Use of Probabilistic Safety Assessment for Infrastructure Risk Modeling

Zdenko Šimić, Vladimir Mikuličić, Igor Vuković
Faculty of Electrical Eng. and Computing, University of Zagreb
Unska 3, 10000 Zagreb, Croatia
Tel.: +385 1 6129-985, fax.: +385 1 6129-890
zdenko.simic@fer.hr

Abstract. This article deals with use of Probabilistic Safety Assessment (PSA) model for infrastructure risk assessment. The first part of the paper provides background information leading to the selection of PSA as the preferred method for risk assessment. The article also discusses the initiating events, consequential events, and the consequences, dealing with scenarios and detailed list of various failure events, the associated failure modes and their cause/effect which could deal with various infrastructure interdependency risk. Example of event tree and fault-tree for selected infrastructure are discussed and presented. Emphases are given on the advantages and disadvantages of using PSA for infrastructure risk assessment. Main advantages are in the capability of PSA to deal with numerous scenarios and to provide comparative risk assessment for various infrastructure types and some interdependencies. PSA is proven methodology for combining available data with expert opinion to model complex systems risk accounting for numerous number of initiating events, systems reliability, human responses and common causes. Final results are both important for qualitative and quantitative usage in infrastructure safety optimization. This is valuable inside particular infrastructure type or between infrastructures for specific region or country. Example of nuclear power plant PSA model and interdependency on power infrastructure is presented.

Keywords. Infrastructure, risk, PSA, event tree, fault tree

1. Introduction

Most of the time key word is risk but driving issue is safety. Since safety is directly determined by risk, and it seems easier to analyze risk, we want to assess the risk. In order to know the risk we have several approaches to predict risk: testing, collecting and processing experience data, or modeling. Least preferable, and most uncertain, way of determining risk is with model assessment. Modeling is last option used only when there is not enough data from tests or experiences. Even when risk is assessed with model any experience and testing of some subsystems or elements is valuable modeling input.

Important reason to find out what is the risk is to compare risk with what is considered acceptable. If estimated risk is greater than what is considered safe or target then system has to be improved or benefit from system has to be proved sufficient to balance higher risk and expense of risk reduction. Hear again testing, experience data or assessment is required for risk reduction. It is common problem for highly safe

systems insufficient experience regarding safety performance and difficult or impossible testing for safety. Therefore, risk assessment with modeling is the necessity.

1.1. Tolerable risk

Acceptable or tolerable risk is very important issue because it sets criteria to determine if something is safe or not. There are huge variations across different countries and sectors in the both the approaches and values for acceptable risk level. Some countries and sectors have established defined levels of what is acceptable, and others are only defining general principles. Here, three well known approaches used in the process of determining acceptable risk level, are presented ([3]):

ALARP – As low as reasonably practicable. Within ALARP method collective risk levels are divided into the three regions by determining acceptable and unacceptable values. Risk between these two values are either further reduced or justified by proving that effort required for further reduction outweighs benefit.

GAME – *Globalement au moins équivalent*, also called GAMAB (Globally at least equivalent). This approach requires that new system must impose global risk level which is at least as low as risk imposed by existing similar systems.

MEM – Minimum endogenous mortality. Based on MEM method additional individual risk imposed from system should not be greater than 5% of defined overall risk without system. This is about 1E-5 per person in one year for developed countries. In order to further reduce risk from accidents with high number of fatalities this value is levered as Figure 1 shows.

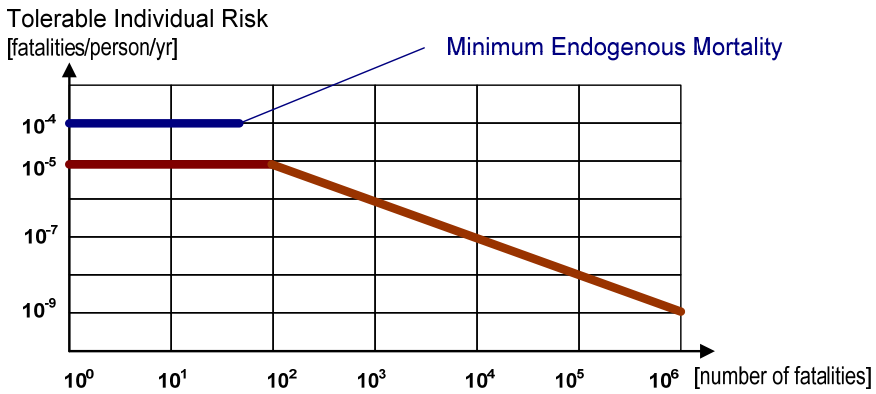

Figure 1 Tolerable Individual Risk and Relationship with a High number of Fatalities - MEM Approach

1.2. Risk Assessment Classification

During last more than 30 years numerous risk assessment methods were developed. There are literally more than hundred known risk/safety techniques/methods. Various fields of application are lesser reason for this huge number of approaches. Major reason is that there is no "silver bullet" when risk is analyzed.

Simplest way to group RA methods is according to quantitative and qualitative differentiation. This is too crude approach to give new user any greater benefit.

Much more complete and systematic classification scheme for risk assessment (RA) methods is developed in [1]. Their classification is based on approach and level

dimensions. Approach is further divided into three types: a. Temporal, b. Functional, and c. Comparative. Level is also subdivided into: 1. Abstract/expert (RA), 2. Mid-level/collaborative, and 3. Concrete/owner (system expert). From approach and level combinations nine RA method groups are defined as: a1. Engagement, b1. Sequence, c1. Principles, a2. Exercise, b2. Assistant, c2. Best practice, a3. Compliance testing, b3. Matrix, and c3. Audit. This approach seems essential for easier understanding of relations between numerous available RA methods, it is constructed to help user to understand what can be expected from given RA method, and to provide insights into how best to use particular RA method.

Additionaly, RA methods are classified based on order in which they are performed: deductive and inductive methods. Deductive methods are starting from unwanted outcome of interest, and then graphical/logical model is developed in order to find influencing factors/events combinations. Inductive methods are starting from some special system state or threat and then developing graphical/logical structure which outlines possible developing scenarios and outcomes. These two approaches are sometime used separately but they also complement each other in more complete and complex assessment which is usually called Probabilistic safety/risk assessment (PSA/PRA).

Finally, there are simulation-based methods which combine probabilistic/stochastic and deterministic models and provide more results from more dynamic scenarios. They provide better view on selected problem but they are usually limited in event and sequence space. There are examples of new methods developed as combined simulation with sequence approach as in [2].

It is out of scope for this paper to give thorough instruction about on most suitable RA method for particular problem. Major focus is to outline most important factors for selection, give basic description for available options, and illustrate in more details event tree method.

2. Risk Assessment Methods

From very rich spectrum of existing methods this paper focuses on assumption that real time testing (temporal category) is prohibitive for systems of interest, and that comparative group is inadequate. This selects from [1] three types of methods: b1. Sequence, b2. Assistant, and b3. Matrix.

Regardless of method and sector/infrastructure of interest all RA frameworks could be separated in four segments: basic events, initiating events, scenarios, and consequence (Figure 2).

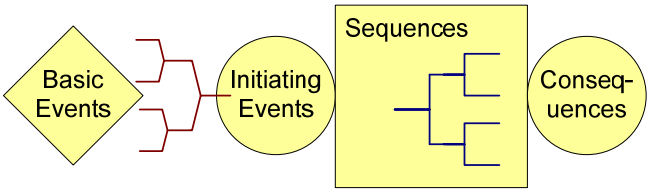

Figure 2 General RA Framework Used in all Methods

RA methods are then differentiated with the way how each of four segments are treated and interconnected. Level of details, completeness, dynamics, special issues (i.e., human errors, common cause events) are just part of particular segment of the

method and model. Choice of details is depending on system complexity and RA objective.

Several examples of RA methods are brieafly presented in order to point out their advantages and limits.

2.1. Selected RA Methods

The simplest approach (b3. Matrix: Functional-Concrete/System expert) would be for example to check for list of scenarios, or list of questions. Problem with this approach is that it is not always consistent, it is not going into the details and there is no guaranteed coverage for all important factors. Combined effect of more then one or few events is hard to capture with this type of approach. This type of methods are usually very labor intensive, but they do not require major RA expert involvement.

More complex approach (2b. Assistant: Functional-Collaborative/Mid-level) is assuring more consistency, improved level of details, but still without sufficient systematic scenario coverage, and without capability to account for multiple events effects. Examples for this type of RA methods are Hazard and Operability Studies (HAZOP) and Failure Mode and Effects Analysis (FMEA).

HAZOP is method which determines potential scenarios based on system parameters deviation with usage of guidewords, [4]. This method is mainly applied in process industry. It is usually applied as self sufficient or in combination with deterministic simulations for selected scenarios and consequences.

FMEA is method which evaluates each failure mode for all components in order to determine and classify effects in accordance with their severity or criticality (FMECA). Method is widely used with different variants in aerospace, military and general industry, [5]. It can be applied as self sufficient or preliminary phase for some other RA methods like in nuclear applications of PSA.

The most complex approach (3a. Sequence-Abstract/RA expert) is required for RA of very safe and complex systems. RA method has to provide means of building scenarios from what is known about system and potential consequences. Combined fault tree and event tree approach with human error and common cause modeling provides such method. Under the name Probabilistic safety/risk assessment (PSA/PRA) this method is in use for last 30 years mainly in nuclear and in some other industries, [7].

2.2. Probabilistic Risk Assessment

PRA/PSA method allows building RA models for very complex systems with huge number of sequences, high level of dependencies, and human factor integration. Basic events are connected thru fault tree (FT) logic which is influencing initiating events, safety functions and sequences. Event tree (ET) is connecting this altogether and producing qualitative and quantitative impact on consequences. This means that both deductive (FT) top-down and inductive (ET) bottom-up approaches are combined to produce total set of scenarios in consistent and comprehensive manner. The whole model is built in steps and connects together thousands of basic events in millions of sequences. Sensitivity and uncertainty analyses are fairly easy to apply and they help to improve model and results.

FT and ET are both logical and complement type of models, and they are easily combined together in PSA methods. In both methods failure and success domain can

be included. FT is used for hardware failure probability or initiating event frequency assessment. ET is method which helps in evaluating functional, procedural and system level dependency and produce sequences from initiating event to various consequences. One example of FT and ET is presented for illustration in this paper (Figure 4 and Figure 5).

3. Infrastructure interdependences and Risk Assessment

People in 21st century are living in extremely interconnected and dependent world. There are a number of infrastructures without which life would be highly disturbed and in great danger. Every infrastructure is both getting more and more complex and interconnected with other infrastructures. It is not new idea to design, build, and operates different infrastructures with both ideas on mind: reliability and safety. Different examples are found in aviation transportation, nuclear and process industry. Because of growing complexity, interdependency, and increased threat from attack special effort is made to analyze further what are additional risks and how they can be removed or reduced.

Most complete assessments are taking into account whole spectrum of infrastructures besides technical including social, political, economic, etc. This paper focuses only on technical infrastructures and, more specifically, on nuclear power plant dependency upon electric power system; to illustrate this dependency Figure 3 presents how selected common infrastructures are interconnected and interdependent. It is clear that some hazards (i.e. earthquake, flood, attack, or major system failure) could make one or more infrastructures damaged and that can propagate to damage other infrastructures.

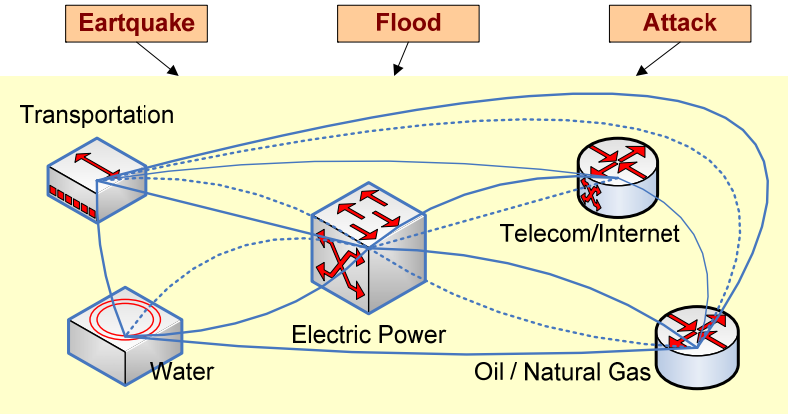

Figure 3 Networked Infrastructure Interdependencies Example

Detailed, individual (separate) safety assessment of any of these infrastructures is very complex task and still work in progress; combined modeling of these infrastructures would be even greater challenge. The assumption of the paper is that further developing of existing models for individual infrastructures or facilities of interest with inclusion of more realistic potential influence on depending infrastructures in models will be sufficient. Therefore, an example of nuclear power plant (NPP) risk and electric power system dependency is selected to illustrate the approach: the

dependency on electric power safety supply is analyzed in more details; the paper analyses the impact of the grid risk on the NPP risk.

4. Electric power safety supply

Electric power supply is needed in order to drive safety systems for reactor core cooling. There are two redundant sources of safety power supply for an NPP: diesel generators (DG) and off-site power. For this specific consideration it is of main interest to know how availability of those two power sources is changing during the NPP operation. Figure 4 presents top level logic structure of example FT for NPP electric safety supply.

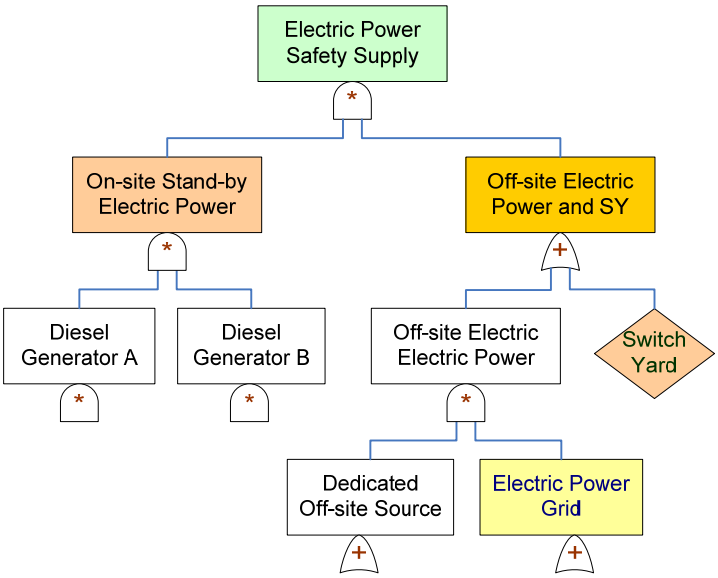

Figure 4 Nuclear Power Plant Safety Supply – Simplified Fault Tree

This FT can be explaned as follows.

DG is unavailable either when failed or when tested and maintained (T&M). Unexpected failure of DG from various causes is included in the FT model of PSA used in this evaluation and kept unchanged during the analysis. Planned unavailability during T&M is modeled in the way that T&M events are removed from PRA and DG are set to being unavailable based on designed scenario. Common cause failures are increasing total redundant DG unavailability.

Off-site source of power could be lost because of the failure of either connection to the grid (switch yard) or grid itself. Failure of the grid is possible from the number of reasons: equipment error, human error, attack, low reserves (LR), and weather. Weather and LR are both most important contributors and suitable for monitoring and predicting.

Reference [8] presents statistics for the various USA regional grids. It is clear that weather and LR are causes of 15% to almost 60% of total outages. More detailed study is done for the German and Norway grids influenced by weather conditions [9]. Results demonstrate how weather conditions strongly influence grid unavailability. For

example, failure rate for 110 kV overhead lines is increasing more than 30 times with storm conditions and more than 130 times with thunderstorm when compared to the normal weather conditions. This shows that average yearly frequency of loss of offsite power (LSP) could be better presented with incorporation of dominant factors and their change into the PSA model.

The influence from the unavailability of dedicated off-site power source (i.e. small natural gas or hydro power plant) is not treated in details in this quantification.

Figure 5 presents LSP ET which is used in one of PSA for this quantification. This is only portion of PSA model which is influenced by safety electric power availability.

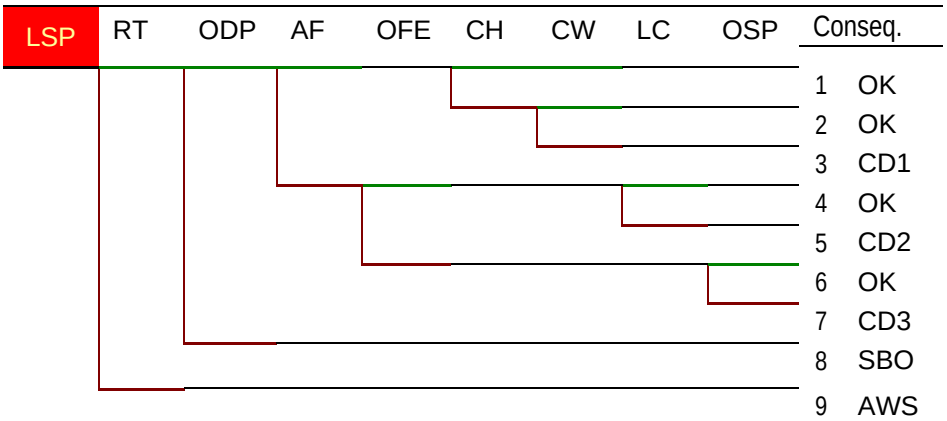

Figure 5 Loss of Offsite Power Event Tree for Nuclear Power Plant

Top Events and Consequence Legend:

LSP	Loss of Offsite Power Initiating Event		
RT	Reactor Trip	**CH2**	Charging Pump Operation
ODP	Power Available DG1 or DG2 (start, run, CC)	**CW2**	Comp. Cooling to RCP Thermal Barrier
AF	Auxiliary Feedwater and Secondary Cooling	**LC**	High Pressure Recirculation
OFE	Operator Action - Bleed and Feed	**OSP**	Offsite Power Recovered and Heat Sink Established
OK	Success.	**SBO**	Input to further Event Tree (Station Blackout)
CDx	Core Damage with certain condition (1,2,3)	**AWS**	Input to further Event Tree (Anticipated Transient without Scram)

Frequencies for example: f_{LSP}=5E-2; f_7=0,3E-6

Probability of failure example: p_{ODP}=1,5E-2; p_{OSP}=8E-1

In order to numerically evaluate risk implications of some grid conditions and NPP configurations two different PSA studies were considered. Scenarios were designed regarding DG and SY maintenance, and weather/LR influence to the LSP frequency. For one PSA study simple scenarios were designed with three levels for weather conditions and three DG maintenance strategies regarding coincidence. These results are taken from [11]. LSP frequencies are set to the highest value at about six times and lowest value at about third of average value. Yearly average LSP frequency is kept unchanged by setting respected time for each changed value in all scenarios. For example, it is assumed that the worst weather/LR condition is expected to take place during les then 4% time fraction of the one year period, etc.

Based on these three different LSP frequencies and two possible DG states, three special scenarios were arranged: worst, moderate, and best. Each scenario assumes that DG is maintained during one specific weather/LR condition. For example in the worst scenario all the DG maintenance activities are done during the worst weather/LR condition. This is unrealistic but it is representing boundary case, and it can be used for some other grid conditions – i.e. higher attack potential.

Second PRA for this analysis was used as much more complicated and realistic evaluation of the same problem. For this evaluation LSP frequency model is more complicated. Two independent factors were assumed in four different states. One factor is weather and the other is LR or some other predictable or detectable state of either grid or plant switchyard. With two possible configurations of DG number of cases increased to 25 (some extreme cases like maintenance of DG during very unfavorable states of other factors were excluded). Two scenarios were evaluated: realistic unplanned and realistic planned.

Results for second PSA and realistic unplanned scenarios are presented in Figure 6.

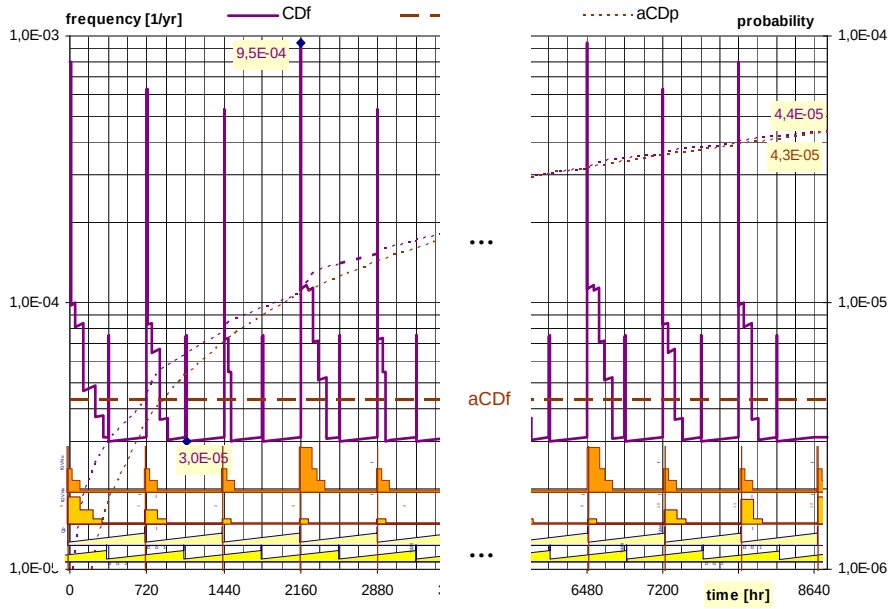

Figure 6 NPP CDF and CDP Influenced with Electric Power Unavailability

Results are indicating that core damage frequency (CDF) is dramatically changing and core damage probability (CDP) for the whole year has also changed. Change in CDP is almost 10%.

Unplanned scenario assumes periodic monthly DG maintenance schedule independently of grid condition (i.e. LSP frequency). Planned scenario assumes that DG is maintained monthly but with flexibility to avoid coincidence of unfavorable IE LSP conditions. Results for planned scenarios, not presented in the paper, are also resulting in up to triple increase of CDF.

Generally results are consistent with simpler evaluation: better planning is resulting in both CDP decrease and avoidance of extreme instantaneous CDF spikes. For facilities like NPP it is of high importance to monitor state of depending infrastructure and include that in operating configuration.

5. Conclusion

Complex facilities risk is possible to estimate only with application of PSA or similar method. This paper describes application of existing PSA model to include influence of depending infrastructure.

Numerical evaluation of PSA for NPP with more included details about operating configuration and depending infrastructures state illustrates how CDF (risk) is significantly changing during the year and what is resulting CDP. This was illustrated with detailed model related to electric power safety supply. Power grid state variations were modeled when influenced by weather and LR conditions. Similar or even higher influence on power grid could be expected from attack or flood for example.

Quantified results illustrate that this impact results in higher CDP and very high CDF spikes. It is clear that better planning will remove extreme instantaneous CDF spikes and also reduce CDP. Resulting change of yearly CDP can be visible only when complete evaluation is done for whole year.

Modeling of interdependencies among complex infrastructures is possible by taking into account their connections, influencing changes and their inclusion in existing PSA model.

Presented evaluation is arguing that more realistic modeling for risk-monitoring purposes is valuable for risk informed decision-making process, and base for the risk reduction applications.

Infrastructure interdependency risk can be reduced by making infrastructure more decentralized and less coupled. In the analyzed case that would be accomplished, for example, by additional, dedicated electric power safety supply system which would, consequently, cause significant risk reduction.

References

[1] P. L. Campbell, J. E. Stamp: "A Classification Scheme for Risk Assessment Methods", Sandia National Laboratories, SAND2004-4233, August 2004

[2] G. D. Wyss, F. A. Duràn: "OBEST – The Object-Based Event Scenario Tree Methodology", Sandia National Laboratories, SAND2001-0828, March 2001

[3] O. Nordland: "When is risk acceptable?", The 19th Int. System Safety Conference 2001 – A System Safety Odyssey, September 2001

[4] Hazard and Operability (HazOp) Studies, http://pie.che.ufl.edu/guides/hazop/

[5] Non-commercial FMEA Info Centre, http://www.fmeainfocentre.com/

[6] V. de Dianous, C. Fievez: "ARAMIS project: A more explicit demonstration of risk control through the use of bow-tie diagrams and the evaluation of safety barrier performance", J. of Hazardous Materials 130, 2006

[7] H. Kumamoto, E. J. Henley: "Probabilistic Risk Assessment and Management for Engineers and Scientists", IEEE Press, 1996

[8] B. J. Kirby, J. D. Kueck, A. B. Poole: "Evaluation of the reliability of the offsite power supply as a contributor to risk of nuclear plants", ORNL/NRC/LTR-98/12, August 1998

[9] W.-H. Wellssow, E. Schick, M. Zdrallek: "Modeling the impact of weather on the reliability of electric power systems", Safety and Reliability, ESREL '99 Vol. 1, 1999

[10] R. Zimmerman, at al.: "Electricity Case: Main Report – Risk, Consequences, and Economic Accounting", CRETE Report, 2005

[11] Z. Šimić, V. Mikuličić, I. Vrbanić “Some Insights Gained from On-Line Risk Monitoring of the Complete Plant Operating Cycle”, Technical Committee on "Risk Informed decision Making", Washington DC, USA, November 2001

[12] L. Mili, Q. Qiu, A. G. Phadke: Risk Assessment of catastrophic failures in electric power systems", Int. J. Critical Infrastructures, Vol. 1, No. 1, 2004

[13] S. A. Patterson, G. E. Apostolakis: "Identification of Critical Locations across Multiple Infrastructures fro Terrorist Actions", Workshop on National Infrastructures: Integrated Approaches to Failure in Complex Networks, University of Glasgow, August 2005