Ensuring the safety and reliability of automated manufacturing processes of hazardous industries

Ensuring the safety and reliability of automated manufacturing processes of hazardous industries

I V Kovalev[1,2,3,4], P A Kusnetsov[2], V V Losev[2], M V Saramud[1,2], A A Voroshilova[4] and A S Andronov[5]

[1]Siberian Federal University, 79, Svobodny pr., Krasnoyarsk, 660041, Russia
[2]Reshetnev Siberian State University of Science and Technology, 31, Krasnoyarsky Rabochy Av., Krasnoyarsk, 660037, Russia
[3]Krasnoyarsk State Agrarian University, 90, Mira pr., Krasnoyarsk, 660049, Russia
[4]Krasnoyarsk Science and Technology City Hall of the Russian Union of Scientific and Engineering Association, 61, Uritskogo Str., Krasnoyarsk, 660049, Russia
[5]Krasnoyarsk complex aviation rescue center EMERCOM of Russia, 12D, Malinovskogo Str., Krasnoyarsk, 660133, Russia

E-mail: forubox@yandex.ru

Abstract. The paper describes one of the approaches to solving the problem of ensuring the reliability of automated manufacturing system of hazardous chemical plants using various hazardous chemicals in the production processes. Exposure to these substances can be harmful to personnel and infrastructure. Our goal is to create an automated manufacturing system that ensures not only fault-free operation, but also the safety of automated manufacturing systems of hazardous chemical plants. Depending on the type and specifics of the hazardous production, the automated manufacturing system should have a certain integral level of safety. We have developed a method for analyzing system reliability, taking into account many reliability indicators. The proposed method, considering the target probability of failure-free operation of the entire system and the probability of failure-free operation of the hazardous module required for the desired integral level of safety, determines the target probability of failure-free operation of all the system modules. It also provides for the inclusion of not only functional modules into the system, but also modules that block failures and dangerous effects. The paper considers an example of chemical production, however, the proposed method is applicable to a wide range of technological processes of hazardous industries.

1. Introduction

Nowadays, there is a rapid development of technical systems, in particular of the automated manufacturing systems (AMS). The use of such systems can significantly increase the productivity of technological industries and their effectiveness. Besides, the degree of effectiveness of automated systems depends on the parameters and indicators of TP ACS [1,2,3].

One of the most significant factors affecting management effectiveness is reliability. Reliability is an indicator including many parameters. There is a whole set of principles for maintaining reliability at the proper level. System failure analysis is a traditional approach used to control reliability. But in practice, other indicators, such as safety, determine the reliability of AMS. Development of both safe and reliable systems is urgent. It is required by modern standards of system reliability, such as IEC

61508 / IEC 61511 [4,5].

According to this standard, system safety is assessed through the safety integrity level (SIL) [6,7].

For many years, technically complex and hazardous industries have been continuously used around the world. Technology is being improved, however, there remains a high risk of technological accidents, the consequence of which is serious damage to the environment. At the same time, environmental standards themselves are being tightened. Thus, there is a need to increase the reliability of AMS in order to increase the reliability of the functioning of technological processes.

An example of technological processes that are subject to increased reliability requirements are chemical production processes (see figure 1).

Hazardous chemicals are often used in such processes, which, due to equipment failure, can have harmful effects on personnel and infrastructure [8,1,9].

When calculating the reliability, the serviceability of the means that regulate and control the operating parameters should be taken into account. Automation tools are functionally connected with equipment carrying out the technological process.

To develop safe and failure-free systems, it is necessary to analyze the relevant reliability indicators at various stages of development. Currently existing solutions [10] are not able to do this. Therefore, there is a need to create a method for analysing the reliability of AMS, taking into account a set of reliability indicators, such as the danger and importance of failure. In order to eliminate this drawback, the authors propose establishing target criteria, an increase in which will determine the reliability of the formed system structure. It is also necessary to ensure that the analysis of systems takes into account various principles of ensuring safety and reliability.

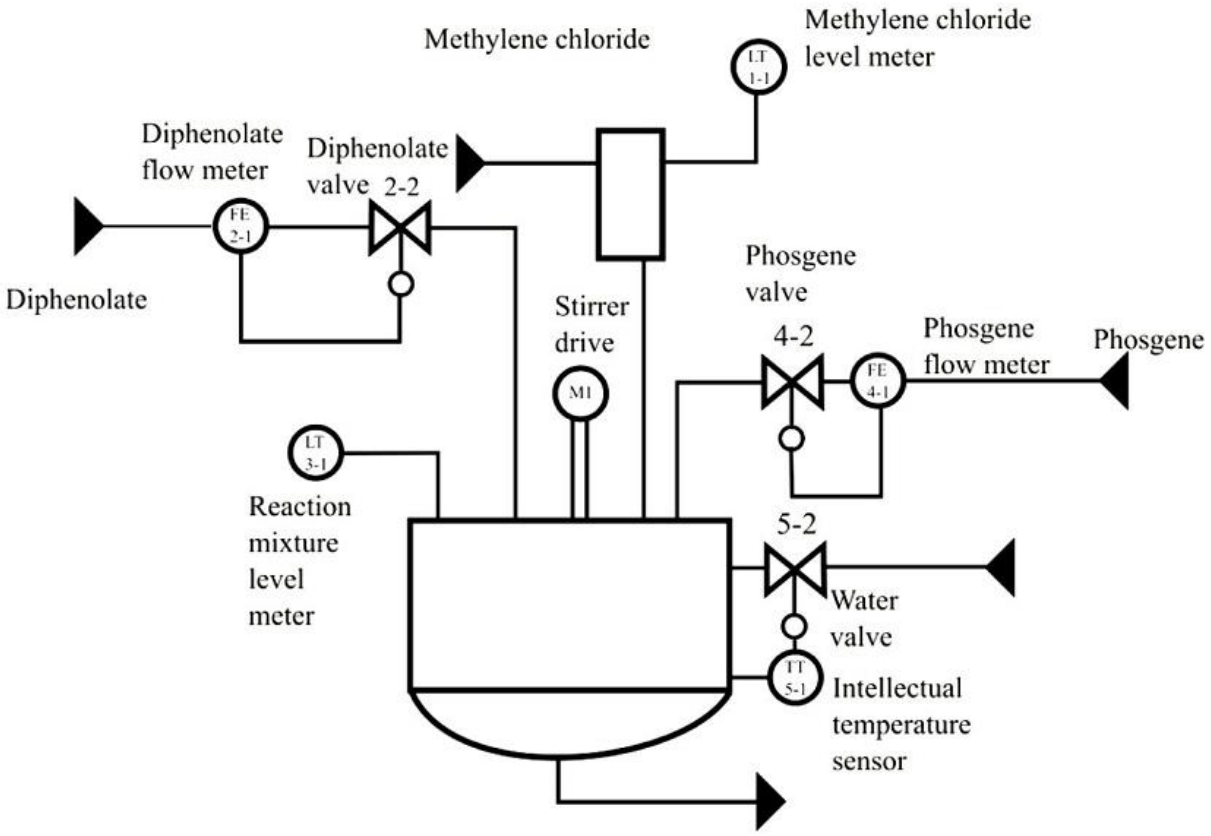

Figure 1. Block diagram of AMS polycarbonate production site.

2. Technological process of hazardous production

The control system under consideration will be AMS of the polycarbonate production process [11]. Polycarbonate production technology using chemical hazardous substances (CHS), in particular phosgene, is typical [12,13].

A simplified diagram of the technological section is described as follows (figure 1). An aqueous solution of sodium diphenolate continuously enters the reactor of the cascade of reactors. Methylene chloride from the tank and phosgene is also supplied here. The consumption of sodium diphenolate is stable. It is measured by the FE 2-1 meter and controlled by the valve (2-2).

Phosgene consumption is also stable. Its flow rate is measured by the flow meter (FE 4-1) to measure gas flow. Phosgene consumption is controlled by the valve (4-2), made in a special design for the regulation of hazardous substances.

The methylene chloride level in the tank is controlled by the flow meter (LT 1-1). The reaction mixture is stirred in a reactor by the stirrer drive (M1). The temperature in the reactor is stabilized, the reaction mixture is heated with hot water. The temperature of the mixture is measured by the sensor (TT 5-1), the water flow is regulated by the valve (5-2). The level of the reaction mixture in the reactor is controlled by the level meter (LT 3-1).

Measuring information from the process is transmitted to the ET200m data acquisition bus. The inclusion of a data bus into the ACS provides additional potential for redundancy of the upper level of the system. Assuming devices from a Simatic range as automation devices of a high level, we select the number (and type) of modules. The data acquisition and control bus ET200m is composed of an IM interface module, a PS power module, and I/O modules.

Thus, the considered example is a typical one of chemically hazardous production, since it includes all the minimum necessary components characterizing the technological process.

3. Solution methods

To solve the problem of improving reliability, there are various structural methods. They are based on the introduction of backup elements. Such methods may include the method of full duplication, the method of optimized reservation, and the method of accounting for reliability indicators proposed by the authors [14,10].

3.1. Basic methods

This article discusses the full duplication method and the optimized backup method as the basic ones. The first one which is the method of complete duplication, involves the inclusion of a backup element in each functional module. It is the least time-consuming one in terms of design costs, but at the same time it is ineffective in terms of reliability indicators, since it does not take into account the reliability indicators inherent in each of the modules of a particular system.

The optimized backup method involves solving the problem of optimizing the reliability indicators of the designed AMS taking into account the reliability of all elements of the system. This task of optimizing redundancy is solved effectively using the method of steepest descent.

So, a certain set of resources is allocated for the construction of a redundant system. It is required to determine the structure of the system that delivers the extremum of the objective function *P(t)* and ensures the successful solution of all the tasks posed to the system with probabilities not lower than the given constraints, while the costs should not exceed the specified boundary.

The objective function *P(t)* is expressed as the product of the probabilities of failure-free operation of all its modules.

$$P(t) = \prod_{i-1}^{n} P_i(t), p(t) \rightarrow max \quad (1)$$

where *P(t)* – probability of the system failure-free operation;
$P_i(t)$ – probability of the i-th module failure-free operation;
t – system uptime.

The limiting degree of redundancy is the reserve of resources allocated for the construction of the

system:

$$L_i \geq \sum_{j=1}^{n} R_{i,j} \quad (2)$$

where L_i – reserve of the i-th resource allocated for the construction of the system;
$R_{i,j}$ – the amount of the i-th resource expended on the j-th module;
i – number of resource types;
j – number of modules in the system.

Thus, having the objective function and limitations, we proceed to the formation of the optimal composition of the redundant system. It should be noted that in the case of a series connection of system elements, the largest increment in the total reliability ensures redundancy of the most unreliable module.

3.2. Suggested method

Increasing system fail-free operation is done by iteratively adding a backup element to the module with the least likelihood of uptime.

$$Ra_i = \frac{1}{P_i(t)} \quad (3)$$

Then there is the number of the module for which this function is maximum, and a backup element is added to this module. Next is the next iteration.

Function (3) will be called the direction selection function or priority function.

The proposed method of accounting for reliability indicators will primarily differ from the previously considered methods by a different priority function.

First, the AMS under consideration should be divided into subsystems that perform various functions and highlight the main functions among them, in order to further ensure a higher priority of redundancy for modules that perform these functions.

To meet the requirements of system safety, it must be ensured that it achieves indicators that correspond to those specified by SIL. Such indicators are SFF and the probability of hazardous failures.

The SFF - safe failure fraction ratio is introduced by IEC 61508/61511. It determines what proportion of all system failures is occupied by hazardous failures. It is selected on the basis of the safety integral level necessary for the system, which is determined during the formation of requirements for AMS. Moreover, the failure of a module operating with hazardous energies or chemicals will be considered a hazardous failure.

Also, when forming requirements, the target probability of failure-free operation of the main function P and the system service life t are selected.

Based on these parameters, the intensity of hazardous failures and the intensity of safe failures are determined:

$$\lambda = \frac{-\ln(\mathrm{P})}{\mathrm{t}} \quad (4)$$

$$\lambda = \lambda_{\mathrm{s}} + \lambda_{\mathrm{d}} \quad (5)$$

where λ_s – safe failure rate,
λ_d –dangerous failure rate:

$$\lambda_s = \lambda \cdot \mathrm{SFF} \quad (6)$$

$$\lambda_d = \lambda \cdot (1 - \mathrm{SFF}) \quad (7)$$

Using λ_s and λ_d target probabilities of hazardous and safe failures are found:

$$P_{fdt} = 1 - e^{-\lambda_{\mathrm{d}}\mathrm{t}} \quad (8)$$

$$P_{fst} = 1 - e^{-\lambda_{\mathrm{s}}\mathrm{t}} \quad (9)$$

Thus we will find the target probabilities of failure-free operation of each module with safe failures:

$$P_{fst} = 1 - \prod_{i=1}^{n} P_{sti} \quad (10)$$

$$P_{sti} = \sqrt[n]{1 - P_{fst}} \quad (11)$$

And with hazardous failures:

$$P_{fdt} = 1 - \prod_{i=1}^{n} P_{dti} \quad (12)$$

$$P_{dti} = \sqrt[n]{1 - P_{fdt}} \quad (13)$$

Among modules with safe failures, hazard grading is not performed, thus, the coefficient for each safe module will be:

$$K_i = P_{sti} \quad (14)$$

Hazard grading is carried out among modules with hazardous failures. Depending on the nature of the hazardous exposure, *C* value is selected to quantify the hazard.

Then, the M_i value is found, which is the ratio of the quantity that quantifies hazard to its critical value, multiplied by the probability of a hazardous failure.

In the case of hazardous chemicals, such a value, for example, can serve as an average lethal concentration.

$$M_i = \frac{C_i}{CCK_i} \cdot P_{fdti} \quad (15)$$

$$P_{fdti}=1-P_{dti} \quad (16)$$

where C_i – concentration arising in the air of the working area during a hazardous failure in the *i-th* module,
CCK_i – average lethal concentration,
P_{fdti} – failure probability.

This value is found for each functional module with a hazardous failure, and then its M_{avg} average value is determined. Then, at constant *c* and *CCK*, it is determined what P_{dtib} should be to achieve this average $\underline{M_{avg}}$.

$$P_{fdti} = M_{avg} \cdot \frac{CCK_i}{C_i} \quad (17)$$

$$P_{dtib}=1-P_{fdti} \quad (18)$$

Achievement of an equal value of M_{avg} by all modules ensures an equal distribution of damage across all modules. In case a hazardous failure occurs in the module

$$K_i=P_{dtib} \quad (19)$$

$$K_{dei}=1 \quad (20)$$

If a hazardous failure occurs in the element

$$K_i=P_{dti} \quad (21)$$

$$K_{dei}=P_{dtib} \quad (22)$$

The operation of the algorithm is not limited only to the consideration of dangers.

The following mechanism is proposed for switching on modules that block failures or danger, the so-called blocking modules (BM). There are many *T* types of functional modules identified during decomposition. Their classification is based on the substances and energies they use. Each type of module has its own blocking failure or danger module.

$$T_i \leftrightarrow Bf_i \tag{23}$$

$$T_i \leftrightarrow Bd_i \tag{24}$$

where *T* is the set of module types, *Bf* is the set of failure-blocking modules, *Bd* is the set of hazard-blocking modules, i is the *BM* type number.

$$T_i = j \rightarrow \mathrm{Bf_i} = \mathrm{j} \tag{25}$$

where *j* is module type number.

Then, for each functional module, its type is determined and a blocking module of the corresponding type is assigned.

$$M_i \leftrightarrow T_i \leftrightarrow Bf_i \tag{26}$$

$$M_i \leftrightarrow T_i \leftrightarrow Bd_i \tag{27}$$

where *i* is module number.

Each module blocking a failure has a certain set of characteristics of reliability, the consumption of resources for implementation, and the formula according to which the probability of failure is reduced.

Based on the probability of failure of the blocking module, the formula for calculating the reliability of each module will have the following form

$$P = (1 - (1 - P_2) \times (1 - P_b)) \times P_c \tag{28}$$

where P is the probability of module failure-free operation after blocking;
P_2 is probability of failure-free operation without blocking;
P_b is probability of blocking;
P_c is probability of blocking module failure-free operation.

As a result, the priority function (3) for the method of accounting for reliability indicators takes the following form

$$Ra_i = (K_{dei} \cdot K_i) / (P_i) \tag{29}$$

where i is the number of the module which priority is being calculated;
K_i is the priority coefficient depending on the importance and danger of the module failure;
P_i is the probability of the module failure;
K_{dei} is the priority coefficient depending on the danger of the module element failure.

Thus, the mathematical apparatus of a new method for acounting reliability indicators in redundancy is proposed, which allows creating a structure of AMS with high reliability, take into account the requirements of safety standards and the influence of risk reduction mechanisms and failure probabilities.

4. Results and discussion

This section presents the results of the implementation of the proposed method for the process considered in the article (figure 1).

With a complete duplication of all the modules of AMS, a system is obtained with a probability of failure-free operation of the main function of 0.89, and the entire system – of 0.87.

Using the optimized backup method without taking into account safety and blocking failures gives the probability of failure-free operation of the main function 0.916, and the entire system – of 0.91.

We will show that the use of the authors' method of accounting for reliability indicators gives the best results. Below is a step-by-step diagram of the method implementation and the results obtained.

The first step in the application of the method is to choose the target probability P=0.99 and the service life t=5 years for the AMS considered. Based on the service life, you can get the probability of failure-free operation of each module, which will serve as the initial data for the calculation.

Then, we will choose SIL for the system equal to 3. The SFF for this level will be 0.9, and the probability of the hazardous failure is 0.989.

Determining the dangers, valves for regulating the flow of sodium diphenolate and phosgene are detected. Their average-lethal concentrations are given in [15].

The next step is to partition the system into functions.

Controlled parameters are the level of methylene chloride in tank and the level of reactants in the reactor.

Adjustable parameters are phosgene consumption, sodium diphenolate consumption, and reactor temperature 2.

The functions performed by the system will be the function of obtaining the reaction mixture and the level control function in tank 1 and reactor 2.

Depressurization of the diphenolate valve can lead to spillage of the substance and its effects on personnel. Depressurization of the phosgene valve will also lead to exposure of personnel.

To assess the danger of a given failure, it is necessary to know the value of the average lethal concentration of substances (ALCS) in the air in the case of phosgene and the value the average lethal concentration in the case of diphenolate. In the case of phosgene, ALCS is 334 mg/m^3, in the case of diphenolate it is 427 mg/kg. The calculated probability of failure-free operation of modules with hazardous failures is 0.99 for a diphenolate flow control valve and 0.999 for a phosgene flow control valve. Having identified the dangers, it is necessary to use the mechanism for switching on the blocking dangers and module failures. To enable hazard-blocking modules, it is necessary to determine the type of modules with hazardous failures.

Phosgene flow control module is a valve that regulates gas flow. Therefore, the module uses hazardous gas. To protect against gaseous chemical hazardous substances, personal respiratory protection is used. Failure blocking modules are selected based on the energies used by the functional modules.

Modules that use 220-volt electrical energy are powered from uninterruptible power supplies, which serve as blocking failure modules, as they prevent unnecessary on-off cycles and power surges.

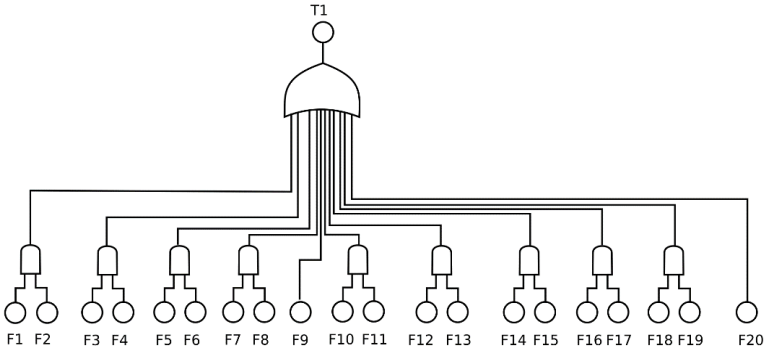

Figure 2. The tree of whole AMS failure.

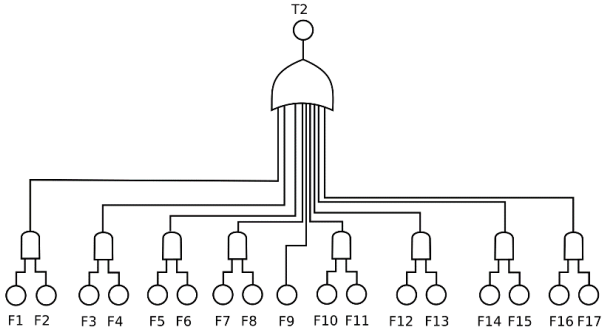

Figure 3. The tree of AMS control function failure.

Iteratively calculating the priority function and adding redundant elements to the system structure, we will build the reliability structure of the automatic process control system presented in figures 2 and 3 in the form of a failure tree. Table 1 shows the decoding of the failure tree nodes.

Table 1. Designation of events presented in the failure tree.

Event designation	Explanation
F1	Failure of the main diphenolate flow meter
F2	Failure of diphenolate backup flow meter
F3	Diphenolate main valve failure
F4	Diphenolate backup valve failure
F5	Failure of the main data acquisition bus
F6	Failure of the backup data acquisition bus
F7	Main controller failure
F8	Backup controller failure
F9	Phosgene flow meter failure
F10	Phosgene main valve failure
F11	Phosgene backup valve failure
F12	Failure of the main thermal converter
F13	Failure of the backup thermal converter
F14	Failure of the main coolant valve
F15	Failure of the backup coolant valve
F16	Main drive failure
F17	Backup drive failure
F18	Failure of the main methylene chloride level meter
F19	Failure of the backup methylene chloride level meter
F20	Reaction level gauge failure
T1	Whole AMS failure
T2	Failure of AMS control function

In the form of a logical expression, the structure of TP ACS will be presented as follows:

$$T1 = (F1 \vee F2) \wedge (F1 \vee F2) \wedge (F3 \vee F4) \wedge (F5 \vee F6) \wedge (F7 \vee F8) \wedge F9 \wedge (F10 \vee F11) \wedge (F12 \vee F13) \wedge (F14 \vee F15) \wedge (F16 \vee F17) \wedge (F18 \vee F19) \wedge F20$$

$$T2 = (F1 \vee F2) \wedge (F1 \vee F2) \wedge (F3 \vee F4) \wedge (F5 \vee F6) \wedge (F7 \vee F8) \wedge F9 \wedge (F10 \vee F11) \wedge (F12 \vee F13) \wedge (F14 \vee F15) \wedge (F16 \vee F17)$$

Hazardous failure modules or phosgene and diphenolate flow control valves will have a failure probability sufficient to achieve the desired SIL. Their overall likelihood of uptime will also provide the required failure-free fraction. Comparison of the full duplication method, optimized reservation using the fastest descent and the authors' method of accounting for reliability indicators gives the following results (table 2).

Table 2. Probability of system serviceability.

Probability of serviceability	Full duplication method	Method of optimized backup	Method of accounting for reliability indicators
AMS for the production of polycarbonate	0.87	0.91	0.94
AMS control function	0.89	0.916	0.96

The increment in the probability of serviceability depending on the iteration number is shown in Figures 4 and 5.

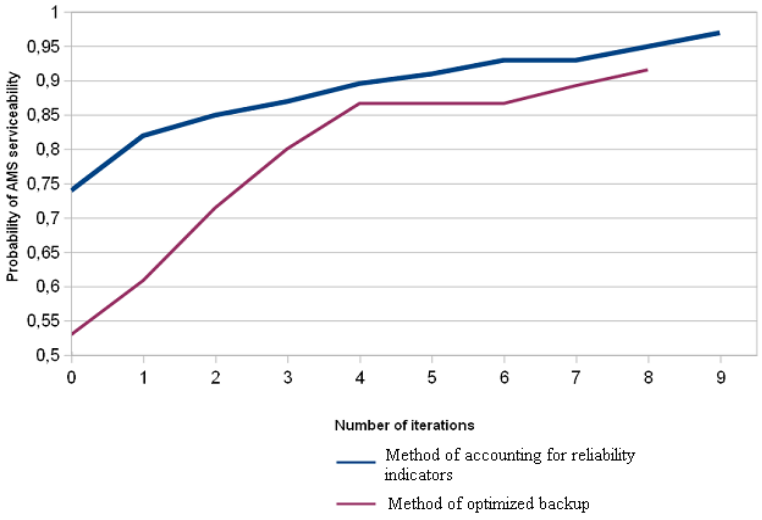

Figure 4. The graph of increasing AMS serviceability.

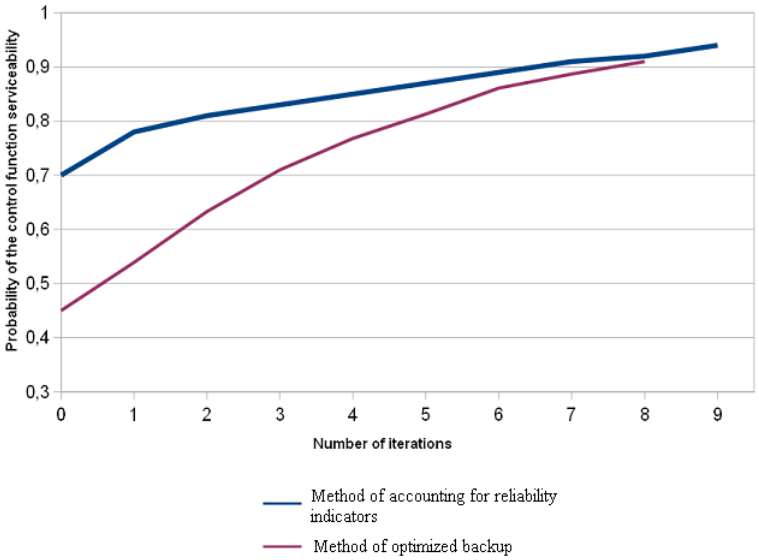

Figure 5. The graph of increasing AMS control function serviceability.

We would like to note that the graphs start from different points in the absence of redundancy due to an increase in the probability of safe operation of elements due to blocking modules. The graph of the system failure probability built using the optimized backup method ends earlier due to the fact that resources when building a system using this method end earlier.

The presented figures illustrate that the proposed method of accounting for reliability indicators allows increasing the reliability and safety of industrial control systems by reducing the probability of hazardous failures and achieve the required SIL for the system.

5. Conclusion

The method proposed in the article is based on taking into account reliability indicators specific to AMS. It allows ensuring not only high reliability, but also the level of reliability required by the IEC 61508/IEC 61511 standard, which is especially critical for hazardous industries.

The results presented in the article illustrate the effectiveness of the developed method and its applicability to the analysis and increase of reliability indicators of industrial control systems. The article considers an example of chemical production, however, the proposed method is applicable to a wide range of technological processes of hazardous industries.

The advantage of the method is that it includes not only the application of the principles of redundancy, but also other structural principles. The method allows using not only mathematical calculations, but also expert knowledge, accumulating and processing them, which opens up further prospects for the development of the proposed approach.

References

[1] Bozek A, Anhalt J and Chin J 2015 The use of infrared emission detection and fugitive emission quantification technologies as a basis for hazardous area classification design *IEEE Transactions on Industry Applications*. 51. 142-7. doi:10.1109/TIA.2014.2348075

[2] Faldella E, Paoli A, Tilli A, Sartini M and Guidi D 2009 Architectural design patterns for logic control of manufacturing systems: The generalized device *XXII International Symposium on Information, Communication and Automation Technologies* doi: 10.1109/ICAT.2009.5348451

[3] Tynchenko V S, Murygin A V, Emilova O A, Bocharov A N and Laptenok V D 2016 The automated system for technological process of spacecraft's waveguide paths soldering *IOP Conference Series: Materials Science and Engineering* **155(1)** 11

[4] Bell R 1999 IEC 61508: Functional safety of electrical/electronic/programme electronic safety-related systems: Overview *Computing and Control Engineering* **11(1)** 5/1-5/5

[5] Gall H 2008 Functional safety iec 61508 /iec 61511 the impact to certification and the user *Proceedings of the 2008 IEEE/ACS International Conference on Computer Systems and Applications, ser. AICCSA '08. Washington, DC, USA: IEEE Computer Society* 1027-31 doi:10.1109/AICCSA.2008.4493673

[6] Lee Y and Kim J 2009 A verification of fault tree for safety integrity level evaluation *ICCAS-SICE 2009 - ICROS-SICE International Joint Conference 2009, Proceedings*

[7] Rástočný K and Ždánsky J 2014 Influence of redundancy on safety integrity of SRCS with safety PLC *10.1109/ELEKTRO.2014.6848947*:508-12

[8] Abramov D G, Kodolov A V, Litvinov A V and Popov F A 2015 Performance evaluation of reliability growth of APCS protection functions at potentially hazardous production *2015 International Siberian Conference on Control and Communications (SIBCON)* **1(4)** doi: 10.1109/SIBCON.2015.7146969

[9] Ilonen J, Kamarainen J K, Kalviainen H and Anttalainen O 2002 Automatic detection and recognition of hazardous chemical agents *Digital Signal Processing, 2002. DSP 2002. 2002 14th International Conference* **2** 1345-8

[10] Kohlik M, Borecky J and Kubatova H 2012 Miscellaneous Types of Partial Duplication Modifications for Availability Improvements *Proceedings - 15th Euromicro Conference on*

Digital System Design, DSD 2012:79-83. doi:10.1109/DSD.2012.86
[11] Kuznetsov E V, Prokhorova I P and Fayzullina D A 1976 *Album of technical schemes for the production of polymers and plastics based on them (*Moscow: USSR, Khimia publ)
[12] Rodriguez F, Cohen C, Archer L and Ober C 2003 *Principles of Polymer Systems* (New York, London: Taylor & Francis)
[13] Zingel T G 2003 Chemical automated manufacturing systems (Krasnoyarsk: Siberian state technological university publ)
[14] Gaitanis N, Kostarakis P and Paschalis A 1995 Totally Self Checking reconfigurable duplication system with separate internal fault indication *4th Asian Test Symposium (ATS '95), November 23-24*: 316-21
[15] Diller W F 1978 *Medical phosgene problems and their possible solution.* J Occup Med *20*:189-93