INTERNATIONAL JOURNAL OF ENGINEERING AND MANAGEMENT SCIENCES
© 2004 -17 Society For Science and Nature (SFSN). All Rights Reserved
www.scienceandnature.org

SOLUTION OF DEPENDABILITY OF COMPUTER SYSTEMS IN BASES OF COMPUTER SCIENCE

Haider Hassan Majeed AlKaraawi
College of Veterinary Medicine, University of Kerbala, Karbala, Iraq
Corresponding Authors' Email: yasser_veterinary@yahoo.com

ABSTRACT
The methods and means of technological element, information, algorithmic program and organization basics in deciding the problem of dependability of CS are considered. The particular attention was pushed to system cybernetic approach in deciding this problem. Among considered means for providing dependability CS there are used the following: regular and crisis controlling, monitoring resources and information flours, functional doubling, net interconnection between components CS and others.

KEYWORDS: Dependability, Reliability, Availability, Integrity, Technology, Computer System.

INTRODUCTION

Due to the fact that the current development is aimed at building an information society, and then the knowledge society (Michael Bucklan*det al*., 2017), therefore, becoming increasingly important reliability and its generalization Dependability of Computer Systems (CS). This process leads to the fact that the Computer system is widely used in various fields of economy, technology, science, medicine, banking, automation and other processes, etc., which require the reliability of the received information. In turn, the concept of dependability has emerged as a result of the integration of concepts such as reliability, fault tolerance, functional safety, maintainability, etc. From this point of view, equivalent to CS Dependability of the system (functional) reliability. But reliability is only indirectly determines the term of dependability. Customer Service CS of little interest to the reliability of the CS. This interest professionals and consumers interested in how it receives from the CS reliable results and how stable CS work process for continuously producing results. The problem of unreliable results CS is compounded by the fact that almost the majority of CS linked Internet, allowing others to use false information to CS (of course, without knowing it). In some cases, it can lead to disastrous consequences. Especially it is dangerous in critical areas of use CS. More detail of these problems are discussed in (Tesler G.S. *et al*., 2006), (Xiaofei Lu.*et al*., 2016). It is in connection with the widespread use of the CS and the Internet in all areas of the information society challenges the decision of dependability is the most relevant and important now.There are various approaches to solving these problems. For more detail on these in subsequent sections of the work. The distinguishing feature of this work is to look at the solution of these problems on the basis of bases of computer science.However, consideration of the bases of computer science should precede systemic cybernetic approach to the processes occurring in the system in general and CS, in particular. In solving the problem of creating a fault-tolerant CS to the fore a variety of technologies, generalized diagnostics (monitoring), adaptability, determination, multiprocessing and reliability (stability) of the operation. So, for dependability assurance necessary to consider manufacturability of the elemental base, programming technology, computing technology, information (computer) technologies, etc.

DEPENDABILITY

In this work (Laprie J. *et al*., 2002), (Avizienes A. *et al*., 2004), we give a few notions Dependability of the term. The original definition of dependability primarily proceeded from the fact that the system provides a service you can trust. Alternative concept defines Dependability of as the ability to avoid service failures more frequent and more severe than is acceptable. And finally, the Dependability of perceived as a synthetic concept, which includes the following indicators:

- Readiness, ie, readiness for proper maintenance;
- Reliability, ie continuity (consistency) proper maintenance;
- Functional safety, ie the absence of catastrophic consequences for the users and the environment;
- Integrity, ie, no incorrect changes to the system;
- Serviceability, ability to undergo modifications and repair or replacement of failed automatic component of the system, as well as stability of operation.

But Dependability is not quite complete, if it is not complemented by the requirement of system security, ie, capabilities to withstand external threats and, above all, unauthorized entry into the system. As shown in this work (Laprie J. *et al*., 2002), (Avizienes A. *et al*., 2004), a prerequisite of dependability for large systems is fault tolerance. But this is only a necessary condition. A

sufficient condition for the achievement of dependability of the system is to meet any and all figures given in the definition of synthetic resiliency. Recall that, in turn, is a necessary condition in constructing fault tolerant systems is the availability and widespread use of various kinds of redundancy. Fig. 1 shows the different types of redundancy that can be used in the creation of dependable CS.

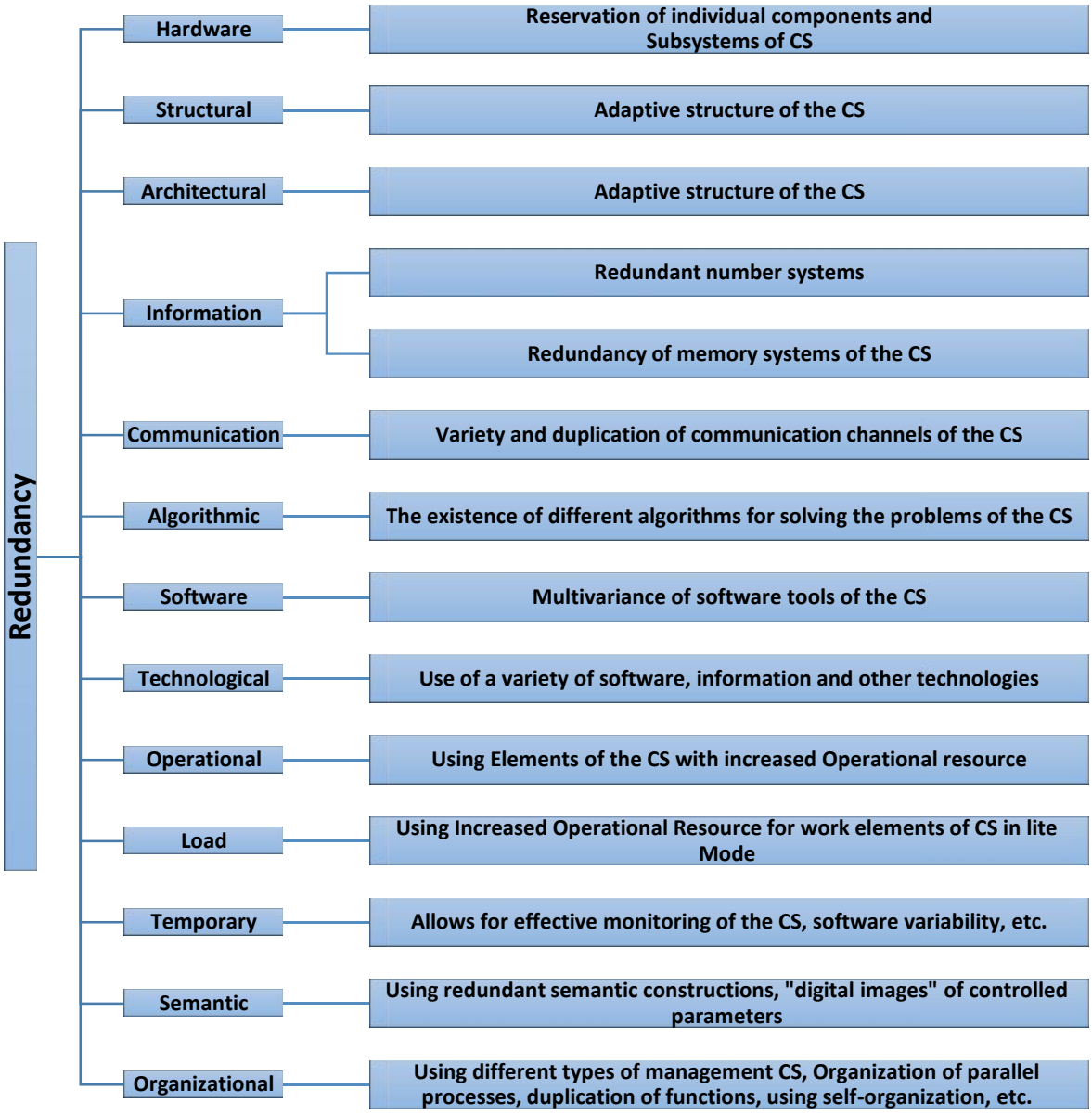

Fig. 1. Types of redundancy.

In (Luigia Petre, Kaisa Sere.*et al*., 2011) it is considered that a Guaranteed CS (GCS) is a system possessing a full or partial set of primary properties constituting a guarantee. At the same time, the primary properties mean reliability, availability, serviceability, functional security, survivability, integrity, confidentiality, and also it is possible to add information security, authenticity, reliability, maintainability, durability, etc. In (Tesler G.S. *et al*., 2006) it is noted that assurance is ultimately a means (technology) that guarantees the reliability of receiving information from the CS as a result of its transformation, storage and transmission, despite the presence of external and internal disturbances affecting the work of the CS. But getting reliable information is associated with reliable operation of all components of the CS and reliable input information. On the other hand, the necessary condition for the guarantee is its stable operation, which allows to adequately react to all internal and external disturbances. Along with the notion of stability of CS, in (Tesler G.S. *et al*., 2006)an expanded notion of operability relative to CS is considered. Continuing this idea, under the assurance of the CS, it is possible to perceive the CS capability correctly and steadily to work both in its normal operation mode and in an abnormal (critical) mode by preserving the performance characteristics of all necessary system components that affect the tasks assigned to the CS. Guarantee as a functional (system) reliability is based on the stable operation of all components of the computer

system (technical and software), mathematical support (methods and algorithms), information, as well as their correct operation, despite the emerged failures and failures associated with internal and external causes , Which ensures the reliability of calculations and services received from the GCS.Guarantee is a further naturaldevelopment of fault tolerance and survivability of computer systems that make extensive use of all types of redundancy, monitoring of the state of the CS and mechanisms for countering the consequences of failures that occurred in the CS, as well as countering external and internal attempts to distort (correct) the operation and functioning of the CS and its information components. Important for the GCS is the provision of guaranteed computing, the presence of input and output filters that exclude distortion of input and output information. As an assessment of the dependability in (Luigia Petre, Kaisa Sere.*et al*., 2011) two types of estimates are proposed:

- Vector, representing a set of indicators that assess certain properties of the dependability (reliability, availability, integrity) or resistance to various types of defects;
- Scalar, with the help of which a generalized estimate is given.

One of the variants of the scalar index is the probability of providing a CS service. Another variant of the scalar estimate is based on a metric approach that uses a detailed guarantee model as a hierarchy of primary and secondary properties, as well as their characteristics, determined by a set of metrics. The latter are estimated experimentally or calculated on the basis of the measured parameters of the system. Next, convolution of metrics is obtained.

SYSTEM-CYBERNETIC APPROACH IN SOLVING PROBLEMS OF DEPENDABILITYOF CS

Within the framework of this section of the work we will consider the possibility of transferring some functions of a person to the CS. This is justified by the fact that man, like many wildlife objects, is well equipped with mechanisms that allow him to maintain vital parameters and processes at the level of their stabilization, which allows him to function within the necessary limits. As noted in (Koss V.A.*et al*., 2006), (Joanne Dosé, Jim Maynard*et al*., 2016), the interaction of a person with the world around him, as well as his autonomous functioning, are mutually conditioned and carried out within the following functions: instinctive, motor, emotional and intellectual. For example, the human instinctive function in the thinking process is manifested as the need to make decisions related to personal security problems, creating favorable conditions for life, removing waste as needed, etc. In cybernetic systems, such as CS, these functions can include the following:

- Monitoring of the surrounding space in real time (parametric signals, values of functions, progress of processes, etc.);
- Analysis of the situation related to the state of the controlled complex system (CS and its elements), based on monitoring data for rapid response, i.e. The self-preservation function of the CS;
- The formation of associative links within the current monitoring information, written to the memory of the CS and its components;
- Management of associative links between monitoring data in the current situation and signs of similarity of past situations;
- Crisis management in the restoration of lost functions.

Thus, the "instinctive" function of the CS basically consists in the following: monitoring of activities (work, functioning, etc.); Monitoring of all types of system resources, monitoring the external space of the system (where necessary); Analysis of current situations; Implementation of situational management in a normal mode to prevent threats to the system in accordance with its regulations and transition to crisis management in the event of a threat transition into a real state. Similarly to the above, it is possible to interpret the motor, emotional and intellectual functions of a person that can be introduced into the CS to ensure its reliability. The human motor function is conditioned by the need to control the motor activity of a person (spatial orientation, coordination of movements, planning and organization of activity). For CS, which work in mobile objects, practically all the motor functions of a person should be present to some extent. And in normal systems, there should be a function of planning and organizing activities within the CS to prevent the threat of normal functioning and its elimination in the event of occurrence. At the same time, the motor mind interacts directly with the intellectual, which is expressed in the possibility of designing appropriate rational technologies for action, as well as organizing the implementation of the necessary projects and plans. The intellectual function of the human mind can perform input (output) control (in our case, input and output information filters of the CS), norm control (control the correctness of the system operation), planning (forming the plan for the future action). Norm control in the CS in many cases is carried out on the basis of an assessment of the location of the values of parameters, constraints, which are determined by the rules of the system. The obtained simulation results are directly used by the control system to take the necessary actions, if necessary. For a correct understanding of how to ensure the reliability of the CS, it is advisable to ensure the balance (harmony) of the course of the six processes taking place in the system (Joanne Dosé, Jim Maynard.*et al*., 2016), (Jack Clark Francis.*et al*., 2013). At the same time, the balance of these processes occurs by stimulating some processes and restraining others, depending on the chosen goal, strategy and tactics of the management process. The main requirement for the facility in general and the CS, in particular, is to ensure its functioning according to its intended purpose, while maintaining its regular work and organization, as well as rational use of available cash resources. The functioning of any active object is provided by the following six processes:

- The process of processing resources and obtaining products. Control information. Control information, starting from the target, is sequentially decomposed into functions, plans, etc. Up to commands and signals. In our case, the goal is to ensure the reliability of the COP.

- Growth process. In this process, management information provides the organization of object resources in structural units. The activity of control information allows to fulfill the resource potential of the structural elements of the object. This information also allows you to balance the processes of the organization of the active object, ensuring the preservation of the possibility of the object functioning according to its intended purpose in the normal mode.
- Self-destruction process. There is a deviation of the work of individual elements of the system from the regular mode, which leads to a deviation of the work from the destination, unless special measures are taken. The nature of this process is connected, on the one hand, with the processes of degradation of the elements of the object under the influence of time, external and internal conditions of their work, and, on the other hand, the process of object degradation is related to the fact that the control and other types of information that go to the structural units of the object And from them, is distorted. This process is opposed by the process of managing security based on situational management.
- The process of self-learning, changes in nature or the acquisition of new functions. This process is due to the fact that the structural units of the object initiate a change in the composition of resources in order to acquire new functions. The process of self-learning involves the generation of new strategies for the functioning of the object, which is the standard function of the object's control body. Within the compensation of an object, the process of self-learning allows you to change the functions performed on the object itself, and also to develop requirements for changing functions to the meta system when interacting with other objects.
- The process of self-organization and the "healing" of the object. This process is aimed at restoring the disturbed functions, in particular, resulting from the process of self-destruction. At the same time, the executive means of the object, self-organizing into the structural hierarchy, restore controllability and work on the object's purpose. The property of self-organization in this case is connected with the need to provide structural units of the object to self-preservation or to heal in case of threats to the object in violation of the intended purpose. At the same time, there is a transition to a crisis management of the facility, which ensures the liquidation of the focus that caused the crisis, and the restoration of the function of the facility in full or partial volume due to existing or attracting new resources.
- The process of monitoring and integrating resources in accordance with the rules for the operation of the facility. In this case, the execution facilities of the object generate (generate) information about the execution of the received tasks, the state of the structure and the resources of the object. This information is analyzed and structured in the relevant structural unit of the facility where it is stored, and on its basis actions are built directly aimed at eliminating the emerging threats, taking into account the forecast of the state of the object's functioning according to its intended purpose.

All six processes, perceived in time and dynamics, represent the functioning of a complex system. Management of any activity of an object is reduced to maintaining a balance between the results of the six processes described above, by restraining one and stimulating others, depending on the chosen management strategy. In the event of one or more processes leaving the scope of the procedure for the functioning of the process, if necessary, the transition from the regular to the situation (crisis) management of the object. The reader can easily interpret these six processes independently within the framework of creating a secure and fault-tolerant CS. The description of the functioning of a complex system in the form of these six processes is one of the theoretical foundations for constructing a theory of the creation of guaranteed CS. It is advisable to supplement the six processes described above with a hierarchy of information structuring in the active object. From the point of view of the system-cybernetic approach (Joanne Dosé, Jim Maynard*et al*., 2016)and the patterns of information transformation in control cycles of complex systems, the active object exists at the following levels:

- Zero level is the objective function of the active object in terms of its purpose, which is generated at a higher level (meta-level) in relation to the object (system);
- First level is a list of the functions of the object with the justification of the need for its creation and the restrictions that the objective function of the object imposes on the functioning;
- Second level is the structural organization of the existence and functioning of the facility, including documents (instructions, etc.) and / or processes that ensure the life cycle of the facility in accordance with the regulations, as well as the process of self-education (for acquiring new qualities, functions and opportunities Adaptation to external and internal influences);
- Third level is the generation of command and signal information and its use in the practical implementation of the objective function of the facility, including the possibility of restoring lost functions or resources using monitoring results to ensure the security and operability of the facility.

In this case, the object is understood CS, and under the objective function - ensuring the reliability of the CS. It should be noted that the guarantee based on the use of functional information blocks requires a systematic approach both from the point of view of allocating system functions in the hierarchy, and in terms of the allocation of goals and sub goals. In addition, the following must be provided:

- System consistency in the goals, objectives, resources and necessary results of the system, as well as ensuring its reliability in the presence of failures and failures;
- Mutual consistency of the goals, objectives, resources and expected results of the system health management;

- Timely detection, guaranteed recognition and system diagnostics of factors and situations leading to failures, malfunctions and delivery of incorrect results of the computer system;
- Operational forecasting, reliable estimation of abnormal and critical situations;
- Timely formation, operational implementation of the management of the guarantee in the process of preventing abnormal and critical situations.

THE ROLE OF COMPUTER SCIENCE BASES IN SOLVING THE PROBLEM OF DEPENDABILITY

The element-technological basis was known even before the author introduced the remaining bases.forms the basis for building hardware and in many respects depends on the technology of manufacturing the hardware of the CS. If earlier the elemental basis was made up of elements from which the processes and other components of the CS were built, constitutes the basis of the elemental technological basis. When solving the problem of reliability, the most important are the following indicators: high reliability, productivity, availability, efficiency, availability of internal monitoring, etc. To improve the reliability of the elements, it is extremely important to improve the performance characteristics of the elements not only through advanced manufacturing technologies, but also by reducing the operating frequency of their operation (reduces the temperature regime and uses elements capable of operating at a higher frequency, and, in the case Underload, have the ability to disable idle items and go into "waiting" mode). In addition, it is important to use the possibility of issuing signals about the occurrence of threats to a higher level, and in some cases, parry failures by using other bases at the micro level. Information basis is a set of tools and methods associated with the presentation, processing, storage and transmission of information, as well as ensuring its integrity. It is important in what form the information is presented, the amount of information to be stored and the access time to it, the speed and amount of information transmitted through the communication channels and processed by the active elements of the CS. This includes not only the information to be processed, but also program information. It is necessary to know that the information basis plays a key role in solving the problem of dependability. First of all, it defines the numbering system of the processing elements included in the CS. The use of encoding information with detection and correction of errors or bringing the errors that occur to the errors corresponding to the unit of the last digit (for example, binary-five-code, cyclic codes, etc.), contribute to the appearance of the architecture of the NonStop system, which provides rapid manifestation of faults and corresponds to that The principle that each component of the CS either functions correctly or stops immediately. The information basis includes the receipt, transfer, transformation, storage, structuring and issuance of information to the CS. This includes data bases of different types, as well as input and output information of machine algorithms. To ensure the reliability of the CS, an input and output information filters must play an important role, ensuring the screening of improbable data at the input and output of both the processing components and the CS themselves. These filters are extremely important due to the fact that the CS has the property of increasing the uncertainty of the output information if the input information is even partially uncertain. It should be noted that the provision of a sufficient level of the guarantee of the CS, from the point of view of the information basis, is provided in each of the components of the CS by its means, with agreement with the overall strategy for ensuring the assurance of the CS. The program-algorithmic basis includes in its composition all the components of software, i.e. System and application software, as well as algorithms, methods, calculation schemes, functional information transformations, decision rules, models of computational processes, standard and defined functions, expressions, chains of operators, macros, etc. Input language of CS. This basis includes all the components that form the basis for the creation and implementation of the computational process of the CS. In addition, the considered basis contains, as its tools, programming technologies and computational technologies, which are extremely important for ensuring reliable computations. The technology of calculations is directly related to ensuring the numerical stability of methods (algorithms) in solving applied problems. The software's reliability in many cases uses the idea of multi variance (Ali Mili, Fairouz Tchier.*et al*., 2015), (Rajkumar Buyya , Amir Vahid Dastjerdi.*et al*., 2016). Undoubtedly, to solve the problem of software availability, the algorithmic basis must effectively interact with other bases of computer science.Above all, refers to the organizational basis, which must take an active part in organizing the emergence of signals about threats, their localization and, if possible, their elimination. Particularly important is the participation of this basis in the management of the computational process and the transition to situational (crisis) management, in the case of turning a threat into reality, and returning the computational process to a normal state, if possible. In the implementation of these processes, the middle level of the hierarchy of the given basis is mainly involved. The organizational basis connects all the processes taking place in the system, and are closely related to the architecture and structure of the CS, as well as system software. It should also organize interaction between the elements and levels of the CS, synchronize their work, monitor the state of the system and restore the correctness of the work in the event of the appearance of various types of defects identified in the monitoring, by using the various types of redundancy available in the CS. An effective computational process inside the machine and information and physical interaction both with intra system components, and with an external medium with respect to the CS, etc. The most effective, from the point of view of the organizational basis, is the adaptive CS with a programmable structure and architecture, based on the backbone network interaction. Note that the organizational basis plays an important role in restarting the processes in the event of the emergence of freelance (crisis) situations and the organization of management processes. This is extremely important to ensure reliable computing. It is important to manage processes on the local (micro), intermediate and global levels. Today's fail-safe CS are mainly based on methods of duplicating components and comparing the

results obtained. Although, if you follow the logic of wildlife, you need to move from simple duplication to duplication of functions and have the intellectual means to detect defects and parry them. The modern organizational basis for ensuring the reliability should use adaptive multi-loop network architectures, NonStop processing element structures, duplication of functions, rather than elements, as is currently done, monitoring all components of the CS, identifying and forecasting threats and eliminating them in case of implementation, implementation Reorganization of the CS, if necessary, to counter internal and external threats, evaluate the reliability of the output information received, and monitor the passage of information within the system and finding it within specified ranges, and much more. The organizational basis must implement the correct execution of six processes at the appropriate levels of the CS hierarchy. But for this, in addition to the above, it is necessary to have an intellectual center in the CS in the form of an expert system working in real time to ensure the forecast of the events taking place, their analysis for making the necessary decisions, as well as self-learning and self-development of the CS. As can be seen from the foregoing, none of the bases of computer science is able to solve the problem of the CS self-sufficiency alone. This is due to the fact that the problem of creating the reliability of the CS is complex and therefore it is necessary to use all bases to solve it. However, contradictions may arise between bases, which can be solved on the basis of the mixed extreme principle (Michael Bucklan*det al*., 2017).

MEANS OF CONSTRUCTION OF DEPENDABLE CS

Trusted computers are key elements for creating fault-tolerant and secure CS for work in retail, finance, telephone switching, etc. One of the most well-known firms in the world, as noted in (Yurchenko Yu. *et al*., 2016), is Tandem. Tandem NonStop systems are based on the implementation of multiprocessing and the distributed memory model. To ensure recovery from hardware failures and software errors, these systems use a message transfer mechanism between process pairs. The NonStop SQL database, which is based on the system model without a partition, allows in some cases to achieve linear scalability from the number of processors used in the CS. However, system Integrity company Integrity methods of hardware redundancy based on a three-time reservation with a majority valve are used. This is not an optimal solution, but it ensures continuation of continuous operation in the face of threats. More advanced is the NonStop architecture with network interaction between CS components. Note that the systems that have a central processor perform a comparison of the outputs of the duplicated inter-synchronized microprocessors. Responsibility after detection of a malfunction in the equipment rests with the software. However, the comparison can be performed not only by the processor element, but also by the computer network, of course, if such exists in the structure of the CS. It can also carry out switching both the message of packets, etc., and connection of elements, including peripheral devices among themselves. Consider in more detail the architecture of NonStop, which is one of the significant components of the reliability of the CS. The NonStop architecture (Yurchenko Yu. *et al*., 2016) involves combining two or more processes using a duplicated high-speed interprocessor bus. As such a bus, a fiber optic interprocessor exchange network can be used. All hardware components of the NonStop system are based on the principle of "rapid manifestation of malfunctions", according to which each component of the system must either function correctly or stop immediately, which otherwise stops the spread of the distorted information. Modern designs for error detection rely mainly on methods of duplication and comparison. But there are other similar methods (hardware and software). However, the restoration of the normal operation of the CS after detection of a malfunction is mainly the responsibility of the software, although in a number of cases it becomes necessary to use hardware. Further development of this architecture involves the use of a duplicated local area network. Its basic element is the router. In a typical configuration of the system, most of its nodes have two-port interfaces. At the same time, the detection of a faulty node is entrusted to the network itself. To recover from hardware failures and software errors, these systems use message transfer mechanisms between processor pairs. In work (Kharchenko V.S.*et al*., 2002)other approaches to the design of fault-tolerant airborne complexes are considered. Among them - single-channel structures with automatic control and recovery; Multi-channel redundant structures; Multi-channel structures with an automatic inter-channel exchange; Software monitoring and information recovery in channels; Multichannel structures with hardware majorization of the input and output information of channels; Multichannel multi-tier structures with hardware majorization of the signals of each functional unit of the airborne complex, and also their analysis. Some of the approaches and mechanisms considered can be used in a perspective network NonStop architecture, whose ideology most fully meets the requirements for building reliable systems. An important task of implementing effective fault tolerance is to prevent the spread of the error to the operation of the serviceable components of the CS. The foregoing is most clearly seen when one of the components of the CS transmits erroneous information to other components using this information. Until recently, the mechanisms of trojaning components with a majority valve (the mechanism of coincidence of two components of three) were mainly used to solve this problem. Currently, for example, for the creation of fault-tolerant servers, the NonStop architecture of the CS component is used, which does not provide erroneous information to neighboring components through self-monitoring. If this component fails, the information comes from a similar component that functionally duplicates the first. As an arbiter in this case is the computer network. Here we observe at once three effects: the localization of error propagation, the continuation of the correct operation of the system and the element of network interaction between the components of the CS. To ensure that the internal computer network does not become the Achilles' heel in solving the problem of fault tolerance, it is also duplicated. Thus, instead of the mechanism "Two out of three" uses a "one in two" mechanism with network

interaction. In case of failure and the second component of the CS in the process under consideration, a functional duplication mechanism can be used, i.e. Transfer of the performed function to another component in the other pair, in the form of additional load and new routing. But for this, the CS must have an intelligent control unit, which is obliged to support the mechanisms described above. During the switching of the CS component to ensure continuous operation (for real time CS), it is necessary to use the predicted values of the process parameters that are operatively transferred to the intelligent control unit of the compressor. In the event of an accidental failure in the system, you can use multiple calculations, but this requires a certain amount of time. Characteristic features of dependability under consideration by the CS are as follows:

- Use of all types of redundancy;
- Network interaction between system components;
- Use of the generalized system readiness, which allows to replace the failed component with a working one;
- Use of processing modules of the system working in the NonStop mode;
- Use of duplication of functions instead of simple duplication of system elements;
- The presence of two types of management system: regular and crisis (situational);
- Availability of system monitoring system at all levels of its work;
- Prediction of the reliability of the elements of the system;
- The possibility of reconfiguration of the system;
- The ability to track information flows of the system;
- Tracking the output of the system parameters beyond the established limits and prompt response to the exit beyond the established "corridor";
- Availability of means of prompt response of the system to the emerged threats, ensuring the continuation of the system operation in the regular mode;
- The presence of intelligent modules in the system, allowing to develop a real-time strategy and tactics to ensure the normal operation of the system in the event of threats and ensuring the self-development of the system taking into account available resources;
- The possibility of resolving the existing contradictions at all stages of the creation and operation of the system on the basis of the mixed extreme principle;
- Have the means to manage the reliability of the system;
- A necessary condition for maintaining the integrity of the system.

In solving the problem of the guarantee of the CS, ensuring their readiness plays an important role. At the same time, a high availability is distinguished which minimizes the time of planned and unplanned downtime of the compressor by rapid restoration of the system after detection of a malfunction, and a continuous readiness that ensures correct operation of the system and eliminates any downtime, either planned or unplanned. In our case, it is the continuous (dynamic) readiness that is most preferable. But for the implementation of continuous readiness, redundant hardware and software are needed, which in some cases can be used to parallelize the necessary work performed by the CS, mechanisms for monitoring the elements of the system, parrying emerging threats and failures, and the ability to adequately respond to the current state. An additional requirement for such systems is the absence of degradation of the system in the event of a failure. To ensure high availability of the CS, it is necessary to ensure, first of all, the protection of the most important part of the system - data, as well as on-line diagnostics, isolation of the wrong process, network organization of communications, etc.In Fig. 2 shows the main set of tools used to create a secure CS.

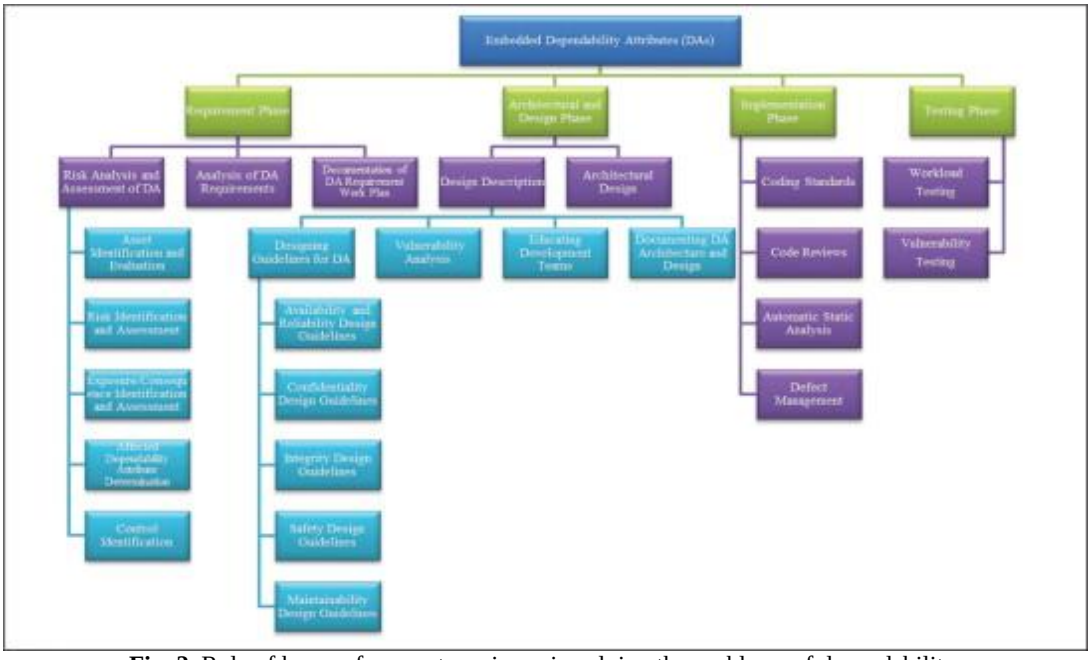

Fig. 2. Role of bases of computer science in solving the problems of dependability

In addition, it is advisable to introduce control over the availability of information and parameters of information flows in all parts of the computer system and especially on the switch in the case of a system with network interaction, a programmable structure and architecture, including information passing indicators. In addition, similar should be done for the control of functional information blocks.For ensure the dependability we should follows:

- Introduce input and output filters at the input and output of the computer system and its function-information blocks that cut values of data values beyond the permitted ranges, accounting for trends, etc.;
- To carry out studies of the stability of computations both in the development of computational algorithms and in the course of computations themselves;
- Verify compliance of the data obtained as a result of calculations with the necessary way of substituting them into the original mathematical dependencies and estimating the values of the resulting residuals;
- Carry out current estimation of different types of errors both at the stage of development of algorithms and during calculations;
- It is widely used iterative methods, in which the error depends mainly on the error of the last iteration;
- To use along with complete algorithms simplified algorithms allowing to carry out a qualitative estimation of the received calculations;
- Calculate the necessary functional dependencies with different accuracy to detect hidden instabilities of calculations;
- To struggle with the possibility of "hovering" of the operating system, and in case of this situation it is necessary to provide for its duplication, etc.

CONCLUSIONS

The material presented in the paper has both theoretical and practical value in the construction of dependability CS. For the first time both in domestic and foreign literature the importance of solving the problem of dependability based on the bases of computer science is shown. This made it possible to see that when solving this problem, it becomes necessary to optimize the contradictions existing between these bases. And, finally, the system-cybernetic approach in a completely different perspective allowed us to look at the problem of dependability. The approaches outlined in the work require further detail and concretization. In general, the problem of the guarantee of the CS is so complex that it is unlikely that its full solution is foreseen in the near future.

REFERENCES

Ali Mili, Fairouz Tchier. 2015. Software Testing: Concepts and Operations (Quantitative Software Engineering Series).

Avizienes A. 2004. Basic concepts and taxonomy of dependable and secure computing.

Jack Clark Francis. 2013. Modern Portfolio Theory, + Website: Foundations, Analysis, and New Developments.

Joanne Dosé and Jim Maynard. 2016. Celestial Influences Eastern Time.

John Knight.2012. Fundamentals of Dependable Computing for Software Engineers (Chapman & Hall/CRC Innovations in Software.

Kharchenko V.S. 2002. Implementation of the projects of fault-tolerant on-board computers of space components Industry.

Koss V.A. 2006. Model of natural intelligence and ways of realizing the tasks of artificial intelligence.

Laprie J. 2002. Fundamental concepts of dependability.

Luigia Petre, Kaisa Sere. 2011. Dependability and Computer Engineering: Concepts for Software-Intensive Systems.

Michael Buckland. 2017. Information and Society (The MIT Press Essential Knowledge series).

Norbert Wiener. 2013. Cybernetics: Second Edition: Or the Control and Communication in the Animal and the Machine.

Peter A. Lee, Thomas Anderson. 2013. Fault Tolerance: Principles and Practice (Dependable Computing and Fault-Tolerant Systems).

Rajkumar Buyya , Amir Vahid Dastjerdi. 2016. Internet of Things: Principles and Paradigms.

Shnitman V.Z., Kuznetsov S.D. Servers of corporate databases. Information and analytical materials of the Information Technologies Center. http // www.ivann.delta.msk.su.

Tesler G.S. 2006. The concept of constructing guaranteed systems.

Xiaofei Lu. 2016. Computational Methods for Corpus Annotation and Analysis.

Yurchenko Yu. IOTS approach: analysis of variants of structures of fail-safe board Complexes with the use of electronic complexes Industry. http // www.cpm.ru.

Zannos S. 2004.Human types: Publishing house "All".