity: in such a case, after implementation of design processes for FPGA chip, that includes application of appropriate tools, they place orders for chip manufacturing among appropriate foundries. Such foundries can introduce additional vulnerabilities into FPGA chips by stealing or modifying FPGA design. Moreover, supply chain of manufactured FPGA chips to developer of I&C system is usually traceable and can be audited that, however, does not reduce its importance from point of view of cyber security assurance problem for FPGA-based I&C systems.

Most of life cycle stages of FPGA chip and FPGA-based I&C system are implemented using software tools. Such tools are usually used, for example, during design of printed circuit boards for FPGA chips, in development of FPGA electronic designs, during simulations, etc. Hence, developers of tools for design automation, in turn, can introduce new vulnerabilities into FPGA-based I&C systems being developed.

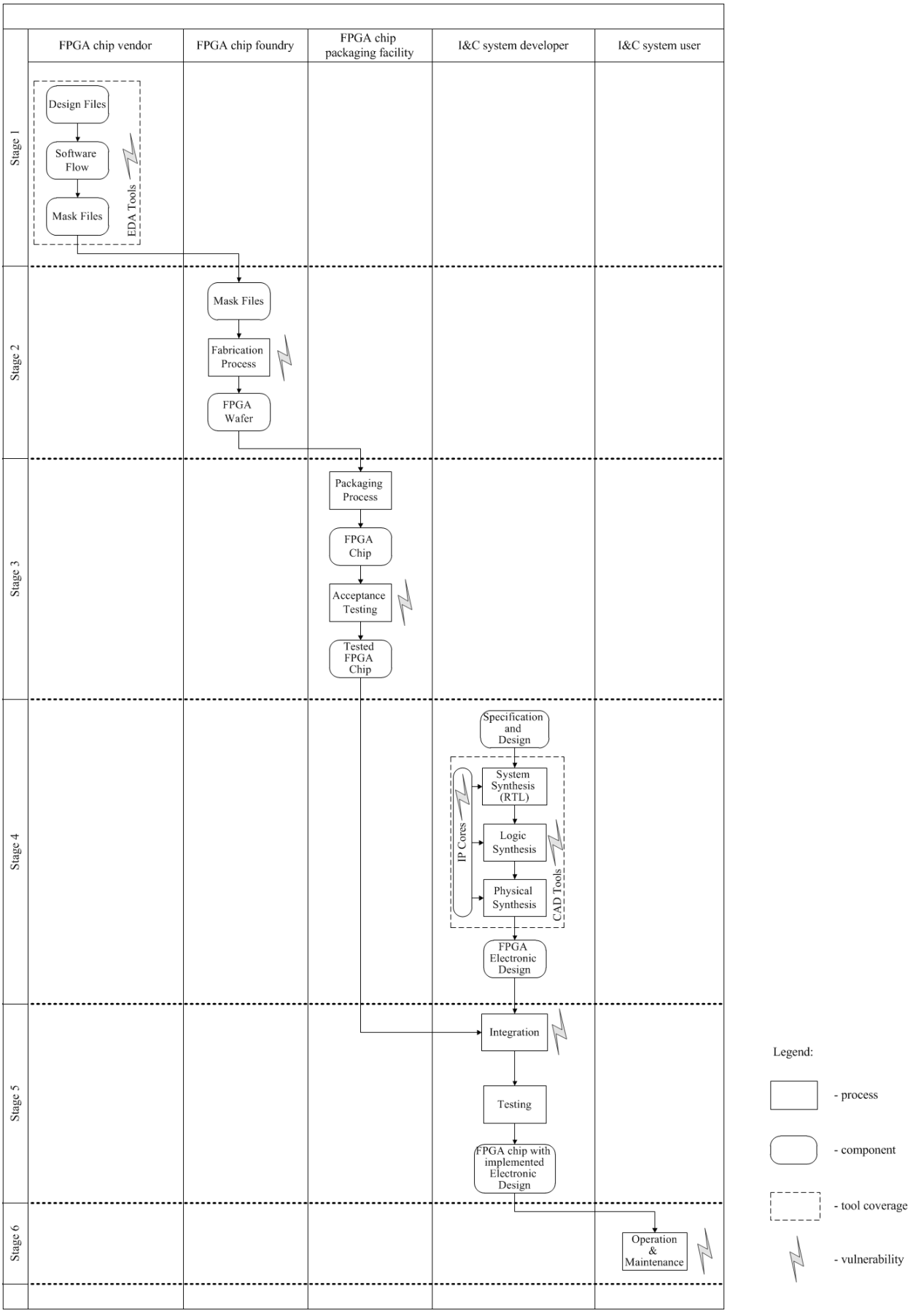

Figure 4. Life cycle model of FPGA-based I&C system

Some vulnerabilities can be introduced into FPGA-based I&C systems by their designers via using of IP-cores in FPGA electronic design. IP-core is completed functional description intended for integration into FPGA electronic design, which is being developed. IP-cores can be either in a form of modules for hardware description languages or in a form of compiled netlists. IP-cores are used by designers to save their resources and time. IP-cores can be produced by FPGA chip vendor or third-party vendors, and, in order to assure cyber security of FPGA-based I&C system, it is necessary to facilitate safe distribution and integration of such IP-cores by designers of I&C systems.

Gap-and-IMECA-based assessment of FPGA-based I&C system

So, proposed gap-and-IMECA-based approach, as applied to cyber security assessment, can be expressed in the following activities sequence:

Step 1. Identification of security gaps lists for all the components (or modules) of I&C system, being assessed, during each life cycle stage. Such lists should include both process gaps (in terms of discrepancies) and product cyber security gaps (in terms of vulnerabilities).

Step 2. Determination of an appropriate set of vulnerabilities for each identified process gap, security gap and possible scenarios to exploit the vulnerabilities. So, for each identified discrepancy or vulnerability, there should be created local IMECA table that reflects: attack mode, attack nature, attack cause, occurrence probability, effect severity, type of effects, and countermeasures.

Step 3. Performance of GA on the basis of IMECA-technique: each gap (identified during Step 1) being represented by one or several rows in a local IMECA table, where the number of such rows corresponds to the number of appropriate discrepancies or vulnerabilities identified during Step 2. GA should be performed in order to reveal appropriate cyber security risks.

Step 4. Assessment of appropriate columns (occurrence probability and effect severity) in each particular IMECA table, for example, on the basis of expert evaluation. Then, each row of such a local IMECA table represents security weaknesses, which should be analyzed further (during Step 6) in context of the whole I&C system.

Step 5. Analysis of cyber security risks of I&C system components during different stages: each row in local IMECA tables forms the basis for creation of security criticality matrix, which reveals the weaknesses of appropriate components

in a visual form. The highest cyber security risk corresponds to the highest row in security criticality matrix.

In order to illustrate IMECA-based assessment, we present results for attacks modes possible during operation and maintenance stage of FPGA-based I&C system (see Table 1).

Conclusion

A problem of I&C systems assessment is still challenging due to the fact that such systems consist of interconnected complex components with different functions and different nature. The majority of modern I&C systems, including safety-critical I&C systems, are being FPGA-based, hence, it is impossible to perform their assessment without consideration of all the special features for all the technologies used. In this chapter we discussed some problems related to assessment of various aspects of I&C systems, including FPGA-based systems.

To assure cyber security of modern complex I&C systems, as well as to decrease a probability of vulnerabilities exploitation and appearance of security breaches, a cyber security assessment approach is proposed. This approach implies identification of all possible discrepancies, on the basis of product and life cycle processes, and their assessment via application of IMECA technique.

The proposed approach is based on both gap conception and IMECA technique. Such an approach is applicable in assessment of various aspects of I&C systems, since it considers process-product model to reveal all the process discrepancies that can potentially result in product anomalies.

Application of the proposed approach and technique was illustrated by an example of cyber security assessment for some FPGA-based I&C system. Gap-and-IMECA-based technique was applied in development of a company standard in Research and Production Corporation Radiy that is harmonized with international standards. This standard is used during implementation of development and verification activities for safety-critical I&C systems for nuclear power plants [2].

Next steps of research and development activities may be connected with creation and implementation of tool-based support for the proposed approach, taking into account results of qualitative and quantitative assessment.

Table 1. Results of IMECA for FPGA attacks

Row number	Attack mode	Attack cause	Occurrence probability	Effect severity	Type of effects	Countermeasures
1	Black Box Attack	Simple logic of electronic design	Very low	Very low	Reverse engineering of logic by adversary	Complication of electronic design logic
2	Readback Attack	Absence of chip security bit and/or availability of physical access to chip interface	Moderate	High	Obtaining of secret information by adversary	The use of security bit. Application of physical security controls
3	Cloning Attack	Storing of decoded configuration	Moderate	High	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)
4	Physical Attack	Absence of monitoring of parameters (voltage, temperature, clock) of environment and chip	Low	Moderate	Obtaining of information concerning patented algorithms by adversary	Decreasing memory retention effect. Monitoring of parameters (voltage, temperature, clock) of environment and chip
5	Side-Channel Attack	Correlation of measurable parameters with its function	High	High	Leak of undesirable informatio	Addition of random noise in measurable parameters (or masking of information by

					n	random values). Decrease of difference in power consumption. Changing of electronic design logic

References

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

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

4. Kharchenko V (Edit) (2011) Critical Infrastructures Safety: Mathematical and Engineering Methods of Analysis and Assurance, Department of Education and Science of Ukraine, National aerospace university named after N. Zhukovsky "KhAI", 2011, 641 p

10. Gorbenko A, Kharchenko V, Tarasyuk O, Furmanov A (2006) F(I)MEA-technique of Web Services Analysis and Dependability Ensuring, Lecture Notes in Computer Science, vol. 4157/2006, pp. 153-167

12. Babeshko E, Kharchenko V, Gorbenko A (2008) Applying F(I)MEA-technique for SCADA-based Industrial Control Systems Dependability Assessment and Ensuring, Dep-CoS-RELCOMEX 2008, pp. 309-315. doi:10.1109/DepCoS-RELCOMEX.2008.23