The paper describes the peculiarities of multiple indicators of reliability of automated control systems. Along with the dependability considered an indicator such as the dangers of system failure. Showing particular account of the reliability of the automated control systems when considering their versatility. We study methods of lowering the probability of dangerous failure. Such method could be the reallocation of resources needed for inclusion of backup elements from module carrying a low danger to modules, carrying high-dangerous failures. Another method is identification of least important functions and transfer resources, needed for inclusion of backup from them to most important and dangerous modules, and preventing threats by blocking modules.

I Introduction

This paper describes the peculiarities of analysis of indicators of reliability for automated control systems (ACS). Reliability of technical systems is one of the most important indicators.

Each ACS includes variety of different elements, executing various functions. Moreover, one element may perform several functions, and, conversely, a single function may be performed by several elements.[1,2]

Reliability of the system is its possibility to keep all of the parameter, qualifying possibility of executing all of the functions in determined range in process of time [3].

There is a variety of different reliability-related indices, for example fault-tolerance, safety, efficiency etc. [4, 5]. In a modern reliability theory fault-tolerance is traditionally accepted as primary reliability parameter. Fault-tolerance usually means the amount of failed elements at the same time which would lead to the failure of the system as a whole. The more elements that are required for the failure of a system, the more fault-tolerant this system is [6].

One of the ways to improve it is redundancy. In redundant systems elements categorized by a role to main and backup. Main elements are the elements of the object, which failure in a case of absence of backup cause failure of the system. Backup elements are the elements purposed to keep system intact in a case of main element failure [7].

II Methods of infallibility increase

The research was done with the financial support of the Ministry of Education and Science of the Russian Federation in accordance with the agreement № 14.574.21.0041, unique identifier RFMEFI57414X0041
There is various method of composing reliable systems, based on stochastic or
determined principles. Main idea of those methods is solving the optimization problem -
maximization of the objective function subject to constraints.

Reliability indices presented by a list of values. Infallibility is the probability of lack
of failure for a certain period of time.

A typical objective function is a function of entire system infallibility, which is
expressed as the product of all modules infallibility.

\[ P = \prod_{i=1}^{N} P_i \]

\( P_i \) – probability of faultless functioning of module \( i \)
\( N \) – number of modules.

Infallible structure is composed by iterative procedure of adding in system modules
with lowest infallibility rate [8].

Function, computing the priority of reservation

\[ Ra_i = \frac{1}{P_i} \]

III Alternative reliability indices

But the conception of maximization of infallibility has certain disadvantages. It should
be considered that with any probability of failure-free operation remains opposite probability -
the probability of failure. Even if arbitrarily large incensement of reliability, we can not rule
out system failure, as this process is probabilistic. [9,10]

Also, any ACS is composed by physical modules, operating physical matter and
energy of technological processes. And in a case of failure correct operation of matter and
energy interrupts. There is an emergency situation that may be dangerous for the personnel
and infrastructure.

Dangerous failures could be appear in modules. System, composed by modules, having
high possibility of absence of failure, anyway could be highly dangerous. Because of that we
need to purposely lowering possibility of failure of highly dangerous modules.

To operating the conception of danger we need to have quantity measure of it. For
eexample, there is a measure by class of danger of chemicals in a case of chemical dangers and
by energy for energetic[11].

IV Redistribution of resources for backup

Considering dangerous failures, it is necessary to further increase the probability of
failure-free operation for the modules highly hazardous failures. One way is to redistribute
resources spent on redundant modules with less dangerous modules to more dangerous. We
should change the priority of the backup priority function.

\[ Ra_i = \frac{D_i}{P_i} \]
Di is danger of failure of module i.

But even the simple redistribution is lowering the possibility of dangerous failure, at
the same time it could increase possibility of system failure.

Possible way to solve this dilemma is to change the objective function of the system.

Automated control systems are multifunctional. ASC generally have one main purpose,
which could be divided into sub-tasks, performed by certain functions of the system. Each
function plays determined role in completing of the system purpose. Some of the functions
take more, and some - less participation in the system. The failure of an individual component
leads to the inoperability of that component and potentially other components, but it does not
lead to the inoperability of the whole system. [12, 13].

Thus, we can, for the sake of improving the safety of the system to announce some
functions less important and to redistribute resources from the modules of these functions into
modules with dangerous failures. We should determine which sequence of elements is
performs which functional task. This procedure of the separation of the existing system into
subsystems, components, called decomposition. Decomposition as dissection process allows
considering any system being studied as a complex consisting of separate interconnected
subsystems, which in turn, can be subdivided into parts. In decomposition each
dismemberment has its own level.

Base system is located on level zero. After its decomposition we get first level systems.
Decomposition of them results second level subsystems etc.

After functional decomposition we should to compute and appoint importance of the
modules executing functions. Total probability of failure could be raised, but probability of
main function of the system failure will not be affected. Also, probability of dangerous failure
will be lowered because of the redistribution of resources from less important functions.

V Blocking modules

But in addition to reducing the probability of failure there are direct ways to reduce the
danger caused by failure - the inclusion of specific modules, blocking harmful effects before
they impact on staff or infrastructure [14]. Such modules may simply discourage dangerous
influences to cause harm, and actively eliminate them. An example of blocking modules,
preventing the effects is individual and collective protective equipment.

Protective equipment - the means used by workers to prevent or reduce the impact of
harmful and hazardous production factors, depending on the purpose protective equipment is
divided into classes:

Means of normalization ambient air of industrial premises and workplaces, means of
protection of high-level ionizing radiation, means of protection from high electric and
magnetic fields etc [15].

And the example of the danger of liquidating modules can be modules neutralizing
emergency chemically hazardous substances. The neutralization of poisonous substances -
action aimed at the destruction of the toxic properties of substances, based on the chemical
conversion of poisonous substances into non-toxic products

The need to include these modules is determined by the safety requirements, and they
includes before the redundant functional modules.

Conclusion

Thus, we conclude that the need for the construction of automated control systems
complement the principles of redundancy by other principles. This will take into account the
full reliability indices. It is necessary to separate the modules which make up the system of importance. This allows you to optimally allocate resources to reserve the most important and dangerous failure of modules. You must also take into account the flow of resources into units to ensure the safety of the system. Review of the operation of these modules in the design phase allows you to specify the consumption of resources on the system and its safety.

References.
[1] GOST 24.701-86  Edinaya sistema standartov avtomatizirovannykh sistem upravleniya. Nadezhnost’ avtomatizirovannykh sistem upravleniya. Osnovnye polozheniya Unified system of computer control systems standards. The reliability of automated control systems. Fundamentals (In Russ.) Moscow. Standards publ.. 11 p.

[2] Kuznetsov P A, Beschastnaya N A, Bakhmareva K K, Antamoshkin O A, Antamoshkin A N 2012 Modification of the Volkovich’s-Michelev’s method to optimize costs in the synthesis of fault-tolerant information systems Vestnik SibGAU 6(46) pp. 97-100 (In Russ.)

[3] Kurochkin Yu A, Smirnov A S, Stepanov V A 1993 Nadezhnost’ i diagnostirovanie tsifrovых ustroystv i sistem Reliability and diagnostics of digital systems (St.Petersburg. St.Petersburg University Publ.) 320 p.

[4] Kovalev I V et al 2015 Model of the reliability analysis of the distributed computer systems with architecture "client-server" IOP Conf. Ser.: Mater. Sci. Eng. 70 012009 doi:10.1088/1757-899X/70/1/012009

[5] Kovalev I et al 2015 The efficiency analysis of the automated plants IOP Conf. Ser.: Mater. Sci. Eng. 70 012007 doi:10.1088/1757-899X/70/1/012007

[6] Kovalev I V et al 2015 The control of developing a structure of a catastrophe-resistant system of information processing and control IOP Conf. Ser.: Mater. Sci. Eng. 70 012008 doi:10.1088/1757-899X/70/1/012008

[7] Kucher V Ya Osnovy tekhnicheskoy diagnostiki i teorii nadezhnosti: Pis’mennye lektssii Fundamentals of technical diagnostics and reliability theory: Lecture (In Russ.) Available at: http://window.edu.ru/resource/967/24967 (accessed 3.05.2015)

[8] Sugak E V, Vasilenko N V 2000 Nadezhnost’ tekhnicheskih sistem. Uchebnoe posobie dlya vyssikh uchebnykh zavedeniy Reliability of technical systems. Study guide (Krasnoyarsk. NII SUVPT Publ.) 608 p.

[9] Ryabinin I A 2007 Nadezhnost’ i bezopasnost’ strukturno-slozhnykh sistem Reliability and safety of structural complex systems (St.Petersburg. St.Petersburg University Publ.) 276 p.

[10] Okhtilev M Yu, Sokolov B V 2006 Intellektual’nye tekhnologii monitoringa i upravleniya strukturny dinamikoy slozhnykh tekhnicheshikh ob’ektov Intelligent technologies for monitoring and management of the structural dynamics of complex technical objects (Moscow, Science Publ.) 410p.

[11] Akimov V A, Lapin V L, Popov V M, Puchkov V A, Tomakov V I, Faleev M I 2002 Nadezhnost’ tekhnicheskikh sistem i tekhnogennyy risk. Uchebnoe posobie Reliability of technical systems and technogenic risk (Moscow. Delovoy ekspres publ.) 368 p.

[12] Kuznetsov P A 2015 Dependent failures in multifunctional systems Vestnik SibGAU 1(57) pp. 86-91.

[13] Kovalev I et al 2015 The minimization of inter-module interface for the achievement of reliability of multi-version software IOP Conf. Ser.: Mater. Sci. Eng. 70 012006 doi:10.1088/1757-899X/70/1/012006
[14] Kovalev I V, Kuznetsov P A, Zelenkov P V, Shaydurov V V, Bakhmareva K K 2013 To the question of the reliability of automated control systems with blocking protection modules *Pribory* 6 pp.20-24 (In Russ.)

[15] Rossiyskaya entsiklopediya po okhrane truda *Russian encyclopedia of labor protection* (Moscow. NC ENAS Publ.) 2007