Сформульовано задачі дослідження, запропонована теоретична і методологічна концепція визначення показників надійності і безпеки апаратного та програмного забезпечення (ПЗ) для систем управління технологічними процесами (АСУТП). Представлені аспекти сучасних підходів до вирішення науково-технічної проблеми щодо забезпечення необхідного рівня повноти безпеки (РПБ) технічних засобів АСУТП об'єктами підвищеної небезпеки. В результаті аналізу та вивчення нормативно-правової бази були запропоновані окремі методи визначення кількісних показників контролю безпеки. Визначення РПБ досліджуваної апаратної частини складової АСУТП пропонується здійснювати гібридними методами експертного аналізу. Пропонується проводити аналіз загроз і функціональності з використанням спеціальних протоколів, які показують зв'язки між можливими причинами відмови елементів джерела, їх впливом на функціонування системи управління і наслідками відмови на функцій системи. Розглянуто існуючі методи та запропоновано оригінальні методи визначення стандартизованих показників надійності при аналізі SIL (safety integrity level). Розглянуто проблеми забезпечення необхідного рівня SIL при розробці систем керування технологічними процесами. Існуючі моделі і методи визначення рівня повноти безпеки систем управління небезпечними об'єктами в повному обсязі відповідають сучасним вимогам до процедур сертифікації. Раціональними для оцінки ймовірності відмов апаратної частини є методи дерев відмов (FTA – fault tree analysis), що визначають ймовірність ініціюючих небезпечних подій і метод дерев подій (ETA – event tree analysis) для урахування відмов систем захисту і визначення сценаріїв наслідків таких відмов

Ключові слова: Safety integrity level, електронні програмовані пристрої, інформаційні технології

UDC 004.942: 052:056
DOI: 10.15587/1729-4061.2019.187716

CONSTRUCTION OF METHODS FOR ENSURING THE REQUIRED LEVEL OF SAFETY INTEGRITY IN THE AUTOMATED SYSTEMS OF CONTROL OVER TECHNOLOGICAL PROCESSES

V. Ivanov
PhD, Associate Professor*
E-mail: vetgen75@gmail.com
O. Baturin
Senior Lecturer*
E-mail: aibaturin1973@gmail.com
V. Lyfar
Doctor of Technical Sciences, Associate Professor*
E-mail: lyfarva61@gmail.com
S. Mytrokhin
PhD, Associate Professor*
E-mail: mytrokhin@snu.edu.ua
L. Lyhina
Senior Lecturer*
E-mail: kaf_mif@ukr.net
*Department of Programming and Mathematics
Volodymyr Dahl East Ukrainian National University
Tsentralnyi ave., 59-A, Severodonetsk, Ukraine, 93400

Received date 29.08.2019
Accepted date 03.12.2019
Published date 25.12.2019

1. Introduction

Prevention of major accidents in the operation of industrial sites of increased danger requires a balanced approach. This approach is based on the theoretically reasonable methods and the models for estimation of reliability level and classification of dangers of consequences for automated system of control of technological processes (ASCTP).

It is also necessary to implement a comprehensive information technology to support decision making to ensure the safety integrity level of the ASCTP. This is of considerable interest for developers and users of such systems at large industrial enterprises. These include: chemical and petrochemical plants, means of transporting dangerous cargoes and substances, railway complexes, facilities of power industry (nuclear and heat stations) and other sites of increased danger. The problem of determining and ensuring the required SIL level is paid little attention to in the scientific and technical area, since the analysis of accidents at large industrial sites often ends in conclusion about the causes of technological faults, external influences or human factors. Sometimes the causes of such accidents are a dangerous and undetected fault of the process control system, which results in an accident. However, these are poorly proved assumptions, especially in the context of increasing complexity and integration of technological processes. Negative scales and consequences of such accidents can significantly exceed the cost of development and implementation of the ASCTP. That is why it is very topical to determine the objective current SIL of the ASCTP elements, implemented in the production of increased danger. This is necessary to prevent technogenic catastrophes, as well as to support the processes of making optimal decisions on controlling the technological risk.

2. Literature review and problem statement

It is stated in paper [1] that the SIL concept was widely used in the models of industrial hazard prevention. However, in paper [2], it was generalized that the SIL is based on the probability-relying data. Research results [3] expand the previous statement on the fact that probabilistic data bring

in some uncertainty in a safety system. However, in view of the latest research [1], the assessment of safety integrity for determining quantitative risk indicators was not performed [4] to the full extent, as the advantage is given to qualitative information and its comprehensive analysis [1]. In this case, various methods and standards [5], such as Program Evaluation and Review Technique, Monte Carlo and others are used [1]. However, they are complicated for classical analytical approaches [6]. As a result, the issue of unbiased determining the quantitative risk indicators arises. The reason for this is often unknown functional purpose of input signals [6], because the systems are different and it is difficult to foresee a dangerous effect of a particular system and its relations to the types of negative effects [8]. In addition, the interpretation of the danger of a fault of automated control systems is also significantly complicated [9]. This is exactly what we can say about processing information by processors and generation of controlling signals [10]. Attempts are made to compensate the above by the use of available tools for analysis and modeling [11]. However, it is possible, when the automated control system is represented by a full closed circuit from sensors and measuring devices, the structure of receiving and processing the signals and giving controlling signals up to executive devices and mechanisms [7]. In this case it is possible to interpret and analyze the hazards of the consequences of system faults or information misrepresentation in it [12]. The implementation of some aspects of the above-mentioned with the use of the SIL analysis was proposed in article [13], but the emphasis was placed on functional security.

However, given the limitations on controlling actions of automated control systems of sites of increased hazard [14], it is necessary to pay attention to safety integrity. For example, using the mechanism introduced in the functional safety standard of the programmed systems of functional safety [15]. That is, there are unresolved issues that are directly related to the maximum precise determining of the reliability level of the ASCTP. All this makes it possible to argue that the problem of conducting the SIL analysis and estimation of the safety integrity level for the central parts of the developed ASCTP (Fig. 1) is relevant. The particular urgency in this issue is to establish the upper limit of the SIL, as well as to make a decision on the technologies of developing such systems.

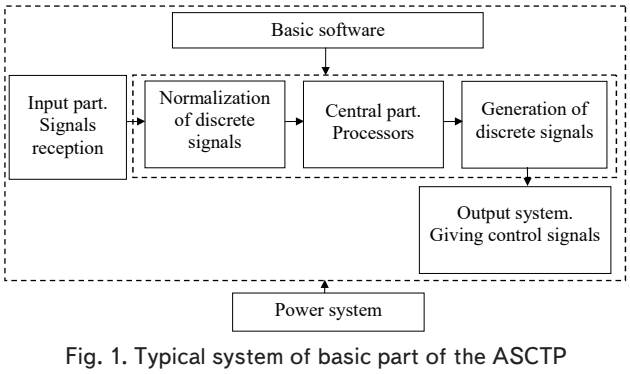

Fig. 1. Typical system of basic part of the ASCTP

In adopted standards, regulatory documents, safety protocols [15–20] and other sources, which are devoted to the problem of providing the necessary SIL, normative and other data, allowing determining the level of the ASCTP reliability mainly by the rank methods, were proved. It was shown that the overall approach to addressing the problems of determining the risk level of the ASCTP operation in most cases relies on qualitative, rather than quantitative assessment of reliability. Thus, the used rank methods involve the conclusions, such as "acceptable", "unacceptable", "inadmissible" and so on. However, the issues related to the objective and impartial approach to determining the quantitative indicators of risk remain unresolved. Developers of basic electronic, electrical, electronic programmable devices and software of the ASCTP have special difficulties. Since functional purposes of input signals, their information significance and correspondence to certain kinds of negative consequences in case of their distortion first are not known for the central electronic control part, the interpretation of the danger of such faults is considerably complicated. The same can be said regarding processing the information by processors and generation of control signals. The task is simplified in the case when the ASCTP is represented by a complete closed circuit from sensors and measuring devices, the structure of receiving and processing of signals and giving control signals up to executive devices and mechanisms. In this case, a more or less complete interpretation and analysis of the hazards of consequences of faults of a system or distortion of information in it is possible.

The estimation of the safety integrity level for hardware parts of the ASCTP is regulated in full in papers [15–18] and involves the FMEA (Fault modes and Effects analysis) as well as their being critical. According to the analysis results, one can determine the types of consequences of faults of the elements of the examined ASCTP units or its central part and qualitative indicators of fault probability are subsequently calculated using the methods for risk assessment.

The most complex part of solving the problem of the SIL assessment for the developed complexes is to identify the software reliability and security. There are also the known regulated methods [15–17] based mainly on rank estimates. The above-mentioned eliminates the probability of determining the software reliability level and represents large difficulty for developers of basic software (S). In addition, this approach does not make it possible to establish and reduce the amount of information on determining the software reliability. The same can be said regarding the development of the central parts of the ASCTP complexes.

The actual lack of methods accounting for the probability of faults of the interconnected software modules is a special problem in the area of determining software reliability [20]. However, logical and functional relations between separate software units significantly affect reliability and should be taken into consideration.

In articles [16, 17], there is an attempt to clarify the generalized approaches to determining the SIL and the application of the methods, described in the standards, to specific security systems. Such approaches are based on the methods of differentiated analysis of the causes and effects of faults of the FMEA (Fault modes and effects analysis) or the method, which takes into consideration their crucial character (FMECA). This supports the ALARP principle (As Low As Reasonable Practible) in order to reduce the risk of occurrence of hazards caused by faults to an acceptable magnitude. For example, papers [18, 19] clearly and in detail explain the approaches and the methods for determining quantitative indicators and qualitative characteristics. The criteria of selecting the components for using in distributed control systems

and special safety systems with different SIL levels, recommended in the IEC standards 61508 and 61511 were also considered. Practical examples of using such criteria were explored as well.

The greatest difficulty and uncertainty in this approach are caused by: determining and formalizing safety functions and establishing unambiguous relations between the significant types of faults of the elements of a control system and the impact of such faults on the scale of hazardous consequences [19].

However, the remaining unresolved issues include:

– a decrease in the volume of information processing to determine the quantitative indicators of software reliability;

– the lack of an established approach to researching the interaction of program formations.

The need to develop the methods for assessing the quantitative indicators of the reliability of software tools that provide functional, operational and technical safety of the ASCTP operation, is caused by the actual lack of such methods [23]. The great role in this case is played by the problem of harmonization of qualitative and quantitative criteria characterizing the security integrity level.

The safety integrity level reflects the degree of risk of operating the sites of critical area. In this sense, "risk" implies the occurrence of certain consequences with certain probability (or frequency for the assigned operation period). The problem of prevention of a technological risk of increased hazard sites, caused by the ASCTP faults, can be solved as a result of consecutive execution of the following actions [20, 21]:

1) analysis of occurrence and development of the processes of faults of the ASCTP elements and assessment of the probability of such events;

2) analysis of effects of examined faults and their attribution to a certain category (dangerous, safe, diagnosed, non-diagnosed, critical, non-critical, not affecting safety) based on the estimation of the scale of such consequences;

3) assessment of reliability of the ASCTP software (indicators of fault probability: PDFavg ($T1$) – Probability of Fault on Demand to perform the safety function within time $T1$; PFH – the average frequency Hazardous Fault Probability within an hour;

4) development of requirements for diagnosis and software verification methods for all life cycle stages;

5) analysis of the received indicators of reliability of software and hardware part of the ASCTP and decision making (recommendations) according to the technology of the ASCTP development based on comparative analysis of normative and current reliability indicators.

Two situations, for which the SIL can be analyzed and determined in order to certify the control system, are considered:

1. When developing the basic ASCTP complex without a specific attachment to the control object. In this case, it is necessary to determine the lower boundary of the SIL, which provides an integral safety level that is not worse than the declared level.

2. When creating an ASCTP with a full attachment to the control object and assessment of the risk caused by operational safety of the ASCTP. In this respect, functional and technical software safety refers to the internal component of the operational software safety.

Input data to determine the indicators of the ASCTP hardware reliability are reliability indicators (operation before a fault, passport information on the fault on demand and the operation period, etc.) of separate electrical, electronic, electronic programmed elements (E/E/PE). In the first case, such elements include only the physical elements of the basic ASCTP set (without measuring and executive devices). In the second case all the E/E/PE elements, including the sensors that transmit and executive devices, are analyzed. The tasks of the SIL assessment for these two situations also differ by the fact that in the first case, the concept of the "safe state" is set a priori. This is understood as a system fault or termination of its operability on condition of its full and unambiguous diagnosis of this condition and normal fault-free disconnection of the ASCTP. In this case, such faults or stops are considered safe. All faults of the ASCTP elements, leading to the distortion or termination of performance of the planned functions of a control system, are considered a priori dangerous. In the second case, the level of the threat of a fault of a control system element is established based on analysis of consequences of such a fault for functioning of the technological elements of the control object.

Fig. 2 shows the relations of different stages of creation of the functional safety system of the assigned level that meets the IEC standards.

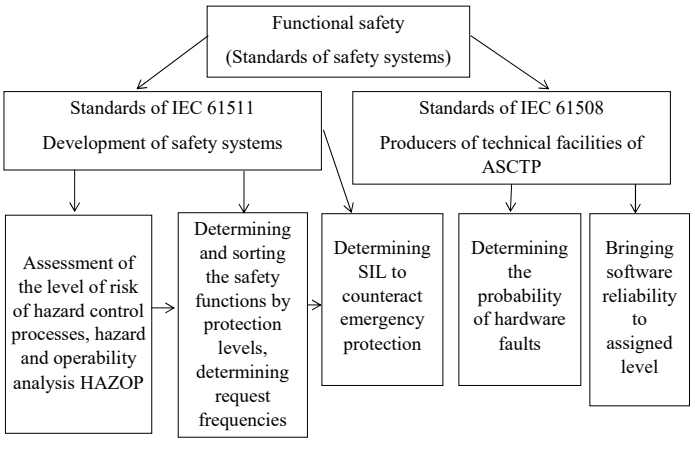

Fig. 2. Areas of application of the IEC standards to assess the ASCTP reliability

The most common methods are high-quality and semi-qualitative methods of risk ranking when assessing the current and required SIL. However, the apparent simplicity of the application of such methods is significantly leveled by their unreliability level.

The primary problem arises when using the HAZOP followed by the division of security functions. Hazard and operability analysis of safety systems is carried out by the methods of expert assessments and does not enable full separation of safety functional from the functions of dual-use features, such as those performing both technological and safety functions, or protection facilities. Formalization of cause-effect relations of faults of control systems and consequences of such faults without quantitative indicators of reliability and risk is largely not effective. In this regard, the development of techniques and models that combine HAZOP and FMEA with the possibility of formalization of cause-effect relations and the events caused by them, to the level of graphs or a fault tree and an event tree, is most promising. It is important to reach quantitative indicators of reliability and safety, rather than only rank estimates.

It is necessary to assess software safety at all stages of the life cycle: systemic analysis of a project, design, de-

velopment, testing, verification and validation, test trials, operation and maintenance, modification and creation of new version, withdrawal from operation. At all stages, any impacts may have consequences for security and change reliability indicators.

These circumstances contributed to the emergence of some techniques [23], which were researched and analyzed to identify the features of the presentation of reliability indicators:

1. Microsoft Solutions Framework (MSF) is a coherent set of concepts, patterns, and rules that ensure management of people and workflows when developing solutions. Software development is implemented by stages using the distributed control points ("waterfall"), and stages of development may be repeated ("spiral").

2. Rational Unified Process (RUP). The project is made in the form of a distributed WEB Knowledge Base using the means of search and separation of events. The methods ensure the distribution of roles and responsibilities in the programmers' team and are provided with tools to automate separate stages of creation.

3. Extreme Programming (XP). The methods are focused on improving the efficiency of cooperation of both programmers and directors and customers through the cycles of approvals and checks of regular parts of customer's requirements.

The main problems that occur when using these technologies and can lead to faults of software functioning are errors of programming and algorithmization. This can be eliminated in a sufficient degree by the methods of comprehensive testing, check and approval during software development and support.

The following types of testing were used in this case:

– module testing – for the groups of independent modules with closed functional integrity;

– integrative testing – takes into consideration functional relations between the groups of modules;

– systemic testing – checking the validity of the entire software package, performance compliance to critical load, user's errors, resilience to software and hardware faults.

Software verification and validation were stipulated by standards [21–23].

Stages of development of software protection systems include [25]:

– search and separation of software safety functions;

– determining the principles of software functioning safety;

– types and criteria of software faults;

– levels of software functioning safety;

– list of external and internal influences that pose a safety threat;

– resources required to ensure the SIL;

– formation and implementation of software protection systems.

The list was used in the study. However, it should be noted that the separation of categories of kinds of faults and their detection is a labor-intensive function and requires a high qualification and profound analysis of functional relations inside the safety system.

It is necessary to separate resources in compliance with the principles of redundancy both of memory resources, and the time for execution of the workflow elements. It is important to ensure:

– control of external data for compliance with the area of software determining and application;

– costs of on-line control of correctness of programs implementation and data translation;

– means of response to national security threats (traps);

– operational procedures for displaying the defect detection and computation

– recovery after faults.

In this case, the security systems integrated into the source code to compilation. However, this approach significantly complicates the code and verification procedures.

Safety means must counteract external and internal threats with a given reliability level that is more effective than it is assumed and claimed by the SIL. It should be borne in mind that complete elimination of any manifestations of such threats is impossible.

To implement the protection systems, it is usually necessary to form a team of specialists performing the functions of:

– a project security manager (leader), who is obliged to satisfy the customer's

requirements for the safety of the ASCPT facilities;

– architects of protection systems and development of basic specification of functional of program tools at critical solutions;

– specialists who develop the entire functional of protection components and relation of the details of functional (algorithmization) for correct creation of the source code and its verification;

– programmers, whose level corresponds to the selected code specification;

– specialists who would perform background verification and testing of a code;

– specialists who are able to develop the summary documents on the operation

of security systems in accordance with the standard requirements.

Software verification was carried out by various methods that were chosen at the initial stage of development.

One of the most common and inexpensive methods is the method of expert assessments. For example, Fagan Software inspection [26] is based on the use of a through technical control (brainstorming). Additionally, the methods of user's interface inspection and examination of the software architecture quality and protection can be used.

Application of static analysis of the source code and its architecture. However, this method causes significant difficulties in the use of control systems of critical importance due to the inability of direct translation of the code of such systems into generally accepted high-level languages, which limits the possibilities of automation of checking the components of functional software.

Formal and semi-formal methods for software verification are based on the development of requirements for logic-algebraic models and abstract models. Such models in some cases can be formalized to the logical level and ensure the development of instrumental means for the automated process of allowing a series of software verification tasks.

3. The aim and objectives of the study

The aim of this study is to develop models and methods for estimation of the safety integrity level of the ASCTP taking into consideration quantitative indicators of reliability of software and hardware of control systems.

To achieve the goal, the following tasks were set:

– to propose the methods for determining quantitative indicators of reliability of both hardware and software of ensuring the ASCTP functioning;

– to conduct verification and testing of the proposed methods and programmed means of their implementation.

4. Methods for determining the comprehensive estimate of risk and the SIL of the ASCTP

As a result of the conducted analysis and the study of the regulatory framework, a number of methods for determining quantitative SIL indicators based of stochastic indicators of reliability of discrete elements of the control system and qualitative indicators of the ASCTP software were presented. Of course, it is possible to determine the probability of accidental faults of hardware and software components based on stochastic indicators only. However, consideration of the logical cause and effect consequences of the events of fault development makes it possible to remove the problems arising from the use of general ranking methods [24].

It is proposed to determine the SIL of the explored hardware component of the ASCTP using hybrid methods of expert analysis taking into consideration cause and effect relations of fault and their consequences. It is proposed to implement the standard approach to determining the area of danger of the consequences of faults of separate hardware elements based on the hazard and operability analysis (HAZOP). Subsequently, to present the obtained results of the HAZOP in the format of automated methods for assessing the probability of such faults. This combination is possible due to special protocols.

The first protocol has the following interconnected data:

– faults of separate elements of the ASCTP (using program elements)® type of critical faults (detectable fault – Df, undetectable fault – Uf, safe fault – Sf, dangerous fault – Dnf)®type of consequences (safe, unsafe, consequence-free);

– response of protection system (or a dual-purpose system) to a fault® corresponding effect.

The elements of the first protocol are presented in the format that links the consequences in a "fault tree" (FTA) from the elementary faults through the tree branches to the "upper event". The reaction of the protection system is presented in the format of the fault development from the upper initiating event of the FTA through binary branching of the "event tree" to the end effects of faults. The second protocol should join the sets of upper events of the "fault tree" (FTA) with the set of initiating events of the "event tree" (ETA) through suractive display.

The hazard and operability analysis should be carried out using the protocols, which show cause and effect relations between the possible causes of faults of output elements, their impact on the operability of the control system and the consequences of the loss of system functions as a result of faults. The use of structured records of such cause-effect relations, arranged by the structured markup language (xml) tools, makes it possible to automate the process of creating a generalized mathematical model for the SIL rating. Such a model appears to be a tuple (graph) of reliability and safety level and can be formalized to the state of the fold/sweep of fault trees (FTA) and event trees (ETA). In this case, the elements of the software used in the ASCTP are also considered as the output (initiating) faults or events.

The authors performed research when setting the tasks, development of algorithms, verification and implementation of software decision support tools in assessing the risk of large industrial enterprises [24]. The software tools that make it possible to realize the relations of protocols and to determine the integrated level of the safe work of ASCTP were developed. The possibilities of the aforesaid protocol and reliability of the results of calculations of the automated FTA and ETA constructions based on logical relations of cause and effect connections of the analyzed ASCTP elements were verified. The use of logical operations AND (Prohibition), OR (Table 1) [27] for the descending method of fault trees sweeping allows determining the probability of critical (upper in a tree) events. To implement the Bernoulli formula for the elements, performing parallel functions, the operation "exclusive OR" (Table 1) was used. Binary branching of events that influence the protection facilities represented in event trees makes it possible to carry out quantitative estimation of probability of occurrence of negative consequences of faults of the ASCTP elements.

Table 1

Correspondence of formulas for determining the probabilities of logical operations

AND ($\wedge$)	OR ($\vee$)	Exclusive OR ($\oplus$)
$P_e = \prod_{i=1}^{n} P_i$	$P_e = 1 - \prod_{i=1}^{n} (1 - P_i)$	$P_e = \sum_{i=1}^{n} P_i$

Software tools (example is shown in Fig. 3) of the support of the automated process of the FTA and ETA formation, based on using the Protocol of HAZOP analysis fully carry out the functional of the project of quantitative assessment of the SIL indicators. They make it possible to separate and sort the combination of faults that affect the level of critical consequences in terms of their significance, which makes it possible to optimize the decisions made.

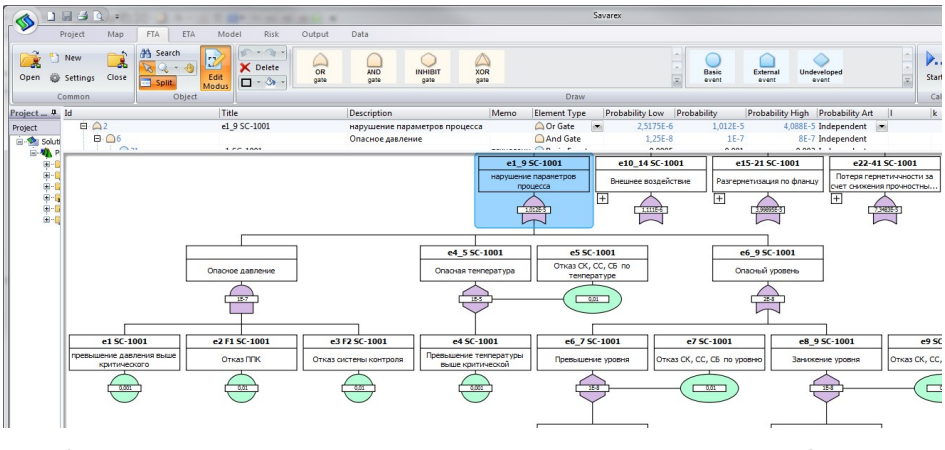

Fig. 3. Example of automatic sweep of a fault tree from the graph of the HAZOP protocol

Autonomous testing of software modules of basic parts of the ASCTP sites of increased hazard sites can be performed based on the abstract syntactic constructions of a tree form.

For structural analysis of the system using the FMEA, the following procedure is proposed:

1. Analysis boundaries are determined. To do this, it is necessary to select the output functions of a system or a unit, which are natural objective functions of a device or a unit, and a fault of which is considered a fault of a device or a unit. The upper limit of analysis is the main output functions of a device (typical for the purpose of a device). The lower limit of analysis is the faults of the functions of elemental base of devices or units and modules, the probability (frequency) of functions fault of which is known or computed as a result of previously conducted analysis.

2. Defragmentation of the circuit and parts of a device is performed based on analysis of cause and effect relations of input and output functions. The causes and effects of operation of the units of a module (device) in the structure of performance of functions by them are recorded. It is recommended to do this in a "top-down" way – from the original main function, for a fault of which the value of probability is determined going down with the use of logical signs and construction of a fault tree (FTA).

3. The structural analysis of performing the functions of fault detection and system protection is conducted. The relations of the second protocol are recorded and the effects of fault of protection systems are detected. This is the base of sweeping the event trees (ETA).

All the results of the FMEA are recorded in the data representation format developed by the authors of software, which makes it possible to unite in one project the model of functioning safety level of the studied ASCTP.

Thus, the general hybrid model is implemented, which simulates the faults of certain independent elements of the system and effects of such faults according to the logic of functional relations constructed in the FTA and ETA.

5. Verification and testing of the proposed methods and program means of their implementation

To prove the above, it is possible to present some results of verification and testing of the proposed method using the example of determining the reliability of the unit of the discrete signal normalizer ND–41.

The objective function of this module is normalization of discrete signals coming at the input (16 channels) and processed by frames, the formation of which occurs from the external side of the module.

1. The output part (unit) is shown in Fig. 4.

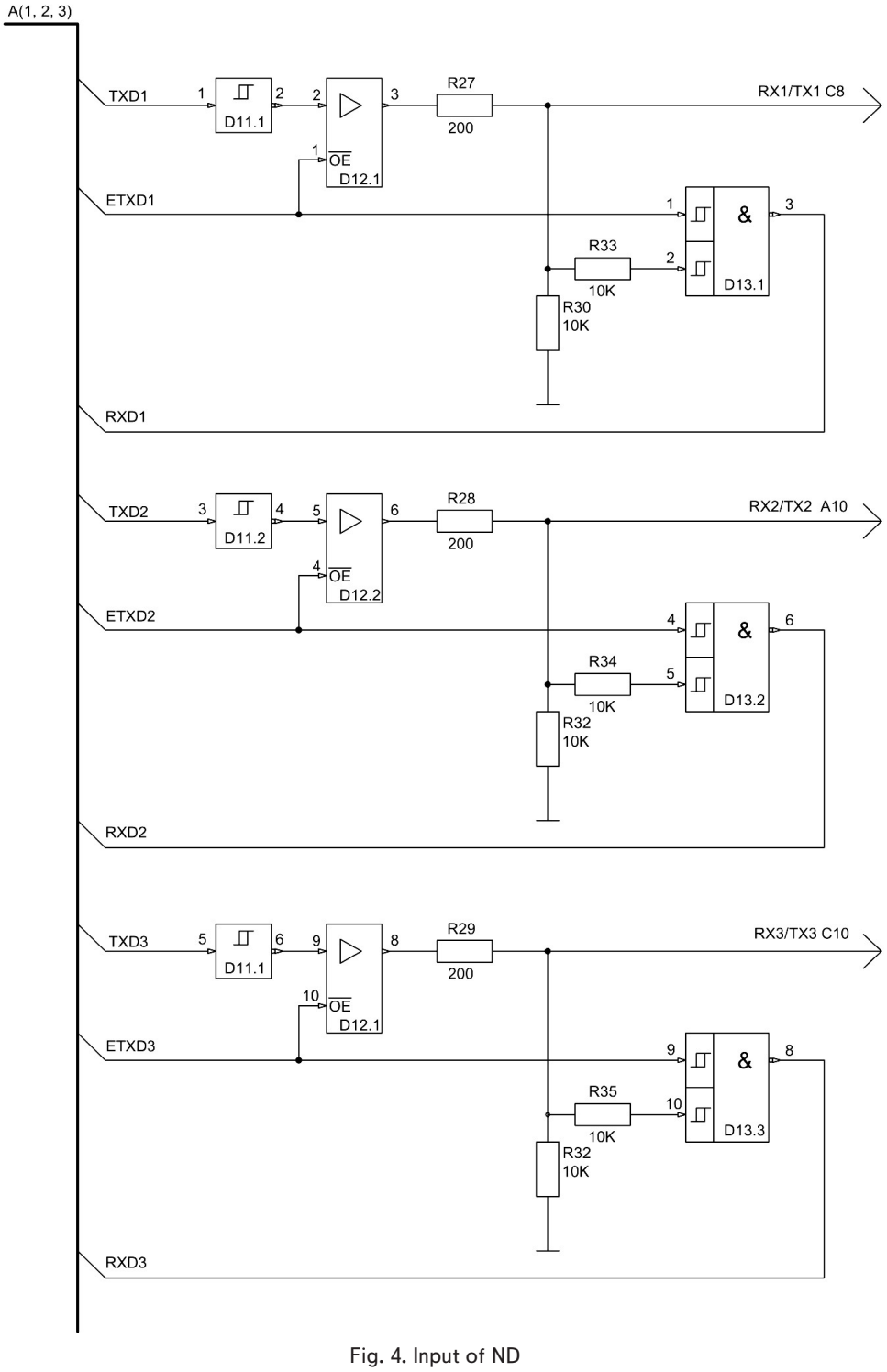

Fig. 4. Input of ND

A fault of any of the three selected channels leads to error normalization and to the fault of function No. 1. In this regard, fault No. 2 corresponds to a fault of three identical channels, united by the logical sign OR (Fig. 7).

2. The probability of a fault of the microprocessor STM32F103 was obtained from the given indicators of the device reliability and makes up PFH=$8{\cdot}10^{-10}$/h.

3. A fault of the microprocessor functions is possible due to a fault of its strapping (function of running and operability ensuring).

The processor circuit is shown in Fig. 5.

A fault of any element is assumed dangerous DnF and detectable DF.

4. Module is powered from an external source +24 A. The structural diagram is shown in Fig. 6.

A power fault is possible at a fault of any independent elements except for the case of a fault of any from V1 or R4 OR V2 or R5 (not less than 1 from 2 channels). This mechanism is revealed for demonstration in a fault tree.

The summing fault tree for computation of PFH was developed in software application of the FTA (Fig. 7).

We obtain PFH=7.49e−4, which corresponds to SIL 2.

The resulting reliability level for the ND−41 is not better than SIL 2. Any analysis of the software for the specified module will not increase the specified characteristic.

The comparative result proves that module ND-41 has worse indicators than those determined by the rank methods. For this module, it is necessary to make a decision to improve its reliability to the SIL 3. In the discussion below, there are only the possibilities of the FTA method, but this is only because it satisfies this type of module. It is similarly possible to apply the ETA methods [24].

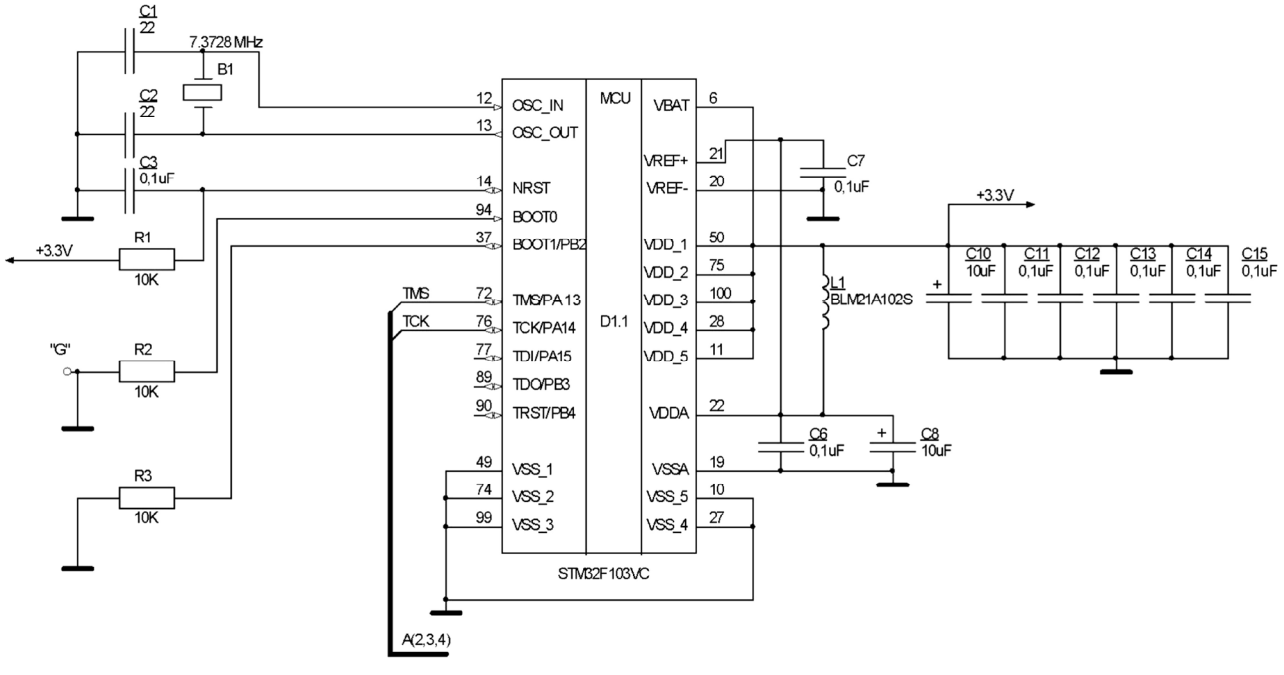

Fig. 5. Processor circuit

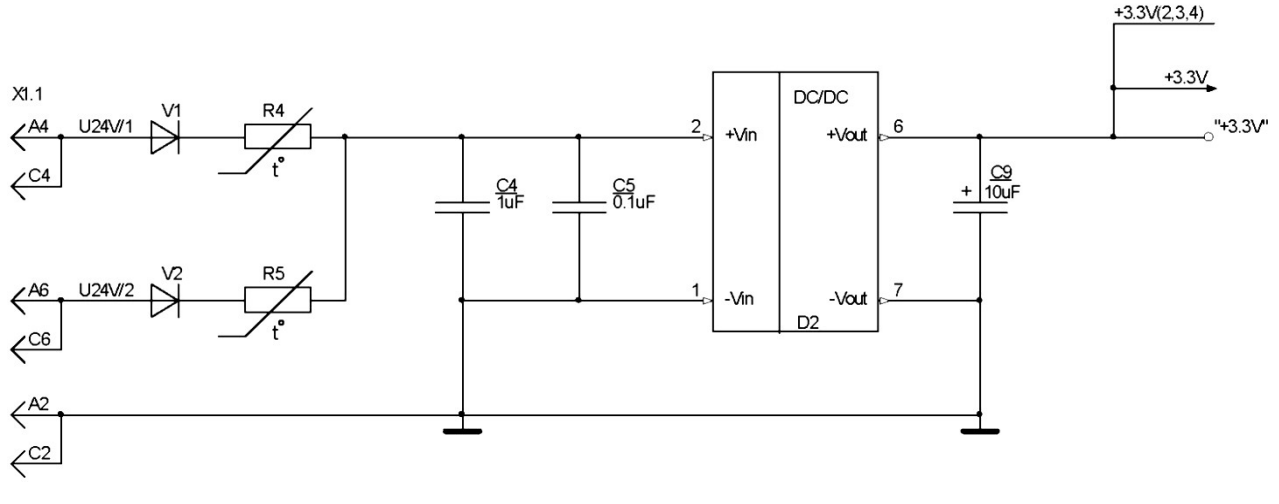

Fig. 6. Structural diagram of power model

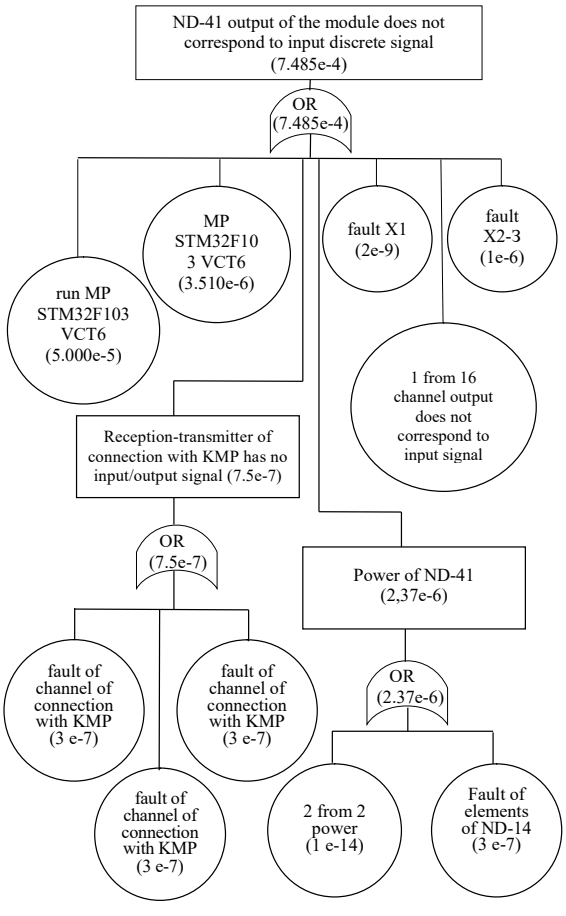

Fig. 7. Summary fault tree for calculation of PFH

6. Discussion of results of studying the methods for ensuring the required level of safety integrity

Taking into consideration that the concept of SIL is based on probabilistic data [2] with a certain share of uncertainty [3], the regulated methods are used to determine the risk [15–18]. However, qualitative indices are analyzed in this case [6]. Quantitative indicators are beyond attention [7], unlike the approach referred to in [24] and detailed in this paper.

In contrast to [1], the SIL assessment is performed when solving the problems of risk determining. During testing in the framework of this work, it was performed for separate modules MSKU–4, in particular, for the normalizer of discrete signals ND-41. And if we leave generalizations [2], the use of the normalized rank methods [15–18] for ND-41 at the 2oo3 architecture will give the indicators of fault-free operation at SIL 3. And it is this result that raises doubts about the use of the methods and approaches [9]. That is why the authors performed the risk assessment by the hybrid methods of combination of HAZOP, FTA, ETA, proposed in this research.

The above was tested, verified and implemented at the scientific-production association "Impulse" producing control complexes of MCKU–4.

During the application of the methods for ensuring the required safety integrity level of automated control systems, the developers have performed consultations on certification for SIL 3 level of the MCKU–4. In addition, the obligatory part of such study included the analysis of standard requirements. This allowed separating the structure and the composition of points and methods for studying the reliability and functionality indicators. As a result, this complex of works enabled analyzing the functionality and assessing the risk of the hardware of the MCKU-4 devices.

According to [20], the method for analysis of the types and consequences of faults was applied based on the logical structural analysis of devices and units.

As a result, the FMEA was applied at different levels of the system decomposition – from the highest level of the system (system in general) to the functions of separate components or software orders.

The FMEA is constantly repeated and updated, because the design of the system is changed and improved in the process of development. Design changes require the introduction of changes to the corresponding parts of the FMEA.

7. Conclusions

1. The methods for determining the quantitative indicators of the SIL criteria, which take into consideration the objective relations of reliability of hardware and software means of the ASCTP, were proposed. The problem is solved by using the sweep of the space of the state of the ASCTP elements to a fault tree (FTA) and event trees (ETA) and their subsequent uniting in the cause and effect mechanism of occurrence and development of faults. This provides an objective approach in comparison with the rank methods and the possibility to search for the most critical emergency combinations of the FTA and ETA branches.

2. The developed program tools for sweeping the graph of the states of controlling complexes, which were explored to the level of uniting the FTA and ETA branches, were tested using the example of the complex MCKU–4. Verification and approbation of the proposed methods and program tools were carried out. The results of verification and approbation proved the possibility to determine the safety indicators of both separate elements of control systems and of the complex in general.

References

1. Ouazraoui, N., Nait-Said, R. (2019). An alternative approach to safety integrity level determination: results from a case study. International Journal of Quality & Reliability Management, 36 (10), 1784–1803. doi: https://doi.org/10.1108/ijqrm-02-2019-0065
2. Ouazraoui, N., Boura reche, M., Nait-Said, R. (2015). Fuzzy modelling of uncertain data in the layers of protection analysis. 2015 International Conference on Industrial Engineering and Operations Management (IEOM). doi: https://doi.org/10.1109/ieom.2015.7093769
3. Ouazraoui, N., Nait-Said, R., Boura reche, M., Sellami, I. (2013). Layers of protection analysis in the framework of possibility theory. Journal of Hazardous Materials, 262, 168–178. doi: https://doi.org/10.1016/j.jhazmat.2013.08.042
4. Nait-Said, R., Zidani, F., Ouzraoui, N. (2009). Modified risk graph method using fuzzy rule-based approach. Journal of Hazardous Materials, 164 (2-3), 651–658. doi: https://doi.org/10.1016/j.jhazmat.2008.08.086

5. Zhao, X., Malasse, O., Buchheit, G. (2019). Verification of safety integrity level of high demand system based on Stochastic Petri Nets and Monte Carlo Simulation. Reliability Engineering & System Safety, 184, 258–265. doi: https://doi.org/10.1016/j.ress.2018.02.004
6. Calixto, E. (2016). Gas and oil reliability engineering: modeling and analysis. Gulf Professional Publishing, 808.
7. Smith, D. J. (2017). Reliability, maintainability and risk: practical methods for engineers. Butterworth-Heinemann, 478.
8. Ahn, J., Noh, Y., Joung, T., Lim, Y., Kim, J., Seo, Y., Chang, D. (2019). Safety integrity level (SIL) determination for a maritime fuel cell system as electric propulsion in accordance with IEC 61511. International Journal of Hydrogen Energy, 44 (5), 3185–3194. doi: https://doi.org/10.1016/j.ijhydene.2018.12.065
9. Musyafa', A., Nuzula, Z. F., Asy'ari, M. K. (2019). Hazop evaluation and safety integrity level (SIL) analysis on steam system in ammonia plant Petrokimia Gresik Ltd. AIP Conference Proceedings. doi: https://doi.org/10.1063/1.5095281
10. Lee, B. C., Lee, H. S., Rhim, J. K. (2018). A Study on Safety Integrity Improvement of Oxidation Reactor on Propylene Oxide Process by Installed Safety Instrumented System (SIS). Advances in Intelligent Systems and Computing, 244–255. doi: https://doi.org/10.1007/978-3-319-94391-6_23
11. Simon, C., Mechri, W., Capizzi, G. (2019). Assessment of Safety Integrity Level by simulation of Dynamic Bayesian Networks considering test duration. Journal of Loss Prevention in the Process Industries, 57, 101–113. doi: https://doi.org/10.1016/j.jlp.2018.11.002
12. S. K. Kim, Y. S. Kim (2018). An Optimal Design Procedure based on the Safety Integrity Level for Safety-related Systems. KSII Transactions on Internet and Information Systems, 12 (12), 6079–6097. doi: https://doi.org/10.3837/tiis.2018.12.025
13. Śliwiński, M. (2018). Safety integrity level verification for safety-related functions with security aspects. Process Safety and Environmental Protection, 118, 79–92. doi: https://doi.org/10.1016/j.psep.2018.06.016
14. Morillo, J. L., Zéphyr, L., Pérez, J. F., Lindsay Anderson, C., Cadena, Á. (2020). Risk-averse stochastic dual dynamic programming approach for the operation of a hydro-dominated power system in the presence of wind uncertainty. International Journal of Electrical Power & Energy Systems, 115, 105469. doi: https://doi.org/10.1016/j.ijepes.2019.105469
15. Funktsional'naya bezopasnost' sistem elektricheskih, elektronnyh, programmiruemyh elektronnyh, svyazannyh s bezopasnost'yu. Ch. 1. Obshchie trebovaniya: natsional'nyy standart Rossiyskoy Federatsii GOST R MEK 61508-1-2007 (2008). Federal'noe agentstvo po tehnicheskomu regulirovaniyu i metrologii. Moscow: Standartinform, V, 44.
16. Funktsional'naya bezopasnost' sistem elektricheskih, elektronnyh, programmiruemyh elektronnyh, svyazannyh s bezopasnost'yu. Ch. 2. Trebovaniya k sistemam: natsional'nyy standart Rossiyskoy Federatsii GOST R MEK 61508-2-2007 (2008). Federal'noe agentstvo po tehnicheskomu regulirovaniyu i metrologii. Moscow: Standartinform, V, 58.
17. Funktsional'naya bezopasnost' sistem elektricheskih, elektronnyh, programmiruemyh elektronnyh, svyazannyh s bezopasnost'yu. Ch. 3. Trebovaniya k programmnomu obespecheniyu: natsional'nyy standart Rossiyskoy Federatsii GOST R MEK 61508-3-2012 (2014). Federal'noe agentstvo po tehnicheskomu regulirovaniyu i metrologii. Moscow: Standartinform, V, 97.
18. Funktsional'naya bezopasnost' sistem elektricheskih, elektronnyh, programmiruemyh elektronnyh, svyazannyh s bezopasnost'yu CH. 6. Rukovodstvo po primeneniyu GOST R MEK 61508-2-2007 i GOST R MEK 61508-3-2007: natsional'nyy standart Rossiyskoy Federatsii GOST R MEK 61508-6-2007 (2008). Federal'noe agentstvo po tehnicheskomu regulirovaniyu i metrologii. Moscow: Standartinform, V, 62.
19. Funktsional'naya bezopasnost' v nepreryvnyh proizvodstvah. Rukovodstvo po bezopasnosti protsessov. Natsional'nyy standart Rossiyskoy Federatsii GOST R MEK 61511-1-2011 (2013). Federal'noe agentstvo po tehnicheskomu regulirovaniyu i metrologii. Moscow: Standartinform, V, 66.
20. Functional safety guidelines for safety related systems and other applications with SIL2, SIL3 level in accordance with IEC 61508 and IEC 61511. GM International Technology for safety (2013). Villasanta, 77.
21. 610.12-1990 - IEEE Standard glossary of software engineering terminology. doi: https://doi.org/10.1109/ieeestd.1990.101064
22. 1012-2004 - IEEE Standard for Software Verification and Validation. doi: https://doi.org/10.1109/ieeestd.2005.96278
23. ISO/IEC 12207:2008 Systems and software engineering – Software life cycle processes.
24. Lyfar', V. A., Safonova, S. A., Ivanov, V. G. (2015). Development of optimization method of the repair work taking into account the risk indicators. Technology audit and production reserves, 2 (2 (22)), 11–17. doi: https://doi.org/10.15587/2312-8372.2015.40768
25. Nair, S., Jetley, R., Nair, A., Hauck-Stattelmann, S. (2015). A static code analysis tool for control system software. 2015 IEEE 22nd International Conference on Software Analysis, Evolution, and Reengineering (SANER). doi: https://doi.org/10.1109/saner.2015.7081856
26. Fagan, M. E. (1976). Design and code inspections to reduce errors in program development. IBM Systems Journal, 15 (3), 182–211. doi: https://doi.org/10.1147/sj.153.0182
27. Henli, E. Dzh., Kumamoto, H. (1984). Nadezhnost' tehnicheskih sistem i otsenka riska. Moscow: Mashinostroenie, 528.