**FEDERAL ENVIRONMENTAL,
INDUSTRIAL AND NUCLEAR SUPERVISION SERVICE**

APPROVED BY
Order  No. 26 of the Federal Environmental, Industrial and Nuclear Supervision Service dated January 28, 2015

**SAFETY GUIDE IN THE USE OF ATOMIC ENERGY
"RECOMMENDATIONS ON THE PROCEDURE FOR RELIABILITY ANALYSIS OF SAFETY-RELATED NPP SYSTEMS AND ELEMENTS"
(RB-100-15)**

EFFECTIVE
from January 28, 2015

**Moscow 2015**

**SAFETY GUIDE IN THE USE OF ATOMIC ENERGY** "**RECOMMENDATIONS ON THE PROCEDURE FOR RELIABILITY ANALYSIS OF SAFETY-RELATED NPP SYSTEMS AND ELEMENTS AND THEIR FUNCTIONS**" **(RB-100-15)**

**Federal Environmental, Industrial and Nuclear Supervision Service**

**Moscow 2015**

This Safety Guide has been developed in accordance with the Article 6 of the Federal Law No. 170-FZ "On atomic energy use for promotion of the requirements of the Federal Rules and Regulations in the field of atomic energy use "General safety assurance provisions of nuclear power plants" (OPB-88/97), approved by the Ordnance of Gosatomnadzor of Russia No 9, dated November 14, 1997, Federal Rules and Regulations in the field of atomic energy use "Requirements to the report content for justification of safety of a NPP with VVER type reactor" (NP-006-98) approved by the Ordnance of Gosatomnadzor of Russia No 7 dated May 3, 1995, Federal Rules and Regulations in the field of atomic energy use "Requirements to the report content for safety justification of nuclear power plants with fast breeder reactors" (NP-018-05) approved by the Rostechnadzor ordnance No. 9 dated December 2, 2005.

The Safety Guide contains recommendations of the Federal Environmental, Industrial and Nuclear Supervision Service on the procedure for performance and presentation of the reliability analysis of the safety-related systems and elements as well as the functions performed by them.

The Safety Guide is designed for use by the design and engineering organizations and the operating organizations.

Published for the first time[[1]](#footnote-1)

**I. General**

1. This Safety guide in the use of atomic energy "Recommendations for reliability assurance procedure of the safety-related systems and elements of nuclear power plants, and their functions" (RB-100-15) (hereinafter the Safety Guide) has been developed in compliance with the Article 6 of the Federal Law No. 170 FZ, dated November 21, 1995 "On atomic energy use" for promotion of the requirements of the item 4.1.12 of the Federal Rules and Regulations in the field of atomic energy use "General safety assurance provisions of nuclear power plants" OPB-88/97 (NP-001-97) approved by the Ordnance of Gosatomnadzor of Russia No 9 dated November 14, 1997 with respect to performance of reliability analysis, assessment of reliability indices and presentation of the results for the normal operation nuclear power plant safety-related systems and their elements classified under safety classes 1 and 2, and safety systems and elements of nuclear power plants; item 1.8.1, and subsection 4 of the section "General requirements" of the Federal Rules and Regulations in the field of atomic energy use "Requirements to the content of report on safety assurance of a NPP with VVER type reactor" (NP-006-98) (PNAE G-01-036-95), approved by the Ordnance of Gosatomnadzor of Russia No 7 dated May 3, 1995, with respect to presentation of information on reliability of the safety-related system elements; item 1.8.1 of the Federal Rules and Regulations in the field of atomic energy use "Requirements to the contents of safety assurance report of nuclear power plants with fast breeder reactors" (NP-018-05) approved by the Rostechnadzor Ordnance No. 9 dated December 2, 2005 (registered by the Ministry of Justice on January 26, 2006, registration No. 7413) with respect to the presentation of information on reliability of performing safety functions.

2. This Safety Guide contains recommendations of the Federal Environmental, Industrial and Nuclear Supervision Service for the objective, scope, procedure for performing reliability analysis of safety-related systems and elements, application of the results of assessments, and on the content and scope of deliverables in performing the specified analysis.

3. This Safety Guide is designed for use by the design and engineering organizations and the operating organizations.

4. The requirements of the Federal Rules and Regulations in the field of atomic energy use may be met using other procedures for reliability analysis of performing functions by the safety-related systems and elements of the nuclear power plants including the reliability analysis (functional safety) of high-end process complexes than those which are available in this Safety Guide, on justifiability of the selected methods (techniques) for safety assurance.

5. A list of abbreviations used in this Safety Guide is given in Appendix No. 1 to this Safety Guide, terms and definitions are given in Appendix No. 2 to this Safety Guide, the list of references recommended for use in performing the reliability analysis in accordance with the recommendations of this Safety Guide is given in Appendix No. 3 to this Safety Guide.

6. The reliability analysis of the safety-related systems and elements (functional safety) of high-technology complexes is made for the designed, constructed and operating NPP units.

7. The reliability analysis shall be performed with respect to:

normal operation, safety-related systems;

safety systems;

elements of normal operation systems classified in safety classes 1, 2;

special technical equipment for managing beyond-design basis accidents;

other NPP systems and elements for which specified reliability measures are stipulated;

safety-related functions (including safety functions), if in performing the safety-related functions more than one system participate (including high-technology complexes).

8. The recommendations presented in this Safety Guide by execution procedure of the system reliability analysis are related also to the reliability analysis of performing safety functions and other required functions.

The reliability analysis of individual systems from among the specified systems (including systems included in the high-technology complexes) for performing the relevant functions shall be allowed to not perform provided that the development of the reliability analysis for performing safety functions (other required functions), which are carried out due to joint operation of several systems (including high-tehnology process complexes).

9. The qualitative reliability analysis of the safety-related systems shall be made in accordance with the provisions of the chapter II of this Safety Guide.

The reliability analysis (determination of reliability indices) of the NPP elements shall be made in accordance with the provisions of the chapter II of this Safety Guide.

The qualitative reliability analysis of the safety-related systems shall be made in accordance with the provisions of the chapter IV of this Safety Guide.

The provisions of chapter V of this Safety Guide are also considered in the quantitative reliability analysis (functional safety) of high-technology complexes along with the provisions of the chapter IV.

10. The result of reliability analysis is the determination (evaluation) of the reliability indices of safety functions and other required functions performance by the system and elements. The indices characterizing the safety of analyzed system (element) shall be taken in the scope of reliability indices.

11. All the safety-related functions (including safety functions) which the system performs during NPP normal operation and during operational occurrences of NPP including accidents shall be determined in the system reliability analysis. The reliability analysis is made individually for each of the system functions stipulated in accordance with this item.

12. The system reliability analysis is made individually for each of the identified normal operation states and states with operational occurrences of NPP whereupon the performance of the required function by the system is necessary, if one of the following condition is true:

for the considered NPP state the failure criterion for performance of the required function by the system differs from the failure criterion for other states;

for the considered state the NPP configuration of the system (set of system elements, the condition thereof affects the performance of the required function by the system) differs from the system configuration in other states;

in the considered NPP state the requirements from the part of the analyzed system to the state of supporting or managing system differ, the operation thereof is required for the system to perform the required function;

for the considered state the list of failures of the system elements capable of having impact on the performance of the required function by the system differs from the list of such failures for other states.

13. The results of reliability analysis of the systems (elements) for which specified reliability measures are stipulated shall be compared with the specified indicators.

14. The results of the reliability analysis of the systems (elements) shall be recommended to use in performing the safety analysis (in particular, probabilistic safety analysis) and in development of the recommendation for enhancing NPP safety.

15. The real state of the NPP systems (elements), effective operation procedures, maintenance, tests and repair (if available) as well as operation experience of the NPP unit for which reliability analysis and operation experience of similar NPP units shall be considered in the reliability analysis of the systems (elements) of the operated NPP units.

16. The reliability of supporting systems and control systems on which the performance of its functions by the analyzed system depend shall be considered in the reliability analysis of the system.

17. The potential personnel errors and common cause failures (common failures) shall be considered in the analysis of system reliability.

**II. Qualitative analysis of system reliability**

18. The qualitative analysis of system reliability shall be made after collection of information on the system and determination of the simulation boundaries carried out in accordance with Appendix No. 4 to this Safety Guide.

19. Quality analysis of the system reliability consists in determining the consequences of failures of elements and personnel errors and performed in the following sequence individually for each function of the system considered in accordance with the item 11 of this Safety Guide:

determination of the failure criteria for performance of the required functions by the system;

development of simplified system diagram;

determination of the consequences of failures and element non-availability, as well as wrong actions of the personnel;

graphic illustration of the system (system functions) operability conditions.

20. A simplified diagram of the system shall be developed based on the complete system diagram. Only those elements, which are included within the simulation boundary of the system in accordance with Appendix No. 4 to this Safety Guide shall be included in the simplified diagram.

21. Groups of system elements for which the potential occurrence of common cause failures (common failures) shall be determined.

The following causes which may lead to such failures shall be considered in determining the groups of elements of the system susceptible to common cause failures (common failures):

element commanility;

identical usage conditions of elements including operation modes and ambient conditions;

identical maintenance and repair conditions.

22. The consequences of failures of elements and personnel errors shall be determined in the following sequence:

for each system element a list of the potential types of failures of the given element is prepared;

for each element or group of elements subject to common cause failures, or the personnel actions are assessed severity of the consequences of element failure, personnel error, failure of group of elements (for example failure of the system, failure of system channel, reduction of the redundancy level);

failures of elements and personnel errors are highlighted, as well as the failures of a group of elements, susceptible to common cause failures which lead to system failure with inclusion in the list of critical failures (errors).

**III. Determination of reliability indicators of the elements.**

23. The possible types of failures capable of having impact on reliability of performance of the required functions by the analyzed system shall established for each element included in the simulation boundaries of the system in accordance with the recommended procedure presented in Appendix No. 4 to this Safety Guide.

The following types of failures are considered:

failure to the request (including the failure to start-up, failure to open, failure to close, failure to change position);

failure during operation (including failure of type inadvertent occurrence of a function).

24. The necessity of taking into account the system reliability for the events related to unavailability of system elements, system channels or system overall due to maintenance, repair or tests is analyzed in the model.

25. The decision on the necessity of taking into account the system reliability for the specific types of failures of the system elements and events of unavailability of system elements, system channels or system overall due to maintenance, repair or tests shall be taken following analysis of the failure types and their consequences performed for the system and presented in the form of a table, an example thereof is presented in Appendix No. 6 to this Safety Guide.

26. The following types of input data shall be used for calculation of the reliability indices:

data obtained in operation of the analyzed system (elements), or analyzed NPP (specific data);

data received in operation of similar NPP systems (elements) (generalized data).

27. The reliability indices of the system elements shall be calculated using specific data, and if unavailable by using generalized data.

28. The following characteristics of the elements shall be determined for evaluation of the reliability indices of the elements:

accumulated operating time (in hours) in standby mode;

accumulated operating time (in hours) in operation mode;

number of requests for actuation (for example, requests for start-up, for opening, for closing);

number of failures for the operation time in standby mode;

number of failures for the operation time in operation mode;

number of failures to respond to request

29. All the periods in standby mode (availability for performing the required function) or in operation mode (performance of the given function) with the NPP unit in the considered state shall be taken into account in evaluating the total operation time.

In calculating the number of requests for actuation of the element all the requests shall be considered for actuation occurring during:

function check (the relevant function check documents shall be used for determining the function check rate of a specific equipment);

normal operation of NPP (by automatic protetions or manually by the operator);

occurrence of other situations, requiring actuations (start) of the element.

The requests for actuation (start) shall be classified in accordance with the types of failures determined for the given type of element (for example, request for opening, closing , start).

30. The following reliability data of its elements shall be required as a rule for determining the reliability indices of the system for performing the required functions (probability of trouble-free performance):

intensity of failures of system elements in standby mode and in operation mode;

periods between the function checks of the system elementsl

duration of function check;

probability of failures to request of system elements;

mean unavailability time of the system (system elements) due to performance of maintenance, repair or tests;

permitted system (system elements) unavailability time in NPP unit operation mode retention

31. The recommended procedure for determining the failures and quantitative assessment of the reliability indices of the NPP elements is presented in Appendix No. 6 to this Safety Guide.

**IV. Quantitative analysis of system reliability**

32. The quantitative analysis of system reliability is made for each of the requested system functions considered in accordance with the item 11 of this Safety Guide.

33. The quantitative analysis of system reliability is made in the following sequence:

qualitative analysis of system reliability is made (in accordance with the recommended procedure presented in the chapter II of this Safety Guide);

reliability indices of the system elements are determined (probabilities of failures of system elements including probability of unavailability due to maintenance, repairs and tests) in accordance with the procedure presented in the chapter III of this Safety Guide;

accounting of the personnel influence of reliability of performance of the requested functions by the system is made (in accordance with the recommended procedure presented in Appendix No. 5 to this Safety Guide);

general failures are accounted (in accordance with the recommended procedure presented in Appendix No. 7 to this Safety Guide);

type of graphic presentation of the structural-logic model of the system used for quantitative analysis of the system reliability is determined (fault trees, functional integrity diagrams, Markovian schemes etc.);

structural-logic models of the system (for example, fault trees) for each of the request system functions are developed;

reliability indices of the system are calculated for each of the required functions;

reliability level of the system is evaluated (including comparison with the standardized reliability indices, if installed).

34. The following shall also be performed in quantitative analysis of the system:

calculation uncertainty estimation of the system reliability indices;

estimation of the significance of system elements and personnel actions (errors);

estimation of the sensitivity of calculation results of system reliability indices to the input data used in their performance.

35. In the analysis of sensitivity to allowances and approximations made it is required to:

consider all the allowances and approximations made, influencing the results of system reliability analysis;

give justifications of the assumptions and approximations made with the required references;

assess the influence of assumptions and approximations on the results and conclusions of the system reliability analysis.

36. The dependencies of the system failure events (trouble-free operation) in performing the required function (in accordance with the established system failure criteria) against occurrence of the following events impacting the reliability of performance of the requested function by the system shall be considered in the development of structural-logic model of the system.

failures (trouble-free operation) of the system elements;

unavailability of system elements (system channels, systems overall) due to maintenance, repair or tests);

errors (error free actions) of personnel;

failures (trouble-free operation) of supporting or control systems;

General failures;

initiating event of the accident or impact occurring during operational occurrences, including accidents (for the functions performed during the accidents) environmental conditions.

37. Scope of reliability analysis report of NPP systems is presented in Appendix No. 8 to these Safety Rules. Example of system reliability analysis is presented in Appendix No. 9 to this Safety Guide.

**V. Reliability analysis (functional safety) of high-technology complex**

38. Reliability analysis (functional safety) of high-technology complex shall be made as follows:

design and operation information gathering and analysis on high-technology complex including determination of the simulation boundaries of the high-technology complex and scope of systems (elements) included in it;

stipulation of safety-related functions performed by the high-technology complex and determination of the failure criteria with respect to each of the functions;

determination and description of the process (processes) performed by the high-technology complex, alloting the basic intervals;

analysis of the technology complex dependency on the supporting and control systems;

accounting of personnel influence on reliability (functional safety) of the complex;

accounting of GF;

determination of the reliability indices of the elements (systems) included in the high-technology complex;

building of the structural-logic model of the high-technology complex and determination of its reliability indices (functional safety) for the performance of requested functions by them;

assessment of the results of analysis.

39. The design and operation information on the high-technology complex shall be gathered and analyzed for each of the systems included in the scope of the specified complex in accordance with the recommended procedure presented in Appendix No. 4 to this Safety Guide.

The main sources of input data on the high-technology complex are the design and operation documentatio, operation experience and test results.

In gathering input data familiarization with the process implemented by this complex shall be made apart from the technical documentation for the high-technology complexes in operation . The familiarization with the process at the NPP pursues the following basic objectives:

verification of data in the technical documentation;

determination of the possibility of common cause failures;

specification of the personnel action procedure for process management, identification of possibility of personnel performing erroneous actions, and factors impacting the reliability of personnel performing actions at the equipment location.

40. In determining and describing the process performed by the high-technology complex based on design and operation documentation all the process operations in the scope of the specified process are highlighted, their performance sequence, start and end process operations are established. The scope of elements (systems) of the high-technology complex participating in its performance and the required NPP personnel actions is determined for each highlighted process operation.

41. The basic intervals, i.e. parts of the process characterized by the permanency of failure occurrence conditions of the high-technology complex for performing the required function shall be highlighted following the highlighting of process operations included in the scope of process carried out y the high-technology complex.

42. In establishing the failure criteria for the high-technology complex it shall be considered that the complex may perform several requested functions, in particular, the function related to the functioning for the purpose specified (first type function) and the function related to prevention of non-compliance with the requirements of the regulatory and/or design documentation (second type function). Respectively for each of the required functions different criteria of failure are assigned and individual reliability analysis is made.

In performing the required functions of second type from the above specified the high-technology complex shall be considered as failed in non-compliance with the stipulated requirements of the regulatory and/or design documentation even if it maintains the ability to function for the designed purpose (i.e. maintain the ability to perform first type function from the functions specified above).

For example, in the reliability analysis of the technology complex of the transportation and processing operations with nuclear fuel the capability of carrying out the transportation and processing operations process may be considered as the first function (failure criteria to perform this requested function - abnormal termination of the transportation and processing operations), and the non-admission of non-compliance with the regulatory documents or design (engineering) documents to performing transportation and processing operations may be considered as the second function (for example non-exceedance of permitted displacement speed, permitted force in removing FA, not violating the requirements of the nuclear and radiation safety).

Reliability analysis of a high-technology complex for performing the required functions similar to the second of the above specified functions is allowed to name as the functional safety analysis of a high-technology complex.

43. The identification of possible cause and effect relationships leading to failure of a high-technology complex is made when determining the consequences of disturbances in the functioning of individual systems (elements) of a high-technology complex.

The consequences of disturbances in the operation of a high-technology complex shall be determined individually for each of the assigned basic intervals.

First the list of elements and (or) actions or personnel engaged in performing the process at each specific basis interval is determined in the analysis. Then the process disturbances characteristic for the considered basic interval are determined and an analysis of their consequences is made.

The consequences of the malfunctions of the high-technology complex is determined considering the operation of protections and interlocks provided for in the high-technology complex.

The identified malfunctions may lead to failure of the high-technology complex not at the basic interval to which the malfunction belongs but at any of the subsequent basic intervals in determining the consequence of malfunctions of the high-technology complex.

The results of determining the consequences of function failure of a high-technology complex are presented in the format of table 1.

Table 1 Specimen of presentation of results of determining the consequences of function failure of a high-technology complex

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Basic interval | List of elements (systems), personnel actions | List of process disruptions | Provisioned protections and interlocks | Disruption consequences (during disability of protections and interlocks) |
|  |  |  |  |  |

*Note:*

*The list of basic intervals assigned in determining and describing the process in entered in the "Basic interval" column.*

The elements (systems) of a high-technology complex used for performing the processes of the relevant basic interval are specified in the column "List of elements (systems), personnel actions", and the required personnel actions are specified.

The process disruptions are specified in the column "List of process disruptions", occurrence thereof is possible at the relevant basic interval.

The protections and interlocks preventing the transition of process disruption to failure of a high-technology complex are entered in the "Provisioned protections and interlocks" column.

Information on the consequences to which the identified failures of a technology complex may lead to if protections and interlocks are inoperable is entered in the column "Consequences of failure" (protections and interlocks are inoperable).

44. The reasons of occurrence of process disturbances shall be determined for establishing the cause and effect relationship of the failures of system elements and personnel errors with process disturbances.

The causes of process disturbance occurrence shall be determined considering the protections and interlocks in the high-tehnology complex.

The result of determining the reasons of occurrence of process disturbances shall be presented in the format of table 2.

Table 2

Specimen for presentation of the results of determining the reasons of process disturbance occurrence

|  |  |  |
| --- | --- | --- |
| Process disturbance | Failures of elements (systems), personnel error leading to process disturbances | Provisioned protections and interlocks |
|  |  |  |

45. Structural-logic model of a complex processing facility, which is a serial (i.e. using logical operator "OR") connection of fault trees of the high technology facility at individual basic intervals is developed.

46. Recommended procedure of determining the reliability indices of the elements of a high technology facility is similar to the procedure presented in the chapter III of this Safety Guide.

47. Recommended procedure of determining the influence of personnel is similar to the recommended procedure presented in Appendix No. 5 to this Safety Guide.

48. Recommended procedure of accounting the general failures is similar to the recommended procedure presented in Appendix No. 7 to this Safety Guide.

49. The results of analysis of the consequences of failures of the operation of a high-technology facility in accordance with the item 43 of this Safety Guide in building the structural and logic model (for example, fault trees) of the high-technology facility, and the analysis results of the reasons for occurrence of process disturbances in building the structural-logic model (for example fault trees) of individual basic intervals, performed in accordance with the item 44 of this Safety Guide.

50. Example of system reliability analysis (functional safety) of a high-technology facility is presented in Appendix No. 10 to this Safety Guide.

**VI. Specifics of reliability analysis of systems with passive elements**

51. Reliability analysis of systems considering the specific features set forth in this chapter shall be made with respect to the systems, the reliability model thereof considers the operability of the passive elements experiencing impact from the operational loads such as own weight, pressure of operating medium (pressure of coolant, fuel or oil, feed or cooling water in the piping or heat exchange unit, gas pressure in the pressure vessel, hydrostatic pressure in the vessel for storage or plant make up tank), temperature loads etc., and experiencing impact of emergency and super loads (for example, emergency pressure, impact loads, including water hammer, fire loads, emergency pressure in the containment) and loads from external impacts (for example, inertia loads, impact loads).

52. The current operational, super and emergency loads shall be combined into the loading modes, which are characterized by the type of loading, parameters of loading and implementation frequency of loading.

53. The failure of the passive element may be the result of occurrence of fully stressed state in the element following the impact of loads shall be considered in the reliability analysis. The failure of elements may be caused by the accumulation processes of damages shall be considered, the reasons thereof may be impact of cyclic loads or impact from the part of operating medium (in time in the process of operation the impact of cyclic loads may lead to the appearance and accumulation of damages, origination and development of cracks; characteristic process in this case may be the mechanical fatigue or thermal fatigue).

The impact on the part of the operating medium (internal and external) with time in the operation process may also lead to the damage accumulation process, which may be characterized by the degradation of the material properties, origination of cracks and (or) discharge of material particles by the operating medium (for example, corrosion, erosion). Besides the impact of loads may accelerate or qualitatively change the process (for example, stress corrosion). The process may lead to reduction of the load bearing capacity of the passive elements (for example, following te reduction of the wall thickness of the vessels , piping). This may lead to reaching the limit state and degradation failure of the element.

54. The limit state criterion shall be set in reliability analysis of the passive elements, as well set what stress modes ad processes during operation potentially may lead to occurrence of limit states for the effective stresses or on conditions of accumulation of damages (figure 1).

55. The failure probability assessments (fail-safe operation) shall be made by calculation methods by employing data on statistical characteristics of the strength of materials and data considering the potential spread of loading state characteristics and medium impact.

56. The following calculation methods shall be used for reliability assessment of the passive elements by the limit states:

factor of margin method (load-strength model);

methods of two moments (first order reliability method FORM and second order reliability method SORM);

statistical modeling methods (for example, Monte-Carlo method, Monte-Carlo method with importance sampling, modeling with area sampling, for exampe, Latin hypercube method).

The approaches most frequently used in the reliability assessment of the elements, the failure thereof is caused by the use of load force are described in detail in the literary sources presented in Appendix No. 3 to this Safety Guide.

Fig. 1. The factors subject to accounting in reliability analysis with passive elements

57. The reliability assessment shall be made with probabilistic methods of fracture mechanics with involvement of data on characteristics of materials for the passive elements, which are under the impact of cyclic load and (or) influence of the impact of operating medium (for example, corrosion, erosio). Statistical data on distribution of discontinuities and defects of materials obtained following non-destructive testing shall also be used. Approaches for use of the probabilistic methods of mechanics of damage for reliability assessment has been described in detail in the literary sources listed in Appendix No. 3 to this Safety Guide and presented in brief in Appendix No. 11 to this Safety Guide.

58. Uncertainty analysis shall be performed, the objective thereof being the determination of the confidence limits of the reliability index of the investigated element, and for this purpose the uncertainty of the parameters of loads, strength of materials, frequency of implementation of each loading mode and potential combinations of the modes are assessed and used.

**VII. Specifics of reliability analysis of software / hardware means**

59. Both the potential failures of hardware (technical) means and the failures due to errors in the SW shall be considered in the reliability analysis of software / hardware means using the SW The possibility of mutual influence on the reliability of technical means and SW shall be considered. For example, some failure of SW may be caused by defects of technical equipment (failures in the operation of memory locations, distortion of information in the communication channels).

60. The approach described in the chapters II-IV of this Safety Guide shall be used in the reliability analysis of technical equipment. The possibility of detecting the failures using built-in self-checking modules shall be considered in performing this reliability analysis.

61. Specialized methods, descriptions and application examples thereof are presented in Appendix No. 12 to this Safety Guide and/or expert evaluations.

62. The reliability indices of the software and hardware means characterize their ability to perform the given functions in accordance with the given requirements in conditions of deviations in the functioning environment caused by various destabilizing factors. The specified factors shall include in particular, changes of the operation condition of the technical equipment, their failures and disruptions, changes in input data, changes in the distribution of memory resources.

63. The SW errors, which prevent the performance of the required functions by the system and errors which do not influence on the performance of the requested functions by the system shall be segregated in analyzing SW reliability.

64. Two types of software failures shall be considered in the model in the software reliability analysis: programming failures and fatal errors potentially leading to required functional failures by the software and hardware means at once in several APS channels.

65. Software failures are caused by undetected programming errors, which mainly influence the organization data exchange. Due to such errors, the software outputs incorrect results, in spite of the fact that the input data complies with the requirements, for example, due to problems with dynamic distribution of resources. Besides, the root cause of SW failure is not eliminated, and in the very same situation the failure must repeat, and an exact repeat of data and respectively failure related to it is improbable. Hence the specified error in the SW development is manifested in the form of intermittent failures, i.e. failures, which are eliminated predominantly by automated methods (re-initialization of SW).

66. The most characteristic consequence of failures in the functioning of SW, which shall be considered in the reliability analysis is the "failure to operate" type failure of the relevant technical equipment. As a rule all the software errors of the hardware are explicitly manifested.

67. If the software implemented in the programmable hardware represents a sufficiently simple direct action software, i.e. no data exchange takes place between other software applications and libraries, then it considerably reduces the probability of errors as such and excludes the situations which lead to spontaneous generation of output signal if there is no input signal (i.e. failures of spurious action type).

68. Programming errors may lead to common cause failure of the entire software in implementing the configurations and boundary conditions not provide for during programming. It shall be assumed that such common cause failures are possible only with respect to failures of non-operate type and do not lead to failure of all the redundant channels of the analyzed system with similar programmable hardware in its scope (i.e. when the redundant channels do not meet the diversity principle). The probability of such global failure cannot be assessed from the operation experience and provided that the proper quality assurance procedures are followed at all life cycle stages of the SW and may be taken as equal to 1.0-10-5 for the requirement.

Appendix No. 1

to the Safety guide in the use of atomic energy “Recommended procedure for NPP safety-related systems and elements reliability analysis, and their functions" approved by the order of the Federal Environmental, Industrial and Nuclear Supervision Service No. 26
dated January 28, 2015

**Abbreviations**

|  |  |  |
| --- | --- | --- |
| ASB | — | Automatic switch-over to backup |
| NPP | — | Nuclear Plant |
| NPP | — | Nuclear Power Plant |
| APCS | — | Automated process control system |
| SFP | — | Spent Fuel Pool |
| BI | — | Basic interval |
| MCR | — | Main control room |
| I&C&A | — | Instrumentation and control and automation |
| RM | — | Reloading (refueling) Machine |
| SAR | — | Safety Analysis Report |
| SFA | — | Spent fuel assembly |
| SNF | — | Spent nuclear fuel |
| SW | — | Software |
| ECR | — | Emergency Control Room |
| I&C | — | Instrumentation and control system |
| FP I&C  | — | Fire protection instrumentation and control system |
| FA | — | Fuel assembly |
| TVM | — | Television mast: |
| THO | — | Transport and handling operation |
| TS | — | Technical Specifications |
| TP | — | Transport package |
| CFF | — | Casings with fresh fuel |
| SNFS | — | Spent nuclear fuel storage |

Appendix No. 2
to the Safety guide in the use of atomic energy “Recommended procedure for NPP safety-related systems and elements reliability analysis, and their functions" approved by the order of the Federal Environmental, Industrial and Nuclear Supervision Service No. 26
dated January 28, 2015

**Terms and definitions**

The following terms and definitions are used for the purposes of these Safety Guidelines.

|  |  |  |
| --- | --- | --- |
| **Reliability analysis** | — | Analysis made for determining the reliability indices of the system (element). |
| **Posterior distribution** | — | Distribution of a random value describing basic knowledge on a reliability parameter after recording the operational information concerning the quantity and chronology of the system (element) failures. |
| **Prior distribution** | — | Distribution of a random value describing basic knowledge on a reliability parameter prior to the moment of receipt of the operational information concerning the quantity and chronology of the component failures. |
| **Basic event** | — | An event considered as elementary, not depending on the occurrence of other events considered in the system reliability analysis. |
| **Basic interval** | — | Totality of process operations characterizing the consistency of conditions of system failure occurrence (high-technology complex). |
| **Faultless Operation** | — | Capacity of system (element) to continuously maintain the operable state for a specific calendar time or operation life. |
| **Probability of fault-free operation:** | — | Probability of the fact that the system (element) failure shall not occure in the given time interval or within the limits of the given hours in operation. |
| **Probability of failure to respond to a request** | — | Probability with which the system (element) fails to perform the required function, designated under the requirement for its performance. |
| **External impacts** | — | impacts of any natural phenomena and human activities characteristic for the NPP site, for example earthquakes, high and low level of surface and ground water, hurricanes, accidents with air, water and land transport, fires, explosions at any facilities adjacent to the NPP, etc. |
| **Recovery time** | — | recovery duration of the system (element) operability state. |
| **Time of repair** | — | Total duration of operations to recover operability of the system (element). |
| **Flaw** | — | Each individual non-conformity of the system (element) to the stipulated requirements. |
| **Dependent failure** | — | Failure caused by other failures or by external impact. |
| **Failures rate** | — | Conventional probability density of a system (element) failure determined provided that the failure was not observed prior to the moment under consideration. |
| **Working condition of the system (element)** | — | Condition of a system (element) in which it meets all the requirements of regulatory and/or engineering (design) documentation. |
| **Testing** | — | Periodic inspection of the system (element) operability by means of testing from the control key or process protections and interlocks. |
| **Failure criterion** | — | attribute or set of attributes of impairment of serviceability stipulated in the regulatory or design (engineering) documents. |
| **Critical failure** | — | event, wherein the system (element) completely loses the capacity to perform the required function at the time when its operation is required. |
| **Minimum cut set** | — | least combination of events (for example, failures of elements, personnel errors) leading to implementation of system failure event. A minimal cut set is the logical product of its constituent basic events, and a package of minimal cut sets is the logical product of individual minimal cut sets. |
| **System (element) reliability** | — | А property of a system (element to keep, in the course of time within the established limits, the values of all parameters characterizing ability to perform the required functions in preset modes and conditions of use, and maintenance. |
|  |  | The reliability of a system (element) is a complex property, which may include no-failure operation, life duration, serviceability and storage property or a specific combination of these properties. The reliability of systems (elements) in this Safety Guide is considered only with respect to their no-failure operation. |
| **Operating time** | — | Duration or scope of system (element) operation. |
|  |  | The operating hours may be both a continuous quantity and an integer value (for example, number of operating cycles, number of start-ups). |
| **Time between failures** | — | Operating time of a system (element) from commencement of operation to the first failure. |
| **Independent failure** | — | Failure not caused by other failures and external impacts. |
| **Non-informative distribution** | — | A special type of prior distribution, which comprises the least possible amount of information on the reliability parameter in relation to that information which may be derived from operation. |
| **Specified reliability measure** | — | Reliability index, the value thereof is established by the regulatory documents and / or engineering (design) documentation. |
| **Generalized distribution** | — | Distribution of a random value, which describes variability of a reliability parameter with regard to a relatively wider population (parent population), as compared to the group to which such element belongs. |
| **Failure** | — | An event representing a violation of the availability of a system (element). |
| **Common failures** | — | A variety of common cause failures resulting from human errors in the design, construction and operation of facilities or from adverse environmental impacts. |
| **Common cause failures** | — | Failures of systems (elements) resulting from single failure or personnel error or external or internal effect or some other internal cause. |
| **Mean assessed failure rates** | — | ratio of expected mean number of failures of the recovered system (element) for the finite non-failure operating time to the value of this operating time. |
| **Personnel error** | — | A singular inadvertent incorrect action on equipment controls or a single omission of correct action; or a single inadvertent incorrect action during maintenance of NPP systems and elements. |
| **Assessed failure rates** | — | Ratio of expected mean number of failures of the recovered system (element) for the finite non-failure operating time to the value of this operating time. |
| **Damage** | — | An event violating the fail free condition while preserving its operable condition. |
| **Reliability index** | — | quantitative characteristic of one or several properties constituting reliability of system (element). |
|
| **Limit state** | — | A state of a system (element) at which its further operation is unacceptable or impractical, or recovery of its availability is impossible or impractical. |
|
| **Working condition of the system (element)** | — | A state of a system (element) under which the values of all parameters characterizing ability to perform the specified functions meet the requirements of the regulatory and (or) engineering (design) documentation. |
|
|
| **Reliability design index** | — | Reliability index, the value thereof is determined by calculation method. |
|
| **Repair** | — | Repair is the package of operations for restoring the good working order or operational integrity of the systems (elements) and recovery the resources of the systems, elements or their component parts. |
| **Maintainability** | — | A property of a system (element) allowing it to support and restore the operable condition by means of maintenance and repair. |
|
| **System** | — | A set of elements designed for performing the specified functions.  |
| **Screening (probabilities of personnel error)** | — | simplified (conservative) assessment of personnel actions performed under simplified models. |
|
|
| **Latent Failure** | — | failure not detected visually or standard method and control and diagnosis facilities but identified in maintenance or special methods of diagnosis. |
| **High-tecchnology complex** | — | aggregate of systems (elements) performing the sequence of process operations for implementing of an unified production process for the given algorithm characterizing by the fact that the reliability indices of performance of each process operation by the technology complex may be substantially different from each other, and the standardized reliability indices (functional safety) are stipulated for performing the requested functions by the technology complex in general. |
|
|
| **Average time to failure** | — | mathematical expectation of system (element) operating hours before first failure. |
|
| **Mean time between failures** | — | ratio of total hours in service of the recovered system (element) to the mathematical expectation of the number of its failures during these hours in service. |
|
| **Maintenance** | — | operation package or operation for maintaining system (element) operability. |
|
| **Process** | — | aggregate of process operations performed according to the given algorithm, each thereof may be implemented both by identical and different systems included in the scope of high-technology complex. |
|
| **Required function** | — | Function, the performance thereof is required by the NPP design from the system or from the systems totality The required functions are divided into safety functions and other functions. |
|
| **Error factor** | — | ratio 95% quantile of the random value to its median value. |
| **Functional safety** | — | reliability (no-failure operation) of the system (or high technology complex) in performing safety-related functions. |
|
| **Safety function** | — | specific objective and actions providing its achievement, directed at prevention and restriction of the consequences of accidents, which were unable to prevent by the normal operation systems. |
|
| **Safety-related function** | — | required function performed by the safety-related system (or totality of systems at least one of them is classified as safety-related) provide that the failure of this function shall lead to one of the following consequences:to failure of safety function;to NPP operational occurrences or to restrictions in the elimination of NPP operational occurrences if in this case the conditional probabilities of transition of the considered failure to severe accident shall be 10-6 or more;to exceedance of the stipulated values of the permitted radioactive discharges or releases, or permitted levels of contamination of NPP rooms. |
| **Elements** | — | equipment, instruments, pipelines, cables, building structures and others items ensuring performance of the prescribed functions independently or within the systems and considered in the design as structural units for reliability and safety analysis. |
| **Evident failure** | — | failure detected visually or standard methods or control facilities and diagnoss in the preparation of the system (element) to commissioning or in the process of its operation. |

Appendix No. 3
to the Safety guide in the use of atomic energy “Recommended procedure for NPP safety-related systems and elements reliability analysis, and their functions" approved by the order of the Federal Environmental, Industrial and Nuclear Supervision Service No. 26
dated January 28, 2015

**List of source ,
recommended for use in performing reliability analysis**

1. V.D. Raizer. Reliability theory in construction design. - Moscow: ASV, 1998.

2. V.V. Bolotin Predicting life of machines and constructions, - Moscow: Machine building, 1984.

3. G.W. Hannaman., F.J.Spurgin and J.R. Fragola. Systematic Human Action Relaibility Procedure (SHARP), NP-3583, Electric Power Research Institute, 1984.

4. A.D. Swain & H.E. Guttman, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Application, NUREG/CR-1278, US NRC, USA, 1983.

5. G.W. Hannaman et.al. Human Cognitive Reliability Model for PRA Analysis, NNUS-4531 (EPRI), Nuclear Utility Service Corp., 1984.

6. Procedure for Analysis of Common-Cause Failures in Probabilistic Safety Analysis NUREG/CR-5801, 1993.

7. IAEA-TECDOC-648, Procedures for Conducting Common Cause Failure analysis in probabilistic safety assessment, Safety Series, IAEA, 1992.

8. NUREG/CR-5485, Guidelines on Modeling CCFs in PSA. Prepared by A. Mosleh, D.M. Rasmuson and F.M. Marshall for USNRC, November 1998.

9. T. Teyer , M. Lipov, E. Nelson Software reliability. - Moscow. Mir, 1981

10. I.B. Shubinskiy Functional reliability of information systems. Analysis methods. - Ulyanovsk: Pechatny Dvor, 2012.

11. US Military Standard. MIL-STD-2629A Procedures for Performing Failure Mode, Effects and Criticality Analysis.

12. G.N. Cherkesov Reliability of software and hardware packages. - St. Petersburg: Peter, 2005

13. Alan Wood. Software Reliability Growth Model. Technical Report 96.1, 1996.

14. US Military Standard. MIL-STD-756A. Simulation and prediction of no-fail operation

15. International Standard. Software dependability through the software lifecycle processes. Application guide. IEC-61713.

16. Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments. NUREG/CR-6901.

17. GOSТ 27.002-89 Reliability of equipment. Basic concepts, terms and definitions.

Appendix No. 4
to the Safety guide in the use of atomic energy “Recommended procedure for NPP safety-related systems and elements reliability analysis, and their functions" approved by the order of the Federal Environmental, Industrial and Nuclear Supervision Service No. 26
dated January 28, 2015

**Recommended information gathering procedure about the system and determination of the
 modeling boundaries**

1. The sources for input data on the system for reliability analysis are project materials of NPP, specification of equipment, commissioning and testing documentation, operation experience, operating records, including technical specification of safe operation, operating manuals and system description manuals, lists of safeguards and interlocks, flow diagrams.

2. Gathered source data in documenting are supported by references to the sources of information.

3. The names of systems and its designation used in the design (operatioon) documentation are used in documenting the results of information gathering about the system.

4. It is recommended to set the limits for system modelling in order to take into account all elements significant from system reliability point of view on the hand, and on the other hand to prevent repeated consideration of one and the same elements within different systems.

5. It is recommended to set boundaries between systems in line with the following rules:

1) For hydraulic and pneumatic system the boundaries as per operating meduim lay:

on pressure piping - at the point of junction of the pressure piping of the given system with the pipeline or vessel of other system (the one the medium is delivered to);

on pipelines of medium feeding from supporting systems - at the point of insertion into suction pipeline of the given system of supporting system's pressure piping;

Heat exchangers with the fluid coolant fed from supporting systems are incorporated into the main system. In such a case, if there are independent shut-off valves on pipeline for feeding fluid coolant to heat exchanges, these pipelines are incorporated into the main system together with these valves;

2) For electricity supply systems, the boundary of electricity supply system with the consumers is set at the point of connection of power bus inlet to circuit breaker of the consumer. In the determination of system boundaries at the point of electric power supply to electrically driven elements (valves, pumps, compressors etc.), it is recommended to take into account electric motor (solenoid) and a breaker within the consuming element;

3) Boundaries between power supply systems are set at the place of connection of the current lead to the section;

4) Safety-related control system starts with transducers (primary instruments) and finishes with output terminals used for control of element's breaker drive.

5) The modeling boundaries of the system are established as a rule in accordance with the system description in the design engineering documentation.

6. All elements of the system, failure thereof or unavailability are capable of leading to failure of this system or to reliability degradation of its functioning in performing the required function.

7. The following system elements shall be included in the scope of its simulation:

thermal and mechanical equipment: all elements having moving parts (electrical pumps; turbine-driven pumps, fans, compressors; valves including check valves etc.); water-jet pumps, ejectors and injectors; tanks; pressurized vessels (including accumulators, receivers); heat exchangers; piping in which the fluid is supplied in performing the required functions to a consumer, and piping, failure thereof shall lead to disturbance of the system's performance of the required functions; filters, including filtering structures of sumps;

electrical equipment, APCS equipment: generators; diesel-generators; storage batteries; inverters; reversible engine generator sets; AC/DC converters; electrical cabinets, sections and assemblies; transformers, including autotransformers; automatic circuit-breakers, disconnectors, keys (switchgears), and electronic switching apparatus; electronic I&C devices (including programmable devices); relay; instrument transformers (current and voltage); primary instruments (sensors); secondary instruments; motors (for the case when they are part of other elements); solenoids (stepwise actuators).

The above list of elements is not exhaustive, and confirmed in respect to the system analyzed.

8. Boundaries of elements are recommended to be set in such a way as to, as far as possible, facilitate determination of their reliability indices on the basis of available specific and generalized data. The boundaries shall be set in accordance with the description of the elements in the engineering design documentation.

9. The boundaries of elements are recommended to be set in such a way that all failure modes which may affect the ability of the system to perform a required function are considered in building the system reliability model.

10. The system boundaries and boundaries of the simulated elements in the reliability analysis document are illustrated using a simplified process diagram (skeleton diagram).

11. Information is gathered and documented about all NPP normal operation conditions as well as the conditions characterizing NPP anticipated operational occurrence under which the system is required to perform its functions.

12. Information is gathered and documented about the master elements of the system in the following scope:

type and operational designation of the element;

basic technical specifications of the element;

element's state in different normal operation modes (anticipated operational occurrences);

the presence of remote (manual) or automated control of the element;

location of the element;

element's demand for power supply, cooling, air conditioning and ventilation, lubrication from external systems and operation of other auxiliary systems;

extreme values of parameters, the operation of the element depends on.

limit states criteria

13. Information is gathered and documented on the controlled variables of the system including the measured variables, list of system protections and interlocks.

14. Information is gathered and documented on the relations of the system being analyzed with other systems required to ensure its functional capability and depend on it themselves. The following relations are subject to accounting:

power supply relations (electricity supply, compressed air supply, fuel supply);

relations regarding cooling of active elements (by water from different circuits, by air and oil);

relations regarding ventilation of the rooms where the system elements are located;

relations with instrumentation and control systems (that are not included in the system under question) where control signals for system elements are generated (including equipment actuation and shutdown signals, switch-on/switch-off and valves repositioning prohibit);

relations stipulated by dependence on upper-level software;

other relations which can include other dependences between the systems (for example, process relations regarding handled medium, lubricant supply etc.).

The documenting of information on the relations with other systems (elements) is supported by a dependence table (matrix) where the relations of these systems (elements) with the systems (elements) of the analyzed system are shown.

15. Information on NPP staff activities which can affect operation of the system shall be gathered and documented.

16. Information about conditions of safe operation formulated for the system shall be gathered and documented. This information is used in order to spot the opportunity to perform this or that equipment operating mode and system configuration.

17. Information about the maintenance procedure, system testing, in particular the data on frequency and scope of operability check and scheduled maintenance of the system or its elements shall be collected and documented.

Appendix No. 5
to the Safety guide in the use of atomic energy “Recommended procedure for NPP safety-related systems and elements reliability analysis, and their functions" approved by the order of the Federal Environmental, Industrial and Nuclear Supervision Service No. 26
dated January 28, 2015

**Recommended accounting procedure of personnel influence**

1. A list of actions, which may impact the performance of the required functions of the analyzed system for accounting the influence of personnel shall be formed, simulation method of these actions shall be described and probabilities of the relevant personnel errors (error-free actions) shall be assessed.

2. The NPP personnel influence on reliability of performance of required function by the system shall be made considering the assumption that the personnel performs its actions in compliance with the requirements of the operation documentation.

3. The actions of personnel are divided into the following categories in forming the list of actions:

actions in confirming the operable state (including during the tests), maintenance or repair of the system (actions before performance of the required function by the system);

personnel actions in the process of the system performing the required function leading to failure of the system or its elements;

actions during disturbances of norms system functioning (corrective actions).

The following types of personnel errors are considered: execution errors (selection errors);

delayed execution errors (delayed detection, diagnosis);

non-execution errors (omission of action).

4. The personnel actions related to system maintenance (of its elements) which may lead to system unavailability to perform the required functions.

5. The probabilities of personnel error shall be assessed by applying special methods of personnel reliability analysis.

6. In determining the probability of personnel errors the actions of personnel are classified by one of the types of personnel actions (behavior):

based on skill;

based on rules;

based on knowledge.

7. The following factors influencing the probability of personnel making mistake:

time factor (time, which the NPP personnel has for performing the requested actions). The time factor is characterized by the reserve of time which the personnel has for taking decision on performing actions and time required for performing the requested actions.

simplicity/complexity of requested actions, degree of detail of the requested actions in the operation documentation;

training (experience) of personnel for actions in similar situations;

maturity of cooperation and quality of information exchange between different categories of NPP personnel involved in performing the required actions;

possibility of control and reinstatement (availability of possibility to verify the correctness of input command (action performance), potential to repeat the action,, perform the operation by another method);

stress level;

degree of the environmental conditions non-conformance to the normal conditions, whereby the required actions are performed

quality of man-machine interface (for example, convenience of reading information from indicating instruments, operations with control devices);

load on personnel (discrete (step by step) operations not requiring operational interference in the process flow, or dynamic operations requiring high concentration of attention);

dependencies in the personnel actions (for example, performing wrong actions following false reading of information from the control instrumentation).

8. The dependencies in the actions of personnel affecting personnel reliability are taken into account, including:

dependencies between the actions performed by the same operator under one task;

dependencies inside the personnel group participating in the resolution of one task including the control of its executionl

dependencies between different task resolved by the personnel in the system management process.

9. Personnel influence shall be accounted in four stages successively.

Stage 1. Analysis of initial information:

determination of the list of personnel actions (errors) impacting the performance reliability of required information analyzed by the system;

analysis of engineering design and operation documentation;

analysis of the performance conditions of personnel actions (errors);

survey of personnel - direct executors of the analyzed actions (errors) (where appropriate).

Stage 2 Sampling analysis:

personnel reliability analysis in maintenance of system (elements);

personnel reliability analysis in system operation;

reliability analysis of the performance of corrective actions by the personnel on occurrence of system operation disturbances;

selection of the most important actions for detailed analysis (following preliminary quantitative analysis of system reliability).

Stage 3 Detailed analysis of personnel reliability (performed if required):

determination of the sequence of actions in performance of each task and critical steps;

analysis of personnel functions at each step;

model building of personnel actions;

analysis of dependencies in personnel actions;

determination of prelimiary (nominal) values of the probabilities of errors (error-free actions) of personnel;

assessment of the relative influence of behavior forming factors;

assessment of restoration factor and dependency levels;

determination of the reliability indices of personnel.

Stage 4. Assessment of uncertainties of the probability of personnel errors.

10. Only sampling analysis of personnel reliability shall be allowed to perform in the preliminary reliability analysis of the system when engineering and diagrammatic elaboration of the equipment is not available, only sampling analysis of personnel reliability shall be allowed to perform. Moreover, the personnel actions for preventing and terminating the potential functional disturbances of the system (corrective actions) may not be considered.

11. Screening assessments of the personnel actions are used for the sampling analysis.

Data on assessments of the probabilities of erroneous actions of personnel in maintenance of the systems and in the operation process recommended for sampling analysis are presented in the table 1 of this Appendix.

**Table 1**

**The probabilities of erroneous actions of personnel during maintenance of the system, as well as in the operation process (use of system for direct purpose) [31**

|  |  |
| --- | --- |
| **Type of actions** | **Type of behavior** |
| **Actions based on skills** | **Action based on rules** | **Actions based on knowledge** |
| Testing (tests) | 2∙10-3 | 2∙10-2 | — |
| Maintenance | 1∙10-2 | 1∙10-2 | 5∙10-2 |
| Operation (use for designated purpose) | 3∙10-3 | 3∙10-2 | 1∙10-1 |

The values presented in the table 1 of this Appendix may also be used for assessment of the probabilities of personnel errors when performing actions causing operational occurrences of the NPP during manual performance of system (element) management operations.

12. The recommended assessment of human erroneous actions during breaches of system functioning are presented in table 2 of this appendix, which consider the factors affecting human reliabilit and can be used for the screening analysis.

**Table 2**

**The probabilities of erroneous actions of personnel during breaches of system function [31**

|  |  |
| --- | --- |
| **Available time** | **Type of behavior** |
| **Actions based on skills** | **Action based on rules** | **Actions based on knowledge** |
| Decisions taken |
| Less than 5 minutes | 0.1 | 0.5 | 1.0 |
| From 5 minutes to 1 hour | 1∙10-3 | 3∙10-2 | 0.3 |
| More than 1 hour | 3∙10-4 | 3∙10-3 | 1∙10-2 |
| Enforcement of decision taken |
| - | 3∙10-3 | 3∙10-2 | 0.3 |

13. The following ratios are used for assessment of the probability of non-performance of the specific task which includes a set of personnel actions

If the non-performance of any of the set of actions related to the considered task shall lead to its non-performance (improper performance), the resulting probability of human error (CS) (for the task overall) shall be determined according to the formula:

, (1)

where: *qi* - error probability when executing the *i*-th action.

If the non-execution of the task is the consequence of simultaneous non-performance of each set of actions, the probability of human error is determined according to the formula:

(2)

14. The set of human actions which has significant impact on the system reliability indicators shall be determined based on the screening analysis and results of preliminary quantitative analysis. Then each selected set of human actions shall be divided into elementary actions and potential errors are analyzed when performing these actions, for example:

incorrest diagnostics of the situation;

non-fulfilment of the instructions for specific actions;

false reading of the device readings;

false choice of the equipment control elements.

The consequences of their non-execution (incorrect execution) from the point of view of influence on the performance of task overall shall be determined for each of the elementary actions.

15. The preliminary (nominal) values of the error probabilities, which do not consider the factors formulating the personnel behavior, control and restoration (correction) factors of errors shall be assessed for each of the above defined elementary actions of personnel. The values presented in the table 3 of this appendix shall be used for assessment of te preliminary values of the probabilities of erroneous actions of the personnel related to decision making.

**Table 3**

**Preliminary (nominal) values of the probabilities of erroneous actions of personnel related to decision making depending on the available time [4]**

|  |  |  |  |
| --- | --- | --- | --- |
| **Time available for decision making, min.** | **Error probability on diagnostics of single event** | **Error probability on diagnostics of second event** | **Error factor** |
| 1 | 1.0 | - | - |
| 10 | 0.1 | 1.0 | 5 |
| 20 | 0.01 | 0.5 | 10 |
| 30 | 0.001 | 0.1 | 10 |
| 60 | 0.0001 | 0.001 | 10 |
| 1500 (one day) | 0.00001 | 0.0001 | 30 |

Reference data for the preliminary (nominal) values of the probabilities of human erroneous actions during direct execution of the actions (i.e. erroneous actions not related to taking decision) are presented in the table No. 4, 5, 6 of this appendix.

**Table 4**

**Preliminary (nominal) values of the personnel not related to decision making**

|  |  |  |
| --- | --- | --- |
| **Characteristic of instruction and situation** | **Personnel error probability** | **Error factor** |
| Instructions with provision mark on execution are used correctly: |
| short list (< 10 points) | 0.001 | 3 |
| long list (>10 points) | 0.003 | 3 |
| Instructions without mark of enforcement: |
| short list (< 10 points) | 0.003 | 3 |
| long list (>10 points) | 0.01 | 3 |
| Instructions are available and must be used, but are not used |
|  | 0.05 | 5 |

**Table 5**

**Preliminary (nominal) values of the personnel not related to decision making**

|  |  |  |
| --- | --- | --- |
| Indicating instrument or performed task | Error probability | Error factor |
| Analog instrument | 0.003 | 3 |
| Read number (4 digits or less) | 0.001 | 3 |
| Recorder of diagrams | 0.006 | 3 |
| Printer with large number of parameters | 0.05 | 5 |
| Schedules | 0.01 | 3 |
| Taking of readings with indicator lamps used as indicating device | 0.001 | 3 |
| Determination of the fact that the device from which information is read is faulty if there is not indication of fault | 0.1 | 5 |
| Record of readings: number of digits or letters which is required to write: |
| three or less | small to negligible |
| more than three | 0.001 (for a symbol) | 3 |
| Simple arithmetic calculations with calculator or without | 0.01 | 3 |
| Determination of miscalculations | 0.05 | 5 |

**Table 6**

**Preliminary (nominal) values of the personnel not related to decision making**

|  |  |  |
| --- | --- | --- |
| Potential errors | Personnel error probability | Error factor |
| Incorrect choice of control device on the panel from group of control devices, which: |
| differ only by marking | 0.003 | 3 |
| divided into clearly limited functional groups | 0.001 | 3 |
| are part of the visual mnemo circuit | 0.005 | 10 |

16. The factors exerting influence on the personnel liability shall include training (qualification) level of the personnel, load level (discreteness of performed operations, task dynamic), personnel interaction environment, stress level Based on the combination of specified factors the coefficient of behavior forming factors shall be estimated as the factor to the preliminary (nominal) estimates of the personnel error probabilities. Reference data for accounting the behavior forming factors (Kfb are available in the sources listed in the Appendix 3 to this Safety Guide).The conditional probability values (Fc/p) are contained in the literature sources of the fact that the error shall not be monitored and restored depending on the condition of monitoring, presence of a second operator or controller, time margin, personnel qualification, stress level.

17. Knowing the time required for performing the tasks (actions) by the personnel Tnecess*.*, the time available Tavail*.* and using the dependency data one can get the personnel error probability. The dependency of personnel error from standardized time is presented in the fig.1 of this appendix and it is determined using the following formula:

(3)



Normalized time, Tn

Error probability

Fig. 1. Dependencies of the human error probability from the available time and type of behavior (A - actions, based on skills, B - actions based on rules, C - actions based on knowledge)

18. In those cases when any of the elementary error actions is critical for the performance of task overall, probability of errorneous non-performance of task is determined according to formula (1) of this appendix. Besides in the probability estimates of personnel error *qi* the nominal values shall be corrected considering the behavior forming factors (coefficient Kbf) and factors for control restoration - correction of errors, with probability of non-performance Fc/R considering the dependency of the probabilities of errors between diverse actions performed by a team of operators (or by one operator):

|  |  |  |
| --- | --- | --- |
| $$q\_{i}=q\_{i}^{ном}∙К\_{фп}∙F\_{к/в}$$ |  | (4) |

In individual cases the resulting probability of not performing the task overall shall be determined by the ration (2) of this appendix as the multiplication of the probabilities of individual erroneous actions, when only a combination of all errors shall lead to non-performance of the task. In more branched dependencies the performance of task from elementary actions the calculation of the resulting personnel reliability index shall be made in accordance with the structure model (for example, event tree) specially developed for analysis of personnel reliability in the considered task in simutaneous use of the ratios (1) and (2) of this appendix.

19. The uncertainty boundaries for the probabilities of elementary erroneous actions of personnel shall be given using the error factor for the index (ratio of 95% quantile to the distribution median). The following values of the error factor shall be used with respect to screening values of personnel error probabilities:

stepwise actions (during normal conditions):

1) estimated probability < 0.001 10

2) estimated probability 0.001 - 0.01 3

3) estimated probability > 0.01 5

dynamic actions (in stressed accident conditions):

1) estimated probability < 0.001 10

2) estimated probability 0.001 - 0.1 5

3) estimated probability > 0.1 3

Recommendations for choice of uncertainty boundaries for estimated probabilities of human errors are given in the table 7 of this appendix.

**Table 7**

**Recommendations for choice of uncertainty boundaries for estimated probabilities of personnel error**

|  |  |
| --- | --- |
| **Task at hand** | **Error factor** |
| Operator's performance of stepwise operations in ordinary conditions (for example, verification, maintenance or calibration); stress level - optimal |
| Estimated probability < 0.001 | 10 |
| Estimated probability 0.001 - 0.01 | 3 |
| Estimated probability > 0.01 | 5 |
| Execution of step-wise operation in abnormal conditions; stress level relatively high |
| Estimated probability < 0.001 | 10 |
| Estimated probability > 0.001 | 5 |
| Relatively dynamic operator interface with the display system in ordinary display system in ordinary conditions |
| Estimated probability < 0.001 | 10 |
| Estimated probability ≥0.001 | 5 |
| Relatively dynamic operator interface with the display system in abnormal conditions; stress level is relatively high | 10 |
| Any task performed in extremely high level of stress, for example, ambiguous safety state of the NPP, incorrect previous decision making and lack of time | 5 |

Appendix No. 6
to the Safety guide in the use of atomic energy “Recommended procedure for NPP safety-related systems and elements reliability analysis, and their functions" approved by the order of the Federal Environmental, Industrial and Nuclear Supervision Service No. 26
dated January 28, 2015

**Recommended procedure for determining the types of failures and quantitative assessment of reliability indices of NPP elements**

1. Determination of element failure types Thermal and mechanical equipment

Basic types of failures of thermo-mechanical elements are presented in the table No.1 of this Appendix.

Failure classification of mechanical elements is given in the ratio of both critical failures and damages. This classification may vary depending on certain conditions. Examples presented below mostly provide general information on the subject.

Table 1

Types of failures of thermo-mechanical elements

| Elements | Critical failures | Non-critical failures |
| --- | --- | --- |
| Pumps | Failures to startFailure to restartFailure during operation | Insignificant leakNoise, vibration |
| Shut-off valve | Failure to open/closeFailure to reopen/closeFalse reposition | Control and indication failure Insignificant leak |
| Control valves | Failure to open/closeFalse reposition.Failure for adjustment function | Control and indication failure Insignificant leak |
| Check valves | Failure to open/closeInterior leak | Control and indication failure Insignificant leak |
| Safety and steam relief valves | False openingFailure to openFailure to reclose | Control and indication failureInsignificant leak |
| Absorber rods and drives | False insertion of the rodFailure to insert rodFalse reposition of rodFalse removal of rod | Insignificant leak |
| Heat exchangers | Large-scale leakageCloggingAir inleakage | Insignificant leak |
| Tanks | Large-scale leakage | Insignificant leak |

Electrical equipment.

The critical failures of electrical equipment shall include:

1) Diesel-generators:

Failure to start;

Failure during operation.

2) Storage batteries:

loss of container;

Short circuit

3) inverters, chargers:

power supply function failure

4) electrical sections (assemblies)

false circuit rupture;

short-circuit;

ground fault

5) circuit-breakers, relay, electric contactors:

failure to open the circuit;

failure to close the circuit;

spurious actuation.

In general case the classification of failure types shall consider the specific impact of each failure type on capability of the analyzed system to perform the required function, as well as the conditions of their detection and operability recovery.

2. Determination of reliability indicators of system elements.

Failure intensity assessment

The assessment of the intensity of failures to respond to a request shall be made according to the following formula:

|  |  |  |
| --- | --- | --- |
| $$λ=\frac{r}{T},$$ |  | (1) |

where:

r - recorded number of failures of the considered type (the formula is recommended to use at r≥10);

*T* - accumulated operating time, for which r failures were recorded.

Assessment of the probability of failure to respond to a request.

The assessment of the probability of failure to respond to a request shall be made according to the following formula:

|  |  |  |
| --- | --- | --- |
| $$p=\frac{r}{D},$$ |  | (2) |

where:

*r* - recorded number of failures to respond to a request of the considered type;

*D* - total quantity of requirements for which the *r* failures were recorded.

Assessment of the frequency and average duration of trial run, maintenance and repair.

The frequency and average duration of trial run, maintenance and repair shall be assessed for individual elements or system channels. The frequency of trial run, maintenance (both scheduled and unscheduled) and repair shall be determined according to the following formula

|  |  |  |
| --- | --- | --- |
| $$λ\_{т/м}=\frac{f\_{т/м}}{Т},$$ |  | (3) |

where:

*f*т/м - number of trial runs of services and repairs performed for this element;

*T* - total system operation time during which *f*t/m trial runs, services and repairs were made.

Mean duration of the trial runs, maintenance or repair shall be determined according to the formula

|  |  |  |
| --- | --- | --- |
| $$\overbar{τ}\_{т/м}=\frac{\sum\_{i=1}^{N}T\_{i}}{f\_{т/м}},$$ |  | (4) |

where:

*Ti* - duration *i*-th trial run, maintenance or repair for this element or system channel;

*N* - number of different kinds of trial runs, maintenances or repairs.

The assessment of unavailability due to trial run, maintenance or repairs for the elememt or system channel shall be made according to the following formula:

|  |  |  |
| --- | --- | --- |
| $$\overbar{Q}\_{т/м}=λ\_{т/м}∙\overbar{τ}\_{т/м}$$ |  | (5) |

If there are no specific data for assessment of the equipment reliability parameters (intensity of failures or probability of failure to respond to request) the most preferable is to use the data with similar NPP. The potential differences in determination of the boundaries and types of failures for the considered types of elements are considered at that. The use of other sources of summarized data or expert assessments are also assumed.

If failures are not observed for the considered type of elements, then for determining the reliability indicators of the element (intensity of failures or probability of failure of the element to respond to the request) Bayesian assessment shall be made using summarized data according to the following algorithm.

Inconclusive distribution is used on limited quantity or lack of summarized data as apriori. In this cases assessment of the intensity of element failures shall be determined according to the formula:

|  |  |  |
| --- | --- | --- |
| $$λ=\frac{2r+1}{2T}$$ |  | (6) |

On inconclusive apriori distribution of probability assessment of failure to respond to request shall be determined using the formula:

|  |  |  |
| --- | --- | --- |
| $$p=\frac{r+0,5}{D+1}$$ |  | (7) |

On choice as apriori lognormal distribution for performing Bayesian assessment the standard deviation of lognormal distribution of summarized data shall be determined as follows:

|  |  |  |
| --- | --- | --- |
| $$σ=\frac{ln⁡(ef)}{z\_{.95}},$$ |  | (8) |

where:

σ - lognormal distribution parameter;

ef - error factor of lognormal distribution of summarized data;

*z.95* - 95-percentile standardized normal distribution (≈1.645).

Then the dispersion of summarized data distribution shall be determined:

|  |  |
| --- | --- |
| $$Var=\overbar{x^{2}}\left(e^{σ^{2}}-1\right),$$ | (9) |

where:

*x* - mean value of summarized parameter.

Further the parameters of distribution of α and β shall be determined*.*

If the Bayesian estimation is made for the intensity of failures, the parameters α and β are gamma distribution parameters:

|  |  |  |
| --- | --- | --- |
| $$α=\frac{\overbar{x}^{2}}{Var}$$ |  | (10) |
| $$β=\frac{\overbar{x}}{Var}$$ |  | (11) |

If the Bayesian estimation is made for the probability of failures to respond to request, then α and β are beta-distribution parameters:

|  |  |  |
| --- | --- | --- |
| $$α=\frac{\overbar{x}^{2}(1-\overbar{x})}{Var}-\overbar{x}$$ |  | (12) |
| $$β=\frac{\overbar{x}(1-\overbar{x})^{2}}{Var}-1+\overbar{x}$$ |  | (13) |

Then the Bayesian modification is made by calculating the parameters of aposterior distribution of α' and β' according to the following formulae:

for intensities of failures:

|  |  |  |
| --- | --- | --- |
| $$α^{'}=α+f\_{Т},$$ |  | (14) |
| $$β^{'}=β+Т,$$ |  | (15) |

where:

fT - total number of failures recorded for this type of elements;

T - full operating hours for this type of elements, h

for probabilities of failures to respond to the request:

|  |  |  |
| --- | --- | --- |
| $$α^{'}=α+f\_{D},$$ |  | (16) |
| $$β^{'}=β+D,$$ |  | (17) |

where:

fD - number of failures to respond to the request, recorded for this type of elements;

D - total number of requirements for actuation recorded for this type of elements.

Then the mean value and dispersion of the aposterior distribution is determined:

for intensity of failures:

|  |  |  |
| --- | --- | --- |
| $$\overbar{x'}=\frac{α'}{β'}$$ |  | (18) |
| $$\overbar{Var'}=\frac{α'}{β'^{2}}$$ |  | (19) |

for probability of failure to respond to the request:

|  |  |  |
| --- | --- | --- |
| $$\overbar{x'}=\frac{α'}{α^{'}+β'}$$ |  | (20) |
| $$Var^{'}=\frac{α'β'}{(α^{'}+β^{'}+1)(α^{'}+β')^{2}}$$ |  | (21) |

where:

*x* - mean aposterior;

*Var'* - aposterior dispersion.

The error factor *ef'*' for aposterior distribution is determined according to the following formula:

|  |  |  |
| --- | --- | --- |
| $$ef^{'}=exp\left[z\_{.95}\sqrt{ln\left(1+\frac{Var'}{\overbar{x'}^{2}}\right)}\right]$$ |  | (22) |

Appendix No. 7
to the Safety guide in the use of atomic energy “Recommended procedure for NPP safety-related systems and elements reliability analysis, and their functions" approved by the order of the Federal Environmental, Industrial and Nuclear Supervision Service

No. 26 dated January 28, 2015

**Recommended procedure for accounting common cause failures**

1. The common cause failures of systems (elements) following dependencies from supporting and managing systems are considered by including the supporting and managing systems in the structure logic model of the analyzed system (in accordance with the recommended procedure presented in the chapter IV of this Safety Guide).

2. Common cause failures following human errors are accounted by inclusion of the analyzed human error system in the structural and logic model, considered in the procedure, stipulated in Appendix No. 5 to this Safety Guide.

4. Common-cause failures following external natural and human-induced impacts on NPP and following the impacts occurring during operational occurrences including the accidents are considered through accounting in the structural and logic model of the analyzed system of occurrence of dependent failures of NPP elements due to external impacts of natural and human-induced nature or internal impacts occurring during operational occurrences, including accidents.

5. Apart from the types specified in the items 2-4 of this appendix

of common cause failures in the system reliability model GF are also considered. GF characterizes the measure of ignorance of potential reasons of dependent failures and are referred to residual dependent failures, i.e. to failures not simulated in the structural-logical model of the system directly, but determined using mathematical models, compensating reduced assessment of the probability of joint failure of several mutually redundant elements (or system channels) by functions performed.

6. The basic task of GF modelling is the accounting of the potential correlation of the flows of element failures being duplicating for the require system functions. GF accounting allows eliminate over-optimism during probability assessment of performing functions by the systems having channel and/or equipment redundancy.

7. Accounting of GF in the system reliability model is made in five stages.

Stage 1. Determination of the groups of elements of the analyzed system subject to GF and determination of the corresponding types of failures.

Stage 2 Choice of GF model and data analysis. The mathematical model allowing calculate the probability of GF for various number of elements is taken at this stage based on the number of elements forming the GF group and having data on operation experience. The use of conservative GF models and summarized data on parameters of models shall be allowed at the given stage

Stage 3 Performance of quantitative analysis of system reliability and determination of GF contribution to system failure probability on its performance of the required function. The stage 5 bypassing the stage 4 is performed on identification of low degree of GF impact on the system failure probability.

Stage 4. Clarification of GF, correction of the GF models and elaboration of the parameters of GF models for rectification of conservatism of analysis.

Stage 5 Documentation of GF analysis results

8. Formation of element groups susceptible to common failures is the most important part of the common failure analysis as unreasonable exclusion of elements from the common failure group can result in significant under-estimation of the system failure probability during execution of the required function. The common failure groups are formed in order to define all elements potentially susceptible to common failures in such a way so that to minimize any potential subjectivity. This aim is achieved by identification of all system elements potentially susceptible to common failures.

9. A common general failure group shall include elements corresponding simultaneously to the criteria listed below (three mandatory criteria and at least one optional one):

Criterion 1 (mandatory). All elements of a common failure group belong to one and the same type of equipment and the structural and logical system reliability model includes the same types of failures for all elements of the group;

criterion 2 (mandatory). A single failure of any element constituting the common failure group does not result in the system failure to execute all required functions;

criterion 3 (mandatory). A common failure of all elements constituting the common failure group results in the system failure to execute any required function;

criterion 4 (optional). Components included into the common failure group have a common manufacturer or similar brand marks (types) of various manufacturers (similarity of design);

criterion 5 (optional). Elements included into the common failure group are exposed to identical physical factors in the course of various accident scenarios: temperature, pressure, humidity, vibration, radiation, electromagnetic emissions, etc. (not necessarily all of them) (similarity of operating conditions);

criterion 6 (optional). Elements included into the common failure group have identical maintenance, repair and testing procedures (similarity of service).

10. When forming common failure groups it is recommended to take into consideration potential common failures for the elements belonging to different channels of the system where it is practicable.

11. One of the following models are used for selected GF groups for determining the probability of GF:

β-factor model and its modification [6];

Multiple Greek Letter model [6];

α-factor model [7, 6, 8];

basic parameter model [7, 6];

binomial model [6].

12. β-factor model

This model is the most conservative model and assumes that all the elements included in the GF group fail due to general reason with probability Pоов, equal to

Роов= β∙Р, (1)

where:

β - failure probability of all elements in the GF group on the condition that failure of one element took place;

P - failure probability of one element from the GF group obtained based on the experience of operation and statistics of all element failures;

Respectively, probability of independent failure Pн of any element in the GF group calculated according to the formula:

Рн = (1-β) Р (2)

The values of β in the range β ≈ 0.07 - 0.1 shall be taken in the absence of specific data.

13. α -factor model

This model takes into account the partial and complete failures of the GF group elements and is recommended as the preferable model for assessment of the probability of GF events.

(3)

,

where:

*αк-* probability that in the GF event exactly *k* elements from the group *m*  shall fail (α-factor);

*PT* - failure probability of one element from the GF group obtained based on the experience of operation and statistics of all element failures;

- number of combinations of *k* elements from *m*

The formula (3) of this appendix is designed for calculations of the GF probabilities if the verification of equipment performance included in the GF group is made simultaneously (without time displacement). If the elements included in the GF group are verified with time displacement, then it is recommended to use the formula (4) of this appendix.

(4)

If there are no specific data it is recommended to use the values of α-factors given in the table 1 (for failures on demand) and table 2 (for failures during operation) [8] of this appendix.

**Table 1**

**Recommended values of α-factors for failures in operation**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **GF group size** | **α1** | **α2** | **α3** | **α4** | **αt** |
| 2 | 0.95 | 0.05 | - | - | 1.05 |
| 3 | 0.95 | 0.04 | 0.01 | - | 1.06 |
| 4 | 0.95 | 0.035 | 0.01 | 0.005 | 1.07 |
| over 4 | 0.995 | - | - | 0.005 | - |

**Table 2**

**Recommended values of α-factors for failures in operation**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **GF group size** | **α1** | **α2** | **α3** | **α4** | **αt** |
| 2 | 0.975 | 0.025 | - | - | 1.025 |
| 3 | 0.975 | 0.02 | 0.005 | - | 1.03 |
| 4 | 0.975 | 0.0175 | 0.005 | 0.0025 | 1.035 |
| over 4 | 0.9975 | - | - | 0.0025 | - |

14. The use of the α-factor model with realistic values of α-factors (i.e. with values of α-factors considering when possible, having specific reliability data of elements) shall be recommended for the GF groups making significant contribution to the assessment of system reliability indicators. The contribution of GF group in the assessment of the system reliability indicators is deemed significant if the system reliability factor considering the probability of GF occurrence of the elements of the considered group differs from the reliability factor calculated in the assumption of GF impossibility of the specified elements by more than 10%.

15. GF is included the structural logic of the analyzed system by highlighting (indicating) the set of relevant basis GF events. An example of the inclusion of GF events in the logical and probabilistic model of the system is shown in this appendix.

16. On documentation of the results of GF accounting th justification of the executed formation of GF groups and the accepted GF models and their parameters are presented.

17. An example of the inclusion of elements in the GF group is show in the table 3 of this appendix (in the example of system valves, schematically shown in the fig. 2 and fig. 3 of this appendix, differing by one or several attributes).



Common cause failure of elements 1, 2 and 3

Common cause failure of elements 1 and 3

Common cause failure of elements 1 and 2

New logical operator "OR" No. 1

Failure of element 1

Failure of element 1

New logical operator "OR" No. 2



Common cause failure of elements 1 and 2

Common cause failure of elements 2 and 3

Common cause failure of elements 1, 2 and 3

Failure of element 2

Failure of element 2



New logical operator "OR" No. 3

Common cause failure of elements 1 and 3

Common cause failure of elements 2 and 3

Common cause failure of elements 1, 2 and 3

Failure of element 3

Failure of element 3

Fig. 1 Example of CF inclusion in the system model (failure tree)

**Table 3**

**Example of CF inclusion in CF group**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Description of elements** | **Number of elements** | **Failure mode**  | **Interval between the tests** | **Additional terms and conditions** | **Recommended model** | **Parameters of GF model** | **Specified parameters of GF or changes of GF model** |
| The system comprising of six redundant valves (a) or partially redundant (b) (fig. 2) a)b) | 6 (Dn 100) |  | Once a month | Manufactured by one manufacturer Are in normal conditions in standby mode. | α-factor | Based on cumulative data [8] | Not required |
| Same | Same | Manufactured by different manufacturers. Are in normal conditions in standby mode. | Same | Same | If the value of GF is high in the system reliability indicators it is possible to specify the model parameters for reducing the weight of GF due to: |
| b) | Same | 3 - once a month3 - once a year | Manufactured by one manufacturer Are in normal conditions in standby mode. | α-factor The maximum interval between the trial runs (once a year) | Same | If the value of GF is high in the system reliability indicators it is possible to specify the model parameters for reducing the weight of GF due to different test intervals |
|  | 3(Dn 100)3(Dn 150) | Same | Same | Same | Same | If the value of GF is high in the system reliability indicators it is possible to specify the model parameters for reducing the weight of GF due to:different test intervals;different diameters |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Description of elements** | **Number of elements** | **Failure mode**  | **Interval between the tests** | **Additional terms and conditions** | **Recommended model** | **Parameters of GF model** | **Specified parameters of GF or changes of GF model** |
| System including 12 valves, each partially operating on standby basis (fig. 3) | 12 (Dn 100) | Failure to change position on demand | Once a month | Manufactured by one manufacturer Are in normal conditions in standby mode. | β-factor | β= 0.1 | At high GF significance in the reliability indicators of the system the specification of the model parameters for reducing the weight of GF is possible. The parameters shall be specified using data on operation experience of a similar equipment at the power units of the Russian NPP.Similarly it is allowed to use the model α-factor with assignment of values to the parameters α5, α6, α7 and α8 accepted for α4 |
| 6 - once a year6 - once a year | β= 0.07 | If the GF is of high significance in the system reliability indicators it is possible to:specify the model parameters for reducing the weight of GF. The parameters shall be specified using data on operation experience of a similar equipment at the power units of the Russian NPP;use of other GF models (for example, unified partial method of β-factor)Similarly it is allowed to use the model α-factor with assignment of values α5, α6, α7 and α8 to the parameters, accepted for α4 |

Appendix No. 8
to the Safety guide in the use of atomic energy “Recommended procedure for NPP safety-related systems and elements reliability analysis, and their functions" approved by the order of the Federal Environmental, Industrial and Nuclear Supervision Service

No. 26 dated January 28, 2015

**Scope of report for reliability analysis of NPP systems**

The results of reliability analysis of NPP systems are presented in accordance with the structure given below.

1. System description and designation

1.1. System description

1.2. System designation in diagrams and operational documentation of NPP.

1.3. System code used in the structural logical model

2. Description of the system.

2.1. System purpose

2.2. System process flow diagram

2.3. Brief characteristic and system composite.

2.3.1. Brief characteristic and system

2.3.2. Description of system components

2.3.3. Support and control systems

2.4. System operation under normal operation conditions of NPP

2.5. Functioning of the system in case of any abnormal operation of NPP, including accidents;

2.6. System control and management, including protection and interlocks

2.7. System safe operation conditions.

2.8. Trial operation and maintenance of the system

2.9. The personnel actions for control and maintenance of the system.

3. System failure (success) functions and criteria.

3.1. Functions performed by the system (safety function and other required functions).

3.2. System failure (success) criteria.

4. Determination of the system modeling scope.

4.1. System modeling limits

4.2. Initial state of the system

4.3. Assumptions and allowance made during modeling

4.4. Determination of boundaries of the system elements

4.5. The list of system components considered in the modeling

4.6. Component failure modes considered in the modeling

4.7. System elements excluded from analysis

4.8. Simplified system schematic diagram

5. Justification of the system reliability modeling method.

6. List and description of the elements of structural logical model of the system.

6.1. Events, related to failures (no-failure operation) of the system elements

6.2. Events associated with unavailability of the system elements due to testing, maintenance and repair.

7. Personnel errors.

7.1. Actions during maintenance, tests, repair (actions before performance of the required function by the system).

7.2. Actions in the process of performance of the required functions by the system.

8. Accounting of dependencies and CCF

8.1. Accounting of system dependencies

8.2. Accounting of CCF

9. Description of design programs

10. Quantitative indicators of system's elements reliability

11. Structural and logical system models.

11.1. Structural and logical system model for the required function No. 1.

11.2. Structural and logical system model for the required function No. 2.

11.3. - 11.N. Structural and logical system model for the required functions No. 3 - N.

12. Calculation results of the system reliability indicators

13. Conclusions and recommendations following the analysis

References

Note: The sources from where the data on equipment reliability, human reliability, parameters of GF models etc. were received shall be included in the references.

Appendix No. 9
 to the Safety guide in the use of atomic energy “Recommended procedure for NPP safety-related systems and elements reliability analysis, and their functions" approved by the order of the Federal Environmental, Industrial and Nuclear Supervision Service

No. 26 dated January 28, 2015

**Example of performing system reliability analysis**

1. System description and designation

1.1. System description

Exhaust ventilation system of fresh fuel unit

1.2. System designation in diagrams and operational documentation of NPP.

4KLЕ81

1.3. System code used in the structural logical model КЕЕ81

2. Description of the system.

2.1. System purpose

The exhaust system 4КLЕ81 is designed for air exhaust from the rooms of the fresh fuel storage facility.

2.2. System process flow diagram

Schematic diagram of the exhaust system 4KLE81 is presented in Fig. 1 of this appendix.



Electrical equipment room

Control room

Fresh fuel storage room

Assembled ventilation duct

To ventilation stack

Fig. 1. Schematic diagram of exhaust ventilation system of fresh fuel unit rooms (4KLE81)

2.3. Brief characteristic and system composite.

2.3.1. Brief characteristic and system

The system is a normal operating system and by safety impact is a safety-related system. The system components are related to safety class 3 according to the General provisions for safety of nuclear plants and to seismic category I according to the Design Standards for Aseismic Nuclear Power Plants.

The system has two required functions.

Function 1 - provision of air flow movement directivity (during normal NPP operation, and during NPP operational occurrences) from the places of lesser contamination to the places of greater contamination; provision of required vacuum in the fresh fuel unit.

Function 2 - isolation of air ducts by fire dampers on signal from the fire alarm during fire.

The operating and standby fan units complete with frequency converter, protection device for preventing impacts of air shock wave, fire dampers, air ducts are included in the exhaust system 4KLE81.

The discharge of exhaust air to the atmosphere from the system 4KLE81 is provided along the assemble ventilation duct through the vent stack locate on the building roof of the special building.

Air supply to the periodically serviced room and removal of air from them shall be made directly by the plenum and exhaust system air ducts. Quantity of air remove exceeds the supply air quantity. The air flow-over from the contaminated rooms to the clean rooms shall be excluded under such ventilation diagram.

Ventilation diagram of rooms with permanent stay of personnel provides for direct supply and removal of the same amount of air by the air ducts of the plenum and exhaust systems.

In the event of fire in the rooms provision is made for automatic closing of fire dampers on the plenum and fire dampers on the exhaust in the fresh fuel storage rooms.

The technical characteristics of the system elements are presented in the table 1 of this Appendix.

**Table 1**

**Technical characteristics of the components of system 4KLE81**

|  |  |  |
| --- | --- | --- |
| **On-site designation** | **Description, technical specification** | **Quantity** |
| of the element | room |
| 4KLЕ81AN0014KLЕ81AN002 | 4UKS152514UKS15251 | Partitioned radial fan, aseismic, special design, integratedFlow rate - summer 23880 m3/hour, winter 9480 m3/hour, head 800 Pa | 2 |
| 4KLЕ81AA6014KLЕ81AA602 | 4UKS152514UKS15251 | Check valves serve for isolating the non-operating fan from the network | 2 |
| 4KLЕ81AA621 | 4UKS | Blast protection damper is designed for protection of ventilation channel from air blast | 1 |
| 4KLЕ81AA7014KLЕ81AA7024KLЕ81АА703 | 3UKS063213UKS063224UKS15251 | Fire control fire dampers installed on the air ducts during their crossing of the enclosing structures of dangerous rooms and ventilation chambers are permanently open and close on fire signal in the relevant room, isolating it from the air duct network | 3 |

The transit air ducts section have fire proof insulation with fire-resistance rating equal to the fire-resistance rating of the intersecting fire barrier.

2.3.2. Description of system components

The state of system components 4KLE81 in different system operation modes is presented in the table 2 of this appendix.

**Table 2**

**State of components in different operation modes of the system 4KLE81**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Component name** | **On-site designation** | **Condition** | **Failure mode**  | **Possibility of recovery** | **Interval between trials, h** | **Failure consequences** |
| **in standby** | **in operation** | **in standby** | **in operation** |
| Air channel closing device | 4KLE81АА621 | Open | Open | — | Spurious closing | Yes | — | System failure |
| Check valve | 4KLЕ81АА6014KLЕ81АА602 | Closed | Open | Failure to close | - | Yes | 672 | System failure (after transition to reserve channel) |
| - | Failure to open | Failure of system channel, reduction of redundancy |
| Fire valve on the exhaust line from the rooms | 4KLЕ81АА7014KLЕ81АА7024KLЕ81АА703 | Open | Open | — | Spurious closing | Yes | — | System failure |
| Fan | 4KLЕ81AN0014KLЕ81AN002 | Disconnected | Connected | - | Failure to start | Yes | 672 | Failure of system channel, reduction of redundancy |
| Failure during operation |

2.3.3. Support and control systems

The functioning of the following systems shall be required for providing performance of its functions by the analyzed system:

auxiliary power supply system (function 1 and 2);

I&C (Instrumentation and control system) (function 1);

FP I&C (function 2)

The auxiliary power supply system provides power supply of all the electric drive elements of the system 4KLE81. The description of the auxiliary power supply system is given in section 8.4 of the SAR.

I&C implements the required interlocks for operation control of the system components and state monitoring of the system in the process of its operation. Description of I&C is given in the section 7.1 of SAR.

FP I&C assures power supply, state monitoring and control of fire dampers forming part of the system. Description of I&C is given in the section 7.7 of SAR.

Dependency matrix of the 4kLE81 system components from the support and control system is given in the table No. 3 of this appendix.

2.4. System operation under normal operation conditions of NPP

One ventilation unit of 4KLE81 system is in operation and the second ventilation unit is in standby during normal operation of NPP.

**Table 3**

**Matrix of dependencies of the 4KLЕ81 system components on the supporting and control systems**

|  |  |  |  |
| --- | --- | --- | --- |
| **Component name** | **On-site designation** | **Electric power supply** | **Control signal** |
| ~6 kV | ~0.4 kV | =220 V | I&C | FP I&C  |
| Fire valve on the supply line in the room | 4KLЕ81AA701 | - | - | Assembly 4PH12 | - | + |
| 4KLЕ81AA702 | - | - | Assembly 4PH13 | - | + |
| 4KLЕ81АА703 | - | - | Assembly 4PH14 | - | + |
| Fan | 4KLЕ81АN001 | - | Section 4PB20 | - | + | - |
| 4KLЕ81AN002 | - | Section 4PB40 | - | + | - |

2.5. Functioning of the system in case of any abnormal operation of NPP, including accidents;

The system operation is similar to operation during normal operation during NPP abnormal operation not related to NPP auxiliary outage or fire.

The system loses the capacity to perform the function 1 and does not lose te capacity to perform function 2 during NPP auxiliary outage.

The system performs the function 2 on fire occurrence on signal from the fire alarm.

2.6. System control and management, including protection and interlocks

The exhaust system 4KLE81 is managed from the control panel of the special building 1UKS where the readings of the measured parameters, alarm, readings of the active system components are output.

The standby plant is run if the operating plant breaks down.

The control of fire dampers of the system 4KLE81, monitoring of their state is made from FP I&C MCR, ECR.

The list of protections and interlocks of the system 4KLE81 are presented in the table No. 4 of this appendix.

**Table 4**

**List of system protection and interlocks**

| **Number of the interlock** | **Component name** | **Provisions for safeguards and interlocks** |
| --- | --- | --- |
| 4KLЕ81 B.1 | Fan4KLЕ81АN0014KLЕ81АN002 | Power on:remote by the operator from the special building control panel;remote by the operator in-situ;by ALT automatic load transfer of standby fan by pressure sensor in the suction header 4KLЕ81СР001>500 Pa with 15 sec delay |
|  |  | Disconnection:remote - by the operator from the special building control panel;remote - by the operator at the place of installation;automatic - by fire signal in the ventilation chamber room;automatic - by pressure sensor in the suction header 4KLЕ81СР001 > -500 Pa with 15 sec delay |
| 4KLЕ81 B.2 | Fire retardant damper4KLЕ81AA7014KLЕ81AA7024KLЕ81AA703 | normally open:closing and opening - remotely by the operator from FP I&C, MCR, ECR;automatic closing - by fire alarm signal in the protected room |

2.7. System safe operation conditions.

In compliance with the requirements of chapter 15 of SAR the considered system (at least one fan) must operate continuously. The safe operation conditions related to the KLE81 system operation has not been established.

2.8. Trial operation and maintenance of the system

The system 4KLE81 and its components undergo verification for conformance to the design characteristics after manufacture, during commissioning, after repair and periodically during the entire NPP lifetime.

The following tests are performed for verifying and confirming the design function of the system:

verification of aerodynamic characteristics;

integrated trial operation.

The operation tests stipulate control of the system components with periodicity once in 3 months.

Presence of redundancy allows perform operational tests under any condition of NPP normal operation without decommissioning the system from the operating state.

The system maintenance, which includes maintenance of valves and air ducts, is performed in NPP normal operation mode, as specified below:

verification by external inspection; minor repair, routine maintenance restoration of paint coatings, check of fastening strength of all elements, condition of sealing elements.

Criterion of operability after testing is compliance of the equipment parameters with the requirements specified in the TS for it, as well as no comments with regard to equipment and valves management by means of control keys.

Periodic state monitoring of the components and transition from te operating fan to the standby fan once in 14 days shall be provided for achieving the required readiness level of the fan in standby mode.

2.9. Personnel actions for system management.

The principle of automatic connection of standby equipment during failure of operating equipment, hence the personnel actions for system management during its operation are not required.

3. System failure criteria

The function 1 is considered as executed if the removal of air from the rooms of fresh fuel unit is provided by the operation of at least one of the two fans of the system for 8766 hours,

The function 2 is considered as executed on closure of all the fire dampers on signal from the fire alarm in the event of fire occurrence.

4. Determination of the system modelling scope.

4.1. System modelling limits

1) Thermomechanical equipment limits:

along pressure lines - tie-in points to the ventilation pipe;

by sources of supplied medium - entry of air ducts into the ventilated rooms.

2) Electrical equipment limits

by control circuits - I&C connection points to the actuators. Relays are part of the system KLE81.

by power supply of the fans and motor operated valves - points of termination of power cables to the power buses.

by the power supply of the control circuits and electromagnets of the equipment and valves activation are the places where the supply cables are connected to the corresponding power buses that are not part of the system KLE81.

4.2. Initial state of the system

The following assumptions with respect to the initial state of the system:

fan KLE81AN001 in operation;

fan KLE81AN002 in a wait state

check valve KLE81AA601 is open;

check valve KLE81AA602 is closed;

fire dampers KLE81AA701...703 are open.

4.3. Assumptions and allowance made during modelling

When modeling the system, the following assumptions and allowances are accepted:

GF (general failures) of motor-operated valve for position keeping are disregarded;

possibility of system standby elements being in unscheduled repair is considered;

failures, increasing functions performance reliability, are not simulated;

combinations of failures for change of the valve position and retention of position of the same valve;

rapid recovery of the failed elements that do not have a backup is not taken into account;

4.4. Determination of boundaries of the system elements

The boundaries for the system elements considered in this analysis were determined as follows:

fan includes a mechanical part, motor, coupling or reducing gear, motor power supply diagram, circuit-breaker, I&C;

motor operated valve includes a mechanical part, motor drive, circuit-breaker, I&C;

circuit-breaker includes an executive element, drive, transfer device, drive feed circuit, insulation, arc blowout device, circuit-breaker control circuits.

other electrical equipment and control instrumentation - element boundaries are the input and output contacts.

4.5. The list of system components considered in the modelling

The system components indicated in the table 5 of this Appendix are considered in the structural and logical model of the system.

**Table 5**

**The list of system components considered in the modelling**

| **Component name** | **On-site designation** | **System function during the modelling thereof the component is considered** |
| --- | --- | --- |
| Check valve | 4KLЕ81AA6014KLЕ81AA602 | Function 1 |
| Fire valve on the exhaust line from the rooms | 4KLЕ81AA7014KLЕ81AA7024KLЕ81AA703 | Function 1 |
| Fan | 4KLЕ81AN0014KLЕ81AN002 | Function 2 |

4.6. Component failure modes considered in the modeling

The types of system component failures presented in the table 6 of this Appendix are considered in the structural and logical models of the systems

**Table 6**

**Types of system component failures**

|  |  |  |
| --- | --- | --- |
| **Component** | **Critical failures** | **System function during the modelling thereof the falure type is considered** |
| Fan | 1) Failure when switching on or failure to reach operating parameters when switching on (start-failure).2) Failure during operation | Function 1 |
| Check valve | Failure to open/close | Function 1 |
| Fire valve on the exhaust line from the rooms | Unauthorized (spurious) closure | Function 1 |
| Failure to close | Function 2 |

4.7. System elements excluded from analysis

The following system elements are excluded from analysis:

all the valves not impacting on system operation on change of its position, hence only the simplified fragments of the process flow diagram of the KLE81 system is given in this analysis;

blast protection dampers 4KLE81AA621 as passive elements actuating only during external impact.

4.8. Simplified system schematic diagram

Simplified process flow diagram of KLE81 system is given in fig. 2 of this Appendix. Only those elements of the system which are considered in the system reliability analysis (included in the modeling boundaries) are shown on the diagram.



Fresh fuel storage room

Control room

Electrical equipment room

Discharge ventilation duct of ventilaton stack

Fig. 2. Simplified diagram of ventilation system 4KLE81

5. Justification of the system reliability modeling method.

The system failure is simulated during the development of failure tree, since it is impossible to highlight one dominant failure for this system, for development of system failure model the devopmet of the column is expedient:

6. List and description of the elements of structural logical model of the system.

6.1. Basic events associated with the system element failures

The list of basic events, associated with system element failures is given in table 7 of this Appendix.

Table 7

List of basiс events related to elements failure

|  |  |  |  |
| --- | --- | --- | --- |
| Element and its identifier | Failure parameters | Time characteristics of the element operation | Failure model |
| Failure type | Basic event identifier | Reliability parameter (in accordance with the table No. 10 of this Appendix) | Required operating time, h | Run-up tests period, h |
| Check valve on the operating fan line 4KLЕ81АА601 | Failure to close (on failure of operating fan) | КLЕ81АА601VСС | FR-VCC-А | - | 672 | Periodically tested element |
| Check valve on the standby line of fan 4KLЕ81АА602 | Failure to open | КLЕ81АА602VСО | FR-VCO-А | - | 672 | Periodically tested element |
| Fire damper on the exhaust line from the rooms 4KLЕ81АА701 4KLЕ81АА702 4KLЕ81АА703 | Spurious closing | КLЕ81АА701VMUKLЕ81АА702VMUKLЕ81АА703VMU | FR-VMU-F | 8766 | - | Failure probability is proportional to operation time |
| Failure to close | KLЕ81АА701VMCKLЕ81АА702VMCKLЕ81АА703VMC | FR-VMC-F | - | 8766 | Periodically tested element |
| Operating fan 4KLЕ81АN001 | Failure during operation | KLЕ81АN001FAR | FR-FAR | 8766 | - | Failure probability is proportional to operation time |
| Standby fan 4KLЕ81АN002 | Failure to start | KLЕ81АN002FAS | FR-FAS | - | 672 | Periodically tested element |
| Failure during operation | KLЕ81АN002FAR | FR-FAR | 8766 | - | Failure probability is proportional to operation time |

6.2. Basic events associated with unavailability of the system components due to testing, maintenance and repair

Tests and maintenance of system and its elements do not affect the system readiness to perform its functions.

The probability of element unavailability (PandMT) due to decommissioning for unscheduled repair following start-up failure on commissioning from standby is equal to the multiplication of the failure probability for start-up (*Q*) and ratio of time restoration (*TR*) to the time in standby (*Tstanby*):

|  |  |  |
| --- | --- | --- |
| $$P\_{UMT}=Q∙\frac{TR}{T\_{рез}},$$ |  | (1) |

If the intensity of failure for start-up is given, the failure probability for start-up on scheduled commissioning from standby is equal to the multiplication of the intensity of failure (λ) and the trial run interval (*Ti*):

|  |  |  |
| --- | --- | --- |
| $$Q=λ∙T\_{i},$$ |  | (2) |

Thus the probability of unavailability is equal to:

|  |  |  |
| --- | --- | --- |
| $$P\_{UMT}=λ∙T\_{i}∙\frac{TR}{T\_{рез}}=λ∙TR∙\frac{T\_{i}}{T\_{рез}}$$ |  | (3) |

Time in standby for the elements of KLE81 system shall be two weeks from four. Thus the probability of KBE81 system elements in unscheduled repair following start-up failures is equal to:

|  |  |  |
| --- | --- | --- |
| $$P\_{UMT}=λ∙TR∙\frac{T\_{i}}{\frac{1}{2}T\_{i}}=2∙λ∙TR$$ |  | (4) |

Unavailability of the system fan is equal to the sum of unavailability of individual elements of the system fan line

By inserting in the formula (4) the intensity of failures and restoration time of the elements considered during calculation of fan unavailability due to decommissioning for unscheduled repair, we get:

|  |  |
| --- | --- |
| $$P\_{UMT\\_VENT}=2∙\left(FR\_{FAS}∙TR\_{FAN}+FR\_{VCO}∙TR\_{VC}+FR\_{VCC}∙TR\_{VC}\right),$$ | (5) |

where:

FRFAS - failure intensity on fan start;

FRVCC - failure intensity for closure of QA;

FRVCO - failure intensity for opening of QA

TRFAN - fan restoration time;

TRVC - restoration time of QA.

The values of restoration time and failure intensity for basic events related to unavailability of the elements of 4KLE81АN002 standby fan line due to decommissioning for unscheduled repair.

**Table 8**

**The restoration time values and intensity of failures for base events related to unavailability of the elements of 4KLЕ81AN002 standby fan line due to decommissioning for unscheduled repair**

|  |  |  |  |
| --- | --- | --- | --- |
| **Basic event** | **Failure rate (FR), 1/h** | **Time of restoration (TR), h** | **Unavailability related to failure** |
| KLЕ81АN002FAS | 1.0∙10’5 | 10 | 2.00∙10-4 |
| KLЕ81АА602VСО | 1.2∙10-6 | 6 | 1.44∙10-5 |
| KLЕ81АА602VСС | 1.2∙10-6 | 6 | 1.44∙10-5 |
| Cumulative unavailability of standby fan: | 2.29∙10-4 |

One basic event is considered in this analysis "Non-availability of KLЕ81АN002 due to unscheduled outage", it is given in the table 9 of this Appendix.

**Table 9**

**List of basic events related to the unavailability of system elements KLE81 due to take-down for unscheduled repairs**

|  |  |  |  |
| --- | --- | --- | --- |
| **Event** | **Model** | **Value** | **Designation in the fault tree** |
| Non-availability of KLE81AN02 due to outage for unscheduled repair | Directly assigned probability | 2.29∙10'4 | KLЕ81AN002 M |

7. Personnel errors.

7.1. Actions in maintenance (actions before performance of the required function by the system).

Personnel errors related to maintenance and repair of system elements already accounted in the system elements reliability data not detected before the receipt of request for actuating. Their individual accouting in the system model is not required.

7.2. Actions in the process of performance of the required functions by the system.

The system is not controlled in the process of performance of the required functions by it, therefore accounting of the personnel actions in controlling the system is not made.

8. Accounting of dependencies and CCF

8.1. Accounting of dependencies

Dependency matrix of the KLE81 system components from the support and control systems is given in the table No. 3 of this Appendix.

8.2. Accounting of CCF

In forming the CCF groups the failures of the elements meeting the criteria 1-3 in accordance with the item 8 of Appendix No.5 to this Safety Guide and meeting one of the following requirements were taken into account:

elements included in the CCF group have a common manufacturer;

elements included in the CCF group have common maintenance and repair procedure;

elements included in the CCF group area characterized by similarity of location.

A CCF group from two fans has been formed in performing the function 1 for similarity criteria and similarity of maintenance and repair procedures. The β-factor model with model parameter value 0.1 has been used for the calculation of CCF probabilities. In execution of the function 2 CCF is not simulated due to non-availability of elements redundant by functions performed.

9. Description of design programs

Simulation and system reliability calculation were performed using the Risk Spectrum program. The program has been certified for use in the field of probabilistic risk and reliability analysis by the fault tree and event tree method (certified data sheet No. 59 dated 28 March 2003)).

10. Quantitative indicators of system's elements reliability

10.1. Reliability parameters of system elements

Summarized data from foreign sources as well as reliability data of equipment of NPP with VVER-1000 type reactors were used due to non-availability of specific reliability data.

The quantitative reliability indices of the KLE81 system elements are represented in the table 10 of this Appendix.

11. Structural and logical system models.

11.1. System fault trees for performing functions 1.

Structural and logic model (fault tree) of the system for performing the function1 is represented in the fig. 3 of this Appendix.

**Table 10**

**Quantitative reliability indices of KLE81 system elements**

|  |  |  |  |
| --- | --- | --- | --- |
| **Element type** | **Parameter ID in the model** | **Parameter type** | **Parameter value**  |
| Fan | FR-FAS | Start-up failure rate, 1/h | 1.0∙10-5 |
| Fan | FR-FAR | Failure rate during operation, 1/h | 3.8∙10-5 |
| Fan | TR-FAN | Recovery time, h | 24 |
| Fan | Ti | Trial run interval, h | 672 |
| Check valve | FR-VCO-А | Failure rate for opening, 1/h | 1.2∙10-6 |
| Check valve | FR-VCC-А | Failure rate for closing, 1/h | 1.2∙10-6 |
| Check valve | TR-VС-А | Recovery time, h | 6 |
| Fire damper | FR-VMС-F | Failure rate for closing, 1/h | 2∙10-6 |
| Fire damper | FR-VMU-F | Spurious closing | 4.8∙10-8 |

Failure of exhaust ventilation system of fresh fuel unit



Unreadiness of KLE81AN002 due to shutdown for unscheduled repair

Failure to output control signal to start

Failure of second power supply system train

Failure of standby fan during operation

Failure of first power supply system train

Failure of operating fan during operation

Failure of check valve to open

Spurious closure of fire damper

Spurious closure of fire damper

Spurious closure of fire damper

Transfer failure

Failure of exhaust line valve from the fresh fuel storage rooms

Failure of fans to start

Failure of check valve to close

Transfer failure

Failure of ventilation

Figure 3. Fault tree "KLE81 system failure for performing the functions for air removal from the fresh fuel unit" (the basic events not included in the CCF groups are circled, basic events included in the CCF group are denoted by double delta, the references to the reliability model of supporting and control systems by a triangle)

11.2. System fault trees for performing function 2.

Structural and logic model (fault tree) of the system for performing the function2 is represented in the fig. 4 of this Appendix.

Failure of KLE81 system insulation during fire



Failure of power supply 4PH14

Failure of power supply 4PH13

Failure of power supply 4PH12

No signal output to fire alarms

Failure of fire damper to close

Failure of fire damper to close

Failure of fire damper to close

Fig. 4. Fault tree "Failure of KLE81 system insulation during fire" (notations similar to fig.3)

12. Calculation results of the system reliability indicators

12.1. Calculation results of fail-safe system for the required function "Air removal from the fresh fuel unit rooms"

Failure probability calculations were performed by using reject criterion 1.00E-15.

The evaluated mean value of system failure probability for performing the required function constituted 2.76∙10-3

The dominating minimum cut sets of failures are given in the table 11 of this Appendix.

**Table 11**

**Dominating minimal failure cut-sets to perform function 1 by KLE81 system**

| **Probability** | **Contribution, %** | **Basiс events** | **Description** |
| --- | --- | --- | --- |
| 9.5∙10-4 | 34.4 | KLЕ81АN001FAR | Failure of fan at operation |
| KLЕ81АN002FAS | Failure of redundant fan to start |
| 4.21∙10-4 | 15.2 | KLЕ81АА701VMU | Inadvertent closure of fire damper |
| 4.21∙10-4 | 15.2 | KLЕ81АА703VMU | Inadvertent closure of fire damper |
| 4.21∙10-4 | 15.2 | KLЕ81АА702VMU | Inadvertent closure of fire damper |
| 2.58∙10-4 | 9.36 | KLЕ81АN001FAR | Failure of fan in operation (including common cause failure) |
| KLЕ81АN002FAR | Failure of standby fan in operation (including common cause failure) |
| 1.14∙10-4 | 4.14 | KLЕ81АN001FAR | Failure of fan at operation |
| KLЕ81АА602VCO | Check valve opening failure |
| 1.14∙10-4 | 4.14 | KLЕ81АN001FAR | Failure of fan at operation |
| KLЕ81АА601VСС | Check valve closing failure |
| 6.49∙10-5 | 2.35 | KLЕ81АN001FAR | Failure of fan at operation |
| KLЕ81АN002\_\_\_\_М | Non-availability of KLE81AN02 due to shutdown for unscheduled repair |
| 1.38∙10-5 | 0.51 | РВ001 | Failure of first power supply system train |
| РВ002 | Failure of second power supply system train |

12.2. Results of calculation of system reliability for the required function "Insulation of KEE81 system during fire".

Probability calculations of failure to not perform the required function were performed by using reject criterion 1.00E15.

The evaluated mean value of the system failure probability to perform the required function constituted 1.05∙10-3.

The dominating minimal cut sets of failures (having contribution more than 1% in the descending order of probability) are given in the table 12 of this Appendix.

**Table 12**

**Dominating minimal failure cut-sets to perform function 2 by KLE81 system**

|  |  |  |  |
| --- | --- | --- | --- |
| **Probability** | **Contribution, %** | **Basiс events** | **Description** |
| 2∙10-4 | 19 | РН12 | Fire damper power supply system failure |
| 2∙10-4 | 19 | РН13 | Fire damper power supply system failure |
| 2∙10-4 | 19 | РН14 | Fire damper power supply system failure |
| 1.1∙10-4 | 10.5 | KLЕ81АА701VMC | Fire damper failure to close |
| 1.1∙10-4 | 10.5 | KLЕ81АА702VМС | Fire damper failure to close |
| 1.1∙10-4 | 10.5 | KLЕ81АА703VМС | Fire damper failure to close |

13. Conclusions and recommendations following reliability analysis

The specified reliability indices have not been stipulated for the systems, hence the reliability analysis results are not compared with them.

The issue on reduction of the influence of events with unauthorized closure of fire dampers for performance of function 1by the system shall be considered.

14. References

The reference list is given.

Appendix No. 10
to the Safety guide in the use of atomic energy “Recommended procedure for NPP safety-related systems and elements reliability analysis, and their functions" approved by the order of the Federal Environmental, Industrial and Nuclear Supervision Service No. 26
dated January 28, 2015

**Example of reliability analysis (functional safety) of high technology complex for transport and process operations with nuclear fuel**

1. Description of the technology complex for transport and process operations with nuclear fuel.

Fresh nuclear fuel is input to the NPP unit with VVER-1000 reactor in fresh fuel guide. At the NPP unit the cask with FA is removed from the in-plant cart using a Polar crane equipped with type 1 cask capture. The cask is installed on the floor it the reactor compartment, where the cover from it is removed by a polar crane. After the cover is removed the cask is placed by the polar crane on the fuel pool step, for this purpose the crane is equipped first with type 1 cask gripper and then with type 2 cask gripper, and the gripper is moved from the SFP step to the casing head of SPF

The SPF pit is filled with water, and all further operations with FA shall be performed under water The SFP rearranging FA from the cask to the FP racks, from the FP racks to the FP racks from the reactor to the SPF racks is made by MP)

The transportation of SFA from the FP to the in-plant SFSF shall be made in TP.

The in-plant platform on which TP is installed by the SFP equipped with an equipment and a cam follower for transporting TP from SFP to the NPP unit and back TP is removed at the NPP unit from the in-plant platform by a polar crane equipped with a cam follower. TP is installed on the floor in the reactor compartment, where the covers No.1 and No. 2 are removed from it by the polar crane equipped with a gripper. Polar crane is equipped with a cross-member, TP is installed in MG of FP pit. Before the start of refuelling works with SFA, the FP well shall be filled with water. RM shall perform the installation operation of SNF from the racks of SPF

The cover No.2 is installed in TP by the polar crane. The container cover gripper shall be used for this purpose. TP is present in MG of FP, filled with water. After the cover No.2 has been installed the water is drained from the pit of SFP and removal by polar crane equipped with a cross-beam TP is decontaminated further and the installation by the polar crane equipped with gripper No. 1 of the roof No. 1 in TP. Polar crane equipped with traverse beam, TP shall be installed on the in-plant platform. The TP is transported from the NPP unit to NPP SFSF is made on the in-plant platform.

2. Determination of the simulation boundaries of a high-technology complex

The following systems form the scope of a high-technology complex providing performance TPE for refuelling:

polar crane (electrical bridge special polar crane of lifting capacity 320+160/2x70 tons span 43 m) with grippers and cross-members;

refuelling machine RM-1000

On-site platform

TP

3. Description of the systems included in the scope of high-technology complex.

3.1 Polar crane

A polar crane shall be installed in the NPP reactor compartment buildings with VVER-1000 type reactor and designed for performing TPE for fuel refuelling, reactor audit etc.

In terms of design the basis of a polar crane is a bridge consisting of two main beams connected by two transverse end beams. The bridge rotates around its axis for ± 360° Two load trolleys move along the crane bridge along the common path. Major bogie and dolly Power lifting mechanisms are installed on the trolleys: on the major bogie - of lifting capacity 370 (200) tons, on the dolly - 160 (140) tons and 2x70 tons.

The crane is remotely controlled from the main control panel installed in the control cabin, or from the standby panel installed in the electrical equipment room.

Control of lifting mechanisms 370 (200) tons, 160 (140) tons, ,2x70 tons and hoists is made using one command controller. The specific device including joint operation of the lifting mechanisms 160 (140) tons and 2x70 tons shall be selected using the additional selector switch on the control panel. The switching over from one lift drive to another shall be made only in stopped lift drives.

The crane operator shall receive information on the status of load transportation, current procedure, status and position of machinery of the crane either automatically or upon a request.

Polar crane power supply shall be from the NPP auxiliary power supply.

Synchronous lifting and lowering of cargo is provided by two redundant lifting systems of the auxiliary cargo cart of lifting capacity 160 tons and lifting capacity 2x70 tons. If one of the lifting systems goes out of order the other system continues the transportation operation. The lifting machineries may operate both synchronously and separately independent of each other. The design of the lifting machinery allows provide completion of the started process operation on outage of one of the motors. The lifting or lowering shall be continued by the second motor but with half the speed. The assembly sling of hoisting capacity 160 tons is equipped with a double-lift plate hook that is pin connected with the fork plate resting on a roller bearing. The hook fork plate is provided with a rotating mechanism which allows carry out automatic rotation of the fork plate with the hook for 270°. The latter is equipped with an extension mechanism of the hook axis for mechanical disconnection of the hook or cargo from the fork plate. The assembly sling of hoisting capacity 2x70 tons consists of two minor hoists of hoisting capacity 70 tons interconnected by a bracket. The minor hoists are equipped with lifting lugs. The lifting lugs reset on the thrust bearing thanks to it may rotate around the vertical axis by 360°.

The polar crane has the following protections and interlocks.

prohibition of the crane operation with tripping of the main contactor and actuation of brakes of all mechanisms if the weight of the load exceeds the rated load lifting capacity by more than 10% from the rated load;

prohibition of the crane operation with disconnection of the main contactor and actuation of brakes of all mechanisms upon actuation of emergency terminal breakers (top hoisting position);

prohibition of the crane operation with disconnection of the main contactor and actuation of brakes of all mechanisms if hoisting speed exceeds the rated value by more than 30%;

prohibition of simultaneous operation of two or more mechanisms, except joint operation of the crane travelling gear and travelling gear of the main or auxiliary trolley, and prohibition of simultaneous operation of hoisting mechanisms 160(140) tons and 2х70 tons of the auxiliary cart during transportation of the container with SNF;

prohibition of switching to choice of lifting drives (main 370(200) tons, main 160(140) tons, auxiliary 2x70 tons, hoists 10 tons) during operation of one of them;

prohibition of hoisting machinery 370(200) tons and 160(140) tons in the down direction on weight reduction of the consignment below the maximum given value;

shutdown of the hoisting machinery when terminal breakers reach terminal positions (movement is possible only in the opposite direction);

transition of the hoisting machinery to minimum speed on actuation of the speed reduction preliminary terminal breakers;

prohibition of the operation of fork axes extension devices 370(200) tons and 160(140) tons if there is load on the suspension;

shutdown of fork axes extension devices 370(200) tons and 160(140) tons on exceedance of the given torque value;

shutdown of the main and auxiliary trolley travelling machinery when terminal breakers reach terminal positions (movement is possible only in the opposite direction);

prohibition for crane displacement of consignment above the spent fuel pool and reactor cavity except special transport operations in the specified areas.

3.2 Refuelling machine RM-1000

RM is designed for performing FHE, related to nuclear fuel refuelling.

RM consists of a bridge traveling along a rail path, and trolley on which the control members of the machine are installed: RSh, guide tube with turntable, RSh swing drive, TVM swing drive, two destructor drive,TVM, installed in the turntable slot. Power supply to RM is made through the current lead of the bridge from the auxiliary power supply system.

The RM is controlled from the stationary remote control panel located in a special room located outside the reactor compartment containment. The controls and control instrumentation are available in the control panel.

The reactor is refueled in semi-automatic mode when the RSh is pointed to the target point, coupled with the refueled product and it is removed in automatic mode, and the command for performing each of the following operation after the performance of the previous operation is given by the operator.

For example, after pointing RM to the target point, the coupling with the removed product is made after verification of the correct exit to the target point by comparing these readings of indices of bridge and trolley displacement with the coordinates specified in the refueling program.

RM has the following protections and interlocks:

prohibition for displacement of bridge and trolley on reaching the extreme positions;

prohibition for rotate of RSh on reaching the end positions;

prohibition for rotate of TVM on reaching the end positions;

prohibition for rotate of RSh for exclusion of permitted areas;

prohibition for displacement of RM machinery except the bridge displacement machinery, on RM location above the transport corridor;

prohibition for displacement of FA up on reaching the maximum load on the FA gripper channel;

prohibition for displacement of the cluster gripper upwards on reaching the maximum load on the cluster gripper;

prohibition for displacement of the cluster gripper downwards on reduction of force in the cable by the value more than the planed;

prohibition for displacement of the FA gripper down on reducing force in the cable by a value more than permitted;

prohibition for vertical displacement of RSh on reducing extreme top position;

prohibition for displacement of FA if the turn mechanism of RSh is not in a permitted angular position;

prohibition for TVM displacement down on loosening of the TVM cable;

prohibition for displacement of bridge and trolley on RSh or TVM not in a transportation position excluding RM operation during step motion or during inspection of the compartments of the service and level control zone of FA in the reactor and movement on low speed;

exclusion being unauthorized displacement of RM mechanism.

3.3. In-plant platform (description of the in-plant platform is given)

3.4 TP (description of TP is given).

4. Determination of the process carried out by the high-technology complex.

Transportation and installation performed by the high-technology complex has been grouped in the following processes:

Process 1 - installation of jacket with FA on the floor of the reactor compartment (from the in-plant platform);

Process 2 - displacement of jacket without cover on the steps of SFP;

Process 3 -Displacement of jacket from the SFP steps at MG;

Process 4 - Displacement of FA from MG to the SFP rack;

Process 5 - Displacement of FA from the rack of SFP to the reactor;

Process 6 - Displacement of SFA from the reactor to the SFP rack;

Process 7 - Displacement of SFA from SFP to MG;

Process 8 - Displacement of TP (from SFA) from MG to wash;

Process 9 - Displacement of TP (from SFA) from wash to car;

Process 10 - removal of CFF from MG;

Process 11 - installation of TP in MG.

5. Process analysis

From the analysis of the process presented in the item 4 of this appendix, the following basic intervals are highlighted.

Basic intervals of process TP1:

BI01 - installation of the gripper of type 1 for CFF on the polar crane main lift fork;

BI02 - polar crane travel with gripper of type 1 without CFF to the retrieval coordinates of CFF from the car;

BI03 - vertical displacement of type 1 gripper without CFF from the transport position level to the gripper seating level on CFFin the car;

BI04 - coupling of type 1 gripper with CFF;

BI05 - vertical displacement of type 1 gripper with CFF from the seating level of gripper on CFF in the car to the transport position level;

BI06 - crane travel to CFF installation coordinates on the floor of the reactor compartment;

BI07 - vertical displacement of type 1 gripper with CFF from the transport position level to the CFF installation level on the floor of the reactor compartment;

BI08 - decoupling of CFF with type 1 gripper.

Basic intervals of process TP2:

BI09 - vertical displacement of type 1 gripper with CFF without cover from the CFF installation level on the floor of the reactor hall to the level of the transport position;

BI10 - polar crane travel to the CFF installation coordinates on the SFP step;

BI11 - vertical displacement of type 1 gripper with CFF from the transport position level to the CFF installation level on the SFP step;

BI12 - decoupling of type 1 gripper from CFF;

BI13 - removal of type 1 gripper from the crane fork;

BI14 - installation of type 2 gripper on the fork for CFF;

BI15 - crane travel with type 2 gripper without CFF to the coupling coordinates with CFF on SFP step;

BI16 - vertical displacement of type 2 gripper without CFF from the transport position level to the gripper seating level on CFF on SFP step;

BI17 - coupling of type 2 gripper with CFF;

Basic intervals of process TP3:

BI18 - vertical displacement of type 2 gripper with CFF from the CFF installation level on the intermediate platform to the CFF end of removal level from the SFP step;

BI19 - crane travel from CFF to the coordinates of installation of CFF in MG;

BI20 - vertical displacement of type 2 gripper with CFF from the CFF end of removal level from CFF to MG;

BI21 - decoupling of type 2 gripper from CFF;

BI22 - vertical displacement of type 2 gripper without CFF from the seating level of gripper on CFF to the transport position level;

BI23 - removal of type 2 gripper from the fork.

Basic intervals of the processes TP4, TP5, TP6, TP7:

Bi24 - displacement of MP over the reactor, SFP or MG without FA;

BI25 - displacement of RM along the transport corridor without FA;

Bi26 - displacement of MP over the reactor, SFP or MG with FA;

BI27 - displacement of RM along the transport corridor with FA;

BI28 - vertical displacement of FA gripper without FA from the transport position up to the level 200 mm above the level of heads of installed FA;

BI29 - vertical displacement of FA gripper without FA from the level 200 mm above the level of heads of installed FA to the FA gripper seating level on FA'

BI30 - swing of FA gripper on connection with FA;

BI31 - vertical displacement of FA gripper with FA from the slot to FA lower end cap position 200 mm above the level of heads of FA installed;

BI32 - vertical displacement of FA gripper with FA from the FA lower end cap position 200 mm above the level of heads of FA installed up to the transport position;

BI33 - vertical displacement of FA gripper with FA from the transport position up to the level, corresponding to FA lower end cap 200 mm above the level of heads of installed FA;

BI34 - vertical displacement of FA gripper with FA from the level corresponding to the FA lower end cap 200 mm above the level of heads of FA installed before the slot;

BI35 - swing of FA gripper on disconnection from FA;

BI36 - vertical displacement of FA gripper without FA from the seating level of FA gripper on FA up to the level 200 mm above the heads of FA installed;

BI37 - vertical displacement of FA gripper without FA from the level 200 mm above the heads of installed FA before the transport position.

Basic intervals of the process TP8:

BI38 - installation on the fork of crane sling;

BI39 - crane travel with cross-arm without TP to the coordinates for container retrieval from MG;

BI40 - vertical displacement of cross-arm without FA from the transport position level to the coupling level with the cross-arm with TP;

BI41 - coupling of cross-arm with TP in MG;

BI42 - vertical displacement of cross-arm with TP from the coupling level of cross-arm with TP up to the start level of installation on the SFP step;

BI43 - crane travel with TP to the coordinates of installation on the SFP step;

BI44 - vertical displacement of cross-arm with TP from the start level of T installation on the intermediate platform to the TP installation level on SFP step;

BI45 - installation of cover in TP;

BI46 - vertical displacement of cross-arm with TP from the installation level of TP on the SFP step up to the transport position level;

BI47 - crane travel with TP to the wash station coordinates

BI48 - vertical displacement of cross-arm with TP from the transport position level to the TP placement level in the wash station.

Basic intervals of process TP9:

BI46 - vertical displacement of cross-arm with TP from the installation level of TP in the wash station up to the transport position level;

BI50 - bridge displacement with TP to the TP installation coordinates in the car;

BI52 - vertical displacement of cross-arm with TP from the transport position level to the TP placement level in the car

BI52 - decoupling of cross-arm with TP in the car;

BI53 - vertical displacement of cross-arm without TP from the decoupling level of cross-arm with TP in the car up to the transport position level;

BI54 - removal of cross-arm from crane fork

Basic intervals of process TP10:

BI55 - vertical displacment of CFF without FA;

BI56 - horizontal displacement of CFF without FA.

Basic intervals of process TP11:

BI57 - vertical displacement of TP without FA;

BI58 - horizontal displacement of TP without FA.

6. Functions executed by the high-technology complex.

The high-technology complex executes the following required functions:

Function 1 - carrying out a complex of operations with FHE in accordance with the stipulated nomenclature of FHE and refuelling procedure (rearrangement, unloading, loading) FA. FHE nomenclature is established individually for each refuelling (rearrangements, unloading and loading) of FA, following which the quantity and procedure of adhering to the process TP1-TP11 of functions performed by the complex and on exercising the function1 is also individual:

Function 2 - prevention of violations in performing a set of actions with FHE of the requirements of regulatory and process documentation related to safety assurance in handling radioactive fuel. As noted above, FHE nomenclature is established individually for each refueling (rearrangements, unloading and loading) of FA, following which the quantity and procedure of adhering to the process TP1-TP11 of functions performed by the complex and on exercising the function1 is also individual.

7. Failure criterion of a high technology complex

Failure criterion of high-technology complex for performing function1 is the crane or RM failure or other failure (personnel error) leading to non-performance of any processes TP1-TP11, subject to performance by the high-technology complex.

Failure criterion of high-technology complex for performing function 2 is the occurrence of any of the events of non-compliance with the requirements of regulatory and process documentation related to safety assurance in handling nuclear fuel presented in table 1 of this appendix.

Table 1 Events on occurrence thereof the high technology complex refuses to perform function 2

| Event | Event characteristic | Basis for selection |
| --- | --- | --- |
| Events related to CFF |
| End impact of protective cover with fresh fuel | End impact, which may cause damage or change of geometry of FA and FE | Item 2.4.4 Safety rules for storage and transportation of nuclear fuel at nuclear facilities |
| Lateral impact of protective cover with fresh fuel | Lateral impact, which may cause damage or change of geometry of FA and FE | Item 2.4.4 Safety rules for storage and transportation of nuclear fuel at nuclear facilities |
| Events related to FA |
| Excessive mechanical loads on FA during refuelling | Torque exceedenceCompressive force exceedenceFA removal force exceedence | Item 2.4.4, 4.6.1 of the Safety rules for storage and transportation of nuclear fuel at nuclear facilities |
| FA bending force | Occurrence of bending force | Item 2.4.4, 4.6.1 of the Safety rules for storage and transportation of nuclear fuel at nuclear facilities |
| Lateral impact of FA | Impaction of refueling machine mast transporting FA with the reactor structures or SFP shall not be allowed | Items 2.4.4, 4.6.1 and 4.6.6 of the Safety rules for storage and transportation of nuclear fuel at nuclear facilities |
| FA lift above the permitted level | FA lift in the process of FHE above the maximum permitted level | Item 4.6.3, 4.6.8 of the Safety rules for storage and transportation of nuclear fuel at nuclear facilities |
| Events related to TP |
| End impactTP with SFA | End impact, which may cause damage or change of geometry of FA and FE | Item 2.4.4 Safety rules for storage and transportation of nuclear fuel at nuclear facilities |
| Lateral impact of TP with SFA | Lateral impact, which may cause damage or change of geometry of FA and FE | Item 2.4.4 Safety rules for storage and transportation of nuclear fuel at nuclear facilities |

8. Analysis of consequences of process disturbances

For each basic interval listed in the section 5 of this appendix, the characteristic for it process disturbances have been determined, as well as the consequences of disturbances have been determined.

The results of determining the consequences of process violations are presented in the table 2 of this appendix (due to the large scope of the table its fragment is represented viz. the results of analysis of the consequences of process disturbances TP4 in the basic interval BI32 for the function 2).

**Table 2**

**Results of determining the consequences of process disturbances TP4 (fragment)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Basic interval** | **System, personnel** | **Process disturbances** | **Protections and interlocks provided for (note 2)** | **Disruption consequences (during disability of protections and interlocks)** |
| BI32 Vertical displacement of FA gripper with FA from the lower end cap position. FA 200 mm above the level of heads of installed FA before the transport position | Reloading (refuelling) machine | F012 Failure of FA gripper displacement drive power circuit | L07(2), L07(3),L56(p), L82(2) | D01Fall of FA |
| F018 FA grapple cable break | Protections (interlocks) not provided for | D01Fall of FA |
|  | F001 Breakdown period | Imposition of FA grapple drive brakes in power-off | D01Fall of FA |
| F030 False activation of bridge drive (note 1) | L03(2), L03(3), L01(4), L01(5) | D05Lateral impact of FA |
| F040 False activation of the cart drive | L04(2), L04(3),L02(4), L02(5) | D05Lateral impact of FA |
| F070 Spurious actuation of the notcher displacement drive towards uncoupling | FA gripper design does not allow notcher to open if FA is available | D01Fall of FA |

Note 1 Results of determining the reasons of occurrence of process disturbance are given in the table No. 3 of this Appendix

Note 2 Description of protections and interlocks

L01(4) - reduction of bridge speed to the specified value if there is signal from the ultrasound approximation sensors to the obstacle;

L01(5) - supply disconnection of bridge if there is the sensor signal "Crash";

L02(4) - reduction of trolley speed to the specified value if there is signal from the ultrasound approximation sensors to the obstacle;

L02(5) - power outage of trolley if there is sensor signal "Crash";

L07(2) - power outage of motors of all RM mechanisms in unauthorized displacement of FA gripper;

L07(3) - power outage of motors of all RM mechanisms in unauthorized displacement of FA gripper;

L03(3)- Bridge traversing stop if RSh is located at a distance of less than the minimum permitted level up to the servicing area boundary;

L04(3) - traversing stop of trolley if RSh is away from the boundary of service area at a distance less than the minimum allowed;

L03(2) - stop of bridge displacement when RSh is at a distance less than the minimum permitted to the boundary of the service area;

L56(3) - stop of FA gripper displacement in speed greater than it is provided for by the process restrictions;

L04(2) - stop of trolley displacement on RSh located at a distance of less than the minimum permitted to the boundary of the service area;

L82(2) - stop of FA gripper in exceedence of displacement speed.

9. Determination of the causes of occurrence of process disturbances

For each process disturbance represented in the table 2 of this appendix, the reasons of its occurrence have been determined.

The results of determination of the reasons of occurrence of process disturbances have been represented in the table 3 of this appendix (fragment - results of analysis of the reasons of process disturbances occurrence "Spuious activation of bridge drive").

Table 3

Analysis of causes of occurrence of process disturbances (fragment)

|  |  |  |
| --- | --- | --- |
| Process disturbance | Failures of system elements, personnel errors leading to disturbance | Protections and interlocks provided for (note 1) |
| F030 Spurious activation bridge drive for BI32 - Vertical displacement of FA gripper with FA from the FA lower end cap position 200 mm above the level of heads of FA installed up to the transport position; | IE 001 Operator errors leading to input of untimely task for bridge displacement | P01(2), P01(3), P02(2), P02(3), P03(2) |
| IE 201 Failure of control console leading to delayed formation of the task for bridge displacement |
| IE 301 Failure of control subsystem leading to untimely formation of the command for bridge displacement | Р01(3), P02(3) |
| IE 401 Failure of frequency converter of bridge displacement drive leading to ill-timed start of bridge displacement | L01(2), L01(3) |

Note 1 Description of protections and interlocks

P01(2) - prohibition for displacement (interlock) of the bridge in displacement of the FA gripper;

P01(3) - prohibition for displacement (interlock) of the bridge in displacement of the FA gripper;

P02(2) - prohibition for displacement (interlock) of the bridge when the FA gripper is not in transport position;

P02(3) - prohibition for displacement (interlock) of the bridge when FA is not in transport position;

P03(2) - prohibition for displacement (interlock) of the bridge when TVM is not in transport position;

P01(3) - prohibition for displacement (interlock) of the bridge in displacement of the FA gripper;

P02(3) - prohibition for displacement (interlock) of the bridge when FA is not in transport position;

L01(2) - power outage of motors (interlock) of all RM mechanisms in unauthorized displacement of the bridge;

L01(3) - power outage of motors (interlocks) of all RM mechanisms in unauthorized displacement of FA gripper;

10. Building of structural and logic model of reliability (functional safety) of high-technology complex of FHE with nuclear fuel

The fault tree method has been selected for development of a structural and logic model of reliability (functional safety) of high-technology complex of FHE with nuclear fuel.

The fault tree of technological complex of FHE with nuclear fuel for performing function 2 is given in the fig. 1-5 of this Appendix (its fragment is given due to large size of the model )



Failure of technological complex Lateral impact of FA

Failure of technological complex in the BI R33: Lateral impact of FA

Failure of technological complex in the BI R32: Lateral impact of FA

Failure of technological complex in the BI R27: Lateral impact of FA

Failure of technological complex in the BI R26: Lateral impact of FA

Fig. 1. Fault tree "Failure of high-technology complex on account of lateral impact of FA (all basic intervals have been considered)



Interlock failure: Supply disconnection of cart if the sensor signal "Collision with obstacle" is available

Interlock failure: Reduction of collision before the given sa if there is signal ot of the approximatios sensors to

Interlock failure: Stop of trolley displacement if RSh is at a distance of less than one min to the boundary of service zone

Interlock failure: Stop of trolley displacement if RSh is at a distance of less than one min to the boundary of service zone

Interlock failure: Supply disconnection of bridge if the sensor signal "Collision with obstacle" is available

Interlock failure: Reduction of collision before the given surveillance area if there is signal from ultrasound approximation sensors to the

Interlock failure: Stop of bridge displacement if RSh is at a distance of less than one min to the boundary of the service aea

Interlock failure: Stop of bridge displacement if RSh is at a distance of less than one min to the boundary of the service aea

Failure of protections and interlocks

Process disturbance at BI R32: False activation of the cart drive

Process disturbance at BI R32: False activation of bridge drive

Failure of protections and interlocks

Lateral impact of FA on account of false activation of bridge drive

Lateral impact of FA on account of false activation of cart drive

Failure of technological complex in the BI R32: Lateral impact of FA

Fig. 2. The fault tree "Failure of high-technology facility on account of lateral collision of FA in the basic interval BI32" (developed based on the table 2 data of this Appendix)



Interlock failure: power outage of motors of all mechanisms of MA in unauthorized bridge displacement

Interlock failure: power outage of motors of all mechanisms of MA in unauthorized bridge displacement

Protection failure: ban on movement of bridge in location of the FA current converter is not in the transportation position

Protection failure: ban on displacement of bridge in displacing FA clamps

Protection failure: ban on movement of bridge in location of the FA current converter is not in the transportation position

Protection failure: ban on displacement of bridge in displacing FA clamps

Protection failure: ban on displacement of bridge in finding TSh is not in the transportation position

Protection failure: ban on movement of bridge in location of the FA current converter is not in the transportation position

Protection failure: ban on displacement of bridge in displacing FA clamps

Failure of remote control console leading to untimely formation of the task untimely for improvement fault movement to location.

Operator error leading to input delayed tasks for displacent from the landlord

Failure of PCh bridge displacement drive leading to ill-timed start of bridge displacement

Failure of protections and interlocks

Failure of protections and interlocks

Failure of power control panel leading to untimely formation of the command for bridge displacement

Failure of protections and interlocks

Failure of RCP or operator error

Spurious bridge actuation due to PCh failure

Spurious bridge activation following PCP failure

Spurios bridge activation following RCP failure or operator error

Process disturbance at BI R32: False activation of bridge drive

Fig. 3. The fault tree "Failure of high-technology facility on account of spurious activation of bridge drive in the basic interval BI32" (developed based on the table 3 data of this Appendix)



Failure of "transport position 3FA with FA" sensor

FA gripper drive encoder failure (PCP)

Failure of strain gauge indicator of 3FA displacement drive (PCP)

Incorrecct presentation of information on the condition of RSh in PCP

Incorrecct presentation of information on the condition of RSh in PCP

PCP failure

Protection failure: ban on movement of bridge in location of the FA current converter is not in the transportation position

Fig. 4. Fault tree "Protection failure: Ban on bridge movement in location of FA clamp not in shipping position" (built on the analysis of protections and interlocks of MA)



"Emergency shutdown" relay failure (PSU)

Emergency releaser relay failure PSE

PCP failure

Bridge encoder failure (PSU)

Failure of power supply current contractor ShUP2 (PSE)

PSU does not impact on the emergeny trip element

ShUP power supply cannot be removed

Interlock failure: power outage of motors of all mechanisms of MA in unauthorized bridge displacement

Fig. 5. Fault tree "Interlock failure: Motor power outage of all mechanisms in MA during unauthorized bridge displacement" (built on the basis of analysis of MA protections and interlocks)

10. Reliability parameters of elements of a high-technology facility.

Results of determining the reliability indices of elements of the process facility TPE with nuclear fuel have been presented in the table 4 of this Appendix

Table 4

Reliability parameters of elements of the process facility of TPE with nuclear fuel (fragment)

| Element type | Failure intensity, 1/h.10-6 |
| --- | --- |
| MotorDRS13286ВЕ5HR/FL/ТF/ЕV7С/V/DH | 0.41 |
| Brake BE5B | 0.41 |
| Position sensor 3SЕ5122-0СD02 | 0.33 |
| Position sensor 3SЕ5122-0СD02 | 0.33 |
| Gear-motorКA37/ТRS80S4ВЕ1НR/ТF/ЕV7С/DН | 0.41 |
| Force measuring transducer | 10.0 |
| Gear motor KA107/TDRS132МВЕ5НR/ТF/ЕV7С/DН | 0.41 |
| Brake NFF630 | 4.88 |
| Gear motor KAF37/DR63L4ВR/HR/ТF/ЕН1С/Н | 0.41 |
| Rotary switch | 1.00 |
| Brake NFF40 | 4.88 |
| Gear motor KA47 R37DR63М4ВR/НR/ТF/ЕН1С | 0.41 |
| Brake NFF4 | 0.57 |
| Encoder CEV 58М-00227 | 4.00 |
| Ultrasound sensor | 3.80 |
| Relay assembly | 0.13 |
| Interface module IM151 | 0.82 |
| Discrete signal input module 8D1 | 0.43 |
| Brake control module BMK | 2.78 |
| Brake control module GSSG | 2.78 |
| Contactor LC1D09 | 1.25 |
| Discrete input module SM321 | 3.74 |
| Relay module PLC-RSC | 0.03 |
| Discrete output module SM322 | 6.37 |
| Analog signal input module 4AI | 1.11 |
| Relay LR-2 | 0.28 |
| Current convertor MD61B |  |
| Discrete signals input module 8DI | 0.43 |
| End switch | 1.00 |
| Discrete output module 8DO | 0.29 |
| Input module of signals 2АI I 2/4 | 0.87 |

11. Accounting dependencies of high-technology facility. Accounting of CCF

The dependencies of the operation of elements and systems constituting the high-technology facility from the NPP auxiliary power supply systems were considered in the analysis.

The groups of elements subject to CCF were determined in the analysis of process facility TPE with nuclear fuel. The CCF groups were formed for the elements meeting the criteria 1-3 in accordance with the item 8 of Appendix No.5 to this Safety Guide and meeting one of the following requirements:

elements included in the CCF group have a common manufacturer;

elements included in the CCF group have common maintenance and repair procedure;

elements included in the CCF group area characterized by similarity of location.

Description of the group of elements (description fragment) subject to CCF is given in the table 5 of this appendix.

**Table 5**

**Group of process facility elements of TPE with nuclear fuel subject to CCF (fragment)**

| **Identification and name of group** | **Identification and name of elements included in the group scope** | **Model for determining the probability of CCF** | **Values of model parameters** |
| --- | --- | --- | --- |
| Refueling machine equipment |
| 1 BS bridge drive encoders | 1VS 1 Bridge drive encoder (PSU)1VS2 Bridge drive encoder (PS3B) | β-factor model  | 0.1 |
| 2BC Encoders of cart drive | 2BC1 Encoder of cart drive (PSU)2BC2 Encoder of cart drive (PSZB) | β-factor model  | 0.1 |
| 4BC Encoders of gripper driveFA | 4BC1 Encoder of FA gripper drive (PSU)4BC2 Encoder of FA gripper drive (PSZB) | β-factor model  | 0.1 |
| 4BP two-channel force sensing converrter Force control on the FA grip rope | 4BR1.1 Force control on the FA rope grip (sensor channel connected to PSU)4BP1.2 Force control on the FA rope grip (sensor channel connected to PSZB) | β-factor model  | 0.1 |
| 3SQ(1,5) Destruct drive 1 sensors "Extreme top position" | 3SQ1 Extreme top position (PSU)3SQ5 Extreme top position (PS3B) | β-factor model  | 0.1 |
| CPU controllers | CPU\_319-3 Suspended Level Alarm CPU Module CPU\_319-3 Module CPU PSZB | β-factor model  | 0.1 |
| 1YB Bridge drive brakes | 1T1 Built-in bridge drive brake1YB1 Bridge drive external brake | β-factor model  | 0.01 |
| 2YB Trolley drive brakes | 2T1 Built in trolley drive brake2YB1 Trolley drive external brake | β-factor model  | 0.01 |
| 4YB FA gripper drive brakes | 4T1 FA gripper built-in brake4YB1 FA gripper driver external brake | β-factor model  | 0.01 |
| К4\_К5 Relay ShUP trolley movement permit | K4 Trolley movement permit relay from control cabinetK5 Trolley movement permit relay from protections and interlocks subsystem | β-factor model  | 0.1 |
| К12\_К13 Relay ShUP FA gripper movement permit | K12 Relay FA gripper movement permit from the control cabinet K13 Relay FA gripper movement permit from protections and interlocks subsystem | β-factor model  | 0.1 |
| КМ11\_КМ12 Contactor for activation of external and built-in brakes of FA gripper motor | KM11 Contactor for activation of external FA gripper motorKM12 Contactor for activation of built-in brakes of FA gripper motor | β-factor model  | 0.1 |

12. Accounting of personnel impact

List of possible personnel errors was formed following analysis of the reasons of process disturbance and failure conditions of protections and interlocks

The actions executed by the personnel during control, maintenance and testing of process complex equipment were considered in performing analysis of the occurrence reasons of process disturbances and conditions of failure of protections and interlocks.

General list of personnel errors was divided into the following groups during control

1) for RM:

errors during bridge control;

errors during trolley control;

errors during control of destructor mechanism

errors in management of FA gripper;

errors in management of FA gripper retention pin;

errors in management of RSh swing

errors in management of cluster gripper;

2) for polar crane:

errors during bridge control;

errors in management of main trolley;

errors in management of auxiliary trolley;

errors in management of lift 370 (200 tons);

errors in management of lift mechanism 160 (140) tons;

errors in maagement of lift mechanism 2x70 tons;

errors in hoist management.

Personnel errors in maintenance and trial runs were divided into the following groups:

errors in input of set points for actuation of protections and interlocks;

errors in calibration of measurement channels;

errors in adjustment of velocity and load cyclograms;

errors in preparation and loading of refuelling program (only for RM);

errors in preparation and loading of reactor and SFP pattern (only for RM)

A fragment of the list of personnel errors with the assigned probabilities following screening and (if required) detailed analysis is given in the table 6 of this appendix.

Following the analysis of dependencies between the errors of personnel significant dependencies between the probabilities of personnel error were not established.

**Table 6**

**Personnel errors (fragment)**

|  |  |
| --- | --- |
| **Name of personnel error** | **Personnel error probability** |
| Errors in management of refueling machine |
| Errors in management of bridge |
| Operator errors leading to input of untimely task for bridge displacement | 3∙10-3 |
| Operator error leading to input of erroneous coordinates of the bridge stop in the permitted area (only for semi--automatic mode) | 3∙10-3 |
| Operator error leading to input of coordinates of bridge stop in the forbidden area (only for semi-automatic mode) | 3∙10-3 |
| Errors in trolley management |
| Operator error leading to input of ill-timed assignment for trolley displacement | 3∙10-3 |
| Operator error leading to input of erroneous coordinates of trolley stop in the permitted area (only for semi-automatic mode | 3∙10-3 |
| Operator error leading to input of coordinates of trolley stop in the forbidden area (only for semi-automatic mode) | 3∙10-3 |
| Errors in FA gripper control |
| Operator errors leading to input of ill-timed task for FA gripper upward movement  | 3∙10-3 |
| Operator errors leading to input of ill-timed task for FA gripper downward movement  | 3∙10-3 |
| Operator error leading to input of coordinates for arresting stop of FA gripper in the forbidden zone (only for semi-automatic mode) | 3∙10-3 |
| Errors in input of trip set points of protections and interlocks  |
| Error in input of the parameter " Maximum permitted force on two FA gripper cables" | 1∙10-3 |
| Error in input of the parameter "Maximum permitted FA grip rate" | 1∙10-3 |
| Errors in calibration of control channels |
| Error in calibration of control channel of force on the FA gripper cable | 2∙10-3 |
| Errors in calibration of control channel of force on the cluster gripper cable | 2∙10-3 |
| Error in calibration of bridge position control channel | 2∙10-3 |

13. Results of reliability analysis (functional safety) of high-technology complex of TPE with nuclear fuel

Based on the developed logic-probability model of high-technology TPE with nuclear fuel for performing the required, minimum cut sets of failures represented in table 7 of this Appendix were formed.

**Table 7**

**Minimum failure cutsets of a high-technology facility TPE with nuclear fuel (fragment for function 2, results for function 1 are presented similarly)**

| **No.** | **Implementation probability in a year** | **Contribution, %** | **Failure of system element, personnel error** | **Failure of protections and interlocks** |
| --- | --- | --- | --- | --- |
| **Event 1** | **Event 2** | **Event 3** | **Event 4** |
| Failure of high-technology facility: Lateral impact of FA |
| 1 | 3.60∙10-7 | 49.67 | НЕ916R26 | - | - | - |
| 2 | 3.60∙10-7 | 49.67 | НЕ915R26 | - | - | - |
| 3 | 1.08∙10-9 | 0.15 | НЕ023R26 | FUZ1(4.1) | KM-ALL | - |
| 4 | 1.08∙10-9 | 0.15 | НЕ022R26 | FUZ1(4.2) | KM-ALL | - |
| 5 | 5.40∙10-10 | 0.07 | НЕ003R26 | FUZ1(4.2) | KM-ALL | - |
| 6 | 5.40∙10-10 | 0.07 | НЕ006R26 | FUZ1(4.1) | KM-ALL | - |
| 7 | 1.24∙10-10 | 0.02 | НЕ022R26 | FPSZВ | FUZ1(4.2) | FKМ3(5) |
| 8 | 1.24∙10-10 | 0.02 | НЕ023R26 | FPSZВ | FUZ1(4.1) | FKМ2(5) |
| 9 | 1.12∙10-10 | 0.02 | НЕ022R26 | FUZ1(4.2) | K5-ALL | - |
| 10 | 1.12∙10-10 | 0.02 | НЕ023R26 | FUZ1(4.1) | K5-ALL | - |
| 11 | 6.19∙10-11 | 0.01 | НЕ003R26 | FPSZВ | FUZ1(4.2) | FKМ3(5) |
| 12 | 6.19∙10-11 | 0.01 | НЕ006R26 | FPSZВ | FUZ1(4.1) | FKМ2(5) |
| 13 | 5.62∙10-11 | 0.01 | НЕ006R26 | FUZ1(4.1) | K5-ALL | - |
| 14 | 5.62·10-11 | 0.01 | HE003R26 | FUZ1(4.2) | K5-ALL | - |
| 15 | 3.27·10-11 | 0.00 | HE022R26 | FPSZB | FUZ1(4.2) | F2SQ7 |
| 16 | 3.27·10-11 | 0.00 | HE023R26 | FPSZB | FUZ1(4.1) | F2SQ8 |
| 17 | 1.88·10-11 | 0.00 | HE022R26 | CPU-ALL | F2BQ1 | FKM3(5) |
| 18 | 1.88·10-11 | 0.00 | HE023R26 | CPU-ALL | F2BQ2 | FKM2(5) |
| 19 | 1.88·10-11 | 0.00 | HE023R26 | FPSU | F2BQ2 | KM-ALL |
| 20 | 1.88·10-11 | 0.00 | HE022R26 | FPSU | F2BQ1 | KM-ALL |
| 21 | 1.63·10-11 | 0.00 | HE003R26 | FPSZB | FUZ1(4.2) | F2SQ7 |
| 22 | 1.63·10-11 | 0.00 | HE006R26 | FPSZB | FUZ1(4.1) | F2SQ8 |
| 23 | 1.38·10-11 | 0.00 | HE023R26 | CPU-ALL | FUZ1(4.1) | FKM2(5) |
| 24 | 1.38·10-11 | 0.00 | HE022R26 | CPU-ALL | FUZ1(4.2) | FKM3(5) |
| 25 | 1.29·10-11 | 0.00 | HE023R26 | FPSZB | FUZ1(4.1) | FK27(5) |
| 26 | 1.29·10-11 | 0.00 | HE022R26 | FPSZB | FUZ1(4.2) | FK27(5) |
| 27 | 1.07·10-11 | 0.00 | HE306R26 | FUZ1(4.1) | KM-ALL | - |
| 28 | 1.07·10-11 | 0.00 | HE302R26 | FUZ1(4.2) | KM-ALL | - |
| 29 | 9.39·10-12 | 0.00 | HE004R33 | CPU-ALL | F2BQ2 | FKM2(5) |
| 30 | 9.39·10-12 | 0.00 | HE001R33 | CPU-ALL | F2BQ1 | FKM3(5) |
| 31 | 9.39·10-12 | 0.00 | HE003R26 | F2BQ1 | VAR | KM-ALL |
| 32 | 9.39·10-12 | 0.00 | HE001R32 | F2BQ1 | VAR | FKM3(5) |
| 33 | 9.39·10-12 | 0.00 | HE003R26 | NEM | CPU-ALL | FKM2(5) |
| 34 | 9.39·10-12 | 0.00 | HE004R27 | CPU-ALL | F2BQ2 | OVA(5) |
| 35 | 9.39·10-12 | 0.00 | HE006R26 | FPSU | F2BQ2 | KM-ALL |
| 36 | 9.39·10-12 | 0.00 | HE004R32 | CPU-ALL | F2BQ2 | FKM2(5) |
| 37 | 9.39·10-12 | 0.00 | HE006R26 | CPU-ALL | F2BQ2 | FKM2(5) |
| 38 | 9.39·10-12 | 0.00 | HE005R27 | CPU-ALL | F2BQ1 | FKM3(5) |
| 39 | 7.87·10-12 | 0.00 | HE023R26 | FUZ1(4.1) | FKM2(5) | FKM9(5) |
| 40 | 7.87·10-12 | 0.00 | HE023R26 | FUZ1(4.1) | FKM2(5) | FKM10(5) |
|  |  |  |  |  |  |  |

The results of quantitative reliability analysis (functional safety) of the process facility of TPE with nuclear fuel for performing the required function 2 are given in the table 8 of this Appendix.

**Table 8**

**Results of reliability analysis (functional safety) of the process set of TPE with nuclear fuel for performing the required function 2**

|  |  |
| --- | --- |
| **Failure of high-technology facility** | **Probability of failure year over year** |
| Failures of high-technology facility related to CFF |
| Fall of CFF | 7.49·10-8 |
| End impact of CFF | 5.75·10-8 |
| Lateral impact of CFF | 4.67·10-5 |
| Failures of high-technology facility related to FA |
| Fall of FA | 5.40·10-8 |
| Compression of FA | 2.38·10-7 |
| FA bending force | 5.29·10-7 |
| Lateral impact of FA | 3.62·10-6 |
| Inadmissible upper position of FA | 1.36·10-12 |
| Tension of FA | 4.16·10-7 |
| Torsion of FA | 1.36·10-9 |
| Failures of high-technology facility related to TP |
| Fall of TP from SFA | 2.25·10-8 |
| Terminal impact of TP with SFA | 6.34·10-8 |
| Lateral impact of TP with SFA | 2.49·10-5 |
| Failure of high-technology facility for any reason |
| Cumulative failure probability of high-technology facility for performing function 2 | 7.67·10-5 |

14. Conclusions and recommendations following reliability analysis

The standard specified reliability indices have not been stipulated for the high-technology complex, hence the reliability analysis results are not compared with them.

The design requirements to the reliability indices (presented in the technical assignment) have been stipulated for the high-technology complex. The carried out analysis shows the compliance of the high-technology complex with the requirements for the reliability indices both in performing the function 1 and in performing the function 2.

From the analysis the supplementation of RM with interlocks protecting against implementation of the dominating minimal cut-sets (a list of interlocks recommended in addition to the implementation, as well as additional measures for reducing the probability of personnel errors forming part of the dominating minimal cut sets (a list of personnel errors and recommended measures for reducing their probabilities is given; they may include for example, correction of operation documentation, supplementation of the personnel training program) shall be recommended for consideration.

15. References

The reference list is given.

Appendix No. 11
to the Safety guide in the use of atomic energy “Recommended procedure for NPP safety-related systems and elements reliability analysis, and their functions" approved by the order of the Federal Environmental, Industrial and Nuclear Supervision Service No. 26
dated January 28, 2015

**Recommendations for use of probabilistic methods of fracture mechanics to reliability assessment of passive elements**

Fig. 1. Passive element failure probability determination diagram

If all the computed values may be divided into two groups, where the first includes the characteristics related to the properties of the construction, and the second characterizes the external impacts, then in the appendix to the calculation tasks for strength the failure condition mathematically shall be expressed by the inequation:

*g*(*x*1,*x*2,...,*xn*)=*R*(*x*1,*x*2,...,*xm*)-*Q*(*xm*+1,*xm*+2,...,*xn*)<0

or

*g*=*R*-*Q*<0, (1)

where:

*g* - operability function or strength margin;

*R* - load bearing capacity expressed in the same units as the loading effect *Q*;

*Q* - loading effect.

At any distribution laws of R and Q the mathematical expectation and standard deviation of strength reserve are respectively equal to:

|  |  |  |
| --- | --- | --- |
| $$m\_{g}=m\_{R}-m\_{Q}, s\_{g}=\sqrt{s\_{R}^{2}+S\_{Q}^{2}},$$ |  | (2) |

where *mR* and *sR* – mathematical expectation and distribution standard of loading capacity;

*mQ* и *sQ* – mathematical expectation and distribution standard of loading effect.F

For normal distribution of random quantities the failure probability Pf is determined using the formula:

*Pf* =1-Φ(*β*), ( 3 )

where:

Φ(*β*) – tabulated Gaussian integral,

$β=\frac{m\_{g}}{s\_{g}}=\frac{m\_{R}-m\_{Q}}{\sqrt{s\_{R}^{2}+s\_{Q}^{2}}}$ – safety characteristic (number of standards *sg*, confined in the interval from *g* = 0 to *g* = *mg* ).

The expression for determining the safety characteristics may be written as:

|  |  |  |
| --- | --- | --- |
| $$β=\frac{n-1}{\sqrt{n^{2}∙v\_{R}^{2}+v\_{Q}^{2}}},$$ |  | (4) |

where:

$n=\frac{m\_{R}}{m\_{Q}}$- safety factor;

*νR* – variation coefficient of load-bearing capacity;

*νQ* – variation coefficient of loading effect.

The following approach may be used for determining the moments (mathematical expectation and standard deviation) of load bearing capacity and loading effect. The standard values of the strength characteristics of materials Rn determined experimentally on the assumption of normal distribution law with confidence probability of exceedence 0.95 are given in the calculation standards, Assuming that the calculated values of the strength characteristics of materials R have the confidence probability of exceedence 0.99865, the mathematical expectation and standard may be determined from the system:

|  |  |  |
| --- | --- | --- |
| $$\left\{\begin{array}{c}R\_{n}=m\_{R}-1,64∙s\_{R}\\R=m\_{R}-3∙s\_{R}\end{array}\right.,$$ |  | (5) |

Then

$$m\_{R}=R\_{n}+1,64∙\frac{R\_{n}-R}{1,36}=R\_{n}∙\left(1+1,64∙\frac{1-\frac{1}{γ\_{m}}}{1,36}\right),$$

$$s\_{R}=\frac{R\_{n}-R}{1,36}=R\_{n}∙\left(\frac{1-\frac{1}{γ\_{m}}}{1,36}\right),$$

where

$γ\_{m}=\frac{R\_{n}}{R}$- material reliability factor (margin).

A similar approach may be used for determining the mathematical expectation and standard deviation of a series of static loads.

Another approximative method - first order reliability method (FORM) is based on the expansion of the operability function into Taylor series in the environs of mathematical expectation of random quantitie and retention of only the linear expansion terms. For the linear operability function *g=g(x1, x2,..., xn)* the expansion to Taylor series shall be as follows:

|  |  |  |
| --- | --- | --- |
| $$g≈g\left(m\_{x\_{1}},m\_{x\_{2}},…,m\_{x\_{n}}\right)+\sum\_{i=1}^{n}\frac{∂g}{∂x\_{i}}\left(m\_{x\_{1}},m\_{x\_{2}},…,m\_{x\_{n}}\right)\left(x\_{i}-m\_{x\_{i}}\right)+\tilde{W}$$ |  | (6) |

where *W* - non-linear expansion terms.

The expansion is made in the distribution center environs, and the non-linear terms may be ignored. This is due to the fact that on modest distance from the center of distribution the contribution of non-linear terms is not significant, and at a considerable distance the values of the distribution functions are quickly damped. Then the initial performance capability function may be replaced by the linear dependency:

|  |  |  |
| --- | --- | --- |
| $$g=g\left(m\_{x\_{1}},m\_{x\_{2}},…,m\_{x\_{n}}\right)+\sum\_{i=1}^{n}\frac{∂g}{∂x\_{i}}\left(m\_{x\_{1}},m\_{x\_{2}},…,m\_{x\_{n}}\right)\left(x\_{i}-m\_{x\_{i}}\right)$$ |  | (7) |

Numerical characteristics for linear performance capability function shall be determined according to the formulae:

|  |  |
| --- | --- |
| $$m\_{g}=g\left(m\_{x\_{1}},m\_{x\_{2}},…,m\_{x\_{n}}\right), s\_{g}^{2}=\sum\_{i=1}^{n}\left(\frac{∂g}{∂x\_{i}}\left(m\_{x\_{1}},m\_{x\_{2}},…,m\_{x\_{n}}\right)\right)^{2}s\_{x\_{i}}^{2}.$$ | (8) |

After finding the numerical characteristics, the failure probability is calculated according to the formula (3) of this appendix.

In some practical tasks the variation range of random arguments is not as small so that the function in its limits could be linearized with adequate accuracy. In these cases, the method based on the retention in the function expansion of not only the linear terms but also certain succeeding terms of higher orders and errors linked to these terms may be applied for verification of the applicability of the method and for specification of the obtained results.

The most universal are the statistical modelling methods, which allow simulate any process, the random factor impact on the flow thereof. The basic idea of the methods is the relation between the probabilistic characteristics of various random processes and quantities being the decisions of tasks of mathematical analysis (for example, values of the intervals, solutions of the differential equations). The value of the corresponding probabilities or mathematical expectations may be experimentally determined instead of the calculations of several complex analytical expressions. It should be noted that the special features of this method consists in the fact that error assessment of the calculations is of probabilistic nature. In this method it is prohibited to assert that the error exceeds some value, but only can specify the boundaries outside thereof the error shall not go outside the probability close to one.

Appendix No. 12
to the Safety guide in the use of atomic energy “Recommended procedure for NPP safety-related systems and elements reliability analysis, and their functions" approved by the order of the Federal Environmental, Industrial and Nuclear Supervision Service

No. 26 dated January 28, 2015

**Additional information for performing software reliability analysis**

1. The basic factors impacting the software safety shall include:

software interface with external medium (software and hardware facilities, translators, operation system);

interface with a person (developer or user);

SW arrangement (design, problem definition and methods of achieving and implementing them) and quality of its development This factor exerts the maximum influence on software reliablity.

testing,

2. The reasons of SW failures are errors in determining the engineering specifications for SW, errors in the program, errors in calculation, logic errors, input/output errors, compilation errors, user errors, defects of software module loaded into the SW memory caused by physical reasons, improper use of the software, conflict with the operation system etc.

Errors in SW Not always it is possible to detect and eliminate all the errors at the testing stage. For this SW, inspite of the performed quality assurance procedures, may fail, if in operation a combination of input data or modes occur that is not provided for during the testing. For example, the syntactical incompatibility may be caused by nonconformities in the methods of data assignment at the programming language level;

The calculation errors include for example, wrong encoding of the forms, errors in signs (arithmetic), continuous transformation. SW failure appears following calculation errors in the form of miscalculated result.

The logic errors include for example, misrepresentation of control, errors in the formation of search conditions. Logic errors shall lead to distortion of data processing algorithm. They also include semantic non-compatibility of the modules of SW used, which occurs when identical well-formed symbols are used for denoting different concepts.

The input-output errors for example refer to the invalid data formats, incorrect indication of the placement on screen or paper, incorrect allotment of the number of charges,

Compilation errors may be caused by compiler defect.

The errors of users include, for example, misunderstanding of the instruction output, input of invalid data.

The defects of the SW module loaded into the memory caused by physical reasons may be related to the failures in the operation of storage cells, distortion of information in the communication channels.

Incorrect use of the SW may take place, if the SW developed earlier is use, for example, after upgrading the hardware

Conflict with the operation system may occur due to limitations of parallel operation and access to the external resources or non-compliances with the requirements to synchronization determined by the possibilities of the hardware part of the system and user interface. Since the managed processes at the NPP have a complex multi-tier nature, the control system SW is multi-tasked, when it is simultaneously required to implement complex control algorithms of various facilities installed at the NPP. In simultaneous performance of several tasks it is required to divide the computing system resources depending on their priority and various event related to the specific tasks. This may be the reason of conflict.

3. SW reliability models

The SW reliability modes are divided into analytical and empiric.

The analytical reliability models of SW give the possibility to calculate the quantitative reliability indices based on the data about program behavior in the testing process. The analytical models are presented by two groups: dynamic models and static models. The behavior of SW (appearance of failures) in the dynamic models is considered in time. In the static models the failure appearance is not connected with time, but only the dependency of the number of errors from the number of test runs (in the field of errors) or dependency of the number of errors from the characteristics of input data (in the data field) are considered. The dynamic models in particular shall include the Schumann Reliability Model [10,11, 12], Software Reliability Growth Models or SGRM-models [13]. The static models in particular shall include the Mills Reliability Model [10, 14], Lipov Reliability Model [9, 10, 15], Bernoulli Sequential Testing Model [10, 11, 16].

Both the groups of analytical models are an extrapolation of the testing process for real operation conditions of SW. The models may be adequate, only if the testing and operation conditions are comparable, such as reliability of SW may change sufficiently strong depending on these conditions.

The SW reliability growth models (most popular) are based on the testing results of the SW versions in the process of its testing (with correction of identified errors) up to the final software test. After identification of the failure SW usually is corrected, hence its reliability does not change. The identified trend of reliability change (usually enhancement) is extrapolated for predicting the current reliability level and its change in the future (functioning up to the next failure and time required for identifying all the errors in the SW). The SW growth models are based on two basic assumptions: failures are recorded in chronological order, and all the errors detected in the SW are corrected. In using these models the severity of the detected failure of SW is usually not considered, i.e. the real failures and small defects are not distinguished. These models are sufficiently subjective, and the determined reliability trends depend on the changes in the testing process (for example, possible change of the scope of group of specialists participating in the SW testing, or integration of new functional possibilities in the SW). The time of identification of the last SW failure shall also render sufficiently large influence on the nature of the trend. Both the assumption that the reliability growth curve tends to the absolute reliability level, and the assumption that there shall always be some residual number of failures which is caused by additional errors, entered in correcting the earlier identified software failures may be taken in the models.

The empiric reliability models of SW are based on the analysis of structural features of the SW. They consider the dependency of reliability indices from the number of inter-module communications, number of cycles in the modules etc. The empiric models often do not give the end results of the reliability indices, however the use of these models allows identify the interrelation between the SW complexity and its reliability. These models may be used at the SW design stage, when the modular decomposition is made and its structure is known.

Regulatory Document

**Safety guide
in the use of atomic energy**

"Recommendations on the procedure for reliability analysis of safety-related NPP systems and components and their functions"

RB-100-15

**Official publication**

Responsible for the issue - T.V. Sinitsyna

The makeup is performed at FBE SEC NRS in full accordance with the appendix to the order of the Federal Environmental, Industrial and Nuclear Supervision Service No. 26 dated January 28, 2015

Passed for printing dd. 05.02.2015

The Federal State-Funded Institution Scientific and Engineering Center for Nuclear and Radiation Safety (FSI SEC NRS) is an official publisher and distributor of the by-laws of the Federal Environmental, Industrial and Nuclear Supervision Service (Order of the Federal Environmental, Industrial and Nuclear Supervision Service No. 384 dated 20.04.06 )

Number of copies: 100

Printed in FBE SEC NRS

Malaya Krasnoselskaya Str., 2/8, block 20, Moscow

Editorial office phone number: 8-499-264-28-53

1. Developed by a team of authors comprising of: M.Yu. Lankin, Ph.D in Engineering Sciences, G.I. Samokhin, Ph.D in Engineering Sciences, D.E. Noskov, A.A. Marienkov (FBU NTTs YaRB Moscow) G.A. Ershov Professo, Doctor of Engineering Sciences (Atomproekt OJSC, St. Petersburg), G.V. Tokmachev Ph.D in Engineering Sciences, I.V. Kalinkin, R.V. Yuriev Ph.D in Engineering Sciences, E.V. Baikova (Atomenergoproekt OJSC, Moscow), I.A. Bylov Ph.D in Engineering Sciences (OKBM Afrikantov OJSC, Nizhny Novgorod), A.V. Antonov, Professor, Doctor of Engineering Sciences (IATE NIYaU MEPhI, Obninsk). [↑](#footnote-ref-1)