Надежность № 3 2016 *Original article*
Dependability no.3 2016 *DOI: 10.21683/1729-2646-2016-16-3-35-38*

Organization features of functional diagnosis of a control computer with improved survivability

Vladimir G. Zarubsky, *Perm Institute of FSIN of Russia, Perm, Russia, e-mail: volen3030@rambler.ru*

Vladimir G. Zarubsky

Abstract. **Purpose.** *Today, the reliability of protection of mission critical objects and objects of increased risk is achieved by applying integrated safety systems, with the integration of subsystems based on control computers. Improvement of survivability of special purpose computers is a critical task that could be solved using the computers with the property of structural stability. Practical realization of such computer is connected with the task of its functional diagnosis and further functional adjustment. This article describes the process of functional diagnosis of structurally stable control computer as a functional system that is fundamentally different from the traditional control of a personal computer made by the known self-checking programs.* **Methods.** *To solve the task of functional diagnosis the article offers a mathematical model of test check that may become the basis of functional diagnosis of a control computer. Besides, based on the proposed mathematical model, possible outcomes of the test are analyzed.* **Results.** *Analysis of the proposed mathematical model defined the variants of how to minimize the risks of categories I and II, i.e. how to transfer faulty functions to a set of fault-free functions (customer's risk) and to transfer fault-free functions to a set of faulty ones (producer's risk), that is achieved by using a diagnosis practice of "promotion" that is standard for computers. The point is to find an operable "core" – a set of basic functions that help to diagnose the remaining functions of the computer's system of commands. I.e. the "core" with any detected defect is not allowed for further functioning, and a fault-free "core" can serve as rather reliable mean of control. When using this practice, the norm of a single test does not guarantee there is no risk of category I, that explains the common practice of check of each function of the command system by a sufficient sequence of test checks, and the risk of category II does not grow.* **Conclusion.** *The proposed model of a functional diagnosis test check made it possible to form the strategy to construct this process for a structurally stable control computer, namely to implement several particular tasks such as: to separate as a specific the task of identification of an operable "core" as a probable cause of risk of category I, that serves as a source of risk of category II; to perform sequential diagnosis of the remaining part of functions as in computing environment with a developed property of slow degradation of functions; to optimize an extending sequence of test checks for each function reducing the risk of category I, irretrievably leading to the growth of time control that is deficit for a pre-staged self-checking; that is also aimed at the adjustment to the current f-state; to proceed with testing in case of negative results using another software implementation to reduce risk of category II; to develop special procedure to substantiate the duration of testing of each function of control computers.*

Keywords: *control computer, survivability, structural stability, functional redundancy, functional diagnosis, accuracy of control, risks of categories I and II.*

Citation format*: Zarubsky V.G. Organization features of the functional diagnosis of a control computer with improved survivability // Dependability. 2016. No.3. P. 35-38. DOI: 10.21683/1729-2646-2016-16-3-35-38*

Introduction

Terrorist activity that has increased dramatically caused strict requirements for a reliable protection of mission critical objects. To solve this task, integrated safety systems (ISS) came into widespread application. The subsystems forming the part of ISS in most cases are integrated on the basis of a control computer (CC) that is represented by a common personal computer (PC), normally of foreign production with a "regular" operating system. Evidently, a failure of the control computer due to deliberate or undeliberate actions will lead to inadmissible changes of the operation of the whole system. In this situation the reliability of protection of mission critical objects becomes rather doubtful. Therefore, the idea to develop a domestic CC with the properties of improved survivability to different threats seems rather crucial.

Such CC can be represented by the computer with the properties of structural stability [1], whose operation is based on functional redundancy of any modern computer. But practical realization of such computer is connected with two particular tasks – functional diagnosis of CC and its functional adjustment.

All modern computers are multilevel devices, and each of these levels has the properties of functional redundancy [2]. That is why this article describes the processes of functional diagnosis on the example of the architecture command level.

Functional diagnosis of structurally stable (StS) CC, as a functional system differs from the traditional process of

PC control made by the known self-checking programs to define the technical condition: "fault-free – faulty", "operable – inoperable". In modern PC, functional diagnosis of the central processing unit is absolutely useless, as a failure to undergo any test makes it unpractical for a PC availability, because the reduced system of commands becomes non-conforming to a special software. That is not the case with common equipment of special digital weapon computer systems that provide a three-edged (three-channel) structure, which is especially effective against failures and their consequences. Here there are the elements of functional diagnosis aimed at the detection of some particular failures, that do not impede the execution of combat missions, but that are definitely eliminated under operational procedures considering the reduction of survivability margins necessary in extreme operating conditions. This category of failures includes inability of a channel to be a master (slave) one in a two-channel structure, inability of majority devices to defend against single errors at the information input, total or partial loss of functions of inter-channel exchange, etc**.** But in this case we deal not with self-checking, but with the determination of technical condition of the devices served to exchange functional features of the central processing unit.

Functional diagnosis of a structurally stable control computer

Functional diagnosis of the central processing unit, typical for the stage of recovery of CC StS availability, is in fact self-diagnosis, i.e. the identification of functional state $\tilde{\rho}^F$ under the conditions of stochastically undetermined splitting of the functional system F up to the classes $\tilde{\rho}^F$ and $\overline{\tilde{\rho}}^F$:

$$F = \tilde{\rho}^F \cup \overline{\tilde{\rho}}^F, \tilde{\rho}^F \cap \overline{\tilde{\rho}}^F = \varnothing, \quad (1)$$

with convergence

$$\tilde{\rho}^F \to \rho_f^F, \overline{\tilde{\rho}}^F \to \overline{\rho}_f^F, \quad (2)$$

where ρ_f^F is the current functional state of CC StS, as well as with the limited duration of the control process

$$t_{fd} \le t_{fd}^{\max}. \quad (3)$$

Expression (2) means that the risks of categories I and II are kept to minimum, i.e. faulty functions are considered as fault-free functions (customer's risk) and fault-free functions are considered as faulty ones (producer's risk).

In general, such task cannot be solved adequately due to certain unreliability of primary self-checking results, and its fast penetration into the further control processes. And the main principle of any process of control is violated here, the principle that requires all objects of control to be of the higher class than the object of this control. This condition is fulfilled in CC StS with a developed property of slow degradation [3, 4], for which the methodology of organization of the self-checking program is chosen as a mean for identification of the current functional state of ECM.

Really, at the first stage of functional diagnosis an operable functionally complete "core" is searched by the procedure that is common for ECM: "promotion" with a declaration of its inoperability by the first failure to undergo a test check. I.e. the "core" with any detected defect is not allowed for further functioning. Fault-free "core" of the PC functional system can serve as rather reliable mean to control single functions form the remaining part of the system of commands. It is facilitated by the developed property of slow degradation of functions implying that for each function to be checked there is a part serving only its part of the equipment that can undergo rather complete sequence of test checks.

Due to the fact that it is not possible to avoid the issue of control reliability at all, we should analyze the terms of its improvement with the reduction of possible consequences in further processes. To do it we need an adequate model of test control process that describes elementary control operations and their structures in relation to the maintenance of the required reliability level.

Let us consider the process of control of an ad hoc command ϑ as the function of the system of commands θ of the digital computer (DC) installed on the self-checking section to solve the alternative

$$\vartheta \in \rho_\phi^F \mid \vartheta \in \overline{\rho}_\phi^F, \quad (4)$$

that in reality transforms into the solution of alternative

$$\vartheta \in \tilde{\rho}^F \mid \vartheta \in \overline{\tilde{\rho}}^F \quad (5)$$

on the set P_F of variants of splitting (1).

Fault-free function of DC ϑ is defined in the finite discrete space of states S of DC, whose components are the cells of memory and general purpose registers taking various values within the limits of their capacity. It means that for any point S' of an arbitrary subset S_ϑ, $|S_\vartheta| \le |X'_\vartheta \cup X''_\vartheta|$, where $X'_\vartheta, X''_\vartheta$ is a set of input and output variables of command ϑ, there is $S'' \in S_\vartheta$, i.e. the following transformation takes place

$$\vartheta : S' \to S'' \quad (6)$$

Each pair (S', S'') can form the basis for a test check that together with the facility of control (OC) ϑ forms an operational system of control, if it has the means that can help to lead the computation process into the point $S' - a'_\vartheta$ (impact on the facility of control ϑ), as well as the means a''_ϑ to estimate the fact

$$\vartheta(S') = S'', \quad (7)$$

i.e. the reaction of the facility of control to the given impact. a'_ϑ adn a''_ϑ are customary to play the role of means of control (MC). In general the test a_ϑ has the following form

$$a_\vartheta = a'_\vartheta(\hat{\rho}^F)\vartheta a''_\vartheta(\hat{\rho}^F) = \\ = \vartheta \notin \tilde{\rho}^F \mid (\vartheta \in \tilde{\rho}^F \mid \vartheta \notin \tilde{\rho}^F) \mid \hat{\rho}^F \cup \vartheta \qquad (8)$$

where $\hat{\rho}^F$ is the state of identification process $\tilde{\rho}^F$ before the test a_ϑ

$$\hat{\rho}^F \subseteq \tilde{\rho}^F. \qquad (9)$$

The result of the process of control of ϑ by test (8) can be the assignment of ϑ to the class $\overline{\tilde{\rho}}^F$ with a failure to undergo the test by feature (7), uncertainty ($\vartheta \in \tilde{\rho}^F \mid \vartheta \notin \tilde{\rho}^F$), if the process of control of ϑ shall be followed by further tests of type (8), or the assignment of ϑ to the class $\tilde{\rho}^F$ and the linking of this function with an identified part of f-state of $\tilde{\rho}^F$, if this test was final one within the process of control of ϑ (Fig. 1).

Despite there are only two outcomes of each separate test check, there are much more internal cases occurring within the process of control (Fig. 2). Let us analyze situations 1-15 that are connected with: – with the reliability of determination of an operable "core" that was taken as initial at the beginning, but then as the current identified part of f-state

$$\hat{\rho}^F := \rho^F_{\text{яη}}. \qquad (2.10)$$

Two variants are possible:

$$\hat{\rho}^F \subset \rho^F_\phi \qquad (2.11)$$

and

$$\hat{\rho}^F \not\subset \rho^F_\phi; \qquad (2.12)$$

- with the reliability of determination of S' initial data predefined by a test check. For case (2.11) the following expression is inevitable

$$a'_\vartheta(\hat{\rho}^F) : \tilde{S}' = S', \qquad (2.13)$$

where $\tilde{S}'$ is an actual result of the execution of part of test a'_ϑ formed on the basis of subset of commands $\tilde{\rho}^F$. For case (2.12) due to test imperfection in addition to the result

$$a'_\vartheta(\hat{\rho}^F) : \tilde{S}' \neq S' \qquad (2.14)$$

the result (2.13) is possible;

- with the uncertainty of state of the object of control ϑ, whose reactions to the initial data S', can be

$$a'_\vartheta(\tilde{S}') : \tilde{S}'' = S'', \qquad (2.15)$$

5 cases in total (1, 2, 4, 5, 8), as well as

$$a'_\vartheta(\tilde{S}') : \tilde{S}'' \neq S'', \qquad (2.16)$$

4 cases (3, 6, 7, 9), where $\tilde{S}''$ is an actual result of command ϑ;

- with the reliability of estimation of the results (2.15), (2.16) by the sequence of commands $a''_\vartheta(\hat{\rho}^F)$ of a test check: N (norm) for 8 variants (1, 2, 4, 6, 8, 10, 12, 14), $\overline{N}$ (no-norm) for 7 variants (3, 5, 7, 9, 11, 13, 15).

Norm situations are split into two groups. The first group (1, 4, 10) corresponds to the case $\vartheta \in \rho^F_f$. They are unified by the lack of growth of category II risk, as a fault-free command is identified as fault-free. The second group (2, 6, 8, 12, 14) corresponds to the case $\vartheta \notin \rho^F_f$ and by confirming the norm it facilitates the growth of category I risk.

No-norm situations are split into two groups as well. The first group (3, 7, 9, 13, 15) corresponds to the case $\vartheta \notin \rho^F_f$. They are unified by the lack of growth of category I risk, as a faulty command is identified as faulty. The second group corresponds to the case $\vartheta \in \rho^F_f$ and by confirming the no-norm it facilitates the growth of category II risk.

Conclusion

Therefore, getting the norm of a single test does not guarantee there is no risk of category I, that explains the common practice of check of each function of the command system by a sufficient sequence of test checks. And the risk of category II does not grow. As norm situations are just a part of whole group of cases 1-15, we can state that risk of category I is getting lower in the sequence of various test checks passing by norm. It is explained by the fact that with each new test, the next variant of the equipment functioning is checked, and the number of unchecked variants is reduced. In case check of all variants of risk of category I after the norm of the last of them is excluded. However, limitation of duration of the check will not bring it to such situation.

Though it was noted above, the risk of category I not eliminated causes the risk of category II in form of a negative result of test of the function under checking under its norm. In this case the terms of f-diagnosis are getting worse. Based on situation 5 of the test outcome, the case could be improved by repeating a test (S', S''), using other commands from the scope of $\tilde{\rho}^F$. A negative result shall confirm the failure of function ϑ, and a positive result will help to pass to a new functional "core".

A model of test check of f-diagnosis will assist to form the strategy of how to develop this process important to CC StS:

1) special attention should be paid to the identification of an operable "core", as at this stage the risk of category I is being originated, serving as a source of category II risk as well;

2) the remaining part of CC functions should be diagnosed one by one as in computing environment with a developed property of slow degradation of functions;

3) extending sequence of test checks for each CC function reduces risk of category I, but at the same time the time spent to control is growing, and it is deficit for a pre-staged self-checking, that is also aimed at the adjustment to the current f-state;

4) to reduce risk of category II, in case of negative results of tests, they should be continued using the same initial data, but another software implementation;

5) substantiation of the duration of testing of each function of CC requires the development of special procedure.

References

1. Zarubsky V.G. Issues of the development of advanced integrated security systems conforming the requirements of improved survivability, based on structurally stable control computers. Reporter of the Perm Institute of FSIN of Russia. Issue 1 (5)/ 2012. P 4-9.

2. Zarubsky V.G., Rybakov A.P. A mathematical model of adjustment of the integrated system control computer to the current functional state. Reporter of the Voronezh Institute of MIA of Russia. Issue 1/2012. P. 170-178.

3. Kharitonov V.A. Foundations of survivability of functionally redundant systems. SPb.: SPIIRAN, 1993. – 60 p.

4. Tyurin S.F. Synthesis of digital equipment adjusted to failures with a redundancy of basic functions / Devices and systems. Operation, control, diagnostics. Issue 1/ 1999. P 36-39.

About the authors

Vladimir G. Zarubsky, PhD Engineering, Associate Professor of the chair, Perm Institute of FSIN of Russia, Perm, Russia, e-mail: volen3030@rambler.ru

Receive on 10.03.2016