APPLYING PETRI NET FORMALISM IN MODELING OF MONTHLY TEST OF VALVE FROM ECC SYSTEM OF CANDU 600 NUCLEAR POWER PLANT

Marilena-Luminița BEDREAGĂ[1], Basarab GUZUN[2]

Pentru realizarea unei analize a fiabilității factorului uman, ca parte a evaluării de securitate nucleare, organismele internaționale au creat ghiduri şi proceduri pentru realizarea unui asemenea tip de analiză [1-2-3]. Lucrarea prezintă modul în care se poate realiza analiza factorului uman din punct de vedere cantitativ aplicând conceptele aferente rețelelor Petri. Aplicarea formalismului logic tip rețea Petri este o modalitatea eficientă pentru evaluarea fiabilității datorită caracteristicilor proprii.Studiul de caz se referă la analiza cantitativă a fiabilității factorului uman privind testarea lunară a vanei PV1 din sistemul ECCS sau SRAZA - Sistemul de Răcire la Avarie a Zonei Active al centralei nucleare de la Cernavoda. Se prezintă modelarea acțiunilor umane prin arbori de evenimente şi prin rețea Petri. Rezultatul obținut prin cele două metode este identic.

For human reliability analysis, as part of probabilistic safety analysis, the international regulatory commission has developed the specific guides and procedures to perform such assessment [1-2-3]. The paper presents the modality to perform human reliability quantification using Petri nets approach. This is an efficient mode to assess reliability systems because of their specific features. The case study refers only to quantitative human reliability analysis for monthly PV1 test from Emergency Cooling Core system (ECCS) of CANDU 600 Nuclear Power Plant (NPP) and we present human actions modelling using event tree and Petri nets approach. The obtained results by these two kinds of methods are in good concordance.

Keywords: human interactions, Petri nets, human reliability, state space

1. Introduction

The human factor modelling in the probabilistic safety analysis framework can be performed using different methods and models, [4]. The start point of these methods is the Technique for Human Error Rate Prediction (THERP) method [5]. It was elaborated in 1983 and it established the underlying of the human reliability field both from conceptual and quantification point of view.

[1] Eng., Institute for Nuclear Research, Piteşti, Romania
[2] Professor, Faculty of Power Engineering, *Power Generation and Use Dept.*, University POLITEHNICA from Bucharest, Romania, guzunbasarabdan@yahoo.com

The human factor quantification by THERP has accomplished using event trees approach. This represents graphical and mathematical the human actions which must be performed by operator in the system. The human actions modelling by event trees still are the accepted approach in the human reliability framework.

In 1962, it appears the concept of Petri net based on the oriented graph theory. This concept is used in modelling of the dynamic systems where the transfer operations are considered without taking into account time in explicitly manner.

The logical formalism of Petri nets grows up during the time; it has developed a particular language for that (tokens, marking, transition/place live or dead, P-invariants, T-invariants and so on) and a specific manner for mathematical representation. The analysis of system applying the concept of Petri nets is a modality of evaluation based on system states. In [9], it has been ascertained that Petri nets can also be applied in human factor modelling due to their flexibility.

In this paper, we have studied human reliability by two approaches: a deductive - which have started with analysis of tasks needed and then representation of the proper event tree, and an inductive method based on features of Petri nets.

The paper consists in following topics. In 2.1 and 2.2 we give a short presentation of the methods used: event tree for human reliability and Petri nets.

In 3, we have presented how these methods can be applied to human reliability modelling for a monthly test [15-16]. The *Petri net 2.1* and *Petri nets simulator* are software programs used in human factor modelling by Petri nets.

2. Methods

2.1 Event trees for human reliability

The modelling of human reliability has been performed by specific event trees for this kind of evaluation. In the event trees, the limbs represent binary process of decision: the task is performed correct or incorrect. For each branches, the sum of probabilities must be equal to 1 [5].

The limbs in the event trees show how can be performed activities taking into account the performance shaping factors. These factors are represented by assigned values for probability to perform tasks successfully or not. The probabilities in the event trees are conditional probabilities, except first branch.

To first branch, we can also assign a conditional probability if that represents an outcome from another event tree.

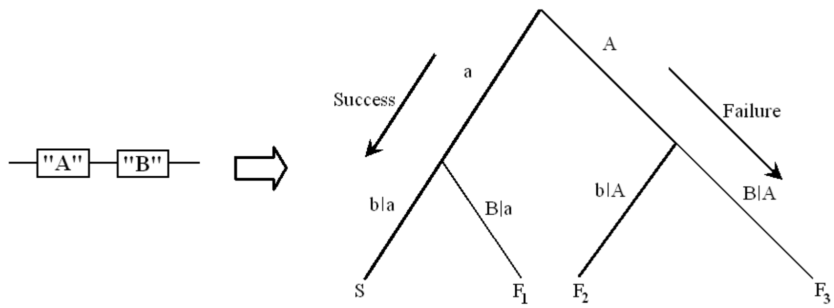

Fig. 1. Event tree of human reliability analysis according with a series diagram [5]

In Fig. 1, we have an example - the operator/technician must perform two tasks, noted by "**A**" and "**B**".

For example: the technician must perform a calibration of the transducer. For this activity, he must install the test equipment (task "**A**") and then he performs the calibration of transducer (task "**B**").

The operator will perform with success the prescribed tasks if he has performed correct both task "**A**" and task "**B**". The probability to perform correct task "**A**" and "**B**" is noted with a, respectively b, and probability to perform incorrect the task "**A**" and "**B**" is noted with A, B. Thus we have the following possibilities:

- b|a the probability to perform correct task "**B**", knowing that task "**A**" have performed successfully;
- B|a the probability to perform incorrect task "**B**", knowing that "**A**" have performed correctly;

and

- b|A the probability to perform correct task "**B**", knowing that task "**A**" have not performed correct;
- B|A the probability doesn't perform correctly both task "**B**" and task "**A**".

In Fig. 1, notations S and F represent the success, respectively failure ways.

The correct performing of tasks is written mathematical thus:

$$S = P(\text{"A"} \cap \text{"B"}) = P(\text{"A"}) \cdot P(\text{"B"} | \text{"A"}) = a \cdot (b|a) \quad (1)$$

The probability to perform incorrect established tasks is written:

$$\begin{aligned} F &= P(\overline{\text{"A"}} \cup \overline{\text{"B"}}) = P(\overline{\text{"A"}}) + P(\overline{\text{"B"}}) = A \cdot (b|A) + a \cdot (B|a) + A \cdot (B|A) \\ F &= 1 - a \cdot (b|a) = 1 - S \end{aligned} \quad (2)$$

Any failure of system due to human action is obviously after the draw of event tree. Since in human reliability analysis we have used conditional probabilities, the specific theory of Markov chains can be applied, the random variable named human error having a lognormal type density distribution [5].

2.2. Logical formalism type Petri nets

Petri nets have a very wide applicability because they have generality and permissive features. Petri nets have been applied with success in: performance evaluation, communication protocols, modelling and analysis of distributed-software systems, distributed-data base systems, concurrent and parallel programs, discrete-event systems, multiprocessor memory systems, data flow computing systems, human factors, neural networks, decisions models [9].

The particular theory of Petri nets is presented in detail in references [11-12-13]. Here, we have condensed only the basic notions required in order to understand the presented models.

Petri nets are graphical and mathematical modelling tool applicable to many systems. As a graphical tool, Petri nets can be used to view evolution of systems, similar to flow charts, block diagrams and networks. As a mathematical tool, it is possible to set up state equations and other mathematical models governing the behaviour of systems.

A Petri net (N, M_0) is a particular kind of directed graph with an initial state called the initial marking M_0. The graph N of a Petri net is a directed, weighed, bipartite graph consisting of two types of nodes called places and transitions, where arcs are either from a place to a transition or from a transition to a place. In graphical representation, places are drawn as circles, transitions as bar or boxes. Arcs are labelled with their weights (natural numbers). An arc with k-weight denotes a set of k parallel arcs.

The marking of the nets assigns to each place a natural number. If a marking assigns to place p a number k, we say, "p is marked with k tokens". The marking of nets is noted by M and it is a column vector with m x 1 dimension where m is total number of places.

In modelling, using the concept of conditions and events, places represent conditions and transitions represent events. The presence of a token in a place denotes that the establish condition for a place is true.

The concept of time is not given explicitly in the definition of Petri nets. However for performance evaluation and scheduling problems of dynamic systems it has necessary to introduce time delayed associated with transitions and/or places.

Such exist: deterministic time net if the delays are deterministic given or stochastic net if the delays are probabilistically specified [9].

A stochastic Petri net (SPN) is a net where each transition is associated with an exponentially distributed random variable that addresses the delay from the enabling to firing of a transition. In a case of a net with several transition simultaneously enabled, the transition with the shortest delay will fire first.

Due to memory less property of the exponential distribution of firing delays, the reachability graph of a bounded SPN is isomorphic to a finite Markov chain, [13]. Thus, it is possible to compute steady state probability distribution and other performance parameters of system modelled: probability of a particular condition; the expected value of the number of tokens; the mean number of firing in unit time. In this paper, we have resumed only to compute steady state probability.

The evaluation of system using Petri nets is accomplished following the steps [14]:

- develop the model using a structural approach (either top-down or bottom-up procedure) depending on system modelled;
- validate model using the results of structural analysis
- establish performance indices in terms of Petri net (places and transitions)
- establish evolution of net to obtain corresponding Markov chain
- solving Markov process
- calculate performance indices.

All these steps are easy accomplished using specialised software programs to model system with Petri nets.

3. Case study

We have modeled human reliability using these different approaches: event tree and Petri net on the case study: monthly PV1 test from ECC system of CANDU 600 NPP.

Emergency core cooling system, knowing as ECCS or SRAZA in Romanian language, is a special safety system of CANDU NPP from Cernavoda. This system has functions to remove residual and decay heat from the reactor core following the loss of coolant accident (LOCA). We present in Fig. 2 this complex system and we describe it in few words.

The system consists of three sub-systems:

- the high pressure system which injects water from ECC water tanks into reactor core using stored energy of compressed air contained in ECC gas tank

- the medium pressure system which supplies water from dousing tank and pumps it to the reactor core through ECC pumps

and finally

- the low pressure system which re-circulates water discharged from the break and dousing and accumulated on reactor building basement floor through ECC pumps. The water has cooled by the ECC heat exchanger and then pumped back into the reactor core, [16].

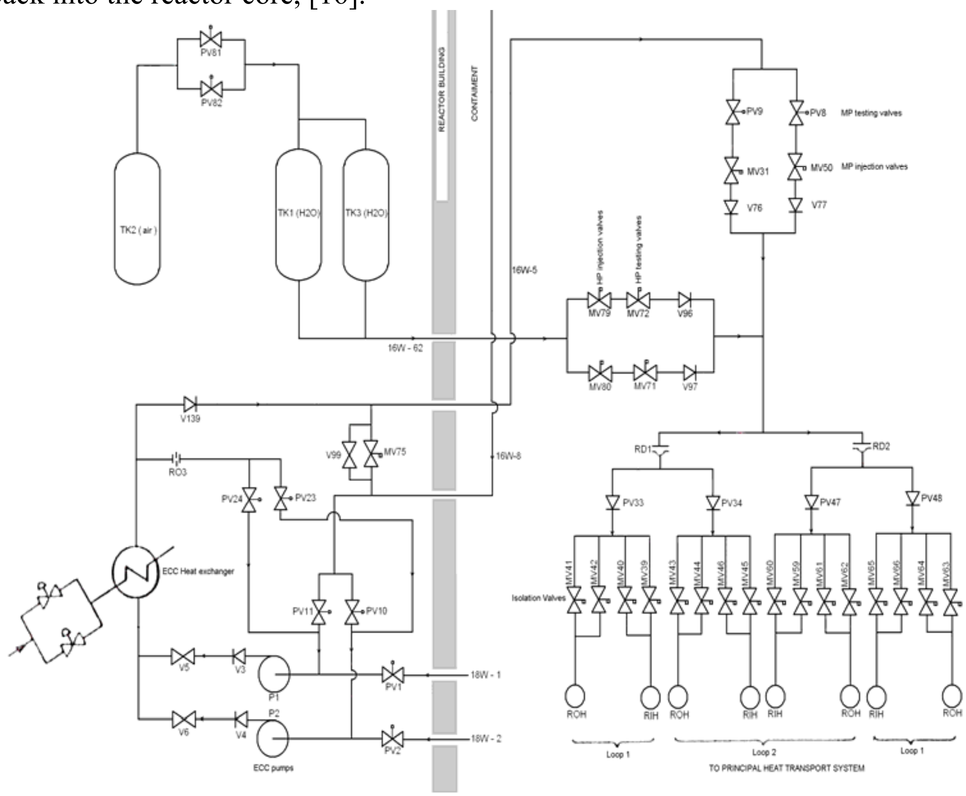

Fig. 2. Schematic representation of Emergency Core Cooling System from CANDU 600 NPP

The PV1 valve for which we have made a human reliability analysis for test activity is part of the low pressure system.

These valves (PV1) and PV2 are pneumatic ones and are normally close. These valves act as containment isolating valves and are manually controlled. In Main Control Room of the NPP these present hand switches in Close position and electromagnetic indicators.

In the main framework of human reliability analysis any human activity is evaluated from the point of view of human actions. The values of human error probability - HEP have been introduced in the probabilistic model of the system evaluated at the corresponding level.

To make a human reliability analysis of monthly PV1 test, we needed the test procedure, code 63432.7 - PV1/PV2 stroking test, [15].

In the procedure it has been established that in order to accomplish the test two operators are needed:

- the one must close V5/V6 valve, which is normally Open. After finished the test, the valve must be re-open.

- the second operator must follow the level of water in reactor building at STR1 and STR2.

The procedure provides the check option after the execution of the task.

The procedure consists of the following important steps from the point of view of human reliability analysis presented in Table 1, [15]:

Table 1

Important Steps of PV1/PV2 stroking test procedure

Step	Action	HEP
1	Check 6342-HS72#1 position (AUTO) *The hand switch corresponds to P2 pump. AUTO position provides a back-up for ECCS*	0.003, EF = 3
2	Move 6342-HS71#1 in OFF position *P1 Pump is out of service*	0.003, EF = 3
	On PL-3 the lamp with message "Hand switch off-normal" is ON	0.003, EF=3
3	Field operator confirm that P1 pump is OUT	0.003, EF = 3
4	Confirm that HS-77 for PV11 is in AUTO position *The PV11 normal state is CLOSE.*	0.003, EF=3
	Check PV11 electromagnetic indication	0.003, EF=3
	Close PV11 - HS-77 hand switch in CLOSE position	0.003, EF=3
	Check PV11 electromagnetic indication	0.003, EF=3
5	Confirm that 63432-HS224 is in OPEN position *This hand switch corresponds to 3432-PV24 valve*	0.003, EF=3
	Check PV24 electromagnetic indication	0.003, EF=3
	Close PV24 - HS224 in CLOSE position	0.003, EF=3
	Check PV24 electromagnetic indication	0.003, EF=3
6	*Close 3432-V5*	0.003, EF=3
7	Check if water level on 63432-LI-11#1 is normal	0.003, EF=3
8	Open PV1 - 63432-HS73 in OPEN position	0.003, EF=3
	Check PV1 electromagnetic indication	0.003, EF=3
	Note time needed to open valve	0.003, EF=3
9	Close PV1- 63432-HS73 in CLOSE position	0.003, EF=3
	Check PV1 electromagnetic indication	0.003, EF=3
	Note time needed to close valve	0.003, EF=3
10	Open PV24 - HS224 in OPEN position	0.003, EF=3
	Check PV24electromagnetic indication	0.003, EF=3
11	*Open 3432-V5*	0.003, EF=3
12	63432-HS77 in AUTO position	0.003, EF=3
	Check PV11electromagnetic indication	0.003, EF=3
13	Move 63432-HS71#1 in ON position	0.003, EF=3
14	Check light off on "Hand switch off normal"	0.003, EF=3
15	Check 3432-V5 is in OPEN position	0.003, EF=3

In Table 1 a column appears in which we have presented our estimated values for human error probability. This value represents the probability of the operator to make an error or failure probability when applying the procedure during the monthly test. The term EF - error factor represents the uncertainty level of the estimated value.

a. Event Tree

Starting with the procedure, we have drawn the event tree corresponding to human reliability analysis in applying the procedure. We considered zero dependence between the operators. The event tree is shown in Fig. 3.

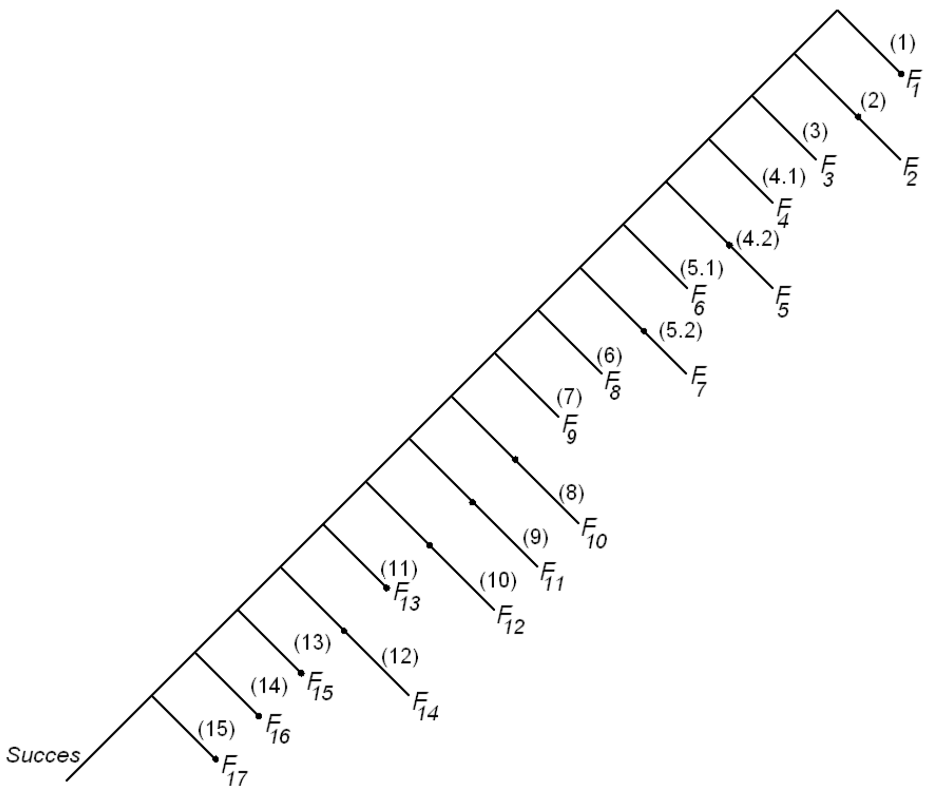

Fig. 3. Event tree for human reliability analysis of monthly PV1 test

Using event tree drawn and the estimated values for human error probabilities, we have obtained the total failure probability in monthly test of PV1 as:

$$F_{total} = \sum_{i=1}^{17} F_i = 0.003 + 0.997 \cdot 9 \cdot 10^{-6} + 0.997^2 \cdot 0.003 + 0.997^3 \cdot 0.003 + 0.997^4 \cdot 9 \cdot 10^{-6} +$$
$$+ 0.997^7 \cdot 0.003 + 0.997^6 \cdot 9 \cdot 10^{-6} + 0.997^7 \cdot 0.003 + 0.997^8 \cdot 0.003 + 0.997^9 \cdot 9 \cdot 10^{-6} +$$
$$+ 0.997^{10} \cdot 9 \cdot 10^{-6} + 0.997^{11} \cdot 9 \cdot 10^{-6} + 0.997^{12} \cdot 0.003 + 0.997^{13} \cdot 9 \cdot 10^{-6} + 0.997^{14} \cdot 0.003 +$$
$$+ 0.997^{15} \cdot 0.003 + 0.997^{16} \cdot 0.003 = 0.029318$$

b. Petri net

To develop the net, first we have defined two states represented as P_1 and P_{11} places.

The P_1 place represents the Success State of PV1 correctly testing and P_{11} place represents the Failure State. The P_2, P_3, P_4, ..., P_{10} are intermediate states.

The net is indicated in Fig. 4 and it has one token in P_1 place and has 26 intermediate transitions. We have assigned a corresponding probability for enabling and firing to every transition.

The type of net is Machine State (Fig. 5) and the corresponding incidence matrix is shown in Fig. 6.

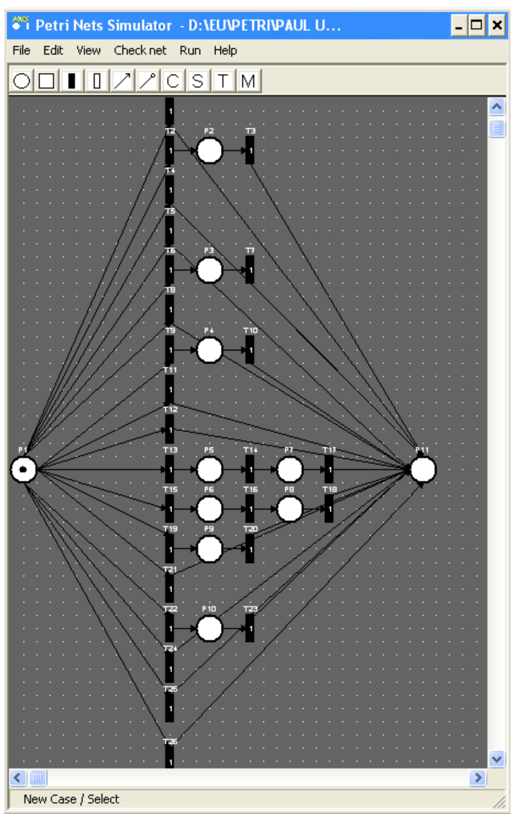

Fig. 4. Petri net corresponding to modelling of human reliability analysis in monthly PV1 test

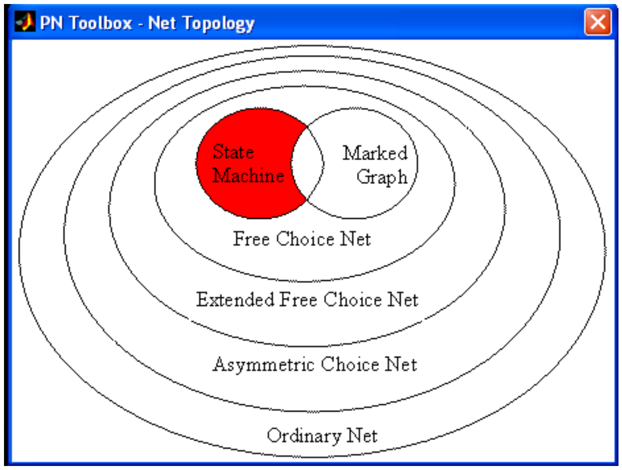

Fig. 5 Type of net

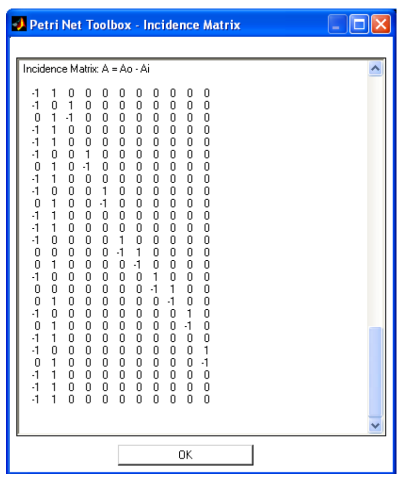

Fig. 6 Incidence matrix of net presented in Fig. 4

Knowing the incidence matrix of net and using the simulation facility of the program, we have obtained the corresponding probabilities of the net states:

- probability of Success State: 0.970682

- probability of Failure State: 0.0293180

It can be seen that the result 0.0293180 is identically with that obtained by the event tree approach.

4. Conclusions

We have presented in this paper how the logical formalism type Petri nets can be applied in the human factor modelling for a case study.

The outcome with this method is identically with the result obtained by the event trees approach.

To model human factor with Petri nets implies to define the system states and to use a specialized software program.

Using Token Game facility of the software program it can be seen the modality in which initial mark is modified by firing the transition(s). This facility transpose in human reliability modelling shows the success way to perform the tasks, respectively the failure way.

In order to apply Petri net in human reliability modelling one should know the corresponding likelihoods to failure of the actions and the logic after which one must perform the actions.

In the classic approach for human reliability analysis, the analyst draws the corresponding tree for analysis. Using this tree, he derives the success probability to perform the task, taking into account the limbs of the tree. The situation becomes difficult where there are recovery factors. A large tree with recovery factors for human actions conducts to possible mistakes in calculus.

Thus, using a software program with Petri net formalism implemented, the quantification of human reliability analysis is automatically achieved without mistakes.

The results of our work prove that human reliability modelling using Petri net concepts is an alternative, efficient modality of the event tree specific for human reliability analysis.

R E F E R E N C E S

[1] International Atomic Energy Agency - Procedures for conducting probabilistic safety assessments of Nuclear Power Plants (Level 1), Safety Series No. 50-P-4, 1992

[2] International Atomic Energy Agency - Human reliability in Probabilistic Safety Assessment for Nuclear Power Plant, Safety Series 50-P-10, 1995

[3] International Atomic Energy Agency - Collection and classification of human reliability data for use in Probabilistic Safety Assessment, TECDOC-1048, 1998

[4] Nuclear Energy Agency Committee on the Safety of Nuclear Installations - Critical operator actions: human reliability modeling and data issues. Principal working group no. 5 - task 94-1 final task report, 1998

[5] *A.D. Swain,* Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. Final Report, NUREG/CR-1278, Washington, DC (USA), 1983

[6] *E. Hollnagel,* Human reliability assessment in context, Nuclear Engineering and Technology, **vol 37**, No 2, April 2005

[7] *E. Hollnagel,* The Reliability of Man-Machine Interaction. Reliability Engineering and System Safety 38, 1992

[8] NUREG-1624 - Technical basis and Implementation guidelines for a Technique for Human Event Analysis (ATHEANA), 2000
[9] *Tadao Murata,* Petri Nets: Proprieties, Analysis and Applications, IEEE **vol. 77**, no. 4, 1989
[10] *C. Ionescu,* Notițe curs master - Calitate, fiabilitate şi mentenanță, risc şi securitate, Universitatea Politehnica Bucureşti, 2004
[11] *M. Ajmone Marsan, G. Chiola,* Performance models of multiprocessor systems, Cambridge, 1988
[12] *M. Ajmone Marsan, Gianfranco Balbo, Gianni Conte,* Modelling with Generalized Stochastic Petri Nets, Universita degli studi di Torino, Dipartamento di Informatica, 1994
[13] *M.K. Molloy,* Performance analysis using stochastic Petri Nets, IEEE Trans. Computerss **vol. C-31**, no. 9, pp. 913-917, 1988
[14] *T. Jucan, F.L. Țiplea,* Rețele Petri - Teorie şi practică, Ed. Academiei Române, 1999
[15] Cernavoda NPP Operating Manual Test - Emergency Core Cooling - 63432.7 - PV1/PV2 Stroking, Rev.0, 1996
[16] Cernavoda NPP, Unit 1, Cernavoda Probabilistic Safety Evaluation CPSE PHASE B Appendix B.3 - Emergency Core Cooling System Fault Tree Rev. 1 - Gabriel Georgescu, 1995, code: 102-CITON/AD-00580-010-031.
[17] *L. Bedreagă, B. Guzun,* Applying Petri nets in human reliability analysis. WESC – Int. World Energy System Conference, Univ. Tehnică din Iaşi, Iulie 2008, 6p.
[18] *L. Bedreagă, B. Guzun,* Modelling human actions for loss of feedwater initiating event using Petri nets formalism, Nuclear 2008 - Sustainable development through nuclear reasearch and education", Int. Symposium, 28-30 May, 2008 - Piteşti, Romania.
[19] *L. Bedreagă, B. Guzun,* Modelling of the human factor using Petri nets, IREP 2007, 19-24 August, Charleston, SC, USA, 5 p.