Abstracts of Dissertations

Institute of Information and Communication Technologies

BULGARIAN ACADEMY OF SCIENCES

6 / 2023

STUDY OF THE DEPENDABILITY CHARACTERISTICS OF A FAULT-TOLERANT DISTRIBUTED REAL-TIME SYSTEM WITH ADJUSTABLE RELIABILITY

Edita Djambazova

ИЗСЛЕДВАНЕ НА НАДЕЖДНОСТНИТЕ ХАРАКТЕРИСТИКИ НА ОТКАЗОУСТОЙЧИВА РАЗПРЕДЕЛЕНА СИСТЕМА ЗА РАБОТА В РЕАЛНО ВРЕМЕ С НАСТРОЙВАЕМА НАДЕЖДНОСТ

Едита Джамбазова

Автореферати на дисертации

Институт по информационни и комуникационни технологии

БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ

ISSN: 1314-6351

Поредицата ***„Автореферати на дисертации на Института по информационни и комуникационни технологии при Българската академия на науките“*** *представя в електронен формат автореферати на дисертации за получаване на научната степен „Доктор на науките” или на образователната и научната степен „Доктор”, защитени в Института по информационни и комуникационни технологии при Българската академия на науките. Представените трудове отразяват нови научни и научно-приложни приноси в редица области на информационните и комуникационните технологии като Компютърни мрежи и архитектури, Паралелни алгоритми, Научни пресмятания, Лингвистично моделиране, Математически методи за обработка на сензорна информация, Информационни технологии в сигурността, Технологии за управление и обработка на знания, Грид-технологии и приложения, Оптимизация и вземане на решения, Обработка на сигнали и разпознаване на образи, Интелигентни системи, Информационни процеси и системи, Вградени интелигентни технологии, Йерархични системи, Комуникационни системи и услуги и др.*

The series ***Abstracts of Dissertations of the Institute of Information and Communication Technologies at the Bulgarian Academy of Sciences*** *presents in an electronic format the abstracts of Doctor of Sciences and PhD dissertations defended in the Institute of Information and Communication Technologies at the Bulgarian Academy of Sciences. The studies provide new original results in such areas of Information and Communication Technologies as Computer Networks and Architectures, Parallel Algorithms, Scientific Computations, Linguistic Modelling, Mathematical Methods for Sensor Data Processing, Information Technologies for Security, Technologies for Knowledge management and processing, Grid Technologies and Applications, Optimization and Decision Making, Signal Processing and Pattern Recognition, Information Processing and Systems, Intelligent Systems, Embedded Intelligent Technologies, Hierarchical Systems, Communication Systems and Services, etc.*

e-ISSN: 1314-6351

BULGARIAN ACADEMY OF SCIENCES

Abstract of PhD Thesis

STUDY OF THE DEPENDABILITY CHARACTERISTICS OF A FAULT-TOLERANT DISTRIBUTED REAL-TIME SYSTEM WITH ADJUSTABLE RELIABILITY

Edita Ananieva Djambazova

Supervisor: Assoc. Prof. Rumen Andreev

Approved by Supervising Committee:

Acad. Vassil Sgurev
Acad. Kirill Boyanov
Corr. M-r. Lyubka Doukovska
Prof. Ivan Kurtev
Assoc. Prof. Petar Popov

IICT

INSTITUTE OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Department of Intelligent Systems

Introduction

Relevance of the study

Real-time systems are implemented in the control of various processes (such as industrial production, automobiles, avionics systems, etc.), where the concept of time is embedded in the production process. They are distributed computer systems having all characteristics that allow them to process data and exchange information with the outside world. They "communicate" with their environment through sensors and actuators and thus they can control real processes. This determines their major characteristic – functioning with time constraints imposed by the environment. Because of their operation between a controlled process in a real physical environment and their computer nature, they are defined as cyber-physical systems. Real-time systems are usually distributed systems which means that they are composed of autonomous components communicating through a communication channel. They are often implemented in safety-critical applications and must obey high dependability requirements considered at their design stage. Dependability is an integral concept that defines trust in the capability of a system to deliver a correct service. All these aspects of real-time systems – to be cyber-physical, distributed, working with time constraints, and fault-tolerant – make their design complex and comprehensive. This generates some research issues that over the years and with the technological progress have found different solutions. The fault-tolerance requirement is a part of the design process. The real-time function defines the dependable distributed systems to operate under a global time base and synchronize all operations with the delivery of a correct service both in the value and the time domain. Their cyber-physical nature requires the fulfillment of various requirements. Often the requirements for fault tolerance and real-time are hard to combine and an acceptable trade-off between them is needed.

Fault tolerance is an irrevocable property of these systems. It is achieved by applying different approaches and techniques for error detection and recovery. To a great extent, they rely on the concept of redundancy. Redundancy is an element of a system's structure without which it can perform its main functions and which assists the system's operation in case of change in its working environment introduced by faults. Redundancy management is important for fault-tolerant systems because it improves their dependability characteristics but at the same time it involves additional elements that have their price in terms of system performance and cost. The introduction of structural redundancy to improve dependability leads to additional delays for synchronization, failure recovery, inclusion and removal of components, etc., which complicates the achievement of real-time requirements. The search for a new approach to redundancy management in dependable distributed systems motivates this Ph.D. research.

Motivation

The dependability requirement to real-time systems for safety-critical applications and the system costs' increase for redundancy motivated the idea of this research to create an architecture of a fault-tolerant distributed real-time system that allows the structural redundancy distribution according to the application requirements – called by the author *a system with adjustable reliability*. The main research question is can the fault-tolerant distributed real-time computer systems achieve flexibility according to the reliability requirements of the application using the proposed approach of adjustable reliability?

The architecture of a fault-tolerant distributed real-time system with adjustable reliability proposed in the thesis is built out of autonomous fault-tolerant components having different redundancy according to their criticality. Component criticality is determined by the component failure severity for the controlled system. The system under study is modeled using a simulation program specifically developed for the research and its dependability characteristics are investigated under different parameters. A scientific and application approach is proposed in the thesis called an approach of adjustable reliability, that determines a hardware structural redundancy distribution following the application requirement for total system reliability. The system and the approach of adjustable reliability propose a way to achieve high reliability through the distribution of the system's hardware resources according to the needs of the application. This makes the fault-tolerant distributed system with adjustable reliability suitable for implementation in domains with various reliability requirements and mixed component criticality, in embedded systems, and less critical applications.

The approach of adjustable reliability has advantages over some well-known systems in achieving higher reliability with the same resources, obtaining high availability, flexibility in the system resources distribution at the design stage, and applicability in compact systems. The modeling of the proposed system with adjustable reliability and its comparison to the models of similar systems shows that there is an opportunity to better distribute the system resources retaining good dependability characteristics.

Scientific attributes of the research

The **object** of the research is dependable distributed real-time systems.

The Ph.D. thesis **subject** is adjustable reliability in fault-tolerant distributed real-time systems.

The **purpose** of this Ph.D. research is to study the dependability characteristics of the proposed fault-tolerant distributed real-time system with adjustable reliability, to compare them to those of the known similar systems, and based on the results to develop an approach (of adjustable reliability) for use in dependable distributed real-time systems.

Hypothesis

Dependable distributed systems achieve fault tolerance by implementing various approaches

at different levels of their architecture. The leading method of their design is the introduction of structural redundancy. There are two main approaches to applying structural redundancy – through specialized hardware and software components and by the use of Commercial Off-The-Shelf software and hardware components. Both approaches achieve fault tolerance against physical faults via hardware component replication and seek flexibility through software component replication. The hypothesis advocated by the Ph.D. thesis is that it is possible to achieve high reliability and flexibility of the system resources' distribution through adjustable reliability, realized by hardware structural redundancy distribution.

To prove the hypothesis the following statements are verified:

1. The fault-tolerant system with adjustable reliability achieves high overall reliability comparable with the reliability of systems without structural redundancy distribution.
2. There are configurations of the system with adjustable reliability that achieve better dependability characteristics than those of systems without structural redundancy distribution.
3. It is possible to identify the conditions under which the fault-tolerant system with adjustable reliability has better dependability characteristics than the compared systems.

Methodology of the research

The Ph.D. thesis applies the basic approaches used in scientific knowledge – analysis, synthesis, comparison, and generalization. A survey of the dependable distributed systems is made in terms of the structural redundancy distribution and their advantages and disadvantages are outlined. Based on this critical analysis, the purpose of this research is set and the leading hypothesis is formulated. A conceptual model is proposed for decision-making in dependability incorporation in systems. Based on the classification of dependable distributed systems the system development life cycle is associated with the design of safety-critical systems.

Following the investigation of the existing dependable systems an architecture of a fault-tolerant system with adjustable reliability is proposed. The modeling methods of dependable systems are surveyed and a research approach is chosen and justified – the simulation modeling. It is implemented by a special software product used to conduct multiple experiments. The obtained results are systemized and analyzed and with their aid, an approach of adjustable reliability is developed. The approach determines the system configurations with overall reliability conforming to the application requirements.

Main tasks of the research

1. To make a study, a survey, and a critical analysis of dependable distributed systems. To synthesize a classification of the existing dependable distributed systems. To outline the research opportunities in structural redundancy distribution.

2. To propose a model and an architecture of a fault-tolerant distributed system with adjustable reliability that gives a solution to the high-reliability requirements of the application.
3. To define a research method for the study of the proposed model. To develop a tool applying the method. To compose a research protocol.
4. To design and conduct experimental research to test and analyze the dependability characteristics of the proposed fault-tolerant system with adjustable reliability using the chosen research approach and developed software product.

Structure of the contents

The Ph.D. thesis is organized into an introduction, four chapters, a conclusion, a bibliography, and two appendices.

In the *Introduction*, the theme, the object, and the subject of the Ph.D. thesis are indicated. The relevance of the study and the motivation behind this research are briefly described. The purpose of the work and the tasks to achieve it are set, as well as the leading hypothesis and the methodology to prove it.

In *Chapter 1*, the basic concepts associated with dependable distributed real-time systems are introduced. The basic methods and techniques to achieve fault tolerance are described. The ways to introduce and manage redundancy are considered. A survey and a critical analysis of the known dependable distributed systems are presented. A conceptual model of an approach to decision-making in providing dependability is derived and a classification of the dependable distributed systems is synthesized. The new research opportunities are outlined.

In *Chapter 2*, the architecture of the proposed fault-tolerant distributed system with adjustable reliability is presented. The modeling methods of dependable distributed systems are also presented, along with the model and the assumptions of the fault-tolerant system with adjustable reliability. The studied dependability characteristics to assess and compare the system to other similar systems are described. The choice of the research approach of simulation modeling is justified.

In *Chapter 3*, the research tasks are described and the simulation results for the fault-tolerant system with adjustable reliability are presented. The developed software program for the simulation of the system with adjustable reliability is introduced. The dependability characteristics of a component and the entire system are investigated: reliability, availability, mean time to failure, mean time to repair, etc. The developed approach of adjustable reliability is introduced. It allows for the selection of the appropriate configuration of the structural redundancy according to the requirements of the application for the overall system reliability.

Chapter 4 constitutes an analysis and discussion of the results. The advantages and the possible applications of the proposed fault-tolerant system with adjustable reliability are pointed out.

The main scientific and scientific and application results of the Ph.D. thesis are derived. The opportunities for further research and implementation of the fault-tolerant system with adjustable reliability are outlined.

The Ph.D. thesis ends with a *Conclusion* where the obtained results are summarized, followed by a *Bibliography* containing 102 sources. In *Appendix A*, the mathematical representations of the dependability characteristics used in the research are presented. In *Appendix B*, the source code of the simulation program NMRSIM is introduced.

Chapter 1. Dependable distributed real-time systems

1.1 Dependability – basic concepts

The notion of dependability is introduced by Jean-Claude Laprie in the 1980s of the 20th century [1], [2] to encompass the different aspects of fault-tolerant systems and to introduce a systematic way to use the concepts associated with the protection against failures in the high-reliability systems. The basic definition of dependability [2,] [3], [4] says that it is "the ability to deliver service that can justifiably be trusted." This definition stresses the justification of trust in the service delivered. In [3], a second definition is added that outlines the importance of failure avoidance: "Dependability is the ability of a system to avoid service failures that are more frequent or more severe than is acceptable."

The specific terminological basis used in the Ph.D. thesis is the established and broadly applied in the dependability field concepts and definitions [3,] [4], [5], and their Bulgarian counterparts [6].

The *service* delivered by a system is its behavior as it is perceived by its user(s) [3]. *Correct service* is delivered when the service implements the system function [3].

1.1.1 Threats to dependability: failures, errors, and faults

The *threats* to computer systems are the causes that lead to deviation from their correct operation. The expression of that deviation at the system level is called service failure [3]. *A failure* is an event occurring when the delivered service deviates from the correct one. The deviation from correct service can take different forms called failure modes and they are ordered according to the *failure severity* – the extent of the failure consequences for the system environment.

Service failure means that at least one (or more) external system state does not conform to the state of correct service. This deviation is called an error. The adjudged or hypothesized cause of an error is called a *fault* [3]. The definition of *error* is part of the overall system state that may lead to its subsequent service failure.

1.1.2 Dependability attributes and means

In the seminal paper [3], the basic concepts and definitions associated with dependability are presented. They are used in the presented research thesis. Here, only the definitions related to the dissertation's theme are cited. According to the terminology established during the last 30 years, dependability is an integral concept that is characterized by the following attributes [3]:

- Availability: readiness for correct service;
- Reliability: continuity of correct service;
- Safety: absence of catastrophic consequences for the user and the environment;
- Integrity: absence of improper system alterations;
- Maintainability: the ability to experience modifications and repairs.

The means to achieve dependability in computer systems are [2], [3] fault prevention, fault tolerance, fault removal, and fault forecasting. Fault tolerance encompasses methods and means aiming at failure avoidance in the presence of faults.

The focus of the Ph.D. thesis is on achieving fault tolerance of distributed real-time computer systems.

1.2 Distributed real-time systems

Distributed systems are built out of components exchanging messages through a communication bus (real-time network) and executing a common control algorithm (*Figure 1-2*). In terms of fault tolerance system components have to ensure that the faults do not propagate towards other components. A system component is a fault-containment unit [17], [19] if the direct effect of a single fault impacts only the operation of a single component [17]. It is assumed that the self-contained units fail independently. This assumption applies for hardware faults that are subject of the presented research.

The system controls an industrial process called the object under control. The components take inputs from the sensors of the object under control, run a control program that calculates some results, and output these results to the actuators of the object (*Figure 1-2*). To fulfill their task, they need to communicate with the other components by exchanging data. System components are designed to have safe behavior, i.e., a fault should not reach the outputs of a component, nor propagate to other parts of the system.

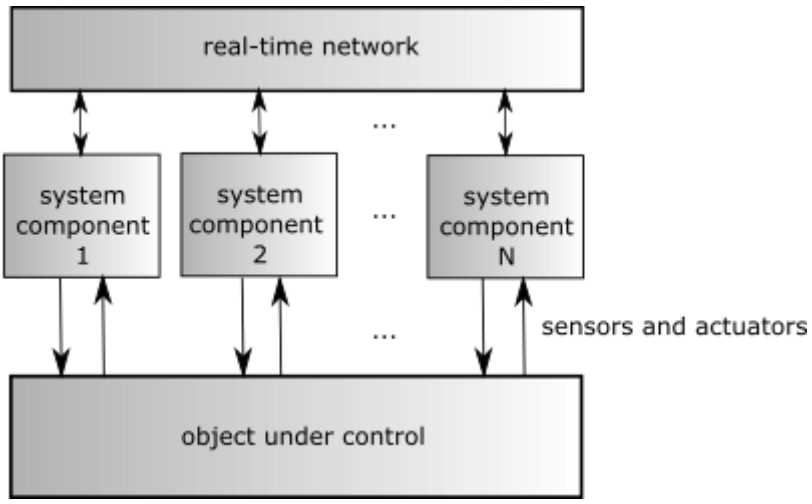


Figure 2. Distributed real-time system

Distributed real-time systems operate with finite time intervals dictated by the environment and the object under control. Their correct service has to be correct both in the value and time domains [17]. This means that the system has to deliver a correct result to the object under control and issue that result within the specified time interval. When the real-time system has to deliver a correct service within a strict time interval the system is *hard real-time* [17]. Otherwise, it is a *soft real-time system* [17]. The system often works under both constraints but if there is at least one hard real-time function, the system is hard real-time. Another classification of the real-time systems is according to the triggering factor that determines the interactions among the system components: event-triggered systems (triggered according to the time instant of a substantial event in the system) and time-triggered systems (triggered according to a time instant in the progress of the physical/real-time) [17]. Dependable distributed systems are often hard real-time and are time-triggered. This allows us to predict their behavior and to efficiently utilize their resources. That type of distributed system is the object of our study.

To achieve fault-tolerant component behavior in dependable distributed systems, they are constructed using replicated modules [17], [21], [22], [23], [24]. A *module* is the smallest replaceable unit in the system. This notion is related to the replication techniques and the method of introducing redundancy in the system. The component-level replication can be hardware- or software-implemented. Additional means for error detection are put in each module [25], [26], [27], [28] called self-checking units. The communication bus itself can also be replicated [25], [29], [30], [31]. The diversity of replication techniques allows one to choose the most appropriate solutions for a specific application.

1.3 Redundancy management in dependable distributed real-time systems

Dependable distributed real-time systems are usually deployed in safety-critical applications.

One of the major requirements for their operation is to be fault-tolerant. Fault tolerance is achieved by using various techniques, most of which are based on redundancy. There are different types of redundancy and techniques of its application.

Introducing redundancy in computer systems as a fault-tolerance method and the replication as its technical realization is well-known and studied [23], [24], [33], [34], [35], [36], [37], [38]. Although redundancy management is a well-studied and broadly implemented fault-tolerance method for many years, the design of new dependable distributed systems, the development of systems of systems, and cyber-physical systems [40], [41] imply a new view and a search for new approaches of redundancy implementation. It would broaden the opportunities for replication application and would help the seeking of optimal and effective solutions compliant with the specific application area.

1.3.1 System design

The distributed system development cycle can be presented as an iterative process [44] which considers the system from two viewpoints: practical and abstract. The practical view of the system is its implementation and the abstract view of the system is its model. These viewpoints of the system have to exchange data with each other to achieve a complete system model that can be validated and verified.

The concept to realize an approach to decision-making for providing dependability of a system by introducing redundancy is shown in *Figure 1-3*. A distributed system controls an industrial process, i.e. the distributed computing environment. The system is subject to faults that disturb its operation and threaten to harm the process under control. The problem with the system's *dependability* becomes a design issue: how to make the system fault-tolerant. Faults are inevitable and unpredictable. Hence, the system should have the resources to deliver its intended service even in the presence of faults. Redundancy is one of the strategies to resolve the problem with the needed fault tolerance. The engineering issues with redundancy implementation have to be combined with the research solutions. In *Figure 1-3* they are united under the name dependability assessment. The models and their parameters depend on the application (e.g., cyber-physical systems, safety-critical systems, automobiles, etc.) and the operational environment, i.e., the distributed computing environment. The dependability attributes are determined based on the particular application. The results obtained from the models' investigation are used in the system's design. The appropriate replication technique is identified.

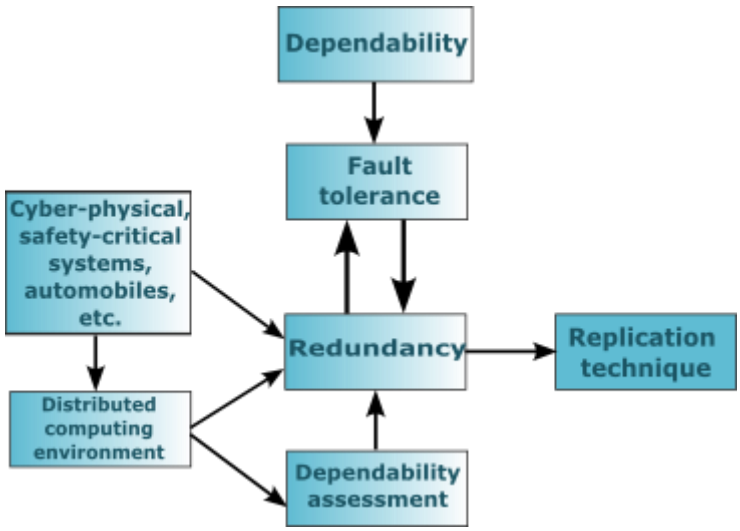


Figure 1-3. Conceptual model of an approach to decision-making in providing dependability

The described general approach gives a view of the dependable systems' design and assists in introducing the fault-tolerance viewpoint. The process of determining a replication technique, shown in *Figure 1-3*, can be used as input data of the scheme of the System Development Life Cycle (SDLC) or be built into it thus specifying the dependability requirements.

1.4 Redundancy in dependable distributed real-time systems

The definition of redundancy used in the Ph.D. thesis is as follows:

Redundancy is a functionality or a component of a computer system that adds resources for the delivery of its correct service.

It is a method of implementing fault tolerance in dependable computer systems and is in turn realized by replication techniques. Redundancy can be structural, time, or functional [23], [33], [34], [37], [38].

1.4.1 Replication style of the structural redundancy

The replication style defines the way the replicated components perform their operation. The fault-tolerant components have replicated modules and only one of them, called primary, issues the output result. The other replicates are secondary. Depending on the replication style the redundancy can be passive or active. Sparing is a passive form of redundancy [23], [33], [35]. The replication is a concurrent operation of identical modules that execute the same functions on the same input data and compare their results [23], [33], [35], [37], [38].

1.4.2 Replication degree of the structural redundancy

The replication degree determines the number of modules in a component. Depending on the importance of a component for the system operation, it can have one or more replicates, or not be replicated at all. The replication degree depends on the fault-tolerance requirements as well.

In hardware, the replication takes the form of *N-modular redundancy* (NMR) [23], [34], [35], [37], [38]. It is mostly applied as dual and triple modular redundancy. In *dual modular redundancy* (DMR), the two replicas compare their results and, in case of discrepancy, the component does not issue any result, remaining fail-silent. Usually, the modules have additional fault-tolerance mechanisms, called *self-checking units*, to decide which module is faulty. In *triple modular redundancy* (TMR), there are three active modules and a voter. The active modules operate simultaneously and the voter determines the majority result that is issued to the object under control.

The replication in software is realized as recovery blocks and N-version programming. In the *recovery blocks* (RB) approach [49], [50], two alternates are produced from a common service specification, and an acceptance test decides whether the result is correct. The acceptance test is applied sequentially to the results of the alternates. If the results of the primary alternate do not pass the acceptance test, the second alternate is executed. The RB approach corresponds to the stand-by sparing in hardware.

In the *N-version programming* [49], [51], [52], there are N (N≥2) variants of the software that are executed simultaneously, and their results are compared. The variants are software routines that are written by different programming teams and possibly using different algorithms. This is supposed to avoid the common errors that programmers tend to do. The results of the software versions are voted upon and the majority result is issued. The hardware equivalent of the NVP is the NMR.

In *N Self-Checking Programming* (NSCP) [49], N self-checking software components are executed; one of them is considered as acting and the other self-checking components are considered as hot spares. Upon failure of the acting component, the operation is switched to a spare self-checking component.

1.4.3 Time redundancy

Time redundancy requires additional time to be allocated to the task execution [23], [37], [53], [54]. It has lower overhead compared to structural redundancy but it may impact the system's performance and should obey the real-time constraints.

1.4.4 Functional redundancy

Functional redundancy is implemented in the software. In [33], it is defined as qualifying the system's behavior relative to its inputs/outputs relationships. Functional redundancy is useful in error detection.

1.5 Redundancy implementation

Dependability in distributed real-time systems for safety-critical applications became a part of their design. All parameters and system components that are important for the fault-tolerant system

operation are included in the SDLC. A descriptive multi-leyer model for distributed systems' design with structural redundancy is illustrated in *Figure 1-4*.

Introducing structural redundancy involves the definition of the critical elements, the important system parameters, and the criticality levels. The components of the distributed system control different parameters of the object under control with different significance for the fault-tolerant operation. At the stage of defining the requirements in the SDLC, the controlled parameters should be defined and the criticality levels should be outlined. The components controlling the important parameters will receive a high criticality level and need to be fault-tolerant.

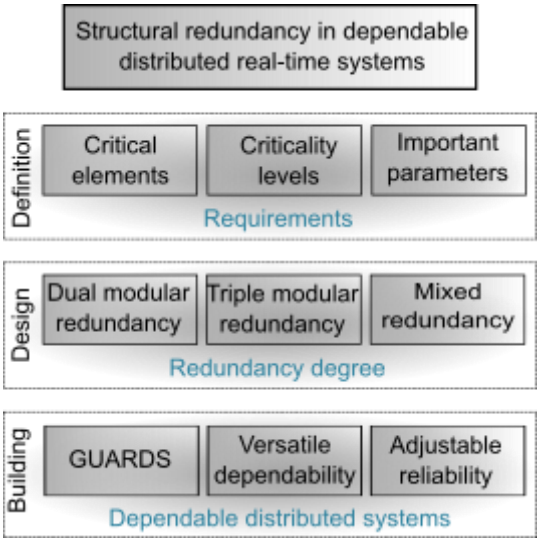


Figure 1-4. Synthesis of an approach to dependable distributed systems with structural redundancy

At the stage of system design, the replication degree and style should be determined. The replication degree defines if single (SMR), dual (DMR), or triple modular redundancy (TMR) components will be applied. The replication style chosen determines whether active or passive replication will be used. Modules in system components can be evenly distributed, i.e., all components can have an equal number of modules, or can use mixed redundancy. The actual building stage of the SDLC implements the decided system architecture, e.g., GUARDS [56], [57], versatile dependability [47], [48], or DECOS [58], [59], as shown in *Figure 1-4*.

1.6 Implementing different replication degrees

1.6.1 Equal redundancy for all components

The most straightforward way of applying redundancy is to replicate the active components and compare their results. In distributed systems, the nodes can be built out of two or three identical modules executing the same task (*Figure 1-5*). The results of the replicas are compared (as in [25], [28], [49], [58]) or voted in the case of TMR (as in [17], [62]). If no discrepancy is shown, the presumably correct result is issued to the object under control. In case of a mismatch, the result is not

issued and the node is put in a safe state according to the system conventions.

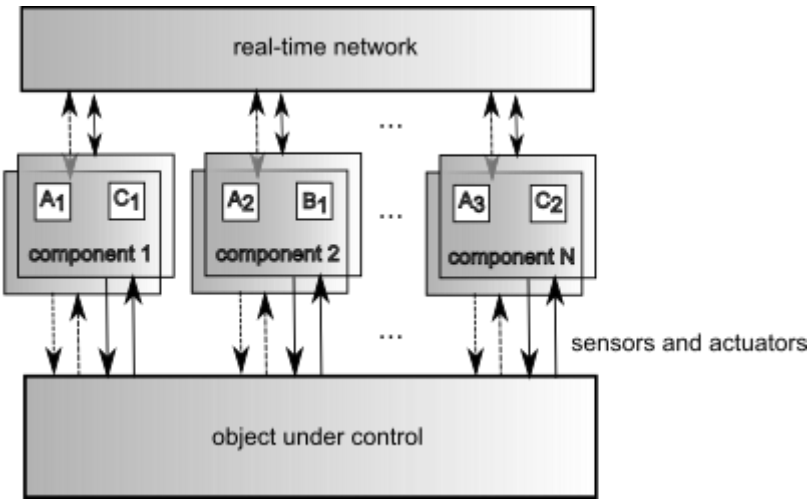


Figure 1-5. Dependable distributed real-time system

The system's hardware components have equal replication degrees but the software components (execution tasks) may have different redundancy. For example, there are three tasks in *Figure 1-5* – A, B, and C; task A has three replicates, task B has one, and task C has two. The replicates may reside on different system components, thus allowing for error isolation.

1.6.2 Different redundancy for the components

Some systems use different degrees of replication for their components. In GUARDS [57], there are integrity levels and criticality levels. The integrity levels are defined according to the degree to which a system component can be trusted – the more trustworthy a component is, the higher its integrity level [56]. The degree of trust placed on a component depends on its criticality. Critical components are considered those whose failure leads to severe consequences. They have a higher integrity level.

The DEAR-COTS model of replication [28], [66] uses active redundancy of the software components and allows for defining the replication degree of specific parts of the real-time application accordingly to the reliability of the components and the desired level of reliability for the application. The DEAR-COTS architecture is intended for distributed computer-controlled systems that operate in real-time and can use both equal and mixed redundancy distribution.

The DECOS project [58], [59] proposes an integrated distributed architecture to support mixed-criticality systems. Mixed-criticality systems consist of distributed application parts with different criticality levels on top of the same physical hardware.

The MEAD system [48] proposes a combination of the conflicting requirements of fault tolerance and real-time for dependability implementation in the middleware. MEAD is an infrastructure that offers transparent and tuneable fault tolerance in real-time, proactive dependability,

system adaptation to crash failure, communication and time faults considering the system resources, and scalable and fast fault detection and recovery. The tuneable fault tolerance is achieved by the so-called approach of versatile dependability [47], [48]. This is an approach to building dependable software architectures considering three important aspects – fault tolerance, performance, and resources. It provides a set of tools, called "knobs", for tuning the trade-offs between these aspects.

Most of the dependable distributed real-time systems follow the architectural style depicted in *Figure 1-5*. They employ equally replicated physical components and mixed redundancy of the software components. There are opportunities to develop systems that adapt to particular applications using a distribution of the hardware structural redundancy.

1.7 Conclusions and results

In *Chapter 1*, the basic concepts of the research area – dependable distributed real-time systems - are presented. Their structure is outlined in terms of dependability and real-time. Structural redundancy management is considered through the prism of system design. A conceptual model of an approach for decision-making to provide dependability is developed. This model fits into the system development life cycle and responds to the requirement to consider dependability as part of the system's specifications.

A brief survey is made of the known dependable distributed systems in terms of structural redundancy management. The two tendencies are to use equal redundancy for all system components or the components to have different redundancy.

The presentation in *Chapter 1* reflects the execution of task 1 of the dissertation.

The achieved scientific and scientific and application results are:

1. A conceptual model of an approach to decision-making to provide dependability is developed.
2. A synthesis of a classification of dependable distributed systems with structural redundancy is proposed.

Chapter 2. Modeling of the fault-tolerant distributed system with adjustable reliability

The architecture of the system with adjustable reliability proposed in the Ph.D. thesis is based on the notion of adjustability.

Adjustability is the property of a dependable distributed real-time system to distribute the structural redundancy according to the reliability requirements of the application.

The fault-tolerant distributed system with adjustable reliability [73], [74], [75], [76] applies

different replication degrees to the hardware components (*Figure 2-1*).

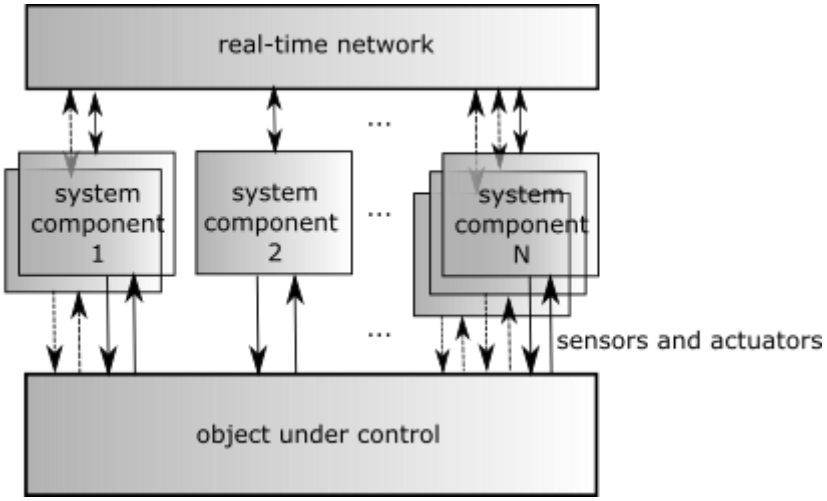


Figure 2-1. The dependable distributed real-time system with adjustable reliability

The necessity to have components with different replication degrees is related to their criticality. Unlike the approaches implementing mixed criticality of the software application parts executed over evenly replicated hardware, the reliability adjustment approach proposes a component's redundancy degree to be determined according to its criticality at the design stage and the fault-containment components to operate with mixed redundancy. A quantitative assessment of the implementation opportunities of dependable distributed systems with the proposed approach is made in the Ph.D. thesis and they are compared to the systems without structural redundancy distribution. The comparison is conducted using models solved through simulation modeling, and the results (presented in *Chapter 3* and [76]) show that there are redundancy distributions that achieve the total system reliability required by the application.

The fault-tolerant distributed system with adjustable reliability (*Figure 2-1*) is built out of components whose fault tolerance is guaranteed by replication and self-checking. The components can have different degrees of replication depending on their criticality. Each module has a self-checking unit that detects errors and provides fail silence. The system operates under hard real-time constraints. This approach allows for the predictability of the system's behavior as the execution times of the system tasks are guaranteed. By changing the component structural redundancy at the design stage a change of systems' reliability according to the requirements of the application is aimed. Hardware faults are modeled and the goal is to achieve hardware reliability.

2.1 Analysis of the approaches of dependable systems modeling

Modeling is a commonly used approach to system investigation before the system is designed and implemented. This allows for checking different hypotheses and finding the appropriate model based on which to seek specific engineering solutions. Modeling allows comparing different variants to building a system or parts of a system in a cost-efficient way because the possible engineering

realizations are not always quantitatively assessable in complex systems.

Because of the stochastic nature of faults, the indicators, by which their impact on the dependable systems' operation is assessed, are probabilistic. For this reason, their description uses concepts and terms from probability theory and mathematical statistics.

2.1.1 Modeling methods for dependable systems

System models can be analyzed and mathematically evaluated through three different approaches [77]: simulation, analytical, and hybrid (a combination of simulation and analytical methods). Only the basic properties of a system are modeled. In the simulation, the system is described in a computer program that imitates its dynamics. In the analytical methods, systems of equations determining the system's dynamics are constructed and solved [77], [78], [79], [80]. The advantage of the simulation is that the properties of the studied system can be presented in detail without imposing too many constraints on the model. In analytical models, the assumptions are often relaxed to solve the system of equations. The accuracy of the simulation is restricted only by the time it takes to obtain the final result. The combined application of both approaches is possible but is not often used [77].

In another classification [81], the models are classified as combinatorial and state-space-based models. *Combinatorial models* include reliability block diagrams [77], [82], [83], [84], event trees [81], and fault trees [77], [85], [86]. They are comparatively easy to design and handle and can be analyzed with combinatorial methods. Their drawback is the limited modeling power due to the assumption of statistically independent events.

State-space-based models include Markov chains and Petri nets [84], [87]. They represent the system's behavior by reachable states and possible transitions among them. They have greater modeling power than the combinatorial models which cannot encompass the characteristics of the modeled system.

The problem with the state-space-based methods is the so-called effect of "explosion" of the state space – an exponential increase of the state space with the increase of the number of components. This raises the computation cost. In that case, the Petri nets and the Markov chains can be simulated [81].

2.1.2 Dependability characteristics of the fault-tolerant system with adjustable reliability

As part of the requirements of the simulation program for modeling the fault-tolerant system with adjustable reliability the following characteristics are calculated: reliability *R*, mean time to failure *MTTF*, mean time to stop *MTTS*, overall downtime, mean time between failures *MTBF*, mean time between stops *MTBS*, mean time to repair *MTTR*, and availability *A*.

The most commonly used distribution function in fault-tolerant systems' modeling is the

exponential distribution. It is suitable because of its property of not having a memory of the system state. The exponential distribution reflects to a satisfying extent the dependable systems' dynamics and offers a suitable mathematical representation. It is also assumed in the modeling that the fault rate is constant [84].

Reliability is the probability of the system being operational at time *t*. Under the assumption of exponential distribution of the events in the system, the distribution function becomes [37], [84]

$$F(t) = 1 - e^{-\lambda t}. \quad (1)$$

The distribution density is [37], [84]

$$f(t) = \lambda e^{-\lambda t}. \quad (2)$$

System reliability is expressed as an exponential function [37], [84]

$$R(t) = e^{-\lambda t} = 1 - F(t). \quad (3)$$

The Mean Time To Failure *MTTF* can be computed as the mean value of the time to component failure for a given period. It is the mathematical expectation of the time to (first) failure. With a constant fault rate *MTTF* is [37], [84]

$$MTTF = \frac{1}{\lambda}. \quad (4)$$

The Mean Time Between Failures *MTBF* can be calculated as the mean arithmetical time between the system failures. *MTBF* is measured for repairable systems. With exponential distribution and a constant fault rate $MTBF=1/\lambda$.

The Mean Time To Repair *MTTR* represents the mean time required to repair failed system components. With exponential distribution and a constant fault rate

$$MTTR=1/\mu. \quad (5)$$

Availability *A* is measured with the probability of the system being operational at time *t* independently of how many times it has been inoperational during the interval (0,*t*). For constant fault and repair rates the availability can be expressed as follows [37], [84]

$$A = \frac{\mu}{\lambda+\mu} = \frac{MTBF}{MTBF+MTTR}. \quad (6)$$

The overall downtime is the sum of all periods during which the system has been inoperational. The mean downtime is expressed with (П12) (*Appendix A*).

The system operates under the following definitions of failure and stop. A system *failure* occurs when more than half of the components fail with an undetected failure or when, in case of more than half of the components failed, the majority have failed with an undetected failure.

$$N_u > \frac{N}{2} \text{ or } N_u + N_d > \frac{N}{2} \text{ and } N_u \geq N_d, \quad (7)$$

where N_u is the number of components with undetected failure and N_d is the number of components with detected failure. The system stops when more than half of the components fail with detected failure or when, in case of more than half components failed, the majority have failed with a detected failure.

$$N_d > \frac{N}{2} \text{ or } N_u + N_d > \frac{N}{2} \text{ and } N_d > N_u. \quad (8)$$

2.2 Assumptions for the system modeling

The model of the fault-tolerant system with adjustable reliability is based on assumptions reflecting its behavior and the fault, failure, and repair modes adopted in the research.

The distributed system with adjustable reliability [73], [74], [75], [76] is built out of components operating in active redundancy. The components have homogeneous modules each of which has self-checking tools with coverage *C*. The replication degree of the components is determined by their criticality – the more important the component for the application, the more critical it is and its replication degree is higher. Three levels of criticality are considered. The components whose failure does not threaten the normal system operation and does not lead to catastrophic consequences can rely only upon their self-checking tools and do not have to be replicated. Their coverage is C_1. The components with bigger criticality for the application but for which it is enough only to stop issuing results in case of a failure are DMR components. For them, it is possible the failed module to be repaired if its failure is detected by the self-checking unit. The DMR components have a coverage factor $C_2 > C_1$. The most critical system components whose failure could have catastrophic consequences for the application are built out of TMR modules and have coverage factor $C_3 > C_2 > C_1$.

The fault-tolerant system with adjustable reliability tolerates permanent hardware faults with fault rate λ_p. In DMR and TMR components, a recovery (local repair) after a module failure with a repair rate μ_p is possible. The system can operate with or without repair and the repairable system has a repair rate μ_{sys}.

2.3 Model of a system component

The component of the distributed system with adjustable reliability is built out of homogeneous modules M_i (i=1, 2, 3), each of which has its own self-checking unit SC_i (*Figure 2-2*) [94]. Depending on their criticality the modules can be with DMR or TMR to achieve bigger

reliability at the point of the control loop where the component is allocated.

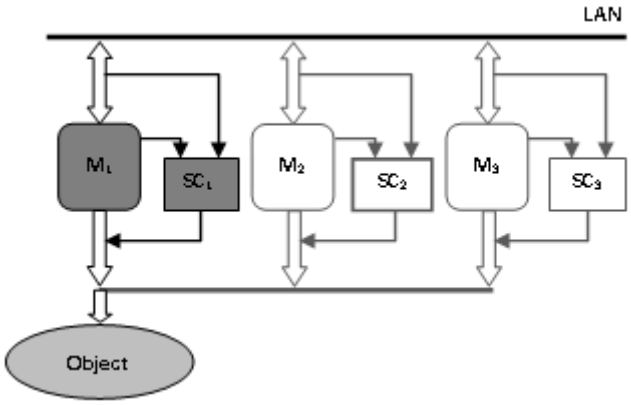


Figure 2-2. Component of the distributed system with adjustable reliability

One of the modules is primary and is the only one that issues the result to the object under control. All modules run the control program concurrently and calculate the output result (active redundancy). The modules that do not issue a result to the object control the primary module and participate in the comparison of the results. They can take over the control in case of failure of the primary module.

In the case of a single module, only the self-checking tools can detect an error in the control program execution and disable the outputs. If the application requires a stronger defense of the outputs and greater fault coverage, additional one or two modules are attached to the single one with their self-checking units, thus allowing it to respond to different criticality levels dictated by the application of the fault-tolerant distributed system with adjustable reliability.

2.3.1 Functions of a system component

A characteristic of the proposed system is the integration of a local self-checking unit in each module, the realization of a protocol for distributed voting, and state control. The self-checking unit [73] is built in as an additional unit to the module configuration and has controlling and checking functions.

2.3.2 Failure mode

The component fails when all its modules fail. Thanks to the introduction of self-checking units and redundancy not every undetected module failure leads to a component failure. There are two states in case of a module failure – stop and failure.

2.4 System model

The system operation is represented with a Markov process where each state in the Markov chain depicts the system state after a fault according to the number of the operational components N and the arcs are the transitions between the states in case of permanent fault occurrence with fault rate λ_p. The coverage factor of the self-checking tools is C. Different operational modes of the system

are considered: with and without permanent fault recovery and with and without system repair.

When the system is without repair, it operates until its resources are exhausted and the impact of the coverage factor *C* on the reliability is unnoticeable (*Figure 2-3*).

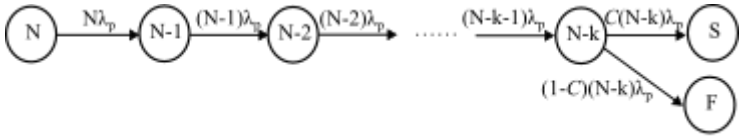


Figure 2-3. A Markov model of a system without permanent fault recovery and repair

If the system can perform local repair, *C* helps extend the component's life and this impacts the system's reliability. The influence of *C* increases because only in case of a detected component failure the component can be repaired before a system failure. A system repair is performed after the system enters a stop state. The operational components continue to function after the repair with the same initial characteristics. The fault-tolerant distributed system with adjustable reliability can operate with system repair and component recovery from a permanent fault (*Figure 2-6*). This implies the achievement of better dependability characteristics.

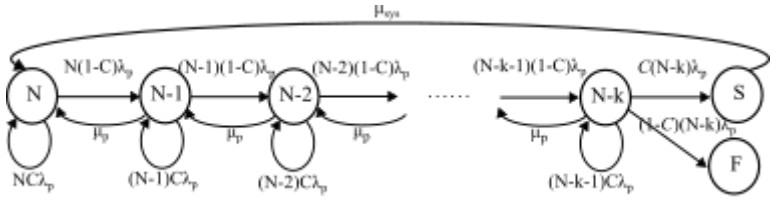


Figure 2-6. A Markov model of a system with repair and recovery from a permanent fault

All described operational modes in the Markov models (*Figure 2-3* - *Figure 2-6*) are studied through the simulation modeling of the system.

2.5 Conclusions and results

In *Chapter 2*, the developed fault-tolerant distributed system with adjustable reliability is presented. It offers different replication degrees of the hardware components. The necessity for the system to have different replication degrees is related to their criticality which is determined by the application requirements. The fault-tolerant system with adjustable reliability is modeled under some assumptions for its operation to check this hypothesis.

The proposed fault-tolerant distributed system with adjustable reliability is modeled based on Markov chains and is validated through simulation. The method of simulation modeling is chosen for its capability to model systems with many components and a great degree of detail. The models of a system component and the entire system are presented. Possibilities are envisioned to model the system with adjustable reliability with and without permanent fault recovery, as well as with and

without repair.

The results presented in *Chapter 2* fulfill tasks 2 and 3 of the Ph.D. thesis. The obtained scientific results are the development of a simulation model of the proposed fault-tolerant distributed system with adjustable reliability and the presentation of a new architectural model of a fault-tolerant distributed system with adjustable reliability, as the requirements to its components and the system as a whole are also defined.

Chapter 3. Study of the fault-tolerant system with adjustable reliability

The fault-tolerant system with adjustable reliability controls an object receiving input data from its sensors, executes a control algorithm, and computes output results to issue to the object's actuators. The parameters of the object under control can be of different importance for the correct system operation. Hence, the system components are replicated according to their criticality level. The adjustment of the system's reliability through the distribution of the components' replication degree according to the needs of the controlled object can utilize system resources more effectively and could improve its reliability.

The simulation modeling of the system with adjustable reliability studies how the change of the structural redundancy influences the overall system reliability. The components with different replication degrees have different criticality levels. This determines the coverage factors of their self-checking tools: C_1 for the single components, $C_2>C_1$ for the DMR components, and $C_3>C_2>C_1$ for the TMR components. The coverage factors can change depending on the environmental or operational conditions within some boundaries. These coverage factors along with the fault rate λ_p determine the components' behavior in the simulation model of the fault-tolerant system with adjustable reliability. The events in the system are related to the change of its state. They are random events characterized by the corresponding fault rate: λ_p, μ_p, and μ_{sys}. It is assumed that a failed component can always be recovered after a permanent fault (local repair) and the times to failure are normally distributed.

The following *research protocol* is developed:

1. Study of a component
2. Study of the system
    a. Input data: number of system components *N*, number of modules in the system *M*, λ_p, μ_p, μ_{sys}, boundaries of the coverage factors C_1, C_2, and C_3.
    b. Output results: *R*(*t*), *A*, *MTTF*, *MTTR*, *MTTS*, *MTBF*, *MTBS*, *downtime*
3. Determining the times to failure for the input parameters and all modular redundancy

distributions of systems with and without adjustment of the structural redundancy.

4. Study the impact of different parameters on the dependability characteristics of the fault-tolerant system with adjustable reliability and systems without structural redundancy distribution.
5. Depending on the results determine the configuration with the highest system reliability.

3.1 Simulation modeling of the fault-tolerant system with adjustable reliability

The research method of simulation modeling chosen in *Chapter 2* is applied by the development of a simulation program. It is designed according to the described research protocol and determines the dependability characteristics of the studied system, formulated in § 2.1.2. The program simulates fault-tolerant systems with different distributions of the structural redundancy and systems without distribution of the structural redundancy, which allows their comparison and analysis.

3.1.1 The simulation program

The developed software product NMRSIM for the simulation of the behavior of fault-tolerant distributed systems (presented in more detail in *Appendix B*) determines the properties of the systems of consideration and allows the comparison of the proposed system with systems without reliability adjustment. The program is written in C++ and its development fulfills the following requirements:

1. To simulate the system's behavior in time reflecting the definitions of stop and failure;
2. To represent the occurrence of a permanent fault as a stochastic process with exponential distribution and fault rate λ_p;
3. To be able to model systems with and without repair;
4. To represent the instants of repair as a stochastic process with exponential distribution and repair rates μ_p (local repair) and μ_{sys} (system repair);
5. To model a system with an arbitrary number of modules and components;
6. To calculate the dependability characteristics, determined in *Chapter 2*, § 2.1.2;
7. To model the behavior upon the fault of a component and the entire system;
8. To distribute the structural redundancy for a given number of components and a given number of modules;
9. To model the coverage factors of the self-checking tools;
10. To calculate the reliability as a function of time;
11. To compute the statistical values of the obtained results;
12. To store the obtained results.

The software product for simulation modeling of the proposed fault-tolerant system with adjustable reliability is based on modeling of the system operation in time and the instants of fault

occurrence. The block structure of the simulation program is depicted in *Figure 3-2*. In the block of input data, the following parameters are given: N, M, λ_p, μ_p, μ_{sys}, C_1, C_2, C_3, and R_{total}. The program uses a pseudorandom number generator executing the algorithm presented in [98]. It is used to determine the instant of fault occurrence and to generate random values of the coverage factors. For given N and M in the block for determining the structural redundancy distributions all possible distributions are determined. The block for determining a component fault determines the instants of fault occurrence for the respective component. The current fault is determined in the respective block after a comparison of the instants of fault in all components.

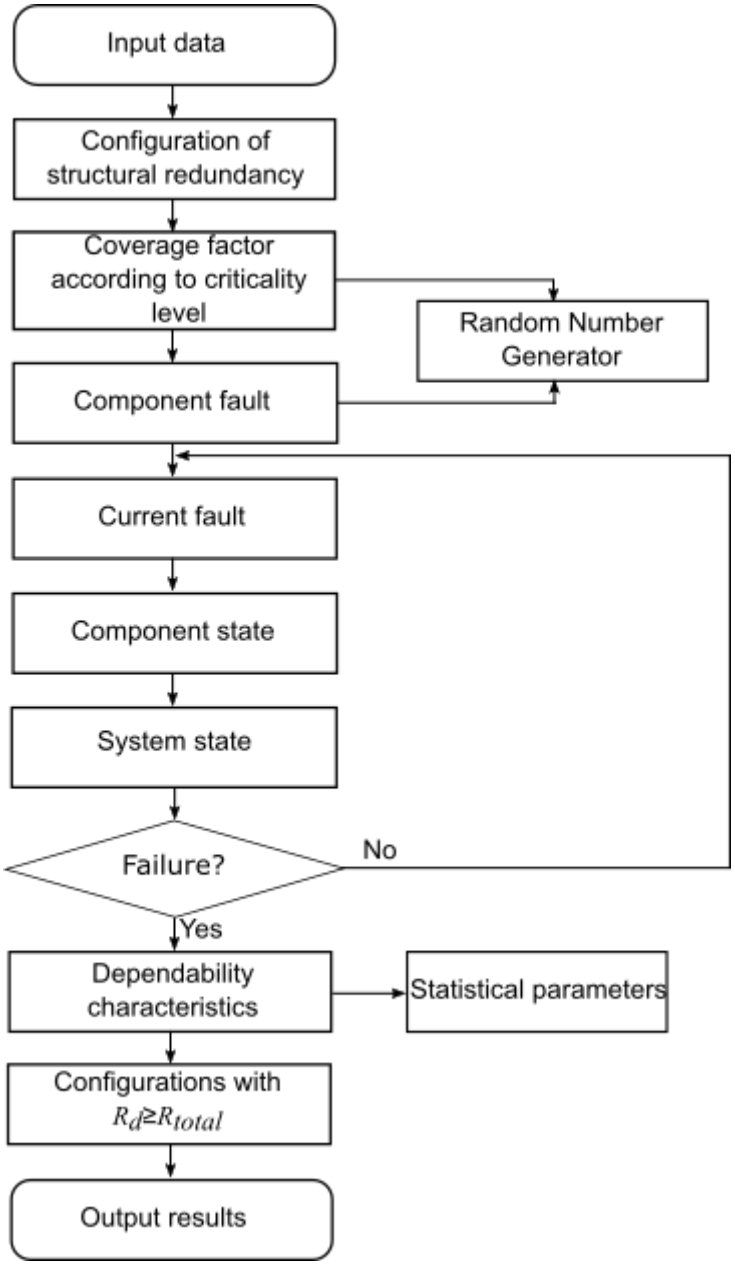


Figure 3-2. Structure of the simulation program NMRSIM

Depending on the replication degree in the block for determining the coverage factors the coefficients C_1, C_2, and C_3 of the components are given. In the block for determining a component's state, it is determined if the component has failed, if its failure is detected, or if it is on repair. In the

block for determining the system's state, is determined whether the system is in a stop or failure state. In the advent of system failure, all accumulated times to failure are recorded and the dependability characteristics are calculated. If the system is in a stop state, the iteration continues and the time of stop is recorded.

In the block for calculation of the dependability characteristics, the following parameters are determined: *R*, *MTTF*, *MTTR*, *MTBF*, *MTBR*, *MTTS*, *MTBS*, *A*, and *downtime*. To realize the approach of adjustable reliability the block for determining the configurations is used. The configurations that achieve the given system reliability R_{total} are identified. All obtained data are statistically handled in the block for determining the statistical parameters. The results for the dependability characteristics of all configurations of the structural redundancy are recorded in files. This is done in the block of output results. The relations among the blocks in the simulation program are schematically depicted in *Figure 3-2*.

The block structure of the program allows its extension and upgrade to model other dependable distributed systems.

3.2 Results of the system simulation

The fault-tolerant system with adjustable reliability is simulated with the following parameters: number of components *N*=10 and *N*=20, number of modules *M*=20 and *M*=40, respectively, permanent fault rate $\lambda_p=10^{-3}$ 1/h and $\lambda_p=10^{-4}$ 1/h, local repair rate μ_p=0.1 1/h, system repair rate μ_{sys}=0.1 1/h, coverage factor boundaries $C_1 \in [0.8, 0.9)$, $C_2 \in [0.9, 0.95)$, and $C_3 \in [0.95,\ 1.0)$.

During the study of the different structural redundancy distributions, the following notation is used:

system (*i*, *j*, *k*),

where *i* – the number of single components, *j* – the number of DMR components, and *k* – the number of TMR components. For example, system (3,4,3) for *N*=10 and *M*=20 means a system with 3 single, 4 DMR, and 3 TMR components.

Structural redundancy distributions are studied that preserve the total number of modules in the systems. The hypothesis of this Ph.D. research implies investigation of the opportunities to distribute the system hardware resources according to their criticality under specified reliability requirements, compliant with the application. As a reference system for comparison the system built out solely of DMR components is chosen since it does not distribute the structural redundancy. In that case, the number of modules in the system is *M*=2*N*. Only the configurations satisfying this condition are considered.

3.2.1 Study of a component

The results of the simulation modeling are presented for a component built out of two and three modules. The dependability characteristics are obtained for a component with and without local repair. The impact of permanent and transient faults is studied. The data are for the following fault and repair rates: permanent processor faults $\lambda_p=10^{-2}$ 1/h, transient processor faults $\lambda_t=10^{-1}$ 1/h, processor recovery after a permanent fault μ_p=0.1 1/h, component repair μ_c=0.1 1/h.

For a DMR component, the fault tolerance is achieved by the self-checking units of the two modules (with coverage factor *C*) and by comparison of the results of the modules. The component *fails* when both processors of the modules fail simultaneously **and** the self-checking units have not detected the failure. The component is in a *stop state* when the comparison indicates a difference but the self-checking tools *have not* detected the failure.

In *Figure 3-3 – Figure 3-10*, the dependability characteristics of a DMR component are shown as a function of the coverage of the self-checking tools *C* and the coefficient of recovery after a transient fault C_r for a system with local repair. For low and high values of the coverage factor, the DMR component has higher reliability and *MTTF* (*Figure 3-3* and *Figure 3-4*) than for average values of that factor. This is due to the influence of the comparison which for low values of *C* practically neutralizes the coverage since in the comparison the component faults are detected with probability 1. For high values of *C*, the fault coverage has strong importance for the better dependability characteristics of the component. The coverage factor of the self-checking units improves the component availability (*Figure 3-9*).

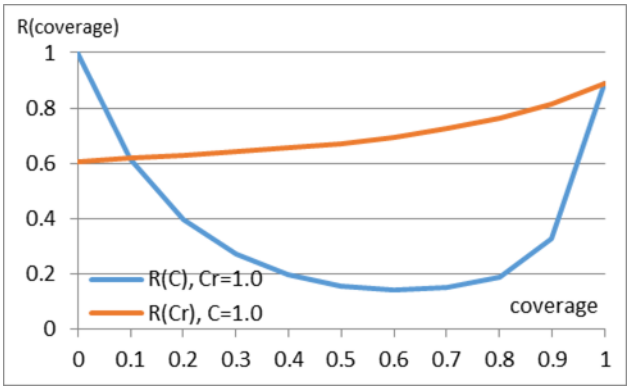


Figure 3-3. Reliability of a DMR component of a system with local repair

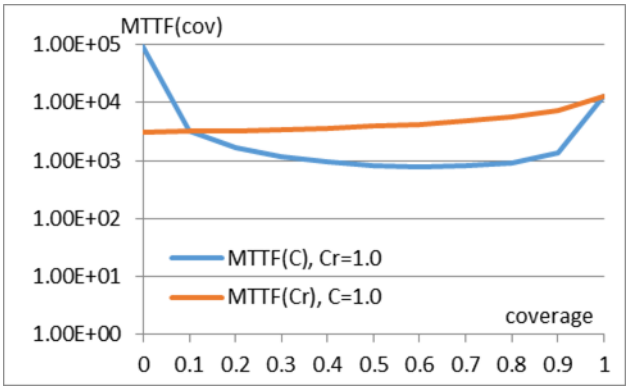


Figure 3-4. MTTF of a DMR component of a system with local repair

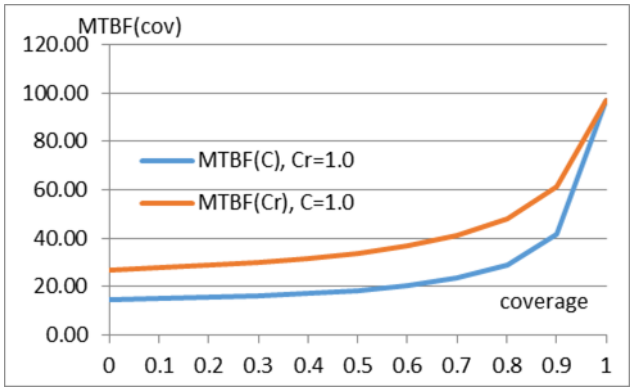


Figure 3-8. MTBF of a DMR component of a system with local repair

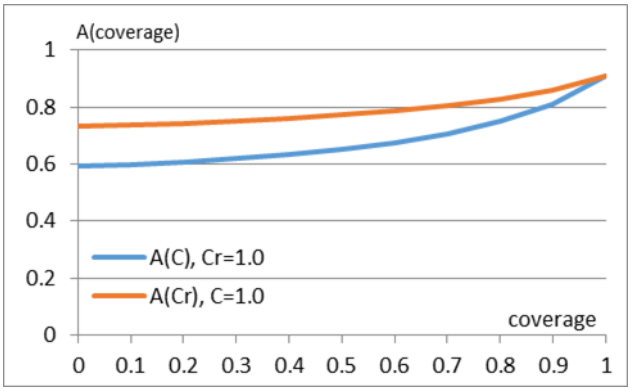


Figure 3-9. Availability of a DMR component of a system with local repair

For a TMR component, the fault tolerance is also achieved through the self-checking units and the comparison is a majority voting. A *failure* occurs when more than half of the modules have an undetected fault. The component is in a *stop* state when more than half of the modules are with a detected fault. In *Figure 3-13 – Figure 3-20*, the dependability characteristics of the component are shown for a system with local repair. The coverage C_r has little influence on the majority of the dependability characteristics of the TMR component (*Figure 3-13 - Figure 3-16*). It decreases the times between failure and the availability of a component (*Figure 3-17 - Figure 3-20*).

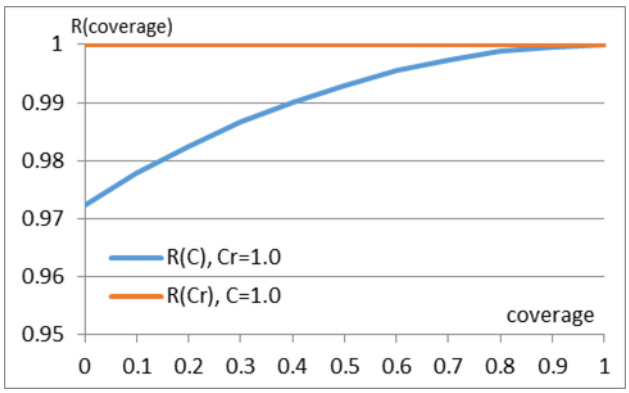


Figure 3-13. Reliability of a TMR component for a system with local repair

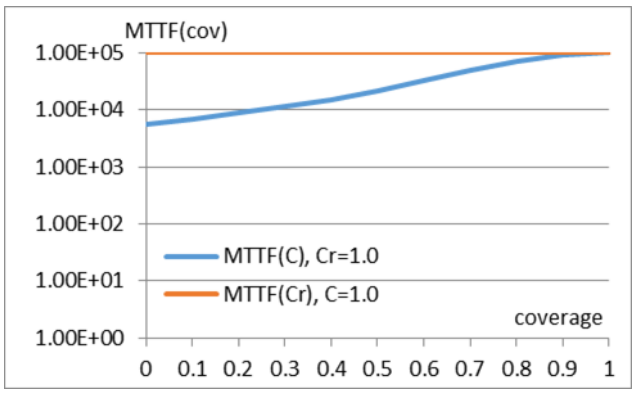


Figure 3-14. MTTF of a TMR component for a system with local repair

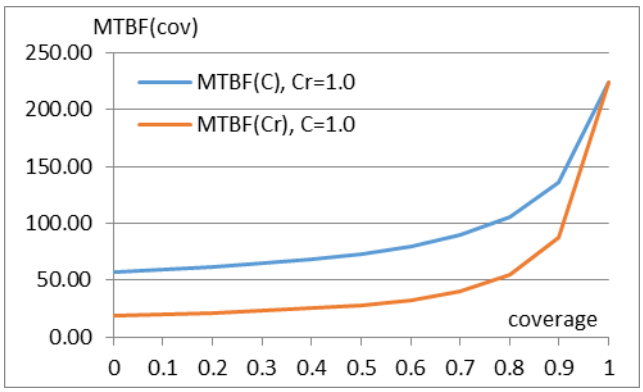


Figure 3-19. MTBF of a TMR component for a system with local repair

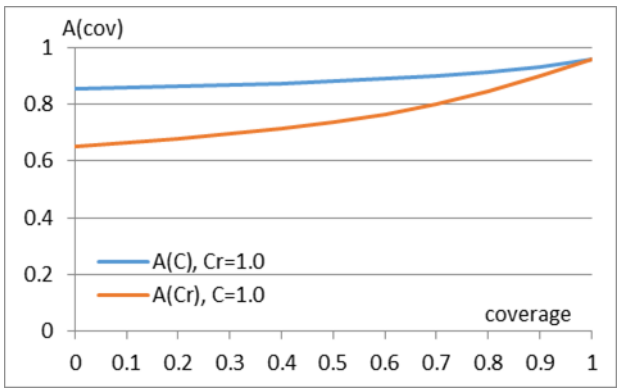


Figure 3-20. Availability of a TMR component for a system with local repair

The coverage factor of the self-checking unit improves the reliability and the time to failure (*Figure 3-13* and *Figure 3-14*), as well as the characteristics related to the component operability (*Figure 3-19* and *Figure 3-20*).

From the conducted study of a DMR and a TMR component of the fault-tolerant distributed system, it can be concluded that the addition of self-checking units to each component's module improves the system's dependability characteristics.

3.2.2 System with 10 components

The system can recover after a permanent fault of a component and to be repaired after a system failure. Six configurations of structural redundancy are studied. Their reliability for C_1=0.88, C_2=0.94, and C_3=0.99 is shown in *Figure 3-23*. The values of the coverage factors with different replication degrees, C_1, C_2, and C_3, are maximal for the study.

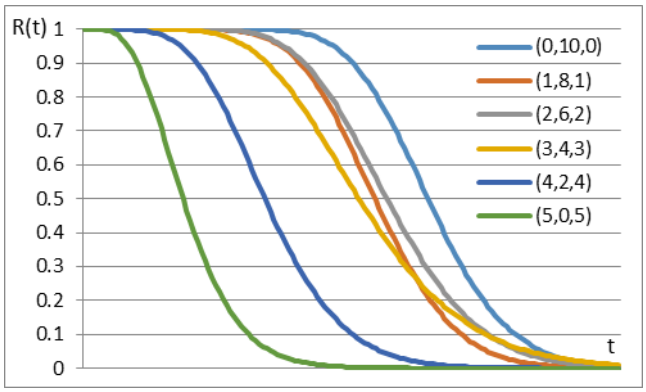


Figure 3-23. Reliability of system with 10 components for C_1=0.88, C_2=0.94, and C_3=0.99

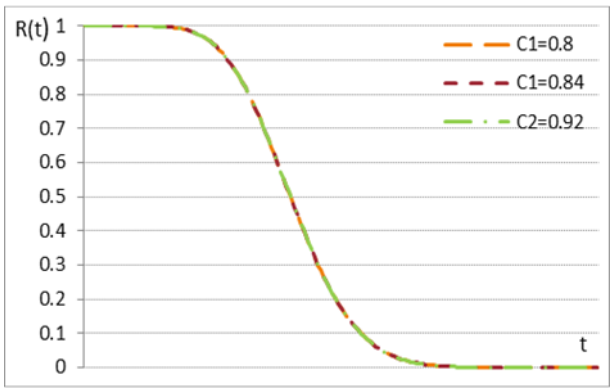


Figure 3-24. Reliability of system (3,4,3) for different values of C_1, C_2=0.94 and C_3=0.97

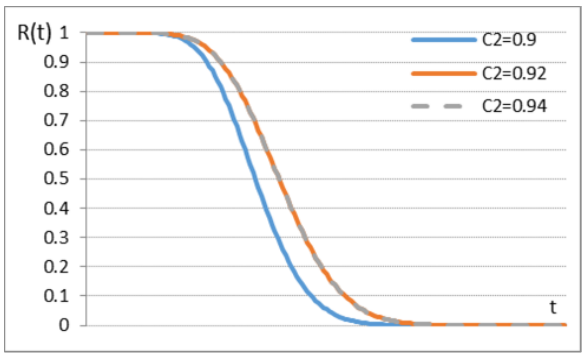


Figure 3-25. Reliability of system (3,4,3) for different values of C_2, C_1=0.88 and C_3=0.97

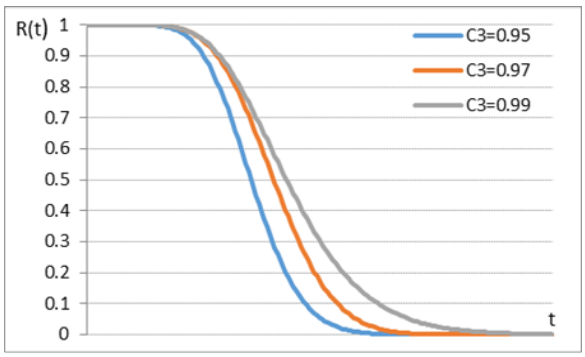


Figure 3-26. Reliability of system (3,4,3) for different values of C_3, C_1=0.88 and C_2=0.94

Under these conditions, the best reliability has the system (0,10,0) (the light blue curve in *Figure 3-23*). This system represents the known systems that operate only with DMR components, i.e., without structural redundancy distribution. The lowest reliability has system (5,0,5) (the green curve in *Figure 3-23*), which is built out only of single and TMR components. Systems (1,8,1) (the orange curve in *Figure 3-23*) and (2,6,2) (the gray curve in *Figure 3-23*) have close reliability values. System (3,4,3) (the yellow curve in *Figure 3-23*) has close reliability to that of systems (1,8,1) and (2,6,2). The systems (3,4,3), (2,6,2), and (0,10,0) are worth considering since they have comparatively high reliability.

The reliability of the system (3,4,3) is studied to trace the influence of the components' coverage factors (*Figure 3-24* - *Figure 3-26*). The coverage factor of the single components C_1 does not influence the reliability of the system (3,4,3) – the reliability curves for the three values of C_1 coincide (*Figure 3-24*).

System (2,6,2) is more strongly influenced by the increase of the coverage factor C_2 (*Figure 3-28*) than by the increase of C_3 (*Figure 3-27*). This is explained by the bigger number of DMR components compared to the number of TMR components. The results for C_3=0.95 (the blue curve in *Figure 3-28*) and C_3=0.97 (the orange curve in *Figure 3-28*) are almost identical. Only the greatest value of C_3=0.99 leads to an improvement in the system reliability (the gray curve in *Figure 3-28*). On the other hand, the increase in the coverage factor C_2 leads to a significant improvement in reliability (*Figure 3-27*).

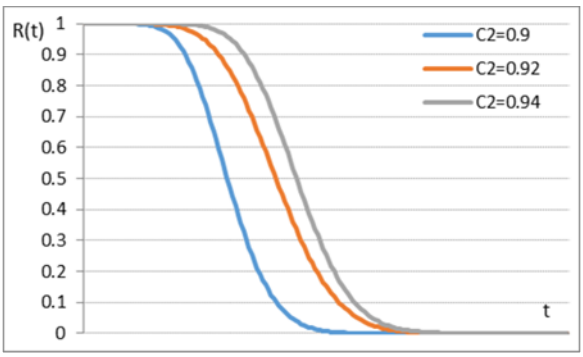


Figure 3-27. Reliability of system (2,6,2) for different values of C_2, for C_1=0.88 and C_3=0.97

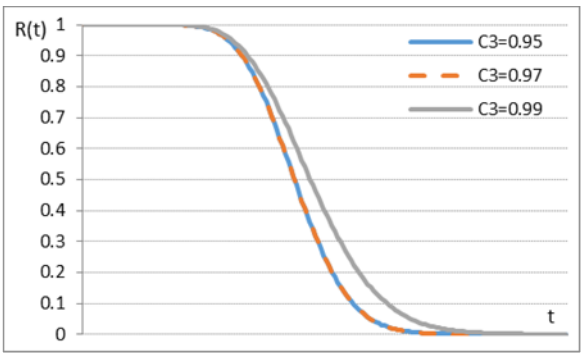


Figure 3-28. Reliability of system (2,6,2) for different values of C_3, for C_1=0.88 and C_2=0.94

In *Figure 3-29* and *Figure 3-30*, a comparison is made of the reliability of systems (3,4,3), (2,6,2), and (0,10,0) for C_1=0.88 and C_2=0.94, while the coverage C_3 is different (C_3=0.97 in *Figure 3-29* and C_3=0.99 in *Figure 3-30*). The best reliability has the system built out solely of DMR components (0,10,0). The system (3,4,3) has the lowest reliability which improves as C_3 increases (*Figure 3-30*, C_3=0.99). The system (2,6,2) shows average reliability. It can be concluded that the systems with a prevailing number of DMR components, (2,6,2) and (0,10,0), achieve better system reliability.

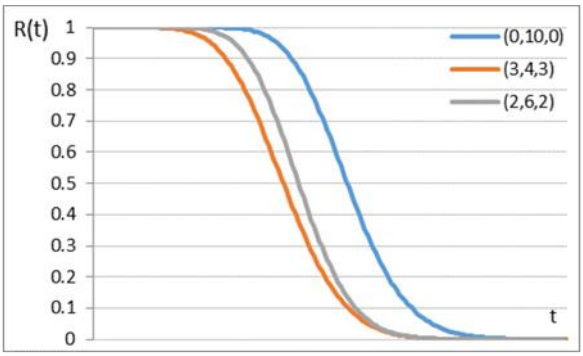


Figure 3-29. Reliability of systems (3,4,3), (2,6,2) and (0,10,0) for C_1=0.88, C_2=0.94 and C_3=0.97

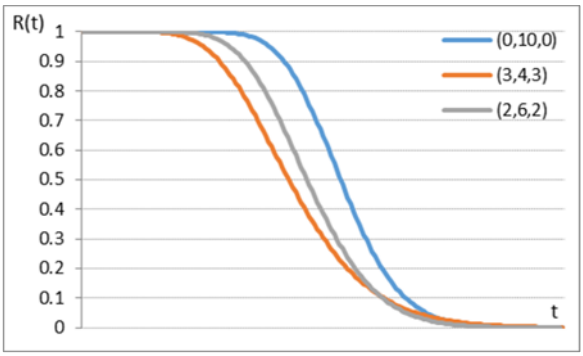


Figure 3-30. Reliability of systems (3,4,3), (2,6,2) and (0,10,0) for C_1=0.88, C_2=0.94 and C_3=0.99

When comparing systems with different structural redundancy distributions for smaller coverage C_2=0.9 (C_1=0.88 and C_3=0.97) (*Figure 3-31*) the ordering of the systems by reliability changes. The highest reliability has system (3,4,3) (the yellow curve in *Figure 3-31*), followed by systems (1,8,1) (the orange curve in *Figure 3-31*) and (0,10,0) (the light blue curve in *Figure 3-31*) which have equal reliability, and systems (4,2,4) (the dark blue curve in *Figure 3-31*) and (5,0,5) which has the smallest reliability (the green curve in *Figure 3-31*).

In *Figure 3-32*, the reliability of all system configurations with 10 components is depicted when the component coverage factors vary within the defined intervals in § 3.2. These results are studied in more detail in § 3.3.

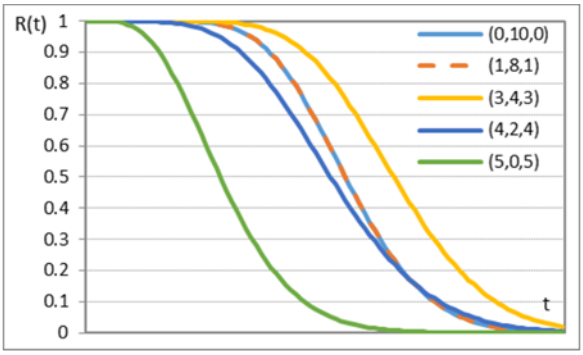


Figure 3-31. Comparison of the reliability of systems with different structural redundancy for C_1=0.88, C_2=0.9, and C_3=0.97

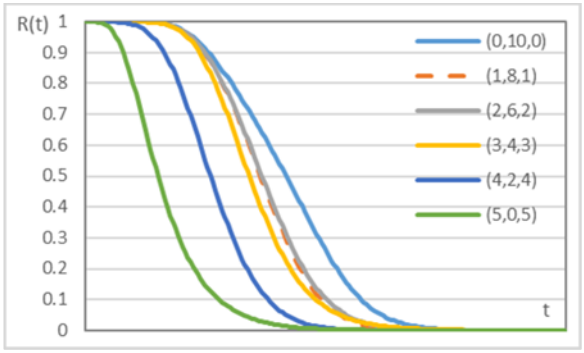


Figure 3-32. Comparison of the reliability of systems with different structural redundancy for $C_1 \in [0.8, 0.9)$, $C_2 \in [0.9, 0.95)$ and $C_3 \in [0.95,\ 1.0)$

It is seen from *Figure 3-32* that the best reliability has the system without reliability adjustment, (0,10,0) (the light blue curve), followed by systems (1,8,1) (the orange curve) and (2,6,2) (the gray curve). Close but lower reliability has system (3,4,3) (the yellow curve). These results are similar to the reliability of the systems in *Figure 3-23* but differ from the results in *Figure 3-31*.

The simulation modeling of the fault-tolerant system with adjustable reliability with 10 components shows that the system has good dependability characteristics. It is seen from the results that there are structural redundancy distributions that improve the system's reliability under certain conditions.

3.2.3 System with 20 components

The fault-tolerant system with adjustable reliability with 20 components and 40 modules is simulated for the same parameters as the system with 10 components (§ 3.2.2). Eleven distributions of the module redundancy are studied. The influence of the permanent faults is investigated for two different fault rates to study different working environment conditions. The assumption is that the systems that operate in more unfavorable conditions are subject to more faults, which is represented in the model with a bigger permanent fault rate $\lambda_p=10^{-3}$ 1/h. The smaller fault rate $\lambda_p=10^{-4}$ 1/h models environments where the faults occur more rarely but the system has to be able to tolerate them.

The system with reliability adjustment has different redundancy distributions of the components. Their reliability, R_d, as a function of time is shown in *Figure 3-33*, where the permanent fault rate is $\lambda_p=10^{-4}$ 1/h.

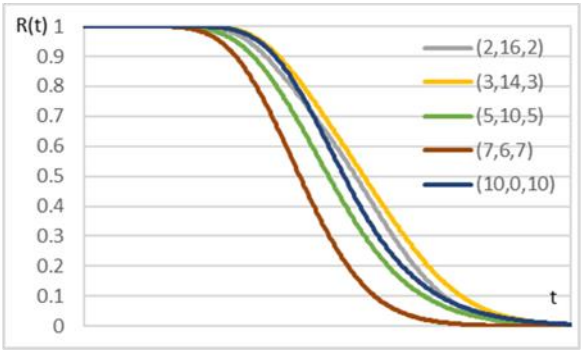


Figure 3-33. Reliability of systems with different structural redundancy distributions, $\lambda_p=10^{-4}$ 1/h, $\mu_p=\mu_{sys}=0.1$ 1/h

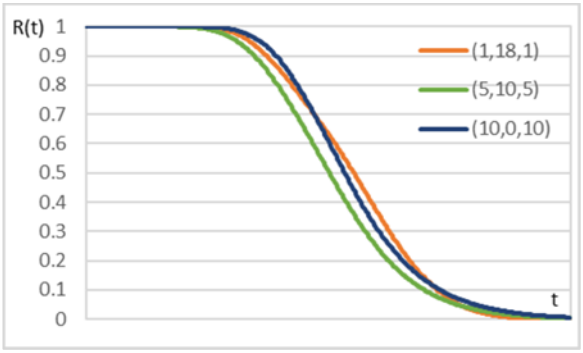


Figure 3-34. Reliability of systems with different numbers of TMR components, $\lambda_p=10^{-4}$ 1/h, $\mu_p=\mu_{sys}=0.1$ 1/h

The systems with a comparatively small number of single and TMR components demonstrate high reliability (systems (3,14,3) in yellow and (2,16,2) in gray in *Figure 3-33*). It cannot be stated however that this is a trend. The system consisting solely of single and TMR components (system (10,0,10) in dark blue in *Figure 3-33*) has close reliability.

To show the influence of the TMR components, the reliability of systems (1,18,1), (5,10,5), and (10,0,10) is depicted in *Figure 3-34*. The introduction of more single and TMR components in the system (system (10,0,10) in dark blue in *Figure 3-34*) improves the reliability and extends the period during which the system maintains high reliability. The functioning with fewer single and TMR components (system (1,18,1) in orange in *Figure 3-34*) however does not deteriorate significantly the system's reliability. System (5,10,5), which has the lowest reliability of the three systems in *Figure 3-34*, still has good reliability compared to the other systems, as can be seen in *Figure 3-33*.

It cannot be drawn clear dependence between the structural redundancy distribution and the reliability (*Figure 3-33* and *Figure 3-34*). The redundancy distribution impacts the system's reliability and some distributions are more favorable for the system than others are. The choice of system configuration depending on the application requirements can lead to system reliability and availability improvement.

The fault-tolerant system with adjustable reliability is simulated for a bigger permanent fault rate to study whether the redundancy distribution influences differently its reliability (*Figure 3-35*). Compared to the reliability of systems for $\lambda_p=10^{-4}$ 1/h (*Figure 3-33*) the reliability for $\lambda_p=10^{-3}$ 1/h is similar and the studied systems are ordered in the same way according to their reliability (*Figure 3-35*).

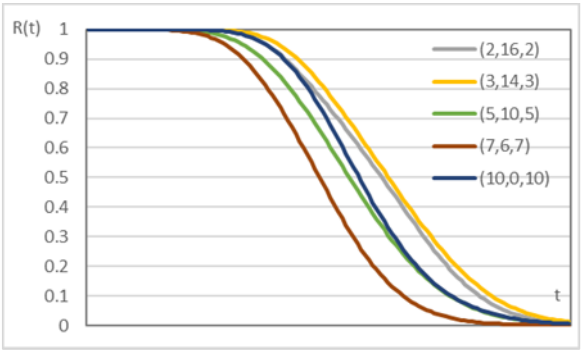


Figure 3-35. Reliability of systems with different structural redundancy distribution, $\lambda_p=10^{-3}$ 1/h, $\mu_p=\mu_{sys}=0.1$ 1/h

3.3 An approach of adjustable reliability

Safety-critical applications require very high reliability to deliver the dependable service that they are intended for. The desired system reliability is defined at the design stage and the other dependability characteristics are compliant with this requirement. The study of the fault-tolerant system with adjustable reliability is extended to allow deeper investigation of its behavior and to propose opportunities for achieving high desired reliability. In the presented dissertation, this reliability is called *total reliability* and is denoted as R_{total}. Based on the research presented in § 3.2.2 and § 3.2.3 and [75], [76], an approach of adjustable reliability is developed for determining the systems that achieve R_{total}.

R_{total} is defined during the process of system design when the specifications of the system are identified according to the application requirements. At the design stage, are defined: the fault and failure modes, the coverage factors of the self-checking units, *MTTF*, *MTTR*, etc. The rates λ_p, μ_p, μ_{sys}, the mission time, and R_{total} are also defined. For a given R_{total} all possible module redundancy distributions are determined and investigated – *system (i, j, k)* for *N* components and *M* modules. The systems (i, j, k), i.e., the system's configurations, are simulated, as described in § 3.1, and the diagrams of their reliability as a function of time are obtained. The reliability of each configuration R_d is compared to R_{total}. Then the systems satisfying the condition $R_d(t) \geq R_{total}$ are determined. The period of high reliability is also determined for every system.

The results for the systems described in § 3.2.2 and § 3.2.3 are shown in *Figure 3-36* for R_{total}=0.9999 and systems with *N*=20. All studied structural redundancy distributions achieve R_{total} but maintain this reliability for different periods. The results of the simulation show the relation between the total reliability and the structural redundancy distribution and illustrate the approach of adjustable reliability.

The system (3,4,3) has the biggest reliability (the yellow curve in *Figure 3-36*), followed by the system (10,0,10) (the dark blue curve in *Figure 3-36*) and system (1,18,1) (the orange curve in *Figure 3-36*). The system built out of DMR components, system (0,20,0), has the lowest reliability

(the red curve in *Figure 3-36*). The component redundancy distribution impacts the system's reliability (*Figure 3-33*, *Figure 3-35*, and *Figure 3-36*). The overall reliability is higher for some structural redundancy distributions, e.g. system (3,14,3) (the yellow curve in *Figure 3-36*), system (1,18,1) (the orange curve), and system (10,0,10) (the dark blue curve), and is lower for others, such as system (7,6,7) (the brown curve in *Figure 3-36*), system (5,10,5) (the light green curve), and system (6,8,6) (the light blue curve in *Figure 3-36*).

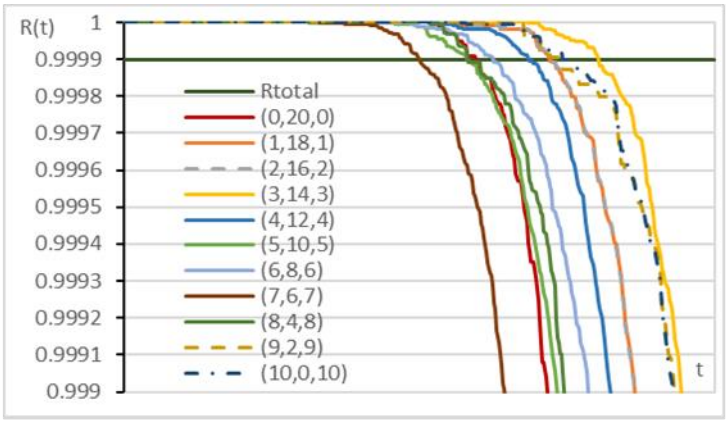


Figure 3-36. Achieving reliability R_{total}=0.9999, $\lambda_p=10^{-4}$ 1/h, $\mu_p=\mu_{sys}$=0.1 1/h

Cannot be derived a clear relation between the redundancy distribution and the system reliability. If the number of components with coverage factor C_3 (i.e. with TMR) is bigger than the number of the components with coverage factor C_2 (i.e. with DMR), this does not necessarily mean that the system reliability will increase. The introduction of single components, on the other hand, does not lead to a significant decrease in the system's reliability. In some cases, e.g. system (10,0,10) (the dark blue curve in *Figure 3-36*), the reliability is bigger than in systems with fewer single components, such as system (6,8,6) (the light blue curve in *Figure 3-36*).

Table 3-3 shows the periods during which the reliability R_d of each system with adjustable reliability exceeds R_{total}=0.9999, starting with the system with the longest period. The system (3,14,3) maintains its reliability above R_{total} for the longest period compared to the other systems. The system (0,20,0) without adjustable reliability has a comparatively shorter period of reliability over R_{total}=0.9999.

Table 3-3. Operational periods of systems (i, j, k) with reliability $R_d \geq R_{total}$=0.9999, $\lambda_p=10^{-4}$ 1/h, $\mu_p=\mu_{sys}$=0.1 1/h, N=20

System	$R_d \geq R_{total}$	Time [h]
(3,14,3)	0.999902	32300
(9,2,9)	0.999904	29800
(10,0,10)	0.999922	29800
(1,18,1)	0.999905	28900
(2,16,2)	0.999909	28900
(4,12,4)	0.999902	27500
(6,8,6)	0.999907	25100
(0,20,0)	0.9999	24000

System	$R_d \geq R_{total}$	Time [h]
(8,4,8)	0.999912	23400
(5,10,5)	0.999902	23400
(7,6,7)	0.999903	20100

In the simulation of the systems for $\lambda_p=10^{-3}$ 1/h (*Figure 3-37*), the order of the reliability diagrams of the different system configurations is approximately the same as for fault rate $\lambda_p=10^{-4}$ 1/h (*Figure 3-36*). Again, the highest reliability shows the system (3,14,3) (the yellow curve in *Figure 3-37*), and the lowest reliability – system (7,6,7) (the brown curve in *Figure 3-37*). The system without adjustable reliability (0,20,0) (the red curve in *Figure 3-37*) shows average reliability.

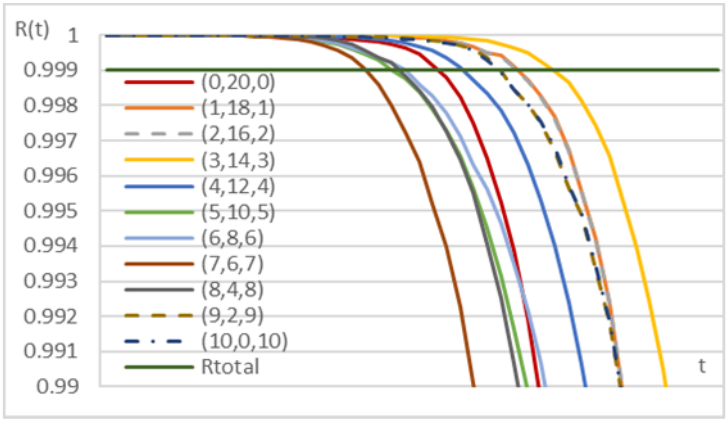


Figure 3-37. Achieving reliability $R_{total}=0.999$, $\lambda_p=10^{-3}$ 1/h, $\mu_p=\mu_{sys}=0.1$ 1/h

The operational periods of the configurations with reliability $R_{total} \geq 0.999$ for $\lambda_p=10^{-3}$ 1/h are shown in *Table 3-4*. As can be seen in the diagrams in *Figure 3-37*, system (3,14,3) maintains the desired reliability R_{total} for the longest period, and the shortest period is for the system (7,6,7). The system (0,20,0) without adjustable reliability has a relatively shorter period of maintaining R_{total} compared to the majority of the systems.

Table 3-4. Operational periods of systems *(i, j, k)* with reliability $R_d \geq R_{total}=0.999$, $\lambda_p=10^{-3}$ 1/h, $\mu_p=\mu_{sys}=0.1$ 1/h, $N=20$

System	$R_d \geq R_{total}$	Time [h]
(3,14,3)	0.999242	3300
(1,18,1)	0.9991	3100
(2,16,2)	0.99908	3100
(9,2,9)	0.999357	2900
(10,0,10)	0.999295	2900
(4,12,4)	0.999098	2700
(0,20,0)	0.99914	2500
(6,8,6)	0.999004	2300
(5,10,5)	0.999022	2200
(8,4,8)	0.999212	2200
(7,6,7)	0.999035	2000

The simulation results show that the distribution of the system resources depending on their importance for the application can give an advantage to the system reliability. For example, a modern

car is equipped with real-time distributed systems that control different blocks, such as the engine, suspension, gearbox, doors, seats, etc. These blocks in turn are subsystems consisting of other modules that operate together on the execution of a specific task. Such a subsystem can use the approach of adjustable reliability to achieve the reliability dictated by the application. Determining R_{total} and knowing the number of subsystem components and their dependability characteristics, the structural redundancy distributions can be derived and simulated to compare their reliability. This way the structural distribution with the highest reliability can be further investigated and developed considering the specifics of the designed subsystem.

The presented results of the simulation modeling (§ 3.2) show that there are structural redundancy distributions where the system with adjustable reliability achieves higher reliability R_{total} and maintains it for a longer period compared to the system without reliability adjustment (*Figure 3-36* and *Table 3-3*, *Figure 3-37* and *Table 3-4*). The conditions under which this happens are hard to establish since there is not a clear dependence between the system reliability and the redundancy distribution. That is why in the Ph.D. thesis an *approach of adjustable reliability* is proposed through which to determine the structural redundancy distributions that satisfy the requirement of system reliability of the application.

The approach of adjustable reliability can be described with the following actions:

1. Determining R_{total},
2. Determining the parameters describing the environment – fault rates,
3. Determining the system requirements – mean time to failure, mean time to repair, availability, mean downtime, possibilities for local and system repair, and the respective repair rates,
4. Determining the important control parameters and the critical components,
5. Determining the criticality levels,
6. Determining the system configurations with adjustable reliability that is equal to or greater than the total reliability R_{total},
7. Checking which of the possible configurations fits in the best way into the application requirements,
8. In case no appropriate configuration is found, the input specifications are changed and the procedure is repeated.

The described actions are illustrated in *Figure 3-38*.

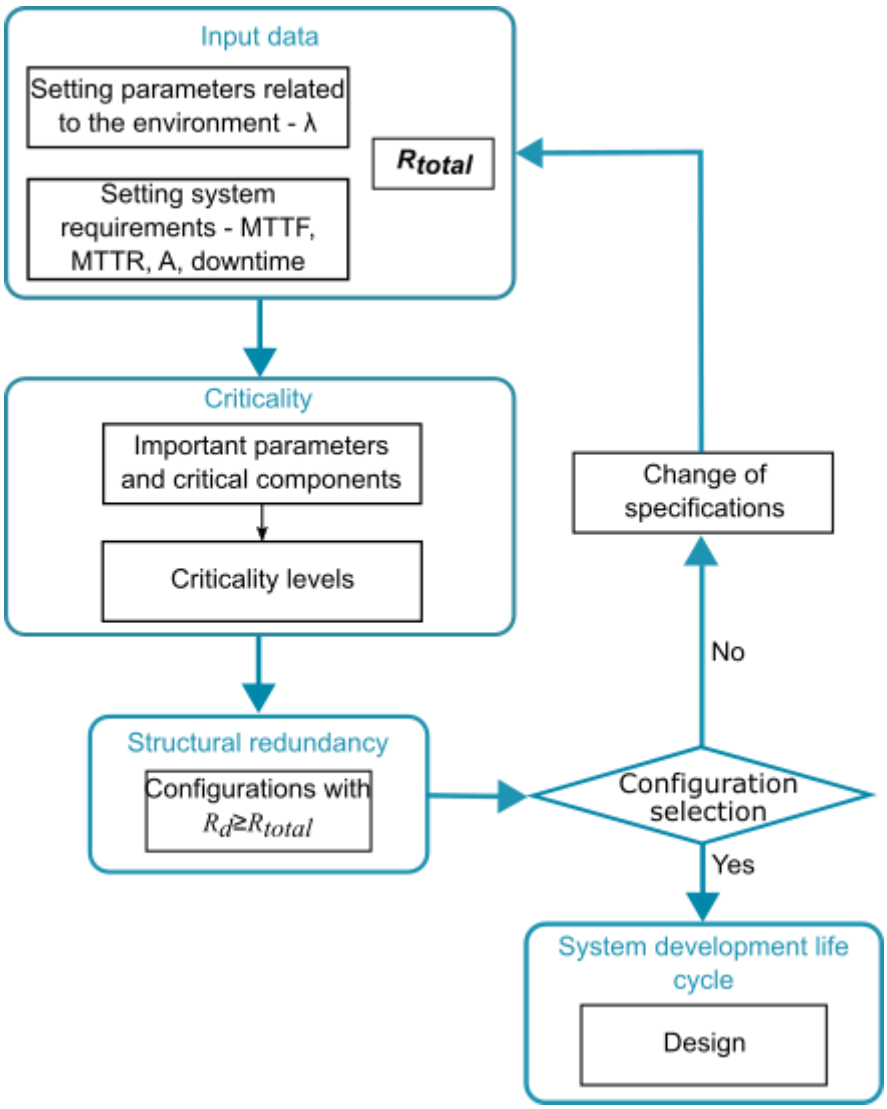


Figure 3-38. Description of the approach of adjustable reliability

If more of the possible system configurations with adjustable reliability fulfill the requirement of system reliability under the identified specifications, the appropriate configuration for the application can be chosen according to additional criteria, such as the number of single, DMR, or TMR components, desired criticality levels, the highest total reliability, the longest operational period with high total reliability, etc. If none of the configurations of the system with adjustable reliability satisfies the requirement of R_{total} of the application, it is necessary to reconsider the system specifications, including the requirement for total reliability.

3.4 Conclusions and results

In *Chapter 3*, the simulation program developed according to the requirements formulated in § 3.1.1 is presented. The main structure and the block scheme of the program are described.

A component of the fault-tolerant system with adjustable reliability is studied depending on the coverage factor of the self-checking unit C and the coverage factor of recovery from a transient fault C_r. Components with dual and triple modular redundancy are simulated operating with and

without local repair. The impact of C and C_r is evaluated concerning component reliability, availability, *MTTF*, *MTTS*, *MTBF*, *MTBS*, and the mean downtime.

According to the research protocol, multiple experiments are conducted for systems with different numbers of components (N=10 and N=20), different permanent fault rates λ_p, and different values of the coverage factors C_1, C_2, and C_3. Data are obtained for $R(t)$, A, *MTTF*, *MTTR*, *MTTS*, and *downtime*. The possible structural redundancy distributions are determined for N and M. The impact of the number of components, the coverage factors, and the fault rate on the dependability characteristics of the fault-tolerant system with adjustable reliability and on systems without structural redundancy distribution is studied. The system configurations satisfying the requirement for total reliability are identified.

An approach of adjustable reliability developed by the author is presented and is used to determine which redundancy distributions of the components satisfy the desired overall system reliability. Based on the application requirements the approach finds out the system configurations that can achieve the total reliability.

The conclusion can be drawn that it is possible to achieve high reliability through structural redundancy distribution and in some cases it exceeds the reliability of systems without redundancy distribution. The configurations that achieve the total reliability can be identified through the approach of adjustable reliability.

The obtained results are of scientific and application nature. The scientific and application results are the development of a simulation program to model dependable distributed systems and the formulation of an approach of adjustable reliability. The application results are related to the conducted experiments with the simulation program aiming at studying the dependability characteristics of the fault-tolerant distributed system with adjustable reliability.

Through the results presented in *Chapter 3* tasks 3 and 4 of the Ph.D. thesis are fulfilled.

Chapter 4. Discussion and analysis of the results

Dependable distributed systems which are the object of the Ph.D. thesis are developed for safety-critical applications. They are built with specialized or Commercial Off-The-Shelf (COTS) components and both approaches have their advantages and disadvantages. The specialized components reflect more adequately the specifics of the application, allow for the achievement of high reliability using methods and techniques compliant with the specific operational environment and context of the system, and are well-verified and validated. This, however, requires time and effort which have their price. Such systems are designed and implemented for longer periods which, on the

one hand, makes them too hard to adapt to changes in the system's operational environment, and, on the other hand, makes their final realization more expensive.

The implementation of COTS components shortens the period between the design and implementation of the distributed system and lowers the costs. This approach has the drawback to introduce additional risks to the system's dependability. The COTS components do not give any guarantees for fulfillment of the dependability requirements. Methods and means are sought to compensate for their low reliability.

The analysis of the dependable distributed systems in terms of the structural redundancy, presented in *Chapter 1*, shows that the basic approaches to achieving more flexibility concerning the application requirements are the change of the software structural redundancy (for a static hardware structural redundancy distribution) and the introduction of criticality levels.

The fault-tolerant distributed system with adjustable reliability proposes and studies an approach to possess the flexibility of the dependable systems with COTS components, to consider the criticality levels of the systems with mixed-criticality, to allow for adjustment of the dependability characteristics, and in the same time to respond to the high-reliability requirements. All enumerated system types realize their fault tolerance through structural redundancy. They apply a uniformly distributed hardware redundancy of the components and a software structural redundancy distribution compliant with the application. The proposed system with adjustable reliability introduces flexibility through hardware structural redundancy distribution.

When developing the idea of a fault-tolerant distributed system with reliability adjustment we considered the conceptual model of an approach to decision-making for dependability and the classification of dependable distributed systems according to their ability to determine the structural redundancy depending on the application. The proposed system is built out of fault-tolerant components with different replication degrees which allows for the study of the dependability characteristics of different configurations of the structural redundancy. The component fault tolerance is determined by the incorporation of a self-checking unit in each module and means for comparison of its results. The presented Markov chains of the fault-tolerant distributed system with adjustable reliability model the system's behavior according to the possibility of component recovery and system repair. These models are the basis of the simulation program by which the experiments in the dissertation are conducted. The selected research approach of simulation modeling offers the opportunity to represent the system's behavior concerning the faults and failures and to investigate its dependability characteristics, defined in *Chapter 2*, § 2.1.2. The simulation allows the modeling of systems with multiple components and states and the introduction of various parameters to study their impact on the system's reliability.

The results of the simulation modeling of the fault-tolerant system with adjustable reliability

presented in *Chapter 3* show that the system under investigation has good dependability characteristics. An analysis of the results is carried out to check whether the research hypothesis is confirmed, namely, can high system reliability and flexibility be achieved through the reliability adjustment according to the application requirements.

During the simulation of a system component, components with dual and triple modular redundancy are considered. We have studied the impact of the coverage factor of the self-checking unit and the coverage factor of the transient fault recovery. The results for the reliability, availability, *MTTF*, *MTTR*, *MTTS*, *MTBF*, *MTBS*, and downtime show that the inclusion of self-checking units in each module of a component improves significantly the system's dependability characteristics, especially when it operates without local repair.

The simulation modeling of the fault-tolerant distributed system with reliability adjustment for 10 components does not outline a clear dependency between the system reliability and the structural redundancy distribution. On the one hand, the system without adjustable reliability (0,10,0) shows the highest reliability. On the other hand, for a lower coverage C_2 some configurations of the structural redundancy have bigger or close reliability. The impact of C_1 on reliability is insignificant. The coverage factors C_2 and C_3 improve significantly the overall system reliability which is logical given their bigger values.

In the fault-tolerant distributed system with adjustable reliability for 20 components, the biggest reliability is achieved by the system (3,14,3). The lowest reliability has the system (7,6,7). The configurations with a small number of single and TMR components, such as (1,8,1), (2,16,2), and (3,14,3), have comparatively high reliability. The increase of the number of TMR components can improve the reliability but this is not valid in all cases.

The experiments for a higher fault rate $\lambda_p=10^{-3}$ 1/h show that some systems with adjustable reliability are more suitable for operation in such conditions. The systems (1,18,1) and (2,16,2) have the second-best reliability, while for fault rate $\lambda_p=10^{-4}$ 1/h, they have lower reliability. The system without adjustable reliability (0,20,0) also works better for a high fault rate. This behavior of the studied systems implies flexibility in the selection of an appropriate system for a specific application.

The systems with the highest overall reliability also have the longest operational periods. This is a measure of their availability. If this property is of importance for the application, it should be considered in the choice of a configuration with adjustable reliability.

During the conducted simulation experiments for N=10 and N=20 the different configurations of the system with adjustable reliability do not show a consistent behavior. Their reliability is influenced by the number of components, the permanent fault rate, and the coverage factors of the self-checking units. For some configurations, the overall reliability is greater than the one of the systems without adjustable reliability, for others it is not. To determine the appropriate configuration

of the fault-tolerant distributed system with adjustable reliability according to the application requirements, an approach of adjustable reliability is developed. It consists of a sequence of actions for the selection of the structural redundancy distribution depending on the requirement for total system reliability. The approach determines all system configurations that achieve the desired reliability and presents an opportunity to choose the one that satisfies the determined system specifications best.

After the experiments with the simulation program, the following conclusions can be made. The configurations with adjustable reliability achieve high system reliability, comparable to and in some cases better than the one of the system without structural redundancy distribution. The approach of adjustable reliability determines the system configurations that satisfy the requirement for overall reliability best. This gives flexibility in the fault-tolerant distributed systems' design to choose a structural redundancy distribution that is most suitable for the needs of a specific realization.

These conclusions confirm the hypothesis of the Ph.D. research that it is possible to achieve flexibility and high reliability of the fault-tolerant distributed systems through the distribution of the hardware structural redundancy according to the application requirements.

4.1 Conclusions and results

The results presented in the Ph.D. thesis are discussed and analyzed and based on the analysis they are grouped as follows:

Scientific results:

1. A new architectural model of a fault-tolerant distributed system with adjustable reliability is presented and the requirements for its components and the system as a whole are defined;
2. A simulation model of the proposed fault-tolerant system with adjustable reliability is developed;
3. A synthesis of a classification and a classification of dependable distributed systems with structural redundancy is proposed.

Scientific and application results:

1. A conceptual model of an approach for decision-making in providing dependability is developed;
2. An approach of adjustable reliability is formulated;
3. A simulation program implementing the method of simulation modeling of dependable distributed systems is developed.

Application results:

1. The developed simulation program can be used for modeling and studying the dependability characteristics of other fault-tolerant systems as well. The impact of transient hardware faults can also be investigated using the program.

The obtained results in the Ph.D. thesis demonstrate that the defined tasks are fulfilled.

The implementation results confirm the statements supporting the research hypothesis of the Ph.D. thesis: It is possible to achieve high reliability and flexibility of the system resources distribution through adjustable reliability implemented by the distribution of the hardware structural redundancy. This is confirmed by the following results:

1. The presented fault-tolerant distributed system with adjustable reliability achieves high overall reliability comparable to the reliability of systems without structural redundancy distribution.
2. The fault-tolerant distributed system with adjustable reliability has configurations of the structural redundancy distribution that possess better dependability characteristics than the ones of systems without structural redundancy distribution.
3. The approach of adjustable reliability allows for determining the structural redundancy distributions that satisfy the requirement for the overall reliability of the application.

Conclusion and future work

In the Ph.D. thesis, the dependability characteristics of a fault-tolerant distributed system with adjustable reliability are studied. The system is proposed as an opportunity to achieve flexibility in the design of dependable distributed systems. In the survey of dependable distributed real-time systems, two main directions of building such systems are outlined – using specialized components and using commercial-off-the-shelf components. Both system types achieve fault tolerance through various approaches to introducing redundancy. Structural, time, and functional redundancy are applied. Structural redundancy adds hardware and software elements to the system architecture. It is often realized as equally replicated hardware components that execute differently replicated software tasks.

A conceptual model of an approach for decision-making is developed and a classification of dependable distributed systems is synthesized based on the system development model.

The author proposed an architecture and a model of a fault-tolerant distributed real-time system, called a system with adjustable reliability. It suggests an adjustment of the hardware structural redundancy to achieve overall reliability according to the application requirements. The system is studied through the method of simulation modeling.

A software product for simulation modeling of fault-tolerant systems is designed and developed. It implements the developed model of the system with adjustable reliability. As a result of its execution, the reliability function is obtained, as well as data for the dependability characteristics of the system. The simulation product is written in C++ and it can be used to investigate fault-tolerant systems with and without structural redundancy distribution.

The results of the conducted experiments show good overall reliability of the system with adjustable reliability. There are structural redundancy distributions that show higher system reliability than that of the system with uniform redundancy distribution. For some configurations a stochastic ordering is observed, i.e., the curves of reliability do not cross each other which means that the choice of an architectural solution does not depend on the respective values of the coverage factors. There are instances where the different architectural solutions are indistinguishable and others where no stochastic ordering is seen. This renders the choice of a specific engineering solution not obvious and dependent on the deeper knowledge of the coverage values. The differences in the reliability function of the studied configurations show that during the system design tools should be used to obtain a quantitative assessment of the variants for structural redundancy distribution to choose the most appropriate solution for the application.

This motivated the author to develop an approach, called the approach of adjustable reliability, which determines the structural redundancy distributions that achieve the reliability required by the application.

The results obtained during the modeling of the fault-tolerant distributed system with adjustable reliability show that the system has advantages concerning the structural redundancy distribution according to the application requirements and they can be used in dependable distributed systems' design. The adjustable reliability is appropriate to use in systems with mixed criticality of the components, in compact systems where multiple nodes are allocated in limited space, in systems with high-reliability requirements that allow for the operation with COTS components, etc. The software product for simulation modeling of fault-tolerant systems with structural redundancy distribution can be used to model other dependable distributed systems by adding blocks describing their characteristics.

Directions for future work

The fault-tolerant system with adjustable reliability can be studied for different applications, requiring criticality levels, high reliability, and structural redundancy distribution. The approach of adjustable reliability can be improved to include the consideration of other application requirements for dependable distributed systems. The model of the fault-tolerant distributed system with adjustable reliability can be extended to modeling software reliability and studying the effect of software faults on the system fault tolerance. The approach and the model of adjustable reliability can be applied to

specific systems.

The simulation program can be improved by accelerating its execution using techniques for parallel processing. It can be extended with more blocks allowing the investigation of other factors' impact on the dependability characteristics of a system. The software product can be further developed to study different types of distributed systems.

List of publications related to the Ph.D. thesis

1. Djambazova, E., & Andreev, R. (2023). Redundancy management in dependable distributed real-time systems. *Problems Of Engineering Cybernetics And Robotics*. (in print)
2. Djambazova, E. (2022). Achieving system reliability using reliability adjustment. International Conference on Computer Systems and Technologies 2022 (CompSysTech '22), Ruse, Bulgaria. ACM, NewYork, NY, USA, pp. 64-68. DOI: 10.1145/3546118.3546129. SJR(SCOPUS) 2020: 0,18
3. Djambazova, E. (2012). Adjusting reliability of a fault-tolerant distributed process control system – Preliminary results. International Conference "Automatics and Informatics 2012", Sofia, Bulgaria, pp. 175-178.
4. Djambazova, E. (2009). Node reliability of a fault-tolerant distributed process control system – Simulation results. International Conference "Automatics and Informatics' 2009", Sofia, Bulgaria, pp. I-131 – I-134.
5. Джамбазов, К., & Ананиева, Е. (1995). Управляващи системи с модулно настройване на отказоустойчивостта. Национална конференция с международно участие „Автоматика и информатика '95", София, стр. 247-250.

Participation in projects

A part of the research is conducted under two national projects:

1. Modeling and Research of Intelligent Educational Systems and Sensor Networks (ISOSeM) – Contract № КП-06-Н 47/4 от 2020 г., funded by the National Science Fund (in progress).
2. Information and Communication Technologies for a unified digital market in Science, Education, and Security (ICTinSES) – Д01-205/2018 г., funded by the Ministry of Education and Science.

Main scientific and scientific and application results

Scientific results:

1. A new architectural model of a fault-tolerant distributed system with adjustable reliability is proposed.
2. A simulation model of a fault-tolerant distributed system with adjustable reliability is developed.

3. A classification of dependable distributed systems according to their ability to determine the structural redundancy depending on the application is synthesized.

Scientific and application results:

4. A critical analysis of dependable distributed systems is made based on which a conceptual model of an approach for decision-making in providing dependability is developed.
5. The main directions to manage structural redundancy in dependable distributed systems are identified and some research opportunities are outlined.
6. A software product for simulation modeling of the studied system is designed and developed.
7. Following a comparative analysis of the fault-tolerant system with adjustable reliability and systems without structural redundancy distribution an approach of adjustable reliability is developed and applied.

Application results:

8. The developed simulation program can be used for modeling and studying the dependability characteristics of other fault-tolerant systems. The impact of transient hardware faults can also be investigated using the program.

БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ

АВТОРЕФЕРАТ НА ДИСЕРТАЦИЯ

за присъждане на образователна и научна степен "доктор" по докторска програма "Компютърни системи, комплекси и мрежи"

ИЗСЛЕДВАНЕ НА НАДЕЖДНОСТНИТЕ ХАРАКТЕРИСТИКИ НА ОТКАЗОУСТОЙЧИВА РАЗПРЕДЕЛЕНА СИСТЕМА ЗА РАБОТА В РЕАЛНО ВРЕМЕ С НАСТРОЙВАЕМА НАДЕЖДНОСТ

Едита Ананиева Джамбазова

Ръководител: Доц. Румен Андреев

Научно жури:

Акад. Васил Сгурев
Акад. Кирил Боянов
Член. кор. Любка Дуковска
Проф. Иван Куртев
Доц. Петър Попов

Институт по информационни и комуникационни технологии

Секция „Интелигентни системи"

Увод

Актуалност на темата

Системите за работа в реално време се прилагат за управление на различни процеси (като индустриални производства, автомобили, авиационни системи и др.), където понятието за време е вградено в цялостния процес на производство. Те са разпределени компютърни системи с всички характеристики, които им позволяват да обработват данни и да обменят информация с външния за тях свят. Те „общуват“ с околната среда посредством сензори и активатори, което им дава възможност да управляват реални процеси. Това определя основната им характеристика – работа при времеви ограничения, наложени от средата. Поради функционирането си между управляван процес в реална физическа среда и компютърната си същност те са определяни като кибер-физични системи. Системите за работа в реално време обикновено са разпределени, което означава, че са съставени от самостоятелни компоненти, които комуникират помежду си през комуникационен канал. Те често са свързани с критични за безопасността приложения и към тях се поставят високи изисквания за гарантоспособност, които се вземат предвид още на етапа на тяхното проектиране. Гарантоспособността е интегрално понятие, което определя доверието в способността на една система да доставя коректна услуга. Всички тези аспекти на реалновременните системи – кибер-физични, разпределени, работещи с ограничения по време, отказоустойчиви – прави проектирането им сложно и многообхватно. Това поражда редица изследователски проблеми, които през годините и с развитието на технологиите са намирали различни решения. Изискването за отказоустойчивост е част от процеса на проектиране. Реалновременната функция определя гарантоспособните разпределени системи да работят с глобална времева база, според която да синхронизират всички операции, като предоставят коректна услуга както в областта на стойностите, така и в областта на времето. Кибер-физичната им природа изисква да съчетават разнообразни изисквания. Често изискванията за отказоустойчивост и работа в реално време са трудно съвместими и се налага търсенето на приемлив компромис между тях.

Отказоустойчивостта е неотменимо свойство на тези системи. Тя се постига чрез прилагането на различни подходи и техники за откриване на грешки и възстановяване от тях. В голяма степен те се основават на понятието за излишък. Излишъкът е елемент от структурата на дадена система, без който тя може да изпълнява основните си функции и който подпомага функционирането ѝ в случай на промяна в работната ѝ среда, породена от настъпването на неизправности. Управлението на излишъка е важно за отказоустойчивите системи, защото той води до повишаване на техните надеждностни характеристики, но в същото време внася

допълнителни елементи, които имат своята цена от гледна точка на производителността и разходите за системата. Въвеждането на структурен излишък с цел повишаване на гарантоспособността води до допълнителни закъснения за синхронизация, възстановяване след отказ, включване и изключване на нови компоненти и т.н., което усложнява постигането на изискванията за работа в реално време. Намирането на компромис е сложна задача и е предмет на сериозни изследователски усилия. Търсенето на нов подход за управление на излишъка в гарантоспособни разпределени системи мотивира това дисертационно изследване.

Мотивация

Изискванията за гарантоспособност на реалновременните системи при критични приложения и повишаването на разходите на системата с цел управление на излишъка мотивира идейния замисъл на дисертацията да се създаде архитектура на отказоустойчива разпределена система за работа в реално време, която да позволява разпределение на структурния излишък според изискванията на приложението – наречена от автора *система с настройваема надеждност*. Основният изследователски въпрос е дали могат отказоустойчивите разпределени компютърни системи за работа в реално време да постигнат гъвкавост по отношение на изискванията за надеждност на приложението чрез предложения в дисертацията подход на настройваема надеждност.

Предложената в дисертационния труд архитектура на отказоустойчива разпределена система за работа в реално време с настройваема надеждност е изградена от самостоятелни отказоустойчиви компоненти с различна модулност, съобразена с тяхната критичност. Критичността на компонентите се определя от тежестта на последствията от техен отказ за управляваната система. Системата е моделирана посредством разработена за целта симулационна програма и са изследвани надеждностните ѝ характеристики при различни параметри. Предложеният в дисертацията научно-приложен подход, наречен подход на настройваема надеждност, определя разпределение на хардуерния структурен излишък, съобразено с изискванията на приложението за обща системна надеждност. Системата и подходът на настройваема надеждност предлагат постигане на висока надеждност посредством разпределение на системните хардуерни ресурси по начин, който е съобразен с нуждите на приложението. Това прави отказоустойчивата разпределена система с настройваема надеждност удобна за внедряване в области с разнообразни изисквания за надеждност и смесена критичност на компонентите, във вградени системи, при по-малко отговорни приложения и пр.

Подходът на настройваема надеждност има предимства пред други широко известни разработки при: постигане на по-висока надеждност със същите ресурси, постигане на висока

готовност, гъвкавост при разпределението на системните ресурси на етапа на проектиране, приложимост в компактни системи. Моделирането на предлаганата разпределена система с настройваема надеждност и сравнението ѝ с моделите на подобни системи показва, че има възможност по-добре да се разпределят ресурсите на системата при запазване на добри нива на нейните надеждностни характеристики.

Научна постановка на изследването

Обект на изследването са отказоустойчиви разпределени системи за работа в реално време.

Предмет на дисертацията е настройваема надеждност в отказоустойчиви разпределени системи за работа в реално време.

Целта на дисертационния труд е да се изследват надеждностните характеристики на предложената от автора отказоустойчива разпределена система за работа в реално време с настройваема надеждност, като те се съпоставят с познатите подобни системи, и на тяхна основа да се разработи подход (на настройваема надеждност) за използване в отказоустойчиви системи за работа в реално време.

Хипотеза

Гарантоспособните разпределени системи постигат отказоустойчивост по много различни начини и на различни нива от своята архитектура. Водещ метод за изграждането им е въвеждането на структурен излишък. Съществуват два основни подхода за прилагане на структурен излишък – посредством специализирани хардуерни и софтуерни компоненти и посредством използване на готови софтуерни и хардуерни компоненти. И при двата подхода отказоустойчивостта срещу физически неизправности се постига чрез репликиране на хардуерните компоненти и се търси гъвкавост при репликирането на софтуерните компоненти. Хипотезата, която се поставя в настоящата дисертация, е, че може да се постигне висока надеждност и гъвкавост на разпределението на системните ресурси посредством настройваема надеждност, реализирана с разпределение на хардуерния структурен излишък.

Доказателствата на хипотезата се измерват чрез верифициране на следните твърдения:

1. Отказоустойчивата система с настройваема надеждност постига висока обща надеждност, съпоставима с надеждността на системи без разпределение на структурния излишък.
2. Съществуват конфигурации на системата с настройваема надеждност, при които се постигат по-добри надеждностни характеристики от тези на системи без разпределение на структурния излишък.

3. Може да се идентифицират условията, при които отказоустойчивата система с настройваема надеждност има по-добри надеждностни характеристики от сравняваните системи.

Методология на изследването

В дисертацията са застъпени основните прийоми на научното познание - анализ, синтез, сравнение и обобщение. Направен е обзор на гарантоспособните разпределени системи от гледна точка на разпределението на структурния излишък, като са откроени техните предимства и недостатъци. На базата на този критичен анализ е поставена целта на настоящото изследване и е формулирана основната хипотеза. Предложен е концептуален модел за вземане на решения при вграждане на гарантоспособност в системи. Въз основа на класификацията на гарантоспособни разпределени системи е направена връзка между жизнения цикъл на разработване на системи и проектирането на системи за критични приложения.

След проучването на съществуващите гарантоспособни системи е предложена архитектура на отказоустойчива система с настройваема надеждност. Направен е преглед на методите за моделиране на гарантоспособни системи и е избран и обоснован изследователски подход – симулационно моделиране. За неговата реализация е създаден програмен продукт, с който са проведени множество експерименти. Получените резултати са систематизирани и анализирани и с тяхна помощ е разработен подход на настройваема надеждност, чрез който да се определят системните конфигурации с обща надеждност според изискванията на приложението.

Основни задачи на изследването:

1. Да се направят проучване, обзор и критичен анализ на гарантоспособни разпределени системи. Да се синтезира класификация на съществуващите гарантоспособни разпределени системи. Да се очертаят изследователски възможности при разпределение на структурния излишък.
2. Да се предложат модел и архитектура на отказоустойчива разпределена система с настройваема надеждност, които дават решение на изискванията за висока надеждност според нуждите на приложението.
3. Да се дефинира метод за изследване на предложения модел. Да се разработи инструмент, реализиращ този метод. Да се състави изследователски протокол.
4. Да се проектират и проведат експериментални изследвания за тестване и анализ на надеждностните характеристики на предложената отказоустойчива система с настройваема надеждност посредством избрания изследователски подход и

реализирания програмен продукт. Да се разработи и приложи подход на настройваема надеждност.

Структура на съдържанието

Дисертационният труд е организиран в увод, четири глави, заключение, библиографска справка и две приложения.

В *Увода* са посочени темата, обектът и предметът на дисертационния труд. Описана е накратко актуалността на темата и мотивацията за извършване на дисертационното изследване. Поставена е целта на изследователската работа и задачите, чрез които тя да бъде постигната, водещата хипотеза и приложената при проведените изследвания методология.

В *Глава 1* са представени основополагащите понятия, свързани с гарантоспособните разпределени системи за работа в реално време. Описани са основните методи и техники за постигане на отказоустойчивост. Разгледани са начините за въвеждане на излишък и неговото управление. Представен е обзор и критичен анализ на познатите гарантоспособни разпределени системи. Изведен е концептуален модел на подход за вземане на решение при осигуряване на гарантоспособност и е синтезирана класификация на гарантоспособни разпределени системи. Очертани са възможностите за нови изследвания.

В *Глава 2* е представена архитектурата на предложената от автора отказоустойчива разпределена система с настройваема надеждност. Представени са методите за моделиране на гарантоспособни разпределени системи, както и модела и допусканията на отказоустойчивата система с настройваема надеждност. Там са описани изследваните надеждностни характеристики, въз основа на които системата може да бъде оценявана и сравнявана с други подобни системи. Обоснован е изборът на изследователски подход – симулационно моделиране.

В *Глава 3* са описани изследователските задачи и са представени резултатите от симулационно изследване на отказоустойчивата разпределена система с настройваема надеждност. Представен е програмният продукт за симулационно моделиране на системата с настройваема надеждност. Изследвани са надеждностните характеристики на компонент на системата и на цялата система: надеждност, готовност, средно време до отказ, средно време за ремонт и т.н. Представен е разработеният в дисертацията подход на настройваема надеждност, който позволява избиране на подходяща конфигурация на структурния излишък в зависимост от изискванията за обща системна надеждност на приложението.

Глава 4 представлява анализ и обсъждане на резултатите. Посочени са предимствата и възможните приложения на предложената отказоустойчива система с настройваема надеждност. Изведени са основните научни и научно-приложни резултати на дисертацията.

Очертани са възможностите за по-нататъшни изследвания и приложение на отказоустойчивата разпределена система с настройваема надеждност.

Дисертационният труд завършва със *Заключение*, в което се обобщават получените резултати. В края е посочена *Библиография*, съдържаща 102 източника. В *Приложение А* са изведени математическите представяния на надеждностните характеристики, с които борави изследването. В *Приложение В* е представен кодът на програмата за симулационно моделиране NMRSIM.

Глава 1. Гарантоспособни разпределени системи за работа в реално време

1.1 Гарантоспособност – основни понятия

Понятието гарантоспособност[1] (на англ. dependability) е въведено от Жан-Клод Лапри през 80-те години на 20. в. [1], [2], за да се обхванат различните аспекти на отказоустойчивите системи и да се въведе системност в използването на понятията, свързани със защитата от откази на високонадеждните системи. Основната дефиниция за *гарантоспособност* [2], [3], [4] гласи, че „Гарантоспособност е способността на една компютърна система да доставя услуга, на която може обосновано да се разчита“. Тази дефиниция поставя ударението върху обоснованото доверие в услугата, предоставяна от системата. В [3] е добавена и втора дефиниция на гарантоспособност, която подчертава значението на предотвратяването на откази: „Гарантоспособност на дадена система е способността ѝ да предотвратява откази в услугата, които са по-чести и по-тежки от допустимото“.

Специфичната терминологична основа, използвана в дисертацията, са утвърдените и широко прилагани в областта на гарантоспособните системи понятия и определения [3], [4], [5] и техните български еквиваленти [6].

Услуга е системното поведение от гледна точка на потребителя на системата. *Коректна услуга* се предоставя, когато услугата прилага системната функция.

1.1.1 Заплахи за гарантоспособността: откази, грешки, неизправности

Заплахите за компютърните системи са причините, които водят до отклонение от коректното им функциониране. Проявата на това отклонение на системно ниво се нарича отказ

[1] Преводът на основните термини, свързани с понятието гарантоспособност, е направен от колектива на секция „Отказоустойчиви компютърни системи“ на Института по компютърни системи (ИКС – БАН) [6]. По-съвременната им интерпретация и превод са на автора.

на услугата [3]. *Отказ* е събитие, което настъпва, когато предоставяната услуга се отклонява от коректната. Отклонението от коректната услуга може да приеме различни форми, наречени режими на отказ и са подредени според *сериозността на отказа* - степента на последствията на отказа за системната среда.

Отказ в услугата означава, че поне едно (или повече) външни състояния на системата се отклонява от състоянието на коректна услуга. Това отклонение се нарича грешка. Доказаната или хипотетичната причина за грешка се нарича *неизправност*. Определението за *грешка* е частта от общото състояние на системата, която е възможно да доведе до отказ.

1.1.2 Атрибути и средства на гарантоспособността

В основополагащата статия [3] са представени основните понятия и дефиниции, свързани с гарантоспособността. Те се използват и в настоящата работа, като тук са цитирани само дефинициите, които имат отношение към темата на дисертацията. Според наложилата се през последните тридесет години терминология гарантоспособността е интегрално понятие, което се характеризира със следните атрибути:

- *Готовност*: наличност на системата за предоставяне на коректна услуга;
- *Надеждност*: непрекъснатост на коректната услуга;
- *Безопасност*: отсъствие на катастрофални последствия за потребителя и средата;
- *Цялостност*: отсъствие на неправилни изменения на системата;
- *Ремонтопригодност*: способност да се предприемат модификации и ремонти.

Средствата за постигане на гарантоспособност на компютърните системи [2], [3] са *предпазване от неизправност*, *отказоустойчивост*, *отстраняване на неизправност* и *прогнозиране на неизправност*. Отказоустойчивостта обединява методи и средства, имащи за цел предотвратяването на откази в присъствието на неизправности.

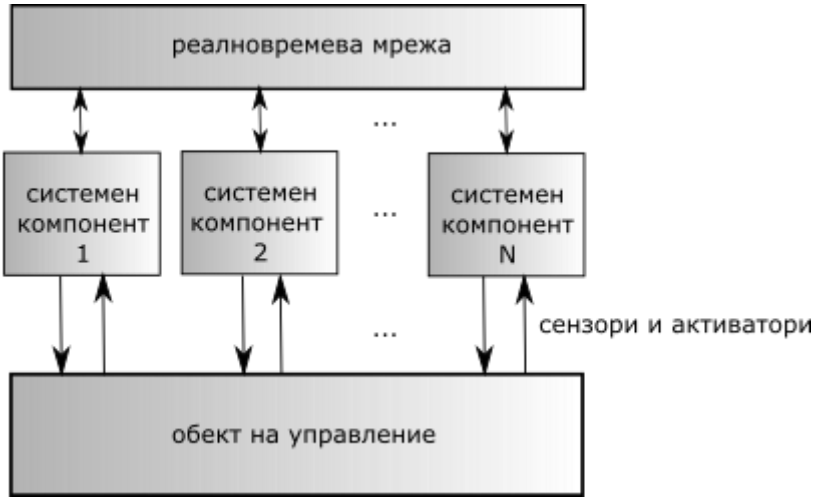
Фокусът на дисертационния труд е върху постигането на отказоустойчивост на разпределени компютърни системи за работа в реално време.

1.2 Разпределени системи за работа в реално време

Разпределените системи са изградени от компоненти, които обменят съобщения през комуникационна магистрала (реалновременна мрежа) и изпълняват общ алгоритъм за управление (*Фигура 1-2*). От гледна точка на отказоустойчивостта компонентите на системата трябва да осигуряват неразпространение на неизправностите към други компоненти. Компонентът на системата е *блок на ограничаване на неизправност* [17], [19], ако прекият ефект от единична неизправност влияе само върху функционирането на един-единствен компонент [17]. Допуска се, че блоковете на ограничаване на неизправност отказват

независимо един от друг. Това допускане е приложимо за хардуерни неизправности, които са обект на настоящото изследване.

Системата управлява индустриален процес, наречен обект на управление. Компонентите получават входни данни от сензорите на обекта на управление, изпълняват управляваща програма, която изчислява резултати, и извеждат тези резултати към активаторите на обекта на управление (*Фигура 1-2*). За да изпълняват задачите си, те трябва да комуникират с останалите компоненти чрез обмен на данни. Системните компоненти са проектирани да имат безопасно поведение, т.е. нито една неизправност не трябва да достига до изходите на компонента, както и да се разпространява към други части на системата.



Фигура 1-2. Разпределена система за работа в реално време

Разпределените системи за работа в реално време работят с крайни времеви интервали, налагани от средата и обекта на управление. При тях коректната услуга трябва да бъде коректна в областта на стойностите и в областта на времето [17]. Това означава системата да предоставя коректен резултат на обекта на управление и да го извежда в рамките на специфицирания времеви интервал. Когато времевите интервали в системата за реално време изискват стриктно спазване, за да бъде доставена коректна услуга, системата за реално време е с *твърди времеви ограничения* [17]. В противен случай тя е система за реално време с *меки времеви ограничения* [17]. Често системите работят и при двата вида ограничения едновременно, но наличието на поне една функция с твърди ограничения по време прави системата система с твърди времеви ограничения. Друго съществено разграничение на системите за реално време е в зависимост от задействащия фактор, който определя взаимодействията между системните компоненти: *събитийни разпределени системи* (задействани според момента на настъпване на съществено събитие в системата) и *периодични разпределени системи* (задействани според определен момент от течението на физическото/реалното време) [17]. Гарантоспособните разпределени системи често

изпълняват функции с твърди времеви ограничения и са периодични. Това дава възможност тяхното поведение да бъде предсказуемо и позволява да се използват по-икономично ресурсите им. Този вид системи са обект на настоящото изследване.

За постигането на отказоустойчиво поведение на компонентите в гарантоспособните разпределени системи те се конструират с репликирани модули [17], [21], [22], [23], [24]. *Модул* е най-малката заменима единица на системата. Това понятие има отношение към техниките за репликиране и метода на въвеждане на излишък в системата. Репликирането на ниво компонент може да бъде хардуерно или софтуерно реализирано. Добавят се и допълнителни средства за откриване на грешки към всеки модул [25], [26], [27], [28] – блокове за самопроверка. Самата комуникационна магистрала също може да бъде репликирана [25], [29], [30], [31]. Разнообразието от техники за репликиране дава възможност за избор на най-подходящите решения за конкретно приложение.

1.3 Управление на излишъка в отказоустойчиви разпределени системи за работа в реално време

Гарантоспособните разпределени системи за работа в реално време обикновено са предназначени за критични по отношение на безопасността приложения. Едно от основните изисквания за тяхната работа е да бъдат отказоустойчиви. Отказоустойчивостта се постига чрез използване на разнообразни техники, повечето от които се основават на някаква форма на излишък. Съществуват различни видове излишък и техники за прилагането му.

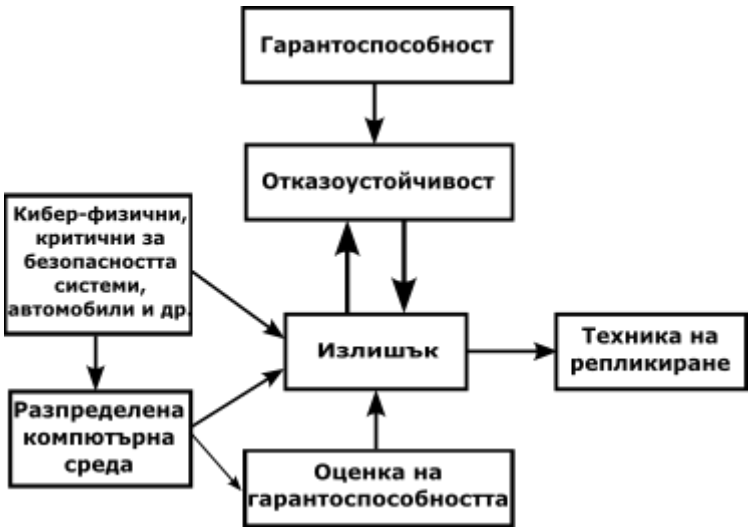
Въвеждането на излишък в компютърните системи, като метод за постигане на отказоустойчивост, и репликирането, като техническа реализация на излишъка, са добре познати и проучени [23], [24], [33], [34], [35], [36], [37], [38]. Въпреки че управлението на излишъка е разработено и приложено в различни отказоустойчиви системи отдавна, проектирането на нови гарантоспособни разпределени системи, разработването на системи от системи и кибер-физични системи [40], [41] налагат нов поглед и търсене на нови подходи за реализиране на излишъка. В критичните инфраструктури (енергийна система, водоснабдителна система, електрическа система и др.), например, критичните елементи на системата, като системата за надзорно управление и събиране на данни (Supervisory Control and Data Acquisition - SCADA), се реализират чрез използване на структурен излишък [39].

1.3.1 Проектиране на системата

Цикълът на разработване, наречен още развой, на разпределената система може да бъде представен като итеративен процес [44], който разглежда системата от две гледни точки: практическа и абстрактна. Практическата гледна точка към системата е нейното внедряване, а

абстрактният поглед върху системата е нейният модел. Тези гледни точки трябва да обменят информация помежду си, за да постигнат цялостен системен модел, който може да бъде валидиран и верифициран.

На *Фигура 1-3* е представена концепцията за осъществяване на подход за вземане на решение по отношение на осигуряване на гарантоспособността на една система чрез използване на излишък. Дадена разпределена система управлява промишлен процес, т.е. разпределена компютърна среда. Системата е подложена на неизправности, които нарушават нейната работа и застрашават управлявания процес. Проблемът с гарантоспособността на системата става въпрос на проектирането: как да бъде направена системата отказоустойчива. Неизправностите са неизбежни и непредсказуеми. Затова системата трябва да има ресурси, с които да доставя услугата, за която е предназначена, дори в присъствието на неизправности. Въвеждането на излишък е една от стратегиите за решаване на проблема с необходимата отказоустойчивост. Инженерните въпроси с прилагането на излишъка трябва да бъдат съчетани с изследователски решения. На *Фигура 1-3* те са обединени под общото наименование оценка на гарантоспособността. Моделите и техните параметри зависят от приложението (например кибер-физични системи, критични за безопасността системи, автомобили и др.) и от работната среда, т.е. разпределената компютърна среда. Атрибутите на гарантоспособността се определят въз основа на конкретното приложение. Резултатите, получени от изследването на моделите, се използват при проектирането на системата. Определя се подходящата техника на репликиране.



Фигура 1-3. Концептуален модел на подход за вземане на решение при осигуряване на гарантоспособност

Описаният процес на определяне на техниката за репликиране (*Фигура 1-3*) може да бъде използван като входни данни на схемата на жизнения цикъл на разработване на системи

или да бъде вграден в него, като по този начин специфицира изискванията за гарантоспособност.

1.4 Излишък при гарантоспособните разпределени системи за работа в реално време

Дефиницията на понятието „излишък“, която ще използваме, е следната:

Излишъкът е функционалност или компонент на една компютърна система, който добавя ресурси за изпълнение на коректната ѝ услуга.

Това е метод за внедряване на отказоустойчивост при гарантоспособни компютърни системи и на свой ред се реализира чрез техники за репликиране. Излишъкът може да бъде структурен, времеви или функционален [23], [33], [34], [37], [38].

1.4.1 Стил на репликиране при структурен излишък

Стилът на репликиране определя начина, по който репликираните компоненти изпълняват своята работа. Отказоустойчивите компоненти имат репликирани модули и само един от тях, първичният, извежда изходния резултат. Останалите реплики са вторични. В зависимост от стила на репликиране излишъкът може да бъде пасивен или активен. Резервирането е пасивна форма на излишък [23], [33], [35]. Репликирането представлява едновременна работа на идентични модули, които изпълняват едни и същи функции върху едни и същи входни данни и сравняват резултатите си [23], [33], [35], [37], [38].

1.4.2 Степен на репликиране при структурен излишък

Степента на репликиране определя броя на модулите в даден компонент. В зависимост от важността на компонента за системната работа той може да има един или повече репликирани модули или въобще да няма излишък. Степента на репликиране зависи и от изискванията за отказоустойчивост на компонентите.

При хардуерните реализации репликирането приема формата на *N-модулен излишък* [23], [34], [35], [37], [38]. Той най-често се прилага във вид на двоен и троен модулен излишък. При *двоен модулен излишък* (ДМИ) двете реплики сравняват своите резултати и, в случай на разминаване, компонентът не извежда резултат, като остава мълчалив при отказ. Обикновено модулите имат допълнителни механизми за отказоустойчивост, наречени *блокове за самопроверка*, за да решат кой модул е отказал. При *троен модулен излишък* (ТМИ) има три активни модула и гласуващ блок. Активните модули работят едновременно, а гласуващият блок определя мажоритарния резултат, който бива изведен към обекта на управление.

Репликирането на софтуера се реализира като блокове за възстановяване и N-версионно програмиране. При подхода с *блокове за възстановяване* [49], [50] се правят две алтернативни

програми (наречени алтернативи) от обща спецификация на услугата и се въвежда приемащ тест, който решава дали резултатът е правилен. Приемащият тест се прилага последователно върху резултатите на двете алтернативи. Ако резултатите на първичната алтернатива не преминат приемащия тест, се изпълнява втората алтернатива. Подходът с блокове за възстановяване съответства на резервирането в готовност при хардуера.

При *N-версионното програмиране* [49], [51], [52] съществуват N ($N \geq 2$) варианта на софтуера, които се изпълняват едновременно и резултатите им се сравняват. Вариантите са софтуерни програми, които са написани от различни екипи от програмисти и по възможност използват различни алгоритми. Предполага се, че това спомага да бъдат избегнати общите грешки, които програмистите са склонни да правят. Резултатите на софтуерните версии се гласуват и се извежда мажоритарният резултат. Хардуерният еквивалент на N-версионното програмиране е N-модулният излишък.

При *N-самопроверяващото програмиране* [49] се изпълняват N самопроверяващи се софтуерни компонента, като един от тях се смята за действащ, а останалите самопроверяващи се компоненти са негови „горещи“ резерви. При отказ на действащия компонент действието се превключва към някой от резервните самопроверяващи се компоненти.

1.4.3 Времеви излишък

Времевият излишък изисква да бъде заделено допълнително време за изпълнението на задачи [23], [37], [53], [54]. Той създава по-малък разход в сравнение със структурния излишък, но може да повлияе на производителността на системата и затова трябва да бъде подчинен на ограниченията за реално време.

1.4.4 Функционален излишък

Функционалният излишък се внедрява в софтуера. В [33] той се дефинира като квалифициране на поведението на системата по отношение на нейните входни/изходни взаимоотношения. Функционалният излишък е полезен при откриването на грешки.

1.5 Въвеждане на излишък

Гарантоспособността в разпределените системи за реално време, които работят в критични за безопасността приложения, е станала част от тяхното проектиране. Всички параметри и системни компоненти, които са важни за отказоустойчивото функциониране на системата, се включват в жизнения цикъл на разработване на системата. Описателен многослоен модел на проектиране на разпределени системи със структурен излишък е илюстриран на *Фигура 1-4*.

Въвеждането на структурен излишък включва определянето на критичните елементи, на важните системни параметри и на нивата на критичност. Компонентите на разпределената система управляват различни параметри на обекта на управление с различна значимост за отказоустойчивото функциониране на системата. На етапа на определяне на изискванията в жизнения цикъл на разработване на системата трябва да бъдат определени контролираните параметри и да бъдат откроени нивата на критичност. Компонентите, които управляват важните параметри, получават високо ниво на критичност и трябва да бъдат отказоустойчиви.

Фигура 1-4. Синтез на подход на гарантоспособни разпределени системи със структурен излишък

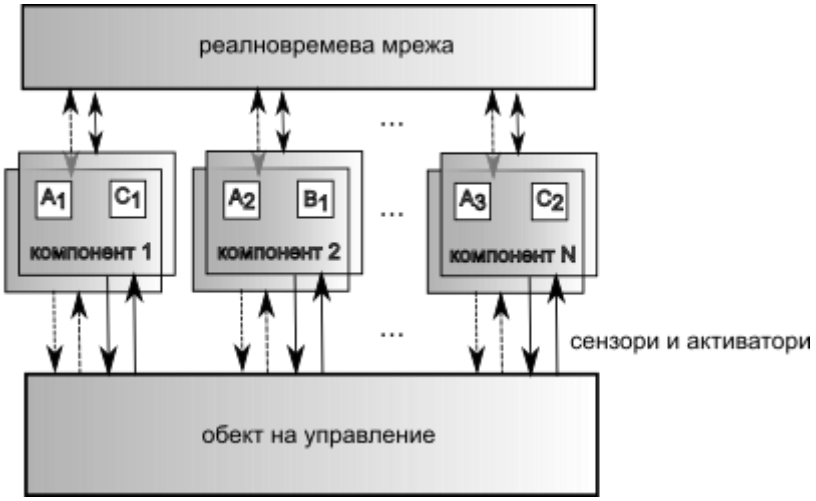
На етапа на проектиране на системата се определят степента и стила на репликиране. Степента на репликиране определя дали ще бъдат приложени компоненти с единичен (ЕМИ), двоен (ДМИ) или троен модулен излишък (ТМИ). Избраният стил на репликиране определя дали ще бъде използвано активно или пасивно репликиране. Модулите в системните компоненти могат да бъдат равномерно разпределени, т.е. всички компоненти могат да имат еднакъв брой модули, или могат да използват смесен излишък. На етапа на действителното изграждане в жизнения цикъл на разработване на системата се внедрява определената системна архитектура, например GUARDS [56], [57], многостранна гарантоспособност [47], [48] или DECOS [58], [59], както е показано на *Фигура 1-4*.

1.6 Внедряване на различни степени на репликиране

1.6.1 Еднакъв излишък за всички компоненти

Най-прекият начин да се приложи излишък е да бъдат репликирани активните компоненти и да бъдат сравнявани техните резултати. При разпределените системи компонентите могат да бъдат изградени от два или три идентични модула, които да изпълняват една и съща задача (*Фигура 1-5*). Резултатите на репликираните модули се сравняват (както е

в [25], [28], [49], [58]) или се гласуват в случай на използване на ТМИ (както е в [17], [62]). Ако няма разминаване, предполагаемо верният резултат се извежда към обекта на управление. При разлика не се извежда резултат, а компонентът се поставя в безопасно състояние според конвенциите на системата.



Фигура 1-5. Гарантоспособна разпределена система за работа в реално време

Хардуерните компоненти на системата имат еднаква степен на репликиране, но софтуерните компоненти, изпълняваните задачи, могат да имат различен излишък. Например, на *Фигура 1-5* са изобразени три задачи – A, B и C; задача A има три копия, задача B има едно, а задача C има две. Копията могат да бъдат разположени в различни системни компоненти, като по този начин се постига изолиране на грешките.

1.6.2 Различен излишък за компонентите

Има системи, които използват различна степен на репликиране за своите компоненти. В GUARDS [57] съществуват нива на доверие и нива на критичност. Нивата на доверие се дефинират според степента, до която може да се има доверие на даден системен компонент – колкото по-доверен е компонентът, толкова по-високо ниво на доверие има [56]. Степента на доверие, възложена на компонента, зависи от неговата критичност. За критични компоненти се смятат тези, чийто отказ води до тежки последствия. Такива компоненти имат по-висока степен на доверие.

Моделът на репликиране в DEAR-COTS [28], [66] използва активен излишък на софтуерните компоненти и позволява определянето на степента на репликиране на специфични части от приложението за реално време в съответствие с надеждността на компонентите и желаното ниво на надеждност за приложението. Архитектурата DEAR-COTS е насочена към разпределени компютърно управляеми системи, които работят в реално време и може да използва както равномерно, така и смесено разпределение на излишъка.

Проектът DECOS [58], [59] предлага интегрирана разпределена архитектура, която да поддържа системи със смесена критичност. Системите със смесена критичност се състоят от разпределени части на приложението с различни нива на критичност, изпълняващи се върху един и същ физически хардуер.

Системата MEAD [48] предлага съчетаване на противоречивите изисквания за отказоустойчивост и реално време при прилагане на гарантоспособност на ниво мидълуер. MEAD е инфраструктура, която предлага прозрачна и регулируема отказоустойчивост в реално време, проактивна гарантоспособност, системно адаптиране към пълен отказ, неизправности в комуникацията и във времето с отчитане на наличните ресурси и скалируемо и бързо откриване на неизправности и възстановяване от тях. Регулируемата отказоустойчивост се постига чрез т.нар. подход на многостранната гарантоспособност (versatile dependability) [47], [48]. Този подход дава възможност за изграждане на гарантоспособни софтуерни архитектури, като се отчитат три важни аспекта – отказоустойчивост, производителност и ресурси. Той предоставя набор от инструменти, наречени „копчета“, за настройване на баланса между тези аспекти.

Повечето гарантоспособни разпределени системи за реално време следват архитектурния стил, изобразен на *Фигура 1-5*. Те използват еднакво репликирани физически компоненти и смесен излишък на софтуерните компоненти. Съществуват възможности за разработване на системи, които се адаптират към конкретни приложения чрез разпределение на хардуерния структурен излишък.

1.7 Изводи и резултати

В *Глава 1* са представени основните понятия от предметната област на дисертацията – гарантоспособни разпределени системи за работа в реално време. Откроена е тяхната структура по отношение на гарантоспособността и реалното време. Управлението на структурния излишък е разгледано през призмата на системното проектиране. Създаден е концептуален модел на подход за вземане на решения при осигуряване на гарантоспособност. Този модел се вписва в жизнения цикъл на проектиране на системи и отговаря на изискването гарантоспособността да бъде заложена в системните спецификации.

Направен е обзор на методите и техниките за въвеждане на излишък в отказоустойчиви системи и е синтезирана класификация на гарантоспособни разпределени системи със структурен излишък, която показва вграждането на изискванията за гарантоспособност в етапите на проектиране на системата.

Представен е кратък обзор на известните гарантоспособни разпределени системи от гледна точка на управлението на структурния излишък. Двете тенденции са да се използва

еднакъв излишък за всички системни компоненти или компонентите да имат различен излишък.

Изложението в *Глава 1* отговаря на изпълнението на задача 1 на дисертацията.

Постигнатите научни и научно-приложни резултати са:

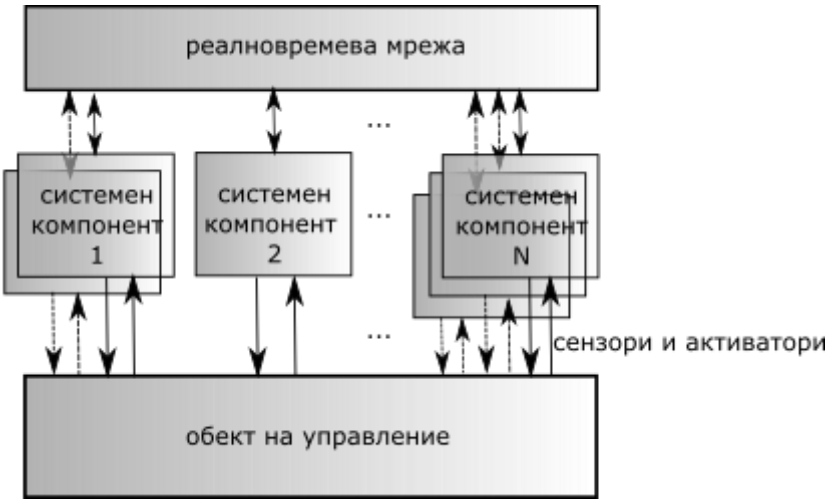
1. Създаден е концептуален модел на подход за вземане на решения при осигуряване на гарантоспособност;
2. Предложен е синтез на класификация на гарантоспособни разпределени системи със структурен излишък.

Глава 2. Моделиране на отказоустойчивата разпределена система с настройваема надеждност

Предложената в дисертацията архитектура на отказоустойчива разпределена система (ОРС) с настройваема надеждност е основана върху понятието за настройваемост.

Настройваемост е свойството на гарантоспособната разпределена система за реално време да разпределя структурния излишък според изискванията за надеждност на приложението.

Отказоустойчивата разпределена система с настройваема надеждност [73], [74], [75], [76] прилага различни степени на репликиране на хардуерните компоненти (*Фигура 2-1*).



Фигура 2-1. Гарантоспособна разпределена система за реално време с настройваема надеждност

Необходимостта системата да има компоненти с различна степен на репликиране е свързана с тяхната критичност. За разлика от подходите, прилагащи смесена критичност на частите на приложния софтуер, които се изпълняват на еднакво/равномерно репликиран

хардуер, подходът с настройваема надеждност предлага степента на репликиране на хардуерните компоненти да се определя според тяхната критичност на етапа на проектиране и те да работят със смесен излишък. В дисертацията е направена количествена оценка на възможностите за реализиране на гарантоспособни разпределени системи с предложения подход и те са сравнени със системи без разпределение на структурния излишък. Сравнението е направено с помощта на модели, решени посредством симулационно моделиране, и резултатите (представени в *Глава 3* и [76]) показват, че съществуват разпределения на излишъка, които постигат общата системна надеждност, изисквана от приложението.

Отказоустойчивата разпределена система с настройваема надеждност (*Фигура 2-1*) е изградена от компоненти, ограничаващи неизправностите. Компонентите могат да имат различна степен на репликиране в зависимост от критичността си. Всеки модул има блок за самопроверка, чрез който се откриват грешки и се осигурява спиране/мълчание при отказ. Системата работи при твърди времеви ограничения. Този подход позволява предвидимост на поведението на системата, като времената за изпълнение на системните задачи са гарантирани. Чрез промяна на структурния излишък на компонентите в етапа на проектиране се цели промяна на надеждността на системата според изискванията на приложението. Моделират се хардуерни неизправности и се цели постигане на хардуерна надеждност.

2.1 Анализ на начините за моделиране на гарантоспособни системи

Моделирането е често използван похват за изследване на системи, преди те да бъдат реално проектирани и внедрени. Това дава възможност да се проверят различни хипотези и да се намери подходящият модел, въз основа на който да се търсят конкретни инженерни решения. Моделирането позволява сравнение между различни варианти за изграждане на системата или на части от нея по ефективен начин по отношение на цената, тъй като възможните инженерни реализации не винаги могат да се оценят количествено при сложни системи.

Поради стохастичната природа на неизправностите показателите, с които се оценява тяхното въздействие върху функционирането на гарантоспособните системи, имат вероятностен характер. Затова за описанието им се използват понятия от областта на теорията на вероятностите и математическата статистика.

2.1.1 Методи за моделиране на гарантоспособни системи

Моделите на системата могат да бъдат анализирани или математически оценявани посредством три различни подхода [77]: симулационен, аналитичен и хибриден (комбинация от симулационни и аналитични методи). Моделират се само основните характеристики на

системата. При *симулирането* тя се описва в компютърна програма, която имитира нейната динамика. При аналитичните методи се съставят и решават системи от математически уравнения, които определят системната динамика [77], [78], [79], [80]. Предимството на симулирането е, че могат да се представят подробно характеристиките на изследваната система, без да се налагат много ограничения върху модела. При аналитичните модели допусканията често се опростяват, за да могат да се решат системите от уравнения. Точността при симулирането се ограничава единствено от времето, необходимо за получаване на краен резултат. Възможно е и комбинираното прилагане на двата подхода, което все още не е честа практика [77].

При друга класификация [81] моделите се разглеждат като комбинаторни и модели, основани на пространство на състоянията. *Комбинаторните модели* включват диаграми с блокове на надеждност [77], [82], [83], [84], дървета на събитията [81] и дървета на неизправностите [77], [85], [86]. Те са сравнително лесни за проектиране и обработване и могат да се анализират с комбинаторни методи. Техен недостатък е ограничената им моделираща способност, дължаща се на допускането за статистическа независимост на събитията.

Моделите с пространство на състоянията включват Марковски вериги и мрежи на Петри [84], [87]. Те представят поведението на системата посредством достижими състояния и възможни преходи между тях. Те имат по-голяма моделираща мощност от комбинаторните модели, които не могат да обхванат характеристиките на моделираната система.

Проблемът при методите с пространство на състоянията е т.нар. ефект на „експлозия“ на пространството на състоянията – експоненциално нарастване на пространството на състоянията при нарастване на броя на компонентите. Това води до повишаване на цената на изчисленията. В такъв случай мрежите на Петри и Марковските вериги могат да бъдат симулирани [81].

2.1.2 Надеждностни характеристики на отказоустойчивата система с настройваема надеждност

Като част от изискванията към симулационната програма за моделиране на отказоустойчивата система с настройваема надеждност се изчисляват следните характеристики на системата: надеждност *R*, средно време до отказ *MTTF*, средно време до спиране *MTTS*, общо време на престой, средно време между отказите *MTBF*, средно време между спиранията *MTBS*, средно време за ремонт след отказ *MTTR*, готовност *A*.

Най-често използваната функция на разпределение при моделиране на отказоустойчиви системи е експоненциалното разпределение. То е подходящо заради свойството си да не съдържа памет за състоянието на системата. Експоненциалното

разпределение в достатъчна степен отразява динамиката на гарантоспособните системи и предлага удобно математическо представяне. При моделирането се допуска също, че интензивността на неизправностите е постоянна [84].

Надеждността е вероятността системата да бъде в работно състояние в даден момент *t*. При допускането за експоненциално разпределение на събитията в системата функцията на разпределение става [37], [84]

$$F(t) = 1 - e^{-\lambda t}. \quad (1)$$

Плътността на разпределение е [37], [84]

$$f(t) = \lambda e^{-\lambda t}. \quad (2)$$

Надеждността на системата се изразява като експоненциална функция [37], [84]

$$R(t) = e^{-\lambda t} = 1 - F(t). \quad (3)$$

Средното време до отказ MTTF се изчислява като средна стойност на времето до отказ на компонент за определен период на работа. То е математическото очакване на времето до (първи) отказ. При постоянна интензивност на неизправностите *MTTF* е [37], [84]

$$MTTF = \frac{1}{\lambda}. \quad (4)$$

Средното време между отказите MTBF може да се изчисли като средно аритметичното време между отказите на системата. *MTBF* се измерва за ремонтируеми системи. При експоненциално разпределение и постоянна интензивност на неизправностите $MTBF = 1/\lambda$.

Средното време за ремонт MTTR представлява средното време, което се изисква за ремонт на отказали елементи на системата. При експоненциално разпределение с постоянна интензивност на неизправностите

$$MTTR = 1/\mu. \quad (5)$$

Готовността A се измерва с вероятността системата да е работоспособна в момент *t*, независимо от това колко пъти е била неработоспособна в интервала (0,*t*). За постоянни интензивности на неизправностите и ремонтите готовността може да бъде изразена чрез следната формула [37], [84]

$$A = \frac{\mu}{\lambda+\mu} = \frac{MTBF}{MTBF+MTTR}. \quad (6)$$

Общото време на *престой* е сумата от всички периоди, през които системата е била неработеща. Средното време за престой се изразява с (П12) (*Приложение А*).

Системата работи при следните определения за отказ и стоп. *Отказ* на системата настъпва, когато повече от половината компоненти откажат с неоткрит отказ или при повече от половината отказали компоненти броят на тези с неоткрит отказ е по-голям от броя на компонентите с открит отказ.

$$N_u > \frac{N}{2} \text{ или } N_u + N_d > \frac{N}{2} \text{ и } N_u \geq N_d, \quad (7)$$

където N_u е броят на компонентите с неоткрит отказ, а N_d – броят на компонентите с открит отказ. Системата *спира*, когато повече от половината компоненти откажат с открит отказ или при повече от половината отказали компоненти броят на тези с открит отказ е по-голям от броя на компонентите с неоткрит отказ.

$$N_d > \frac{N}{2} \text{ или } N_u + N_d > \frac{N}{2} \text{ и } N_d > N_u. \quad (8)$$

2.2 Допускания при моделирането на системата

Моделът на отказоустойчивата система с настройваема надеждност е изграден въз основа на допускания, отразяващи нейното поведение и възприетите за изследването режими на неизправност, отказ и ремонт.

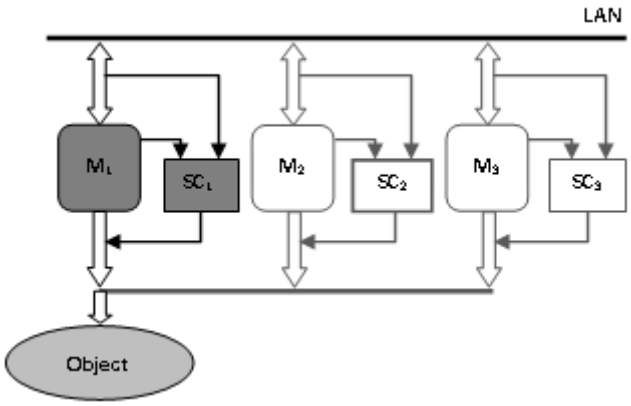
Разпределената система с настройваема надеждност [73], [74], [75], [76] е изградена от компоненти с активен излишък. Компонентите имат еднотипни модули, всеки от които притежава средства за самопроверка с покритие C. Степента на репликиране на компонентите се определя в зависимост от тяхната критичност – колкото по-важен за приложението е даден компонент, толкова по-критичен е той и е по-висока степента му на репликиране. Разглеждат се три степени на критичност/репликиране. Компонентите, чийто отказ не застрашава нормалното функциониране на системата и не води до катастрофални последствия, могат да разчитат само на средствата си за самопроверка и да не бъдат репликирани. Техният коефициент на покритие е C_1. Компонентите с по-голяма критичност за приложението, които обаче е достатъчно просто да спрат да извеждат управляващо въздействие в случай на отказ, са компоненти с ДМИ. При тях е възможно отказалият модул да бъде ремонтиран, стига неизправността му да е открита от блока за самопроверка. Компонентите с ДМИ имат коефициент на покритие $C_2>C_1$. Най-критичните компоненти за системата, чийто отказ би имал катастрофални последствия за приложението, се изграждат с ТМИ и имат коефициент на покритие $C_3>C_2>C_1$.

Отказоустойчивата система с настройваема надеждност толерира постоянни хардуерни неизправности с интензивност λ_p. При компоненти с двоен и троен модулен излишък е

възможно възстановяване (локален ремонт) след неизправност на модул с интензивност на възстановяване μ_p. Системата може да работи без или с ремонт, като при ремонтируема система интензивността на ремонтите е μ_{sys}.

2.3 Модел на компонент на системата

Компонентът на разпределената система с настройваема надеждност е изграден от еднотипни модули M_i (i=1, 2, 3), всеки от които има собствен блок за самопроверка SC_i (*Фигура 2-2*) [94]. В зависимост от критичността им модулите могат да се дублират или триплират, за да се постигне по-висока надеждност в точката от управляващия контур, където е разположен компонентът.



Фигура 2-2. Компонент на разпределената система с настройваема надеждност

Един от модулите е основен и той единствен извежда управляващо въздействие към обекта на управление. Всички модули изпълняват едновременно управляващата програма и изчисляват управляващото въздействие (активен излишък). Модулите, които не извеждат резултат към обекта на управление, извършват контрол на основния модул и участват при сравнението на резултатите. Те могат да поемат управлението при отказ на основния модул.

При единичен модул само средствата за самопроверка могат да открият отказ при изпълнението на управляващата програма и да забранят извеждането на управляващо въздействие. Ако приложението налага по-силна защита на изходите и по-високо покритие на неизправностите, към единичния модул се добавят допълнителни един или два модула със собствени средства за самопроверка, като по този начин може да се отговори на различни нива на критичност, диктувани от приложението на ОРС с настройваема надеждност.

2.3.1 Функции на системен компонент

Характерно за предложения подход е вграждането на локален блок за самопроверка във всеки модул, реализация на протокол за разпределено гласуване и следене на състоянието.

Блокът за самопроверка [73] е вграден като допълнителен блок към конфигурацията на модула и има проверяващи и управляващи функции.

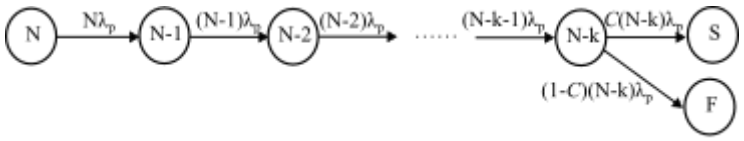
2.3.2 Режим на отказ

Компонентът отказва, когато откажат всички негови модули. Благодарение на въвеждането на средства за самопроверка и излишък не всеки неоткрит отказ в отделен модул води до отказ на целия компонент. Възможни са две състояния при отказ на модул – стоп и отказ.

2.4 Модел на системата

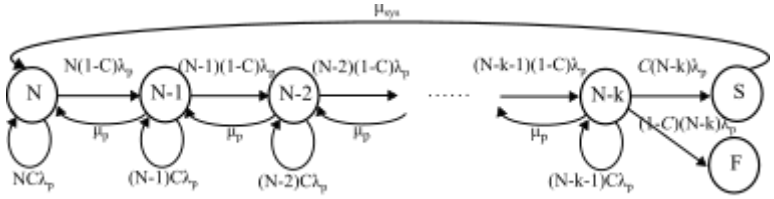
Работата на системата е представена с Марковски процес, където всяко от състоянията в Марковската верига изобразява състоянието на системата след настъпила неизправност според броя на работещите компоненти *N*, а дъгите са преходите между отделните състояния при възникване на постоянна неизправност с интензивност на потока на неизправностите λ_p. Покритието на механизмите за самопроверка е *C*. Разгледани са различни възможности за работата на системата: с и без възстановяване след постоянна неизправност и с и без системен ремонт.

Когато системата е без ремонт, тя работи до изчерпване на ресурсите си и влиянието на коефициента на покритие *C* върху надеждността е незабележимо (*Фигура 2-3*).



Фигура 2-3. Марковски модел на система без възстановяване след постоянна неизправност и без ремонт

Ако системата има възможност за локален ремонт, *C* спомага за удължаване на живота на компонента, това влияе и върху надеждността на системата. Влиянието на *C* расте, защото само при детектиран отказ на компонент той може да бъде ремонтиран преди да настъпи системен отказ. Системен ремонт се извършва след попадане на системата в стопово състояние. Изправните компоненти продължават работа след ремонта със същите начални характеристики. Отказоустойчивата разпределена система с настройваема надеждност може да работи и със системен ремонт и възстановяване на компонент от постоянна неизправност (*Фигура 2-6*). Това предполага постигане на по-добри надеждностни характеристики.



Фигура 2-6. Марковски модел на система с ремонт и възстановяване от постоянна неизправност

Всички описани възможности в Марковските модели (*Фигура 2-3* - *Фигура 2-6*) са изследвани чрез симулационното моделиране на системата.

2.5 Изводи и резултати

В *Глава 2* е представена разработената от автора отказоустойчива разпределена система с настройваема надеждност. Тя предлага различни степени на репликиране на хардуерните компоненти. Необходимостта системата да има компоненти с различна степен на репликиране е свързана с тяхната критичност, която се определя от изискванията на приложението. Отказоустойчивата система с настройваема надеждност е моделирана при определени допускания за нейната работа с цел да се провери тази хипотеза.

Предложената от автора отказоустойчива разпределена система с настройваема надеждност е моделирана въз основа на използване на Марковски вериги и валидирана чрез симулация. Методът на симулационното моделиране е избран, защото симулацията дава възможност да се моделират системи с множество компоненти и голяма степен на детайлизация. Представени са моделите на компонент на системата и на цялата система. Предвидени са възможности за моделиране на системата с настройваема надеждност с и без възстановяване от постоянна неизправност, както и с и без системен ремонт.

Представените в *Глава 2* резултати изпълняват задачи 2 и 3 на дисертацията. Постигнатите научни резултати са създаването на модел на предложената отказоустойчива разпределена система с настройваема надеждност и представянето на авторски архитектурен модел на отказоустойчива разпределена система с настройваема надеждност, като са дефинирани изискванията към нейните компоненти и системата като цяло.

Глава 3. Изследване на отказоустойчивата система с настройваема надеждност

Отказоустойчивата система с настройваема надеждност управлява обект, като получава входни данни от неговите сензори, изпълнява управляващ алгоритъм и изчислява изходни резултати, които извежда към активаторите на обекта. Параметрите на обекта на управление могат да имат различна важност за коректната системна работа. Затова компонентите на

системата са репликирани според своето ниво на критичност. Настройването на системната надеждност посредством разпределяне на степента на репликиране на компонентите според нуждите на управлявания обект може да използва ресурсите на системата по-ефикасно и би могло да подобри нейната надеждност.

Симулационното моделиране на системата с настройваема надеждност изследва как промяната на структурния излишък влияе върху общата системна надеждност. Компонентите с различна степен на репликиране имат различно ниво на критичност за системата. Това определя и коефициента на покритие на техните средства за самопроверка: C_1 за единичните компоненти, $C_2>C_1$ за компонентите с двоен модулен излишък и $C_3>C_2>C_1$ за триплираните компоненти. Коефициентите на покритие могат да се изменят в зависимост от условията на средата или от условията на функциониране в рамките на някакви граници. Тези коефициенти заедно с интензивността на неизправностите λ_p определят поведението на компонентите в симулационния модел на отказоустойчивата система с настройваема надеждност. Събитията в системата са свързани с промяната на нейното състояние. Това са случайни събития, характеризиращи се със съответната интензивност на възникване: λ_p, μ_p и μ_{sys}. Допуска се, че отказал компонент може винаги да бъде възстановен след постоянна неизправност (локален ремонт), а времената до отказ са нормално разпределени.

Разработен е следният *изследователски протокол*:

1. Изследване на компонент
2. Изследване на системата
   - Входни данни: брой компоненти в системата N, брой модули в системата M, λ_p, μ_p, μ_{sys}, граници на коефициентите на покритие C_1, C_2 и C_3.
   - Изходни резултати: $R(t)$, *A, MTTF, MTTR, MTTS, MTBF, MTBS, downtime*
   - Определяне на възможните разпределения на структурния излишък при зададените N и M.
3. Определяне на времената до отказ при дадените входни параметри за всички разпределения на модулния излишък на системи с и без настройване на структурния излишък.
4. Изследване на влиянието на различни параметри върху надеждностните характеристики на отказоустойчивата система с настройваема надеждност и на системи без разпределение на структурния излишък.
5. В зависимост от резултатите определяне на конфигурациите с най-висока системна надеждност.

3.1 Симулационно моделиране на отказоустойчива система с настройваема надеждност

Избраният в *Глава 2* изследователски метод на симулационно моделиране е приложен чрез разработване на симулационна програма. Тя е проектирана според описания изследователски протокол и определя надеждностните характеристики на изследваната система, формулирани в т. 2.1.2. Програмата симулира отказоустойчиви системи с различно разпределение на структурния излишък и системи без разпределение на структурния излишък, което дава възможност за тяхното сравнение и анализиране.

3.1.1 Симулационна програма

Разработеният програмен продукт NMRSIM за симулиране на поведението на отказоустойчиви разпределени системи (представен по-пълно в *Приложение В*) определя показателите на системите от интерес за изследването и дава възможност за сравнение на предложената система със системи без настройване на надеждността. Програмата е написана на език за програмиране C++ и разработването ѝ изпълнява следните изисквания:

1. Да симулира поведението на системата във времето, като отразява зададените дефиниции за стоп и отказ;
2. Да представя настъпването на постоянна неизправност като стохастичен процес с експоненциално разпределение и интензивност на неизправностите λ_p;
3. Да има възможност да моделира система с ремонт и без ремонт;
4. Да представя моментите на извършване на ремонтите като стохастичен процес с експоненциално разпределение и интензивност на ремонтите μ_p (за локален ремонт) и μ_{sys} (за системен ремонт);
5. Да моделира система с произволен брой модули и компоненти;
6. Да изчислява надеждностните характеристики, посочени в *Глава 2*, т. 2.1.2;
7. Да моделира поведението при неизправност на компонент и цялата система;
8. Да разпределя структурния излишък при зададен общ брой компоненти и общ брой модули;
9. Да моделира коефициента на покритие на средствата за самопроверка;
10. Да изчислява надеждността като функция на времето;
11. Да изчислява статистическите показатели на получените резултати;
12. Да съхранява получените резултати.

Програмният продукт за симулационно моделиране на предложената отказоустойчива разпределена система с настройваема надеждност е основан на моделиране на

функционирането на системата във времето и моментите на настъпване на неизправност. Блоковата структура на симулационната програма е изобразена на *Фигура 3-2*.

Фигура 3-2. Структура на симулационна програма NMRSIM

В блока на входни данни се задават N, M, λ_p, μ_p, μ_{sys}, C_1, C_2, C_3 и R_{total}. Програмата използва генератор на псевдослучайни числа, работещ според алгоритъма, представен в [98]. Той се използва при определяне на момента на настъпване на неизправност и за генериране на случайни стойности на коефициентите на покритие. При дадени N и M в блока за определяне на конфигурациите на структурния излишък се определят всички възможни разпределения на структурния излишък. Блокът за определяне на неизправност в компонент определя моментите на неизправност за съответния компонент. Текущата неизправност се определя в съответния блок след сравнение на моментите на неизправност във всички компоненти.

В зависимост от степента на репликиране в блока за определяне на коефициентите на покритие се задават коефициентите C_1, C_2 и C_3 на отделните компоненти. В блока за определяне на състоянието на компонент се определя дали компонентът е отказал, дали отказът му е открит и дали е в ремонт. В блока за определяне на системното състояние се определя дали системата е в стопово или отказово състояние. При наличие на системен отказ се записват всички натрупани времена до отказ и се преминава към определяне на надеждностните характеристики. Ако системата е в стопово състояние цикълът продължава, а моментът на спиране се записва.

В блока за изчисляване на надеждностните характеристики се определят *R*, *MTTF*, *MTTR*, *MTBF*, *MTBR*, *MTTS*, *MTBS*, *A* и *downtime*. За реализиране на подхода на настройваема надеждност се използва блока за определяне на конфигурациите, които постигат зададената системна надеждност R_{total}. Всички получени данни се обработват статистически в блока за определяне на статистически параметри. Получените резултати за надеждностните характеристики на всички конфигурации на структурния излишък се записват във файлове. Това се прави в блока на изходните резултати. Взаимодействието между отделните блокове на симулационната програма е изобразено схематично на *Фигура 3-2*.

Блоковата структура на програмата дава възможност тя да бъде разширявана и надграждана, за да могат да се моделират и други гарантоспособни разпределени системи.

3.2 Резултати от симулационно моделиране на системата

Отказоустойчивата система с настройваема надеждност е симулирана при следните параметри: брой компоненти N=10 и N=20, брой модули съответно M=20 и M=40, интензивност на постоянните неизправности $\lambda_p=10^{-3}$ 1/h и $\lambda_p=10^{-4}$ 1/h, интензивност на възстановяване след постоянна неизправност μ_p=0.1 1/h, интензивност на ремонтите μ_{sys}=0.1 1/h, граници на коефициентите на покритие $C_1 \in [0.8, 0.9)$, $C_2 \in [0.9, 0.95)$ и $C_3 \in [0.95,\ 1.0)$.

При изследването на различните разпределения на структурния излишък в компонентите е използвана следната нотация:

система (i, j, k),

където i – брой на единичните компоненти, j – брой на компонентите с двоен модулен излишък, k – брой на компонентите с троен модулен излишък. Например, система (3,4,3) при N=10 и M=20 означава система с 3 единични, 4 дублирани и 3 триплирани компонента.

Изследвани са разпределения на структурния излишък, които запазват общия брой на модулите в системата. Хипотезата на настоящото изследване предполага проучване на възможностите за разпределение на хардуерните ресурси на системата според тяхната критичност при определени изисквания за надеждност, съобразени с приложението. Като

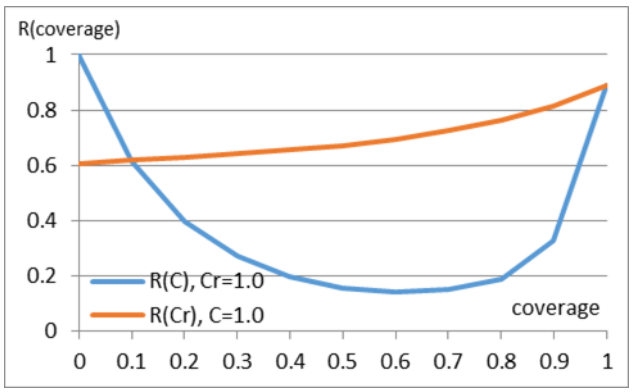
еталонна система за сравнение е избрана система, изградена само от дублирани компоненти, която не разпределя структурния излишък. При това положение броят на модулите в системата е $M=2N$. Интерес представляват само конфигурациите, които удовлетворяват това ограничение.

3.2.1 Изследване на компонент

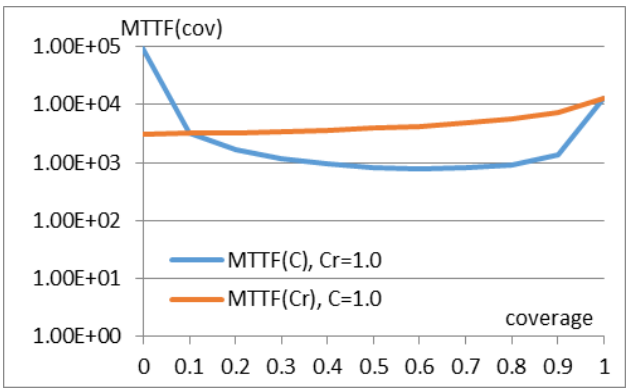
Резултатите от симулационното моделиране са представени за компонент, изграден от два и от три модула. Показателите на надеждността са отчетени за случаите на компонент с локален ремонт и без локален ремонт. Изследвано е влиянието на постоянни и случайни неизправности. Данните са за следните интензивности на неизправностите и ремонтите: постоянни неизправности на процесор $\lambda_p=10^{-2}$ 1/h, случайни неизправности на процесор $\lambda_t=0.1$ 1/h, възстановяване на процесор след постоянна неизправност $\mu_p=0.1$ 1/h, ремонт на компонент $\mu_c=0.1$ 1/h.

При компонент с двоен модулен излишък отказоустойчивостта се постига чрез блоковете за самопроверка на двата модула (с коефициент на покритие C) и чрез сравнение на резултатите на модулите. Компонентът *отказва*, когато едновременно откажат и двата процесора на модулите **и** средствата за самопроверка не са открили отказа. Компонентът попада в *стопово състояние*, когато сравнението показва разлика, но средствата за самопроверка **не са** открили отказа.

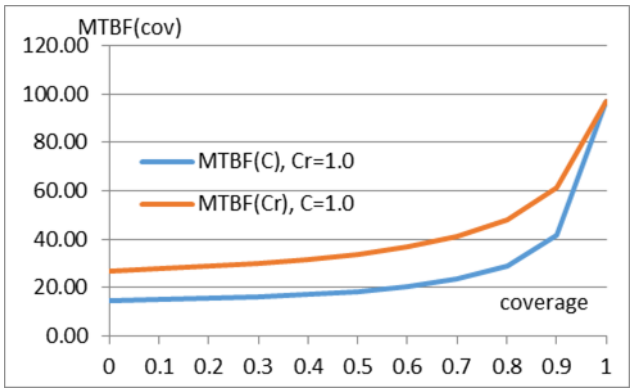
На *Фигура 3-3 – Фигура 3-10* са показани надеждностните характеристики на дублиран компонент във функция от коефициентите C и C_r за система с локален ремонт. За ниски и високи стойности на коефициента на покритие дублираният компонент има по-висока надеждност и *MTTF* (*Фигура 3-3* и *Фигура 3-4*), отколкото за средни стойности на този коефициент. Това се дължи на влиянието на сравнението, което при ниски стойности на C на практика го неутрализира, защото при сравнение неизправностите в компонента се откриват с вероятност 1. При високи стойности на C покритието на неизправностите има силно значение за по-добрите надеждностни показатели на компонента. Коефициентът на покритие на средствата за самопроверка подобрява готовността на компонента (*Фигура 3-9*).



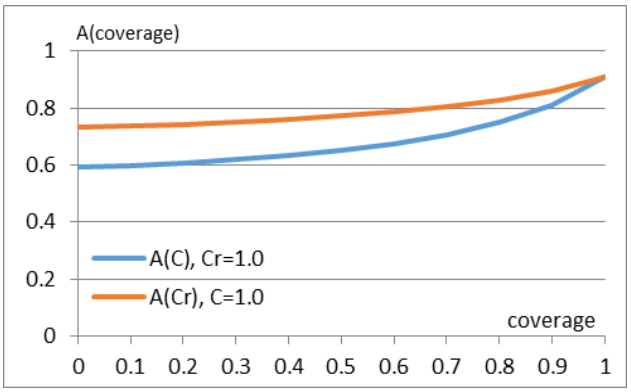
Фигура 3-3. Надеждност на дублиран компонент на система с локален ремонт



Фигура 3-4. MTTF на дублиран компонент на система с локален ремонт

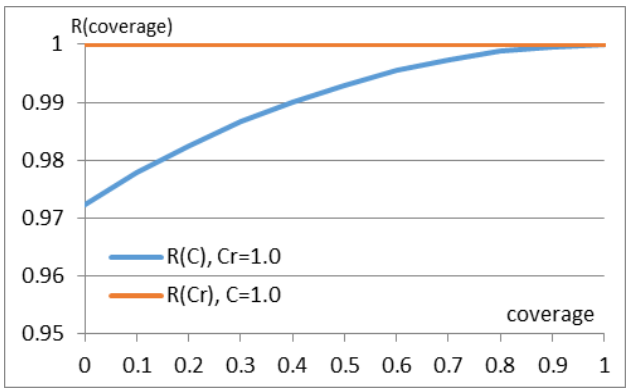


Фигура 3-8. MTBF на дублиран компонент на система с локален ремонт

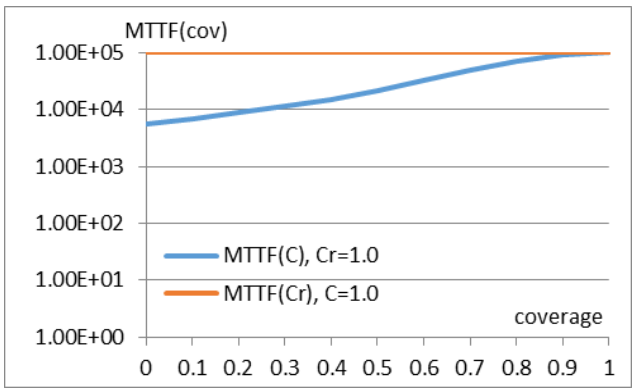


Фигура 3-9. Готовност на дублиран компонент на система с локален ремонт

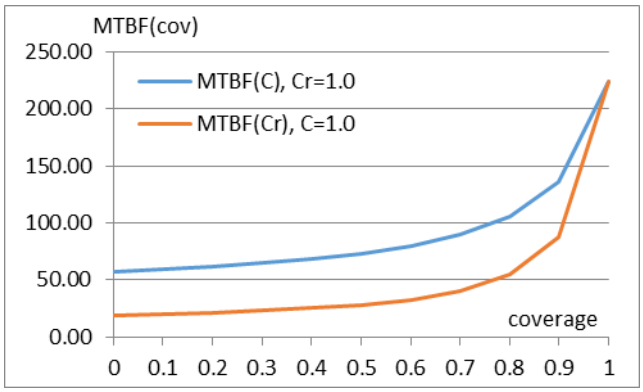
При компонент с троен модулен излишък отказоустойчивостта се постига отново чрез блоковете за самопроверка, а сравнението е всъщност мажоритарно гласуване. *Отказ* настъпва, когато повече от половината модули са с неоткрита неизправност. Компонентът попада в *стопово състояние*, когато повече от половината модули са с открита неизправност. На *Фигура 3-13 – Фигура 3-20* са представени надеждностните характеристики на компонента за система с локален ремонт. Коефициентът C_r влияе слабо върху повечето надеждностни показатели на триплирания компонент (*Фигура 3-13 - Фигура 3-16*). Той обаче води до намаляване на времената между отказите и на готовността на компонента (*Фигура 3-17 - Фигура 3-20*).



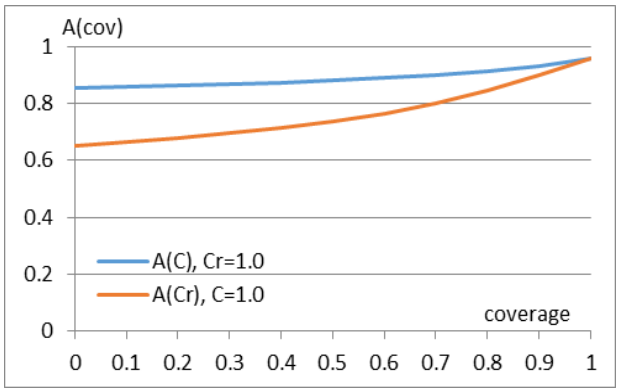
Фигура 3-13. Надеждност на триплиран компонент на система с локален ремонт



Фигура 3-14. MTTF на триплиран компонент на система с локален ремонт



Фигура 3-19. MTBF на триплиран компонент на система с локален ремонт



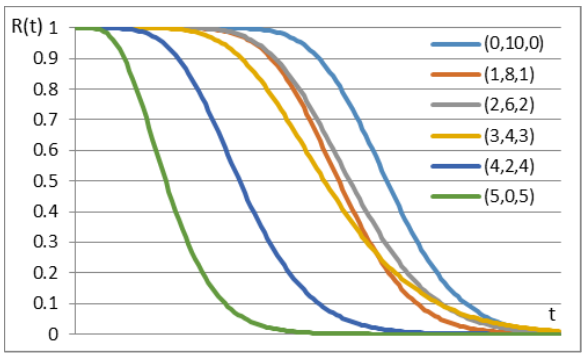
Фигура 3-20. Готовност на триплиран компонент на система с локален ремонт

Коефициентът на покритие на блока за самопроверка очаквано подобрява надеждността и времето до отказ (*Фигура 3-13* и *Фигура 3-14*), както и показателите, свързани с работоспособността на компонента (*Фигура 3-19* и *Фигура 3-20*).

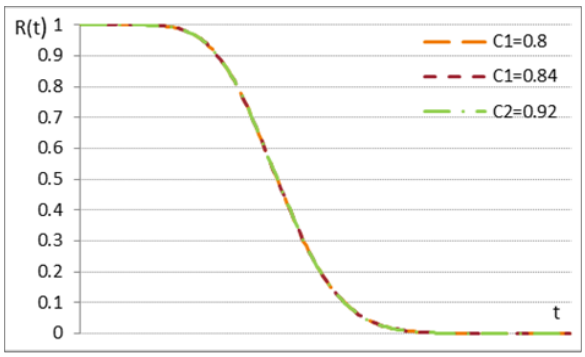
От направените изследвания на дублиран и триплиран компонент на отказоустойчива разпределена система може да се направи извод, че добавянето на блокове за самопроверка към всеки модул от компонента подобрява значително надеждностните характеристики на системата.

3.2.2 Система с 10 компонента

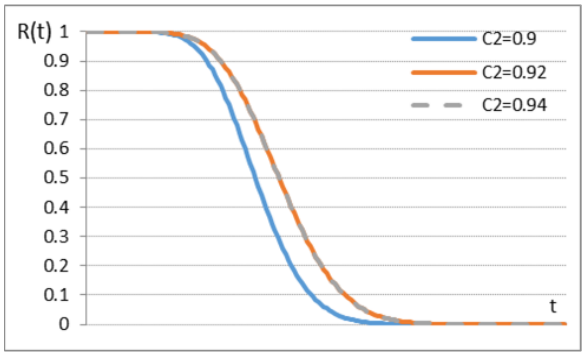
Системата има възможност за възстановяване от постоянна неизправност на компонент и за ремонт след системен отказ. Изследвани са 6 конфигурации на структурния излишък. Тяхната надеждност при C_1=0.88, C_2=0.94 и C_3=0.99 е показана на *Фигура 3-23*. Стойностите на коефициентите на покритие на компонентите с различна степен на репликиране, C_1, C_2 и C_3, са максимални за изследването.



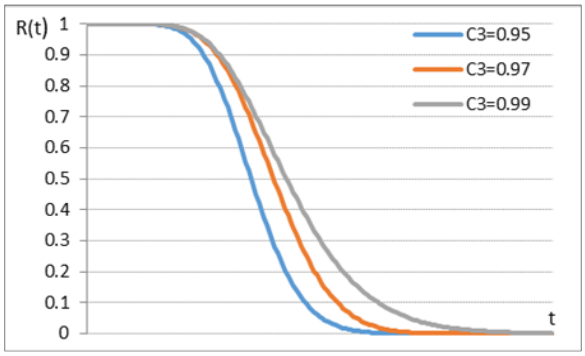
Фигура 3-23. Надеждност на система с 10 компонента за C_1=0.88, C_2=0.94 и C_3=0.99



Фигура 3-24. Надеждност на система (3,4,3) за различни стойности на C_1, при C_2=0.94 и C_3=0.97



Фигура 3-25. Надеждност на система (3,4,3) за различни стойности на C_2, при C_1=0.88 и C_3=0.97



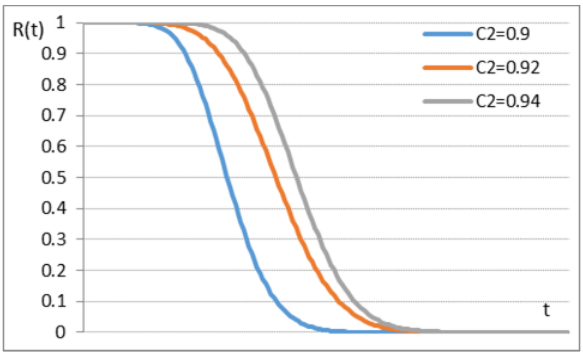
Фигура 3-26. Надеждност на система (3,4,3) за различни стойности на C_3, при C_1=0.88 и C_2=0.94

При тези условия най-висока надеждност има системата (0,10,0) (светло синята графика на *Фигура 3-23*). Тази система представлява известните системи, които работят само с дублирани компоненти, т.е. без разпределение на структурния излишък. Най-ниска надеждност има система (5,0,5) (зелената графика на *Фигура 3-23*), която е изградена само от единични и триплирани компоненти. Системи (1,8,1) (оранжевата графика на *Фигура 3-23*) и (2,6,2) (сивата графика на *Фигура 3-23*) имат близки стойности на надеждността. Система (3,4,3) (жълтата графика на *Фигура 3-23*) се доближава по надеждност до системи (1,8,1) и (2,6,2). Интерес представляват системите (3,4,3), (2,6,2) и (0,10,0) поради сравнително по-високата си надеждност.

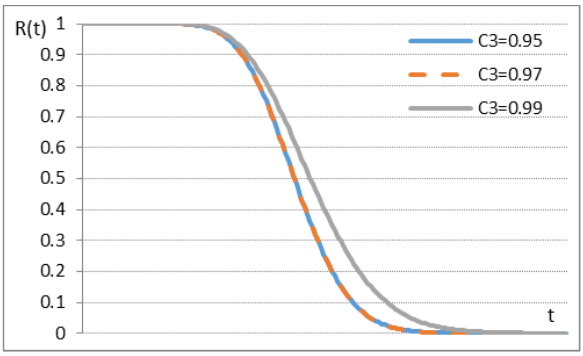
Надеждността на системата (3,4,3) е изследвана, за да се проследи влиянието на коефициентите на покритие на компонентите (*Фигура 3-24* - *Фигура 3-26*). Коефициентът на покритие на единичните компоненти C_1 не влияе въобще върху надеждността на системата (3,4,3) – графиките на надеждността за трите стойности на C_1 съвпадат (*Фигура 3-24*).

Система (2,6,2) е по-силно повлияна от увеличаването на коефициента на покритие C_2 (*Фигура 3-28*), отколкото от увеличението на C_3 (*Фигура 3-27*). Това се обяснява с по-големия брой дублирани компоненти в сравнение с броя на триплираните компоненти. Резултатите за C_3=0.95 (синята графика на *Фигура 3-28*) и C_3=0.97 (оранжевата графика на *Фигура 3-28*) са почти еднакви. Само най-голямата стойност на C_3=0.99 води до подобряване на системната

надеждност (сивата графика на *Фигура 3-28*). От друга страна, увеличаването на коефициента на покритие C_2 води до значително подобряване на надеждността (*Фигура 3-27*).

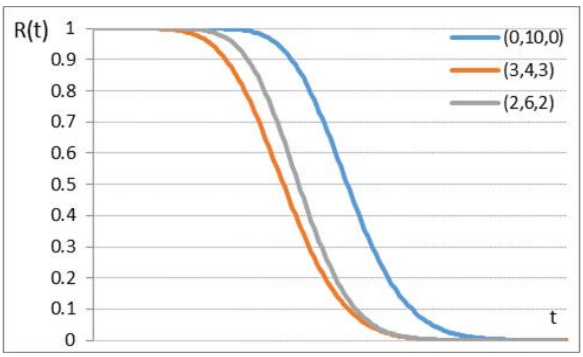


Фигура 3-27. Надеждност на система (2,6,2) за различни стойности на C_2, при C_1=0.88 и C_3=0.97

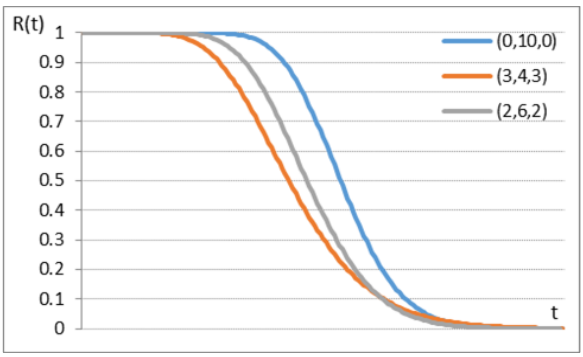


Фигура 3-28. Надеждност на система (2,6,2) за различни стойности на C_3, при C_1=0.88 и C_2=0.94

На *Фигура 3-29* и *Фигура 3-30* е направено сравнение на надеждността на системите (3,4,3), (2,6,2) и (0,10,0) при C_1=0.88 и C_2=0.94, а коефициентът C_3 е различен (C_3=0.97 на *Фигура 3-29* и C_3=0.99 на *Фигура 3-30*). Най-висока надеждност има системата, изградена изцяло от дублирани компоненти (0,10,0). Системата (3,4,3) е с най-ниска надеждност, която се подобрява при увеличение на C_3 (*Фигура 3-30, C_3*=0.99). Системата (2,6,2) показва средна стойност на надеждността. Може да се направи изводът, че системите с преобладаващ брой дублирани компоненти, (2,6,2) и (0,10,0), постигат по-висока системна надеждност.



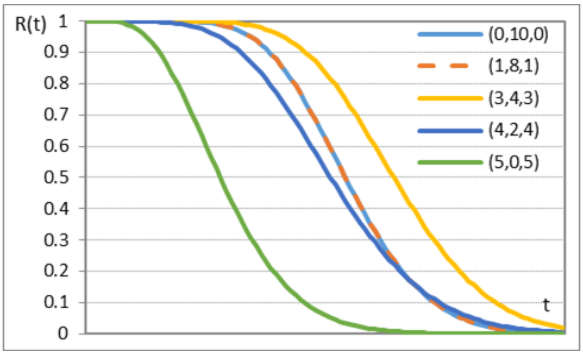
Фигура 3-29. Надеждност на системите (3,4,3), (2,6,2) и (0,10,0) при C_1=0.88, C_2=0.94 и C_3=0.97



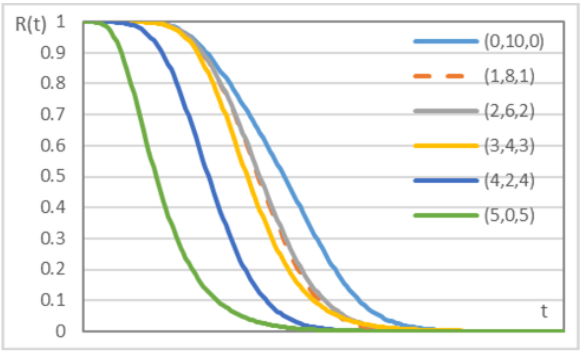
Фигура 3-30. Надеждност на системите (3,4,3), (2,6,2) и (0,10,0) при C_1=0.88, C_2=0.94 и C_3=0.99

При сравнение на системи с различно разпределение на структурния излишък за по-малък коефициент на покритие C_2=0.9 (C_1=0.88 и C_3=0.97) (*Фигура 3-31*) подреждането на системите по надеждност се променя. Най-висока надеждност има системата (3,4,3) (жълтата крива на *Фигура 3-31*), следвана от системите (1,8,1) (оранжевата крива на *Фигура 3-31*) и (0,10,0) (светло синята крива на *Фигура 3-31*), които имат еднаква надеждност, и системите (4,2,4) (тъмно синята крива на *Фигура 3-31*) и (5,0,5), която има най-ниска надеждност (зелената крива на *Фигура 3-31*).

На *Фигура 3-32* е изобразена надеждността на всички конфигурации на системата с 10 компонента, когато коефициентите на покритие на компонентите се менят в зададените в т. 3.2 интервали. Тези резултати са разгледани по-подробно в т. 3.3.



Фигура 3-31. Сравнение на надеждността на системи с различен структурен излишък при C_1=0.88, C_2=0.9 и C_3=0.97



Фигура 3-32. Сравнение на надеждността на системи с различен структурен излишък при $C_1 \in [0.8, 0.9)$, $C_2 \in [0.9, 0.95)$ и $C_3 \in [0.95,\ 1.0)$

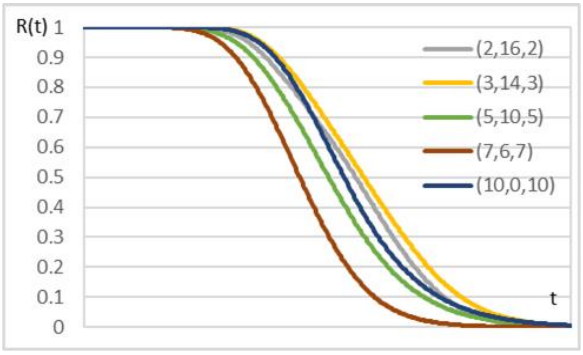
На *Фигура 3-32* се вижда, че най-висока надеждност има системата без настройване на надеждността, (0,10,0) (светло синята крива), следвана от системите (1,8,1) (оранжевата крива) и (2,6,2) (сивата крива). Близка, но по-ниска, надеждност има системата (3,4,3) (жълтата крива). Тези резултати са сходни с надеждността на системите от *Фигура 3-23*, но се различават от резултатите на *Фигура 3-31*.

Симулационното моделиране на отказоустойчивата система с настройваема надеждност с 10 компонента показва, че системата има добри надеждностни характеристики. От резултатите се вижда, че има разпределения на структурния излишък, които подобряват системната надеждност при определени условия.

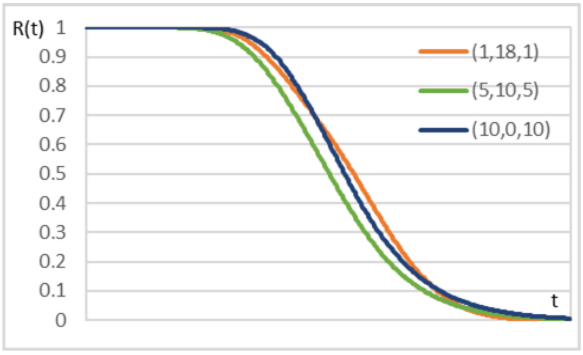
3.2.3 Система с 20 компонента

Отказоустойчивата система с настройваема надеждност с 20 компонента и 40 модула е симулирана при същите параметри като системата с 10 компонента (т. 3.2.2). Изследвани са 11 разпределения на модулния излишък в компонентите. Влиянието на постоянните неизправности е разгледано при две различни интензивности на неизправностите, за да се изследват различни условия на работната среда на системата. Допускането е, че системите, които функционират при по-неблагоприятни условия, търпят повече неизправности, което в модела се изразява с по-голяма интензивност на постоянните неизправности $\lambda_p=10^{-3}$ 1/h. По-малката интензивност на неизправностите $\lambda_p=10^{-4}$ 1/h моделира среди, където неизправностите настъпват по-рядко, но системата трябва да е в състояние да ги толерира.

Системата с настройваема надеждност има различни разпределения на излишъка в компонентите. Тяхната надеждност, R_d, във функция от времето е показана на *Фигура 3-33*, където интензивността на постоянните неизправности е $\lambda_p=10^{-4}$ 1/h.



Фигура 3-33. Надеждност на системи с различни разпределения на структурния излишък, $\lambda_p=10^{-4}$ 1/h, $\mu_p=\mu_{sys}=0.1$ 1/h



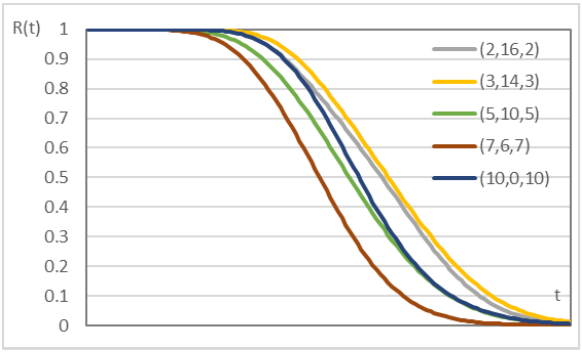
Фигура 3-34. Надеждност на системи с различен брой триплирани компоненти, $\lambda_p=10^{-4}$ 1/h, $\mu_p=\mu_{sys}=0.1$ 1/h

Системите със сравнително малък брой единични и триплирани компоненти демонстрират висока надеждност (системи (3,14,3) в жълто и (2,16,2) в сиво на *Фигура 3-33*). Не може да се твърди обаче, че това е тенденция. Системата, състояща се само от единични и триплирани компоненти (система (10,0,10) в тъмно синьо на *Фигура 3-33*) има близка надеждност.

За да се покаже влиянието на триплираните компоненти, на *Фигура 3-34* е изобразена надеждността на системи (1,18,1), (5,10,5) и (10,0,10). Въвеждането на повече единични и триплирани компоненти в системата (система (10,0,10) в тъмно синьо на *Фигура 3-34*) подобрява надеждността и удължава периода, през който системата поддържа висока надеждност. Функционирането с по-малко единични и ТМИ компоненти (система (1,18,1) в оранжево на *Фигура 3-34*) обаче не влошава значително системната надеждност. Система (5,10,5), която има най-ниската надеждност от трите системи на *Фигура 3-34*, все пак има добра надеждност в сравнение с останалите системи, както се вижда от *Фигура 3-33*.

Не може да се изведе ясна зависимост между разпределението на структурния излишък и надеждността (*Фигура 3-33* и *Фигура 3-34*). Разпределението на излишъка влияе върху системната надеждност и някои разпределения са по-благоприятни за системата от други. Изборът на системна конфигурация в зависимост от изискванията на приложението може да доведе до подобряване на надеждността и готовността на системата.

ОРС с настройваема надеждност е симулирана за по-голяма интензивност на постоянните неизправности, за да се провери дали разпределението на излишъка влияе по различен начин върху нейната надеждност (*Фигура 3-35*). В сравнение с надеждността на системи при $\lambda_p=10^{-4}$ 1/h (*Фигура 3-33*) надеждността при $\lambda_p=10^{-3}$ 1/h е подобна и изследваните системи са подредени по същия начин според тяхната надеждност (*Фигура 3-35*).



Фигура 3-35. Надеждност на системи с различно разпределение на структурния излишък, $\lambda_p=10^{-3}$ 1/h, $\mu_p=\mu_{sys}=0.1$ 1/h

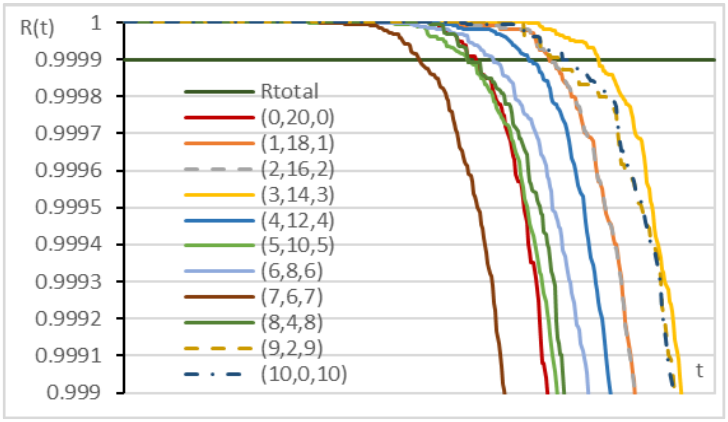
3.3 Подход на настройваема надеждност

Критичните за безопасността приложения изискват много висока надеждност, за да предоставят гарантоспособната услуга, за която са предназначени. При проектирането им се задава желаната системна надеждност и останалите ѝ характеристики се съобразяват с това изискване. Изследването на отказоустойчивата система с настройваема надеждност е разширено, за да може в повече дълбочина да се проследи нейното поведение и да се предложат възможности за постигане на висока желана надеждност. В представения дисертационен труд тази надеждност се нарича *обща надеждност* и се означава с R_{total}. Въз основа на изследванията, представени в т. 3.2.2 и 3.2.3 и [75], [76], е разработен подход на настройваема надеждност за определяне на системите, които постигат R_{total}.

R_{total} се определя при задаването на спецификациите на проектираната система според изискванията на приложението. По време на проектирането се дефинират режимите на неизправност и отказ, коефициентите на покритие на средствата за самопроверка, *MTTF*, *MTTR* и т.н. Определят се λ_p, μ_p, μ_{sys}, време на живот/мисия и R_{total}. При дадена R_{total} се определят и изследват всички възможни разпределения на модулния излишък, *система (i, j, k)*, за *N* компонента и *M* модула. Системите (i, j, k), т.е. системните конфигурации, се симулират, както е описано в т. 3.1, и се получават техните графики на надеждността във функция от времето. Надеждността на всяка конфигурация R_d се сравнява с R_{total}. След това се определят системите с $R_d(t) \geq R_{total}$. За всяка система се определя и периодът на висока надеждност.

Резултатите за системите, описани в т. 3.2.2 и 3.2.3, са показани на *Фигура 3-36* за R_{total}=0.9999 за система с N=20. Всички изследвани разпределения на структурния излишък постигат R_{total}, но поддържат тази надеждност за различни периоди. Резултатите от симулирането показват взаимоотношението между общата надеждност и разпределението на структурния излишък и илюстрират подхода на настройваема надеждност.

Система (3,14,3) има най-висока надеждност (жълтата крива на *Фигура 3-36*), следвана от система (10,0,10) (тъмно синята крива на *Фигура 3-36*) и система (1,18,1) (оранжевата крива на *Фигура 3-36*). Системата, изградена само от дублирани компоненти, система (0,20,0), има най-ниска надеждност (червената крива на *Фигура 3-36*). Разпределението на излишъка в компонентите на системата влияе върху системната надеждност (*Фигура 3-33, Фигура 3-35* и *Фигура 3-36*). Общата надеждност е по-висока за някои разпределения на структурния излишък, например система (3,14,3) (жълтата крива на *Фигура 3-36*), система (1,18,1) (оранжевата крива) и система (10,0,10) (тъмно синята крива), и е по-ниска за други, като система (7,6,7) (кафявата крива), система (5,10,5) (светло зелената крива) и (6,8,6) (светло синята крива на *Фигура 3-36*).



Фигура 3-36. Постигане на надеждност R_{total}=0.9999, $\lambda_p=10^{-4}$ 1/h, $\mu_p=\mu_{sys}$=0.1 1/h

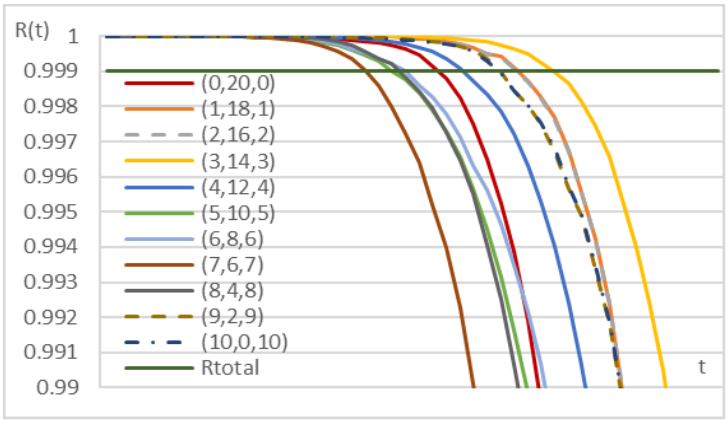
Не може да се изведе ясна зависимост между разпределението на излишъка и системната надеждност. Ако броят на компонентите с коефициент на покритие C_3 (т.е. с ТМИ) е по-голям от броя на компонентите с коефициент на покритие C_2 (т.е. с ДМИ), това не означава непременно, че системната надеждност ще се повиши. Въвеждането на единични компоненти, от друга страна, не води до значително намаляване на системната надеждност. В някои случаи, например система (10,0,10) (тъмно синята крива на *Фигура 3-36*), надеждността е по-добра отколкото при системи с по-малък брой единични компоненти, като система (6,8,6) (светло синята крива на *Фигура 3-36*).

Таблица 3-3 показва периодите, през които надеждността R_d на всяка от системите с настройваема надеждност надвишава R_{total}=0.9999, като се започва от системата с най-дълъг период. Системата (3,14,3) поддържа своята надеждност над R_{total} за най-дълъг период от време в сравнение с останалите системи. Система (0,20,0) без настройваема надеждност има сравнително по-кратък период на надеждност над R_{total}=0.9999.

Таблица 3-3. Периоди на работа на системи (i, j, k) с надеждност $R_d \geq R_{total}=0.9999$, $\lambda_p=10^{-4}$ 1/h, $\mu_p=\mu_{sys}=0.1$ 1/h, N=20

Система	$R_d \geq R_{total}$	Време [h]
(3,14,3)	0.999902	32300
(9,2,9)	0.999904	29800
(10,0,10)	0.999922	29800
(1,18,1)	0.999905	28900
(2,16,2)	0.999909	28900
(4,12,4)	0.999902	27500
(6,8,6)	0.999907	25100
(0,20,0)	0.9999	24000
(8,4,8)	0.999912	23400
(5,10,5)	0.999902	23400
(7,6,7)	0.999903	20100

При симулиране на системите за $\lambda_p=10^{-3}$ 1/h (*Фигура 3-37*) подреждането на графиките на надеждността на различните конфигурации на системата е приблизително същото като при интензивност на неизправностите $\lambda_p=10^{-4}$ 1/h (*Фигура 3-36*). Отново най-висока надеждност има система (3,14,3) (жълтата крива на *Фигура 3-37*), а най-ниска – система (7,6,7) (кафявата крива на *Фигура 3-37*). Системата без настройваема надеждност (0,20,0) (червената крива на *Фигура 3-37*) показва средна надеждност.



Фигура 3-37. Постигане на надеждност $R_{total}=0.999$, $\lambda_p=10^{-3}$ 1/h, $\mu_p=\mu_{sys}=0.1$ 1/h

Периодите на работа на конфигурациите с надеждност $R_{total} \geq 0.999$ за $\lambda_p=10^{-3}$ 1/h са показани в *Таблица 3-4*. Както личи и от графиките на *Фигура 3-37*, система (3,14,3) най-дълго поддържа желаната надеждност R_{total}, а най-кратък е периодът за система (7,6,7). Система (0,20,0) без настройваема надеждност има сравнително по-кратък период на поддържане на R_{total} в сравнение с повечето от останалите системи.

Таблица 3-4. Периоди на работа на системи *(i, j, k)* с надеждност $R_d \geq R_{total}=0.999$, $\lambda_p=10^{-3}$ 1/h, $\mu_p=\mu_{sys}=0.1$ 1/h, *N*=20

Система	$R_d \geq R_{total}$	Време [h]
(3,14,3)	0.999242	3300
(1,18,1)	0.9991	3100
(2,16,2)	0.99908	3100

(9,2,9)	0.999357	2900
(10,0,10)	0.999295	2900
(4,12,4)	0.999098	2700
(0,20,0)	0.99914	2500
(6,8,6)	0.999004	2300
(5,10,5)	0.999022	2200
(8,4,8)	0.999212	2200
(7,6,7)	0.999035	2000

Резултатите от симулирането показват, че разпределянето на системните ресурси в зависимост от тяхната важност за приложението може да даде предимство за системната надеждност. Например, един съвременен автомобил е оборудван с реалновременни разпределени системи, които управляват различни блокове, като двигател, окачване, скоростна кутия, врати, седалки и др. Тези блокове на свой ред са подсистеми, състоящи се от други модули, които работят заедно в изпълнение на конкретна задача. Една такава подсистема може да използва подхода на настройваема надеждност, за да постигне надеждността, диктувана от приложението. Определяйки R_{total} и знаейки броя на компонентите в подсистемата и техните надеждностни характеристики, могат да бъдат изведени и симулирани разпределенията на структурния излишък, за да се сравни тяхната надеждност. По този начин може по-нататък да се изследва и разработи модулното разпределение с най-висока надеждност, отчитайки особеностите на проектираната подсистема.

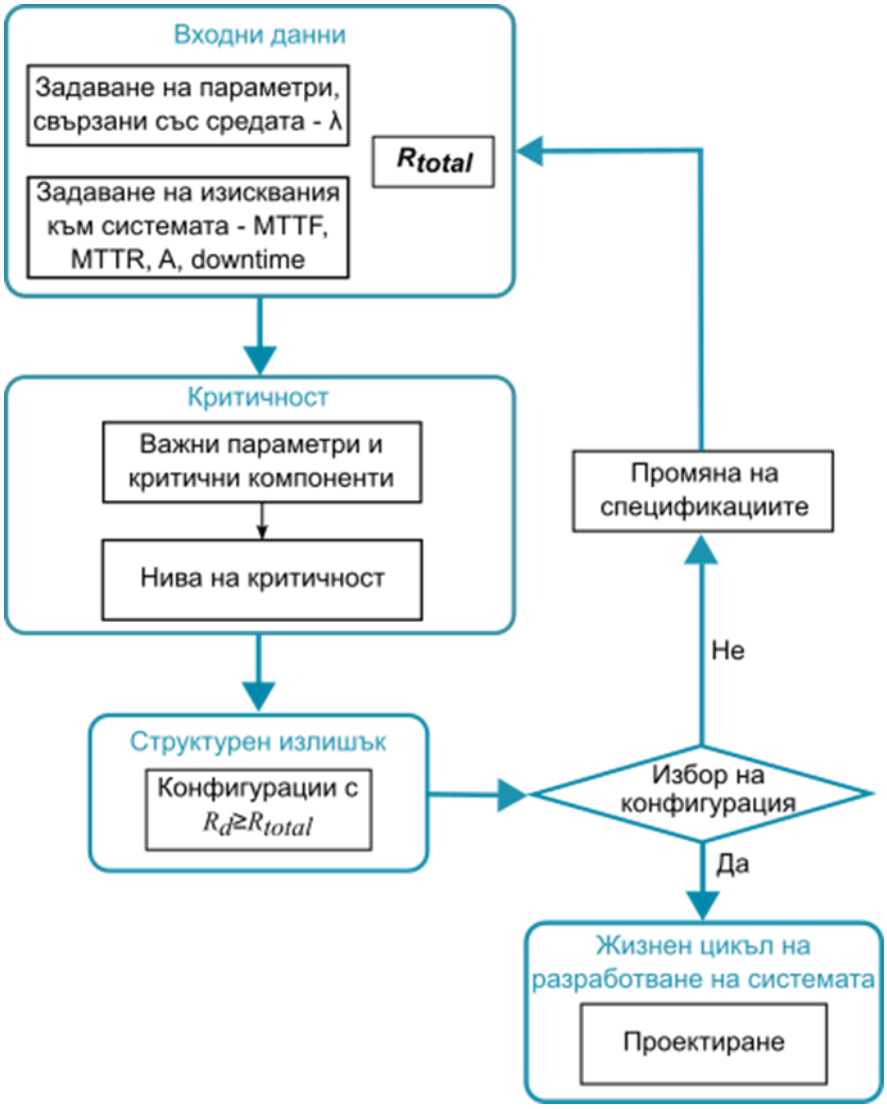
Представените резултати от симулационното моделиране (т. 3.2) показват, че има разпределения на структурния излишък, при които системата с настройваема надеждност постига по-висока надеждност R_{total} и я поддържа за по-дълъг период от време в сравнение със система без настройване на надеждността (*Фигура 3-36* и *Таблица 3-3, Фигура 3-37* и *Таблица 3-4*). При какви условия се случва това обаче е трудно да се установи, тъй като няма ясна зависимост между системната надеждност и разпределението на излишъка. Затова в дисертационния труд се предлага *подход на настройваема надеждност*, чрез който да се определят конфигурациите на структурния излишък, удовлетворяващи изискването за системна надеждност на приложението.

Подходът на настройваема надеждност може да се опише със следните действия:

1. Задаване на R_{total},
2. Задаване на параметрите, описващи средата – интензивност на неизправностите,
3. Задаване на изискванията към системата – средно време до отказ, средно време до ремонт, готовност, средно време на престой, възможности за локален и системен ремонт и съответно интензивности на локалните и системните ремонти,
4. Определяне на важните контролирани параметри и на критичните компоненти,

5. Определяне на нивата на критичност,
6. Извеждане на системните конфигурации, при които настройваемата надеждност е равна или по-голяма от изискваната обща надеждност R_{total},
7. Проверка коя от възможните конфигурации отговаря най-добре на изискванията на приложението,
8. При липса на подходяща конфигурация се променят входните спецификации и процедурата се повтаря.

Описаните действия са онагледени на *Фигура 3-38*.



Фигура 3-38. Описание на подхода на настройваема надеждност

Ако повече от възможните конфигурации на системата с настройваема надеждност изпълняват изискването за системна надеждност при зададените спецификации, подходящата за приложението конфигурация може да се избере според допълнителни критерии, като брой единични, дублирани или триплирани компоненти, желани нива на критичност, най-висока обща надеждност, най-голям период с висока обща надеждност и т.н. Ако нито една

конфигурация на системата с настройваема надеждност не удовлетворява изискването за R_{total} на приложението, е необходимо да се преразгледат системните спецификации, включително и изискването за обща надеждност.

3.4 Изводи и резултати

В *Глава 3* е представена симулационната програма, разработена според изискванията в т. 3.1.1. Представени са основната структура и блоковата схема на програмата.

Изследван е компонент на отказоустойчивата система с настройваема надеждност в зависимост от коефициента на покритие на блока за самопроверка C и коефициента на възстановяване от случайна неизправност C_r. Симулирани са компоненти с двоен и троен модулен излишък при работа с и без локален ремонт. Оценено е влиянието на C и C_r върху надеждността на компонентите, тяхната готовност, *MTTF, MTTS, MTBF, MTBS* и средното време за престой.

Според предвидения изследователски протокол са проведени експерименти за системи с различен брой компоненти (N=10 и N=20), различна интензивност на постоянните неизправности λ_p и различни стойности на коефициентите на покритие C_1, C_2 и C_3. Получени са данни за: $R(t)$, *A, MTTF, MTTR, MTTS, downtime*. Определени са възможните разпределения на структурния излишък при зададените N и M. Изследвано е влиянието на броя компоненти, коефициентите на покритие и интензивността на неизправностите върху надеждностните характеристики на отказоустойчивата система с настройваема надеждност и на системи без разпределение на структурния излишък. Определени са конфигурациите на системата, удовлетворяващи изискването за обща надеждност.

Създаден и представен е авторски подход на настройваема надеждност, чрез който да се определя кои разпределения на излишъка в компонентите удовлетворяват желаната обща системна надеждност. Въз основа на изискванията на приложението подходът намира системните конфигурации, които могат да постигнат общата надеждност.

Налага се изводът, че може да се постигне висока надеждност чрез разпределение на структурния излишък, като в някои случаи тя надвишава надеждността на системи без разпределение на излишъка. Конфигурациите, при които това е изпълнено могат да бъдат определени чрез подхода на настройваема надеждност.

Постигнатите резултати имат научно-приложен и приложен характер. Научно-приложни са разработването на симулационна програма за моделиране на гарантоспособни разпределени системи и формулирането на подход на настройваема надеждност. Приложните резултати са свързани с провеждане на експерименти със симулационната програма с цел да

се изследват надеждностните характеристики на отказоустойчива разпределена система с и без настройваема надеждност.

Чрез изследванията, представени в *Глава 3*, са изпълнени задачи 3 и 4 на дисертацията.

Глава 4. Обсъждане и анализ на резултатите

Гарантоспособните разпределени системи, които са обект на дисертацията, се разработват за приложения, които са критични по отношение на безопасността. Те се изграждат със специализирани или с готови компоненти, като и двата подхода имат своите предимства и недостатъци. Специализираните компоненти отразяват по-адекватно особеностите на приложението, дават възможност за постигане на висока надеждност с методи и техники, съобразени с конкретната работна среда и контекст на системата, и са добре верифицирани и валидирани. Това обаче изисква време и усилия, които имат своята цена. Такива системи се проектират и внедряват по-бавно, което, от една страна, ги прави твърде трудни за адаптиране към промени в средата на функциониране на системата и, от друга страна, оскъпява крайната им реализация.

Прилагането на готови компоненти скъсява периода между проектиране и внедряване на разпределената система и намалява цената. Той има недостатък, че внася допълнителни рискове за надеждността на системата. Готовите компоненти не дават гаранции за изпълнение на изискванията за отказоустойчивост. Затова се търсят методи и средства за компенсиране на ниската собствена надеждност на готовите компоненти.

Анализът на гарантоспособните разпределени системи от гледна точка на структурния излишък, направен в *Глава 1*, показва, че основните подходи за постигане на повече гъвкавост по отношение на изискванията на приложението са промяна на софтуерния структурен излишък (при статично разпределение на хардуерния структурен излишък) и въвеждане на нива на критичност.

Отказоустойчивата разпределена система с настройваема надеждност предлага и изследва подход, който да притежава гъвкавостта на гарантоспособните системи с готови компоненти, да отчита нивата на критичност на системите със смесена критичност, да дава възможности за настройване на надеждностни характеристики и в същото време да отговаря на изискванията за висока надеждност. Всички изброени видове системи реализират отказоустойчивостта си посредством структурен излишък. Те прилагат равномерно разпределен хардуерен излишък на компонентите и съобразяват с приложението разпределението на софтуерния структурен излишък. Предложената система с настройваема надеждност внася гъвкавост чрез разпределение на хардуерния структурен излишък.

При изграждане на идеята за ОРС с настройваема надеждност са взети под внимание концептуалният модел на подход за вземане на решения във връзка с гарантоспособността и класификацията на гарантоспособните разпределени системи според възможностите им за определяне на структурния излишък в зависимост от приложението. Предложената система е изградена от отказоустойчиви компоненти с различна степен на репликиране, която дава възможност да бъдат изследвани надеждностните характеристики на различни конфигурации на структурния излишък. Отказоустойчивостта на компонентите се определя от наличието на блок за самопроверка на всеки модул и средства за сравнение на неговите резултати. Представените Марковски вериги на ОРС с настройваема надеждност моделират поведението на системата при отсъствие или наличие на възможности за възстановяване на компонент и ремонт на системата. Тези модели стоят в основата на симулационната програма, чрез която са проведени експериментите в дисертацията. Избраният изследователски подход на симулационно моделиране предлага възможност за представяне на поведението на системата по отношение на неизправностите и отказите и изследване на нейните надеждностни характеристики, дефинирани в *Глава 2*, т. 2.1.2. Симулацията позволява моделиране на система с много компоненти и състояния и задаване на различни параметри за изследване на тяхното влияние върху системната надеждност.

Представените в *Глава 3* резултати от симулационното моделиране на отказоустойчивата система с настройваема надеждност показват, че изследваната система има добри надеждностни характеристики. Направен е анализ на резултатите, за да се провери дали се потвърждава хипотезата на дисертационния труд, а именно постига ли се висока надеждност и гъвкавост на системата чрез настройване на надеждността според изискванията на приложението.

При симулирането на компонент на системата са разгледани варианти на компонент с двоен и троен модулен излишък. Изследвано е влиянието на коефициента на покритие на блока за самопроверка и коефициента на възстановяване след случайна неизправност. Резултатите за надеждността, готовността, *MTTF, MTTR, MTTS, MTBF*, *MTBS* и времето за престой показват, че добавянето на блокове за самопроверка към всеки модул от компонента подобрява значително надеждностните характеристики на системата, особено когато тя работи без възможност за локален ремонт.

Симулационното моделиране на ОРС с настройваема надеждност с 10 компонента не очертава ясна зависимост между системната надеждност и разпределението на структурния излишък. От една страна, системата без настройваема надеждност (0,10,0) показва най-висока надеждност. От друга страна, при по-нисък коефициент на покритие C_2 някои конфигурации с разпределение на структурния излишък имат по-висока или близка до нейната надеждност.

Влиянието на C_1 върху надеждността е незначително. Коефициентите на покритие C_2 и C_3 подобряват значително общата надеждност на системата, което е логично, предвид по-голямата им стойност.

При ОРС с настройваема надеждност с 20 компонента най-висока надеждност показва системата (3,14,3). Най-ниска надеждност има система (7,6,7). Конфигурациите с малко единични и малко триплирани компоненти, като (1,8,1), (2,16,2) и (3,14,3), имат сравнително висока надеждност. Увеличаването на броя на триплираните компоненти може да повиши надеждността, но това не е валидно във всички случаи.

Изследванията при по-висока интензивност на неизправностите $\lambda_p=10^{-3}$ 1/h показват, че някои системи с настройваема надеждност са по-подходящи за работа при такива условия. Системи (1,18,1) и (2,16,2) имат втората по големина надеждност, докато при интензивност $\lambda_p=10^{-4}$ 1/h имат по-ниска надеждност. По-добре работи при висока интензивност и системата без настройваема надеждност (0,20,0). Това поведение на изследваните системи предполага гъвкавост при избора на подходяща система за конкретно приложение.

Системите с най-висока обща надеждност имат и най-дълги периоди, през които я поддържат. Това е мярка за тяхната готовност. Ако този показател е важен за приложението, той трябва да се вземе под внимание при избора на конфигурация с настройваема надеждност.

При проведените симулационни изследвания за N=10 и N=20 различните конфигурации на системата с настройваема надеждност не показват постоянно поведение. Надеждността им се влияе от броя на компонентите, интензивността на постоянните неизправности, коефициентите на покритие на средствата за самопроверка. При някои конфигурации общата надеждност е по-висока от тази на система без настройваема надеждност, при други не е. За да се определи подходящата конфигурация на ОРС с настройваема надеждност според изискванията на приложението, е създаден подход на настройваема надеждност. Той предвижда последователност от действия за избор на разпределение на структурния излишък в зависимост от изискването за обща системна надеждност на приложението. Подходът определя всички системни конфигурации, които постигат желаната надеждност, и представя възможност за избор на онази, която в най-голяма степен удовлетворява зададените системни спецификации.

От направените експерименти със симулационната програма могат да се направят няколко извода. Конфигурациите с настройваема надеждност постигат висока системна надеждност, съпоставима и в някои случаи по-висока от тази на системи без разпределение на структурния излишък. Подходът на настройваема надеждност определя системните конфигурации, които най-добре изпълняват изискването за обща системна надеждност на приложението. Това дава гъвкавост при проектирането на отказоустойчиви разпределени

системи да бъде избрано разпределение на структурния излишък, което най-добре отразява нуждите на конкретната реализация.

Тези изводи потвърждават хипотезата на дисертационния труд, че може да се постигне гъвкавост и висока надеждност на отказоустойчивите разпределени системи чрез разпределение на хардуерния структурен излишък според изискванията на приложението.

4.1 Изводи и резултати

Направено е обсъждане и анализ на резултатите, представени в дисертационния труд и на тази основа те са групирани, както следва:

Научни резултати:

1. Представен е нов архитектурен модел на отказоустойчива разпределена система с настройваема надеждност, като са дефинирани изискванията към нейните компоненти и системата като цяло;
2. Създаден е симулационен модел на предложената отказоустойчива разпределена система с настройваема надеждност;
3. Предложен е синтез на класификация и класификация на гарантоспособни разпределени системи със структурен излишък.

Научно-приложни резултати:

1. Създаден е концептуален модел на подход за вземане на решения при осигуряване на гарантоспособност;
2. Формулиран е подход на настройваема надеждност;
3. Разработена е симулационна програма, реализираща метода за симулационно моделиране на гарантоспособни разпределени системи.

Приложни резултати:

1. Създадената симулационна програма може да се използва за моделиране и изследване на надеждностните характеристики и на други отказоустойчиви системи. С нея може да се изследва влиянието и на случайни хардуерни неизправности.

Получените в дисертационното изследване резултати показват, че поставените задачи са изпълнени.

Приложните резултати доказват твърденията, поддържащи научната хипотеза на дисертацията: Може да се постигне висока надеждност и гъвкавост на разпределението на системните ресурси посредством настройваема надеждност, реализирана с разпределение на хардуерния структурен излишък. Това се доказва със следните резултати:

1. Представената отказоустойчива разпределена система с настройваема надеждност постига висока обща надеждност, съпоставима с надеждността на системи без разпределение на структурния излишък.
2. Отказоустойчивата разпределена система с настройваема надеждност има конфигурации на разпределението на структурния излишък, които притежават по-добри надеждностни характеристики от тези на системи без разпределение на структурния излишък.
3. Подходът на настройваема надеждност дава възможност за определяне на конфигурациите на структурния излишък, които удовлетворяват изискването за обща надеждност на приложението.

Заключение и бъдеща работа

В дисертационния труд са изследвани надеждностните характеристики на отказоустойчива разпределена система с настройваема надеждност. Системата е предложена като възможност за постигане на гъвкавост в проектирането на гарантоспособни разпределени системи. При направения обзор на гарантоспособни разпределени системи за работа в реално време са очертани две основни направления на изграждане на такива системи – с използване на специализирани компоненти и с използване на готови компоненти. Системите и от двата вида постигат отказоустойчивост посредством разнообразни начини за въвеждане на излишък. Прилагат се структурен, времеви и функционален излишък. Структурният излишък добавя хардуерни и софтуерни елементи към системната архитектура. Най-често той се реализира като еднакво репликирани хардуерни компоненти, които изпълняват различно репликирани софтуерни задачи.

В дисертационния труд е разработен концептуален модел на подход за вземане на решение при осигуряване на гарантоспособност и е направен синтез на класификацията на гарантоспособни разпределени системи на базата на модела за разработване на системи.

Предложени са авторска архитектура и модел на отказоустойчива разпределена система за работа в реално време, наречена от автора система с настройваема надеждност. Тя предлага настройване на хардуерния структурен излишък за постигане на обща надеждност според изискванията на приложението. Системата е изследвана посредством метода на симулационно моделиране.

Проектиран и създаден е програмен продукт за симулационно моделиране на отказоустойчиви системи. Той реализира създадения модел на системата с настройваема надеждност. В резултат от изпълнението му се получава функция на надеждността, както и

данни за надеждностните характеристики на системата. Симулационният продукт е написан на език за програмиране C++ и с него могат да се изследват отказоустойчиви системи с и без разпределение на структурния излишък.

Резултатите от проведените експерименти показват добра обща надеждност на системата с настройваема надеждност. Съществуват разпределения на структурния излишък, при които системната надеждност е по-висока от тази на система с равномерно разпределен излишък. При някои от конфигурациите се наблюдава стохастично подреждане, т.е. кривите на надеждността не се пресичат, което означава, че изборът на архитектурно решение не зависи от съответните стойности на коефициентите на покритие. Има случаи, при които различните архитектурни решения са неразличими, и други, при които не се наблюдава стохастично подреждане. Това прави избора на конкретно инженерно решение не очевиден и зависим от по-задълбоченото познаване на стойностите на коефициентите на покритие. Разликите във функцията на надеждността на изследваните конфигурации показват, че при проектиране на системата трябва да се използват средства, които да дадат количествена оценка на вариантите на разпределение на структурния излишък, за да бъде избрано най-подходящото за приложението решение.

Това мотивира и създаването от автора на подход, наречен подход на настройваема надеждност, който определя при какви конфигурации на структурния излишък системата постига надеждността, изисквана от приложението.

Получените при моделирането на отказоустойчивата разпределена система с настройваема надеждност резултати показват, че системата има предимства по отношение на разпределянето на структурния излишък според изискванията на приложението, които могат да се използват при проектирането на гарантоспособни разпределени системи. Настройваемата надеждност е подходяща за използване в системи със смесена критичност на компонентите, в компактни системи, където множество възли са разположени в ограничено пространство, в системи с високи изисквания за надеждност, които позволяват работа с готови компоненти и др. под. Програмният продукт за симулационно моделиране на отказоустойчиви системи с разпределение на структурния излишък може да се използва и за моделиране на други гарантоспособни разпределени системи с добавяне на модули, които описват техните характеристики.

Насоки за бъдеща работа

Отказоустойчивата система с настройваема надеждност може да се изследва за различни приложения, изискващи нива на критичност, висока надеждност и разпределение на структурния излишък. Подходът на настройваема надеждност може да се усъвършенства, за да включва съобразяване и на други изисквания на приложението на гарантоспособни

разпределени системи. Моделът на отказоустойчивата разпределена система с настройваема надеждност може да се разшири за моделиране на софтуерна надеждност и изследване на ефекта на софтуерните неизправности върху отказоустойчивостта на системата. Подходът и моделът на настройваема надеждност могат да се приложат за конкретни системи.

Симулационната програма подлежи на усъвършенстване, като се ускори нейното изпълнение чрез прилагане на техники за паралелна обработка. В нея могат да се включат още блокове за изследване на влиянието на други фактори върху надеждностните характеристики на дадена система. Програмният продукт може да се развие и за изследване на други видове разпределени системи.

Списък на публикациите по дисертацията

1. Djambazova, E., & Andreev, R. (2023). Redundancy management in dependable distributed real-time systems. *Problems Of Engineering Cybernetics And Robotics*. (под печат)
2. Djambazova, E. (2022). Achieving system reliability using reliability adjustment. International Conference on Computer Systems and Technologies 2022 (CompSysTech ’22), Ruse, Bulgaria. ACM, NewYork, NY, USA, pp. 64-68. DOI: 10.1145/3546118.3546129. SJR(SCOPUS) 2020: 0,18
3. Djambazova, E. (2012). Adjusting reliability of a fault-tolerant distributed process control system – Preliminary results. International Conference “Automatics and Informatics 2012”, Sofia, Bulgaria, pp. 175-178.
4. Djambazova, E. (2009). Node reliability of a fault-tolerant distributed process control system – Simulation results. International Conference “Automatics and Informatics’ 2009”, Sofia, Bulgaria, pp. I-131 – I-134.
5. Джамбазов, К., & Ананиева, Е. (1995). Управляващи системи с модулно настройване на отказоустойчивостта. Национална конференция с международно участие „Автоматика и информатика ‘95”, София, стр. 247-250.

Участие в проекти

Част от разработките са включени в работата по два национални проекта:

1. Моделиране и изследване на интелигентни системи за обучение и сензорни мрежи“ (ИСОСеМ) – Договор № КП-06-Н 47/4 от 2020 г., финансиран от ФНИ (текущ).
2. Информационни и комуникационни технологии за единен цифров пазар в науката, образованието и сигурността (ИКТ в НОС) – Д01-205/2018 г., финансиран от МОН.

Основни научни и научно-приложни резултати

Научни резултати:

1. Предложен е нов архитектурен модел на отказоустойчива разпределена система с настройваема надеждност.
2. Създаден е симулационен модел на отказоустойчива разпределена система с настройваема надеждност.
3. Синтезирана е класификация на гарантоспособни разпределени системи според възможностите им за определяне на структурния излишък в зависимост от приложението.

Научно-приложни резултати:

4. Направен е критичен анализ на гарантоспособни разпределени системи, на базата на който е разработен концептуален модел на подход за вземане на решения при осигуряване на гарантоспособност.
5. Идентифицирани са основните направления на управление на структурния излишък в гарантоспособни разпределени системи и са очертани изследователски възможности.
6. Проектиран и реализаран е софтуерен продукт за симулационно моделиране на изследваната система.
7. След сравнителен анализ на отказоустойчивата система с настройваема надеждност със системи без разпределение на структурния излишък е разработен и приложен подход на настройваема надеждност.

Приложни резултати:

8. Създадената симулационна програма може да се използва за моделиране и изследване на надеждностните характеристики и на други отказоустойчиви системи. С нея може да се изследва влиянието и на случайни хардуерни неизправности.

Abstracts of Dissertations

Number 6, 2023

INSTITUTE OF INFORMATION AND COMMUNICATION TECHNOLOGIES

BULGARIAN ACADEMY OF SCIENCES

БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ

ИНСТИТУТ ПО ИНФОРМАЦИОННИ И КОМУНИКАЦИОННИ ТЕХНОЛОГИИ

Брой 6, 2023

Автореферати на дисертации