UDC 681.324

**V.S. KHARCHENKO[1,2], A.A. KOVALENKO[2,3], A.A. SIORA[4]**

*[1] National Aerospace University "KhAI", Kharkov, Ukraine*
*[2] Centre for Safety Infrastructure-Oriented Research and Analysis, Kharkov, Ukraine*
*[3] Kharkov National University of Radio Electronics, Kharkov, Ukraine*
*[4] RSC «Radiy», Kirovograd*

# GAP- AND HTT-BASED ANALYSIS OF SAFETY-CRITICAL SYSTEMS

*The paper discusses importance of assessment of interference degree for various attributes of safety-critical systems, as well as proposes applicable metrics. Also, the paper presents an approach to analysis of safety-critical systems. Such approach relies on performance of gap analysis and consideration of influence of human, technique and tool. The approach is applicable to various safety-critical systems, including complex instrumentation and control systems and FPGA-based systems.*

***Keywords**: safety-critical system, instrumentation and control, analysis, assessment, attribute, development life cycle.*

## Introduction

Nowadays safety-critical systems (SCSs) are widely used by the world industry in various areas in forms of Instrumentation and Control (I&C) systems for Nuclear Power Plants (NPPs), on-board computer-based systems, electronic medical systems, etc. Moreover, Field Programmable Gate Arrays (FPGA) technology is now being trend in SCSs implementation that inevitably leads to new challenges in various aspects of such systems design, operation and maintenance requiring new approaches, techniques and appropriate requirements [1]. The objective of this paper is to customize the elements of gap analysis (GA), Intrusion Modes and Effects Criticality Analysis (IMECA) technique and analysis of development processes related to the developer (human), technique, and tool (HTT) to develop an approach, which can be used in analysis and assessment of SCSs [2].

## 1. Taxonomies of SCS's attributes

### 1.1. Possible attributes and taxonomies of SCSs

One of the most important attributes of SCS is dependability. Dependability of a system is the ability to deliver required services (or perform functions) that can justifiably be trusted. Dependability is a complex attribute of a SCS that can be represented by a set of primary attributes, including:

– reliability: continuity of correct (required) services;

– availability: readiness for correct services;

– survivability: ability to minimize loss of quality and to keep capacity of fulfilled functions under failures caused by internal and external reasons;

– safety: absence of catastrophic consequences for the user(s) and the environment;

– integrity: absence of improper system alternations;

– confidentiality: absence of unauthorized disclosure of information;

– high confidence: ability of correct estimation of services quality, i.e. definition of trust level to the service;

– maintainability: ability to undergo modifications and repairs;

– security: the protection from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

In turn, safety attribute of SCS can have some particular (or secondary) attributes depending on exact system, environment and conditions that have influence on the primary attribute. Here, we distinguished the following attributes (see Fig. 1): reliability, security and trustworthiness, and we denoted their two-way influence.

We should note that such particular attributes may be defined for each of primary attributes, thus, representing hierarchical structure of SCS's generic attributes set. Moreover, those secondary and further attributes may turn to be common for different primary attributes due to their incomplete "orthogonality".

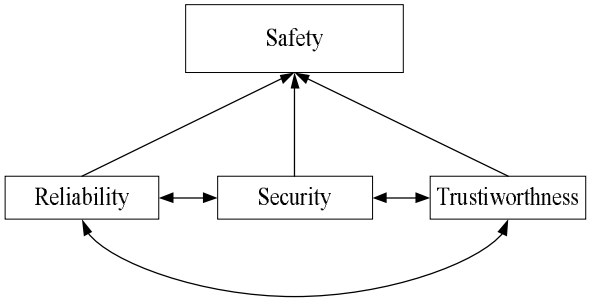


Fig. 1. Taxonomy of safety attribute

### 1.2. Metrics of Interference

Thus, we can state that a set of SCS attributes can be represented in a form of *i*-level hierarchical model, and each of *i* levels contains $k_i$ attributes. As an example, Fig. 2 represents an element of last two levels of an SCS attributes hierarchical model consisting of *i* levels.

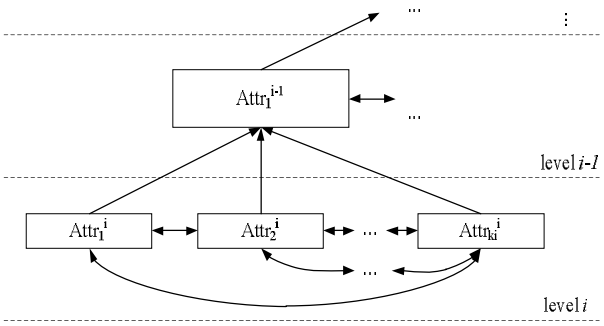


Fig. 2. Levels of SCS attributes hierarchy

One of the possible ways to reveal criticality of two-way influence for SCS's attributes, is in creating of attributes influence matrix. Such a problem can be solved, in particular, in the following ways:

1. Create a set of *n* "local" influence matrixes for *i* hierarchical levels; each of the matrixes consists of $k_i$ attributes (see Fig. 3), and, therefore of $k_i$ rows. Such number *n* can be calculated using the following equation:

$$n = \sum_{x=1}^{i-1} k_x . \qquad (1)$$

The number of rows in each matrix associated with the level *m*, where *m*=[*1,i-1*], is equal to a number of attributes ($k_m$) at the lower level *m+1*: for example, the local matrix for a single attribute of *i-1* level consists of $k_i$ rows.

A set of such "local" influence matrixes represents the case of a metric mostly intended for independent assessment of the SCS's attributes within the single level.

2. Create the single "global" influence matrix where each of all the *n* attributes (see Eq. (1)) is reflected by a single row and appropriate column (see Fig. 4).

"Global" influence matrix can be considered as another metric, which is suitable for assessment of the SCS as a whole.

Thus, on the one hand, such metrics allow sharing SCS resources in order to assure the required level of security (a vertical related to different levels in Fig. 2), on another hand, they allow optimizing the use of the resources (within the same level, see Fig. 2).

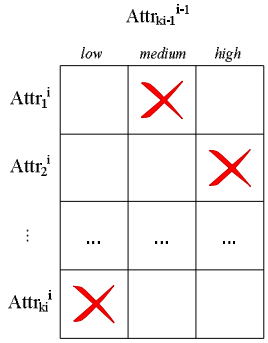


Fig. 3. Local influence matrix

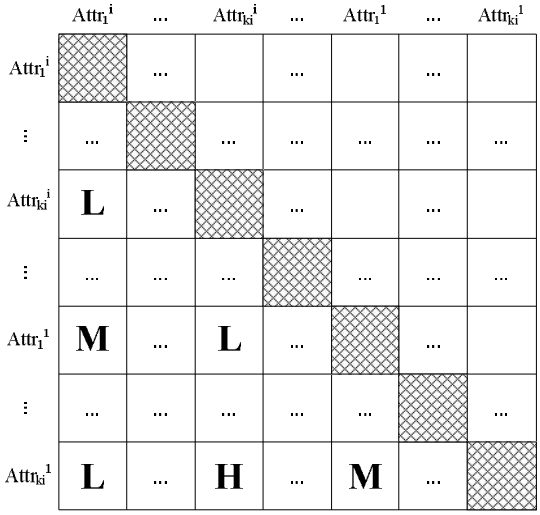


Fig. 4. Global influence matrix

## 2. Extension of DLC-based Analysis for SCSs

Development process of modern SCSs requires strong formalized processes for both design and verification and validation (V&V) activities. Thus, development life cycle (DLC) of a SCS can be represented in a form of V-model. To illustrate an example of such model, we present software systematic capability and the DLC (the V-model) in Fig. 5 [3].

In terms of the whole system, such V-model implies development of certain artifacts (or components) after completing specific design activities. Each artifact is under strong verification activities in order to prevent unauthorized design and/or functionality of the system.

FPGA technology is now being widely used by the world industry and more often in SCSs for various areas [4, 5]. Application of FPGA technology allows developers to implement intended functions in a convenient and reliable way.

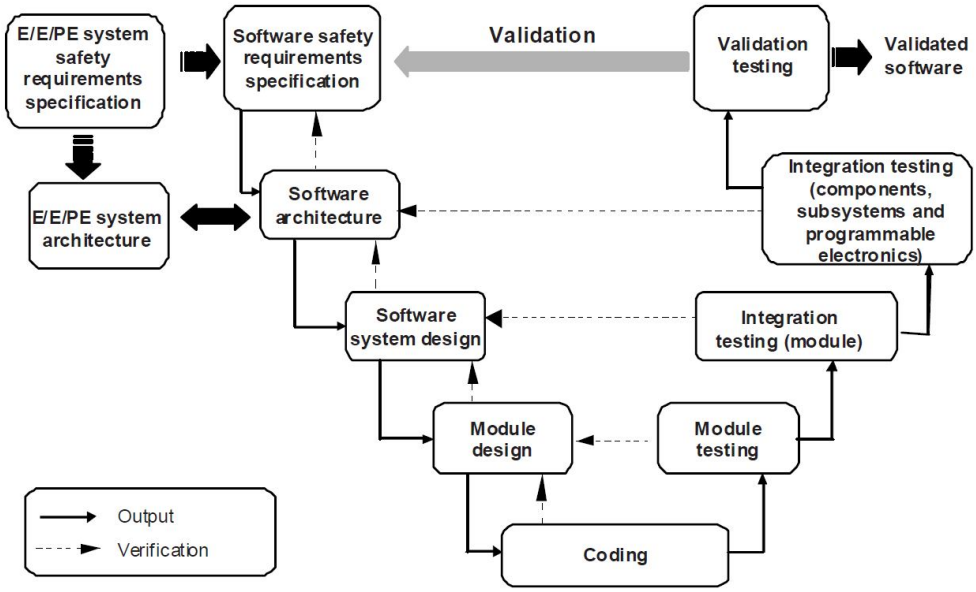


Fig. 5. Software systematic capability and the DLC (the V-model)

Modern trend is in that SCSs are being complex, containing plenty of components, and often based on FPGA technology. In order to consider all the features of such complexity and used technologies, the analysis of SCS attributes should be performed. In such a case, overall DLC of a SCS can be represented in a form of a set of particularly overlapped "sub-V-models" corresponding to each of SCS components' DLCs.

Each of "sub-V-models" covers component-specific development stages and contains appropriate return points.

In a general case, both start point and length of a component's DLC are different from SCS's overall DLC due to various reasons. Hence, it is possible to separate all "sub-V-models" of components DLCs to perform comprehensive assessment of required attribute related with the component. Such complete set of all "sub-V-models" for each of the SCS components DLCs forms a plane, or component-oriented V-model of SCS's DLC (see Fig. 6).

Further, it is possible to associate DLC of exact attribute with each of the SCS's components within the component-oriented V-model. A set of components' attributes, again, forms another one plane – attributes plane. Hence, we already have two planes: for components and attributes, and, in a bundle with the DLC, it is possible to address the aspect under interest in three-dimension space defined by the three coordinates, which are related with the SCS component, SCS attribute, and DLC stage (see Fig. 7).

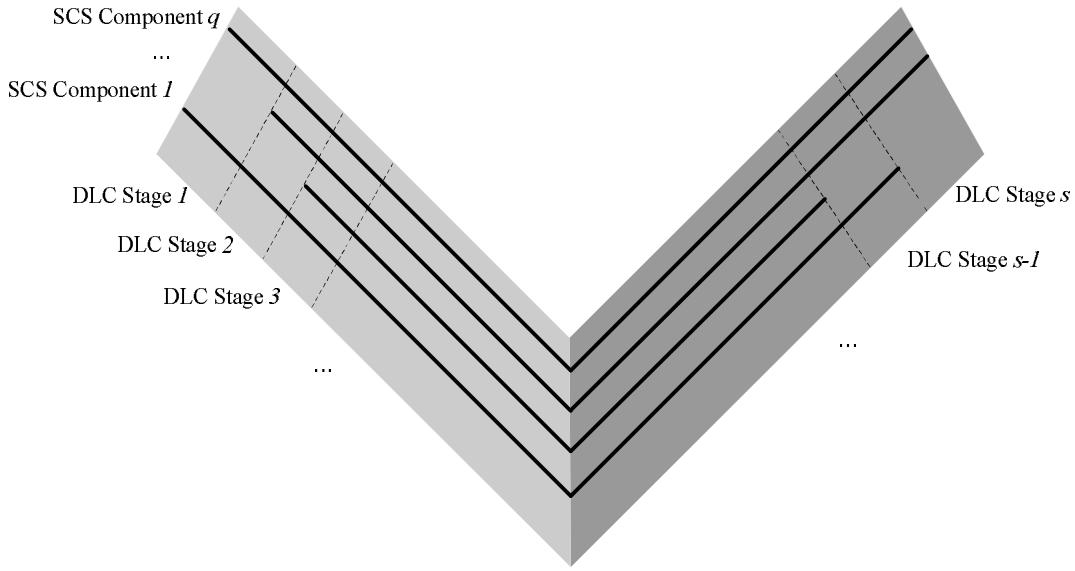


Fig. 6. Component-oriented V-model of SCS's DLC

Thus, now we can talk about attribute-oriented extension to component-oriented V-model of SCS's DLC (see Fig. 8).

Such approach allows us to independently assess each of SCS components and attributes of the component during the component-specific DLC stage.

The proposed extension allows separation of specific DLC stages for each of components' attributes (for example, safety, security, etc.) to reveal discrepancies of appropriate development processes that can potentially result in anomalies (for example, faults for safety or vulnerabilities for security) of the final product (i.e. SCS or its component).

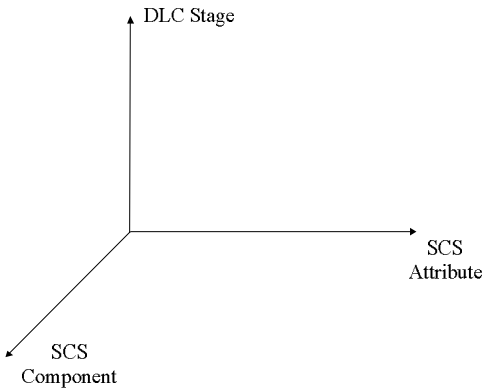


Fig. 7. Three-dimension space

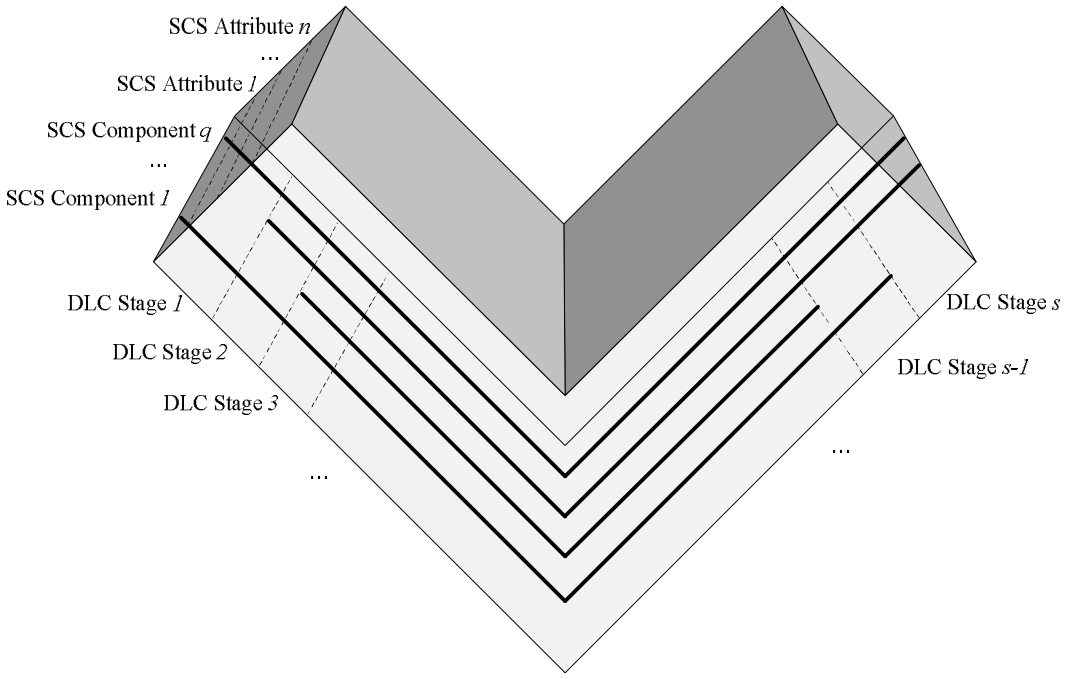


Fig. 8. Attribute-oriented V-model of SCS's DLC

## 3. General conception of gap-and-IMECA-based approach to analysis of SCSs

In this section, as one of the possible solutions for SCS analysis problem, an approach, which is based on IMECA technique [6], is proposed.

One of the fundamental concepts behind the underlying idea of the approach is the concept of gap. Here we can define gap as a set of discrepancies of any single process (which, in a general case, consists of a set of sub-processes) within the SCS's DLC 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 (or even representation), implementation, verification, and/or other non-compliances.

For example, 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.

In this way, 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 $Product_p$ even if $Product_{p-1}$ is "ideal".

2. Presence of anomalies within $Product_{p-1}$ 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 SCS's DLC model, where the input of $Process_j$ is represented by $Product_{p-1}$, and the output (result of process implementation) – is $Product_p$ (see Fig. 9). Such a situation represents, for example, results of implementation of *i-1* and *i* stages of SCS's DLC, respectively.

The transition from the previous product (*p-1*) to next one (*p*) is accomplished by the implementation of a prescribed process (*j*) by developers, using certain tools in compliance with certain prescribed techniques. Thus, this process can be represented as a set of sub-processes, which are related to the developer (human), technique, and tool, respectively. Such sub-processes are being implemented in serial and/or parallel ways, and each of them may contain problems (or discrepancies towards appropriate "ideal" sub-process) due to various reasons caused by the developer, the used technique 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.

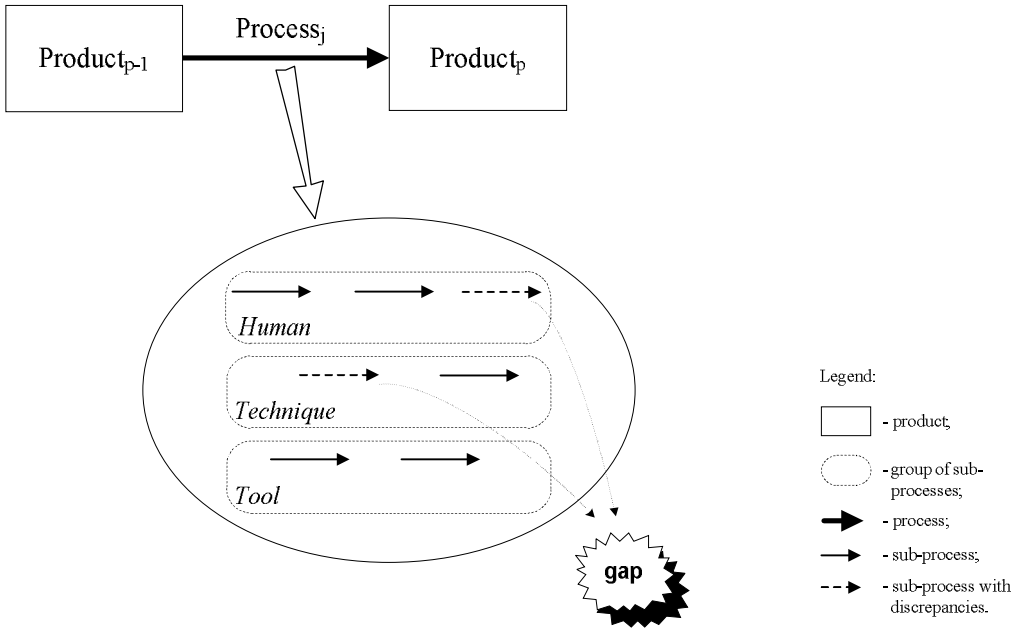


Fig. 9. Development process in the SCS DLC model

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

The key idea of assessment is in the application of the process-product approach. Therefore, the DLC model of SCS should include detailed representation of DLC 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 SCS, depending on what system attributes are assessed (for example, safety and security).

Hence, depending on the SCS 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 SCS 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 SCS as a whole. Then, a set of particular IMECA tables (which represent all the identified gaps by a set of discrepancies) should be inte-

grated 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 SCS. 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:

$$e_{yz}^{G} = \bigcup_{r=1}^{g} e_{yz}^{L_r} , \qquad (2)$$

where $e^G$ is an element of the global criticality matrix, $e^{L_r}$ is the corresponding element of the *r*-th local criticality matrix, and *g* 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 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:

$$R = \sum_{t=1}^{g} \sum_{w=1}^{m} p_{tw} D_{tw} , \qquad (3)$$

where *g* 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 SCS.

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 SCS. 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 of the vulnerabilities is represented within single rows. In such cases, it is possible to manage the security risks of the whole SCS 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 SCS 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.

## Conclusion

A problem of SCS analysis and 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 SCSs are being FPGA-based; hence, it is impossible to perform their assessment without consideration of all specific details, including interference of various SCS's attributes and the special features for all the technologies used. In this paper we discussed some problems related to assessment of various aspects of SCSs.

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

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 [5].

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.

## Aknowledgment

The presented paper has been conducted by V. Kharchenko within framework of the project "Integrating the National Aerospace University into ERA" (294311 KhAI-ERA, FP7-INCO-2011-16).

## References

*1. Ranta, J. The current state of FPGA technology in the nuclear domain [Text]/ J. Ranta. – VTT Technical Research Centre of Finland, 2012. – 62 p.*

*2. Gap-and-IMECA-based Assessment of I&C Systems Cyber Security [Text]/ V. Kharchenko, A. Andrashov, V. Sklyar, A. Kovalenko, O. Siora // Accepted to Proc. of DepCoS-RELCOMEX 2012. – P. 123 -128.*

*3. IEC 61508:2010. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems. – 2010.*

*4. NUREG/CR-7006. Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems. – U.S. Nuclear Regulatory Commission, 2010.*

*5. Kharchenko, V.S. (Edits). FPGA-based NPP Instrumentation and Control Systems: Development and Safety Assessment [Text]/ V.S. Kharchenko, V.V. Sklyar. – 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.*

*6. Babeshko, E. Applying F(I)MEA-technique for SCADA-based Industrial Control Systems Dependability Assessment and Ensuring / E. Babeshko, V. Kharchenko, A. Gorbenko // DepCoS-RELCOMEX. – 2008. – P. 309-315.*

*Поступила в редакцию 16.02.2012*

**Рецензент**: д-р техн. наук, проф. О.Г. Руденко, Харківський національний університет радіоелектроніки, Харків, Україна.

### GAP- ТА HTT- АНАЛІЗ КРИТИЧНИХ СИСТЕМ

***В.С. Харченко, А.А. Коваленко, О.А. Сіора***

В статті розглянуто важливість оцінки ступеня впливу різних атрибутів систем, критичних з точки зору безпеки, а також запропоновано відповідні метрики. Крім того, в статті запропоновано підхід до аналізу систем, критичних з точки зору безпеки. Такий підхід оснований на проведенні GAP-аналізу та урахуванні впливу людини, використовуваних методик та інструментальних засобів. Запропонований підхід можливо застосовувати для різноманітних систем, критичних з точки зору безпеки, включаючи також комплексні інформаційно-управляючі системі, а також системи, що базуються на ПЛІС.

**Ключові слова**: критична система, інформаційно-управляюча система, аналіз, оцінка, атрибут, життєвий цикл розробки.

### GAP- И HTT- АНАЛИЗ КРИТИЧЕСКИХ СИСТЕМ

***В.С. Харченко, А.А. Коваленко, А.А. Сиора***

В статье рассмотрена важность оценки степени влияния различных атрибутов систем, критических с точки зрения безопасности, а также предложены применимые метрики. Кроме того, в статье предложен подход к анализу систем, критических с точки зрения безопасности. Такой подход основывается на проведении GAP-анализа и учете влияния человека, используемых методик и инструментальных средств. Предложенный подход применим к различным системам, критическим с точки зрения безопасности, включая также комплексные информационно-управляющие системы, а также системы, основанные на ПЛИС.

**Ключевые слова:** критическая система, информационно-управляющая система, анализ, оценка, атрибут, жизненный цикл разработки.

**Харченко Вячеслав Сергеевич** – д-р техн. наук, проф., зав. каф. компьютерных систем и сетей Национального аэрокосмического университета им. Н.Е. Жуковского «ХАИ», Харьков, Украина, e-mail: V.Kharchenko@khai.edu

**Коваленко Андрей Анатольевич** – канд. техн. наук, доц., доц. каф. электронных вычислительных машин Харьковского национального университета радиоэлектроники, Харьков, Украина, e-mail: andriy_kovalenko@yahoo.com

**Сиора Александр Андреевич** – канд. техн. наук, председатель правления Научно-производственного предприятия «Радий» Кировоград, Украина, e-mail: marketing@radiy.kr.ua.