ELECTRONIC JOURNAL
OF INTERNATIONAL
GROUP ON RELIABILITY

10 YEARS

JOURNAL IS REGISTERED
IN THE LIBRARY
OF THE U.S. CONGRESS

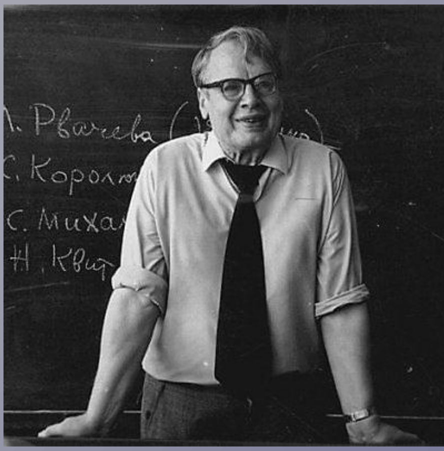
•

ISSN 1932-2321

•

VOL.12 NO.1 (44)
MARCH, 2017

Gnedenko Forum Publications



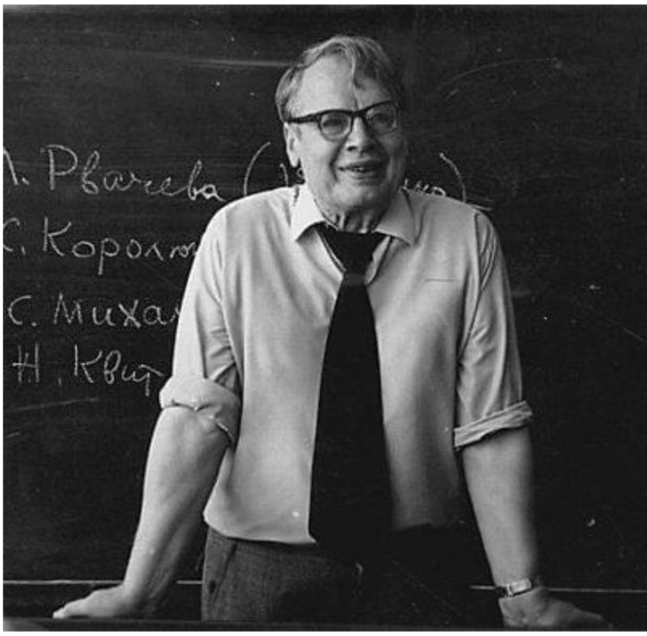
RELIABILITY:
THEORY&APPLICATIONS

San Diego

ISSN 1932-2321

http://www.gnedenko-forum.org/Journal/index.htm

Journal of International Group on Reliability



RELIABILITY:

THEORY & APPLICATIONS

Vol.12 No.1 (44),
March, 2017

San Diego
2017

Editorial Board

Editor-in-Chief

Managing Editors

Deputy Editors

Associate Editors

e-Journal ***Reliability: Theory & Applications*** publishes papers, reviews, memoirs, and bibliographical materials on Reliability, Quality Control, Safety, Survivability and Maintenance.

Theoretical papers have to contain new problems, finger practical applications and should not be overloaded with clumsy formal solutions.

Priority is given to descriptions of case studies.
General requirements for presented papers

1. Papers have to be presented in English in MS Word format. (Times New Roman, 12 pt, 1 intervals).
2. The total volume of the paper (with illustrations) can be up to 15 pages.
3. A presented paper has to be spell-checked.
4. For those whose language is not English, we kindly recommend to use professional linguistic proofs before sending a paper to the journal.

The Editor has the right to change the paper title and make editorial corrections.

The authors keep all rights and after the publication can use their materials (re-publish it or present at conferences).

Publication in this e-Journal is equal to publication in other International scientific journals.

Papers directed by Members of the Editorial Boards are accepted without referring.
The Editor has the right to change the paper title and make editorial corrections.

The authors keep all rights and after the publication can use their materials (re-publish it or present at conferences).

Send your papers to Alexander Bochkov, e-mail: a.bochkov@gmail.com

Table of Contents

EDITORIAL

Dear Readers and the Authors of the Journal,

For the preceding year in the life of Gnedenko Forum and our journal there were essential changes. The President of the Forum came off duty and the members of the Editorial Board of the journal were considerably renewed. We hope that all of us together not only will keep spirit and the atmosphere of our journal, but also, we will manage to give to the business begun by Igor Ushakov, a new impulse.

Since January 2006, Gnedenko Forum began releasing its quarterly electronic journal «Reliability: Theory & Applications» (RT&A). The journal is registered in the Library of Congress (ISSN 1932-2321). Over 10 years since the publication of the first issue, in 43 issues of the journal over 400 articles have been published. Articles undergo a compulsory stage of editing and are published in PDF format on the journal's website. The journal publishes articles, reviews, memories, information and bibliographies on theoretical and applied aspects of reliability and quality control, security, survivability, maintenance and methods of analysis and risk management. Preference is given to the editorial board materials, reflecting the practical application of these methods in the articles of a theoretical nature must necessarily contain new problems designation practical application and should not be excessive use of formal calculations.

The editorial board of the journal includes scientists and experts who are recognized experts in their fields of activity and well versed in the essence of the problems discussed in the journal.

Publication in the RT&A is equivalent to publication in scientific journals. Articles recommended by the members of the editorial board for review are routed. The editors reserve the right to change the title of the article, as well as spend editing. The author retains full right to use their materials after publication in the journal of your choice (to send them to other publications, to submit to conferences, etc.).

The editorial board of the journal carries out reviewing of all articles presented to the journal. Now, the journal is included into the Russian Science Citation Index information base and we are planning its inclusion into SCOPUS and Web of Science bases.

Being the "information window" of Gnedenko Forum the RT&A promotes implementation of the mission of Forum including:

- Establishing sustainable development of the professional contacts among experts, young specialists and prospective students around the world in the field of reliability and applications. Publication and dissemination of personal information and news about members and participants;
- Publishing scientific and essential technical achievements in peer reviewed papers in the Forum’s e-journal;
- Exchanging information between Member and participants of Forum:
- Information about new publications of books and other journals (review papers and/or other forms of personal information);
- Announcements about international conferences, meeting, symposiums, lectures, new books, job offers, professional development and other current or modern events in this field;
- Helping the Forum members in getting job, consulting, grants, funded research etc.;
- Collaborating in organization of conferences, meetings, symposiums;

- Working on foundation of an International Gnedenko's school for professional development of researchers and practitioners in support of Gnedenko scholars, pupils of their pupils. *(Gnedenko Brand is one of the most valuable and vital peculiarity in the Forum)*;
- Organization of discussions around some of important questions;
- Creation of the Forum free e-library.

The experience of journal releasing for more than 10 years and real-life communication of experts and young researchers at the Forum show that Igor Ushakov's idea about informal union of experts in the field of the theory of reliability and risk analysis was fruitful and viable.

Ten years are sufficient term for intermediate summarizing. We won't confirm that everything turned out as it had to be and how it was planned. We are far from anniversary self-complacency. Besides, despite solidity, ten years are not anniversary at all but it is rather the reason to estimate whether we are moving to intended success or the business was too heavy to lift. We think that you support us in confidence that we did right thing, the mission of the journal is demanded, and it surely carries it out. It's our general merit: both activities of the editorial board, and the authors who send original and attractive articles and the problem of selection of texts for the publication becomes very difficult, but very interesting. You can distinctly see on the pages of our journal the mutual enrichment process of somniferous knowledge in the field of the theory of reliability, risk analysis and their appendices.

We are sure that the next years will become very fruitful for those whose area of professional interests relates to questions of reliability and risk analysis.

Thanks to all who have passed this ten-year way with us, helping us to find self-confidence and to become useful to scientific community, we are ready and we want to move surely together with you further!

Vladimir Rykov

Alexander Bochkov

Ekaterina Gnedenko

Fukushima Lessons for Safety of Critical Control Systems

Prof. Mikhail Yastrebenetsky,
Dr. Alexander Klevtsov,
Yuri Rozen,
Serhii Trubchaninov

State Scientific and Technical Center for Nuclear and Radiation Safety (SSTC NRS)
53, Chernishevska str., of.2, 61002, Kharkov, Ukraine
E-mail: ma_yastrebenetsky@sstc.com.ua

Abstract

The accident at Japan nuclear power plant (NPP) "Fukushima-Daiichi" has influenced not only to future development of the nuclear energetics as whole and different NPP systems (including, of course, their control systems). However, the lessons of this accident are important for safety of critical control systems in different branches of industry. Some propositions for their safety assurance followed from nuclear post-Fukushima experience are discussed below.

Key words: Fukushima, safety, control system, accident, earthquake.

Russian academician Boris Chertok, a designer of control systems for space vehicles, including the vehicle for the first cosmonaut Yuri Gagarin, noted subsequently: "When I wrote these memoirs, I have received validity of the statement that catastrophic, accident-related and off-nominal situations are one of the most powerful stimulus of the cosmic technics progress speeding up" [1]. This statement takes place not only for space, but for other branches of technics, where safety problems are very important. Meanwhile, catastrophic, accident-related and off-nominal situations in one branch, where there are critical control systems, can affect to critical system's[1] progress in the other branches of technics.

The accident on Japan NPP "Fukushima-Daiichi" in 2011 (so as accidents on NPP "Three Miles Islands" in the USA in 1979 and on Ukrainian NPP "Chernobyl" in 1986) exerted an essential influence on the development of safety activity not only for nuclear energy, but for different branches of the industry.

The reasons of the Fukushima accident had natural types. This accident was caused by the combination of off-design earthquake and tsunami. The signals about the earthquake entered the reactor control systems, resulted in an emergency shutdown of all units. The reserve diesel-generators were started-up after the loss of external power supply. However, the technological safety systems for reactor core cooling ceased their actions: the power supply commutators from normal supply to reserve diesel-generators were installed in flooding area. The design mistake was added: the spent fuel pools for the most dangerous nuclear fuel were outside of reactors containment. The nuclear fuel was overheated and the reactors were destroyed. The Fukushima

[1] Systems which purpose is the prevention of the equipment, machinery, plants from going into a dangerous state by taking appropriate actions on the receipt of the commands are known as the critical systems

accident did not have direct connections with mistaken actions of reactor control systems. But this accident leads to necessity to pay attention to a lot of new problems related to NPP safety of critical control systems and to such systems not only for NPP.

There are many publications devoted to Fukushima lessons for nuclear energy (e.g. [2-5]). These lessons were analyzed by international organizations in the nuclear energy area, first of all- International Atomic Energy Agency (IAEA), and by all countries where NPP are operated. These lessons

have a technical character (as set of actions on assessment and increasing of NPP safety), as well as a political character (related to the refusal from the building of new NPP or the discontinuation of existing NPP's operation). As opposed to the publications where lessons from the NPP Fukushima accident were analyzed for nuclear application, the lessons for safety of critical control systems (CCS) for other branches of industry will be considered below in this paper. Examples of these branches are chemical, petrochemical and gas industries, gas and oil transport, etc. The consideration of the main principles of NPP safety assurance will proceed with these lessons.

The principles of NPP safety assurance

The principles of NPP (including their control systems) safety assurance are described in IAEA documents [6-8] and in the national documents of different countries (e.g. [9]).

- There are special state organizations in all countries where NPP's are operated. The aim of these organizations is the regulation of the nuclear and radiation safety. These organizations are independent from NPP, from NPP designers or developers and suppliers of NPP equipment. The general name of these organizations is "Regulatory body", but official names are various in different countries (e.g., "Nuclear Regulatory Commission" in USA). Regulatory bodies fulfill different functions with the aim to create of regulatory mechanism for nuclear and radiation protection of people and the environment. The control of every NPP safety is realized not only by NPP equipment and personnel, but by Regulatory body as well - by central office and by their representatives who constantly are located at NPP sites. One of the functions of Regulatory body is the realization of the independent expert reviews for research, testing and analysis of compliance of all safety important NPP systems and components (including, of course, control systems and their components) with the requirements to nuclear and radiation safety. General diagram of NPP unit safety control is presented in fig.1. On this fig. 1 are shown the following elements:

1. The influence of the external environment to the NPP (from power consumers, earthquakes, flooding, dropping of an airplane, etc.).
2. The information about the technological equipment conditions entered to the control system.
3. The control action from the control system to the technological equipment.
4. The information about the technological equipment and the control system conditions, which represented to NPP operating personnel.
5. The control action from NPP operating personnel to the control system.
6. The information from the control system and NPP operating personnel about safety important parameters, which represented to the NPP administrative-technical personnel.
7. The information (directives) from NPP administrative- technical personnel represented to NPP operating personnel.
8. The information about parameters which defined unit safety, which represented in Regulatory body.
9. Directives of Regulatory body (safety standards, safety reviews, results of supervision by representatives of Regulatory body at the NPP site, etc.) to NPP administrative-technical personnel.

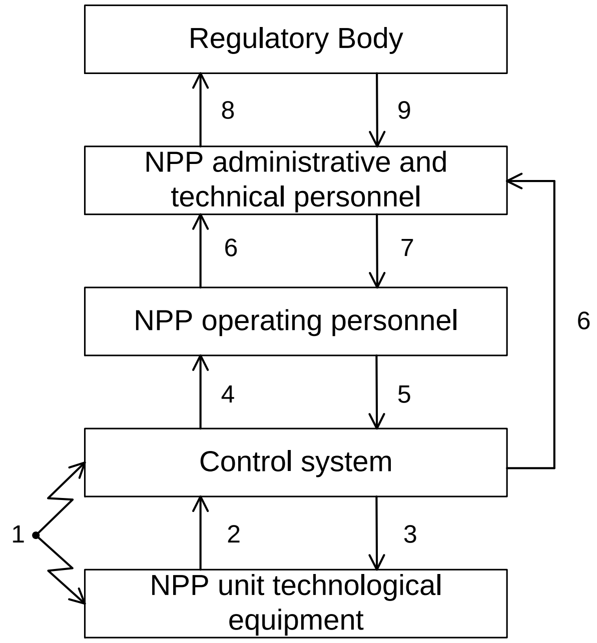

Regulatory Body
8
9
NPP administrative and technical personnel
6
7
NPP operating personnel
6
4
5
Control system
1
2
3
NPP unit technological equipment

Figure1. General diagram of NPP unit safety control

- The operating organization ensures NPP safety and bears full responsibility for it, including the measures to prevent the accidents and mitigate their consequences, the inspection of nuclear materials and radioactive substances, the protection of the environment. This responsibility doesn't reduce connection with independent activity and responsibility of the designers, suppliers, builders and the Regulatory body.
- Observance of normative documents (norms, rules, guidelines, standards, etc.), which pertain to NPP safety, is mandatory in carrying out of all kinds of activity related to the use of nuclear power. One can agree that the necessity of a special permission system in this field of relationships replaces the popular democratic principle of "everything is permitted that is not prohibited in particular" with the opposite one - "everything is prohibited that is not permitted in particular".
- Fundamental principle of NPP safety assurance is "defense in depth" which based on:
  - the system of physical barriers, which assure the possibility of continuous prevention of the release of the ionizing radiation and the radioactive substances into the environment;
  - the system of levels of technical and organizational measures to protect the physical barriers and preserve their effectiveness for the purpose of protecting the personnel, the population and the environment.
- One of the factors that substantially influences on NPP safety is activity of IAEA – the international organization which is connected by an Agreement with the United Nations Organization. Activity of the IAEA consists in emergency assistance in case of accidents, technical cooperation, information exchange, different inspections of NPP and suppliers (examples: missions of NPP control systems independence review in the Republic of Korea, Russia and Ukraine), training of personnel, and also development of IAEA safety standards coordinated at an international level.

Propositions for the control systems safety improvement

The aim of this section and this paper as a whole isn't the recommendations for implementing post-Fukushima actions for the concrete equipment under control (EUC) and the concrete EUC control systems. But the aim is to draw attention of safety specialists on post-Fukushima actions for following evaluation of the possibility of implementing these actions in non-nuclear EUC.

- After the Fukushima accident the reassessment of the safety vulnerabilities of NPP took place in the light of lessons learned from the accident. These actions for different types of NPP systems (including control systems) received the name "stress-tests" - the additional checkup based on the design documents, the safety analysis reports, the performed researches, the expert assessments, the tests and the engineer assumptions by taking into account more severe impacts and the possible overlap of negative factors. The initiating events conceivable at the plant site are earthquake, flooding, and other extreme natural events (e.g., extreme high and low temperature).

The most important initiating event that leads to the accident was the earthquake, exceeding the design basis. Earthquake in Fukushima forced to the revise parameters of the seismic influence spectrum. After the Fukushima accident, seismic analysis of control systems equipment was fulfilled for all NPP's. During this analysis was taken into account the accelerograms of the ground for maximum earthquake, the coefficient of building constructions damping, the height of placing, the intermediate constructions (the panels, the desks, the consoles, the technological equipment, if the devices were mounted on them), ageing. The analysis covered all components of the NPP safety important control systems (e.g. a control system for the emergency diesel-generators), including not only devices, but electrical and optical cables in the places of their connections with hardware devices. The requirements for the testing impact, which imitate of the earthquake response spectrum, became tougher.

This practice may be recommended for the critical control systems for the different EUC located in the places where earthquakes are possible. It should be noted, that one of the first investigations devoted to analysis of mechanical impacts to hardware was fulfilled by Igor Ushakov with his colleague Yuri Konenkov [10].

- The Fukushima accident had shown the necessity of the taking into account not only of possible influence taken separately, but also the combination of the different extreme influences (fire, extreme high/low temperature, flood, tsunami, tornado), as well as the common cause failures of control systems due to the extreme influences and their effects. The requirements for the defense in depth, reservation, diversity, independence have to be determined by the accounting of the combination of these influences.

- The identification of dangerous events is actual task as well. Some of the control systems should detect dangerous external and internal events, which can lead to extreme influences on equipment and initiate the operation of the actuating systems for the minimization of the risk from these influences. The failure of these systems (components) with the high probability leads to the abnormal situation what can grow into accident. The examples are seismic sensors, which have to identify earthquakes. It is necessary to make the reassessment, which confirms compliance of these sensors with new, more severe requirements. The actual problem for seismic sensors is the experimental validity of sensor response to different forms of the spectrum acceleration on the sensor input.

- After the Fukushima accident took place loss of external power supply because of the earthquake. The next event was loss of internal power supply from 13 diesel-generators because of the tsunami. These events led to full de-energization of all NPP units and reactor cores were melted. The most of control system instruments remained unbroken, but the absence of power supply by either direct or indirect current provoked a full loss of the information. The main control room and the supplementary control rooms were useless due to loss of power supply. It's interesting to describe some measures, which were already realized or planning to realization in future to avoid the same situation:

  - The development of indicating and recording devices for the most important safety parameters, which can operate regardless of general power supply of the equipment under control. It is necessary to provide the autonomous power supply for these devices during some time after the accident. Another further way is a creation of the sensors which can operate without an external supply (e.g. receiving energy thanks to high temperature on the placement of location);

- The installation of the special mobile and moveable individual diesel-generators for power supply in the case of fault of the stationary diesel-generators.

- The necessity of NPP control assurance by the personnel after accident (the control rooms "habitability"). A destruction of infrastructure near control systems, including communication cables and channels of data communication should be taken into account.

- There is a new type of NPP control system – post-accident monitoring systems (PAMS). PAMS began to operate before Fukushima accident, but these systems received wide distribution after this accident. PAMS realizes support of NPP personnel and safety experts during and after accident for:
  - receiving of information about the type and the time of the initiating events appearance, the violations of operating limits and conditions, the emergency situations and accident development;
  - receiving information about the state of safety important constructions, systems and elements, the values of technological parameters, about radiological conditions of environment;
  - the elimination of the accident consequences;
  - return of reactor facility to controllable state;
  - following analysis of the causes and the ways of the passing of design basis and beyond design basis accidents;
  - saving of archive data about accident against premeditated or unpremeditated alternations.

PAMS should provide acquisition, archiving, saving, displaying and registration of information in severe conditions, during internal and external influences after an emergency, including accidents. Now International Electrotechnical Commission (IEC) is elaborating international logo-standard IEEE/IEC devoted to PAMS on the base of the Institute of Electrical and Electronic Engineers (IEEE) standard [11]. NPP's experience in the creation of PAMS may be useful for some branches of industry (e.g., chemical and petrochemical).

- After the Fukushima accident the standards related to safety of NPP control systems were revised by many organizations. New IAEA standard related to NPP control systems safety, issued in 2016, is described in the paper [12] in this Journal. The authors of this paper were the heads of the international team, which elaborated this standard. The Technical Committee "Nuclear Instrumentation" of IEC made changes in their set of standards, as well as the Regulatory bodies of many countries. For example, new Ukrainian standard [13], related to NPP safety important control systems, established new regulatory requirements for these systems:
  - the requirements to archiving and storage of the data needed to analyze the accident causes and progress, which should remain intact under any possible effects during the design and beyond design basis accidents;
  - the seismic resistance classification criteria and rules for modeling the seismic impact under seismic resistance testing are established. They take into account conservative assessment of the damping coefficient of the building structures in defining their response to the ground movement, etc.

It may be recommended for designers of critical control systems in the other branches of industries to take into account some of provisions of these standards (of course, taking into account the branch specifics).

- It should be noted that one of possible directions for NPP safety increasing, accident management and post-accident monitoring is the use of wireless technologies, which give some advantages in comparison with traditional cable links:
  - The possibility of placing of wireless sensors in places where the use of cables is complicated or impossible;
  - increasing of reliability of data transferring from wireless sensors by means of excluding of the potential possibilities of cables damages (particularly, in accident conditions);

- increasing of mobility by means of easy replacing of wireless devices;
- the possibility of installation of any quantity of additional sensors for more accurate monitoring or in case of failures of the operated sensors.

Without doubt, the use of wireless technologies on NPPs requires the solution of some technical problems (supply with electrical power, high data transfer rate, resistance to electromagnetic interferences, protection of information, etc.), approbation, nuclear and radiation safety assurance and development of an appropriate regulatory framework. However, this is a prospective direction for further research.

Conclusions

The Fukushima accident lessons which were used for safety of NPP control systems could be applied for development and manufacturing of components, for design, integration, tests, operation of critical control systems not only for NPP, but for critical control systems in the other branches of industry.

References

1. Chertok B. Rockets and people. Moon race. Moscow, Mashinostroenie. 1998. (In Russian)
2. The Fukushima Daiichi Accident. Report by the Director General and Technical Volumes. Vienna, IAEA, 2015.
3. Way Kyo. Energy: Environmental Protection and Safety in the Wake of the Fukushima Nuclear Accident, John Wiley & Sons, 2012.
4. G. Johnson (Editor). Severe Nuclear Accidents: Lessons Learned for Instrumentation, Control and Human Factors. Electric Power Research Institute, Technical report, 3002005385, Palo Alto, CA, USA, 2012.
5. M. Yastrebenetsky, Y.Rozen, A.Klevtsov, S.Trubchaninov, V.Lebedynskiy, V.Martinenko, S.Lebedynskyy. Fukushima Accident Lessons for I&C Systems 8th International Topical Meeting on Nuclear Power Plant Instrumentation and Control, and Human-Machine Interface Technologies (NPIC&HMIT 2012), American Nuclear Society, San Diego, 2012.
6. IAEA Fundamental Safety. Principles Safety Fundamental. SF-1. Vienna, IAEA, 2006.
7. Safety of Nuclear Power Plants: Design. SSR- 2/1. Vienna, IAEA, 2016.
8. Safety of Nuclear Power Plants: Commissioning and Operation. SSR- 2/1. Vienna, IAEA, 2016
9. General Provision of Nuclear Power Plants Safety. NP 306.2.141-2008. Ukrainian State Committee of Nuclear Regulation. Kyiv, 2008. (In Ukrainian).
10. I. Ushakov, Yu.Konyonkov. Reliability of Mechanical Equipment. (part1,2). Znanie, Moscow, 1973, 1974. (In Russian).
11. IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations. IEEE Std 497™-2010.
12. G.Johnson, A.Duchac. The development of the new IAEA safety guide for design of instrumentation and control systems for nuclear power plants. Reliability: Theory and Applications. 2017, 1.
13. Requirements for nuclear and radiation safety of instrumentation and control systems important to safety of nuclear power plants. NP 306.2.202:2015. Official Bulletin of Ukraine, 2015, No.56 (In Ukrainian).

Adaptive Fault Tolerance in Real-Time Information Systems

Shubinsky I.B., Rozenberg I.N., Papic L.

Russia, Moscow, JSC NIIAS, Serbia, Prijevor, ICDQM

Abstract

Real-time information systems (IS) control mission-critical processes. Violation of functioning in these systems may lead to dangerous errors in control and to intolerable risks. The general disadvantage of traditional ways of IS reliability assurance is an autonomous implementation of fault tolerance mechanisms, as well as breaks of calculation which is unacceptable for real-time systems. All known ways to assure IS reliability are based on the application of large volumes of artificial structure and information redundancy. The technology of adaptive fault tolerance proposed in this article consists in the active use of natural time and structure redundancy, as well as in the active (and automatic) reassignment of available computer power not only for operational processing of information, but also for implementation of observability of the system under the conditions of limited control means. The technology of adaptive fault tolerance in information systems when solving real tasks in limited time conditions provides for a timely automatic detection and handling of failures and glitches by means of operational localization of faulty computation modules and by subsequent automatic rearrangement of the system with removal of faulty modules from the process of functioning.

Keywords: Information system, computation modules, faults, failures, errors, reliability, fault tolerance, beats of active protection, reassignment of modules, adaptation to failures, automatic control, comparison of results, failure detection, rearrangement, process recovery.

I. Introduction

Real-time information systems (IS) control mission-critical processes. Violation of functioning in these systems may lead to serious errors in control and to intolerable risks [1]. Main causes of dangerous errors in control processes are known – these are glitches and software errors, data errors, failures of a system's equipment [2]. That is why to assure a reliable task solution under the conditions of failures, two essentially different approaches are applied – recovery of the solution after a failure of the system (or its component) and prevention from the system failure (fault tolerance). In real-time systems termination of the control process for the time necessary to recover the system functioning is in most cases unacceptable – the main way of the reliable solution of control tasks is to assure fault tolerance.

Traditional ways to assure fault tolerance are as follows: *reservation of resources* (for instance, computation modules (CM); *protecting against overconsumption of resources*; *clusterization*; *rejection of failures and fault shielding,* i.e. prevention from the distribution of fault consequences while the system continues the execution of its functions; *applications isolation; creation of microkernel architecture of the operating system (OS); isolation of the OS kernel from applications* and isolation of applications from each other, etc. [3,4,5, etc.].

The general disadvantage of the above mentioned ways is an autonomous implementation of fault tolerance mechanisms, as well as breaks of calculation, which is unacceptable for real-time systems. Attention is drawn to the fact that absolutely all considered ways to assure IS reliability are based on the application of large volumes of artificial structure and information redundancy, i.e. are practically based on the extensive way of fault tolerance assurance. That is why this is obviously very much a current challenge – to construct such a system to assure IS fault tolerance that under little structure and time reserve in real time it shall guarantee the assurance of IS adaptation to faults and failures of technical devices, as well as to exclude the cases of termination of the control process during the period of time that is longer than the acceptable period. The main way to solve this task is to develop the adaptive fault tolerant systems.

II. Task description

Adaptive fault tolerance is possible in information systems by means of introducing a subsystem of assurance of fault tolerance (SFT) into their structure. This software or software and hardware subsystem is formed at the stage of IS design using the provisioned redundant computing means with the help of communication media available in IS. It serves to provide timely protection or prevention from the failures of basic IS hardware and software.

A high level of SFT organization can be achieved using an adaptation mechanism. Let us consider a variant of the creation of SFT adaptive structures. This system contains (Figure 1):

– **information transducer** (IT), performing two groups of tasks: *the first group* is to connect the measurable states X of the system, unmeasurable states E and an adaptive action U. Measurable states are the data about current states of basic hardware and software and a resource. Unmeasurable states are the flows of failures, faults, software errors. *The second group* of tasks performed by IT is to form a vector T of time of adaptation to failures, faults, software errors, as well as of the control commands Y on the ongoing change of the resource, on the rearrangement of the information system, on the adjustment of current states of the system;

- **hardware and software resource *R*** of the system. It includes both, natural and artificial resources;

- **operator of adaptive control AC,** intended to form adaptive action in compliance with a certain algorithm F. A task of adaptation is to find such adaptive action U, so that vector T of SFT system in the field of measurable states X and in the field of unmeasurable states E stay in line with the objectives Z to be achieved

$$Z:\begin{cases} q_j(X,T)\to extr,\ j=1,...,k_1; \\ h_i(X,T)\le \tau_A; i=1,...,k_2; \\ g_i(X,T)\ge \beta\ , i=1,...,k_2 \end{cases}$$

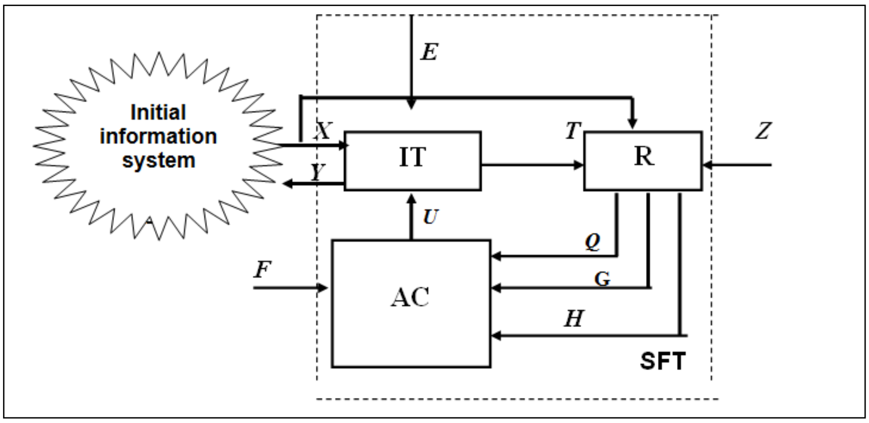


Figure 1: *System of assurance of fault tolerance in an information system*

where the parameters of object function q_j for each *j*-th control are related to the reaching of extreme values, for example, minimum losses of IS efficiency due to SFT actions, minimum additional storage consumptions, minimum delays when solving the tasks of observability and controllability, minimum structure reserve, maximum level of performance indicators of IS in the field *X*, etc. These parameters that could be minimized (maximized) are the aim of adaptation. Not only the information about the aim of adaptation should be transferred to the center of adaptive control, but also the following information: data about resource R, within which adaptation is possible ($U \subset R$), as well as data about adaptation algorithm F that assures the synthesis of adaptive action according to available information:

$$U = \Phi(X, T, Z, R) .$$

Algorithm F solves the task of optimization. In this regard the task of reaching the goals Z is reduced to a famous task of multicriteria optimization

$$q_j(X, T) \to extr_{U \subset S},\ j = 1,\dots,k_1,$$

where a set S is defined by condition $U \subset R$ and restrictions h_i, g_i.

Restriction h_i is in fact a requirement for a random time of adaptation $v_i = t_i - x_i$, that for the period from the moment x_i when a failure occurs till the moment t_i when the protection against this failure is over, not more than allowed time τ_A of the interruption in operation should be spent. Restriction g_i consists in the fulfillment of the first requirement of restriction h_i provided that the given level of assurance – the given probability of successful adaptation of SFT to the system failure – is kept.

To solve this task of multicriteria optimization, it is necessary to reveal the dependence of the object function q_j on the control *U* by a direct calculation of the values of restriction h_i, g_i and of the object function. Fig. 1 shows the adaptation scheme where Q, H, G are the vectors with components q_j and h_i, g_i, that are required to implement adaptive control.

III. Ideas of adaptive fault tolerance of information systems

The basic concept of adaptive fault tolerance is an active use of natural time and structure redundancy, as well as reassignment of available computer power not only for operational processing of information, but also for implementation of observability of the system under the conditions of limited control means. We shall further substitute the notion "adaptive fault tolerance of real-time information systems" with a short notion *"active protection (AP)"*

Active protection (AP) is intended to reach the required levels of fault tolerance of real-time information systems (IS) under little time reserve, limited efficiency of means used to detect failures of computation modules, as well as provided that the scope of redundant equipment does not exceed the scope of basic equipment. It also deals with the assurance of the given probability level of successful IS adaptation to faults and failures of the constituent elements and programs without much increase in the number of provisioned means of control and diagnostics.

Active protection is based on the following ideas [6,7]:

1. The duration of all cycles of the information processing divides into certain time intervals that shall be further called **A3 beats** or just beats. The beats are introduced to sample the continuous time of the information processing. Moments of sampling serve to register the fault-free CMs that are available at these moments in IS, as well as to tie the operations of IS observability and controllability to the A3 beats (vector X of measurable states is being formed). *Each A3 beat ends with*

forming a hold point, that stores the results of CM operation during the previous beat. Operations of observability and controllability, in particular the mechanisms of hold point, restart and etc. are in a strict compliance with the indicated moments of sampling. Thus, the hold point formed for a computation process of any CM, is updated in the A3 beats in time moments t_i, t_{i+1}, t_{i+2} etc.; a restart is made for a depth not exceeding the time τ_A; comparison of the results of the parallel operation of two CMs is done either in one, or in two beats and etc., but not more than in m of A3 beats. These processes in IS perform the functions of the **information transducer** in SFT – **IT** (see Fig.1).

A3 beats can have both *constant duration* (for instance, in IS with a pipeline processing of information), and *random duration*, which is specific to concurrent IS with different architecture. Average duration of a beat corresponds to the time spent to perform several hundreds of computation modules.

2. The whole set of the constituent computation modules of an information system is divided into two compound sets: *computing environment* – a set consisting of $l \leq m$ similar CMs; *protective environment* – a set consisting of $k \leq m$ similar CMs (**resource of** SFT - **R**). If $l + k = m$, (where m is a maximum number of the main CMs), then the IS is considered to have no artificial redundancy (there are no additional CMs). But with such correlation there is still the possibility to use $k < m$ of naturally redundant CMs, in favor of IS fault tolerance. If $l + k > m$, then the system has $l + k - m$ of additional CMs, and $m - l$ of naturally redundant CMs. At each moment of sampling to solve the tasks there may occur the necessity to use $l_i \leq m$ of the main CMs, as well as the availability of $m - l_i + k_i$ of redundant CMs in IS. If at this moment of time only l_i CMs are operable, it means that the protective environment has reached its limits, but there are enough available main CMs to solve the task of the information processing. Therefore, the registration of fault-free CMs of the main and protective environments at each moment of sampling is required to define the possibility to proceed with solving the processing tasks during an A3 beat with a sufficient amount of operable CMs. It is also necessary for a sustainable assurance of IS fault tolerance during the next beat with the help of redundant operable CMs if there are such modules at the moment t_i.

3. *Dynamic rearrangement of IS is carried out in the A3 beats* for the organization of a beat-by-beat parallel operation of the required number of the main CMs and available fault-free redundant modules. This will ensure the implementation of external control of CM operating capability. Thus, if at the moment t_i a restraint $m - l_i + k_i \geq l_i$ is fulfilled, then it is possible to form l_i of CM pairs and, therefore, to implement the control of faults and failures of all main CMs. If at this moment there is only one redundant fault-free CM, then, as expected, it switches to the next main CM, and during the next A3 beat one pair of CM operates in parallel, and the rest $l_i + 1$ CMs are not controlled during one A3 beat. Then in the next beat, with the help of the this particular fault-free redundant CM another pair of CM is formed and etc. As the result, for the number of beats equal or less than l_i it is possible to detect an event of failure in any CM from the cope of $l_i + 1$ that remained in the system arrangement. These processes in IS solve the tasks of **adaptive control** – **AC**.

4. *Virtual redundancy of all l of the main CMs with the availability of at least one fault-free redundant CM* is achieved owing to the fact that during a very short period of time that does not esceed l of beats, each of the main CMs operates in parallel with a similar CM. Therefore, in these short time spaces those pairs of modules operate in which all main CMs participate. With k of fault-free redundant CMs there is k which is a multiple virtual redundancy of all main CMs, as each main CM commutates with any redundant module.

5. All stages of IS observability (detection of an event of failure, localization, classification and location) **are performed on real tasks with no application of detecting devices during the processing of information**. Therefore, for the estimation of IS fault tolerance it does not matter that

under a parallel operation of the pair of CMs no faulty element of the module was detected, that was not used when solving this task. It should be noted that the higher is the intensity of applications coming to IS for handling (i.e. the higher the system is loaded), the more often IS is observed in the A3 beats. And conversely, the lower the system is loaded, i.e. the more pauses are there between the tasks, the less often IS is observed in the A3 beats. In long pauses between the tasks it is reasonable to use traditional means of control and diagnostics.

6. For the classification of failures, and for their location on the CM level, the system should have **not less than *m* = 2 main and one redundant CM**. With the simple active protection the additional CM opeates in parallel with the first main CM, and during the next beat (or in a beat) — with the second main CM. If the results of operation of the pair of CMs do not coincide, a double count is made during the previous beat, and it helps to eliminate error or identify a failure of one from the pair of CMs in case of repeated noncoincidence of the results. The failed CM is identified during a current beat upon the results of operation of the additional CM with the second main one. If the results do coincide, a decision is made in relation to the failure of the first main CM, If the results do not coincide, a decision is made in relation to the failure of the additional CM.

7. **Capabilities of active protection** considerably depend on the choice of **average duration of the beat τ of active protection.** Value τ should be selected so that during the time allowed for failure (fault, error) detection, defined by the duration of the processing cycle $\tau^{\bullet}_{Д} = \tau_{Д} - t_{У}$ the failed CM with the given level of assurance is localized and reswitched to an additional fault-free CM. Time τ_{L} is required for the recovery of a computation process from the last hold point with a respective implementation of active protection. When determining the value τ it is necessary to consider the times of solving the tasks and the pauses between them, laws of idistribution of these time periods, and the duration of a beat of active protection, number *m* of the main CMs, ways of implementation of active protection, number of redundant CMs.

VI. Example of automatic detection and elimination of failures of the system modules

In certain A3 beats CMs are redistributed between the computing and protective environments. Certain modules of the protective environment for an A3 beat hold the functions of the main modules, and vice versa. Under the reassignment all modules participate in pair operation, and as the result the A3 cycle is getting shorter. Let us illustrate this situation on the following example. Let *1 = m = 4, k=l.* The main CMs are enumerated from 1 to 4, the initial redundant CM is 5. Let us assume that in the first beat there was no reassignment of modules, and module 5 performed the control of the main module 1 (pair 5—1). In the second beat the modules have already been reassigned. And moudule 5 performd the functions of the main module 2, ehich now performd the control of the main module 3 (pair 2—3 in Table1). As the reuslt of this operation, for two A3 beats it is possible to control the operation of four CMs out of five (1, 2, 3 and 5). Under the CM reassignment for five A3 beats all modules are controlled twice.

The efficiency of CM reassignment grows with increase of *m* of initial main modules. Thus, with *m* = *6* and *k* = *2* it is possible to control all 8 modules during two A3 beats. System with 8 reassignable CMs is organized as follows. The cycle of single check of modules contains.

A = *2* beats. In the first beat module 7 of the protective environment performs the functions of the main module 2, which performs the control of the main module 1 (pair 2—1). Besides, in this particular beat module 8 of the protective environment performs the control of the main module 5 (pair 8—5). In the second beat module 8 performs the functions of the main module 4, forming the pairs 4—3 and 7—6. Other variants of the organization of the system with 8 reassignable CMs are also possible, but this variant has an important benefit — only modules 7→2 and 8→4 are reassigned, it significantly simplifies necessary means of commutation and control in the system.

Table 1

No. of beat	Numbers of main CMs	No. of controlling CM	Pairs of CMs under control	Reassigned CMs
1	1 2 3 4	5	5—1	-
2	1 5 3 4	2	2—3	5 2
3	1 2 3 5	4	4—5	5 4
4	5 2 3 4	1	1—2	5 1
5	1 2 5 4	3	3—4	5 3

In general, with the availability of fault-free *m* of the main CMs and *k* of the redundant modules it is possible to define the number of beats *A* in the cycle A3, meaning they underwent a single check, based on the considered logic of CM pair assignment

$A = int[(m + k)/2k]$

Here operation *int* is the operation of rounding of the result up to the nearest whole number. For example if $m = 5, k = 2$, then $A= int(1,75) = 2$. The same values of *A* shall hold with $m = 6, k = 2$. That is why under the organization of A3, having a known value *k* of redundant CMs, it is reasonable to protect such amount *m* of the main modules, so that the following relations are true.

$int\ (m/k) = m/k$ and $int[(m + k)/2k] = (m + k)/2k.$

Based on the CM reassignment it is possible to organize their *priority control***.** If under the reassignment of the modules it was necessary to equalize the frequency of controls of the main and redundant CMs, then under the priority control we solve the task to increase the frequency of controls of the indicated modules.

Let us illustrate the possibilities of the construction of systems with one module indicated as a priority one. It is assumed that all modules except the indicated one are controlled with one and the same frequency, and the indicated CM is controlled with a higher frequency.

Let us assume that the system contains $m = 4$ main (numbers from 1 to 4) and one (number 5) redundant CM. Module 2 is indicated as a priority one (Table 2). It is required to assure the frequency of controls of module 2 to be twice higher in comparison to the other four CMs. The solution of this task is described in Table 2. The cycle A3 is realized for three beats, and module 2 is controlled twice during the cycle, and modules 1, 3, 4, 5 are controlled just once.

Table 2

No. of beat	No. of cycle	Numbers of main CMs	No. of controlling CM	Pairs of CMs under control	Reassigned CMs
1	1	5 2 3 4	1	1—2	5—1
2		1 5 3 4	2	2—3	5—2
3		12 3 5	4	4—5	5—4
1	2	5 2 3 4	1	1—2	5—1
2		15 3 4	2	2—3	5—2
3		12 3 5	4	4—5	5—4

The reduction of time intervals between controls of some CMs is possible by increasing the time between controls of non-priority CMs. It is necessary to keep a rational compromise when solving such tasks of active protection.

V. Conclusion

Limited capabilities of redundancy, means of concurrent detection of failures, faults, errors during the implementation of information processes, limited capabilities of the set “hardware – software” – these all calls for the necessity to develop non-typical technologies to assure reliability of information systems. One of them is the proposed technology of *adaptive fault tolerance.* This technology consists in the active use of natural time and structure redundancy, as well as in the active (and automatic) reassignment of available computer power not only for operational processing of information, but also for implementation of observability of the system under the conditions of control means. The technology of adaptive fault tolerance in information systems, when solving real tasks in limited time conditions provides for a timely automatic detection and handling of failures and glitches by means of operational localization of faulty computation modules and by subsequent automatic rearrangement of the system with a removal of faulty modules from the process of functioning.

References

[1] Shubinsky, I. B. Functional reliability of information systems. Methods of synthesis [Text] / I. B. Shubinsky. – M. : Journal dependability, 2012. – 296 p.

[2] Shubinsky, I. B. Structural reliability of information systems. Methods of analysis[Text] / I. B. Shubinsky. – M. : Journal dependability, 2012. – 216 p.

[3] Avizienis, A. Dependability of computer systems [Text] / A.Avizienis, J-C Laprie, B. Randell / Fundamental concepts, terminology and examples. Technical report, LAAS – CNRS, October, 2000.

[4] Zyl, S. Standard devices QNX Neutrino to provide fail-safety of mission-critical computer systems [Electronic resource] / S. Zyl. – CTA. – 2009(3). – 118 p. – Access mode: http://www.cta.ru/cms/f/389405.pdf.

[5] Fogelin, D. Implementation of high availability in embedded systems [Electronic resource] / D. Fogelin, K. Kving. – Access mode: http://www.asutp.ru/?p=600410.

[6] Shubinsky, I. B. Active protection against the failures of microprocessing computer systems [Text] / I. B. Shubinsky. – M. : Znanie, 1987. – 60 p.

[7] Shubinsky, I. B. Reliable fail-safe information systems. Methods of synthesis [Text] / I. B. Shubinsky. – M. : Journal dependability, 2016. – 541 p.

About the author

Shubinsky Igor Borisovich – Dr.Sci., Professor, member of several academies of sciences, Expert of Research Board under RF Security Council, editor-in-chief of scientific and research journal "Dependability", deputy editor-in-chief of journal "Reliability: Theory and Applications" (USA), director general of JSC "Information safety on transport – IBTrans" (Russia, Moscow).

Contacts:
119333, Russia, Moscow, Vavilova Str. 48-339;
Tel. +7(499) 137 70 42; tel/fax +7(495)786 68 57; mobile +7(985) 774 34 29
e-mail: igor-shubinsky@yandex.ru

Application of Reliability Theory to Functional Safety of Computer Control Systems

Vladimir Sklyar

•

National Aerospace University "KhAI", Ukraine
Indian Institute of Technology Bombey, India
v.sklyar@csn.khai.edu

Abstract

Taxonomy for Dependability and Security has been updated to reflect all used attributes as well to refine orthogonal relations between attributes. Functional Safety is a part of Reliability that has dealt with Safety Functions and related dangerous failures. From this point of view, all the Reliability Theory methods, models and indicators may be applied for the Functional Safety domain without any essential change. The three main types of architecture of modern safety critical computer control systems are considered (Embedded Systems, Industrial Control Systems, and Internet of Things). Application of Reliability and Safety indicators to Industrial Control Systems of Nuclear Power Plants is given. Internet of Things has just started to be applied to safety critical systems during the last years. Research and Development program is proposed to study IoT Reliability and Functional Safety.

Keywords: functional safety, dependability, security, reliability theory, industrial control systems, embedded system, internet of things, research and development

I. Introduction

A goal of this paper is to analyze Reliability Theory applications for safety critical computer control systems (CCS).

Reliability Theory has been developed as an applied science in 50-s to decide a general problem to create reliable systems from unreliable components. To 80-s the main theoretical results have been obtained so since 80-s we have proven in use engineering practices to assure and assess reliability of control systems.

Since 80-s computer systems became too complex and too responsible to be described only with reliability, so new attributes like dependability, security, safety, and others have been implemented by researchers [1]. A joint committee on "Dependable Computing and Fault Tolerance" was formed by the Institute of Electrical and Electronics Engineers (IEEE) Computer Society (CS) and the International Federation of Information Processing (IFIP) Working Group (WG) 10.4 (http://www.dependability.org). A general terminology has been developed and presented in 2004 in the paper [2]. For safety critical control systems this concept should be refined to emphasis a background for requirements and compliance evaluation implementation.

Today we have a set of theoretical results implemented in industrial standards which define state-of-the-art for safety-critical applications in different domains, as following:

- Umbrella functional safety standard: IEC 61508, Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety-related Systems
- Process industries: IEC 61511, Functional safety – Safety instrumented systems for the

process industry sector;

- Machinery IEC 62061, Safety of machinery: Functional safety of electrical, electronic and programmable electronic control systems;
- Nuclear: IEC 61513, Nuclear power plants – Instrumentation and control for systems important to safety;
- Automotive: ISO 26262, Road vehicles – Functional safety;
- Railway: EN 50129, Railway Industry Specific – System Safety in Electronic Systems;
- Medicine: IEC 62304, Medical Device Software;
- Avionic: DO-178C, Software Considerations in Airborne Systems and Equipment Certification;
- Space: NASA-STD 8719.13, Software Safety Standard.

Safety and security are important features for new developed industrial domain of Internet of Things (IoT). IoT is defined as an infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react. IEEE started a project to develop standard for an Architectural Framework for the IoT (IEEE P2413) in 2014. At the same year the Joint Technical Committee on Information Technologies of International Electrotechnical Commission and International Standardization Organization (ISO/IEC JTC1) created the Working Group on Internet of Things (WG 10) to develop a new standard ISO/IEC 30141 "IoT Reference Architecture".

It is worth to mention, IEEE P2413 (Standard Project) "Standard for an Architectural Framework for the IoT" already discusses issues related to safety and security for critical domains. Since IoT Architecture is defined clearly, safety and security risks for critical applications will be analyzed on the standard base. At the same time typical reference architectures for safety-critical Embedded Systems (ES) and Industrial Control Systems (ICS) on the base of Programmable Logic Controllers (PLC) are well known and defined in the standards. These three types of architectures (ES, PLC-based ICS and IoT) are mainly used at the present time to implement safety-critical control systems.

This paper contains the following parts:

- Firstly, terminology attributes and taxonomy in Dependability and Security are discussed;
- Secondly, reference architectures for ES, ICS and IoT are presented;
- Thirdly, Reliability, Availability and Safety indicators are discussed in this paper to support engineering solutions in safety critical domains;
- After that, the main Research and Development (R&D) tasks are formulated for Functional Safety of IoT as for relatively new domain which request intensive investigation in safety and security critical applications.

II. Terminology and Taxonomy Discussion in Dependability and Security

Let's consider existing approaches to the state taxonomy of dependability.

Four of the attributes RAMS (Reliability, Availability, Maintainability, Safety) used to be considered as extensions for "classical" Reliability. The paper "Basic Concepts and Taxonomy of Dependable and Secure Computing" [2] launched in 2004 the new IEEE Transactions on Dependable and Secure Computing. It explains the complexity of dependability in relation with security of modern computer-based systems (see Figure 1).

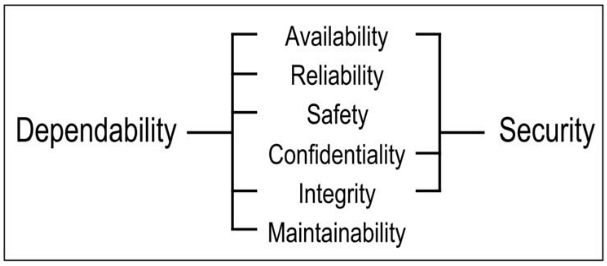


Figure 1: *Dependability and security attributes*
(as per "Basic Concepts and Taxonomy of Dependable and Secure Computing" [2])

In the [2], dependability is considered as an integrating concept including the following attributes:

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

Security is a composite of the attributes availability, integrity, and confidentiality. When addressing security, availability is considered for authorized actions as well as integrity is considered for a proper authorization. Confidentiality is a supplementary, in comparison with dependability, security attribute, which means the absence of unauthorized disclosure of information.

It is worth also to mention the paper "Reliability: Past, Present, Future" by Igor Ushakov [3], which lays the cornerstone of the e-journal "Reliability: Theory & Applications". The author discussed directions of Reliability Theory, which are still to be state-of the-art after a decade. Such directions, in fact, represent attributes, which can complement dependability, including the following:

- Effectiveness ("performability") relates to systems for which one is not able to formulate "all or nothing" type of failure criterion; effectiveness characterizes a system's ability to perform its main functions even with partial capacity;
- Survivability is a special property of a system to "withstand impacts"; in this case one assumes that the impacts are directed to the most critical components of the system;
- Safety is a special property of a system characterizing effective performance of its main predetermine functions without dangerous environmental consequences for people and nature;
- Security is sometimes considered as a part of reliability-survivability problem; indeed, many systems must not only operate reliably but also at the same time provide protection against non-sanctioned access.

After that publication, effectiveness and survivability were included in dependability and security attributes [4]. Author cannot guess was it done independently or dependently from the [3].

We need to mention two more essential attributes used for state-of-the-art CCSs.

Firstly, it is Quality of Services (QoS) which describes the overall performance of networks and is widely applicable for web-based application. In fact, it is some extension of the above mentioned Performability.

Secondly, we have Resilience which is an attribute close to Survivability [5]. In the know proceedings Resilience has never been integrated with Dependability and Security attributes.

Resilience is the ability of a system to cope with changes which usually lay in challenges to normal operation such as faults, cyber threats and others.

In the former Soviet Union, Dependability taxonomy was based on the government standards (as named "GOST") which are still remaining in force in many countries. The umbrella standard in

Dependability taxonomy is GOST 27.002-89 "Industrial product dependability. General concepts. Terms and definitions".

The following definitions and taxonomy are stated in GOST 27.002-89. Dependability is the property to keep within the established values of the parameters under all the stated conditions within a stated period of time.

It includes the following four attributes:

- Reliability is continuity of the operation state during some time;
- Durability is continuity of operation with periodic maintenance and repairs until retirement time; it is highly related with long term operation.
- Maintainability is an ability to support operation state and to turn back to operation state after periodic maintenance and repairs.
- Storability is an ability to support all dependability attributes during storage.

A problem appears when somebody tries to harmonize dependability issues as (RAMS – Integrity) with (Reliability – Durability – Maintainability – Storability).

To make it consistent, let's analyze dependency between all proposed Dependability and Security attributes. Taxonomy is refined to make it orthogonal (see Figure 2).

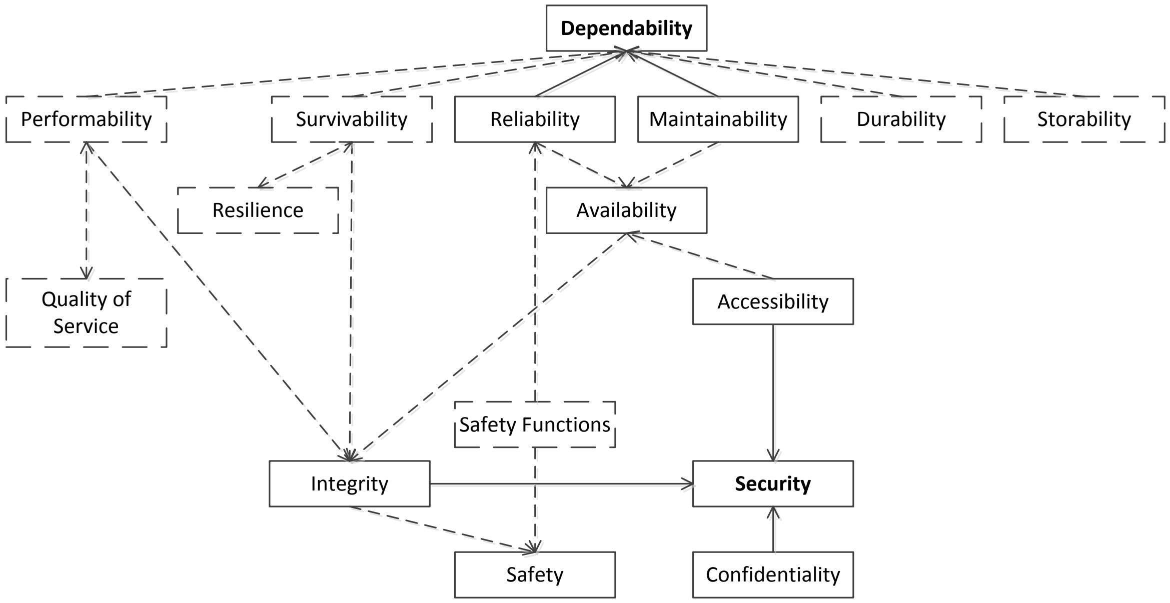


Figure 2: *Updated Dependability and Security Taxonomy*

Squares with a dotted border are used at Figure 2 to highlight new attributes versus traditionally used Dependability and Security attributes (see Figure 1) with regular borders. The same, dotted lines are used in Figure 2 to highlight new dependencies between attributes versus dependencies on Figure 1, which are highlighted with regular lines. Arrows on the lines show that attributes of the low level is included in attribute of high level. If such hierarchy is not established, then arrow has both side arrows (as, for example, between Performability and Quality of Service, between Survivability and Resilience).

Update of Dependability and Security taxonomy is supported with the following statements, which underline differences between Figure 2 and Figure 1.

1. Additional Dependability attributes are added to make taxonomy consistent with [2-4] and GOST 27.002-89. It is Performability, Survivability, Durability, and Storability. Added attributes are highlighted in Figure 2 with dotted borders.

2. Quality of Service is added as additional attribute related to Performance. Application domains of these attributes are a bit different, so established relations between them does not

indicate which attributes have the highest level. The same things are with a pair of Survivability and Resilience.

3. Availability is a combination of Reliability and Maintainability what is from equation A = MTTF / (MTTF + MTTR), where MTTF – Mean Time to Failure, MTTR – Mean Time to Restoration.

4 Accessibility is more appropriate term for safety domain the Availability. However Accessibility is a part of Availability, so such relation is established.

5. Safety takes a care mostly about the failures of Safety Functions (dangerous failure), which are intended to achieve or maintain a safe state of a system. So there is a relation between Reliability and Safety, and this relation is established via Safety Functions.

6. At the same, Safety includes both Safety Functions and Integrity, what is stated in the standards IEC 61508 as the confidence level (sometimes, probability) of a system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time.

7. Integrity consideration as a Safety attributes entails that Integrity shall be complimented with Performability, Survivability and Availability.

A proposed Dependability and Security taxonomy can be used for safety and security critical domains to highlight attributes which are essential for implementing one or the other CCS application [6,7].

III. Architecture of Computer Control Systems

Control Systems fundamentals lay in interaction with some processes of the real World via three the main parts which are sensors, controllers and actuators (see Figure 3). For modern CCSs not mandatory, but typically is a presence of Human-Machine Interface (HMI) with monitoring data transmission, processing and storage.

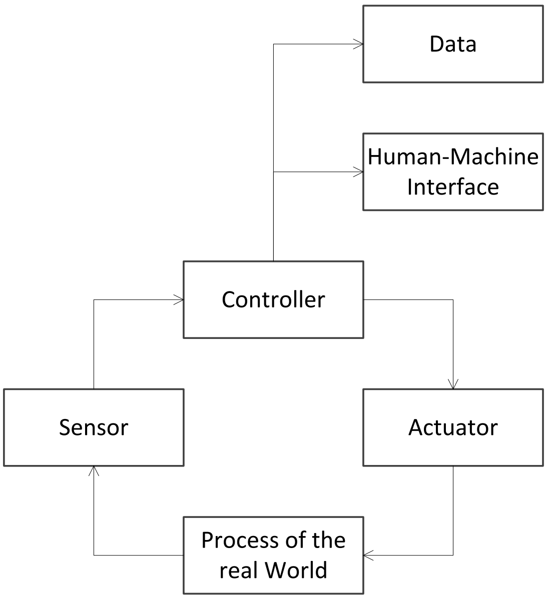


Figure 3: *Typical Architecture of Computer Control Systems*

For ES such architecture can be implanted on one chip or on one board.

ES applications are used in the presence in such domains as consumer electronics, control systems and industrial automation, bio-medical systems, field instrumentation, handheld computers, data communication, network information appliances, telecommunications, wireless communications, robotics and helicopters (drones), computer vision etc.

Typical programmable components of ES are Microcontroller Units (MCU), Digital Signal Processors (DSP), Field Programmable Gates Arrays (FPGA), Complex Programmable Logic Devices (CPLD), and Application Specific Integrated Circuits (ASIC).

ICS structure [8] includes a wide range of sensors and transmitters, PLCs, actuators, HMI workstations and data storages, combined with the networks (see Figure 4). Design parts for ICS include mechanical, electrical, firmware, hardware, and software.

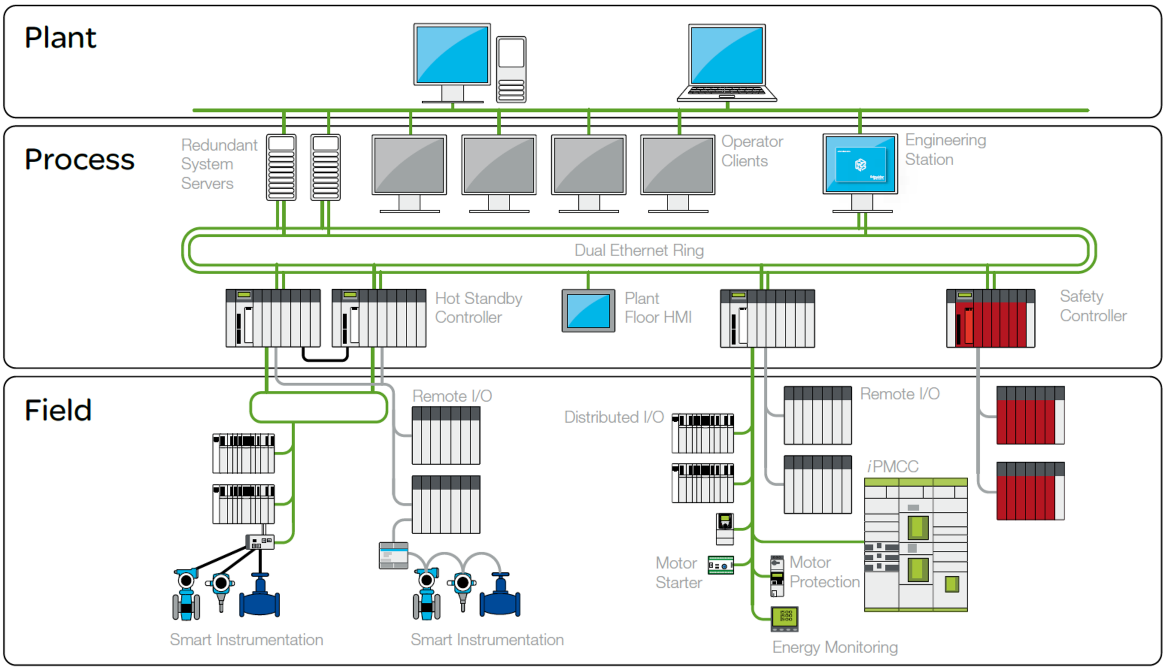


Figure 4: *Typical Architecture of Computer Control Systems*
(Source: Schneider Electric – Modicon Quantum PLC)

Reference architecture of IoT [9,10] is presented as a set of layers with interfaces (see Figure 5). Each of the layers has its own architecture. Interfaces can use different communication protocols with different security measures.

Device Layer is directly responsible for control functions performance, including for that a set of sensors, on the board controllers and actuators (see Figure 3), which can have the same with ES structure. Digital control is usually restricted on this layer. All other layers are supplementary from the point of view of CCS. From this prospective the interfaces DL-NL and DL-AL are the most interfering for CCS Functional Safety.

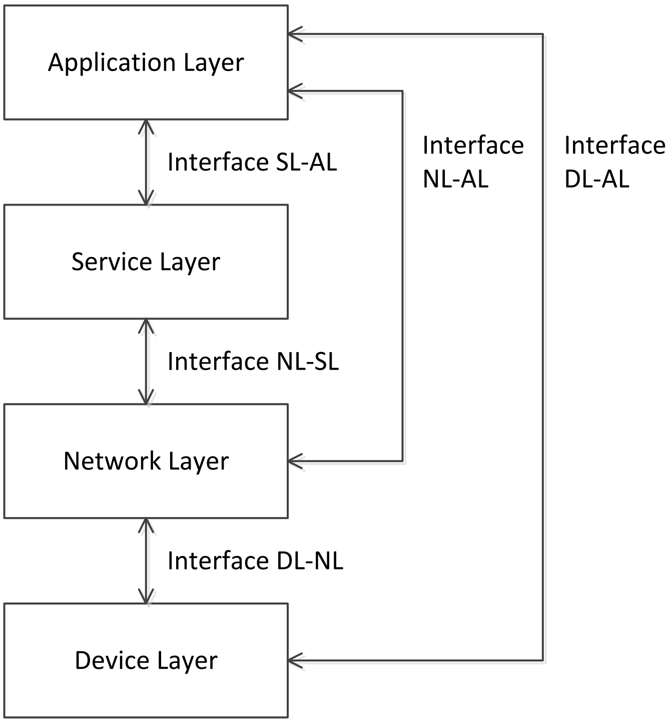


Figure 5: *Typical Architecture of IoT*

IV. Reliability, Availability and Safety Indicators: Fundamentals

Let's consider the statement of the standards series IEC 61508 "Functional safety of electrical/electronic/programmable electronic safety-related systems" which discuss Safety Indicators. At the same time, let's try to compare these Safety indicators with well-known Reliability and Availability indicators.

The basic concept of Functional Safety assessment is dividing a common failure rate Λ (let us begin with the exponential distribution with a constant failure rate) into dangerous and safe failures as well as into detected and undetected failures. This is a main difference of Functional Safety from Reliability. From this point of view we have four failures sets (see Figure 6):

- Safe Detected failures with a failure rate λ_{Sd} – failures which put the equipment under control (EUC) to a safe state and are discovered by self-diagnostics;
- Safe Undetected failures with a failure rate λ_{Su} – failures which put the EUC to the a state and are not discovered by self-diagnostics;
- Dangerous Detected failures with a failure rate λ_{Dd} – failures which put the EUC to a potentially dangerous state and are discovered by self-diagnostics;
- Dangerous Undetected failures with a failure rate λ_{Du} – failures which put the EUC to a potentially dangerous state and are not discovered by self-diagnostics.

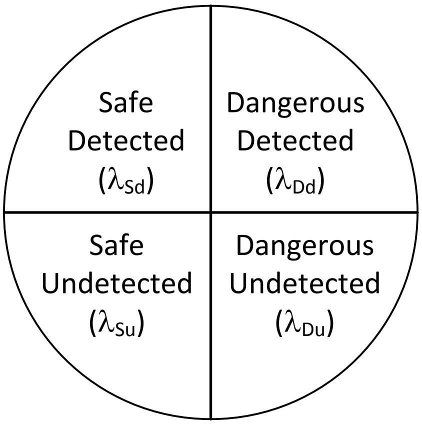

Safe Detected (λ_{Sd})
Dangerous Detected (λ_{Dd})
Safe Undetected (λ_{Su})
Dangerous Undetected (λ_{Du})

Figure 6: *Failures Theoretical-Set Model*

So, there are some obvious dependencies following from Figure 6:

- Common failure rate is $\Lambda = \lambda_{Sd} + \lambda_{Su} + \lambda_{Dd} + \lambda_{Du}$;
- Dangerous failure rate is $\lambda_D = \lambda_{Dd} + \lambda_{Du}$;
- Safe failure rate is $\lambda_S = \lambda_{Sd} + \lambda_{Su}$;
- Detected failure rate is $\lambda_d = \lambda_{Sd} + \lambda_{Dd}$;
- Undetected failure rate is $\lambda_u = \lambda_{Su} + \lambda_{Du}$.

Also a lot of relative metrics can be extracted from dependencies between sets cardinality and different failure rates values. The most important from these metrics are the following:

- Safe Failure Fraction (SFF) in accordance with IEC 61508 is SFF = $(\lambda_S + \lambda_{Dd}) / \Lambda$;
- Dangerous Failure Fraction (DFF) in accordance with IEC 61508 is DFF = 1 – SFF = λ_{Du} / Λ;
- Diagnostic Coverage (DC) for dangerous failures in accordance with IEC 61508 is $DC_D = \lambda_{Dd} / \lambda_D$;
- More widely used dependency for Diagnostic Coverage is DC = λ_D / Λ;
- Proof Test Coverage (PTC) should be calculated from the total failure rates for the using the formula PTC = $1 - \lambda_{DuaPT} / \lambda_{Du}$, where λ_{DuaPT} is λ_{Du} after Proof Test.

To move ahead with Safety indicators we need to introduce some definitions from the standards series IEC 61508.

Safety Function is a function to be implemented by a safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event; all the above indicators are usually calculated for specified Safety Functions; sometimes for ICS a term **Safety Instrumented Function (SIF)** is used as equal;

Safety Integrity is a probability of a safety-related system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time.

Safety Integrity Level (SIL) is a discrete level (one out of a possible four), corresponding to a range of safety integrity values, where SIL 4 has the highest level of safety integrity and SIL 1 has the lowest.

Mode of Operation is a way in which a safety function operates, which may be either

- Low Demand Mode: where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year; or
- High Demand Mode: where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year; or
- Continuous Mode: where the safety function retains the EUC in a safe state as part of

normal operation.

IEC 61508 states different Safety Indicators depending from the Mode of Operation.

For Low Demand Mode average probability of dangerous failure on demand (PFDavg) shall be calculated. PFDavg is mean unavailability of a safety-related system to perform the specified safety function when a demand occurs from the EUC.

The IEC 61508 states that only Dangerous Undetectable failures contribute to PFDavg, the last can be calculated as PFDavg(Du) = 1 – A(Du) = U(Du) = λ_{Du} / (λ_{Du} + μ_{Du}), where μ_{Du} is restoration rate of Dangerous Undetectable failures.

Also for Dangerous failures PFDavg(D) = 1 – A(D) = U(D) = λ_D / (λ_D + μ_D), where μ_{Du} is restoration rate for all the Dangerous failures.

For High Demand Mode and Continuous Mode average frequency of a dangerous failure per hour (PFH) shall be calculated. PFH is the average frequency of a dangerous failure of a safety related system to perform the specified safety function over a given period of time.

Usually PFH is defined as failure rate, so on the base of Dangerous Undetectable failures PFH(Du) = λ_{Du}, and on the base of all the Dangerous failures PFH(D) = $\lambda_{D.}$

Also the IEC 61508 states that PFH can be calculate as unavailability or as unreliability depending from a safety-related system application conditions.

So, the general conclusion is a typical Reliability Theory method, models and indicators can be directly applied for the Functional Safety domain.

V. Reliability, Availability and Safety Indicators: Application for Nuclear Domain

This section provides a case study for application of the above indicators for safety assessment of ICSs integrated on the base of safety PLC named RadICS designed by company Radiy (www.radiy.com).

The RadICS PLC is composed of a logic module (LM) and a number of varied I/O modules contained within a chassis. There is the following scope of available I/O modules for the RadICS PLC:

- Analog Input Module (AIM);
- Discrete Input Module (DIM);
- Analog Input Flux Module (AIFM);
- Analog Output Module (AOM);
- Discrete Output Module (DOM);
- Optical Communications Module (OCM).

The RadICS PLC performs the safety function defined in its application (ICS) layer logic, which will be specified by and possibly implemented by the end-user (Nuclear Power Plants). Diagnostics are executed at both the application and the platform level, and detected failures that are potentially unsafe are converted to safe events by opening the discrete outputs.

The target in the considered case was to determine SIL of the RadICS PLC as a platform for future applications for Nuclear Power Plants.

Reliability, Availability and Safety are investigated in special Failure Mode Effect and Diagnostic Analysis (FMEDA) Report. FMEDA is a modification of well-known FMEA technique. A difference lays in assessment of diagnostic coverage, which is an essential part of Functional Safety implementation. Also the FMEDA generates failure rates and the Safe Failure Fraction. The analysis assumed that the FSC will be used in de-energize–to–trip applications.

For hardware assessment only random equipment failures are of interest. It is assumed that the equipment has been properly selected for the application and is adequately commissioned such that early life failures (infant mortality) may be excluded from the analysis. Failures caused by external events, however should be considered as random failures. Examples of such failures are loss of power, physical abuse, or problems due to intermittent instrument air quality.

The first step to in FMEDA is to define the failure rate for fail safe detected, safe undetected, dangerous detected, and dangerous undetected failures. Electrical and mechanical component Reliability Handbooks with statistical data are used to define the failure rate of separated components. Criticality analysis is used to divide components failures between safe and dangerous. Diagnostic coverage analysis is used to divide components failures between detected and undetected.

Calculation of the above failure rates is a basic for calculation of application specific indicators depending of ICS hardware configuration. For example, typical single-channel Safety Function (SIF), based on a CANDU 6 reactor (http://www.candu.com/en/home/candureactors/default.aspx) heat transport high pressure trip parameter, consists of the following:

- 1 pressure sensor measuring one outlet header pressure (requires 1 AIM);
- 2 discrete outputs used to provide trip signals to the 2oo3 voting logic (using 1 DOM);

This trip system is modeled in two parts; the individual channel, and the inter-channel voting. The example configuration as used for the sensors and PLC comprising each individual channel of the 3-channel safety system is as follows:

- One LM uses no on-board discrete inputs or outputs;
- One AIM reads a typical pressure transmitter used in CANDU plants, with both off-scale low or high leading to trip;
- One DOM using a total of two discrete output channels (used to drive the 2oo3 inter-channel voter consisting of 6 solenoid valves).

Note that this SIF operates in a low demand mode; however the modeling is complicated by the 2 layers of logic solving. This requires modeling the real sensors and the PLC in one model operating in continuous demand mode. This determines a failure rate to be used in the inter-channel voting part of the model, which operates in a low demand mode.

To confirm that the PLC has met its requirement to consume less than 15% of the allowable PFDavg of SIL 2, the channel model is also examined in low demand mode.

The described approach allows to calculate the above indicators (SFF, DFF, DC, PTC) for specific applications.

As a result of the above case the RadICS PLC has been certified by exida LLC (exida.com) as a product complied with SIL3 requirements of IEC 61508 (http://www.exida.com/SAEL/rpc-radiy-fpga-based-safety-controller-fsc-radics). At the present some tens of applications are implemented on the base of RadICS PLC for Nuclear Power Plants in Europe and Americas. The mentioned applications demonstrate the specified level of Functional Safety.

VI. Discussion: a Proposed Research and Development (R&D) Program for IoT Reliability and Functional Safety

An updated taxonomy has been proposed in this paper for Dependability and Security. This taxonomy integrates all known attributes in safety and security critical domains. Relations between Safety and all other attributes are established.

Functional Safety is a part of Reliability that has dealt with Safety Functions and related dangerous failures. Safe failures do not affect Functional Safety features. From this point of view, all the Reliability Theory method, models and indicators may be applied for the Functional Safety domain without any essential change.

ES, ICS, and IoT Device Layer have been considered in Section III as three the main architectures used for CCSs. ES and ICS have a long references story for safety critical applications while IoT has only started to be applied during the last five years.

Taking into account the above, the following Research and Development (R&D) program is proposed to study IoT Reliability and Functional Safety:

- Task 1 "IoT Reference Architecture Development" with the following subtasks: Standards for safety critical applications. Standards for IoT. Case Study: Analysis of existing IoT platforms. Used programmable components and challenges in safety assessment. Layers of architecture. Communications between layers of architecture. Functions distributions between layers of architecture. Opportunities for isolation of safety from non-safety functions. Prospective of IoT based applications for safety critical domains;
- Task 2 "Safety and Reliability Models Development" with the following subtasks: New challenges for Reliability Theory from the IoT prospective. Application of Reliability, Availability and Safety indicators for IoT. Trade-in between Safety and Availability. Comparative risk analysis for IoT based applications versus PLC based applications. Safety assurance methods: redundancy, diversity, diagnostic, separation, qualification testing, etc.;
- Task 3 "Application of Reliability and Safety Assessment Methods for IoT" with the following subtasks: Overview of safety assessment methods and tools. Hazard Analysis. Fault Tree Analysis. Markov models. Failure Mode, Effect and Criticality Analysis;
- Task 4 "IoT Safety Life Cycle" with the following subtasks: Safety management. Safety Life Cycle structure. Verification & Validation methods. Software tools evaluation. Configuration management and change control;
- Task 5 "IoT Testing" with the following subtasks: Test coverage approach for IoT Safety Life Cycle. Review of technical specifications. Static code analysis. Unit and integration testing. Fault Insertion Testing. Validation testing with physical I/O. Environmental impact testing. Model-based testing (MBT). Formal verification;
- Task 6 "Computer Security of IoT" with the following subtasks: Vulnerabilities and treats for IoT. Case studies of existing malware. Recommendations for security management system: business protection, data protection, operation protection;
- Task 7 "Assurance Case for IoT" with the following subtasks: Assurance Case notation and methodology updating. Tools for Assurance Case building. Implementation of IoT Assurance Case methodology for licensing and certification framework;
- Task 8 "Energy consumption efficiency assessment for IoT" with the following subtasks: Energy consumption model for IoT. Energy consumption assessment tools. Energy consumption measurement experiment;
- Task 9 "Design and testing of a representative IoT based application" with the following subtasks: Choice of application. Choice of hardware-software platform and design technology stack. Model-based design methodology. Design implementation. Trial operation.

References

[1] Laprie, J.-C. (1985). Dependable Computing and Fault Tolerance: Concepts and Terminology. *Proceedings of the 15th IEEE International Symposium Fault-Tolerant Computing (FTCS-15).*

[2] Avižienis, A., Laprie, J.-C., Randell, B. and Landwehr, C. (2004). Basic Concepts and Taxonomy of Dependable and Secure Computing. *IEEE Transactions on Dependable and Secure Computing*, 1(1): 11-33.

[3] Ushakov, I. (2006). Reliability: Past, Present, Future. *Reliability: Theory & Applications,* 1(1): 10-16.

[4] Trivedi, K., Kim, D.S., Roy, A. and Medhi, D. (2009). Dependability and Security Models. *Proceedings of the 7th International Workshop on the Design of Reliable Communication Networks.*

[5] Castet, J. and Saleh, J. (2006). Survivability and Resiliency of Spacecraft and Space-Based Networks: a Framework for Characterization and Analysis. *Proceedings of the Conference on Network Protocols (ICNP 2006).*

[6] Yastrebenetsky, M. and Kharchenko, V. (Edits) (2014). Nuclear Power Plant Instrumentation and Control Systems for Safety and Security, IGI Global, 2014.

[7] Sklyar, V. (2016). Safety-critical Certification of FPGA-based Platform against Requirements of U.S. Nuclear Regulatory Commission (NRC): Industrial Case Study. *Proceedings of the 12th International Conference on ICT in Education, Research and Industrial Applications (ICTERI 2016).*

[8] Andrashov, A., Bakhmach, I., Sklyar V., Kovalenko A. (2015). FPGA-based I&C applications in NPP's modernization projects: Case study. *Proceeding of the 9th International Conference on Nuclear Plant Instrumentation, Control & Human-Machine Interface Technologies (NPIC&HMIT 2015).*

[9] Top 10 IoT Technologies for 2017 and 2018. Technical Report G00296351, Gartner Inc., 2016.

[10] Sajid, A., Abbas, H., Saleem, K. (2016). Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges. *IEEE Access*, 4:1375-1384.

Mathematical Model for Calculating Reliability Characteristics NPP Equipment Under Honhomogeneous Flows Failure

Antonov A., Chepurko V.

•

Obninsk Institute for Nuclear Power Engineering (OINPE)
antonov@iate.obninsk.ru, chepurko@iate.obninsk.ru

Abstract

Describes the different mathematical models of nonhomogeneous in time event streams. A review of the literature on the subject of the study. The basic premise models of nonhomogeneous Poisson processes, gamma processes, geometric renewal process, the trend renewal process, the processes Kijima-Sumita. Defines the main features of the model normalizing of the flow function to calculate the required parameters of reliability. A special case of this model is an nonhomogeneous Poisson process. This model will form the basis of calculation methods of NPP equipment reliability indicators change over time and the conditions of their condition. The paper describes a method for estimating the parameters of NPP equipment reliability, which allows to take into account heterogeneity failure flow. It noted the specificity of the incoming statistical data on failures. Noted the specificity of the incoming statistical data on failures. The application of the model normalizing the flow function to calculate the required parameters of reliability. An example of a practical analysis of the failures of some elements of the reactor protection management system (PMS) NPP Bilibino.

Keywords: Failure flow, nonhomogeneous process, normalizing flow function, renewal function, intensity function

I. Introduction

The technical equipment during their deliberations goes through three stages. At each step the intensity of the flow of failures have a certain tendency. For example during normal operation the failure intensity value is approximately constant. In this case it is assumed homogeneity in time equipment operation process. Reliability indexes are calculated by classical methods. At the stage of running the failure intensity decreases with time on the stage of aging increases (there may be more complex regularities). Consequently, at the stages of running and aging operating time between two consecutive failures taken place are not equally distributed random variables. The flow of failures can not be considered recurrence [1-3]. In view of this the use of traditional methods of calculation of reliability characteristics at these stages incorrectly. In the calculations of reliability characteristics necessary to take into account the inhomogeneity of of the failure flow in time.

Consider the literary sources, the authors of which relate to the problem of the failure flow heterogeneity. Separately, we note [2,5-7]. Tutorial [2] is a fairly complete exposition of the current state of the mathematical theory of reliability. The most important issues addressed in the handbook should include the study of various accounting models of aging, degradation, accelerated testing models, etc. The monograph [5] devoted to the review and study of the theory of point processes. In [6] describes some of the models of nonhomogeneous processes of aging accounting models, etc. Manual [7], partly subsumed in [2], is entirely devoted to models of inhomogeneous renewal processes, such as nonhomogeneous Poisson processes, gamma processes, the trend renewal processes, geometric processes, processes and models Kijima, normalizing flow function (NFF).

For the first time the emergence of heterogeneous processes should include nonhomogeneous Poisson process- NHPP-process. Poisson process is called nonhomogeneous if the function of the intensity $\lambda(t)$ of the depends on the time. The intensity may be either a deterministic or random. The most detailed and complete property of this kind of processes were investigated in [2,5,7]. It should be noted that the failure rate is defined as the intensity ratio of the average number of failures – $N[t,t+\Delta t]$ that occurred in the interval $[t,t+\Delta t]$ to the length of the interval Δt:

$$\lambda(t) = \lim_{\Delta t\to 0}\frac{E\left(N[t,t+\Delta t]\right)}{\Delta t}.$$

The renewal process is necessary more detailed description, which is carried out such concepts as stochastic intensity and conditional intensity function (CIF), see. [2,5,7].

The next type of nonhomogeneous renewal processes are gamma processes, first appeared in the article [8]. Inhomogeneity of the gamma process (IGP) is called the multiplicity k of the process, formed by the flow of failures points $\{\tau_{kn}\}$, ie points τ_k, τ_{2k}, τ_{3k},... . The mathematical model of the process, which is, in fact, a generalization NHPP-process can be interpreted as follows. Let us consider NHPP-process with intensity function $\lambda(t)$. Assume that there is every k-th event process. At this point the flow is meant as impacts, i.e. failure occurs only on the occurrence of each k-th shock. If, for example, $k=4$ then every fourth load will cause failure. Thus, the IGP-process actually is sparse NHPP-process, each of which is k-th point. In the particular case, $k=1$ the model is reduced to the usual NHPP-processes.

In [9-11] describes a model object changes efficiency, presented equation to calculate availability. Process equipment operation is described by the progressive degradation. The heterogeneity of the flow of events is accounted for as a change in the distribution function of operating time between failures, and recovery time of the distribution function. The study model is a geometric process. The properties of this type of processes described in the books mentioned above [2,6,7]. It is worth noting that the model geometry process is fairly new and many of its properties has not been studied thoroughly. The most interesting seems the problem of determining the asymptotic properties of the failure intensity of this type of processes. In [12, 13] are devoted to the point and interval estimation coefficient degradation of geometrical processes, the study of well-known and little-known features of these processes.

The following model of non-homogeneous recovery processes, in fact, is a "bridge" between the (fully) renewal (like new) and not fully renewal (as before failure) systems. She first appeared in [14].

GRP-inhomogeneous flows pattern is a flow formed by time to failure Δ_n with the following conditional distribution functions:

$$F_{\Delta_n}\left(x\,|\,V_{n-1}=y\right)=\frac{F\left(x+y\right)-F\left(y\right)}{1-F\left(y\right)};$$

$$V_n = V_{n-1}+q\Delta_n = q\sum_1^n \Delta_i,\ V_0=0 \text{ – Kijima model GRP-1;}$$

$$V_n = q\left(V_{n-1}+\Delta_n\right)=\sum_1^n q^{n+1-i}\Delta_i,\ V_0=0 \text{ – Kijima model GRP-1;}$$

Note that V_n- virtual age of the system, see [6,14,15]. Kioima models allow to take into account the incomplete recovery of the failed element. In fact, this is a very important feature of the model. Until now it was assumed that after a failed repair of the technical system is returned to its original condition - like new. However, even after the overhaul, a number of replacements of old items with new items, the system as a whole can hardly be considered completely new. This is just an idealized assumption allows to simplify the mathematical calculations.

Trend renewal process -TRP is fairly new and is closest to the model of normalizing the function. She first appeared in [16]. We define this type of processes. Let $\lambda(t)$ – non-negative random function defined for $t \in [0, \infty)$, and $\Lambda(t) = \int_0^t \lambda(u)du$. Process $\tau_1, \tau_2, ...$ is a trend renewal process, if $\Lambda(\tau_1)$, $\Lambda(\tau_2)$,... is an ordinary recovery process. The cumulative distribution function of time to failure $F(x)$ and his expectation 1. The function $\lambda(t)$ is called the trend of the process. It should be noted that, generally speaking, $\Lambda(t)$ not a renewal function. Description taken from the source. Later, the requirement on the expectation of the authors of the model refused, saying that such a requirement. Only necessary for the model to be unique.

Let us consider sources of which the authors used in the research model of NFF. The method of accounting of heterogeneity using NFF model is described in [17-21], in which the properties of the resulting processes are studied in sequence. These works are entered asymptotic characteristics similar meaning to the coefficient of readiness, the first results concerning the study of the behavior laws of distribution of the *i*-th time to failure. In [17-19] presented an equation for determining the function of an arbitrary allocation of time to failure under the conditions of the event flow heterogeneity, knowing that you can evaluate, for example, the remaining service life. In [18] obtained the distribution function of the second and subsequent developments up to the power failure pattern NFF. In [19] derived the equations to calculate the average direct and inverse average remaining time based on the event flow heterogeneity. In [20, 21] the model of joint event flow for the calculation of the coefficient of readiness in terms of the event flow heterogeneity, the idea that some overlap with the two-dimensional renewal process [22]. In [20] also presented equation to calculate the resource characteristics and an example of their calculation. In [23] proposed a method for treating inhomogeneous flow of statistical data on failures. The authors present this kind of feedback NFF, which would lead to a heterogeneous flow of failures simple flow. They find an expression for the distribution function of any developments. That is, in fact, the authors used a model of an nonhomogeneous Poisson flow, which is a special case of the model NFF.

The purpose present work is to describe and research methodology for assessing NPP equipment reliability indicators to take into account the possible inhomogeneity of the flow of failures and demonstration of the results of applying methods on real data obtained from operating experience.

II. Initial data

The main sources of information on the operation of NPP facilities are “defects journal” a passport and technical descriptions of the equipment, certificate of technical condition of objects and a number of other documents.

The existing NPP procedure for collecting statistical information on faults reveals the date of failure detection object from the set of the same elements, and the reason why the failure occurred. In this often is not possible to identify a failed object. Suppose that the statistical information delivered for analysis, presented as follows (see table 1):

m- the number of elements in aggregate similar objects;

ν_i - the number of failures in the *i*-th observation interval.

After another failure, repair is of this piece of equipment. The recovery time of the object is assumed to be negligible compared to the time to failure. Broken objects are recovered and returned to the system for later use. Thus, we have grouped expression failure flow. Also, we assume that the failure rates are not equally distributed (generally speaking) and there is a certain pattern in the changing of the law of distribution with changes in the observation interval (index) *i*. For example, we will process the statistics on failures of two elements PMS- compensates neutron camera

(CNC56) and protection amplifier of the speed (PAS). The failure rate of these elements are shown in Figure 1.

Table 1: *Example of presentation of statistical information about failures*

Year of exploitation	1974	1975	1976	…	2015
Failure rate ν_i	5	3	4	…	0
m	25				

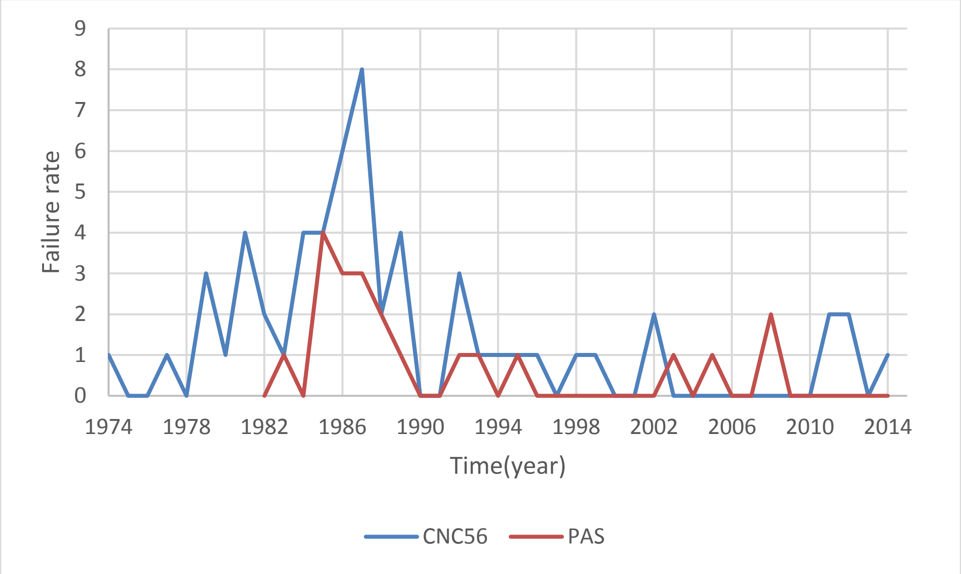


Figure 1: *Failure rate of CNC56 and PAS*

Analysis of the data presented in the form of a group the failure rate is a a nontrivial problem, as the classical methods of calculation of reliability indicators require input data in the form of a known operating time between failures. Methods for calculating the reliability of indicators on statistical information about the grouped failure renewal items worked enough. Classic algorithms outlined in [3, 27, 28], in the presence of the grouped data allow to obtain histogram estimation failure flow parameter. However, the definition of recovery by the equation (see e.g. [1]) on the histogram evaluation of the failure flow parameter distribution density may result in some intervals of negative density values. This is contrary to the basic property of this characteristic. Consequently, this method of calculation should be recognized as incorrect [24-26].

We propose two possible approaches to overcome this problem. The first is based on the assumption that the flow of failures is the simplest. In this case, the failure rate is estimated parameter constant, and the distribution is exponential with a failure rate that is calculated based on statistical information. The second approach is more flexible and is based on the histogram smoothing estimation failure flow parameter, the method of nuclear non-parametric estimates of the flow of the [24-26].

And in fact, and in another case method is based on the assumption of homogeneity of the flow of failures. However, the statistical study of the flow of failures nature suggests that, for example, for Bilibino NPP some of the investigated elements PMS a heterogeneous forms of failure flow of time. In particular, this applies to the CNC56 and PAS.

Appropriate statistical criteria for determining of the hypothesis of a uniform stream of test failures are presented in [4, 20] and we shall not be considered. Nevertheless, by analyzing Fig. 1 can be seen in the failure rate heterogeneity. Over time, the frequency of the a homogeneous flow of failures should stabilize. However, in our case there is a surge of failures in 90 years and the relatively low incidence in the future.

After deciding that the PMS investigated element forms the assumption is made a heterogeneous flow of failures that flow obeys a model normalizing the flow function, the essence of which is set out below.

III. NFF-model

Let us consider mathematical model [2, 7, 17-21], consider the possibility of "distortion" flow of events and allows to determine the parameters of reliability elements, provided that the probability characteristics of the process of change over time. In this model, the actual a heterogeneous flow of failures is the display of a homogeneous flow of events using the monotonic transformation $\Psi(x)$, called normalizing the flow function (NFF) or the function of the inhomogeneity.

The heterogeneity of the flow of events given by $\Psi(x)$ function, the role of which is as follows. Applying this function to hypothetically "abstract" homogeneous flow of failures, we should be getting close to the "real" flow. Using the inverse transformation of "real" flow is roughly homogeneous flow of events. In the "real" flow may be present condensations place (thinning) - when at a certain time interval the number of events will be substantially greater (or less) the number of events in neighboring, similar in duration intervals.

Fig. 2 shows a homogeneous flow of events in the transformation using arbitrary flow function $\Psi(t^*)$. Events homogeneous and inhomogeneous flow of events displayed on the X-axis and Y-axis respectively. The Y-axis of Fig. 2 shows the actual flow of failures with the stages of running and aging when the relatively high failure rate. When the non-linear mapping $\Psi(\cdot)$ of the change will occur over time from cycle to cycle distribution law time between failure. By cycle is meant the work of an element of the system from the beginning of its operation (installation or after repair) to failure, after every repair and installation of the system begins a new cycle of the item. The duration of each cycle of operation is exactly equal to the corresponding time between failures. If a uniform flow of failures in time, his law remains unchanged with the passage of time (from cycle to cycle).

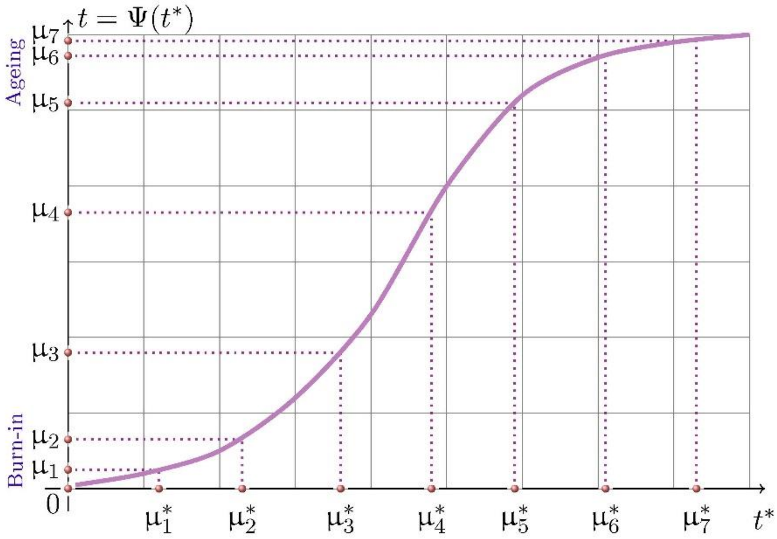


Figure 2: *NFF model*

If the flow is not homogeneous, the law of distribution of operating time will vary depending on the operation cycle. We now turn to the formal description of the essence of the model normalizing the flow function.

As mentioned above, the basic idea is to build a model of NFF continuous strictly monotone increasing mapping abstract recurrent flow of events in the real flow of events [2, 7]. This abstract flow, obviously, will have a dimension of function $\Psi^{-1}(t)$, where t - time. Suppose that system restore is instantaneous.

Definition. Let $\xi_1,\xi_2,\ldots$ *– independent identically distributed (i.i.d) random variables. They are essentially non-negative operating time between failures abstract homogeneous flow with cumulative distribution function (CDF)* $F(x)$. μ_n^* *– time of the n-th event of such a flow, i.e.*

$$\mu_n^* = \sum_{i=1}^{n} \xi_i . \qquad (1)$$

Let $\Psi(t)$ *– be a continuously differentiable strictly increasing function on* $[0;\infty)$*, and* $\Psi(0)=0$.

Then the sequence $\mu_1,\mu_2,\ldots$ *defined by the formula*

$$\mu_n = \Psi\left(\mu_n^*\right); \quad n=1,2,\ldots; \quad \mu_0 = 0, \qquad (2)$$

is the renewal process NFF-model: $\mathrm{NFF}\left(F(x),\Psi(\cdot)\right)$.

Obviously, *i-th* operating time between failures will be determined as follows:

$$\zeta_i = \mu_i - \mu_{i-1} = \Psi\left(\mu_i^*\right) - \Psi\left(\mu_{i-1}^*\right). \qquad (3)$$

The value of ζ_i shall call duration *i* cycle of the system. Similarly, the classical theory of renewal, the sequence $\zeta_1,\zeta_2,\ldots$ can also be defined as renewal process.

For this model, renewal function is given by

$$\tilde{\Omega}(t) = \Omega\left(\Psi^{-1}(t)\right), \qquad (4)$$

where $\Omega(t) = F_\xi(t) + \int_0^t \Omega(t-\tau)\, f_\xi(\tau)\, d\tau$ - renewal function abstract failure flow (see [2,7]).

It is also proved the asymptotic behavior of the renewal function:

$$\lim_{t\to\infty} \frac{\tilde{\Omega}(t)}{\Psi^{-1}(t)} = \frac{1}{\mathrm{E}\xi}, \quad \tilde{\Omega}(t) \sim \frac{\Psi^{-1}(t)}{\mathrm{E}\xi}, \qquad (5)$$

where ξ - abstract operating time between failures, $\mathrm{E}\xi$ – its expectation.

The intensity failures NFF model will be equal to:

$$\tilde{\omega}(t) = \left[\Psi^{-1}(t)\right]' \omega\left(\Psi^{-1}(t)\right), \qquad (6)$$

where $\omega(t) = f_\xi(t) + \int_0^t \omega(t-\tau)\, f_\xi(\tau)\, d\tau$ - intensity failures of abstract flow.

Asymptotically [2,7]:

$$\lim_{t\to\infty} \frac{\tilde{\omega}(t)}{\left[\Psi^{-1}(t)\right]'} = \frac{1}{\mathrm{E}\xi}, \quad \tilde{\omega}(t) \sim \frac{\left[\Psi^{-1}(t)\right]'}{\mathrm{E}\xi}. \qquad (7)$$

A nonhomogeneous Poisson process (NHPP) is a special case of an inhomogeneous flow of events model [2,7]. If we assume that the real flow of failures is described by the model of an nonhomogeneous Poisson process in time - NHPP, then the flow will be abstract usual homogeneous Poisson process (elementary stream) with an intensity of 1. The intensity of the process will be equal

NHPP

$$\lambda(t)=\left[\Psi^{-1}(t)\right]'. \tag{8}$$

Symbolically, this can be written as:

$$\mathrm{NHPP}\left(\lambda(t)\right)=\mathrm{NFF}\left(1-e^{-x},\Psi(t)\right), \tag{9}$$

where $\lambda(t)$ defined by the expression (8).

Within the framework of these two models and the subsequent statistical analysis of baseline information will be made. More specifically, in both cases NFF- model will be applied to the parameter evaluation of function heterogeneity $\Psi(t)$.

In one model, will attend nonparametric density estimation abstract time between failures $f_\xi(x)$, and in the other it will be assumed that $f_\xi(x)=e^{-x}$. In the latter case, we make the assumption that there NHPP process. In view of the foregoing, the first NFF model can be called semi-parametric and parametric second. Build a fully parametric model hard. Firstly, the nonhomogeneity function must satisfy the necessary conditions. Secondly, they must be sufficiently simple calculations not only the function but also the inverse to it and its derivatives.

In terms of mathematical statistics further parameterization of the task is carried out by using an NHPP model. Usually the decision of the parametric task somewhat simpler than nonparametric, while the result has the necessary smoothness. Moreover, the accuracy of the results may be somewhat higher than the results obtained in nonparametric formulation. However, if the prerequisites of parametric models prove to be incorrect, the relative efficiency of the estimates in comparison with the non-parametric counterparts would be extremely low.

Let us consider methods of assessment of heterogeneity functions.

IV. Estimation of heterogeneity function

From (5) it follows that the function heterogeneity $\Psi(t)$ asymptotically uniquely determined from renewal function $\tilde{\Omega}(t)$. Character of interrelation functions next $\tilde{\Omega}(t)$ □ $\frac{m}{\mathrm{E}\xi}\Psi^{-1}(t)$, where m - number of similar objects under observation.

Thus, the problem consists in the qualitative selection (evaluation) functions $\Psi^{-1}(t)$ on the basis of the renewal function. This is a classical problem of mathematical statistics, which can be solved by the method of least squares.

Consider the example of evaluation the reverse of function of the inhomogeneity- $\Psi^{-1}(t)$. As an example, consider the statistics obtained from the experience of operating elements CNC56 and PAS working as a part of standard equipment power EGP-6 NPP Bilibino. Statistical information on faults, refer to Tables 2 and 3. In this case, for the CNC56 the number of flows $m=16$, for PAS- $m=12$.

Table 2: Statistical information on failures elements CNC-56. *m*=16.

Year	№	ν_i	Year	№	ν_i	Year	№	ν_i
1974	0	1	1988	14	1	2002	28	2
1975	1	0	1989	15	2	2003	29	0
1976	2	1	1990	16	0	2004	30	0
1977	3	1	1991	17	3	2005	31	0
1978	4	8	1992	18	3	2006	32	0
1979	5	7	1993	19	1	2007	33	0
1980	6	0	1994	20	1	2008	34	0
1981	7	5	1995	21	2	2009	35	0
1982	8	2	1996	22	2	2010	36	0
1983	9	3	1997	23	0	2011	37	2
1984	10	4	1998	24	1	2012	38	2
1985	11	4	1999	25	1	2013	39	0
1986	12	9	2000	26	0	2014	40	1
1987	13	11	2001	27	0			

We construct a nonparametric estimation averaged renewal function the usual method based on the determination of the ratio of the accumulated frequency of failures $\Omega(t)$ to a given point in time t to the number of observed elements *m*.

$$\tilde{\Omega}(t) = \Omega(t)/m\,.$$

Visual analysis of nonparametric estimation of the renewal function (points in Fig. 5) shows that superficially reminds function of the probability distribution function. The richest in terms of modeling of various forms of random variable distribution of parametric laws is the Weibull-Gnedenko. The range of renewal function will not be a segment $\left[0;1\right]$ and will be semi-infinite straight $\left[0;\infty\right)$. It is expedient to multiply the distribution function of the Weibull-Gnedenko by a constant *a*:

$$\Psi^{-1}\left(x\right) = \begin{cases} F\left(x\right) = a\left(1-exp\left(-l\cdot x^{b}\right)\right), x \le T \\ Cx, x > T \end{cases}. \tag{10}$$

Table 3: Statistical information on failures elements PAS. *m*=12.

Year	№	ν_i	Year	№	ν_i	Year	№	ν_i
1982	0	0	1993	11	1	2004	22	0
1983	1	1	1994	12	0	2005	23	1
1984	2	0	1995	13	1	2006	24	0
1985	3	4	1996	14	0	2007	25	0
1986	4	3	1997	15	0	2008	26	2
1987	5	3	1998	16	0	2009	27	0
1988	6	2	1999	17	0	2010	28	0
1989	7	1	2000	18	0	2011	29	0
1990	8	0	2001	19	0	2012	30	0
1991	9	0	2002	20	0	2013	31	0
1992	10	1	2003	21	1	2014	32	0

The model parameters are estimated, as mentioned above, OLS and their values are shown in Table 4.

Table 4: Estimates of the parameters of the nonhomogeneity function

Name	l	a	b	T	C	R^2
CNC56	0.0011	2.5595	3.1990	37	0.1267	0.9859
PAS	0.0338	1.7649	1.1453	21	0.0255	0.9816

Research has shown (see. Figure 3 a, 4 a), which parameterization Weibull-Gnedenko ideal only for a certain time interval $\left[0;T\right]$, where for $T=37$ years about CNC56, and $T=21$ for PAS. We can assume that the heterogeneity of function in the area $\left[T,41\right]$ for CNC56 and $\left[T,32\right]$ for PAS is described by a linear function. Her subsequent behavior can only predict. As the most appropriate forecast model was chosen the same linear growth model. Thus, the parameter T - a point in time immediately preceding the last failure (failure of one or a group). It is determined visually. The angular coefficient is determined by the OLS for evaluating restoration of function in the area $\left[T;41\right]$ for KNK56 and $\left[T;32\right]$ for PAS. Estimation the slope on the "final" phase of operation is clearly more consistent and accurate data available, because it does not clearly overestimated the value of the initial phase of operation. Fig. 3a, 4a is a graph of the reverse NFF – $\Psi^{-1}(t)$ (trend, solid line) and estimation $\tilde{\Omega}(t)$.

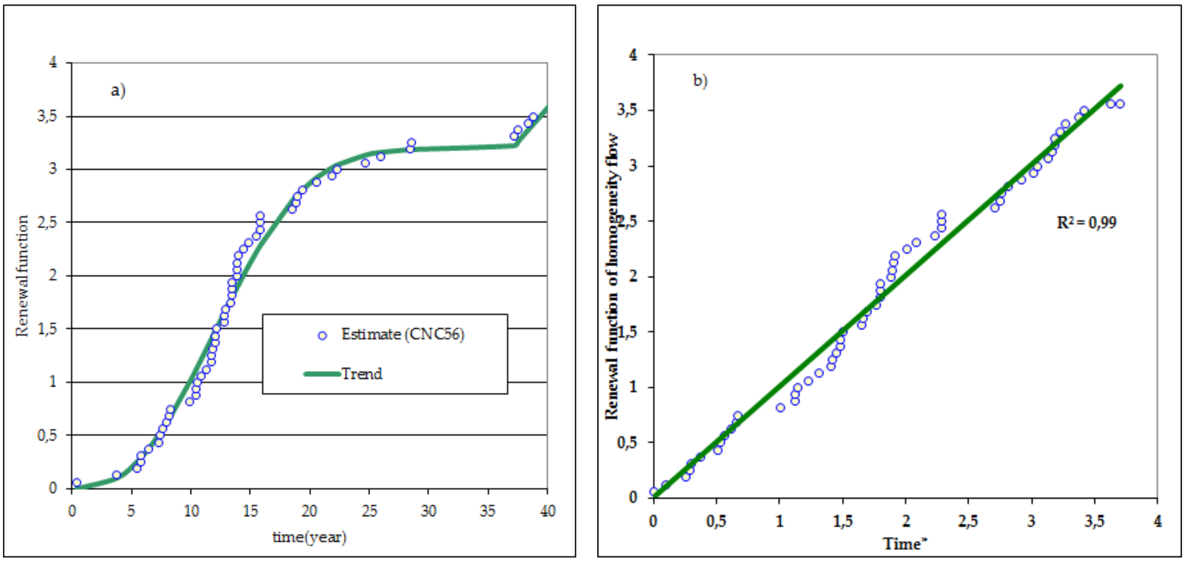


Figure3: *a) Estimate* $\tilde{\Omega}(t)$ *and its trend NFF model* $\Psi^{-1}\left(x\right)$ *b) Normalazing estimate* $\tilde{\Omega}(t^{*})$ *and its linear trend NFF model* $\Psi^{-1}\left(x\right)$

V. Failure flow straightening

The essence of this stage reduced to transformation of an inhomogeneous flow of failures in the abstract homogeneous flow, using the relation

$$t^{*}=\Psi^{-1}\left(t\right).$$

In this case, obviously, t^{*} has the meaning of "abstract" time, and t - represents the actual operating time on the time axis. Thus, by the time t^{*} the flow axis to abstract the number of failures occurs, the corresponding point on the "real" axis t. After converting the time axis construct a "normalized" renewal function to abstract time. Fig. 3b, 4b is a graph of the normalized renewal function $\tilde{\Omega}\left(t^{*}\right)$ after conversion to the time axis.

The result was a homogeneous "rectified" failure flow. The figure also shows the approximating function, which is represented as a linear trend also shows the value of the coefficient of determination R^2, which is the usual square of the correlation coefficient. The closer this coefficient is to 1, the greater the proportion of the variance of the dependent variable explained by the considered model of addiction.

The results shown in Fig. 3b, 4b show that the failure rectified flow has a high level agreement with a linear model.

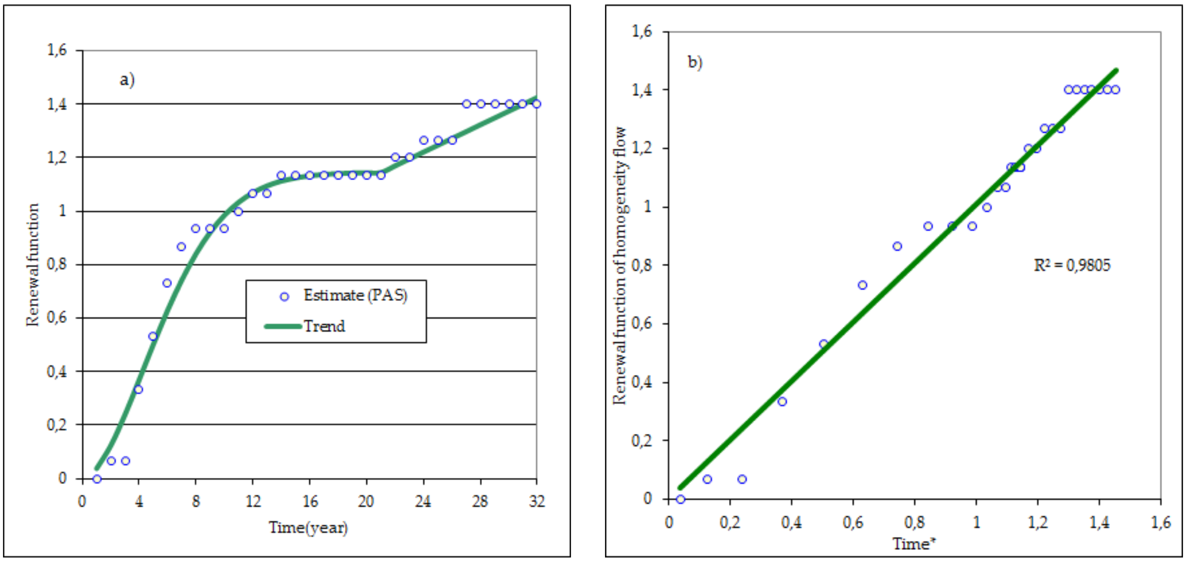


Figure 4: *a) Estimate* $\tilde{\Omega}(t)$ *and its trend NFF model* $\Psi^{-1}\left(x\right)$ *b) Normalazing estimate* $\tilde{\Omega}(t*)$ *and its linear trend NFF model* $\Psi^{-1}\left(x\right)$

VI. Nonparametric estimation of the failure intensity of "rectified" failure flow

Estimation parameter rectified flow of events for the grouped data can be obtained by the following methods (see [2, 4, 24-26].)

1. *Histogram.* Estimation is determined by the formula

$$\hat{\omega}_{hist}(t)=\frac{\nu_t}{m\cdot\Delta},$$

where ν_t – the number of failures recorded in the *i*-th observation interval on the axis of "abstract" time; m – the number of similar objects; $\Delta=t_i-t_{i-1}$ – length of the interval, which are realized on the number of failures ν_t.

2. *Kernel.* Kernel estimation is determined by the formula

$$\hat{\omega}_{kern.}(t,h)=\sum_{i=1}^{s}\frac{\nu_i}{m\cdot(r_i-l_i)}\cdot\left[G\left(\frac{t-l_i}{h}\right)-G\left(\frac{t-r_i}{h}\right)\right]+\varepsilon(t), \tag{10}$$

where *t* – "abstract" time; *h* ($h>0$) – smoothing parameter; $\vec{\nu}$ – frequency array; l_i and r_i – the left and right boundary of observation interval; $G(x)=\frac{1}{\sqrt{2\pi}}\int\limits_{-\infty}^{x} e^{-u^2/2}du$ – CDF of the standard normal distribution; $\varepsilon(x)$ – systematic error, which is defined by the formula [2]:

$$\varepsilon(t,n,m)\approx\frac{1}{2a}\operatorname{erfc}\left(\frac{aN-t}{\sqrt{2N\sigma}}\right)+\frac{\sigma}{\sqrt{2\pi a}}\frac{\sqrt{N}}{aN+t}e^{-\frac{(aN-t)^2}{2n\sigma^2}}$$

.

Fig. 5a, 6a presents estimates calculated histogram– $\hat{\omega}_{hist}(t)$ and kernel– $\hat{\omega}_{kern.}(t,h)$ techniques.

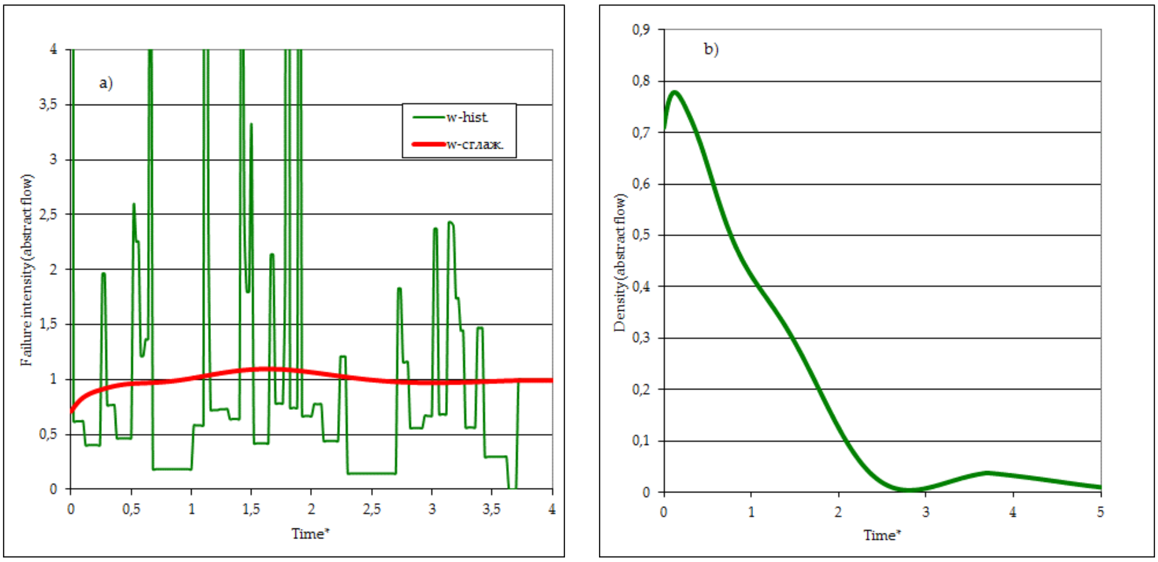


Figure 5: Histogram $\hat{\omega}_{hist}(t)$ and kernel (smoothed) $\hat{\omega}_{kern.}(t,h)$ estimation rectified failure intensity CNC56; b) estimate of the density of the abstract operation times between failures $\hat{f}_{\xi}(t)$ CNC56.

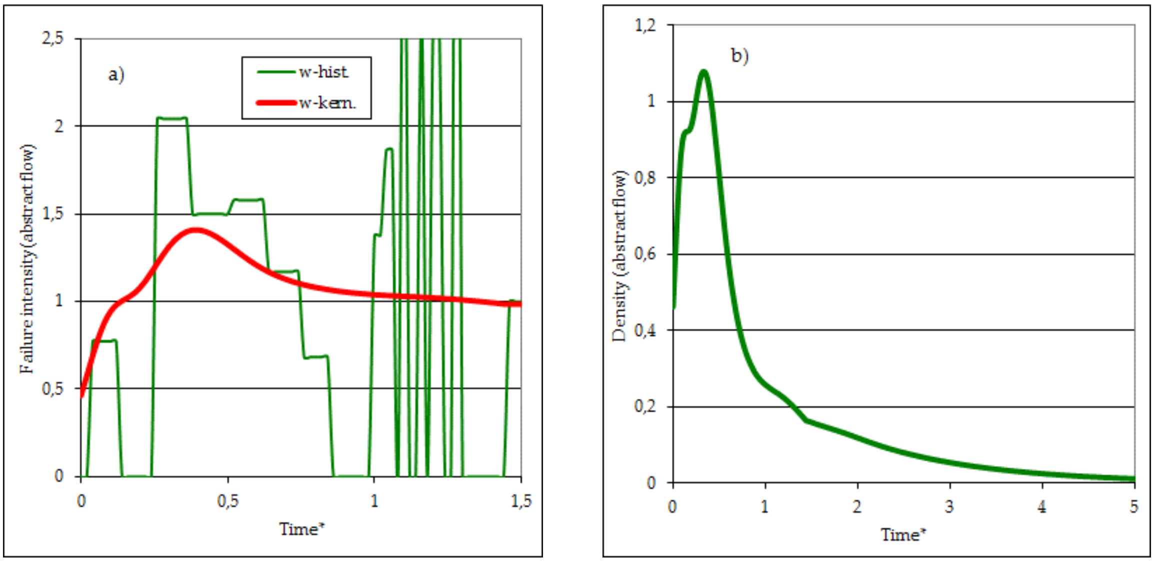


Figure 6: Histogram $\hat{\omega}_{hist}(t)$ and kernel (smoothed) $\hat{\omega}_{kern.}(t,h)$ estimation rectified failure intensity PAS; b) estimate of the density of the abstract operation times between failures $\hat{f}_{\xi}(t)$ PAS.

Direct substitution histogram estimation of failure intensity in the renewal equation may lead to some negative timeslots density distribution. It is contrary to the properties of the density. Therefore, for further calculations will use the kernel estimate of failure intensity, allows to obtain a solution of the renewal equation, which has the necessary properties of density distribution.

VII. Estimating the density distribution of the "abstract" operating time between failures

The density of operating time between failures a homogeneous flow of events in the "abstract" the time axis can be determined by solving the renewal equation – Volterra equation of the second kind [1]:

$$\hat{f}_{\xi}(x) = \omega_{kern.}(x) - \int_{0}^{x} \hat{f}_{\xi}(u)\omega_{kern.}(x-u)du\,, \tag{11}$$

where $\omega_{kern.}(x)$ – kernel estimate of failure intensity.

Fig. 5b, 6b shows the estimate of the density of the abstract operating time obtained based on the assessment of kernel rectified the failure intensity. This estimate of density $\hat{f}_{\xi}(x)$ has a non-negative function satisfying the normalization condition. It is because of these reasons was chosen smoothing parameter *h* in (10).

For further calculations on the NFF model will use this estimate distribution density operating time abstract homogeneous stream of refusals. Recall that the model for NHPP

$$\hat{f}_{\xi}(x) = e^{-x} \text{ and } \omega(x) = 1\,. \tag{12}$$

VIII. Estimation of distribution of operating time – ζ_i.

Let the length of the *i*-th cycle of working capacity ζ_i - is the *i*-th operating time between two successive failures of the inhomogeneous flow of events. In [2, 7] gives expression to find the value of the distribution function ζ_i in the framework of NFF model:

$$F_{\zeta_i}(t) = \int_{0}^{\infty} f_{\mu_{i-1}}(u) F_{\xi}\left(\Psi^{-1}\left(t+\Psi(u)\right)-u\right)du\,, \tag{13}$$

where $\mu_k = \sum_{i=1}^{k} \xi_k$ – the time of the *k*-th event "abstract" homogeneous flow of failures; $F_{\xi}(x)$ – CDF of "abstract" operating time; $f_{\mu_{i-1}}(t) = \int_{0}^{t} f_{\mu_{i-2}}(t-u) f_{\xi}(u)du$.

The CDF and the density to failure of the first time are determined by the formulas:

$$F_{\zeta_1}(t) = \mathrm{P}\left(\zeta_1 < t\right) = F_{\xi}\left(\Psi^{-1}(t)\right), \quad f_{\zeta_1}(t) = \left(\Psi^{-1}(t)\right)' f_{\xi}\left(\Psi^{-1}(t)\right). \tag{14}$$

By differentiating (13), we find an expression for the density of the duration of the cycle performance:

$$f_{\zeta_i}(t) = \int_{0}^{\infty} f_{\mu_{i-1}}(u) f_{\xi}\left(\Psi^{-1}\left(t+\Psi(u)\right)-u\right)\cdot\left(\Psi^{-1}\left(t+\Psi(u)\right)\right)' du;\ i = 2,3,\ldots, \tag{15}$$

where $f_{\xi}(x)$ – density of the "abstract" operating time.

The CDF of the first time to failure ζ_1 under the NHPP model is defined as follows:

$$F_{\zeta_1}(t)=1-e^{-\Lambda(t)};\ f_{\zeta_1}(t)=\Lambda'(t)e^{-\Lambda(t)}, \qquad (16)$$

where $\Lambda(t)=\Psi^{-1}(t)$.

CDF and density of the remaining operating time between failures within NHPP model will be equal

$$F_{\zeta_i}(x)=1-\int_0^\infty \frac{u^{i-2}}{(i-2)!}e^{-\Lambda\left(\Lambda^{-1}(u)+x\right)}du, \qquad \mathbf{(17)}$$

$$f_{\zeta_i}(x)=\int_0^\infty \lambda\left(\Lambda^{-1}(u)+x\right)\frac{u^{i-2}}{\Gamma(i-1)}\cdot e^{-\Lambda\left(\Lambda^{-1}(u)+x\right)}du;\ i=2,3,\ldots.. \qquad \mathbf{(18)}$$

On basis of the presented formulas The calculation of these characteristics to the statistics available for the elements CNC56 and PAS. We represent the results of calculations of use density distributions for the first, second, third and fourth performance cycles performed for NFF models (Fig. 7a, 8a) and NHPP model (Fig. 7b, 8b). On the basis of the calculated density of the calculations of durations of *i*-functionality cycle. Fig. 9 shows the mean time to the first, second, third and fourth bounce calculated NFF semi-parametric model and parametric models NHPP. Average values were determined by numerical integration of the respective distribution density.

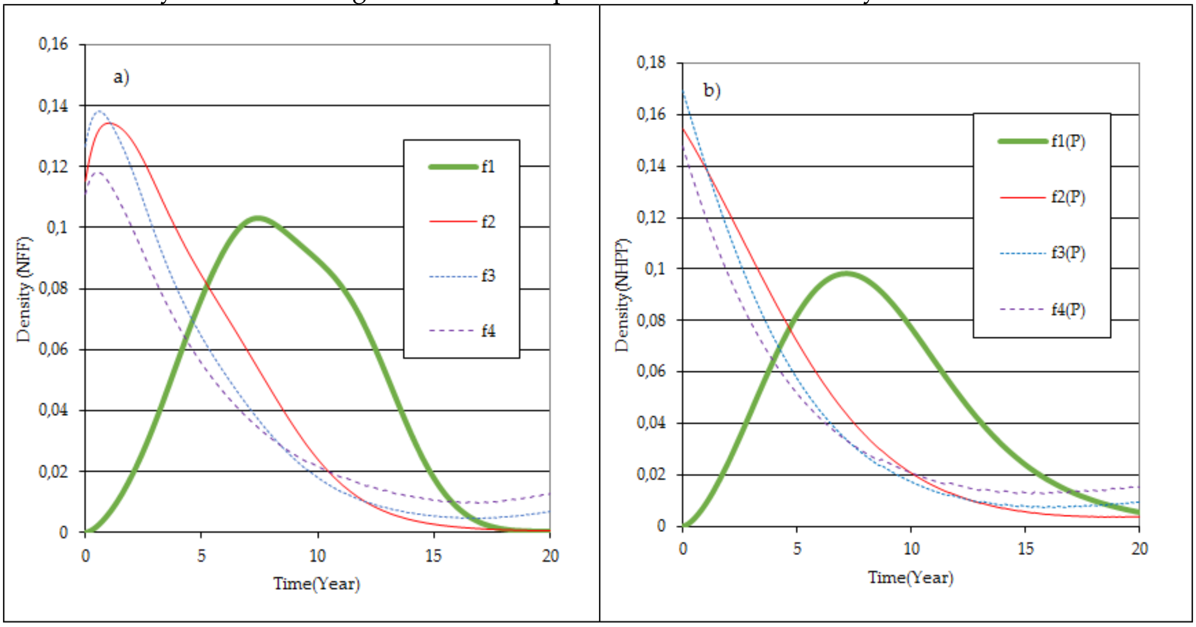


Figure 7: The densities of the four cycles for CNC56: a) NFF, b) NHPP.

By analyzing data on failures CNC56 element shown in Table 1, it can be noted that all failures occurred mainly in the period from 1974 to 1999. Ie for the first 25 years of operation. flow failure $m=16$ form the same elements. By the beginning of 1980 there were 18 failure. Assuming that the operating conditions are the same set of 16 elements, with high probability we can say that each of the elements together broke down at least once. Those. by 1980 for each of the elements together first functionality cycle ended, then the element was replaced and started the second cycle functionality of a particular element. It is advisable to assume that the average first cycle functionality is approximately 8 years. The calculation results are presented in Fig. 7, allow us to estimate the mean value of operating time. You can also note that in the period from 1978 to 1987. There was an increased frequency failure CNC-56. It is equal to about 5 years of failures in a group of similar items in an amount of 16 units. By the beginning of 1985 there were 32 of failure, ie, on average, each element is broken twice. The average value of the second functionality cycle falls on the interval of three to five years (see. Fig. 9a).

The graph functionality density of the second cycle $f_{\zeta_2}(t)$ should shift to the left - the likelihood of small operating time increased, and large declined (Figure 7.). The densities of the 3rd and 4th cycle of about the same and only slightly different from a density of 2 - second cycle. In summary, it can be noted that the behavior of the density of cycle functionality and average operating time adequately describes the input information. Knowing $F_{\zeta_i}(t)$ or $f_{\zeta_i}(t)$, we can find any interesting safety characteristic for an the *i*-th cycle functionality.

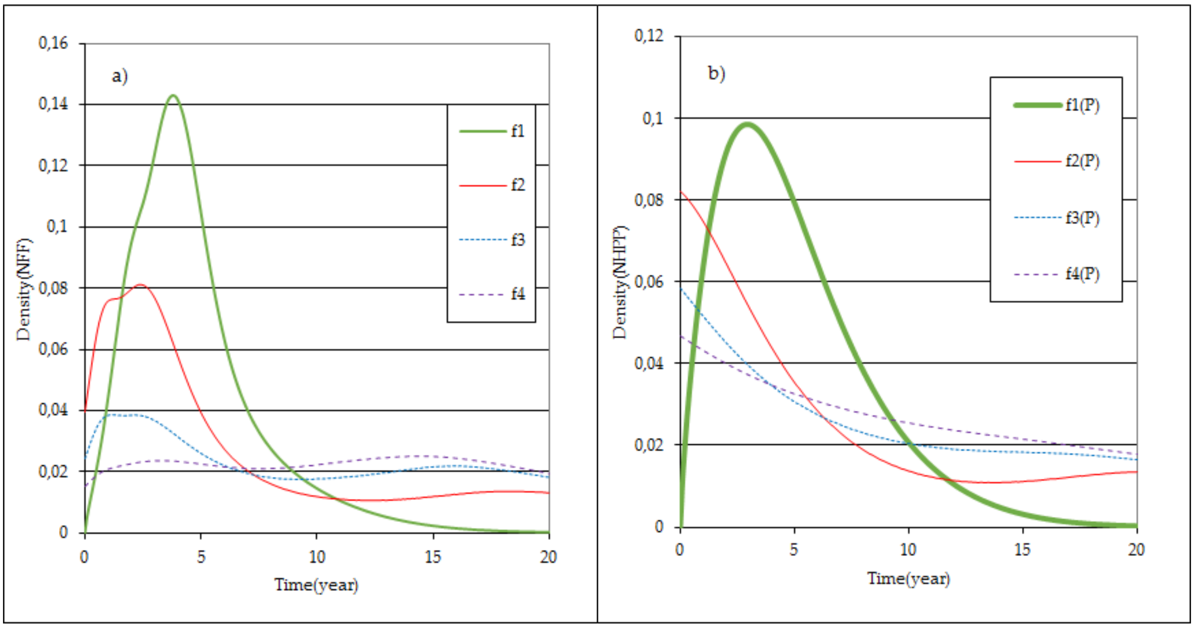


Figure 8: The densities of the four cycles for PAS: a) NFF, b) NHPP.

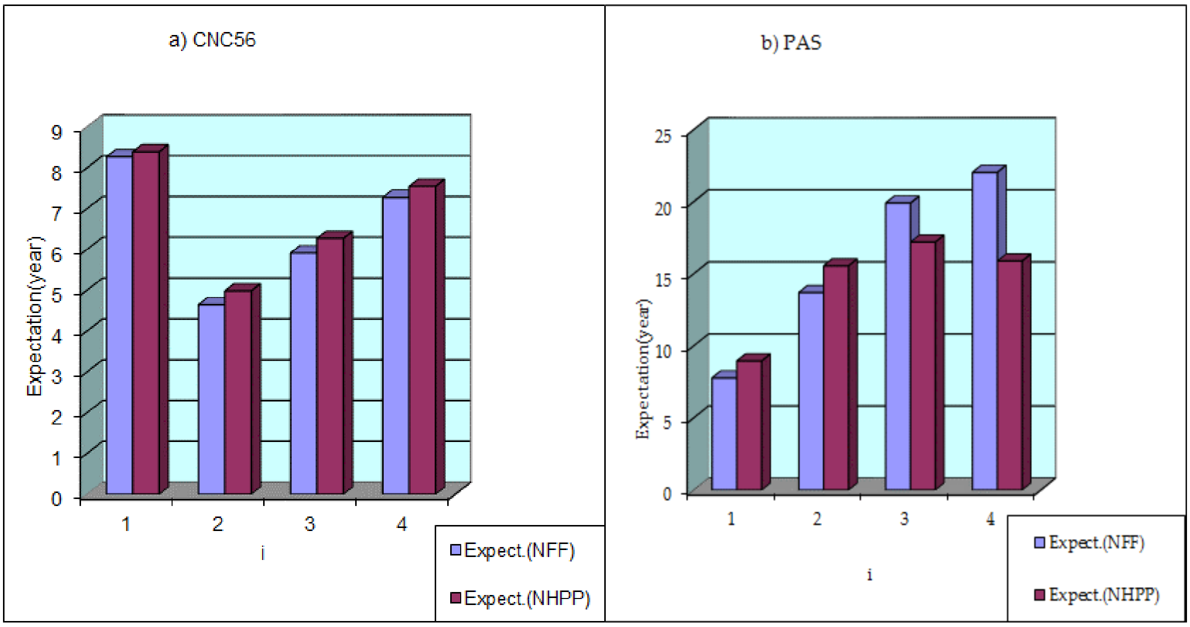


Figure 9: Mean time between failures a) CNC56, b) PAS.

Histograms of mean operating time almost identical, have very different densities and graphics. This suggests that the flow of data elements failure is a NHPP. Therefore, this element can be applied more simple methods of model of an NHPP. In addition, the model of an inhomogeneous Poisson flow is possible to construct confidence intervals.

Now let's analyze the results of calculations for the PAS. This element is in operation since 1982. The failure rate generates $m=12$ identical elements. There was a total of 21 rejected. The mean number of failure is equal to 1.4. Thus, on average, each of the 15 elements already broke once and stored in the second operation cycle. Failures are mainly observed the first 14 years, then they were not there for 13 years, on the 27th, there was a 2 failure. Since there were no failures. Evaluation PPO differs significantly from the constant 1 (see. Fig. 6a). This explains the gradually emerging a significant difference in the distributions (Fig. 8a) and estimates the average operating time (Fig. 9b) NFF calculated by the model and the model of an NHPP. Those. it can be assumed that the behavior of the flow of failures PSM poorly described by the model of an NHPP. Therefore, further focus on the assessment, obtained by the NFF model. Fig. 9b is a tendency to an increase in the average operating time between failures. In the second cycle of mean time between failures is approximately 13 years on tretem- 19.

IX. Estimating resource characteristics

In [2,7], the expression for the calculation in a failure flow heterogeneity of resource characteristics of reliability, as the average reverse residual time $\mathrm{E}R_t$ and average direct residual time $\mathrm{E}V_t$ the remaining time (method of determining the characteristics R_t and V_t homogeneous flow can be found, for example, in [2]). In the case of an inhomogeneous flow NFF model calculations should be carried out according to the formulas:

$$\mathrm{E}R_t = t\cdot\left(1-F_\xi\left(\Psi^{-1}(t)\right)\right)+\int_0^\infty g_R(x;t)\,f_\xi(x)dx, \tag{19}$$

$$\mathrm{E}V_t = \int_{\Psi^{-1}(t)}^{\infty}\left(\Psi(x)-t\right)f_\xi(x)dx+\int_0^\infty g_V(x;t)\,f_\xi(x)dx, \tag{20}$$

где $g_R(x;t)=\int\limits_{\left(\Psi^{-1}(t)-x\right)\vee 0}^{\Psi^{-1}(t)}\left(t-\Psi(u)\right)v(u)du$; $v(x)=F_\xi(x)+\int_0^x v(x-u)\,f_\xi(u)du$;

$$g_V(x;t)=\int\limits_{\left(\Psi^{-1}(t)-x\right)\vee 0}^{\Psi^{-1}(t)}\left(\Psi(u+x)-t\right)v(u)du\,.$$

Calculation of the resource reliability indices for the case NHPP model is greatly simplified.

Average direct residual time:

$$EV_t=\int_0^\infty e^{-x}\Psi\left(x+\Psi^{-1}(t)\right)dx-t\,. \tag{21}$$

Average reverse residual time:

$$ER_t=t-\int_0^{\Lambda(t)}e^{-x}\Psi\left(\Psi^{-1}(t)-x\right)dx\,. \tag{22}$$

Along with these characteristics, you can restore the system to determine the average resource:

$$ED_t = EV_t + ER_t . \qquad (23)$$

In fact, this value will be the average cycle time of the system at the time of inspection.

In the above formulas based on statistical information on failures elements CNC56 and PAS have calculated indicators: average residual direct and reverse time, average life. The calculation results are shown in Fig. 10-13.

The behavior of the characteristics of the data leads to the conclusion that :

- To CNC56 average reverse residual time reaches local maximum of 5 years to the eighth year of operation (1982). Therefore, in the previous period in 1982 element failure occurred, most likely in mid-1978. In 1978, finished the stage failure flow dilution, their intensity increased sharply.
- To CNC56 average reverse residual time reaches a local minimum of 4 years We have 15 year of operation (1989). By the early 1987 peak failure observed. In 1987 he completed phase failure rate of condensation.

The subsequent behavior of the indicator ER_t is characterized by almost linear dependence of its operating time. This is due to the fact that in the interval from 1999 to 2011. failure almost was not.

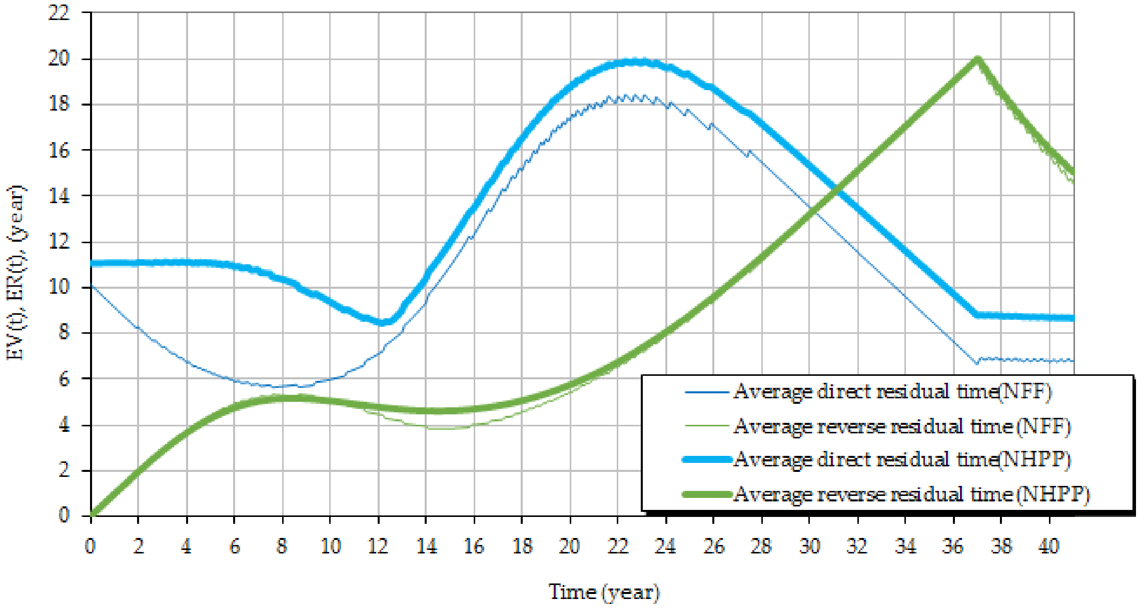


Figure 10: Average reverse residual time ER_t and direct residual time EV_t CNC56

Average direct residual time reaches (by NFF model) local minimum of 5.5 years on the 8 year of operation (1982). Consequently, failure peaked in 1987 (1982 + 5.5). Average direct residual time reaches (by NFF model) a local maximum of 18 years on 22 year of operation (1996). Consequently, the next peak failure can be expected by 2014. Indeed, the failures began to appear in the last 4 years.

In the future, the graph EV_t decreases to 37 years as in the period from 1996 to 2011. there was virtually no failure, and, consequently, less time is left of the current moment of observation before the expected next failure.

The calculations of the direct and reverse residual time allow to predict the remaining service life of products at the time of inspection.

Similar detailed analysis of indicators of resource scheduling can be done for the PAS. But this we will leave to the reader. Consider Fig. 12, which shows the average graphics resource for CNC56. You may notice a local minimum of the characteristics in the 12th year of operation, which is practically the same from 1985 g.- year maximum failure rate.

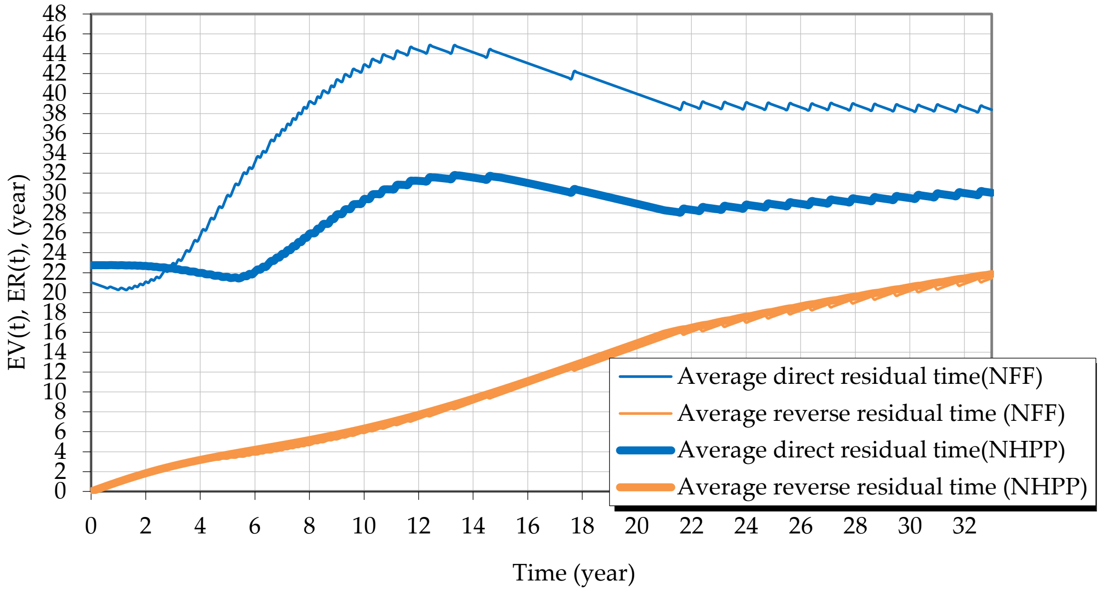


Figure 11: Average reverse residual time $\mathrm{E}R_t$ and direct residual time $\mathrm{E}V_t$ PAS

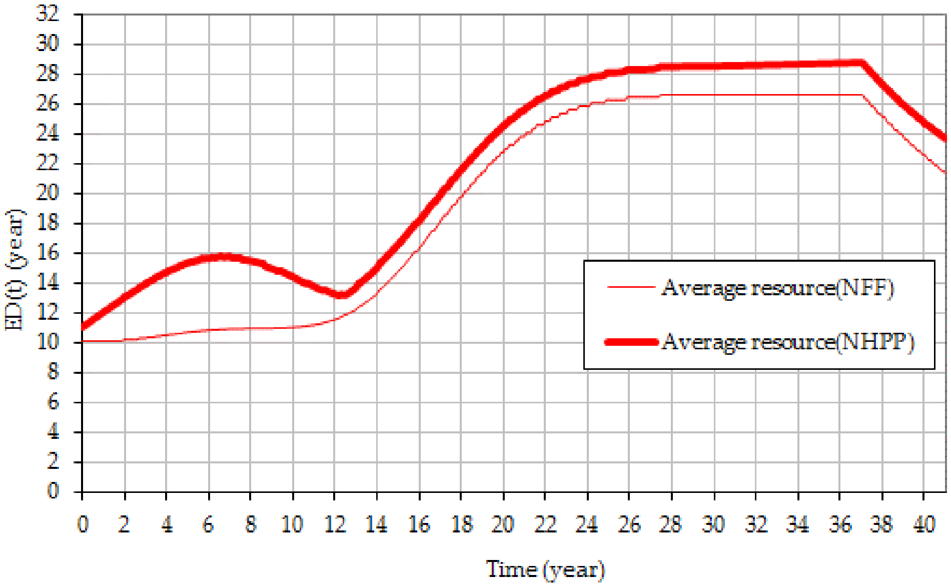


Figure 12: Average resourse $\mathrm{E}D_t$ CNC56

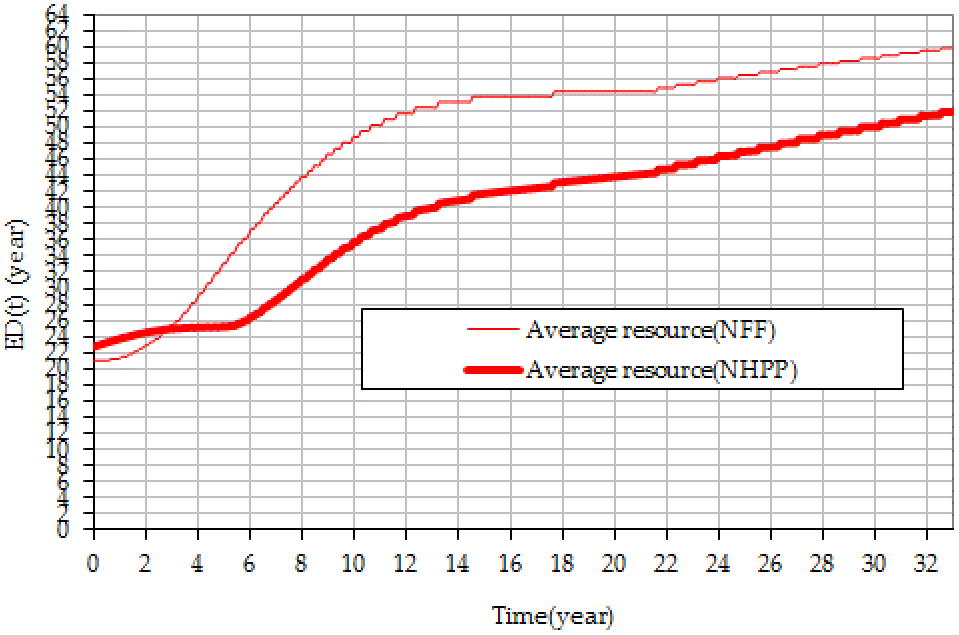


Figure 13: Average resourse ED_t PAS

X. Conclusion

The article describes a new method of analysis of statistical data on failures to estimate the NPP equipment reliability indicators, which allows to take into account the possible heterogeneity of the flow of events. Examples of data analysis at each stage of the study on the basis of statistical information on faults elements CNC56 and PAS derived from operating experience. According to the procedure provided by the calculations of a large group of control components and power protection EGP-6 on the basis of information over a long period of operation (1974 and 2014). The results are presented in [4].

References

[1] Bayhelt F., Franken P., The Reliability and Maintenance. Mathematical approach: first with it, Moscow, Radio and Communication, 1988, 392 pp. (in Russian)

[2] Antonov A.V., Nikulin M.S., Nikulin A.M., Chepurko V.A. Theory of reliability. Statistical Models. Moscow. SIC INFRA-M Publ., 2015. 576 pp. (in Russian).

[3] GOST 27.002-89 Industrial product dependability. General concepts Terms and Definitions. (in Russian).

[4] Probabilistic analysis of the residual resource of reliability indicators subsystems equipment CPS Bilibino on the basis of information about failures in the period 1974-2014. / Moiseev I.F., Antonov A.V. etc. Technical Report, -. M .: VNIIAES, 2015. - 164 p.

[5] Daley D.J., Vere-Jones D. An introduction to the theory of point processes: Vol. 1: Elementary theory and methods. Verlag New York - Berlin - Heidelberg: Springer, 2003. 469 p.

[6] Finkelstein M. Failure rate modelling for reliability and risk. Verlag London Limited: Springer, 2008. 290 p.

[7] Chepurko V.A. Chepurko S.V. Models of nonhomogeneous flows in the renewal theory. Obninsk. INPE Publ., 2012, 164 p. (in Russian)

[8] Berman M. Inhomogeneous and modulated gamma processes.// Biometrica. – 1981. – Vol. 68(1). – pp. 143-152.

[9] Saenko N.B. Accounting for incomplete recovery of elements in the calculation of the

reliability of systems. *Izvestiya vuzov. Priborostroenie.* 1994, v. 37, no. 11-12, pp. 76-79 (in Russian).

[10] Antonov A., Chepurko V. On some characteristics of geometric processes //Journal of Reliability and Statistical Studies; ISSN (Print): 0974-8024, (Online):2229-5666, Vol. 5, Issue Special (2012). pp. 1-14.

[11] Lam Y. Geometric processes and replacement problem // Acta Mathematicae Applicatae Sinica. English Series.– 1988.- Vol. 4(4). – pp. 366-377.

[12] Antonov A., Polyakov A., Chepurko V. Estimation of the model parameters of the geometric process by the method of maximum likelihood // Nadezhnost.-2012.-№ 3 (42) .– pp. 33-41.

[13] Chepurko V. Chepurko S. A method for the detection failure rate heterogeneity equipment NPP // *Izvestiya vuzov. Yadernaya energetika*.- 2012.- № 2 - pp. 65-73.

[14] Kijima M.. Sumita N. A useful generalization of renewal theory: Counting process governed by non-negative markovian increments // Journal of Applied Probability. — 1986. – Vol. 23. – pp. 71-88.

[15] Chumakov I., Antonov A., Chepurko V. Some properties of incomplete recovery Kizhima models // Nadezhnost.-2015.-№ 3 (54) .- pp.3-15.

[16] Lindqvist B.H. The trend renewal process, a useful model for repairable systems // Tillforlitlighet i reparerbara system. Society of Reliability Engineers, Scandinavian Chapter, Annual Conference, Malino, Sweden. — 1993.

[17] Antonov A., Belova K., Chepurko V. On one method of reliability coefficients calculation for objects in non-homogeneous event flows // Mathematical and Statistical Models and Methods in Reliability. Applications to Medicine, Finance, and Quality Control / Ed. By V.V. Rykov, N. Balakrishnan, M.S. Nikulin. –Statistics for Industry and Technology. Springer, 2010. – pp. 51-67.

[18] Antonov A.V., Chepurko V.A. The account of ageing effect in operation of the equipment at the stage of nuclear power plant reliability and safety analysis. / Second International Conference on Accelerated life testing in reliability and Quality control «ALT 2008» (University V. Segalen. Bordeaux 2, France). pp. 35-39.

[19] Ivanova K., Skiba M., Chepurko V. Method for assessing the reliability of nuclear power plant systems performance in a nonuniform flow of failures // *Izvestiya vuzov. Yadernaya energetika*. 2009.№ 4. - pp.29-38.

[20] Antonov A., Ivanova K., Chepurko V. Statistical analysis of the failures of nuclear power equipments, taking into account the failure rate heterogeneity // *Izvestiya vuzov. Yadernaya energetika*. 2011.№ 2. – pp.75-87.

[21] Antonov AV, VA Chepurko Estimation of the reliability of the aging systems like the example of the nuclear power industry systems // Nadezhnost.-2010.-№ 1(33) .- pp.18-29.

[22] Hunter J.J. Renewal theory in two dimensions: Basic results // Advances in Applied Probability. — 1974. — Vol. 6. — Pp. 376- 391.

[23] Sahakyan S., Ostreykovsky V., Chepurko V. The method of processing of statistical data on the reliability of the equipment during the operation of nuclear power plants. // *Izvestiya vuzov. Yadernaya energetika*. 2007.№ 3. Issue 1. - pp. 30-37.

[24] Chepurko V. Kernel estimation of the failure intencity. // Diagnostics and forecasting of complex systems. Coll. scientific. tr. №15 cafes. ACS. - Obninsk: INPE, 2004. - pp. 19-31.

[25] Antonov A., Salnikov N., Khromova M., Chepurko V. An estimate reliability indices recovered technical systems // Information technologies. 2013, №12, pp.56-61.

[26] Antonov A., Salnikov N., Khromova M., Chepurko V. The justification of the nuclear parameter estimation flow of failures of technical systems recovered // Information technologies. 2014, №12, pp.3-8.

[27] Kozlov B., Ushakov I. Handbook on the calculation of grade electronics and automation equipment - M.: Soviet Radio, 1975. - 472 p.

[28] Ostreykovsky V., Antonov A. Assessing the reliability characteristics of elements and systems of nuclear power combined methods. - M .: Energoatomisdat, 1993. - 368 p.

The Development of the New Idea Safety Guide for Design of Instrumentation and Control Systems for Nuclear Power Plants

Gary Johnson

Independent Consultant
Livermore, California
kg6un@alumni.calpoly.edu

Alexander Duchac

International Atomic Energy Agency
Vienna, Austria
a.duchac@iaea.org

Abstract

The International Atomic Energy Agency (IAEA) is a United Nations organization that was formed to "accelerate and enlarge the contribution of nuclear energy to peace, health and prosperity throughout the world." The IAEA prepares Safety Standards in accordance with the IAEA. These Standards are not binding on Member States, but may be adopted by them. The Safety Standards are, however, binding for the IAEA's own activities (safety reviews, technical cooperation missions, training activities), on the IAEA, and on Member States. IAEA Safety Standards are organized into three levels: Safety Fundamentals, Safety Requirements, and Safety Guides. It is necessary to take the measures recommended. Currently nearly 120 safety guides are in effect. The article gives an extensive review of existing documents.

Key Words: Instrumentation and control, safety, nuclear power plants, standards

Background

The International Atomic Energy Agency (IAEA) is a United Nations organizations that was formed to, "accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world [1]." As of February 2016, one hundred and sixty eight nations were members of the IAEA.

The IAEA prepares Safety Standards in accordance with the IAEA Statute which mandates that the IAEA "establishes or adopts… [in consultation with…] standards of safety for the protection of health and minimization of danger to life and property, and provides for the application of these standards." These Standards are not binding on Member States but may be adopted by them. The Safety Standards are, however, binding for the IAEA's own activities (safety reviews, technical cooperation missions, training activities), on Member States in relations to operations assisted by the IAEA, and on Member States wishing to enter into project agreements with the IAEA.

As illustrated in figure 1, IAEA Safety Standards are organized into three levels: Safety Fundamentals, Safety Requirements, and Safety Guides. The Safety Fundamentals are given in one document that establishes the fundamental safety objective and principles of protection and safety for nuclear facilities and activities. Safety Requirements establish an integrated and consistent set the requirements that must be met to ensure the protection of people and the environment, both now and in the future. At this moment these documents describe member state consensus for the implementation of the Safety Fundamentals in fourteen topic areas. Safety Guides provide recommendations and guidance on how to comply with the Safety Requirements. Safety Guides present international good practices to help users striving to achieve high levels of safety. The guides represent member state consensus that it is necessary to take the measures recommended, or equivalent alternative measures. Currently nearly 120 safety guides are in effect.

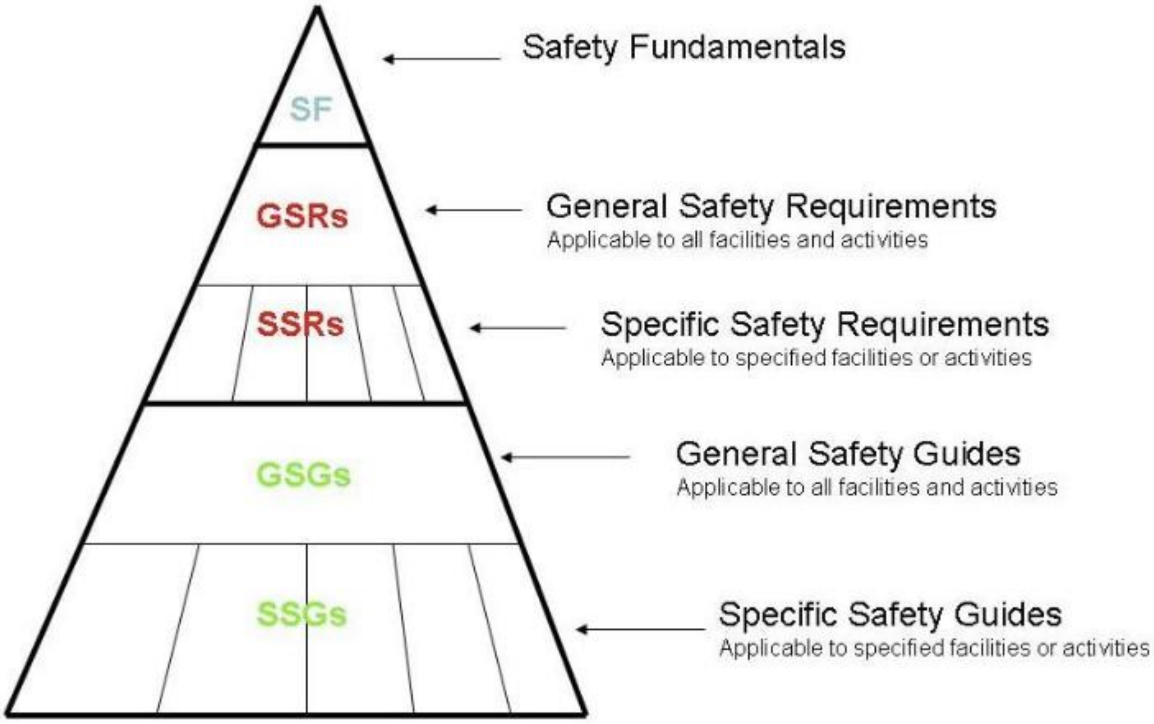

SF
Safety Fundamentals
GSRs
General Safety Requirements
Applicable to all facilities and activities
SSRs
Specific Safety Requirements
Applicable to specified facilities or activities
GSGs
General Safety Guides
Applicable to all facilities and activities
SSGs
Specific Safety Guides
Applicable to specified facilities or activities

Figure 1. The hierarchy of IAEA Safety Standards[2]

In 2009 the IAEA undertook work to update and replace two existing safety guides that dealt with Instrumentation and Control for Nuclear Power Plants. These guides were:

NS-G-1.3 [2] which provided recommendations regarding the implementation of IAEA requirements for Instrumentation and Control (I&C) Systems, and

NS-G-1.1 [3], which provided detailed guidance on the development of software for I&C systems important to safety.

In 2009 NS-G-1.1 was nine years old and NS-G-1.3 seven. Since the publication of these two standards there had been many developments in the I&C domain. These developments involved both technical advances and advances in the criteria provided by non-governmental standards development organizations.

IAEA published a new I&C standard, SSG-39 [4], in 2016 to replace NS-G-1.3 and NS-G-1.1.

[2] From: Long Term Structure of The IAEA Safety Standards and Current Status (2016).
Electronic version available at: https://www-ns.iaea.org/committees/files/CSS/205/status.pdf

Merger of the Two Safety Guides

In updating these, I&C safety guides one important question was should NS-G-1.1 and NS-G-1.3 each be updated or should the two standards be merged into one standard. Ultimately a number of considerations led to the decision to merge the documents. Some of the main reasons for the merger were:

Safety is a systems issue and it was felt that the segregation of guidance for I&C systems into two documents, one dealing with hardware and systems, and the other dealing with software, complicated discussion of the interactions of these topics.

Since the development of NS-G-1.1 many of the topics it covered had been addressed by standards prepared by international standards development organizations (SDO's), i.e., the International Electrotechnical Commission (IEC) and the Institute for Electrical and Electronic Engineers (IEEE). It was felt better not to duplicate the work of these bodies.

The SDOs were also rapidly expanding digital systems guidance to address new topics such as the use of field programmable gate arrays, the acceptance of industrial digital devices, and data communications. It would have been difficult for IAEA to revise a document such as NS-G-1.1 at a pace that could match the growing list of topics to be addressed.

Consequently it was decided that the IAEA guidance in the software area should focus on the elemental and basically static guidance for real-time software for nuclear power plants important to safety. Nevertheless, many points were carried over from NS-G-1.1. A concerted effort was made to extract fundamental recommendations into a specific software section in SSG-39. Also, much of the lifecycle guidance in NS-G-1.1 was recast as guidance for both software and hardware development in SSG-39.

Relationship to Non-Governmental Standards

Non-governmental standards such as those produced by IEC and IEEE respond to one of two basic sets of requirements those of the U.S. Nuclear Regulatory Commission, and those given in the IAEA Safety Requirements. Most countries have taken one of these sets of requirements as the starting point for developing their own regulations.

IAEA safety standards should not unnecessarily conflict with national requirements (otherwise the member states would not endorse them). By extension the IAEA standards should not unnecessarily conflict with the existing standards that support the two main sets of requirements as this could force unnecessary changes to existing standards. To avoid such conflicts it was necessary to conduct a deep technical review that involved representation from a broad range of experts from the international community. Section 6 discusses this review.

Overview of the Safety Guide

As with NS-G-1.3 and NS-G-1.1, SSG-39 gives guidance meant to ensure the suitability and reliability of nuclear power plant I&C systems. The document mainly provides recommendations for systems important to safety. A fundamental assumption behind the safety guide is that commercial industry is already highly proficient at developing I&C systems, but they may not be fully aware of specific methods that are employed to ensure that I&C systems provide the levels of safety and reliability required by the nuclear industry.

One view of the safety guide is that it describes a consensus set of design practices intended to ensure the reliability of I&C systems. The guide addresses reliability, not just in terms of failure rates and fault tolerant architecture, but from the fundamental requirement that I&C systems must have characteristics that ensure that safety functions can be performed with the necessary reliability. The main subjects covered and the motivation for discussing these subjects are described below.

The management system for I&C design

Management systems focus on all phases of the I&C development lifecycle to ensure that safety requirements (including reliability) are included in the design and continue to support their function during the entire life of the I&C system. Two fundamental mechanisms may contribute to system reliability: 1) component failures and 2) errors that result in failure of system functions even when all components are working normally. Design, operational, or maintenance errors can affect system reliability even if no component failures occur.

Design basis for I&C systems

The development of high reliability systems depends upon the availability of correct and complete design requirements that identify the overall I&C systems and each individual I&C system's necessary capability, functionality, and reliability. This section provides a guide to identifying such features.

I&C architecture

This section provides criteria that should be considered when developing I&C architectures. I&C architecture identifies the I&C functions that will be provided to support normal operations and the response to accidents. At the overall plant level the I&C architecture defines the systems that will be provided to support normal operations, control of abnormal operations, and response to accidents. At this level the architecture defines features needed to maintain independence between the I&C systems that support normal operations and the systems that:

Are intended to respond to abnormal plant operation including conditions:

Are intended to initiate mechanical systems that prevent fuel damage in the event serious failures in plant equipment

Are meant to control the consequence of common cause failures in the systems that respond to serious failures in plant equipment.

In all cases the failures considered include component failure, design errors, operational errors, and maintenance errors.

At the individual system level architecture describes the features to be provided to limit propagation of individual failures within the individual systems.

Safety classification

Economic and staffing limitations necessitate that the highest level of resources be provided for the development of I&C systems having the greatest safety importance. This section discusses the grouping of I&C safety functions and associated systems according to their importance to safety and the assignment of design requirements for each class.

Recommendations for I&C system design

This section describes methods that may be used to achieve the functional and reliability requirements established by the I&C design basis, architectural requirements, and safety classification. There are two sections dealing with this topic: one deals with generic recommendations that apply to all systems and the other deals with recommendations for specific types of systems. These two sections give guidance for reliability design to cope with single failures as well as other features to ensure reliability is not jeopardized by conditions that may occur during the systems' lifetime. For example, as a result of exposure to harsh environments, unauthorized operation, measurement drift, and ageing.

Considerations relating to the human-machine interface

This section deals with characteristics that the human-machine interface should have to help operators make reliable operational decisions and to avoid making operational errors.

Software

Software does not fail, but software systems may be more prone to design errors than hardware. This section elaborates on the management system recommendations to present techniques and features intended to improve software reliability.

Correlation with other international instrumentation and control standards for nuclear power plants

Safety guides give only high level recommendations that are meant to ensure the functionality and reliability of I&C systems in nuclear power plants. Standards development organizations such as IEC and IEEE provide much more detailed recommendations that support the ideas in SSG-39. For that reason the guide has an annex that identifies the IEC and IEEE standards that have a strong relationship to each section of the safety guide. Some IEC and IEEE standards deal with even more detailed ideas that do not correlate directly to the safety guide. It is believed that the standards listed in the annex are sufficient to lead users to the more detailed recommendations.

Main Technical Differences From the Previous Safety Guides

In the 1990's the nuclear power plant I&C community adopted the concept of formal development lifecycles as a fundamental approach to ensure and demonstrate the quality of software development. The principles for the development of software lifecycles were described in documents such as IAEA NS-G-1.1, reports developed by various regulatory organizations, and international standards such as IEC 60880 [5] and IEEE 7-4.3.2 [6]. Since that time both the nuclear industry and other process industries have recognized that formal development lifecycles should play the same role for hardware systems as well, as evidenced by the development of IEC 61508 [7] for commercial products, and IEC 61513 [8] for nuclear power plant systems. To reflect these developments SSG-39 includes a full section describing the fundamental characteristics expected in the development of hardware systems and components, and both the hardware and software development for digital systems.

SSG-39 takes into account the continuing development of computer applications and the evolution of the methods necessary for their safe, secure and practical use. The document identifies two very important interfaces with I&C design: Human Factors Engineering and Cyber Security. When designing the I&C systems, it is necessary to coordinate with these two engineering domains and to integrate human factors engineering inputs and computer security inputs into I&C life cycles.

SSG-39 references the IAEA computer security guide, NSS-17 [9] and provides criteria for avoiding negative safety effects from computer security features. The intent of SSG-39 is to identify major interfaces with the computer security activities, and to give recommendations on I&C design features that affect these activities, e.g. interaction with cybersecurity programs in the overall I&C process planning, graded approach to security in the I&C system design, impact assessment for mal-operation of critical digital assets, incident response and periodic vulnerability assessment in individual system lifecycle phases. More detailed information on computer security is provided in NSS-17.

SSG-39 accounts for developments in human factors engineering and provides considerations on the interactions of I&C design with human factor engineering programs. The document contains specific clauses that identify major interfaces with the human factors activities, and gives recommendations on I&C design features that affect these topics, e.g. the human-machine interface in the design of the main and supplementary control rooms. Guidance is also given for user displays and controls.

Although SSG-39 covers certain aspects of human factors as they relate to I&C, it does not provide comprehensive guidance on this domain. The development of human factors engineering requirements and the verification and validation of human factors engineering activities are normally performed as part of a human factors engineering program. Currently, IAEA is developing a new dedicated Safety Guide on Human Factors Engineering (the working draft is numbered as DS492) that provides a set of specific recommendations on how to deal with human factor engineering in the design and operation of nuclear power plants. This standard will address:

Considerations specific to human factors engineering, including the human machine interface(s) for achieving compliance with the requirements established in SSR 2/1, Rev.1 [10];

Competences needed for integrating human factors engineering into the design of nuclear facilities throughout the plant lifecycle for achieving compliance with the requirements established in GSR-Part 2 [11] (Leadership and management for safety; published in 2016 as a revision of GS-R-3);

The human factors engineering process to be considered in achieving human machine interface design across plant states.

Digital systems consist of both software and hardware. A certain amount of guidance on digital system hardware and hardware systems that needed to be recognized at a high level. Criteria that existed in NS-G-1.1 and other criteria developed after the publication of that standard were included in SSG-39 to cover topics that mainly involved system performance requirements, communications systems, and cyber security considerations.

When NS-G-1.1 was written most digital systems were being developed using general purpose microprocessors or programmable logic controllers. Since that time the industry has witnessed the use of other kinds of digital platforms such as systems programed using hardware description languages (e.g., field programmable gate arrays) and industrial digital devices having limited functionality, The selection and use of such devices raise issues that are different from the older technologies. Thus a discussion of high level principles for such systems were given.

SSG-39 is closely related to IAEA Safety Guide SSG-34 [12], Design of Electrical Power Systems for Nuclear Power Plants, which provides recommendations for power supply, cable systems, protection against electromagnetic interference, equipment and signal grounds, and other topics that are necessary for the satisfactory operation of I&C systems. With regard to I&C systems, SSG-34 gives recommendations on power supplies to ensure that requirements on their safety class, reliability provisions, qualification, isolation, testability, maintainability and indication of removal from service that are consistent with the reliability requirements of the I&C systems they serve. Wherever possible SSG-34 and SSG-39 give identical criteria for such topics.

Special recommendations are given to address electromagnetic interference, because power supplies can provide a transmission path for electromagnetic interference that might originate outside the I&C systems or might arise from other I&C systems that are connected directly or indirectly to the same power supply. Particular consideration is also given to ensuring the long term availability of the electrical systems that are necessary for the operation and monitoring of safety systems.

Coordination With Other Organizations

The development of SSG-39 was coordinated with three other international organizations concerned with standards for nuclear power plant I&C: The OECD/NEA Multi-national Design Evaluation Program (MDEP) Digital I&C Working Group (DI&CWG), the IEC Subcommittee for Instrumentation, Control, and Electrical Systems of Nuclear Facilities (IEC SC45A), and the IEEE Nuclear Power Engineering Committee (NPEC).

MDEP is a multinational initiative taken by national safety authorities to develop innovative approaches to leverage the resources and knowledge of the national regulatory authorities who will be tasked with the review of new reactor power plant designs. Within MDEP the DI&CWG works to document common positions in the DI&C safety systems design areas and harmonize and converge national codes, standards and regulatory requirements and practices in the area of digital I&C.

During the development of SSG-39 the DI&CWG was working actively in the areas of the treatment of common cause failure, qualification of software tools, verification and validation, communications independence, selection and configuration of hardware description language programmed devices, simplicity in design, selection and use of industrial digital devices, interaction between safety and cyber security, and safety criteria for I&C architecture. IAEA staff actively participated in the DI&CWG work and strove to achieve consistency between SSG-39 recommendations and the common positions of the DI&CWG regulators. The continued cross discussion between IAEA and MDEP resulted in the development of consistent approaches between the documents published by the two organizations.

The experts participating in the development of SSG-39 included members of the SC45A and NPEC standards development committees who had deep and broad understanding of each group's standards. Their participation was vital to avoiding unnecessary conflicts between SSG-39 and the two non-governmental standards organizations. The participants also took back to their organizations new ideas that may be incorporated into the SDO documents in the future. Furthermore, IAEA staff continually participated in SC45A and NPEC meetings to keep them informed of the status of the SSG-39 draft and the key technical issues under discussion.

Development and REview process

The core team that drafted the standard was made up of about 15 experts from Canada, Czech Republic, France, Korea, Russia, the United Kingdom, and the United States. The number 15 includes several people who could not participate in all meetings so the typical drafting meeting involved less than 10 participants.

Several drafting meetings were needed for the group to develop a draft that was considered to be sufficiently mature for industry wide review. This draft was sent directly to more than 100 known experts in twenty-two countries. The experts were offered the opportunity to make comments and were asked to share the draft with other experts who may also wish to comment. In addition IEC SC45A and IEEE NPEC were specifically asked to review the draft to identify any conflicts with their standards. In addition to these personal contacts the draft was distributed and comments were solicited from all IAEA member states via the announcement of a technical meeting to review the draft.

More than eleven hundred comments were received from thirty individuals or organizations representing about twenty nations or international institutions. The IAEA staff grouped the comments and developed proposed dispositions. These proposed dispositions and residual comments were discussed at a technical meeting hosted by Electricity de France in Lyon during the week of 12 December 2011. Thirty experts from seventeen nations or international organizations attended. A large number of the comment dispositions were rapidly accepted but several hundred still needed to be discussed. Thanks to the hard work and determination of the experts and the excellent meeting arrangements the review was completed with only a small number of comments identified as needing further discussion. Of course, being in Lyon, the meeting was also a gastronomic success.

Establishment of the new IAEA safety standard required a comprehensive step-by-step preparation and review process which contains 14 steps and involves different review committees. In case of SSG-39, the main review committees were the Nuclear Safety Standard Committee (NUSSC), the Nuclear Security Guidance Group (NSGC) and Commission of Safety Standard (CSS). Each draft safety guide is reviewed internally before its submission to the review committee.
The first review of Draft G by the 34th NUSSC meeting during 19-21 November 2012 was unsuccessful; the draft was rejected due to prevailing disagreement among NUSSC representatives on the three topics such as reliability determination for digital systems, assessment of common cause vulnerabilities in safety systems, and criteria for implementation of diverse actuation systems. A compromise solution was found during an extraordinary consultancy meeting that was held in February 2013. It was decided to move these three topics into an informative Annex.

The review of a revised draft by the 35th NUSSC meeting was successful and the safety guide was sent to member states for their comments. After 8 months, which is a period given to member states to review draft safety guide, the IAEA received 386 comments from which 159 comments were accepted. The comment resolution was not easy, because several “critical” comments related to the effects of automatic control system failures ignited a new discussion among three influential NUSSC members. After several iteration cycles a common position was found and a new draft was provided to the 37th NUSSC meeting in June 2014, which eventually endorsed this draft for the final step – CSS endorsement.

As mentioned in section 4, the safety guide references the IAEA computer security guide, NSS-17 and provides criteria for avoiding negative safety effects from computer security features. With this regard the draft safety guide was also reviewed in a NSGC meeting in June 2014. Although it looked initially as an easy review, it turned to be a difficult step to obtain an approval by NSGC. The main reason for a long and heavy discussion in the group was that the NSGC group did not like quite many clauses on security interface arguing that sufficient security guidance is provided in the IAEA security series publications. It was explained that provisions for ensuring the security of digital safety systems need to be included in different stages of I&C design and the NSGC eventually endorsed this draft.

SSG-39 was established as the new safety guide by the 36th CSS meeting in November 2014; however at that time several IAEA requirements documents were under revision to address the lessons learned from the accidents at Fukushima Daiichi. It was decided not to release SSG-39 until after these requirements documents were approved. In the end this delayed publication by one and a half years and resulted in: bringing the terminology “Technical Support Centre” in line with that agreed for revision of SSR 2/1, and revised sections on accident monitoring and communications facilities which addressed the fundamental points concerning accident monitoring from IAEA publication NP-T-3.16 [13] on Accident Monitoring Systems for Nuclear Power Plants. After these changes were made, the document was finally published in May 2016

Conclusion

SSG-39 provides recommendations on the design of I&C systems to meet the requirements established in IAEA Safety Design Requirements SSR-2/1 (Rev. 1). It provides guidance on the overall I&C architecture and on the I&C systems important to safety to ensure safe operation of the plant in all plant states. SSG-39 integrates two very important interfaces with I&C design such as Human factors engineering and Cyber Security. Special attention was given to reduce duplication of guidance that is already in industry standards of IEC and IEEE to avoid confusion and result in unnecessary conflicts.

The preparation of SSG-39 took 8 years and involved considerable engineering and editorial work to produce drafts, reviews by member states and review committees, resolutions of numerous comments and final editorial work to publish it as a safety standard series publication in May 2016. The SSG-39 is a consensus document; some topics related to design of digital systems in safety applications, although important, were moved into and informative Annex, because consensus on those topics among several members states could not have been accomplished. Nevertheless, the SSG-39 provides a solid engineering basis to be considered when designing or reviewing various aspects of I&C systems.

References

[1] IAEA Statute, https://www.iaea.org/about/about-statute (1989)

[2] IAEA, Safety Guide No. NS-G-1.3, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, IAEA (2002)

[3] IAEA, Safety Guide No. NS-G-1.1, Software for Computer Based Systems Important to Safety in Nuclear Power Plants, IAEA (2000)

[4] IAEA, Specific Safety Guide No. SSG-39, Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA (2016)

[5] IEC 60880, Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions, IEC (2006)

[6] IEEE 7-4.3.2, IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations, IEEE (2016)

[7] IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems, IEC (2010)

[8] IEC 61513, Nuclear power plants – Instrumentation and control systems important to safety – General requirements for systems, IEC (2011)

[9] IAEA Nuclear Security Series No. 17, Computer Security at Nuclear Facilities, IAEA (2011)

[10] IAEA, Specific Safety Requirements No. SSR-2/1 (Rev. 1), Safety of Nuclear Power Plants: Design, IAEA (2016)

[11] IAEA, General Safety Requirements No. GSR Part 2, Leadership and Management for Safety, IAEA (2016)

[12] IAEA, Specific Safety Guide No. SSG-34, Design of Electrical Power Systems for Nuclear Power Plants, IAEA (2016)

[13] IAEA Nuclear Energy Series No. NP-T-3.16, Accident Monitoring Systems for Nuclear Power Plants, IAEA (2015)

Heuristic Principles of Phase Merging in Reliability Analysis

Volodymyr S. Koroliuk, Dmitri Koroliouk
•
Institute of Mathematics,
Institute of Telecommunications & Global Information Space
National Academy of Sciences of Ukraine
mailto:vskorol@yahoo.comvskorol@yahoo.com, dimitri.koroliouk@ukr.net

Abstract

B.V. Gnedenko was the founder of reliability analysis for stochastic systems. His works [1]-[2] have inspirited, in reliability theory, the development of analytical methods of phase state merging principles for Markov and semi-Markov processes.

Keywords: duplicated system, phase merging principles, potential matrix.

1 Introduction

The fundamental works of Boris V. Gnedenko in the reliability analysis for stochastic systems [1]-[3] laid the foundation in many areas of specific research.

In particular, there where developed the methods of phase space merging in reliability theory for Markov and semi-Markov processes with the corresponding heuristic approach [4, 5]. A surprising property of such heuristic principles is that any results obtained with their use can be justified rigorously by mean of the phase merging algorithms [6]. The stationary phase merging techniques represent a particular cluster analysis, based on asymptotic properties of semi-Markov systems and is useful for simplification of reliability analysis, as shown for a duplicated renewal system.

2 The duplicated renewal system

B.V. Gnedenko in [1, 2] has studied the reliability problem for the stochastic systems with two identical working devices and one repairing facility.

The description of such a duplicated renewal system is determined by the working times α_k, $k = 1,2$ of devices with an arbitrary distribution function $F_k(t) = P(\alpha_k \leq t)$, and by the repairing times β_k, $k = 1,2$ with the distribution function $G_k(t) = P(\beta_k \leq t)$.

The working times of the system up to the first failure $\tau_k, k = 1,2$ are dependent on the type of the initial working components.

The Laplace transform functions of the working times of the system, that are

$$\varphi_k(s) := Ee^{-s\tau_k} = \int_0^\infty e^{-st} d\Phi_k(t) \ , \ = 1,2$$

may be obtained by using the stochastic relations (see [1, 2] and also [5])

$$\begin{aligned} \tau_1 &\doteq \alpha_1 + I(\alpha_1 \geq \beta_2)\tau_2, \\ \tau_2 &\doteq \alpha_2 + I(\alpha_2 \geq \beta_1)\tau_1. \end{aligned} \tag{1}$$

The equality $\doteq$ means that the left and the right parts are identically distributed.

The stochastic relations (1) mean that during the working times α_k, $k = 1,2$, the failure of the system can occur under the condition $\alpha_k < \beta_{k'}$, $k = 1,2$, $k' = 2,1$ with probabilities

$$q_k = \int_0^\infty \overline{G}_{k'}(\mathrm{t}) dF_k(t) \ , \quad k = 1,2 \ , \quad k' = 2,1.$$

So, the relations (1) imply the following system of algebraic equations:

$$Q(s)\varphi(s) = \psi(s), \tag{2}$$

where $\varphi(s) = (\varphi_1(s), \varphi_2(s))$, $\psi(s) = (\psi_1(s), \psi_2(s))$,

$$\psi_1(s) := \int_0^\infty e^{-st}\overline{G}_1(t)dF_2(t) \ , \quad \psi_2(s) := \int_0^\infty e^{-st}\overline{G}_2(t)dF_1(t). \tag{3}$$

The matrix Q is defined as follows:

$$Q(s) := \begin{bmatrix} 1 & -g_1(s) \\ -g_2(s) & 1 \end{bmatrix}, \tag{4}$$

where

$$g_1(s) := \int_0^\infty e^{-st}G_2(t)dF_1(t), g_2(s) := \int_0^\infty e^{-st}G_1(t)dF_2(t). \tag{5}$$

3 The duplicated renewal system in the series scheme

In order to simplify the duplicated renewal system, described by the linear algebraic equations (2)-(5), let's introduce the series scheme with a small series parameter $\varepsilon \to 0$ ($\varepsilon > 0$), under the following asymptotical conditions

$$C1: 1cm\psi_k^\varepsilon(s) = \varepsilon \int_0^\infty e^{-\varepsilon st}\overline{G}_{k'}(t)dF_k(t) = \varepsilon q_k + o(\varepsilon) \ , \quad q_k := P\{\beta_{k'} > \alpha_k\} \ , \quad k = 1,2 \ ; \quad k' = 2,1.$$
$$C2: 1cm1 - f_k^\varepsilon(s) = \varepsilon s \int_0^\infty e^{-\varepsilon st}\overline{F}_k(t)dt = \varepsilon s a_k + o(\varepsilon) \ , \quad a_k := E\alpha_k \ , \quad k = 1,2.$$

The asymptotical conditions C1 – C2 mean that the probabilities of falure $q_k^\varepsilon := P\{\beta_{k'}^\varepsilon > \alpha_k^\varepsilon\}$ tend to zero together with the mean values $a_k^\varepsilon = E\alpha_k^\varepsilon$ such that the ratio $q_k^\varepsilon \lambda_k^\varepsilon = \mathrm{q}_k^\varepsilon / a_k^\varepsilon$ tend to finite values $\Lambda_k = q_k \lambda_k$, $k = 1,2$.

Then the matrix of system (2) in the series scheme has the following asymptotic representation:

$$Q^\varepsilon(s) = Q_0 + \varepsilon Q_1(s) + o(\varepsilon), \tag{6}$$

where

$$Q_0 = \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \ , \quad Q_1 = \begin{bmatrix} 0 & q_1 + sa_1 \\ q_2 + sa_2 & 0 \end{bmatrix}. \tag{7}$$

The singularity of the matrix Q_0 ($\det Q_0 = 0$) means that the phase merging algorithm [5] may be applied to solve the singularly perturbed (truncated!) equation

$$[Q_0 + \varepsilon Q_1(s)]\varphi^\varepsilon(s) = \psi^\varepsilon(s). \tag{8}$$

According to the phase merging principles (see [4, 5, 6]), the average (limit) result takes place in the following form:

$$\varphi_1^0(s) = \varphi_2^0(s) = q/(q+sa) \ , \quad q = (q_1+q_2)/2 \ , \quad a = (a_1+a_2)/2. \tag{9}$$

The times-to-failure limits of the duplicated renewal systems, under the asymptotical assumptions C1-C2, have identical exponential distribution

$$\lim_{\varepsilon\to 0} P\{\tau_k^\varepsilon > t\} = e^{-\Lambda t} \ , \quad \Lambda = q/a. \tag{10}$$

Remark 1. Let us introduce the mean intensity of the working time $\lambda := 1/a$. Then the intensity of the failure time is $\Lambda = q\lambda$. So the formula (10) represents the failure time of the duplicated system with the failure probability q and with intensity λ.

4 Heuristic principles of the phase merging

The phase merging algorithms described in [5, 6] may be formulated as some *heuristic phase merging principles* in the reliability analysis of redundant renewal stochastic systems with N elements (see [5], Ch.3).

1) The lack of memory. The common working time of a system till the instant of failure τ is determined by exponential distribution:

$$P(\tau > t) = e^{-\Lambda t} t \geq 0. \tag{11}$$

2) The superposition of failures. The intensity of the system failure is determined by the sum of intensities of system failures in every renewal state:

$$\Lambda = \sum_{k=1}^N \Lambda_k \ , \quad \tau = \min_{1\leq n\leq N} \tau_n. \tag{12}$$

According to the Principle 2), the failure of the system can occur in every renewal state as was explained in Section 3 for duplicated systems.

3) The independence of the elements failures. The system failures for every element are determined by the failure rule as follows:

$$1/E\tau_k = \Lambda_k = q_k\lambda_k, \tag{13}$$

where q_k is the probability of failure for k-th state and λ_k is the stationary intensity of working time for k-th state.

The heuristic principles action can be illustrated by analysis of *the duplicated renewal system.* Namely, two working devices are described by independent working-repearing processes with given distribution functions of the working times α_k and the repairing times β_k

$$F_k(t) = P(\alpha_k \leq t) \ , \quad G_k(t) = P(\beta_k \leq t) \ , = 1,2. \tag{14}$$

Such a classical example of the system is usually called "two lifts system" [9, 10].

The heuristic principles of the phase merging technique are based on use of the limit renewal theorem [7] for the stationary residual time α^* expressed as:

$$P(\alpha^* \leq t) = \lambda \int_0^t \overline{F}(s)ds \ , \quad \lambda = 1/E\alpha.$$

According to heuristic principles, the described above the failure intensity of two lift system is the following:

$$\Lambda = q_1\lambda_1 + q_2\lambda_2 \ , \quad \lambda_k = 1/E\alpha_k \ , \quad k = 1,2. \tag{15}$$

The failure probabilities $q_k, k = 1,2$ are determined as follows:

$$q_1 = P(\alpha_2^* > \beta_1) \, , \quad q_2 = P(\alpha_1^* > \beta_2). \tag{16}$$

Here the stationary remaining working times α_k^*, $k = 1,2$, have the following distribution functions:

$$P(\alpha_k^* \le t) = \lambda_k \int_0^t \overline{F}_k(s)ds \ , \quad k = 1,2. \tag{17}$$

Under the natural *assumption of the repairing relative brevity*:

$$E\beta_k \ll E\alpha_k \ , \quad k = 1,2, \tag{18}$$

the intensity of the system failure for the duplicated renewal system may be estimated as follows:

$$\Lambda \simeq [E[\alpha_2 \wedge \beta_1] + E[\alpha_1 \wedge \beta_2]]/E\alpha_1 E\alpha_2. \tag{19}$$

The phase merging algorithms in [5] are the basis to verify the heuristic phase merging principles.

5 The duplicated renewal system without failure

The duplicated renewal system without failure ($\beta_k = 0, k = 1,2$) is described by a superposition of two renewal processes given by sums

$$S_n^\pm = \sum_{r=1}^n \alpha_r^\pm, \tag{20}$$

of jointly independent and identically distributed (by $r \ge 1$) random variables $\alpha_r^\pm$, $r \ge 1$. For simplicity, we denote the working times α_1 and α_2 as α^+ and α^-, correspondingly.

The duplicated renewal system without failure and with working times α_k^+, α_k^-, $k \ge 0$, means that the working device substitution is accompanied by its instantaneous repairing.

The phase merging principles provide the base model of the duplicated renewal system without failure as a Markov chain $\hat{x}_n, n \ge 0$ on the phase space $E = \{+,-\}$, is given by the sojourn times

$$\hat{\theta}_n^\pm = \alpha_n^\pm \wedge \alpha_n^{\mp *} \ , \quad n \ge 1. \tag{21}$$

The transition probabilities of the Markov chain $\hat{x}_n, n \ge 0$ with the sojourn times (21) are calculated as follows:

$$q_\pm = P\{\hat{x}_{n+1} = \mp | \hat{x}_n = \pm\} = P(\alpha_n^\pm > \alpha_n^{\mp *}),$$

that is

$$q_\pm = q\lambda_\mp \ , \quad q = \int_0^\infty \overline{F}_+(t)\overline{F}_-(t)dt \ , \quad \lambda_\pm = 1/E\alpha^\pm. \tag{22}$$

Its generating matrix has the following form:

$$Q = P - I = \begin{bmatrix} -q_+ & q_+ \\ q_- & -q_- \end{bmatrix}. \tag{23}$$

The stationary distribution of the Markov chain with the generating matrix (23) is given by

$$\Pi = \begin{bmatrix} \rho_+ & \rho_- \\ \rho_+ & \rho_- \end{bmatrix} \;, \quad \rho_\pm = \lambda_\pm/\lambda \;, \; \lambda = \lambda_+ + \lambda_-. \tag{24}$$

Introduce the orthogonal matrix

$$\overline{\Pi} := \Pi - I = \begin{bmatrix} -\rho_- & \rho_- \\ \rho_+ & -\rho_+ \end{bmatrix}. \tag{25}$$

It is easy to note that the generating matrix (23) has the following representation:

$$Q = \lambda q \overline{\Pi}. \tag{26}$$

Now let us define the potential matrix R_0 as a solution of the following equation:

$$QR_0 = R_0 Q = \overline{\Pi} \;, \quad R_0 \Pi = \emptyset. \tag{27}$$

It is easy to verify that

$$R_0 = -(\lambda q)^{-1} \overline{\Pi}. \tag{28}$$

Now, using the Markov chain, given by the generating matrix (26) and the potential matrix (28), we can analyze the asymptotic properties of the reward functional, defined on the duplicated renewal system with failure.

The limit working time of the system with failure gives us the following approximation estimate:

$$\begin{aligned} &E\zeta_\pm \simeq [\lambda_+ c_+ + \lambda_- c_-]/q, \\ &c_\pm := E\gamma^\pm. \end{aligned} \tag{29}$$

The real valued random variables $\gamma_n^\pm := \gamma_n(\pm)$ is given by the distribution functions

$$\Gamma_\pm(u) = P(\gamma^\pm \leq u) \;, \; \in R. \tag{30}$$

The heuristic principles of the phase merging formulated in Section IV, are based on limit theorems for semi-Markov processes with absorbing state.

References

[1] Gnedenko B. V. (1964). On spare duplication. *Engrg. Cybernet.*, 4:3–12.

[2] Gnedenko B.V. (1964). On duplication with renewal. *Engrg. Cybernet.*, 5:111–118.

[3] Gnedenko B.V., Belyaev Yu.K., Solovyev A.D. Mathematical Methods of Reliability Theory, New York, Academic Press, 1969.

[4] Korolyuk V.S., Turbin A.F. Markov renewal processes in problems of reliability of systems, Kyiv, Naukova Dumka, 1982 (in Russian).

[5] Korolyuk V.S., Korolyuk V.V. Stochastic models of systems, Kluwer, 1999.

[6] Korolyuk V.S., Limnios N. Stochastic systems in merging phase space, WSP, 2005.

[7] Feller W. An Introduction to Probability Teory and its Applications, Vol.1-2, Wiley, 1966.

[8] Gnedenko B., Ushakov I. Probabilistic Reliability Engineering, Section 6.2, New York, Wiley, 1995.

[9] Szász D. (1977). A problem of two lifts. *Ann. Probab.*, 5,4:550-559. *Engrg. Cybernet.*, 5:111–118.

[10] Zubkov, A.M. (1975). On the rate of convergence of a renewal density. *Math. USSR-Sb.*, 27-1:131-142.

System Reliability for Shock and Lottery Models

Ilya Gertsbakh
Yoseph Shpungin

Abstract

In this note we consider how system signatures (D-spectra) can be used in computing system reliability for "shock" and "lottery" models of system reliability.

Key words: shock model, lottery model, signatures, D-spectra.

Suppose you have a coherent binary system with n binary components subject to failure. To make this note more visual, imagine that the system is a network and the components subject to failure are the edges. So, any edge can be in two states, *up* and *down*, i.e. operational or not, respectively. The network can be in two states UP and $DOWN$. For example, the network is UP if two nodes of the network, S and T, are connected, and $DOWN$, otherwise. Let the components be numbered as $1,2,\ldots,n$. Let us consider two situations which seem quite different. The first we will call "The shock model".

1. The shock model

Suppose there is an external source of "shocks" which act on our system in the following way. A shock chooses randomly one component of our system and hits (erases) it as a result of which this component goes from *up* to *down*. The next shock chooses randomly one of the remaining (non hit, *up*) components and hits it. This process continues until the system goes $DOWN$. This model has been considered in literature many times, see for example [1] and references there.

Suppose we check system state after each shock. Initially, before the shock process starts, the system is UP. Sooner or later the shocks will cause the system to go $DOWN$. Let us register the ordinal number of the shock which turns the system from UP to $DOWN$.

If it happens on the first hit, this number is one, if on the second - this number will be 2, and so on. By the definition of the shock process, all random sequences of component numbers hit by shocks are equally probable, and each particular sequence has probability $1/n!$ So, we can speak about random events $\{A_k\}$ and their probability $\{f_k\}$

$$A_k = (\ system\ went\ DOWN\ on\ the\ k-th\ shock\ ), f_k = P(A_k).$$

Obviously the collection of numbers $f = (f_1, f_2, \ldots, f_n)$ is a discrete density and $\sum_1^n f_k = 1$. F. Samaniego [4,5] called the collection f *signature* . M.Lomonosov [5] suggested the name -"ID" (*internal distribution*).

Let us look now into $F(x) = f_1 + f_2 + \ldots + \mathrm{f}_x = \sum_{k=1}^{x} f_k$ which is called *cumulative signature* or *D-spectrum* [6].

The probabilistic meaning of $F(x)$ is the following. Suppose we know that the system is $DOWN$. Given this fact, the probability that the system has suffered k shocks equals $F(k)$. If the shocks process starts at $t = 0$ and shocks come with interval 1 hour, then $F(k)$ will be the CDF of system lifetime in hours. Or in other words: in the shock model scheme, $F(k)$ is the probability that the system failed on the first or the second,..., or the k-th shock.

In the shock model, finding $F(k)$ is the central issue of the resilience study of the system, see [6] where we describe Monte Carlo algorithms for obtaining an unbiased estimates for $F(x)$. These algorithms are based on simulating the process of sequential destruction of system components to locate the position of the $UP -> DOWN$ transition -from this process comes the prefix "D"-destruction.

Our personal impression that reliability engineers don't like too much the signature issue. For them the shock process looks as something artificial and not relevant to the main problem which is finding system reliability. Let us describe this problem.

2. The lottery model

Suppose the system consists of independent components and each component is up with probability p and $down$ with probability $q = 1 - p$. We can think also that these probabilities are related to a particular instant t, i.e. the component is up at t with probability $p = p(t)$. If the components have i.i.d. lifetimes, then $p(t)$ is the probability that component lifetime $\tau \geq t$.The central problem is finding system reliability, i.e. $P(\ \ system\ \ is\ \ UP)$, or $P(DOWN) = 1 - P(UP)$.

We will call this situation "the lottery" model. Assume that for each system component we carry out an independent lottery. In this lottery, the component is declared to be in state up with probability p and $down$with probability $q = 1 - p$. After the lottery ends, the system will be either in UP or in $DOWN$, and we are interested in finding $P(UP)$.

This is a solid reliability problem and its solution is an important practical issue. From the first sight, this problem has nothing in common with the above artificial shock model. How the reliability engineer would solve his problem? Most probably, by using the following formula

$$P(DOWN) = \sum_{k=1}^{n} C(k) q^k (1-p)^{(n-k)}, \tag{1}$$

where $C(k)$ is the number of *failure sets* having exactly k components $down$ and the remaining $(n - k)$ components up. The real issue is finding the $C(k)$'s.

But it turns out that the solution of the shock model provides easily the solution of the lottery model and vice versa. It turns out that there is a simple formula connecting $F(k)$ and $C(k)$:

$$C(k) = F(k) \frac{n!}{k!(n-k)!} \tag{2}$$

The proof of (2) can be carried out by purely combinatorial arguments or analytically. We will present both proofs in the

Appendix Important is the following fact: $F(k)$ and $C(k)$ do not depend on p or q. They are what we call a *combinatorial invariant*, depending only on system structure and not depending on probabilistic properties of its components.

Let us consider an

Example

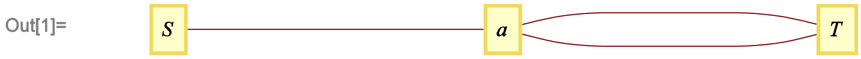


Figure 1: (S-a) -edge 1, (a-T)-edge 2, (a-T)-edge 3. UP is S-T connection

The figure shows a network with three edges, which is UP if S is connected to T. In shock model, the first shock "kills" the system if it hits component 1. So, $f_1 = 1/3$. If the system survives the first shock, then the second shock always kills the system. So, $f_2 = 1 - f_1 = 2/3$. Then $f_3 = 0$. So, $F(1) = 1/3$, $F(2) = 1, F(3) = 1$. By (1), $C(1) = (1/3) \cdot 3!/2! = 1$. Indeed, there is only one failure set with one component down: $\{1\}$. $C(2) = 1 \cdot 3!/2! = 3$. The failure sets with two components down are: $\{1,2\}, \{1,3\}, \{2,3\}$. There is only one failure set with three components down- $\{1,2,3\}$. So, system is $DOWN$ with probability

$$P(DOWN) = qp^2 + 3p\dot{q}^2 + q^3.$$

The traditional reliability analysis would be the following. Denote the $downcomponent$ by zero and the up component by one. The list of all $2^3 = 8$ system states is the following:

$$000,001,010,011,100,101,110,111.$$

The numbers 000,001,010,100,011 correspond to the $DOWN$ state. There is exactly one state with three zeroes, one state with only one zero on the first position (shown bold), and three states with two zeroes, which are failure states with two $down$ components. This is exactly the above result obtained in the shock model.#

APPENDIX

a. Combinatorial proof of (2) ([2], page 114-115).

Consider random permutation of component numbers $\pi = i_1, i_2, \ldots, i_n$. Declare the first x of its members as system component's numbers which are *down* and all the rest -as being up.

If this permutation now determines system *DOWN* state, call it the $(x; D)$-type permutation. Denote by $N(x)$ the total number of of $(x; D)$ permutations. Obviously, the probability to have an $(x; D)$ permutation is $N(x)/n!$. On the other hand, this probability equals $f_1 + f_2 + \ldots + f_x$, which follows from the definition of the destruction process. Suppose that the permutation π has the property that the system failure was observed at the instant of k-th failure, $1 \le k \le x$. Declare for this permutation that all components whose numbers appear on the next $x - k$ positions as being $down$, and all the other components -as being up. In this way we will reconstruct all permutations of $(x; D)$-type. Note also that any permutation which in the destruction process produces $DOWN$ state **after** the x-th step is not of $(x; D)$-type. Therefore,

$$N(x) = (s_1 + s_2 + \ldots s + x) \cdot n!$$

Now note that we define system $DOWN$ state with exactly x components being $down$, the order of their appearance is not relevant. All permutations obtained by permuting x *down* components between themselves, and $(n - x)$ remaining also between themselves, determine, in fact, the **same** system failure state. Therefore,

$$C(x) = \frac{N(x)}{x!(n-x)!}\#$$

b. Analytic proof of (2)

Take the well known Samaniego formula for system lifetime probability [4,5]:

$$P(\tau_s \le t) = \sum_{k=1}^{n} f_k F_{(k:n)}(t),$$

where $F_{(k:n)}$ is the CDF of the k-th order statistics from the sample of n i.i.d random variables with CDF $F(t)$. Substitute the explicit formulas for the order statistics and change the order of summation. You will obtain the expression

$$P(\tau_s \le t) = \sum_{k=1}^{n} (f_1 + \ldots + f_k) q^k (1-q)^{(n-k)} n!/(k!\,(n-k)!),.$$

where $q = F(t)$. But the right-hand side of this expression is system $DOWN$ probability expressed via its failure sets:

$$P(DOWN) = \sum_{k=1}^{n} C(k) q^k (1-q)^{(n-k)}.\#$$

References

[1] Maxim Finkelstein, and Ilya Gertsbakh, 2016, Preventive maintenance of multistate systems subject to shocks, *Applied Stochastic models* in business and industry, November.

[2] Ilya Gertsbakh and Yoseph Shpungin, Models of Network Reliability: Analysis, Combinatorics and Monte Carlo. 2010, CRC Press.

[3] Elperin, T, Gertsbakh, I and M.Lomonosov,1991, Estimation of Network Reliability Using Graph Evolution Models. *IEEE Transactions on Reliability* R-40, 572-581.

[4] Samaniego, F. J.1985. On Closure of the IFR under formation of coherent systems, *IEEE Transactions on Reliability*, 34:69-72.

[5] Samaniego, F.J. 2007.System Signatures and Their Application in Engineering Reliability.Springer: Berlin, New York.

[6] Ilya Gertsbakh and Yoseph Shpungin, 2014, Network Reliability and Resilience, *Springer briefs in electrical and computer engineering, Springer Heidelberg, Berlin, New York.*

Evaluation of System Performance Measures of Multi State Degraded System with Minimal Repair

M. Manoharan & Vidhya G Nair

•

Department of Statistics, University of Calicut
mailto:vidhyagn17@gmail.commanumavila@gmail.com,vidhyagn17@gmail.com

Abstract

There is a recent surge of interest in multi state systems mainly due to their wide applications in engineering. Multi state degraded systems have been used in modeling of power generating-supply systems, communication systems and transportation systems etc. In this article we propose a new approach ie, a combination of stochastic process approach and Universal Generating Function(UGF) technique by decomposing system in to several subsystems. Analyzing models through this approach, several system performance measures are evaluated. A real data obtained from a power station modeled as a MSS which has two subsystems with many states of degradation, has been used for illustration to apply the approach presented here.

Keywords: Multi state Systems, Power generating System, Repairable System, System Performance Measures, Universal Generating Function(UGF).

1 Introduction

In binary reliability models the system or its components is assumed to be either in a perfectly functioning state or in a completely failed state. But in most of the real life situations this assumption may not be adequate. There are intermediate states between perfectly functioning state and completely failed state. So we make use of the Multi State system (MSS) reliability model in which the system may rather have more than two states of performance between working perfectly and total failure. The basic concept and further developments of binary system reliability theory were dealt in [2 , 3]. The basic concepts of MSS, tools for MSS reliability assessment and optimization and application problems were discussed in [8]. Multi state with degrading components and concerned with the application of reliability functions to the reliability evaluation of large systems emphasis in [4]. A comprehensive introduction to system reliability theory along with failure models, qualitative system analysis and reliability importance were discussed in [10]. The joint importance measures for multi state reliability systems have been discussed in [13] and[14]. According to [1] Repairable system is a system which after failing to perform one or more of its functions satisfactorily, can be restored to fully satisfactory performance by a method other than replacement of the entire system. The UGF was first introduced by Ushakov [11] for MSS. The mathematical basics of this technique were available in [12]. An updated version of the UGF with many application was presented in [5, 8]. The combined method using random process and UGF was suggested in [8] and further extended in [6 , 7]. In [9], a new approach was used to evaluate the dynamic reliability of MSS with redundancy.

In this article description of models with assumptions has been presented in section 2. In section 3 the combined stochastic process and UGF technique approach is applied for multi state degraded system for avoiding dimension damnation problem of the stochastic process approach. A new approach of decomposing a system in to two or more sub systems (each sub system consists of the same type of components) has been proposed. Steady state probabilities and system performance characteristics are calculated for subsystems using the random process method and at last reliability indices of the entire system in steady state situation are evaluated using UGF technique. A more realistic system has been taken to validate the applicability of this approach.A power station with two sub systems (each sub system with three generators) has been illustrated in section 4 of this article. Reliability indices of this power station are evaluated in this paper.

2 Multi state degraded system

Any subsystem j of a MSS have k_j different states with performance rates represented by the set $g^j = \{g_1^j, g_2{}^j, g_3^j, \dots, g_{k_j}^j\}$ where g_i^j is the output of subsystem j in state i, $i \in \{1,2, \dots k_j\}$. The output $G_j(t)$ of subsystem j at any instant $t \geq 0$ is a random variable and it takes values from g^j: $G_j(t) \in g^j$. **Assumptions** The system or subsystem may have many levels of degradation which vary from perfect functioning to complete failure. The system or subsystem might fail any 'up' state to its 'down' states and it is minimally repaired. The components of the system might fail independently and they are operated continuous basis. The components of the system are repaired independently.

3 Analysis of Model

Consider a subsystem with m components having $0,1,2,\dots k$ states where k is the best functioning state and 0 is the worst state. The state space of the system is $S = \{0,1,2,\dots k\}$. Components of the system have variable failure rates and variable repair rates . When a component fails a repair action is initiated to bring the component back to its initial up state. The transition probabilities of the Markov process $\{X(t), t \geq 0\}$ with state space $S = \{0,1,2, \dots, k\}$.

$p_{ij}(t) = Pr\{X(t) = j/X_0 = i\}$ for all $i,j \in S$ arranged as a matrix,

$$p(t) = \begin{bmatrix} p_{00}(t) & p_{01}(t) & \cdots & p_{0k}(t) \\ p_{10}(t) & p_{11}(t) & \cdots & p_{1k}(t) \\ \vdots & \vdots & \vdots & \vdots \\ p_{r0}(t) & p_{r1}(t) & \cdots & p_{kk}(t) \end{bmatrix}$$

$0 \leq p_{ij}(t) \leq 1$ for all $t \geq 0 i,j \in S$

$$\sum_{j=0}^{k} p_{ij}(t) = 1 for all i \in S.$$

Specify the transition rates a_{ij} for $i \neq j i,j \in S$. Each transition will usually involve a failure or a repair. The transition rates will therefore be failure rates and repair rates and combinations of these. Hence the infinitesimal generator of the process is

$$A = \begin{pmatrix} a_{00} & a_{01} & \cdots & a_{0k} \\ a_{10} & a_{11} & \cdots & a_{1k} \\ \vdots & \vdots & \vdots & \vdots \\ a_{k0} & a_{k1} & \cdots & a_{kk} \end{pmatrix},$$

where $a_{ii} = -\sum_{j=0, j\neq i}^{k} a_{ij}$.

Let $p(t) = \begin{bmatrix} p_0(t), p_1(t), \cdots, p_k(t) \end{bmatrix}$ denote the distribution of Markov process at time t, when we know that the process started in state i at time 0. The distribution $p(t)$ may be found from the Kolmogrov forward equations given in matrix form (see[10]) as

$$p(t)A = \dot{p}(t). \tag{1}$$

Equation (1) is called state equation for the Markov Process. In many application the long run (steady state) probabilities are of interest.

The steady state probabilities $p = \begin{bmatrix} p_0 & p_1 & \cdots & p_k \end{bmatrix}$ are given by must therefore satisfy the matrix equation.

$$pA = 0 \tag{2}$$

and

$$\sum_{j=0}^{k} p_j = 1.$$

This can be computed easily using computation algorithms based on MATLAB.

In general, a system consists of n subsystems with each subsystem possessing k states.Here $g^j = \{g_1^j, g_2{}^j, g_3^j, \dots, g_k^j\}$ is the performance level of subsystem j. The steady state probability of j^{th} subsystem is determined by previously described stochastic process approach.

ie,$p^j = \{p_1^j, p_2^j, \dots p_k^j\}$.

The UGF[12] of the j^{th} subsystem is determined as

$$u^j(z) = \sum_{i=1}^{k} p^i z^{g^i}$$

The structure function of a MSS consisting of series and parallel subsystem may be determined by reliability block diagram method ie, iteratively composing the structure functions of the independent subsystems. In order to find u-function for the entire MSS the corresponding operators $\Omega_\Phi$operators should be applied. $\Omega_{\Phi s}$and $\Omega_{\Phi p}$ are used the subsystems connected in series and parallel respectively. For MSS with n subsystem connected in parallel the system structure function is in the form

$$U(z) = \Omega_{\Phi p}\{u^1(z), u^2(z), \dots u^n(z)\}$$

Reliability indices of the system in steady state situation

1. **Steady state MSS availability**

Steady state MSS availability can be obtained for any constant demand w

$$A_\infty(w) = \delta_A(U(z), w) = \sum_{i=1}^{k} (p^i z^{g_i}, w)$$

2. **Mean Steady state MSS performance**

Mean Steady state performance is

$$E_\infty = \sum_{i=1}^{k} p^i g^i$$

3. **Expected steady state MSS performance deficiency**

Expected steady state MSS performance deficiency can be obtained for any constant demand w

$$D_\infty(w) = \sum_{i=1}^{k} p^i max(w - g^i, 0)$$

4 Numerical Example

In Kuttiady Hydro Electric Project , governed by Kerala State Electricity Board(KSEB) under Govt.of Kerala , there are three generators with installed capacity 75MW (each with 25MW) and have same features. States and outputs of Generator 1, 2 and 3(G1, G2 and G3) are respectively 1(0MW), 2(12.5MW) and 3(25mw) and these constitute Subsystem 1. Other three generators with installed capacity 150MW (each with 50MW) have same features. States and outputs of Generators 4, 5 and 6 (G4, G5 and G6) are respectively 1(0MW), 2(25MW)and 3(50MW) and these generators constitute subsystem 2.

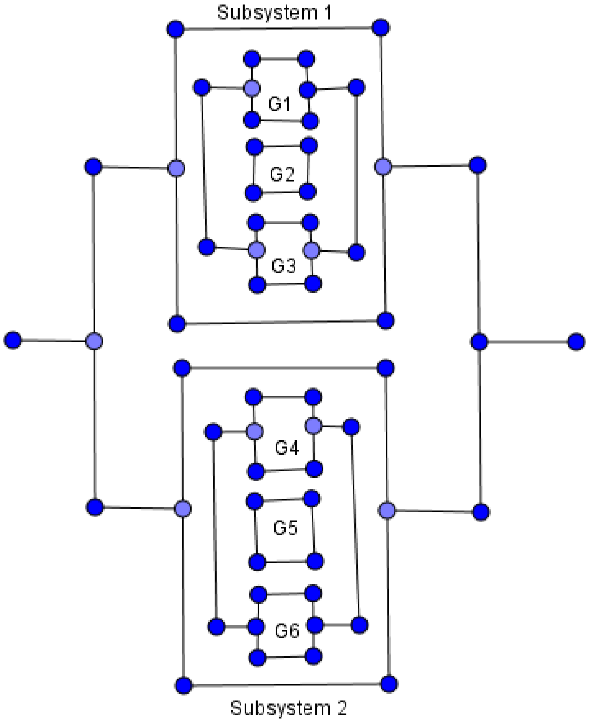


Figure 1: Reliability block diagram of power station

Subsystem 1

Transition rates of the generators G1,G2 and G3 per hour(h^{-1}) are calculated from the collected data and are given in the table below.

Table 1: Transition Rates

Generator	μ_{12}	μ_{23}	λ_{21}	λ_{32}	λ_{31}
G1	6.1×10^{-2}	6.4×10^{-2}	3×10^{-3}	6.7×10^{-2}	3.3×10^{-3}
G2	6.7×10^{-2}	6.5×10^{-2}	3×10^{-3}	6.8×10^{-2}	3.3×10^{-3}
G3	7.1×10^{-2}	5.6×10^{-2}	3×10^{-3}	5.9×10^{-2}	3.3×10^{-3}

The steady state probabilities are obtained using the following system of equations

$$p = [p_1^1 p_2^1 p_3^1 p_4^1 p_5^1 p_6^1 p_7^1]A = [0,0,0,0,0,0,0]$$

$$\sum_{j=1}^{7} p_j = 1.$$

$$\begin{gathered}
-2.1247\times10^{-1}p_1^1 + 9\times10^{-3}p_2^1 + 9.927\times10^{-3}p_3^1 + 5.9427\times10^{-5}p_4^1 \\
+3.2759\times10^{-5}p_5^1 + 9.801\times10^{-8}p_6^1 + 9.9\times10^{-3}p_7^1 = 0 \\
1.99\times10^{-1}p_1^1 + -6.4375\times10^{-1}p_2^1 + 2.7821\times10^{-1}p_3^1 + 2.0955\times10^{-2}p_4^1 \\
+1.3549\times10^{-3}p_5^1 + 3.5986\times10^{-3}p_6^1 + 1.94\times10^{-1}p_7^1 = 0 \\
1.3175\times10^{-2}p_1^1 + 5.9618\times10^{-1}p_2^1 - 1.3058p_3^1 + 4.8802\times10^{-1}p_4^1 \\
+1.1254\times10^{-1}p_5^1 + 3.3693\times10^{-3}p_6^1 + 1.2554\times10^{-2}p_7^1 = 0 \\
2.9018\times10^{-4}p_1^1 + 3.7755\times10^{-2}p_2^1 + 9.6792\times10^{-1}p_3^1 - 1.5005p_4^1 \\
+4.7544\times10^{-1}p_5^1 + 3.7498\times10^{-2}p_6^1 + 1.5492\times10^{-3}p_7^1 = 0 \\
8.1484\times10^{-4}p_2^1 + 4.8944\times10^{-2}p_3^1 + 9.5461\times10^{-1}p_4^1 - 1.1705p_5^1 \\
+3.9899\times10^{-1}p_6^1 + 2.2421\times10^{-2}p_7^1 = 0 \\
7.5753\times10^{-4}p_3^1 + 3.654\times10^{-2}p_4^1 + 5.6973\times10^{-1}p_5^1 - 6.2489\times10^{-1}p_6^1 \\
+1.94\times10^{-1}p_7^1 = 0 \\
2.3296\times10^{-4}p_4^1 + 1.1384\times10^{-2}p_5^1 + 1.85\times10^{-1}p_6^1 - 4.3442\times10^{-1}p_7^1 = 0 \\
p_1^1 + p_2^1 + p_3^1 + p_4^1 + p_5^1 + p_6^1 + p_7^1 = 1
\end{gathered}$$

Using MATLAB, we get the steady state probabilities $p_1^1, p_2^1, p_3^1, p_4^1, p_5^1, p_6^1 and p_7^1$ and tabulated below.

Sub system	Sub system	Steady state	Average hours
state	Output	Probabilities	in state/year
	0MW	0.015606342403632	136.71
	12.5MW	0.100286202268650	878.51
	25MW	0.128418120076977	1124.94
	37.5MW	0.163690419570730	1433.93
	50MW	0.226938419267982	1987.98
	62.5MW	0.251796810833076	2205.74
	75MW	0.113263685578953	992.19

Subsystem 2

Transition rates of the generators G4 , G5 and G6 per hour(h^{-1}) are calculated from the collected data and are given in the table below.

Table 2: Transition Rates

Generator	μ_{12}	μ_{23}	λ_{21}	λ_{32}	λ_{31}
G4	7.8×10^{-2}	6.6×10^{-2}	3.3×10^{-3}	6.9×10^{-2}	3×10^{-3}
G5	8.9×10^{-2}	2.4×10^{-2}	3.4×10^{-3}	2.7×10^{-2}	3.8×10^{-3}
G6	9×10^{-2}	2.6×10^{-2}	3.3×10^{-3}	2.9×10^{-2}	3.8×10^{-3}

The steady state probabilities are obtained using the following system of equations

$$[p_1^2 p_2^2 p_3^2 p_4^2 p_5^2 p_6^2 p_7^2]A = [0,0,0,0,0,0,0]$$

$$\sum_{j=1}^{7} p_j = 1$$

$$\begin{gathered}
-0.2796p_1^2 + 0.01p_2^2 + 1.0633\times10^{-2}p_3^2 + 7.0677\times10^{-5}p_4^2 \\
+3.7358\times10^{-5}p_5^2 + 1.2403\times10^{-7}p_6^2 + 4.332\times10^{-8}p_7^2 = 0 \\
0.257p_1^2 - 0.705p_2^2 + 1.489\times10^{-1}p_3^2 + 2.2074\times10^{-2}p_4^2
\end{gathered}$$

$+9.6363\times10^{-4}p_5^2+3.9215\times10^{-5}p_6^2+1.425\times10^{-6}p_7^2=0$
$2.1972\times10^{-2}p_1^2+6.5197\times10^{-1}p_2^2-1.1878p_3^2+2.2146\times10^{-1}p_4^2$
$+1.0533\times10^{-1}p_5^2+8.5445\times10^{-4}p_6^2+4.6729\times10^{-3}p_7^2=0$
$6.2478\times10^{-4}p_1^2+4.216\times10^{-2}p_2^2+9.8186\times10^{-1}p_3^2-1.1305\times10^{-1}p_4^2$
$+3.3913\times10^{-1}p_5^2+2.9187\times10^{-2}p_6^2+9.5923\times10^{-4}p_7^2=0$
$8.7763\times10^{-4}p_2^2+4.6084\times10^{-2}p_3^2+8.6276\times10^{-1}p_4^2-9.3872\times10^{-1}p_5^2$
$+2.6094\times10^{-1}p_6^2+1.5243\times10^{-2}p_7^2=0$
$3.4396\times10^{-4}p_3^2+2.4136\times10^{-2}p_4^2+4.8914\times10^{-1}p_5^2-4.0702\times10^{-1}p_6^2$
$+0.125p_7^2=0$
$4.1184\times10^{-5}p_4^1+3.924\times10^{-3}p_5^1+0.116p_6^1-1.4588\times10^{-1}p_7^1=0$
$p_1^2+p_2^2+p_3^2+p_4^2+p_5^2+p_6^2+p_7^2=1$

Using MATLAB, we get the steady state probabilities $p_1^2,p_2^2,p_3^2,p_4^2,p_5^2,p_6^2 and p_7^2$ and tabulated below.

Sub system	Sub system	Steady state	Average hours
state	Output	Probabilities	in state/year
	0MW	0.00532437363217	46.6415
	25MW	0.07393101898536	327.5636
	50MW	0.114533450326305	1003.313
	75MW	0338786626776639	2967.7709
	100MW	0.341863201329831	2994.7216
	125MW	0.084842959602057	743.2243
	150MW	0.076756286703414	672.3850715

For Subsystem 1

$g^1=0,12.5,25,37.5,50,62.5,75$
$p^1=p_1^1,p_2^1,p_3^1,p_4^1,p_5^1,p_6^1,p_7^1$
$u_1(z)=p_1^1z^0+p_2^1z^{12.5}+p_3^1z^{25}+p_4^1z^{37.5}+p_5^1z^{50}+p_6^1z^{62.5}+p_7^1z^{75}$

For Subsystem 2

$g^2=0,25,50,75,100,125,150$
$p^2=p_1^2,p_2^2,p_3^2,p_4^2,p_5^2,p_6^2,p_7^2$
$u_2(z)=p_1^2z^0+p_2^2z^{25}+p_3^2z^{50}+p_4^2z^{75}+p_5^2z^{100}+p_6^{21}z^{125}+p_7^2z^{150}$

The u-function [12]of the structure of entire system in which two subsystems are connected in parallel(total output of the power station is determined as the outputs of the two sub systems) is

$U(z)=\Omega_{\phi p}(u_1(z),u_2(z))=\Omega_{\phi p}(p_1^1z^0+p_2^1z^{12.5}+p_3^1z^{25}+p_4^1z^{37.5}+p_5^1z^{50}+$
$p_6^1z^{62.5}+p_7^1z^{75}$
$,p_1^2z^0+p_2^2z^{25}+p_3^2z^{50}+p_4^2z^{75}+p_5^2z^{100}+p_6^2z^{125}+p_7^2z^{150})$
$=p_1z^0+p_2z^{12.5}+p_3z^{25}+p_4z^{37.5}+p_5z^{50}+p_6z^{62.5}+p_7z^{75}+p_8z^{87.5}+p_9z^{100}+$
$p_{10}z^{112.5}$
$+p_{11}z^{125}+p_{12}z^{137.5}+p_{13}z^{150}+p_{14}z^{162.5}+p_{15}z^{175}+p_{16}z^{187.5}+p_{17}z^{200}+$
$p_{18}z^{212.5}+p_{19}z^{225}$

where

$p_1=p_1^1p_1^2,p_2=p_2^1p_1^2$
$p_3=p_1^1p_2^2+\mathrm{p}_3^1p_1^2,p_4=p_2^1p_2^2+p_4^1p_1^2$
$p_5=p_1^1p_3^2+p_3^1p_2^2+p_5^1p_1^2,p_6=p_2^1p_3^2+p_4^1p_2^2+p_6^1p_1^2$
$p_7=p_1^1p_4^2+p_3^1p_3^2+p_5^1p_2^2+p_7^1p_1^2,p_8=p_2^1p_4^2+p_4^1p_3^2+p_6^1p_2^2$
$p_9=p_1^1p_5^2+p_3^1p_4^2+p_5^1p_3^2+p_7^1p_2^2$
$p_{10}=p_2^1p_5^2+p_4^1p_4^2+p_6^1p_3^2$
$p_{11}=p_1^1p_6^2+p_3^1p_5^2+p_5^1p_4^2+p_7^1p_3^2$

$$p_{12} = p_2^1 p_6^2 + p_4^1 p_5^2 + p_6^1 p_4^2, p_{13} = p_1^1 p_7^2 + p_3^1 p_6^2 + p_5^1 p_5^2$$
$$p_{14} = p_2^1 p_7^2 + p_4^1 p_6^2 + p_6^1 p_5^2, p_{15} = p_3^1 p_7^2 + p_5^1 p_6^2 + p_7^1 p_5^2$$
$$p_{16} = p_4^1 p_7^2 + p_6^1 p_6^2, p_{17} = p_5^1 p_7^2 + p_7^1 p_6^2$$
$$p_{18} = p_6^1 p_7^2, p_{19} = p_7^1 p_7^2$$

Steady state MSS availability for the constant demand $w = 206.44$

$$A_\infty(w) = \delta_A(U(z), w) = \delta_A(\sum_{i=1}^{19} p_i z^{g_i}, 206.4)$$
$$= p_{18} + p_{19} = p_6^1 p_7^2 + p_7^1 p_7^2$$
$$= 0.0004126$$

Mean Steady state performance

$$E_\infty = \sum_{i=1}^{k} p^i g^i = 91.14MW$$

Expected steady state MSS performance deficiency For w = 206.4 MW

$$D_\infty(w) = \sum_{i=1}^{19} p^i max(206.4 - g^i, 0) = 114.97MW$$

5 Conclusion

Here a combination of stochastic process and UGF technique is applied for analysis of a real data of a power station by decomposing the system in to two sub systems. Steady state probabilities of the subsystems and steady state reliability indices of the power station are evaluated. Mathematical model based on straight forward stochastic process is not effective enough for system with several components with huge number of states. A new approach has been introduced in this paper by decomposing the entire MSS in to several subsystems. By using the method of combination of Markov process and UGF technique, analysis of system has been greatly simplified and reliability indices of MSS with minimal repair can be determined easily.

References

[1] Ascher H and Feingold H . Repairable Systems Reliability. Modeling, Inference, Misconceptions and their Causes. Dekker, New York. MR0762088 1984.

[2] Barlow R E and Proshan F. Mathematical Theory of Reliability, John Wiley, New York 1965.

[3] Barlow R E and Proshan F Statistical Theory of Reliability and Life Testing, HOH, Rinehart and Winston Inc, New York 1975.

[4] Kolowrocki K. Reliability of Large Systems, Elsevier, New York 2004.

[5] Levitin G. Universal generating function and its applications. Berlin: Springer; 2005

[6] Lisnianski A.Combined Universal generating functions and semi-Markov process technique for multi-state system reliability evaluation.In:Communication of fourth international conference on mathematical method in reliability, methodology and practice, MMR2004,Santa-Fe,New Mexico,June 21-25 , 2004.

[7] Lisnianski A. Extended block diagram method for a multi-state system reliability assessment. Reliability Engineering and System Safety 2007:92(12):1601-7.

[8] Lisnianski A. and Levitin G. Multi-state Reliability-assessment, Optimization and applications World Scientific:Singapore:World Scientific:2003.

[9] Lisnianski A and Ding Yi.Redundancy analysis for repairable multi-state system by using stochastic processes methods and universal generating function technique. Reliability Engineering and System Safety 2009: 94(12): 1788-95.

[10] Marvin Rausand and Arnjolt Hoyland. System Reliability theory Models, Statistical

Methods and Applications 2004.

[11] Ushakov I. A universal generating function, Sov J Comput. Syst Sci;1986:24:37-49.

[12] Ushakov I. Optimal stand by problem and universal generating function.Sov j Comput syst,Sci;1987:25.p.61-73.

[13] V M Chacko and M Manoharan. Joint Importance measures for multistate reliability systems, Opsearch(Springer) 2011: 48(3): 257-278.

[14] V M Chacko and M Manoharan. Joint Importance measures in network systems,Reliability Theory and Applications 2011: 04(23): Vol 2:December: 129-139.

ISSN 1932-2321