The Operating Risk Assessment for Dependable Systems

GABRIELA TONȚ
Department of Electrical Engineering, Measurements and Electric Power Use,
Faculty of Electrical Engineering and Information Technology
University of Oradea
Universității st., no. 1, zip code 410087, Oradea, România,
gtont@uoradea.ro, http://www.uoradea.ro

The dependable and predictable behaviour of systems provides the basis for trustworthiness and confidence in any meaningful realizations of the global Information Society. However, the expectation and perception of robustness, complexity and resilience of systems are changing under the pressures of new business, technological and societal drivers.
The operating risk estimation is aligning in the larger framework of solving business and technical issues by adopting solution and decision-making under the simultaneous multi-objective conditions Dependability approached through its main attributes: Reliability, Availability, Maintainability Safety and Security (RAMSS) has requirements that may be identified by analyzing the risks faced by critical systems.
Excluding requirements that systems face related to maintain nominal specification of states and conditions, a basic taxonomy of requirements is dedicated to of the functional ones regarding error checking, recovery and protection against system failures and non-functional requirements defining the required RAMSS of the system. A shared vision in risk management regarding the stages of risk-based analysis include identification prioritization assess and decomposition of risk.
Modeling the behavior of dependable systems under realistic time-dependent operational conditions, in order to allow an incremental development, requires assessment of architecture and core capabilities of a given system in the human – machine interactions and socio–technical cohesion condition analysis.
The understanding and implementation, in context of use of dependable system, considering human factors and the quantification of the reliability of human performance in the regulatory process, are the key problem in the safety analysis and risk quantification.
The paper focuses on the modeling the robust systems, insensitive to variation, yet flexible, highly available, and safe, using Bayesian associated analysis technique expanded to support Probabilistic Risk Assessments (PRA). This methodology examines low- and high- probability consequence scenarios which can emerge as a result of occurrence of multiple events individual events. The case of study, developed in terms of operational performance validates, analytically and experimentally, the effectiveness of the proposed method for quantifying risk in systems.
Key-Words: - risk, quantification, system, configuration, probability, dependability.

1 Summary

Exponential increase of competition in the business market faced information systems with socio-technical and organizational change that demands adaptation to altered requirements of the business environment. In the state of change and risk, an anticipation of changes and feedforward adaptation forms of system to approach new real conditions is explored.
In defining risk, a common criterion is that is stemming from uncertainty, the decision taking place today and the results of implementation will be generated in the future. The uncertainty roots from the lack of full knowledge about which event of those identified will take place, at what time and which complex effects including, future effects, will be generated, their magnitude and the impact on human activity in chaotic world. Secondly, the risk involves the idea of potential loss produced by the development of a factor or a set of factors opposites to the expectation of the decision maker. It should be noted that several areas within decision analysis deal with normative results that are provably optimal for specific quantifiable decisions, and for which human intuition alone will almost never be correct or even close to correct. Using interdisciplinary dependability approach and modeling techniques paper bridged the disciplinary viewpoints towards supporting the system in operation with the aim of facilitating effective decision-making during the task.

The risk management is based on several basic components, namely: risk identification, risk assessment, development a strategy for responding to risk factors and risk control. The proposed method tries to solve a risk assessment problem through analysis and modeling the influences of the critical operating parameters in the nuclear plant.

2. Problem formulation

During the operating stage appear functional situations and running regime different from nominal values, thus is necessary to set the conjunctural optimum parameters, which adjust the system flexibly to the operating situation. The proposed method tries to solve a risk assessment problem through analysis and modeling the influences of the critical operating parameters that can be associated with the optimal allocation of redundancy.

Adverse events affecting a nuclear system may be due to external accidents or failure of the system components. Component failures are due to the occurrence of risk factors such as: design error, faulty construction, error handling, and material degradation under the environmental influences

The probability of occurrence of a nuclear accident is evaluation by the accident occurrence likelihood addition of initiation and the probability of failure of security technical systems involved in limiting the consequences of the accident initiation [2]. Analysis of accident sequences that might result from an accident initiation is using the event trees and failure. Analysis objective is to limit the expansion of a system failure. Events may occur simultaneously or may be in a cause-effect relationship some determining the effect on the other during the observation system.

2 Event propagation probability estimation

Damage conditional model with common cause in which different events express depending to the same generating cause are evaluated with relation:

$$\begin{aligned} A_1 &= B_1 \bigcup (D_2 \bigcap C) \\ A_2 &= B_2 \bigcup (D_2 \bigcap C) \end{aligned} \quad (1)$$

where B_1 and B_2 are independent causes of damage (eg. refusal to start a Diesel group);

C is the common cause (eg overload at startup);

D_1, D_2 are conditional events which must follow cause C to produce A_1, A_2 crashes.

Interconditioned events, D_1, D_2, C and A_1, A_2 is as follows:

- if D_1 and D_2 are represented by the sure event, C is event - directly common cause. If t D_1 and D_2 are represented by the impossible event, A_1 and A_2 crashes are independent. In running regime are encountered usually intermediate situations.

Neglecting events less likely, double crash event may be expressed by:

$$A_1 \cdot A_2 = (B_1 \bigcap B_2) \bigcup (D_2 \bigcap D_2 \bigcap C) \quad (2)$$

WE note that common cause events contribute decisively to double damage and negligible to the simple damage. For these events Cernavoda Power Plant has the following probabilities:

$$\begin{aligned} &P(B_1) = P(B_2) = 10^{-3}; P(C) = 10^{-4}; \\ &P(D_1) = P(D_2) = 10^{-3} \end{aligned} \quad (3)$$

Common cause event contributes more than 3% to the likelihood of single damage and to a 90% probability to double fault. This model is advantageous in the analysis of dynamical systems because it provides information on the propagation of damage. Be considered as random variables and application loading equipment with normal or lognormal distribution. If A_1 and A_2 are two unwanted events they are linked by double inequality (4) which has the significance of occurrence of simultaneous events probability**:**

$$P(A_1) \cdot P(A_2) \le P(A_1 \cdot A_2) \le \min(P(A_1), P(A_2)) \quad (4)$$

Occurrence of simultaneous events probability A_1, A_2 can be approximate as:

$$P(A_1 \cdot A_2) = \sqrt{P(A_1) \cdot P(A_2) \cdot \min(P(A_1), P(A_2))} \quad (5)$$

If $P = P(A_1) = P(A_2)$ relation (5) becomes (6):

$$P(A_1 \cdot A_2) \approx P^{\frac{3}{2}} \quad (6)$$

If N identical components are affected by the same cause (the same solicitation applied), the N random variables are associated with the density of probability $f_s(x)$. Structure resistance contains another type of random variable of probability density $f_R(x)$ and repartition function (7):

$$F_R(x) = \int_{-\infty}^{x} f_R(y)dy \quad (7)$$

same for each element considered independent, except the common cause event. Likelihood that K of the N items to defect is (8):

$$P_{\frac{K}{N}} = C_N^K \int_{-\infty}^{\infty} f_s(x)(F_R(x))^K (1 - F_R(x))^{N-K} dx \quad (8)$$

Noting with $P_{\frac{K}{K}} = P_K$ the probability of failure of the K elements of system, then P_K it will be of the form (9):

$$P_K = \int_{-\infty}^{\infty} f_s(x)(F_R(x))^K d \quad (9)$$

This model applies especially in estimating the probability of failure for mechanical components (cables, parallel loop injection) subjected to transient operating conditions. The importance of this model lies in the analysis of systems as a whole and can make reliable estimates, the boundary of the application is insufficient information on the initial data.

Establishing protection systems of a nuclear power plant is to estimate the level of safety. Structure safety system (SS) contains safety auxiliary subsystems (SAS) and special security subsystems (SSS). The concept of system has relative connotation gaining relevance only in the context in which it is invoked. An example in this regard is the auxiliary systems (SAS) and the special security systems (SSS) are regarded as elements of reliability analysis covering the safety system (SS) and if the reliability analysis reading SAS and SSS, they are treated as systems consisting of subsystems and components.

Reliability function, evaluated on the basis of block diagram in figure 1, is:

$R_{SS} = R_{SAS} + R_{SSS}$ (10)

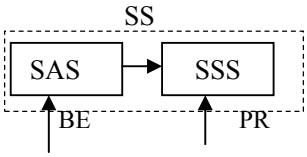

Figure 1. Block diagram of safety system (SS)

Where: BE is evacuation loop subsystem;
PR is fuel elements subsystem

The factors of importance for components in the system architecture are determined by [2]:

- the position of the component in the system;
- intrinsic reliability of element;
- others elements reliability

Assuming exponential distribution and known reliability indicators of the elements can determine failure and the repair equivalent intensities of the safety system (SS):

$$\begin{cases} \lambda_{SS} = \lambda_{SAS} + \lambda_{SSS} \\ \mu_{SS} = \dfrac{\lambda_{SS}}{\dfrac{\lambda_{SAS}}{\mu_{SAS}} + \dfrac{\lambda_{SSS}}{\mu_{SSS}}} \end{cases} \quad (11)$$

Intrinsic reliability indicators are:

$$\begin{cases} R_{SS} = \dfrac{\mu_{SS}}{\lambda_{SS} + \mu_{SS}} \\ F_{SS} = 1 - R_{SS} \\ MTBF_{SS} = \dfrac{1}{\lambda_{SS}}, MTM_{SS} = \dfrac{1}{\mu_{SS}}, M[\nu(T)\} \\ = \dfrac{\lambda_{SS}\mu_{SS}}{\lambda_{SS} + \mu_{SS}} \end{cases} \quad (12)$$

Reliability analysis takes into account that operational state of safety system is possible only in context of links with external systems (SS entries). Link status is evaluated by the associated reliability function (extrinsic), expressed by the relationship:

$R_{as} = P_{BE} + P_{PR}$ (13)

where P_{BE} is the probability of damage of heat evacuation loops from the primary and secondary circuit of the nuclear power plant;

P_{PR} is the probability of damage to fuel elements.

Reliability of the safety system of the will be:

$R_{TSS} = R_{SS} + R_{AS}$ (14)

Based on the relations above, in the following we will emphasize the way in which the safety system reliability is affected by likelihood of damage

Safety auxiliary subsystems (SAS) is composed of specific sub-systems of nuclear power plant: subsystem of auxiliary electric power supply to vital consumers (SEA) subsystem of atmospheric circulation in the outer container (SCC) subsystem protection of damage pumps for circulation (SPC) . Block equivalent reliability diagram is presented in figure 2.

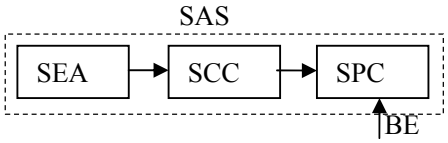

Fig. Block equivalent reliability diagram of safety auxiliary subsystems (SAS)

Reliability function of safety auxiliary subsystems (SAS) is evaluated with relation:

$$R_{SA} = R_{SEA} + R_{SCC} + R_{SPC}$$

Intrinsic reliability indicators are formulated under the form:

$$\begin{cases} SAS = \lambda_{SEA} + \lambda_{SCC} + \lambda_{SPC} \\ R_{SAS} = \dfrac{\mu_{SAS}}{\lambda_{SAS} + \mu_{SAS}} \\ \mu_{SAS} = \dfrac{\lambda_{SAS}}{\dfrac{\lambda_{SEA}}{\mu_{SEA}} + \dfrac{\lambda_{SCC}}{\mu_{SCC}} + \dfrac{\lambda_{SPC}}{\mu_{SPC}}} \end{cases} \quad (15)$$

Total reliability function of the safety auxiliary subsystems can be written as follows:

$$R_{tSAS} = R_{SA} P_{BE}$$

Special security subsystems (SSS) contains cooling subsystem in case of damage in the active reactor area, SRZA, the control loss of radioactive substance subsystem (SCP), the storage of radioactive waste subsystem (SDRR). Reliability block equivalent diagram of SSS is shown in figure 3:

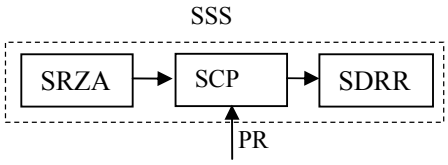

Figure 3 Reliability block equivalent diagram of SSS

Reliability function of special security subsystems (SSS) is formulated as follows:

$$R_{SSS} = R_{SRZA} + R_{SCP} + R_{SDRR} \quad (16)$$

Intrinsic reliability indicators may be represented as:

$$\begin{cases} \lambda_{SSS} = \lambda_{SRZA} + \lambda_{SCP} + \lambda_{SDRR} \\ \mu_{SSS} = \dfrac{\lambda_{SSS}}{\dfrac{\lambda_{SRZA}}{\mu_{SRZA}} + \dfrac{\lambda_{SPC}}{\mu_{SPC}} + \dfrac{\lambda_{SDR}}{\mu_{SDR}}} \\ R_{SSS} = \dfrac{\mu_{SSS}}{\lambda_{SSS} + \mu_{SSS}} \end{cases} \quad (17)$$

Total reliability function of the special security subsystems (SSS) can be written as follows:

$$R_{tSSS} = R_{SSS} P_{PR} \quad (18)$$

The obtain values of total reliability of will be introduced in relations 13 and 14 to evaluate the reliability indicators of the security system of nuclear power plant.

For the computation of damage likelihoods P_{BE} P_{PR} are take into account the relationships between subsystems highlighted by events and damage tree of auxiliary and safety systems (initiating event: pipeline rupture in the primary circuit) (fig.5).

The obtained tree shows events:

- time sequence while the intervention of security system needed, triggered in the moment the initiation accident;
- functional correlation between systems security, operation failure of the security systems can lead to other functional unsuccess.

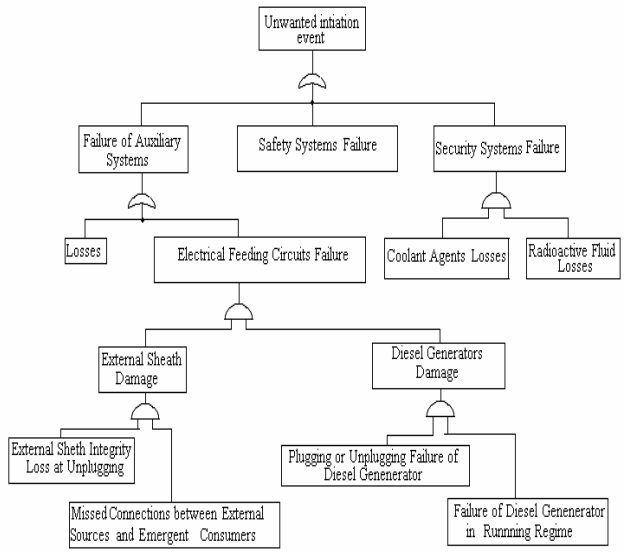

Figure 5 Events and damage tree of auxiliary and safety systems of nuclear power plant

Security systems operating at the injection phase in approximately 30 min. after the accident initiation. The probability of occurrence of damage to an item of power supply after event initiation, P_1, is greater than the probability of damage in subsystem of auxiliary electric power supply to vital consumers (SEA):

$$P_1 > P_{SEA} \quad (19)$$

Restrictive conditions are written under the form:

$$P_{SEA} << P_{SRZA}$$
$$P_{SEA} << P_C \quad (20)$$

The damage probability to the subsystem of auxiliary electric power supply to vital consumers (SEA) must be lesser than the likelihood of the core cooling damage and the container. However the likelihood of damage to auxiliary safety systems (SAS) is required to be smaller in relation to the likelihood of damage to special security system (SSS) according to the relationship:

$$P_{SAS} << P_{SSS} \quad (21)$$

Essential component of the special security system (SSS) of the nuclear power plant is a safety regulation system which detects a situation that requires intervention and safety system must have the highest reliability. Probability of failure of this system (including equipment for measuring and regulating) noted P_{SI} the need to be less than P_{SSS}:

$$P_{SI} << P_{SS}$$
$$P_{SI} << P_{SEA} \quad (22)$$

and can be estimated as:

$$P_{SI} \le 10^2 \cdot P_{SS} \tag{23}$$

Considering general criterion (23) the level of maximum permissible probability of damage in the safety system of nuclear power plant is estimated considering that the reliability of system security has the tolerated limit value (24):

$$P_{SS} < 2 \cdot 10^{-5} \tag{24}$$

The damage likelihood P_{SEA} must satisfy the relation (25):

$$P_{SEA} \le 10^{-1} \cdot P_{SS} \approx 2 \cdot 10^{-6} \tag{25}$$

Heat evacuation loops from the circuits nuclear power plant has permitted limit of damage likelihood P_{BE} as in the relation (26)

$$P_{BE} \le \frac{1}{5} P_{SS} \cong 4 \cdot 10^{-6} \tag{26}$$

and for the safety subsystem with adjustment function and measure has the maximum value allowed as in relation (27)

$$P_{RM} \le 2 \cdot 10^{-7} \tag{27}$$

2 Simulation of the cooling circuit in the presence of risk factors

The simulation of cooling agents' circuit and electrical equipment of nuclear power with the reporting of risk factors was performed using the LabVIEW graphical programming based on the heat cycle in Cernavoda nuclear-power plant.

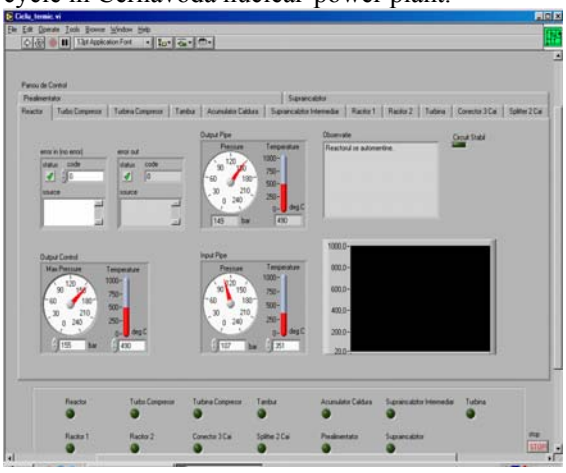

Fig. 6. Front Panel of the thermal cycle with saturated steam for rapid reactor

The Nuclear-vi provides the necessary support for measurement and simulation of the behavior of the nuclear-power plant groups in the presence of risk factors. Due to similarities with the real system by the objects contained in the interface can control application functionality through the entry and viewing of data processed. Front panel for Ciclu_termic.vi. (fig. 6) has been designed to meet practical needs, so that the operator quickly identify changes in functional parameters.

Block diagram in figure 7, conduct in the graphic language G, is the code source of the application Tambur.vi. Components are connected to define the data flow based on model transport agent in a saturated steam cycle for the fast reactor in transitional regimes. The application hierarchy is represented Nuclear vi. (fig.7).The sub-vi, Reactor.vi, simulate the reactor where the nuclear fuel burn and having the same level with Tambur1.vi in which the heat of the primary circuit water is taken by conversion to saturated steam at the same level with them is Turbina4.vi., that simulate the aggregate in which take place the adiabatic detente of cooling agent producing mechanical energy needed to power the electric generator.

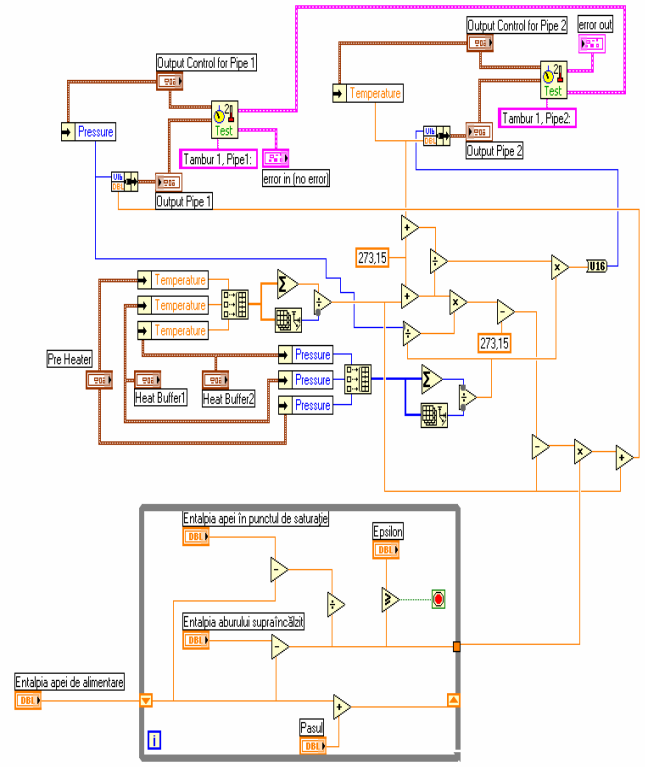

Fig.7. Steam generator diagram

Modules are subordinated Ciclu_termic.vi. Once created a .vi. can be used as a subvi. in a higher level .vi. diagram. There is no limit on the number of levels of hierarchy.

5. Case study

The supply with cooling agent for steam generator integrated in a single circuit system is provided by heater 3 and prefeeder 8, (fig.6).

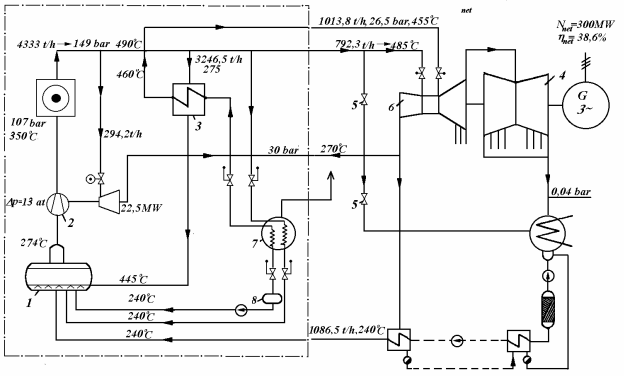

Fig.8. Diagram of a pressurized heavy water reactor

A first set of values assumed that water saturation temperature is calculated by the relationship:

$$T_s = T_x - \Delta T_{\min}^{vap} \tag{28}$$

To solve this equation, is used the finite difference method:

$$T_s = T_1 + (T_2 - T_1)\frac{i_1^{'} - i_{a1}}{i_1 - i_{a1}} \tag{29}$$

where: i_1 is superheated steam enthalpy, [kJ / kg];

i_{a1} – feedwater enthalpy, [kJ / kg];

$i_1^{'}$ – feedwater enthalpy, in the saturation point [kJ / kg];

State parameters are given in Table 1 for pr-efeeder 8 and Table 2 for supraheater, obtain both, analiticaly and by simulation.

Table1. State parameters for pre-feeder

State parameters	$t_1^{'}$ [oC]	$p_1^{'}$ [bar]	$t_2^{'}$ [oC]	$p_2^{'}$ [bar]	$t_1^{''}$ [oC]	$p_1^{''}$ [bar]
Analytically	319	45	167	21	243	33
LabView simulation	317	46	163	22	240	34

Table 2. State parameters for supraheater

	$t_1^{'}$ [°C]	$p_1^{'}$ [bar]	$t_2^{'}$ [°C]	$p_2^{'}$ [bar]	$t_1^{''}$ [°C]	$p_1^{''}$ [bar]	$t_2^{''}$ [°C]	$p_2^{''}$ [bar]
Calcul	491	149	434	101	460	124	444	124
Lab View	490	149	435	100	460	124	455	123

Similarly, are calculated both analytically and by simulation the parameters in the steam generator and turbine. The obtain values of the parameters of these equipments are also validated by Rankine cycle.

6. Conclusion

It ca be notice a good concordance between the values obtained by computation and values obtained by LabVIEW simulation, which validates the correctness of application. In the event of a emerging risk factor in one of the plant equipment using simulation parameter values are obtained depending on the parameter affected variation. Operating status of equipment is reported to the operator at the bottom of the monitor.

The operator can apply the next procedure in risk management is based on risk assessment, development a strategy for responding to risk factors and risk control.

References:

[1] Căruneanu, V. M., Mihalache A., *Bazele teoretice ale fiabilităţii*, Editura Academiei, Bucureşti, 1983.

[2] IVAS, D., MUNTEANU, F. *Modelarea cheltuielilor în calcule de optimizare a structurilor în energetică,* Rev. Energetica, seria A, nr.2, pp. 56-62, 1992.

[3]Gabriela Tonț, Dan George TONȚ, *A Simulation Method for Risk Assessment,* Analele Universităţii din Oradea, EMES 2007, pp. 165-169, 2007.

[4] Nitu, V.I., *Fiabilitate, disponibilitate, mentenanţă în energetică,* Editura Tehnică, 1987;

[5] N. A. Panayiotou, S. P. Gayialis, T. A. Panayiotou, V.I.N Leopoulos *Risk Management Issues in the Implementation of an ERP System for a Large Greek Company*, WSEAS TRANSACTION on COMPUTERS, Issue 4, Volume 3, October 2004, pp. 1005-10013., 2004.

[6] Zhang Yong-Zheng, Fang-Xing, Yun Xiao-Chun, Zhang Tao, *Quantitative Risk Assessment Approach for Host Software System Based on Network Scanning*, WSEAS TRANSACTION on INFORMATION SCIENCE AND APPLICATION, Issue 5, Volume 1, November 2004, pp. 1134-1138, 2004.

[7] H. Abdi, M. Parsa Moghaddam, M. H. Javidi, Applying Fuzzy Risk Assessment to Transmission Expansion Planning in Deregulated Power Systems, WSEAS TRANSACTIONS on POWER SYSTEMS Issue 6, Volume 1, June 2006, pp.1117-1125.