UDC 004.056

ANASTASIYA OREKHOVA, VIACHESLAV MANULIK, AL-JAHLAWEE AKRAM FADHIL KADHIM, AL-KHAFAJI AHMED WALEED

National Aerospace University named after N. E. Zhukovzky «KhAI», Ukraine

SAFETY ASSESSMENT OF CRITICAL SYSTEMS BASED ON THE COMBINATION OF RISK ANALYSIS TECHNIQUES

This work is devoted to the problem of assessing the functional safety of critical systems. The existing risk analysis techniques have been analyzed and the possibility to apply them for functional safety assessment of critical systems has been considered. The possibility to combine the chosen techniques has been proven and carried out. As a result, the complex technique for functional safety assessment of critical systems has been developed. The tool for automation of the technique has been elaborated. The developed technique and the tool have been tested on the critical systems.

Keywords: *risk analysis, safety, critical system, assessment, tool, HAZOP, FMEA.*

Introduction

Development of evaluation information technology is one of the important fields of safety-critical systems research. Models, methods, and evaluation tools are the elements of information technology. Risk analysis approach has spread in assessing the safety of critical systems [1-5]. The most common methods for risk assessment are given in the standards [6, 7]. One of the problems is the necessity of the methods choice for particular applications. A study of methods of risk analysis for the safety assessment of automotive information systems is conducted in [8].

The HAZOP process is similar to the FME(C)A method in the possibility of identifying failure modes, their causes, and consequences. The difference is the reverse order of HAZOP, which performs basing on unwanted results and deviations and results in possible causes and failure modes, whereas FME(C)A begins with the determination of the mode of failure. The advantage of FME(C)A is the ability to obtain quantitative estimates of risk (probability and severity of consequences). The similarity of the methods allows to consider the problem of techniques aggregation to get a more accurate assessment of the systems safety. The purpose of this work is improving the methodology of assessment of critical systems functional safety by risk analysis methods aggregation to improve the completeness and accuracy of assessment. The structure of the article is organized as follows. The first section analyzes the existing methods of risk analysis, proved the possibility of chosen methods aggregation and implemented their union. The second section provides a tool that automates the process of evaluation. The third section provides examples of using the method to assess the safety-critical systems.

1. Combining of risk analysis methods

1.1. Choice of methods

To date, the task of choosing methods for safety assessment in the Safety Case was complicated by the large number of techniques of varying degrees of formality, complexity, ability to use of the life cycle stages, etc. We believe these methods are the most effective at the pre-design gathering stage, at the stage of analysis of the use context (task analysis), as well as at the stage of verification and validation of the finished product (usability testing). Processes and methods of safety HMI evaluation, developed within a software engineering, are mainly focused on the metric evaluation of the finished product.

Methods of risk assessment are given in [6]. Risk assessment can be carried out with varying degrees of depth and detail. The use of one or more methods is possible. When selecting methods, the rationale for their suitability should be presented.

Methods must have the following features:

- to be scientifically sound;
- conform to the system under study;
- to give an understanding of nature and the nature of risk, how to control and process.

Method selection can be implemented based on the following factors:

- purpose of the evaluation;
- system development;
- type of system;
- resources and opportunities;
- nature and degree of uncertainty;
- ability to obtain quantitative data output;

Table 1

Comparative analysis of risk assessment methods

Type of risk assessment methods	**Relevance of influencing factors**		
	Resources, and capability	**Nature and degree of uncertainty**	**Complexity**
Checklists	Low	Low	Low
Preliminary analysis of the hazards	Low	High	Average
Scenario Analysis	Average	High	Average
Fault tree analysis (FTA)	High	High	Average
Analysis of the "tree" of events	Average	Average	Average
Analysis of the causes and consequences	High	Average	High
The analysis of types and the consequences of failures (FMEA and FMECA)	Average	Average	Average
Hazard and Operability Study (HAZOP)	Average	High	High
Reliability assessment of the operator (HRA)	Average	Average	Average
Multi-criteria decision analysis (MCDA)	Low	High	Average

– availability and accessibility of information for the system;

– the applicability of the method;

– complexity of methods;

– needs of decision makers.

Table 1 shows the results of a comparative analysis of several method-candidates for Safety Case.

Identification of potential hazards and performance problems is a key aspect of HAZOP method. For these purposes, an expert study is conducted to examine the deviations of system behavior. HAZOP is based on defining the entities and attributes, which are relevant to the system under study, and the possible deviations from the planned behavior. These deviations are represented by the guide words that stimulate creative analysis of experts. Experts have to assess if “standard” guide words can be used and make changes in interpretive translation in terms of each area of analysis where HAZOP is applied.

FMEA methodology allows you to identify the nature of failures, mechanisms for their occurrence and impact. FMEA can be accompanied by a critical analysis, when the significance of each type is determined (FMECA). FMEA analysis is applicable to both systems, and their component, including software.

HAZOP process is similar to the FMEA. It allows failure modes identification, their causes, and consequences. The difference is that HAZOP is carried out in reverse order of unwanted results and deviations to the possible causes and failure types, whereas FMEA starts with the failure type determination.

1.2. HAZOP and FME(C)A models

Classic HAZOP-table (table 2) can be represented by a set of F-vectors:

$$Fh =< e_f, c_f, kw_f, t_f, r_f, a_f >_{f=1}^{F}, \qquad (1)$$

where e_f – the failed element;

c_f – characteristic of the element;

kw_f – guideword;

t_f – deviation;

r_f – cause of failure;

a_f – consequence of failure.

Table 2

Classic table of HAZOP

Element	Characteristic of the element	Guideword	Deviation	Cause of failure	Consequence of failure
1.	...	...	...	...	...
2.	...	...	...	...	...

The number of lines in table 2 can be equal or more than a number of elements in the system, depending on a number of guide words used in the analysis..

Classic FME(C)A-table (table 3) is a list FT that can be represented by a set of F-vectors (number of table lines – elements in system):

$$FT =< e_f, k_f, r_f, p_f, u_f >_{f=1}^{F}, \qquad (2)$$

where e_f – the failed element;

k_f – failure mode;

r_f – consequence of failure;

p_f , u_f .– failure probability and severity that can be configured using indistinct scale (for example, «high» - «average» - «low»).

Table 3

Classic table of FME(C)A

Element	Failure mode	Consequence of failure	Criticality of failure	Probability of failure
1.	...	...	...	...
2.	...	...	...	...

1.3. Combining of FME(C)A and HAZOP

Models of FME(C)A and HAZOP are similar to each other, and many fields are the same (figure 2.3). It allows to use the advantages of one methodology while using the other and, thus, extend the field of use and covering of failures developing of analyzed systems.

The key feature of HAZOP method to include to result table model 3 is using of guide words. In this case, it is recommended to move from table *Fh*, described by the model 1, to table Fh_t, described by the model 2:

$$Fh_t =< e_f, c_f, kw_f, k_f, a_f, p_f, u_f >_{f=1}^{F}, \qquad (3)$$

where e_f – element;

c_f – characteristic of the element;

kw_f – guideword;

k_f – cause of failure;

a_f – consequence of failure;

p_f , u_f – – failure probability and severity that can be configured using indistinct scale (for example, «high» - «average» - «low»). In this way, every combination of element and a failure will have a corresponding cases described in the table. The result of combining is the following table 4.

For critical system, the important indicator is covering of all possible failure cases, therefore entering of key words that improve expert's analysis, has a prospect to be productive developing of the methodology.

2. Tool for risk analysis

2.1. Purpose

In order to support the methodology, of risk-analysis a tool named Risk Analysis Environment (RAE) has been developed. The tool makes it possible for user to combine the methods of risk analysis by picking the most relevant information regarding a specific research work into the human-machine interface security.

This tool has been localized in English and Russian and provide the possibility of adding new localizations. In addition, RAE has to provide the possibility to make add-ins modules that describe the methods of risk analysis.

2.2. Functions

The purpose of the tool is automatization of risk analysis of critical systems using the developed methodology. The tool has the following functions:

–forming of domain-specific feature set for analysis taking into account the capabilities;

– use standard methods set;

–use user characteristics;

–use user characteristics;

–combine them;

–storing of information for each research and the whole project (dates, descriptions, additional information and so on);

–capability to switch between different research works, to view and edit information about them;

–generation of a research report and exporting it to pdf;

–capability to extend the tool by adding the new methodology of risk analysis;

–switching of user interface language when the program is executed;

–storing of user settings and the capability of their export and import;

–registration of the tool in operating system as a file handler for the project of .raeproj format.

2.3. Architecture and components

The software has been implemented as a desktop application.

System architecture includes three layers:

1. UI – user interface level.
2. Logic – business logic of the application.
3. Storage – layer of data storing.

Figure 1 shows the component architecture of Risk Analysis Environment.

The tool consists of 4 main modules:

1. UI – user interface that has all components of interaction with user (windows, dialogues, wizards and control elements to create them);

2. Logic – component that stores the main logic of the application (research models managers, results export, options control and so on);

Table 4

Table of combination

Element	Characteristic of the element	Guideword	Cause of failure	Consequence of failure	Probability of failure	Criticality of failure
1.	...	...	...	...	...	...
2.	...	...	...	...	...	...

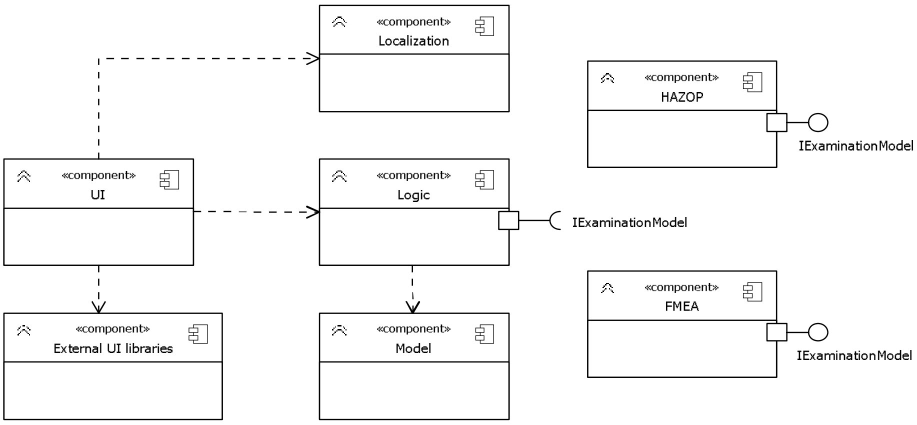

Fig. 1. Component architecture of the tool

3. Model – component that describes the hierarchy of carrying-out the risk analysis and determines the IExaminationModel interface describing the research methodology;

4. Localization – component that provides the support of different application parts localization.

Figure 1 also shows the components HAZOP and FMEA, which are the standard methods of risk analysis provided along with the software tool.

3. Study case

3.1. The unmanned aerial vehicle

The system under research is the unmanned aerial vehicle (UAV). Its purpose is of no interest in terms of this research. The system consists of two parts (figure 2): the control unit (CU) located on the ground and the UAV. Communication between the CU and the UAV are done wirelessly. The CU receives data from the aerial vehicle. The operator uses the CU to monitor data from the aerial vehicle and manage the vehicle.

Figure 2 shows the control unit. It consists of a display and control elements. The display shows the information received from the aerial vehicle: height, speed, battery charge and so on. Control elements are control sticks for spatial movement, ignition, etc.

3.2. Risk analysis

First, interface elements have to be classified. UAV control unit elements can be divided into three groups (figure 3):

- group 1 – elements of power control and control elements activation;

- group 2 – elements of space position and speed control;

- group 3 – display and elements of menu navigation.

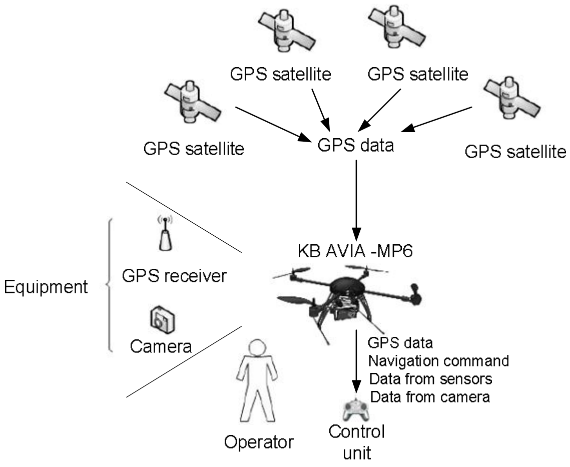

Fig. 2. UAV complex

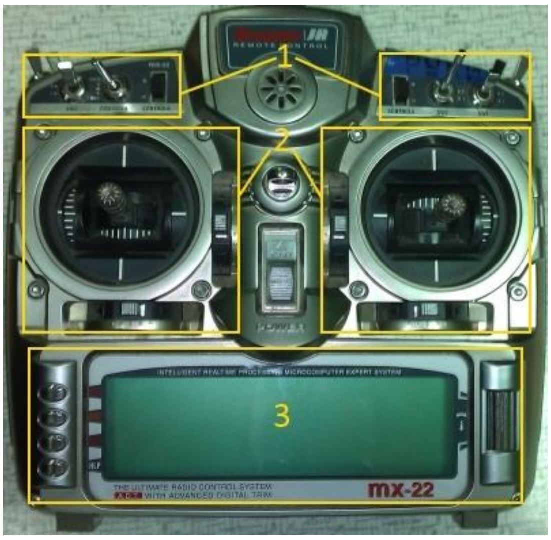

Fig. 3. UAV control unit

The appropriate research has been picked up for each group. For elements of groups 1 and 2 analysis of the location and configuration of control elements will be carried out. For group 3 analysis of data stream shown on display will be carried out. The analysis of operator's work scenarios can also be implemented. This analysis will be carried out for the scenario of vehicle's flying-off. The results will form group 4 of the research.

This system is classified as critical, so it requires a risk analysis.

Table 5 gives a fragment of functional safety research for UAV control unit. It shows cases for each group of the control unit.

Table 5 is a fragment of the table of the research into human-machine functional safety in terms of the analysis of operator's work scenarios.

For example, the following line of reasoning can be used for altitude measurer:

1. The altitude measurer is in the 3rd logical group. Therefore, data stream has to be analyzed.
2. Values displayed on the indicator of the measurer can be incorrect, therefore one of the key words CHANGE; NO; OTHER THAN; MORE or LESS has to be applied to the characteristic «Readings».
3. In case the readings of the altitude measurer are higher than actual ones, incorrect actions of the operator (drifting down or crash) are possible.
4. In this case, failure severity is high but the probability of it is low since it can be caused by the UAV altimeter sensor failure.

Conclusion

The task of choosing the profile of methods to ensure the completeness and reliability of safety assessment is further complicated by the fact that a great number of methods of various complexity. Risk assessment can be carried out to various levels of depth and detailing. One or more methods can be applied. The choice of methods has to base on their proved suitability.

The research work (study, thesis) the profile of methods for complex assessment at all stages of the life cycle has been grounded and the tool to automate assessment process has been proposed. This profile is based on HAZOP and FMEA methods but it is more adaptable and allows using of other methods.

The tool ensures techniques to be adaptable due to applying it to the domain area and special features of the interface. It has been made possible due to generating of the table model for risk analysis of every new research. In this way, the technique and the tool allow to increase reliability and completeness of functional safety assessment. The examples of using the method to assessment of critical systems are given.

References

1. Bishop, P. G. A Methodology for Safety Case Development [Text] / P. G. Bishop, R. E. Bloomfield // Industrial Perspectives of Safety-critical Systems : proceedings of the Sixth Safety-critical Systems Symposium. – Birmingham, 1998. – P. 194 – 203.

2. Case-assessment of critical program systems [Text]: monographs / V. Kharchenko, Y. Netkacheva, A. Orekhova, O. Tarasiuk, A. Gorbenko, V. Skliar, V. Brezhnev, Y. Babeshko, O. Illiashenko. – Kh. : National aerospace university named after N. Y. Zhukovski «KhAI», 2012. – 301 p.

3. Safety Case-Oriented Assessment of Critical Software: Several Principles and Elements of Techniques [Text] / A. Andrashov, V. Kharchenko, K. Netkachova, V. Sklyar, A. Siora // Monographs of System Dependability. Vol. 2. Dependability of Networks. – Wroclaw : Oficyna Wydawnicza Politechnki Wroclawskiej, 2010. – Chapter 1. – P. 11 – 25.

4. Orekhova, A. A. Safety case-oriented assessment of human-machine interface for NPP I&C system [Text] / A. A. Orekhova, V. S. Kharchenko, V. R. Tilinskiy // Reliability: Theory & Applications. – 2012. – Vol. 7, № 3 (26). – P. 27 – 38.

5. Orekhova, A. A. Information technology security evaluation of Human machine interfaces I&C systems [Text] / A. A. Orekhova // Information processing systems. – 2013. – Vol. 1 (108). – P. 267-271.

6. ISO/IEC 31010:2000 Risk management – Risk assessment techniques [Electronic resource] / ISO. – Access mode: http://www.iso.org/iso/home/store/catalogue_tc.htm. – 9.11.2015.

Table 5

Fragment of the research into UAV control unit

Group	Element	Element characteristic	Key word	Type of failure	Consequences of failure	Probability of failure	Failure importance
1	Ignition	Activity	CHANGE	Cutoff	Losing of height, crash	High	High
2	Flipper trimmer	Position	CHANGE	Lower controllability	Trouble control, losing of height, crash	High	High
3	Altitude measurer	Readings	MORE	Signal readings are higher than they are actually	Incorrect input of user, losing of height, crash	High	Low

7. Functional Safety of Electrical, Electronic, and Programmable Electronic Safety Related Systems, IEC 61508 [Electronic resource] / International Electrotechnical Commission. – 1998-2000. – Parts 1 to 7. – Access mode: http://www.iec.ch/functionalsafety. – 9.11.2015.

8. Fowkes, M. Recommended methodology for preliminary safety analysis of the HMI of an IVIS concept or design [Electronic resource] / M. Fowkes, D. D. Word, P. Jesty // HASTE Deliverable 4. – Access mode: http://www.its.leeds.ac.uk/projects/haste/downloads/Haste_D4.pdf. – 9.11.2015.

Поступила в редакцию 9.11.2015, рассмотрена на редколлегии 18.11.2015

ОЦІНКА БЕЗПЕКИ КРИТИЧНИХ СИСТЕМ НА ОСНОВІ КОМБІНУВАННЯ МЕТОДІВ РИЗИК-АНАЛІЗУ

А. О. Орєхова, В. С. Манулік,
Аль-Джахлаві Акрам Фаділ Кадім, Аль-Хафаджі Ахмед Валід

Дана робота присвячена проблемі оцінки функціональної безпеки критичних систем. У роботі було проаналізовано існуючі методики ризик-аналізу, а також розглянуто можливість їх застосування для оцінки функціональної безпеки критичних систем. Доведено можливість комплексування вибраних методик і здійснено їх об'єднання. У результаті було розроблено комплексну методику оцінки функціональної безпеки критичних систем. Розроблено інструментальний засіб, призначений для автоматизації методики. Методику та інструментальний засіб було випробувано на критичних системах.

Ключові слова: ризик-аналіз, безпека, критичні системи, оцінка, інструментальний засіб, HAZOP, FMEA.

ОЦЕНКА БЕЗОПАСНОСТИ КРИТИЧЕСКИХ СИСТЕМ НА ОСНОВЕ КОМБИНИРОВАНИЯ МЕТОДОВ РИСК-АНАЛИЗА

А. А. Орехова, В. С. Манулик,
Аль-Джахлави Акрам Фадил Кадим, Аль-Хафаджи Ахмед Валид

Данная работа посвящена проблеме оценки функциональной безопасности критических систем. В работе были проанализированы существующие методики риск-анализа, а также рассмотрена возможность их применения для оценки функциональной безопасности критических систем. Доказана возможность комплексирования выбранных методик и осуществлено их объединение. В результате была разработана комплексная методика оценки функциональной безопасности критических систем. Разработано инструментальное средство, предназначенное для автоматизации методики. Методика и инструментальное средство были испытаны на критических системах.

Ключевые слова: риск-анализ, безопасность, критические системы, оценка, инструментальное средство, HAZOP, FMEA.

Орехова Анастасия Александровна – канд. техн. наук, старший преподаватель каф. компьютерных систем и сетей, Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», г. Харьков, Украина, e-mail: nastya.orehova@rambler.ru.

Манулик Вячеслав Сергеевич – аспирант каф. компьютерных систем и сетей, Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», г. Харьков, Украина, e-mail: viacheslav.manulik@gmail.com.

Аль-Джахлави Акрам Фадил Кадим – магистр каф. компьютерных систем и сетей, Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», г. Харьков, Украина, e-mail: faakram@yahoo.com.

Аль-Хафаджи Ахмед Валид – аспирант каф. компьютерных систем и сетей, Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», г. Харьков, Украина, e-mail: eng_ahmed.waleed@yahoo.com.