https://doi.org/10.31891/csit-2025-4-10
UDC 004.93

BABESHKO Ievgen, KHARCHENKO Viacheslav
National Aerospace University "Kharkiv Aviation Institute"
LEONTIIEV Kostiantyn
Research and Production Corporation "Radiy"

METHOD FOR ENHANCING FMECA (XMECA) SAFETY ASSESSMENT PROCEDURES CONSIDERING THE CRITICALITY OF ASSUMPTIONS AND ANALYSIS ERRORS

In existing studies that discuss the Failure Modes, Effects, and Criticality Analysis (FMECA, XMECA) method, two principal limiting factors are commonly identified: the significant influence of engineers' and auditors' experience on the resulting safety assessments, and the presence of restrictive assumptions embedded in assessment procedures and supporting tools. To address these limitations, this paper proposes a method for enhancing FMECA (XMECA) safety assessment procedures that explicitly accounts for the criticality of underlying assumptions and analysis errors. Case study of applying the proposed method demonstrate that it can serve as an effective instrument for researchers and developers working on reliability and safety assessment problems in critical systems. Further research is devoted to application of the method in different contexts and industrial sectors.

Keywords: safety assessment, assumption, criticality, FMECA, XMECA

БАБЕШКО Євген, ХАРЧЕНКО Вячеслав
Національний аерокосмічний університет «Харківський авіаційний інститут»
ЛЕОНТІЄВ Костянтин
Науково-виробниче підприємство «Радій»

МЕТОД УДОСКОНАЛЕННЯ FMECA (XMECA)-ПРОЦЕДУР ОЦІНЮВАННЯ БЕЗПЕКИ З ВРАХУВАННЯМ КРИТИЧНОСТІ ПРИПУЩЕНЬ І ПОМИЛОК АНАЛІЗУ

Зростання складності, гетерогенності та ієрархічної організації критичних систем керування й контролю істотно ускладнює процеси оцінювання їхньої надійності та безпеки. У таких умовах широкого застосування набули напівформальні методи аналізу, серед яких одним із найбільш поширених є аналіз видів, наслідків і критичності відмов FMECA (Failure Modes, Effects and Criticality Analysis) та його численні модифікації XMECA. Попри практичну цінність і гнучкість, зазначені методи мають низку суттєвих обмежень, зокрема високу залежність результатів оцінювання від експертного досвіду, наявність застарілих або неявних припущень у процедурах аналізу, а також імовірність виникнення помилок під час формування та інтерпретації FMECA-таблиць.

У статті запропоновано метод удосконалення FMECA (XMECA)-процедур оцінювання безпеки, що базується на явному врахуванні критичності припущень і помилок аналізу. Метод передбачає формалізацію структури FMECA-таблиці у вигляді множин компонентів, видів відмов, наслідків та показників критичності, а також введення множин припущень і потенційних помилок, які впливають на результати оцінювання. Для аналізу впливу таких факторів використовується ризик-орієнтований підхід із застосуванням нечіткої шкали оцінювання та багаторівневої експертної процедури, що враховує типи запитань і профілі практичного та теоретичного досвіду експертів.

Запропонований підхід дозволяє обґрунтовано визначати необхідність модифікації як структури FMECA-таблиць, так і послідовності виконання процедур аналізу залежно від критичності виявлених припущень і помилок. Наведений приклад застосування методу демонструє його ефективність для зменшення ризиків переоцінювання або недооцінювання безпеки. Отримані результати свідчать про доцільність використання методу в задачах оцінювання надійності та безпеки критичних систем у різних галузях промисловості.

Ключові слова: оцінювання безпеки, припущення, критичність, FMECA, XMECA

Received / Стаття надійшла до редакції 14.11.2025
Accepted / Прийнята до друку 27.12.2025

Introduction

The increasing complexity, heterogeneity, and hierarchical organization of safety-critical instrumentation and control systems have significantly intensified the challenges associated with their safety assessment. As a result, purely formal methods based on exhaustive mathematical modeling are often impractical, while fully informal approaches lack sufficient rigor. This has led to the widespread adoption of so-called *semi-formal* assessment techniques, which integrate expert-driven reasoning and risk-based procedures with elements of reliability theory, including probabilistic models, Markov chains, and state-transition representations [1].

Related works

A key advantage of semi-formal methods is their ability to support controllable scalability of assessment tasks. This property is particularly important for complex instrumentation and control systems characterized by a large number of components, functional diversity, and multi-level architectural hierarchies.

Among the earliest and most established semi-formal techniques is Failure Modes, Effects, and Criticality Analysis (FMECA) [2,3]. Developed and refined over several decades, FMECA has undergone substantial methodological evolution, resulting in numerous domain-specific adaptations. These variants are often collectively denoted as XMECA, where the placeholder "X" may represent failures, intrusions, events, or other phenomena of interest. Additional qualifiers – such as software, hierarchical, or security – are commonly introduced to reflect the specific analysis focus [4,5].

In recent years, FMECA-based methods have also been increasingly applied to security-critical systems. Notable examples include IMECA (Intrusion Modes and Effects Criticality Analysis), which focuses on cybersecurity threats, and FMEDA (Failure Modes, Effects, and Diagnostics Analysis), which explicitly considers the effectiveness of diagnostic mechanisms for detecting both safe and unsafe failures [6].

Despite their flexibility and practical relevance, FMECA and XMECA techniques suffer from several fundamental limitations.

First, the identification and justification of system components, failure modes, and their safety relevance is inherently complex. Estimating failure probabilities and severities – key parameters for determining criticality via criticality matrices – requires substantial engineering expertise. Consequently, safety assessment outcomes are highly sensitive to expert judgment, including potential inaccuracies, biases, and uncertainty. These risks have been highlighted in multiple studies [4,7, 8].

Second, many FMECA applications rely on long-standing assumptions that were introduced during the early development of the method and are embedded in existing software and toolchains [9, 10, 11]. The validity of these assumptions under modern system architectures and operational conditions is not always adequately re-evaluated.

Third, traditional FMECA approaches often treat safety and cybersecurity as largely independent concerns, resulting in limited adoption of security-informed safety methodologies [12].

Addressing these challenges requires systematic involvement of experts who are capable not only of providing domain knowledge but also of critically reassessing the assumptions and methodological choices underlying reliability and safety evaluations, based on real operational experience [4]. In our previous works [4, 13], we analyzed several risks associated with FMECA assumptions and proposed approaches for aligning expert assessments, particularly for qualitative (verbal) information. However, further refinement is necessary, especially with respect to differentiating expert roles, experience profiles, and the nature of assessment questions across distinct FMECA stages.

Model for Safety Assessment using FMECA (XMECA) Procedures

As discussed in our previous work [13], the initial structure of FMECA-table, denoted as FMT_0, could be defined by tuple of sets:

$$FMT_0 = < \{Comp_i\}, \{Mod_{ij}\}, \{Eff_{ij}\}, \{Crit_{ij}\}>, \quad (1)$$

where $MComp = \{Comp_i\}$, $i = 1,\ldots,n$, is the set of system components under analysis;
$MMod = \{Mod_{ij}\}$, $j = 1,\ldots,m_i$ is the set of safety-critical failure modes associated with $Comp_i$.
$MEff = \{Eff_{ij}\}$ is the set of effects corresponding to every failure mode Mod_{ij} of the component $Comp_i$;
$MCrit = \{Crit_{ij}\}$ is the set of criticality assessments of every failure mode Mod_{ij} that is defined as:

$$Crit_{ij} = Prob_{ij} \times Sev_{ij}, \quad (2)$$

where $MProb = \{Prob_{ij}\}$ and $MSev = \{Sev_{ij}\}$ are the sets of probability and severity of failures Mod_{ij}.
Figure 1 shows visual mappings of abovementioned sets to FMECA table columns.

It is assumed that classic FMECA considers only single failures of individual components. Therefore, total power of set FMT_0 is defined as the following sum:

$$N = m_1 + m_2 + \ldots + m_i + \ldots + m_n ; \quad (3)$$

Moreover, set of assumptions that determine the construction of FMT_0: can be also represented as set:

$$MAsm = \{Asm_k\}, k = 1,\ldots,a; \quad (4)$$

As well as set of errors that could be made during analysis using FMT_0:

$$MErr = \{Err_r\}, r = 1,\ldots,e. \quad (5)$$

Method proposed intends to justify and develop modifications to the FMECA table and procedure by considering the criticality of safety assessment impacts caused by assumptions MAsm and errors MErr.

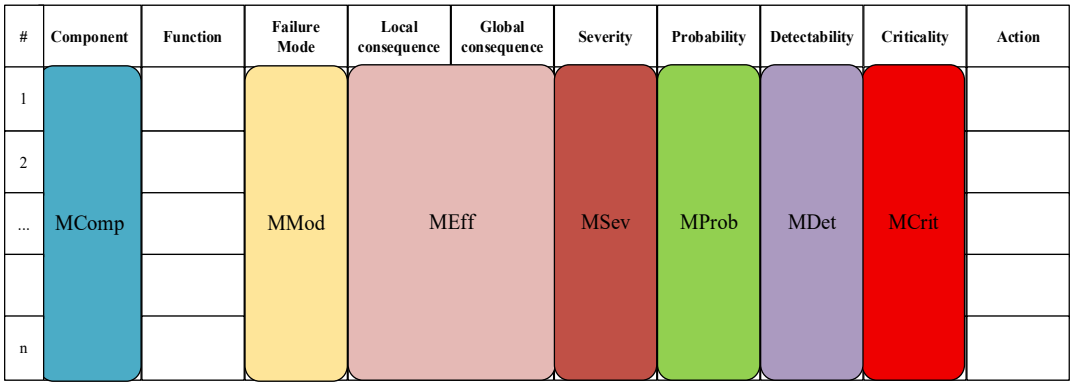

Fig. 1. Representation of FMECA as sets

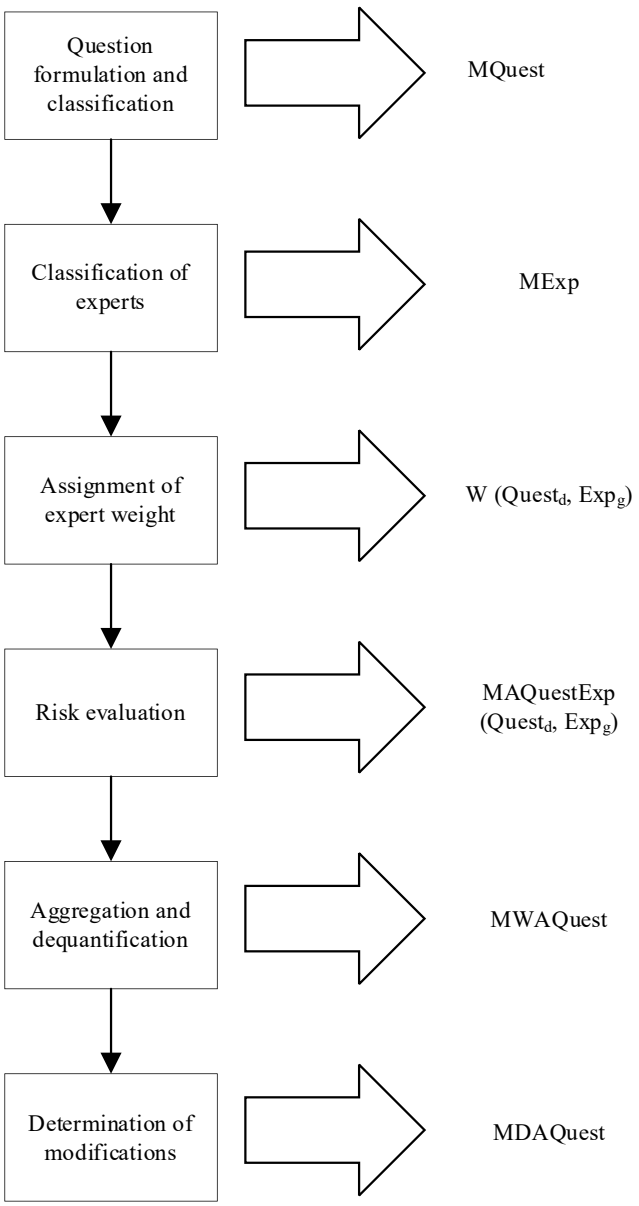

Fig. 2. Method steps and artifacts

Principles and Procedure for Enhancing FMECA (XMECA) Safety Assessment

The following key principles are utilized by the method:

1) Risk-oriented assessment. For criticality analysis of impact of assumptions from set MAsm and errors from set MErr on safety assessment result we choose the fuzzy risk scale:

– H (High) – significant impact,

– M (Medium) – moderate impact,

– L (Low) – minor impact:

2) Expert risk assessment. A group of professional experts with significant practical and research experience in instrumentation and control systems is formed. Requirements include: at least 10 years of practical and scientific work in the relevant field. To ensure high accuracy (fairness) of risk assessment method proposes:

– questions are categorized based on their focus (theoretical, practical, or mixed);

– experts are ranked according to their dominant experience profiles;

– expert answers are ranked based on both question type and expert specialization.

Sequence includes the following steps (Fig. 2):

1) Question formulation and classification. Sets of questions are related to sets of assumptions MAsm and sets of errors MErr.

$MQuest = \{Quest_d\}$, $d = 1,\ldots,q$;

$MQuest = PQuest \cup TQuest \cup PTQuest$,

$PQuest \cap TQuest = \emptyset$, $PQuest \cap PTQuest = \emptyset$, $TQuest \cap PTQuest = \emptyset$,

where PQuest, TQuest, PTQuest subsets that correspond to practical, theoretical, and mixed questions, respectively.

2) Classification of experts considering priorities of practical and theoretical experience:

$MExp = \{Exp_g\}$, $g = 1,\ldots,h$;

$MExp = PExp \cup TExp \cup PTExp$,

$PExp \cap TExp = \emptyset$, $PExp \cap PTExpt = \emptyset$, $TExp \cap PTExp = \emptyset$,

where PExp, TExp, PTExp – subsets of experts with larger practical, theoretical and universal experience.

3) Assignment of expert weight based on sets MQuest and MExp using H/M/L scale (depicted in Figure 3):

$W(Quest_d, Exp_g) = H$, if $Exp_g \subseteq PTExp$ independently from question types, or

if $Quest_d \subseteq PQuest$ and $Exp_g \subseteq PExp$, or if $Quest_d \subseteq TQuest$ and $Exp_g \subseteq TExp$;

$W(Quest_d, Exp_g) = M$, if Questd $\subseteq$ TPQuest and Expg $\subseteq$ PExp $\cup$ TExp;

$W(Quest_d, Exp_g) = L$, if $Quest_d \subseteq TQuest$ and $Exp_g \subseteq PExp$ or if $Quest_d \subseteq PQuest$ and $Exp_g \subseteq TExp$.

4) Risk evaluation of assumption risks MAsm and error risks MErr by experts, mapping back to H/M/L categories, forming the set MAQuestExp:

$MAQuestExp(Quest_d, Exp_g) = \{A_{dg}\}$.

5) Development of set of values of general (quantified) aggregated assessments:

$MWAQuest = \{WA_d\}$

and their dequantification by H/M/L scale

$MDAQuest = \{DA_d\}$.

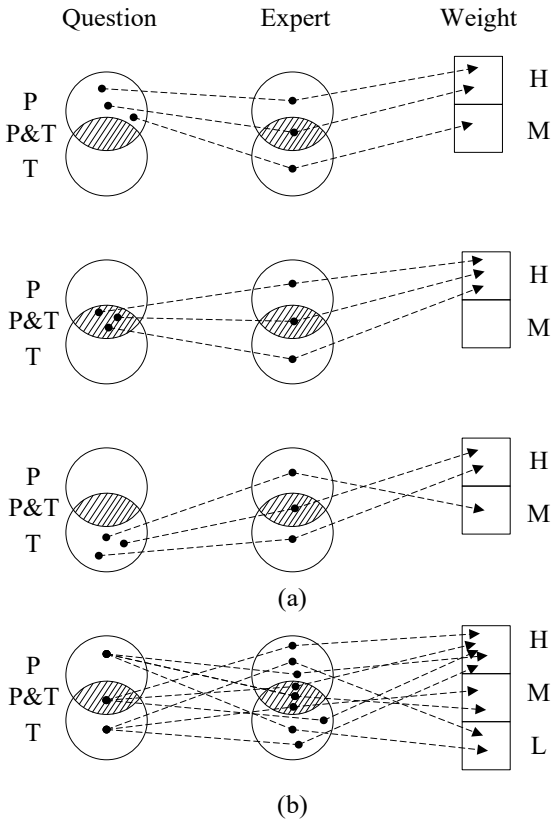

Fig. 3. Two-level (a) and (b) three-level ranking

6) Determination of FMT_0 and FMECA modification ways considering criticality of assumption impact from set MAsm and error impact from set MErr on safety assessment result according to the set MDAQuest:

– refinement of object of modification – FMT_0 table or FMECA method procedures. To achieve this set MQuest is being divided into subsets of questions that may require making changes into MQuestT table, MQuestM method sequence, as well as making changes into table and sequence MQuestTM:

– MQuest = MQuestT U MQuestM U MQuestTM;

– clarification of modification type for the subsets MQuestT, MQuestM, MQuestTM;

– determination of modification obligation level using the rule:

– modification by question $Quest_d$ is required, if $DA_d = H$;

– modification by question $Quest_d$ is recommended, if $DA_d = M$;

– modification by question $Quest_d$ is required, if $DA_d = L$;

– implementation of FMT_0 modification and relevant change of FMECA sequence;

– implementation of FMECA sequence modification without changing the FMT_0.

Case Study

Table 1 summarizes the possible error modes and describes their corresponding effects on safety. Possible effects include safety overestimation and safety underestimation. Safety overestimation occurs when the analysis indicates a higher level of safety than actually exists, which may lead to insufficient safeguards, delayed corrective actions, or unwarranted confidence in normal operation. In contrast, safety underestimation arises when risks are assessed as being greater than they truly are, potentially resulting in overly conservative designs, unnecessary operational restrictions, or increased costs. Both effects have negative impact and therefore must be carefully identified and mitigated.

Table 1.

Error modes and effects on safety

Error Modes	Effects
Not all components are defined for safety assessment	Safety overestimation
The number of components used for safety assessment is given too high	Safety underestimation
Not all failure modes are considered	Safety overestimation
Excess failure modes are considered	Safety underestimation
Failure criticality (probability, severity) is underestimated	Safety overestimation
Failure criticality (probability, severity) is overestimated	Safety underestimation
Failure mistakenly treated as detected	Safety overestimation
Failure mistakenly treated as undetected	Safety underestimation
Failure multiplicity is underestimated	Safety overestimation
Failure multiplicity is overestimated	Safety underestimation
Multiple faults of different components at one level are not considered	Safety overestimation
Multiple faults of different components at different levels are not considered	Safety overestimation
Multiple faults of different versions are not considered	Safety overestimation
Not all levels are considered	Safety overestimation
Excess levels are considered	Safety underestimation
Interaction between levels is not considered	Safety overestimation
Excess interaction between levels is considered	Safety underestimation
Not all software faults are considered	Safety overestimation
More than required software faults are considered	Safety underestimation
Not all hardware faults (physical and project) are considered	Safety overestimation
More than required hardware faults (physical and project) are considered	Safety underestimation
Hardware and software faults are not considered with respect to possible attacks	Safety overestimation

Table 2 contains analysis results of error risks.

Conclusions

This paper examined the existing limitations of the Failure Modes, Effects, and Criticality Analysis (FMECA/XMECA) method and proposed an enhanced approach that explicitly accounts for the criticality of underlying assumptions and potential errors in expert assessments. The proposed method proved effective in mitigating key limitations of traditional FMECA applications, particularly those related to the influence of human factors and entrenched stereotypes in expert judgment. Examples of practical application of the new approach demonstrate its potential to improve the accuracy of reliability and safety assessments for critical systems.

The obtained results indicate that integrating enhanced FMECA procedures can significantly increase the effectiveness of safety assessment processes. This, in turn, may contribute to the development of safer and more reliable systems across various industrial domains. To confirm the general validity of the proposed method, further research is required, including its application in different contexts and industrial sectors. Of particular importance is the investigation of the scale and boundaries of the proposed approach's impact under varying technological constraints and domain-specific operational scenarios.

Table 2.

Analysis results

Error Modes	Effects	Probability	Severity	Risk
Not all components are defined for safety assessment	Safety overestimation	2,1	1,6	3,36
The number of components used for safety assessment is given too high	Safety underestimation	2,4	2,3	5,52
Not all failure modes are considered	Safety overestimation	1,5	1,5	2,25
Excess failure modes are considered	Safety underestimation	2,3	2,6	5,98
Failure criticality (probability, severity) is underestimated	Safety overestimation	2	1,6	3,2
Failure criticality (probability, severity) is overestimated	Safety underestimation	2,2	2,3	5,06
Failure mistakenly treated as detected	Safety overestimation	2,3	1,7	3,91
Failure mistakenly treated as undetected	Safety underestimation	2,1	2,1	4,41
Failure multiplicity is underestimated	Safety overestimation	1,6	1,3	2,08
Failure multiplicity is overestimated	Safety underestimation	2	2,2	4,4
Multiple faults of different components at one level are not considered	Safety overestimation	1,9	1,6	3,04
Multiple faults of different components at different levels are not considered	Safety overestimation	1,8	2	3,6
Multiple faults of different versions are not considered	Safety overestimation	1,8	2	3,6
Not all levels are considered	Safety overestimation	2,1	1,7	3,57
Excess levels are considered	Safety underestimation	2,4	2,5	6
Interaction between levels is not considered	Safety overestimation	1,7	1,7	2,89
Excess interaction between levels is considered	Safety underestimation	2,3	2,5	5,75
Not all software faults are considered	Safety overestimation	1,7	1,9	3,23
More than required software faults are considered	Safety underestimation	2,2	2,7	5,94
Not all hardware faults (physical and project) are considered	Safety overestimation	1,9	1,6	3,04
More than required hardware faults (physical and project) are considered	Safety underestimation	2,2	2,7	5,94
Hardware and software faults are not considered in respect to possible attacks	Safety overestimation	2	1,9	3,8

Author Contributions according to CRediT

Conceptualization, I.B. and V.K.; methodology, V.K.; case study, K.L.; writing - original draft preparation, I.B and K.L.; writing - review and editing, V.K; visualization, I.B. All authors have read and agreed to the published version of the manuscript.

Declaration on the use of generative artificial intelligence tools

In preparing this work, no generative artificial intelligence tools were used by the authors. Authors take full responsibility for the content of this publication.

References

1. Ozirkovskyy L., Volochiy B., Shkiliuk O., Zmysnyi M., Kazan P. Functional safety analysis of safety-critical system using state transition diagram. *Radioelectronic and Computer Systems*. 2022. No. 2. P. 145-158. DOI: https://doi.org/10.32620/reks.2022.2.12
2. Signoret JP., Leroy A. Failure Mode, Effects (and Criticality) Analysis, FME(C)A. In: *Reliability Assessment of Safety and Production Systems*. Springer Series in Reliability Engineering. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-64708-7_10
3. Oliveira J., Carvalho G., Cabral B., Bernardino J. Failure Mode and Effect Analysis for Cyber-Physical Systems. *Future Internet*. 2020. 12. 205. DOI: https://doi.org/10.3390/fi12110205
4. Babeshko I., Illiashenko O., Kharchenko V., Leontiev K. Towards Trustworthy Safety Assessment by Providing Expert and Tool-Based XMECA Techniques. *Mathematics*. 2022, 10, 2297. DOI: https://doi.org/10.3390/math10132297
5. Catelani M., Ciani L., Cristaldi L., Faifer M., Lazzaroni M. and Khalil M. Toward a new definition of FMECA approach. *2015 IEEE International Instrumentation and Measurement Technology Conference (I2MTC) Proceedings*, Pisa, Italy, 2015. P. 981-986. DOI: https://doi.org/10.1109/I2MTC.2015.7151403
6. Park J. I. A Case Study on FMEDA Process to Evaluate Hardware Safety Integrity Level. DOI: https://doi.org/10.13140/RG.2.2.33330.94407
7. Suharjo B., O.S. Suharyo, Bandono A. Failure Mode Effect and Criticality Analysis (FMECA) for Determination Time Interval Replacement of Critical Components in Warships Radar. *Journal of Theoretical and Applied Information Technology*. 2019. Vol. 97. No 10. P. 2861 – 2870
8. Kiran M.B. A Review of Failure Mode Effect and Criticality Analysis (FMECA). Proceedings of the International Conference on Industrial Engineering and Operations Management, Istanbul, Turkey, March 7-10, 2022. P. 4506 - 4512.
9. Zanardi D., Barbieri M., Uguccioni G. DRIFT: A Data-driven Failure Mode, Effects and Criticality Analysis Tool. *Enterprise Interoperability: Smart Services and Business Impact of Enterprise Interoperability*. 2018. P. 285-290. DOI: 1 https://doi.org/10.1002/9781119564034.ch35
10. Meng X., Huang D., Dong Z. Military Software Fault Analysis Method Based on Improved SFMEA. 2023 14th International Conference on Reliability, Maintainability and Safety (ICRMS), Urumuqi, China, 2023. P. 480-485. DOI: https://doi.org/10.1109/ICRMS59672.2023.00091

11. Catelani M., Ciani L., Cristaldi L., Khalil M., Toscani S., Venzi M. A condition monitoring tool based on a FMECA and FMEA combined approach in Oil&Gas applications. *2016 IEEE International Instrumentation and Measurement Technology Conference Proceedings*, Taipei, Taiwan, 2016. P. 1-6. DOI: https://doi.org/10.1109/I2MTC.2016.7520373

12. Babeshko E., Kharchenko V., Leontiiev K., Ruchkov E. Practical Aspects of Operating and Analytical Reliability Assessment of FPGA-based I&C Systems. *Radioelectronic and Computer Systems*. No 3 (2020). P. 75-83. DOI: https://doi.org/10.32620/reks.2020.3.08

13. Babeshko I., Kharchenko V., Leontiiev K. Enhancing FMECA(XMECA)-based Safety Assessment Considering Criticality of Assumptions and Analysis Errors. *2024 14th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Athens, Greece, 2024. P. 1-5. DOI: https://doi.org/10.1109/DESSERT65323.2024.11122229

Ievgen Babeshko **Євген Бабешко**	PhD, Associate Professor, Doctoral Student of the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine, e-mail: e.babeshko@csn.khai.edu https://orcid.org/0000-0002-0244-1657 Scopus Author ID: 24823713000, ResearcherID: I-9973-2018	кандидат техн. наук, доц., докторант кафедри комп'ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет «Харківський авіаційний інститут», Харків, Україна
Vyacheslav Kharchenko **Вячеслав Харченко**	DrS on Engineering, Professor, Head of the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine, e-mail: v.kharchenko@csn.khai.edu https://orcid.org/0000-0001-5352-077X Scopus Author ID: 22034616000, ResearcherID: A-7719-2017	доктор техн. наук, проф., зав. кафедри комп'ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет «Харківський авіаційний інститут», Харків, Україна
Kostiantyn Leontiiev **Костянтин Леонтієв**	Technical Director of the Research and Production Corporation "Radiy", Kropyvnytskyi, Ukraine, e-mail: ksleontiev@radiy.com https://orcid.org/0000-0001-7315-0913 Scopus Author ID: 57195923255	технічний директор, Науково-виробниче підприємство «Радій», Кропивницький, Україна