IOP Conference Series: Materials Science and Engineering

Dependent failure in multifunctional automatic control systems

Dependent failure in multifunctional automatic control systems

A S Degtyarev[1], **V I Usakov**[1,5], **P A Kuznetsov**[3], **I V Kovalev**[2,3,4] **and M V Karaseva**[2,3]

[1] JSC "Central Construction Bureau “Geofizika”, 89 Kirenskogo street, Krasnoyarsk, Russia
[2] Siberian federal university, 79 Svobodny avenue, Krasnoyarsk, 660041, Russia
[3] Reshetnev Siberian State University of Science and Technology, 31, Krasnoyarsky Rabochy Av., Krasnoyarsk, 660037, Russia
[4] Krasnoyarsk Science and Technology City Hall of the Russian Union of Scientific and Engineering Associations, 61 Uritskogo street, Krasnoyarsk, 660049, Russia

[5] E-mail: usakovvl@mail.ru

Abstract. The paper considers the components interference of the automated control system. The safety and survivability are investigated. The failure gradation is given. The failure consequences of components and modules of the system that cause failures of other components and modules, the capabilities to prevent these failures are considered. Some probable variants of the dependent failures are provided. It is shown that a possible source of danger can be both module failure and failure of redundant components in these modules. It is assumed that at least the potential danger is not reduced to zero due to the increase in the number of redundant components. The various logical structures of the compound components in the automated control systems (ACS) for spacecraft are discussed. A typical structure of reliability of the automated control system that performs several functions, i.e. a tree structure is presented. The process of failures development in multifunction systems, the mutual influence of components in case of simple linear and branching redundant structures are illustrated. The negative effects of redundancy are considered. An example of the reliability calculation of the system with a parallel connection of the components and their dependent failures caused by these components are given. The conclusion about the necessity of non-redundant methods for improving the reliability and dangerous impact prevention is made.

1. Introduction

The reliability of the automated data collection and control systems is one of the most important indicators. The success of any technical system functioning depends on the correct operation of these systems. The association the Institute of Electrical and Electronics Engineers (IEEE) defines the reliability as "the ability of the system or component to perform the required functions under certain conditions over a certain period of time" [1-2].

The reliability means the property of the system to remain operational for a certain time under normal conditions. The survivability is the ability of any technical object, construction, device or system to perform its basic functions despite the received damage. As the concepts of malfunction and damage are indistinct, their concretization led to the choice of two subsets of their states: "big" failure;

it means a fault, "permissible" failure; it means a defect. The testability level of the defect is defined as the probability of detecting a fault at a randomly selected output [3].

The safety is the ability of the system not to enter a dangerous state, into a state with the "large scale" damage. The capacity of very complex, multiple combinations of failures, each of them is incredibly small, and the number of such incredible states is enough to make the system in a dangerous state is typical for complex systems [4]. It may be the release of energy or materials causing harm to surrounding objects and humans. The transition of the system into a dangerous state is caused by failures of its functional modules or their redundant elements. The failure of both the entire module and its component can lead to a dangerous effect [5].

The failure probability of the systems and therefore their modules should be reduced. A lot of principles are applied to develop the systems with high reliability. They are a principle of simplification, a principle of control, a principle of redundancy. Let’s take the last principle in more detail. The redundancy means the use of certain technical means to ensure the operability of the object in case of failure. The primary and backup elements are selected in systems with redundancy [6].

The failure can occur both in the module and in a redundant element. And analogously the release of energy or materials after the failure of the element may occur. And, therefore, both the module and its redundant elements carry the danger. These dangers should be divided into dangers arising from the failure of the module and the failure of the components. In the case of hot redundancy, the number of the components failures increases correspondingly to the number of components. In the case of a cold redundancy, the number of the components failures is not less than without redundancy, while the number of the module failures decreases. Thus, increasing the number of reserve elements at least does not reduce a potential danger to zero. The dangerous impacts can influence the personnel and infrastructure of the enterprise within the automated control system operates, and in this case, these impacts will be damaged [7-8].

2. Dependent failures in single-function systems

But along with the impact on personnel and infrastructure the dangerous impact that was caused by the failure of one module of the system can affect other modules of the system and cause their failure. It is so-called a dependent failure [9].

Automated control systems have a different logical structure. In the case when all modules of the system are connected in series, the failure of at least one module leads to the failure of the whole system and the dependent failures do not change its state in any way.

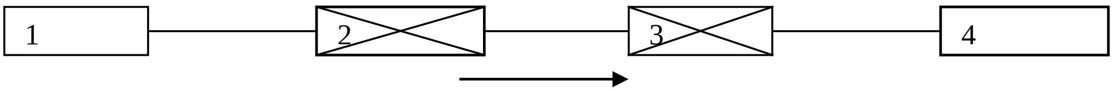

Figure 1. Dependent failure in the system of series-connected modules.

In the system shown in Figure 1 the failure of the module 2 causes the failure of the module 3 but, regardless of this fact, the system will be defective due to the module failure 2. A more complex case is when the system has a branching structure. In the case when the system performs several functions but not all components participate in performing any of the functions. Then the failure of one module will lead to the failure of only those functions in which performance it participates.

3. Dependent failures in multifunctional systems

As a rule, one system of the automated control system for technological processes performs several functions. One and the same technological process although it is considered as a single unit, often performs several functions. Also, the automated control system itself has the functions that do not affect the whole process. And to determine the reliability of the system, it is necessary to determine which elements are involved in performing particular functions. It is necessary to determine the sequences of components that perform a particular functional task. This procedure for dividing an existing system into subsystems (components) is called decomposition.

Decomposition as a process of partition allows us to treat any investigated system as a complex one consisting of separate interconnected subsystems, which, in turn, can also be broken up into parts. In decomposition each partition forms its own level. At the stage of decomposition which provides a general representation of the system the definition and decomposition of the overall target of the investigation and the main function of the system as a restriction of the trajectory in the state space of the system or in the field of admissible situations are carried out. More often decomposition is carried out by developing a target tree and a function tree.

The depth of the decomposition is limited. Decomposition should stop if it is necessary to change the level of abstraction, i.e., to present a component as a subsystem. If the decomposition reveals that the model begins to describe the internal algorithm of the component functioning instead of the law of its functioning as a "black box" then in this case the level of abstraction has changed. It means going beyond the target of researching the system and therefore the decomposition stops.

The functional decomposition is based on the analysis of the system functions. The question appears about what the system does, no matter how it works. The basis for splitting it into functional subsystems is the commonality of functions performed by groups of components. In order to obtain a more complete understanding of the system and its links, the supersystem and its constituent parts are included to the structure.

Often, the automated control system has a tree structure when other functions, mainly functions of monitoring the system parameters, branch out from one functional sequence performing the function of obtaining the final product. In some situations, the failure of a component in a hot redundancy can affect the main component.

The repeatedly reserved "root" module in the event of the failure of its component can put out of action the reliably logically unrelated sequence and carry an increased danger in general.

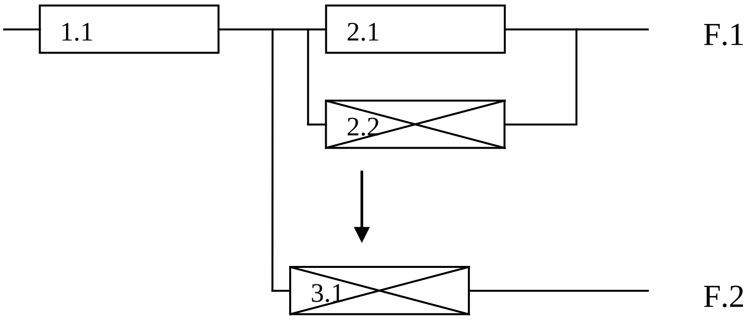

Figure 2. Dependent failure in multifunctional automated control system.

Figure 2 illustrates the words said above. There exists a system that performs two functions. The first function is performed by modules 1 and 2; the second function is performed by modules 1 and 3. Moreover module 2 is duplicated. The native failure of the redundant component 2.2 of module 2 does not lead to termination of the first function. But this failure causes a dependent failure of module 3. And that is why, the second function stops its execution. Thus, the redundancy of one module prevents its failure, but simultaneously causes the failure of other modules of the system, and, therefore, puts out of action other functions. Therefore, when calculating the fail-safe, it is necessary to take into account the probability of the system failure due to dependent failures.

4. Reliability calculation taking into account dependent failures

The account for the dependent failures changes the reliability model of the system very earnestly. For example, if we take into account the capability of a dependent failure call by a component of the module, including a redundant one, we have a method to take into account the capability that the increase of the degree of redundancy will reduce the reliability of the system with a certain probability of failure destroying other modules. Let's consider an example illustrating this.

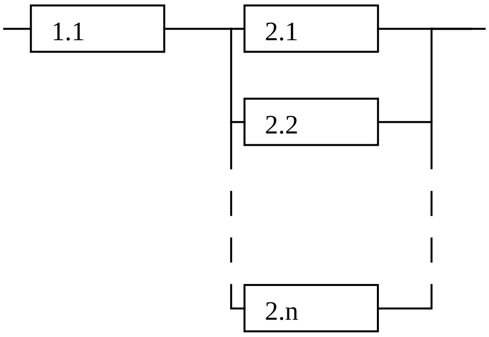

Figure 3. System with redundancy and dependent failures.

Let's take a system consisting of two series-connected modules; the second module has n-fold redundancy. Suppose P_1 is the probability of failure-free operation of the component of the first module; P_2 is the probability of failure-free operation of the component of the second module.

Without regard to dependent failures, the probability of failure-free operation is as follows:

$$P=P_1\cdot(1-(1-P_2)^n).$$

Now let’s suppose that each component of the second module has the probability of causing the failure of the first module. Let's say that P_d is the probability of the failure of the second module rejecting the first one.

The system will be operational at the following events:

S_1 - the first module is correct;

S_2 - at least one of the component of the second module is functional;

S_3 - there was no dependent failure of the first module caused by the second component.

Therefore, for the system to be reliable, the following expression must be true

$$S_1 \wedge S_2 \wedge S_3$$

The probability S_1 is equal to P_1, and the probability of the event S_2 is determined by the formula

$$P_{s2}=1-(1-P_2)^n$$

The probability of the event S_3 is found as the back probability of two events occurring simultaneously (failure of the second module component and dependent failure call by them).

$$Ps_3=1-(1-P_2^n)\cdot P_d$$

The probability of failure-free operation taking this into account, is calculated as

$$P=P_1\cdot(1-(1-P_2)^n)\cdot(1-(1-P_2^n)\cdot P_d) \quad (1)$$

5. Conclusion

Expression (1) shows that when the redundancy is increased, the reliability of the system taking into account the dependent failures, simultaneously grows due to the redundancy and decreases due to the presence of the dependent failures. Therefore, in order to improve the reliability of systems, one should apply instead the introduction of redundant components other methods of increasing the reliability and introduce measures to prevent dangerous effects.

Thus, the formalization of the approach to the assessment of the reliability of automated control systems with the dependent failures makes it possible to build a model that will have greater flexibility, take into account the impact of dangerous situations on the reliability of multifunction automated control systems.

References

[1] Avizhenis A N and Lapri Zh K 1986 *TIIER* **5** 8-21

[2] Kurochkin Yu A, Smirnov A S and Stepanov V A 1993 *Reliability and diagnostics of digital systems* (St.Petersburg: St.Petersburg University Publ)

[3] Kovalev I V 2014 *Vestnik SibGAU* **3(55)** 78-92

[4] Ryabinin I A 2007 *Reliability and safety of structural complex systems* (St.Petersburg: St.Petersburg University Publ)

[5] Kovalev I V, Kuznetsov P A, Zelenkov P V, Shaydurov V V and Bakhmareva K K 2013 *Pribory* **6** 20-4

[6] Kuznetsov P A, Beschastnaya N A, Bakhmareva K K, Antamoshkin O A and Antamoshkin A N 2012 *Vestnik SibGAU* **6(46)** 97-100

[7] GOST R 22.10.01-2001 2015 *Safety in emergencies. Damage assessment. Terms and definitions* Available from http://vsegost.com/Catalog/64/6474.shtml

[8] RF Federal Standards and Rules in the Field of Nuclear Energy NP-022-2000 2000 Available from http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=EXP;n=424308