CERTIFICATION OF THE SOFTWARE FOR AUTOMATED CALCULATIONS OF SYSTEMS' SAFETY AND TECHNICAL RISKS "ARBITER"

Alexander S. Mozhaev

JSC "Specialized Engineering Company "SEVZAPMONTAGEAUTOMATICA" (JSC SPIK SZMA)
E-mail: Alexander_Mozhaev@szma.com

Abstract: The paper describes the software "ARBITER", organization and results of its expertise by Software Certification Committee of ROSTECHNADZOR of the Russian Federation, its application and further development trends.

Key words: system, structure, reliability, survivability, safety, risk, general logic probabilistic method, functional integrity scheme, technology of automated structural logic simulating, SC ASLS SZMA.

Software ARBITER - **Software complex for automated structural logic simulating and computing of reliability and safety measures of control systems (SC ASLS SZMA), version 1.0, base sample** [1], developed by JSC "SPIK SZMA", has successfully passed certification expertise in the Software Certification Committee of the Federal environmental, technological & nuclear supervision agency (Rostechnadzor) of the Russian Federation at R&D Center of Nuclear and Radiation Safety [2]. An Expertise Certificate No.222 dated of February 21, 2007 was issued for a 10-year period authorizing ARBITER application at the Rostechnadzor sites and objects.

ARBITER's theoretical base is a General Logic Probabilistic Approach (GLPA) used for analysis of large-scale, structurally complicated objects & processes of various types and applications [3-5]. The following features make it unique:

- Traditional logic probabilistic methods [6] support a functionally incomplete operational basis **AND, OR** and, therefore, can generate only monotonous models of the system reliability and safety using flowcharts, connectivity graphs, event trees, fault-trees, etc. GLPA is the first to use a full logic operational basis **AND**, **OR**, **NOT**. ARBITER is, thus, the first to support all capabilities of Boolean algebra simulating. It, therefore, can perform all monotonous analysis tasks (solved by other theories and techniques), and, moreover, a new class of non-monotonous analysis tasks for reliability, survivability, safety and risk of large-scale, structurally complicated objects for various applications.
- Four other similar software complexes (two versions of Risk Spectrum (Sweden) [7], RISK [8], CRISS 4.0 [9] (Russia)) use only fault trees technology. ARBITER uses an innovative graphical technology of GLPA, i.e. functional integrity schemes (FIS) [3-5, 10] to represent reliability, safety and technical risks. FIS capabilities help to represent all monotonous structural models (flowcharts, connectivity graphs, event trees, fault-trees), and a new class of non-monotonous models of system's reliability and safety.
- Users of fault trees technology-based software can apply only a reverse logic for a reliability and safety analysis task statement development. This technique implies a clear understanding and graphical representation of conditions of system's availability, failure and emergency occurrence. For a large-scale structurally complicated system, e.g. a system with multiple cyclic (bridge) bonds or multiple elements' states, correct development of a fault tree may become an intractable problem [9]. Graphical FIS capabilities used in ARBITER provide the user with three optional methods of the task statement development:
  1. traditional **reverse logic**, resulting in development of the system's fault tree FIS;
  2. **direct logic**, resulting in FIS development of the flowchart [1] for the system's availability (non-failure operation, emergency non-occurrence), and, moreover, with an opportunity to represent unlimited amount of the system's cyclic (bridge) bonds;

3. **combined (mixed) logic**, helping to develop non-monotonous FIS for reliability, survivability, safety and risk of structurally complicated objects' operation.

Whichever method is used for FIS development, ARBITER may further automatically define the shortest paths of efficient operation and minimal cut sets, and their non-monotonous combinations. The practice shows that direct and combined methods help the user to develop more complicated and large-scale structural schemes of the system, with further automated definition of the minimal cut sets (i.e. automated generation of structurally complicated and large-scale fault trees).

- All other certified software used for a similar purpose (Risk Spectrum, RISK, CRISS 4.0) perform only approximate computing of system reliability and safety probabilistic measures, and the element's failure probability shall not exceed 0.01 [6]. ARBITER has been developed as a tool for exact probabilistic measures simulating and computing. Exact calculations are based on the procedure of automated generation of regular probabilistic function polynomials which was for the first time developed in GLPA and implemented in ARBITER [10]. Therefore, ARBITER is the first to perform exact probabilistic measures computing within all potential range of the elements' probabilistic values, from 0 to 1 inclusive.
- ARBITER provides an additional (supplementary) mode for approximate probabilistic measures simulating and computing. It helps to develop truncated logic functions which exclude low-probability conjunctions (paths and/or cuts). Two methods are used for approximate calculations: (i) computing of independent elements failures (similar to the method used in Risk Spectrum [7] and Saphire-7, USA), and (ii) a method considering three types of the elements' failure – "failure to operate", "failure in operation mode" and "latent failure in standby mode". These methods were for the first time developed and implemented in the certified software "CRISS 4.0" [9].

ARBITER intended use:

- Automated reliability simulating and computing for structurally complex systems, including objects of nuclear energy use and other hazardous industrial sites;
- Automated probabilistic simulating and computing of failure and emergency occurrence / non-occurrence for hazardous industrial site, including objects of nuclear energy use.

Practical application of ARBITER software is based on the new information technology of automated structural logic simulating (ASLS) [4, 5], including the stages as follows:

1. Formalized task statement for analysis of structurally complex system's reliability, survivability, safety (risk) based on the initial functional schema and description of the system's functionality. It can be made in any structure form, for example, using flowchart, connectivity graph, fault trees, event trees. Based on the initial formalized description a system's functional integrity scheme (FIS) is developed. Parameters of the system's elements reliability are determined and logic criteria of the system functions are specified.
2. After formalized initial data input into ARBITER, automatic generation of mathematical models and computing of the system's reliability, survivability and safety measure are performed. At this stage ARBITER performs:
   - Representing in the initial FIS (supergraph) of up to 400 elements (nodes) and up to 100 elements in each equivalented node (subgraph) of the main system's graph;
   - Automated generation of logic functions, representing shortest paths of efficient operation and minimal cut sets or their non-monotonous combinations (deterministic models of the system's features and parameters);
   - Automated generation of probabilistic functions for exact computing of the system's reliability, safety and risk;
   - Probabilistic calculations of logic criteria of reliability, failure and risk of the system and/or its subsystems;

- Computing of probabilistic measures of unrestorable system's non-failure operation and failure, computing of MTBF;
- Computing of restorable system's availability / non-availability factor, MTBF, mean restoration time and non-failure operation / failure probabilistic measures;
- Computing of availability of the mixed system, consisting of restorable and unrestorable elements;
- Computing of elements' significances, positive & negative contributions in the system's logic criteria probability;
- Approximate computing of probabilistic measures (without generation of probabilistic functions) with or without consideration of insignificant shortest paths and cuts;
- Computing of probabilistic measures of the system's specific shortest paths of efficient operation and minimal cut sets;
- Computing of individual and total failure cuts significances according to Fussell-Vesely;
- Computing of elements' significances, risk decrease / increase factors according to Fussell-Vesely;
- Approximate computing of the system's probabilistic measures based on three types of elements' failure (failure to operate, failure in operation mode and latent failure in standby mode [9]);
- Structural and automatic accounting of elements' group failure due to common cause (alfa-factor, beta factor and factors marked using Greek symbols);
- Consideration of various elements' dependencies and multiples states, represented by groups of incompatible events;
- Consideration of two-level decomposition of the structural schema, disjunctive and conjunctive multiplicity of complex elements (subsystems);
- Consideration on unlimited cyclic (bridge) connections between the system's elements;
- Consideration of various combinatory relations (K of N) between elements and subsystems' groups.

3. Deterministic (logic) and probabilistic parameters received as a result of automated simulating and computing shall be used for development and justification of managerial decisions on systems' reliability, survivability, safety and risk, and for development of the reporting documentation.

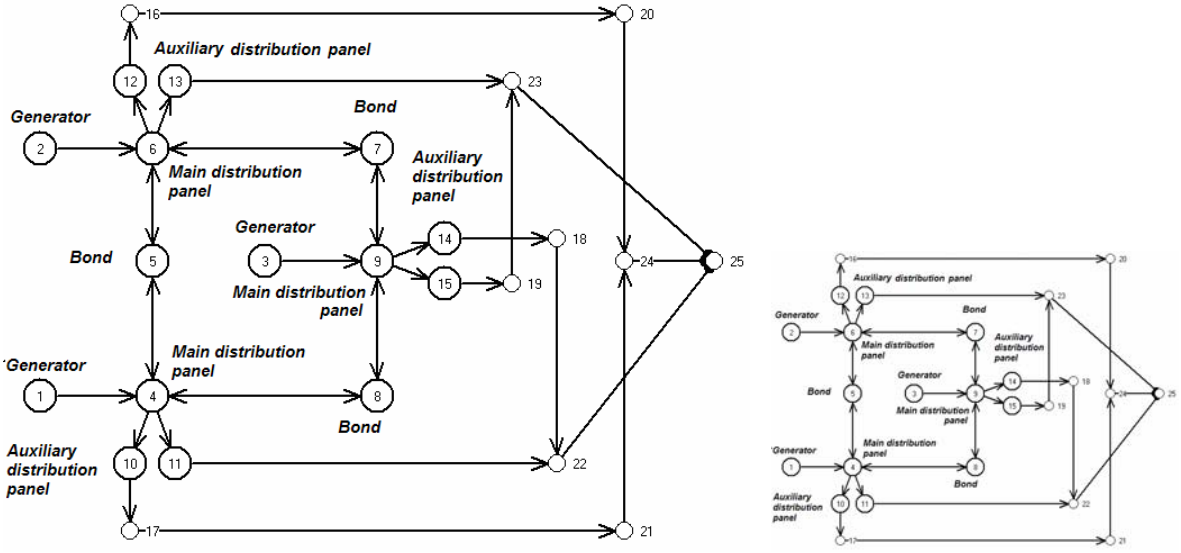
Certification procedure of ARBITER software

The certification expertise was carried out from November 21, 2005 till November 21, 2006. Experts from leading designing companies took part in the expertise, i.e. St. Petersburg ATOMENERGOPROJECT, All-Russian Research Institute for Nuclear Power Plant Operation VNIIAES, ATOMENERGOPROJECT, R&D Center of Nuclear and Radiation Safety (Moscow) and I.I. Afrikantov OKB Mechanical Engineering (Nizhny Novgorod). JSC "SPIK SZMA", the applicant, developed and submitted to experts the Verification report [2], including decisions of 10 computing and analytical Tests (42 examples, total of 184 tasks). The tests show decision of the following tasks resolved by ARBITER:

- Probabilistic analysis of hazardous objects' reliability, failure and emergency occurrence (Test No.1, total of 12 tasks);
- Computing reliability of systems with multiple cyclic (bridge) bonds (Tests 2, 10; total of 20 tasks);
- Reliability simulating and computing for nuclear energy sites and installations (Test No.3; total of 9 tasks);
- Probabilistic analysis of emergency scenarios (Test No.4; total of 6 tasks);
- Probabilistic system safety analysis using fault trees (Tests No. 5, 3, 10; total of 9 tasks);
- Standard and specific models of failures due to common cause (Tests No. 6, 7; total of 68 tasks);

– Reliability models of combinatory subsystems (Tests No. 8, 4; total of 14 tasks);
– Simulating of large-scale systems (Tests No. 9, 10; total of 64 tasks).

Below is an example of the test task resolved by ARBITER:



a) b)

Fig.1. Reliability FIS of large-scale cyclic system

Fig.1.a shows a FIS supergraph of a well-known task No.35 developed by Igor A. Ryabinin, founder of Logic Probabilistic Method [6]. Each system's element (each functional node 1-15 shown in Fig.1.a) includes a subsystem, all these subsystems have a similar structure form and their FIS is shown in Fig.1.b. Therefore, the system consists of 225 elements with multiple external and internal cyclic connections at various decomposition levels. Results of this problem which was decided using direct (non-failure operation) and reverse (failure) logic are shown below ($p_i = 0.9, i = 1,2,...,225$).

Logic criteria of the system's functions	Response time	Evaluation of total amount of logic function conjunctions	System reliability
Non-failure operation: y25	1 sec.	Shortest paths of efficient operation: 3.49409450070874 E+19	0.886737948063
Failure: y"25	1 sec.	Minimal cut sets: 8 621 131	0.113262051937

ARBITER can calculate exact probabilistic measures of the system reliability, in despite of the logic models' large scale, by using the structural decomposition (equivalising) method [3].

During certification expertise, it was proposed to resolve five Test Cases "Simulating and analysis of safety systems and nuclear plants in probabilistic safety analysis" (initial data on 201 pages, 20 tasks), earlier decided by CRISS 4.0 [9]. Using ARBITER, three types of decisions of the Test Cases were submitted:

– Approximate decisions of all five Test Cases according to CRISS 4.0 method, over 2000 compared parameters coincided;
– Approximate decisions of all five Test Cases according to Saphire-7 method (for independent elements' failures), over 2000 compared parameters coincided;
– Additionally, ARBITER was the first to calculate exact probabilistic measures of fault trees' node events for three Test Cases (models with independent elements' failures).

Tests and Test Cases decisions made by ARBITER have been checked in accordance with Regulations on software certification (RD-03-17-2001) and compared with:

- analytical tasks decisions;
- decisions provided in other sources;
- decisions received using other certified software - Risk Spectrum and CRISS 4.0;
- decisions received using Saphire-7 software, authorized by the US Nuclear Regulatory Commission;
- decisions received by RELEX (USA) software which is used worldwide.

During certification the experts had no critical remarks regarding accuracy of decisions by ARBITER of all 204 analytical & computing Tests and Test Cases.

ARBITER application experience

ARBITER is applied by several companies having appropriate licenses, including, but not limited to:

- JSC "SPIK SZMA", St. Petersburg, developer of ARBITER software; control system reliability computing has been implemented for hazardous industrial sites, i.e. Kirishi Oil Refinery (6 projects); LLC "MIR" (1 project); Mozyr Oil Refinery (4 projects); JSC "Kazanorgsynthesis", Tatarstan Republic (2 projects).
- Interindustry expert-certifying, R&D and control center of nuclear and radiation safety", St. Petersburg; 13 projects have been implemented for computing of reliability, residual life and risk of objects of nuclear energy use FGUP "PO Sevmach", Severodvinsk.
- ZAP "Company SZMA", St. Petersburg, reliability computing has been implemented for the automated information and measuring energy metering system (AIMEMS) of FGUP "Petersburg subway".
- JSC "Giprovostokneft", Samara, etc.

At present time JSC "SPIK SZMA" in cooperation with a group of companies launched joint work on development and adaptation of ARBITER's base version to various application domains of reliability and full risk simulating and analysis for hazardous industrial sites, nuclear energy plants, financial risks, and institutes educational and R&D activities.

Standards and Regulations met by ARBITER

1. GOST 24.701-86. Reliability of automated control systems. General provisions. Moscow, 1986. - 17 pp.
2. GOST 27.301-95. Reliability in technique. General provisions. M., 1996. – 15 pp.
3. RD 03-418-01. Instructions on the Risk Analysis Performance For Hazardous Industrial Sites // Interindustry regulations on industrial safety and resources conservation. Series 03. Volume 10. Moscow, 2001. – 60 pp.
4. GOST R 51901-2002 (IEC 60300-3-9:1995). Dependability management. Risk management of technological systems. Moscow, 2002. – 22 pp.
5. GOST R 51901.14-2005 (IEC 61078:1991). Risk management. Reliability block diagram method. Moscow, 2005. – 18 pp.
6. GOST R 51901.13-2005 (IEC 61025:1990). Risk management. Fault tree analysis. Moscow, 2005. – 11 pp.

More information is available at: http://www.szma.com

BIBLIOGAPHY

1. ARBITER, “Software complex for automated structural logic simulating and computing of reliability and safety measures of control systems (SC ASLS SZMA), version 1.0, base sample”. State registration Certificate No. 2003611101. Issued by ROSPATENT (Moscow) in 2003. Expertise Certificate No.222 dated of February 21, 2007, issued by the Software Certification Committee of the Federal environmental, technological & nuclear supervision agency (Rostechnadzor) of the Russian Federation at R&D Center of Nuclear and Radiation Safety паспорт.
2. A.S. Mozhaev, A.V. Kisilev, A.V. Strukov, M.S. Skvortsov. Verification report of the software “Software complex for automated structural logic simulating and computing of reliability and safety measures of control systems (SC ASLS SZMA, base sample, version 1.0, ARBITER). Final revision. St. Petersburg, 2007. - 498 pp.
3. A.S. Mozhaev. General logic probabilistic method of complex system reliability analysis. Educational book. Leningrad, 1988. – 68 pp.
4. A.S. Mozhaev. Theory and practice of automated structural-logical simulation of system. International Conference on Informatics and Control (ICI&C'97). Vol. 3. St. Petersburg: SPIIRAS, 1997, pp. 1109-1118.
5. A.S. Mozhaev. Automated structural logic systems simulating. St. Petersburg, 2006. – 590 pp.
6. I.S. Ryabinin. Reliability and safety of structural complex systems. St. Petersburg, 2000. – 248 pp.
7. Risk Spectrum PSA Professional 1.20 / Theory Manual. RELCON AB, 1998. – 57 pp.
8. RISK code for standard probabilistic calculations. Moscow. http://www.insc.ru/PSA/risk.html.
9. A.M. Bakhmetiev, I.A. Bylov, Yu.V. Milakova. R&D report “Verification and foundation of the software CRISS 4.0 for nuclear plant safety simulating and analysis within safety probabilistic analysis”. Part 1 (Final revision). Nizhny Novgorod, 2005. – 88 pp.
10. A.S. Mozhaev, I.A. Gladkova. Library of software modules for automated generation of system availability monotonous and non-monotonous logic functions and probabilistic function polynomials (LOG&PF). State registration Certificate No. 2003611100. Moscow, 2003.
11. A.S. Mozhaev, I.A. Gladkova. Software complex for automated structural logic simulating of structural complex systems 2001 (SC ASLS 2001). State registration Certificate No. 2003611099. Moscow, 2003.
12. A.S. Mozhaev. Universal graphic-analytical method, algorithm and software for development of monotonous and non-monotone logical functions of system's efficiency. // Proceedings of the International Scientific School “Modeling and analysis of safety and risk in complex systems”. St. Petersburg, 2003, pp. 101-110.
13. A.S. Mozhaev. Software complex for automated structural logic simulating of structural complex systems 2001 (SC ASLS 2001). // Proceedings of the International Scientific School “Modeling and analysis of safety, risk and quality in complex systems”. St. Petersburg, 2001, pp. 56-61.
14. A.S. Mozhaev. Software for automated simulating and evaluation of designed control systems reliability and safety. // Online R&D journal “Industrial labour safety”, No.6, 2003. http://www.alf-center.com/pbt/magazine6/mozhaev.shtml
15. A.S. Mozhaev. Technology and software complex for automated simulating and evaluation of reliability, safety and risk for hazardous industrial sites. // Fifth Workshop “On expertise of industrial safety declaration and liability insurance. Development of methods of emergency risk evaluation at hazardous industrial sites”. Moscow, Federal environmental, technological & nuclear supervision agency, 2004, pp. 50-58.
16. A.S. Mozhaev. Comparative analysis of fault trees technology and automated structural logic simulating technology applied for probabilistic safety analysis of designed nuclear power plants and process control systems.// The 9th Scientific Workshop “Software for industrial risk analysis” at Educational center of R&D Center “Industrial Safety” of RF Rostechnadzor. Abstract published in “Industrial labour safety”, No. 12, 2005, pp. 61-63.

17. Sh.V. Kamynov, M.I. Rylov, A.S. Mozhaev, A.A. Nozik. Application method of the software complex ASLS SZMA for calculations of reliability and no-failure operation of the physical measurements stand. // Risk management, Moscow. – 22 pp.