UDC 004.6 **doi: 10.20998/2522-9052.2018.1.12**

O. Illiashenko [1], V. Kharchenko [1,2], A. Kor [3]

[1] National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine
[2] Research and Production Company Radiy, Kropyvnytskyi, Ukraine
[4] Leeds Beckett University, LS1 3HE, Leeds, United Kingdom

GAP-ANALYSIS OF ASSURANCE CASE-BASED CYBERSECURITY ASSESSMENT: TECHNIQUE AND CASE STUDY

The **subject matter** of the article is the processes of cybersecurity assessment. The **goal** is to develop technique for gap-analysis of cybersecurity analysis process. The **task** to be solved is to develop a method for analyzing gaps in the process of assessment of non-functional requirements for safety and cybersecurity of ICS. It is based on the classification of requirements, taking into account the possibility of their decomposition, which includes the construction of an advanced security assurance and determination of counter-measures to address detected gaps. **Conclusions**. The scientific novelty of the results obtained is as follows: the method for ensuring the information security of digital components of the I&Cs was further developed by analyzing the discrepancies of requirements using vulnerability description procedures and assessing the severity of the intrusions consequences, as well as determining the set of countermeasures by the "security-cost" criterion, which makes it possible to reduce risks to an acceptable level.

Keywords: ASAC – Advanced Security Assurance Case; gap-analysis; cybersecurity; assessment; requirement; conformance.

Introduction

MOTIVATION. With the continuous emergence of new technologies and the improvement of the old ones, new challenges arise for trusting the devices used, especially if these devices perform security functions or access to confidential data. The problems of safety, security and particularly cybersecurity assessment and assurance of such systems became even more crucial when the peculiarities of technologies used during the process of development of the final product should be addressed.

Modern companies are paying the most attention to the issues of ensuring the cyber security of their IT systems during last years. However, in fact, it turns out that even compliance with all requirements to cybersecurity could not ensure the absolute protection of digital assets. The Cisco 2017 Annual cybersecurity report [1] (which is based on the research done in 13 countries with more than 2900 participants from 130 companies in different branches of economy) contains information that among the processed alerts about threats, only every second one (28%) is justified. Real countermeasures, which are implemented to mitigate the threats, are taken only with respect to half of the reasoned cases (46%). The bad consequences of this situation are as follows: over a third of the companies affected by the attack lost at least 20% of their income.

Unfortunately, existing regulatory documents (both local and international) trying to cover the intended areas of technologies and, which are particularly important, critical applications, are insufficiently structured. They are developed without sufficient consideration of related technologies and should be more detailed in the terms of description of appropriate approaches for assessment and assurance of cybersecurity requirements and their relationship with the technologies used [2]. The problem of "branch customization" of the regulation documents is still challenging.

Based on the developed taxonomy of used notions [3] the main notions in accordance with product-process approach of cybersecurity assessment are *process, product and intrusion*. Processes are being implemented through the development stages of Instrumentation and Control systems (I&Cs)' life cycle in order to produce products.

The products can be vulnerable to intrusions of various types that can affect the product itself. Results of the implementation of the processes (i.e., all the processes that led to the creation of the product) can have effects on possible consequential changes in such processes. Each process comprises activities, and, in case of "non-ideal" process, some of them can contain discrepancies, e.g. anomalies. In terms of cybersecurity some of the anomalies can be vulnerabilities of the product. Vulnerabilities, in turn, can be exploited by an adversaries during intrusion into the product to implement an by adversaries attack in order to introduce some unintended functionality into the product. And thereby, the gaps are introduced in the process of the cybersecurity assessment and, finally, in the product.

One of the main milestones in achieving security objectives is the unification of the process of analyzing and ensuring the cybersecurity of complex systems. Another problem is the correctness and validity of the assessment process itself, which can potentially harm the assessment result at the end of the day. Thus, both industry and the academic sector need to have cybersecurity assurance technique that will take into account all the features of the technologies used in the product and possible gaps in the assessment process of assurance the cybersecurity of such systems.

WORK-RELATED ANALYSIS. There are several different ways of constructing the cases [4]. They can be characterized in terms of a safety justification "triangle" [5]: claims – standards – vulnerabilities. As soon as safety plays master role in safety-critical systems the adaptation of this triangle to the cybersecurity assurance was made as follows:

- claims (or positive properties) about the systems' cybersecurity behavior. Here the specific claims for the I&Cs are supported by arguments and evidences at progressively more detailed level;
- the use of accepted standards and guidelines which is connected with demonstrating compliance to a known safety standard [6];
- vulnerabilities analysis (or negative properties) where it is demonstrated that potential vulnerabilities within a system do not constitute a problem.

The basic understanding of assurance in this paper is treated from [7]. The case-based assessment practices for different domains can be found in [8]-[9].

OBJECTIVES AND STRUCTURE. The objective of the paper is to briefly describe the results of development and application of the technique for providing the gap-analysis of assurance case-based cybersecurity assessment

The structure of the paper is as follows. Section II presents description of main entities, which can play role of possible gaps during the cybersecurity analysis and describes main stages of gap-analysis of assurance case-based cybersecurity assessment. Section III contains the example of the gaps which could possibly arise during stages of cybersecurity analysis. Section IV contains conclusions and future work directions.

Description of the Cybersecurity Assurance Case-oriented Technique

The main stages of the overall cybersecurity assurance case-based technique are depicted on the fig. 1. The brief description of the main stages is as follows:

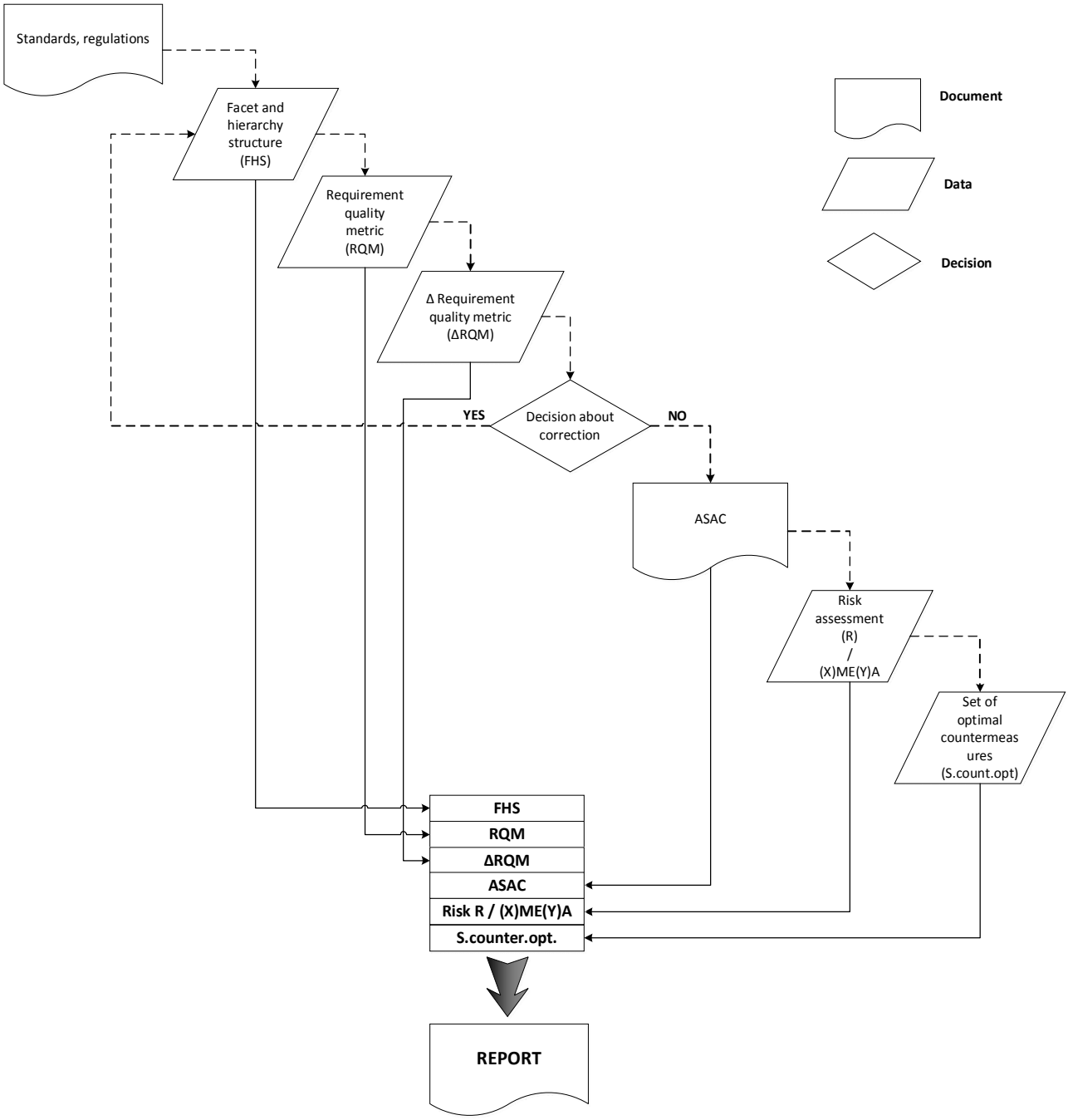

Fig. 1. The overall picture of assurance case-based cybersecurity assessment

- Building the **requirements profile** for the particular product and requirements for its cybersecurity assessment and assurance. The requirement profile should take into account international standards, local regulations, best practices with the detailed description of the technologies used.
- Building the **facet and hierarchical structure** of the requirements profile. This stage allows establishing the interrelations of the requirements, which are "located" at different levels of abstraction (which were initially taken from different levels of the normative documents, e.g. international and local level) or represent different branches. FHS allows representing the requirement profile in way that is more convenient for understanding. It implies the analysis of semantics and classification of requirements.
- It is especially crucial because for complex systems, e.g. safety-critical, mission-critical systems the amount of requirements and thus the size of the resulting requirement profile can be extremely huge in its size and its interpretation is a separate and complex issue. The requirements for cybersecurity assessment and assurance process should be addressed carefully.
- Assessment of the corresponding **Requirement Quality Metric (RQM).** It implies analysis of semantics and classification of requirements, representation of FHS in the form of multigraph, determination of weighting coefficients and calculation of the fuzzy / entropy coefficient, which is named Requirement Quality Metric ("actual").
- Assessment of the **delta-RQM** to the required level. During this stage, the determination of the requirements for RQM important for cybersecurity ("ideal") should be done. After this the delta-RQM should be calculated by comparison of RQM "ideal" with RQM "actual".
- Decision **about correction**. At this stage the person or group of persons conducting the cybersecurity assurance analysis should make a decision about correction of the FHS (which was built earlier) on the basis of delta measure of effectiveness. If the decision is affirmative then the facet and hierarchical structure should be modified and the process of RQM assessment will start again.
- If the decision to amend the system was not made then the **Advanced Security Assurance Case (ASAC)** should be developed. The process of development of ASAC is described in detail in [10]. The example application of ASAC in the process of cybersecurity assurance of multi-version safety-critical I&Cs based on Field Programmable Gate Arrays (FPGA) is described in [11].
- For assessment of risks related with the intrusion to the system (e.g. unrealized countermeasures) the Intrusion Modes, Effects and Criticality Analysis **IMECA** should be executed. IMECA is a modification of FMEA (Failure Modes and Effects Analysis) which takes into account possible intrusions to the system [12]. Since any vulnerability can become a failure if an intrusion occurs, the IMECA should be used. It allows taking into account failures caused by intrusions "using" system vulnerabilities. During this stage the *(X)ME(Y)A* modifications of FMEA family can be used depending on the task as well, where $X \in \{Concept, Design, Failure, Intrusion, Process, Product, Software, System\}$ and $Y \in \{Criticality, Diagnostic\}$. At this stage the level of acceptable risk is assessed. All related risks are calculated, studied and ranged according with their criticality using criticality matrixes. Here the joint use of gap-analysis together with IMECA is also possible. It is based on the identification of all possible discrepancies which can be introduced by intrusions that in its turn could arise during the cybersecurity assessment stages. Ranging of gaps (which arise during the I&Cs' development process) which could lead to intrusions is made by its criticality of using them by an intruder to perform successful attack. The joint application of gap-analysis together with IMECA provided for cybersecurity assessment of I&Cs used in nuclear power plant is presented in [3].
- To eliminate the identified (or even possible) vulnerabilities (furthermore attacks and threats) or make them difficult (or even impossible) to exploit by an intruder/attacker the determination of both sufficient and cost-effective countermeasures should be done. The **set of countermeasures** is developed during this step taking into account maximum of effectiveness (maximum level of cybersecurity) and minimum costs.

All data from previous steps are convoluted into the case report, which contain the resulting data received from all steps and description of the corresponding identified gaps in order to make them traceable, verifiable and justifiable.

It allows both developers, evaluators, owners and any kind of parties involved implement changes to the system within their competencies and thus this mechanism itself provide confident and scalable solution.

All abovementioned steps are forming the overall picture of gap-analysis of assurance case-based cybersecurity assessment.

Gap-analysis of Assurance case-based cybersecurity assessment technique

The gaps could be introduced into the result of cybersecurity assessment (final product of the cybersecurity assessment) through imperfection of the following entities:

- *human* (process developer). Gaps of such type can appears in the final product due to insufficient knowledge of the developer, validator, owner, etc. or due to the fact that the person or group of persons conducting the cybersecurity analysis are insiders pursuing destructive purposes;
- *technique*. Usage of inappropriate techniques during cybersecurity analysis or incorrect interpretation of the results obtained could possible lead to the gaps of such type;
- inappropriate *tools*, which are used during the cybersecurity assessment process.

Each stage of the assurance case-based cybersecurity analysis technique can possibly contain gaps itself. So, in order to obtain the correct results of cybersecurity assessment the developer, validator, owner or any stakeholder should be confident that no gaps were introduced during the cybersecurity analysis stages.

The example of results of the gap-analysis for each stage of the algorithm is represented in Table I.

Table I. **Identification of Gaps**

Stage	Identified gaps
Standards, regulations	Not all standards and regulations are taken into account Standards do not include all the features of used technologies Not all requirements are included in the profile of requirements (the requirements profile is incomplete) Implementation of unnecessary requirements (unimportant for security) Standards do not include all the features of used technologies
Facet and hierarchy structure (FHS)	The facet and hierarchy structure is made incorrectly Not all requirements are included in the structure (the FHS is incomplete)
Requirement Quality Metric (RQM)	The weights for the requirements are defined inaccurately Classification of requirements is made incorrectly (e.g. Boolean - like not Boolean; Not Boolean - like Boolean)
Requirement Quality Metric (ΔRQM)	The requirements for Δ Effectiveness criterion (ΔEf.cr.) are determined incorrectly (overestimated / underestimated)
Decision about correction	Decisions about correctness of the requirements are erroneous (incomplete, inaccurate)
ASAC	ASAC is built erroneously (incomplete, inaccurate) Expert' activities algorithm is determined erroneously (incomplete, inaccurate, not in detail) The final results of conformity is determined erroneously
Risk assessment (R) / (X)ME(Y)A	The list of gaps is incomplete Not all gaps are itemized and included to (X)ME(Y)A / IMECA The probability and severity of the non-conformity of the system with the requirements is determined inaccurately The risk is calculated inaccurately
Set of optimal countermeasures (S.count.opt)	The list of countermeasures is incomplete The coverage of the system by countermeasures is done erroneously (incomplete, inaccurate, incorrect) Generalized indicators of countermeasures optimality were calculated erroneously The optimization procedure is not implemented correctly
REPORT	Negotiation of results is not traced back The report is made with errors

Conclusions and Future Work

To sum up, the cybersecurity analysis process using the case approach may have inconsistencies that need to be evaluated and accounted for so that their impact on the outcome of the assessment is minimal.

The development and implementation of methods and tools for cyber security analysis can improve the reliability of evaluation and enforcement of cyber security requirements. The use of ASAC as an algorithmic mechanism for representing the requirements for cybersecurity allows the analysis process to be conducted in an understandable and reproducible way by any party involved. Thus, the subjectivity of evaluating cybersecurity is reduced.

The paper discusses the main elements of performed gap-analysis for assurance case-based cybersecurity assessment using ASAC. The application of such technique allows decreasing a probability of discrepancies (furthermore vulnerabilities) exploitation and appearance of security flaws of the cybersecurity assessment technique itself.

The proposed cybersecurity assessment approach and technique were applied to cyber security assessment of RadICS FPGA-based I&C platform, developed by Research and Production Corporation Radiy. Gap-analysis and IMECA were applied in development of a company standard in Research and Production Corporation Radiy that is harmonized with international standards.

This normative document is used during implementation of development and verification activities for safety-critical systems for nuclear power plants in Ukraine.

Future steps of the research will be dedicated to more careful determination of gaps during the stages of assurance-based cybersecurity analysis as well as development of the tool for automation of the described technique.

Acknowledgment

This paper is based on the experience obtained during constant work within of the EU-funded projects, namely in the frame of the educational project: SEREIN project funded under Tempus programme – «Modernization of postgraduate studies on SEcurity and REsilience for human and INdustry related domains» (543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCP) [13].

REFERENCES

1. *Cisco 2017 Annual cybersecurity report*, available at: https://www.cisco.com/c/m/en_au/products/security/offers/annual-cybersecurity-report-2017.html (last accessed March 4, 2018).
2. Illiashenko, O., Kharchenko, V. and Jervan, G. (2013), "Security of industrial FPGA-based I&C systems: normative base and sis approach", *Radioelectronic and computer systems*, No. 3 (62), pp. 86-91.
3. Illiashenko, O., Kharchenko V., Kovalenko, A., Sklyar, V. and Boyarchuk, A. (2014), "Security informed safety assessment of NPP I&C systems: GAP-IMECA technique", *Proceedings of the 22nd International Conference on Nuclear Engineering ICONE 22*, Chezh Republic.
4. Bishop, P.G., Bloomfield, R.E. and Guerra, S. (2004), "The future of goal-based assurance cases", Workshop on Assurance Cases, *2004 International Conference on Dependable Systems and Networks*, Florence.
5. Bloomfield, R., Netkachova, K. and Stroud, R. (2013), "Security-Informed Safety: If It's Not Secure, It's Not Safe", A. Gorbenko, A. Romanovsky, V. Kharchenko (Eds.): *SERENE 2013, LNCS 8166*, pp. 17-32.
6. Cyra, L. and Gorski, J. (2011), *SCF - A Framework Supporting Achieving and Assessing Conformity with Standards*. Special Issue: Secure Semantic Web. 33(1), 80 p.
7. Williams, J.R. and George, F.J. (1998), *A Framework for Reasoning about Assurance*, Document Number ATR 97043, Arca Systems, Inc. 23 April 1998.
8. *Towards an Assurance Case Practice for Medical Devices, Carnegie Mellon University*, available at: http://www.sei.cmu.edu/reports/09tn018.pdf (last accessed March 4, 2018).
9. *A Method of Trust Case Templates to Support Standards Conformity Achievement and Assessment*, available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.163.906&rep=rep1&type=pdf (last accessed March 4, 2018).
10. Illiashenko, O., Potii, O. and Komin D. (2015), "Advanced security assurance case based on ISO/IEC 15408", Conference: *DepCoS - RELCOMEX 2015, At Brunow Palace*, Vol.: Theory and Engineering of Complex Systems and Dependability, Proc. of the Tenth Int. Conf. on Dependability and Complex Systems DepCoS-RELCOMEX, Brunów, Poland, pp 391-401.
11. Illiashenko, O., Broshevan, Ye. and Kharchenko, V. (2016), "Cybersecurity Case for FPGA-Based NPP Instrumentation and Control Systems", Paper No. ICONE24-60440, pp. V005T15A027, *24th International Conference on Nuclear Engineering*, Vol. 5: Student Paper Competition; Charlotte, North Carolina, USA, DOI: 10.1115/ICONE24-60440.
12. Babeshko, E. (2008), "Applying F(I)MEA technique for SCADA-based industrial control systems dependabilty assessment and ensuring", *Proc. of Int. Conf. on Dependability of Computer Systems DepCoS-Relcomex 2008*, Academic Press, 5.
13. Tempus SEREIN. Modernization of postgraduate studies on security and resilience for human and industry related domains, available at: website http://serein.eu.org/ (last accessed March 4, 2018).

Надійшла (received) 7.03.2018
Прийнята до друку (accepted for publication) 25.04.2018

Геп-аналіз оцінювання кібербезпеки за допомогою кейсів запевнення: техніка та приклад використання

О. О. Ілляшенко, В. С. Харченко, А. Кор

Предметом вивчення в статті є процеси оцінювання кібербезпеки інформаційно-керуючих систем (ІКС). **Метою** є розробка техніки аналізу розрив процесу проведенні аналізу кібербезпеки. **Завдання:** розробити метод аналізу розривів у процесі оцінювання не функціональних вимог до функціональної та кібербезпеки ІКС, заснований на класифікації вимог з урахуванням можливості їх декомпозиції, який включає в себе побудову поліпшеного кейса запевнення інформаційної безпеки і визначення контрзаходів щодо усунення виявлених розривів. **Висновки.** Наукова новизна отриманих результатів полягає в наступному: отримав подальшого розвитку метод забезпечення інформаційної безпеки цифрових компонентів ІКС шляхом проведення аналізу невідповідностей вимог з використанням процедур опису вразливостей і оцінки критичності наслідків вторгнень, а також визначення множини контрзаходів за критерієм «безпека-вартість», що дозволяє зменшити ризики до прийнятного рівня.

Ключові слова: ПКЗІБ – Покращений Кейс Запевнення Інформаційної Безпеки; аналіз розривів; кібербезпека; оцінювання; вимога; відповідність.

Геп-анализ оценки кибербезопасности с помощью кейсов заверения: техника и пример использования

О. А. Ильяшенко, В. С. Харченко, А. Кор

Предметом изучения в статье являются процессы оценивания кибербезопасности информационно-управляющих систем (ИУС). **Целью** является разработка техники анализа разрывов процесса анализа кибербезопасности. **Задачи:** разработать метод анализа разрывов в процессе оценивания нефункциональных требований к функциональной и кибербезопасности ИУС, основанный на классификации требований с учетом возможности их декомпозиции, который включает в себя построение улучшенного кейса заверения информационной безопасности и определение контр-мер по устранению выявленных разрывов. **Выводы.** Научная новизна полученных результатов состоит в следующем: получил дальнейшее развитие метод обеспечения информационной безопасности цифровых компонентов ИУС путем проведения анализа разрывов требований с использованием процедур описания уязвимостей и оценки критичности последствий вторжений, а также определения множества контрмер по критерию «безопасность-стоимость», что позволяет уменьшить риски до приемлемого уровня.

Ключевые слова: УКЗИБ – Улучшенный Кейс Заверения Информационной Безопасности; анализ разрывов; кибербезопасность; оценивание; требование; соответствие.