I.B. Shubinsky

"DEPENDABLE FAIL-SAFE SYSTEMS"

The book "Dependable fail-safe information systems. Synthesis methods" proposed to the attention of the reader is the third and final part of the project "Dependable of information systems".

The first chapter "Basic concepts of dependability and fault tolerance of information systems" offers main ideas for construction of reliable and safe information systems. This chapter is for decision-makers who only need to understand the problem conceptually. This chapter contains the postulates of dependability of information systems, key concepts of redundancy, fault tolerance, fail safety and cyber security of systems.

The second chapter of the book represents traditional models of reliability of both non-restorable and restorable objects with common and separate constant redundancy as well as with standby redundancy for the purpose of considering latent failures and taking into account real capabilities for their detection. Of special interest are the models of dependability of objects with majority architectures combining a model of the structural reliability of a majority object and the functional reliability of its restoring element. This chapter gives limits of the reliability of redundant objects with an endless number of standby facilities, but with the limited efficiency of a failure detection system strongly indicating that we should not cherish illusions concerning the achievement of the required level of system reliability by means of increasing the number of standby facilities. Limited capabilities of structural redundancy with restoration and even more so without restoration generate needs for the development of nontrivial methods to ensure fault tolerance of information systems. This is all the more important because it does not appear feasible to rely on the efficient use of time and/or functional redundancy in information and control systems operating in real time. Information redundancy methods based on various requirements for the efficiency of control of stored information authenticity are also classified in the chapter.

The third chapter introduces original methods for construction of modular information systems with adaptive fault tolerance. It presents the ideas of adaptive fault tolerance (active protection), the ways of implementation of active protection, methods of automatic detection and elimination of failures, time intervals and active protection disciplines. The application of active protection methods is assessed. The method of active protection synthesis is described. The analysis shows obvious advantages of active protection compared to traditional methods of structural redundancy in relation to reliability as well technical and economic characteristics. In addition, active protection enables a system's adaptation not only to failures but also to glitches and software errors.

The fourth chapter is devoted to the methods of construction of reliable software tools, with discussion of their inherent disadvantages. This section contains some recommendations for the development of requirements specifications for software programs to be designed, as well as the technology of the development of a reliable software program architecture is sufficiently detailed. A lot of attention is paid to the design of reliable software and its implementation, including the verification of programs and their integration with hardware, as well as certification, operation, maintenance and configuration.

The fifth chapter covers the topical issues of the functional safety of information and control systems of critical objects. It describes the key concepts of safety state, safety function and integrity, main principles of functional safety, including the principles of fail safety, redundancy, diversity and localization of undesired events. The assessment of allowed time for detection of single and double hazardous failures is provided. The chapter also describes and studies the models of functional safety of a two-channel system with built-in diagnostics tools and with an external control. The problem of channel restart is also defined. It offers the model for the assessment of the probability of hazardous failures under restart of two-channel systems. The combined application of different information technologies for construction of information systems to control critical objects provides natural conditions for construction of a two-level safety ensuring system. It is possible to use non-vital systems in a two-level system. This chapter contains the results of the mathematical simulation of various strategies for construction of two-level information systems. It is shown that if there are insufficiently safe constituent systems, a more effective strategy in comparison to other strategies is the strategy, which provides an efficient use of additional information occurred after previous control cycles.

The sixth chapter includes the principles and methods for demonstrating the conformance of information systems to the requirements of Technical Regulations and normative documents. It describes the methods of testing software tools to prove the conformance to the requirements of quality assurance and functional safety, as well as of information security. The issues of the practical application of software test methods are studied. Principal attention is paid to the problem of testing acceleration. This section also describes the main ways of testing acceleration based on the reduction of variance of the obtained indicators of quality, reliability and safety for objects under testing: a Monte-Carlo method and a method of relevant retrieval. It defines engineering practice of accelerated field tests of functional reliability and functional safety of information systems for control of critical objects, including the basic theory of such practice, test procedures and estimation of its duration, procedures of results processing and data representation form. The chapter gives an example of the practical application of accelerated field testing of an information system of railway dispatch control. It also defines basic stipulations of software test procedures according to the quality requirements and requirements of functional safety and absence of undeclared program capabilities, as well as the procedure of confirmation of software integrated safety and security.

In the end of each chapter there are test questions for the most difficult and relevant material. The book is designed primarily for specialists engaged in practical work on development, production, operation and modification of information systems. It is intended for researchers worked in the field of reliability of software and hardware systems, academic teaching stuff, postgraduates and students specialized in information technologies, information systems and automated control systems.

The book completes the project of three books created to provide a wide audience of specialists with methods of analysis of structural and functional reliability of information systems and particularly, methods of synthesis of reliability, fault tolerance and functional safety of such systems.

От редколлегии

Редколлегией журнала произведен сопоставительный анализ статьи «Методика определения ожидаемой стоимости гарантийных обязательств предприятия-изготовителя» (авторы: Ахрамович И.Л., Когут С.А., Терещенко Ф.В.) (журнал «Надежность», № 3, 2013) и статьи «Методика расчета стоимости гарантийных обязательств» (авторы Зайко Ю.Г., Искандарова Л.Н., Мишин В.Ф.) (журнал «Надежность», № 3, 2015). Анализ показал следующее.

Обе статьи «Методика определения ожидаемой стоимости гарантийных обязательств предприятия-изготовителя» и «Методика расчета стоимости гарантийных обязательств» имеют общий предмет и объект исследования, и практически одинаковые научные результаты, приоритет разработке которых принадлежит Ахрамовичу И.Л. и его соавторам. В статье Зайко Ю.Г. с соавторами результаты вторичны и детализированы только в части видов гарантийных обязательств. Они не имеют самостоятельного научного значения.

С уважением, Главный редактор журнала «Надёжность» д.т.н., профессор Шубинский И.Б.

From Editorial Board

Editorial board of the journal carried out a comparative analysis of the articles “Methods for defining of a manufacturer’s warranty expected costs” (by Akhramovich I.L., Kogut S.A., Tereschenko F.V.) (Dependability, № 3, 2013) and “Methodology for calculating the cost of warranty obligations” (by Zayko Y.G., Iskandarova L.N., Mishin V.F.) (Dependability, №3, 2015). The analysis showed the following.

Both articles “Methods for defining of a manufacturer’s warranty expected costs” and “Methodology for calculating the cost of warranty obligations” have common subject and object of the research, and almost common scientific results, developed with the priority of Akhramovich I.L. and his co-authors. The results represented in the article of Zayko Y.G. and his contributors, are secondary, and are extended only in the part related to the types of warranty obligations. They do not possess a self-contained scientific value.

Sincerely yours, Editor-in-Chief Journal “Dependability” Dr.Sci., professor Shubinsky I.B.