8

Probabilistic Safety Assessment and Risk-Informed Decision-Making

Marko Čepin
University of Ljubljana
Slovenia

1. Introduction

Probabilistic Safety Assessment is a standardized tool for assessing and improving nuclear power plant safety (ASME RA-S-2002, 2002; S-294, 2005; RA-S-2008, 2008). It is also used for assessment and improvement of the reliability of various systems in other industries, e.g. air and space industry and chemical industry. For the case of new nuclear power plants it may be required as a part of the safety analysis report, which is the main document needed for licensing of the plant operation.

2. History and State of the Art

Probabilistic risk analysis or probabilistic safety assessment has developed significantly in the last five decades from its first steps (Keller & Modarres, 2005), when the report known as WASH-740 was written in the year 1957 (WASH-740, 1957).
The term probabilistic risk analysis was more used in United States of America, while term probabilistic safety assessment was more used in Europe. Sometimes, the term probabilistic safety assessment was even used to specify only the systems reliability and accident sequences up to the core damage frequency, which may only refer to level 1, while the term probabilistic risk analysis was used to specify also the containment systems, which may refer to level 2, and consequence analysis, which may refer to level 3, in addition (NUREG/CR-2300, NUREG/CR-2815, 1985).
The WASH-740 study focused on the undesired consequences of large loss of coolant accident as the leading source of the worst radiation release into the environment.
A decade later, the risk curves were developed, which showed the small risk of nuclear power plants compared to other risks including risk caused by human activities and risk caused by nature itself (Farmer, 1967).
A report WASH-1400 was written in the year 1975 and a large debate followed about the applicability of the methods and results (WASH-1400, 1975). When the accident at Three Mile Island happened, it was soon concluded, that suggestions of WASH-1400 were very useful and wider applicability of the methods and results followed in the United States of America in order to prevent similar and other accidents (NUREG/CR-2300, 1982; NUREG/CR-2728, 1983; NUREG/CR-2815, 1985). Similarly, more efforts were put to

probabilistic safety assessment in other countries such as Germany (GRS, 1980) and France (Brisbois et al., 1990).
After the Chernobyl accident in Ukraine, the probabilistic safety assessment has become an obligation for all plants worldwide e.g. the Generic Letter 88-20 in United States of America (GL 88-20, 1988), e.g. the decree for probabilistic safety assessment in Slovenia.
A number of documents were prepared nationally (NUREG/CR-1150, 1989; NUREG/CR-4550, 1990; HSE, 1992) and internationally (50-P-4, 1992; 50-P-8, 1995; 50-P-12, 1996) including guidelines and examples of applications (NUREG/CR-6141, 1995). Wider performance of probabilistic safety assessment followed in the industry and in the regulatory bodies (YVL-2.8, 2003; S-294, 2005). The activities include the developed standards for probabilistic safety assessment (ASME RA-S-2002, 2002; S-294, 2005; IEC 61025, 2006; RA-S-2008, 2008). Standard ASME RA-S-2002 evolved from year 2002 to 2005 and 2008.
The further step of assessing risks was achieved by development of risk-informed decision-making, which has brought forward the risk analyses into the acceptance of decisions considering the risk analyses results. The background for risk-informed decision-making in United States of America is policy document from 1995 (60 FR 42622, 1995). The application procedures are described in regulatory guides, which evolved in years of their use (RG 1.174, 2002; RG 1.177, 1998; RG 1.200, 2007; RG 1.201, 2006). The practical applications are conducted (Vaurio, 1995; Harunuzzaman & Aldemir, 1996; Čepin & Mavko, 1997; Martorell et al., 2006).
National Aeronautics and Space Administration began to use probabilistic risk assessment methods in 1967, following the disastrous fire on Apollo 1 (PRA NASA Guide, 2002). Engineers completed a fault tree analysis for the entire Apollo system. They relied on highly conservative measures and data. They estimated so high failure probabilities for Apollo missions that the results led to a distrust of probabilistic risk assessment results. However, following the Challenger explosion in 1986, probabilistic risk assessment at national aeronautics and space administration was revived, and the Columbia break-up in 2003 reiterated the need for risk analyses.
National aeronautics and space administration used risk assessment and a combination of fault and event trees methods to model possible accident scenarios for the shuttle and International Space Station (ISS) programs (Maggio, 1996).

2.1 Lessons from the past

Unfortunately, the probabilistic safety assessment has always achieved more attention after some major accident. That was the case with Three Mile Island and Chernobyl in the nuclear industry and in the case of Apollo and Challenger in the case of space industry.
Nowadays, the probabilistic safety assessment is performed and it is used for decision-making in the most of the nuclear power plants and in the space programs (Apostolakis, 2004). The emphasis of probabilistic safety assessment to nuclear power plants as a standardised way to assess and improve safety is placed forward in this book.

3. Methods of Probabilistic Safety Assessment

The primary methods, which are integrated into probabilistic safety assessment, include fault tree analysis and event tree analysis (Kumamoto & Henley, 1996; NUREG/CR-2300,

1982; NUREG/CR-2815, 1985). The fault tree analysis is oriented to analyses of systems (NUREG-0492, 1981; Vesely et al., 2002; IEC 61025, 2006). The event tree analysis is oriented to connections between the systems (Papazoglou, 1998; Swaminathan & Smidts, 1999).

3.1 Fault Tree Analysis

The fault tree is a tool to identify and assess all combinations of undesired events in the context of system operation and its environment that can lead to the undesired state of a system (NUREG-0492, 1981; Vesely et al., 2002; Čepin & Mavko, 2002). It is not a process to identify all undesired events, but it is oriented only to those which can lead to the undesired state of the system.

Undesired state of the system is represented by a top event. The top event is an undesired event, which represents undesired state of the system of interest. The top event of the fault tree example on Fig. 1 is defined as "SS1 fails to deliver water from point A to point B" and it means that the safety system 1 fails to accomplish its mission.

The bottom part of Fig. 1 represents the example system, for which the fault tree is developed. SS1 system has to deliver specified amount of water from point A to B. Example system includes two redundant lines of the system. One line of the system is of enough capacity to accomplish success criteria of the system: line 1 or line 2 can realise the system mission.

Box B3 represents the pump B3, which has to run and box B4 represents the valve B4, which has to be open in order that the water is delivered to point B. Box B1 represents operator action, which insures water, if automatic pump operation and valve opening on line 1 are not successful. Box B5 represents the pump B5, which has to run and box B6 represents the valve B6, which has to be open in order that the water is delivered to point B. Box B2 represents operator action, which insures water, if automatic pump operation and valve opening on line 2 are not successful. The initial states of components include stopped pumps and closed valves.

The fault tree is developed in sense of faults. So, the top event usually means that the system under investigation fails or at least one of its functions fails. If the system success criteria require at least one out of two system portions to operate, the failure to meet this success criteria is represented in the top event as a failure of two out of two system portions. The duality between success criteria and failure occurrences has to be considered properly.

Logical gates connect the basic events to the top event. Logical gates on Fig. 1 are represented with abbreviations Gi (e.g. G1, G2, G3 and G4). They represent the logic connections between the components of the system. They include the logic connection between operation of the system and operator actions. They are identified by the name code and they include description. They are defined from point of view of possible faults, which can cause the top event. Each logical gate can be either the AND gate, where both input event occurrences are required for the output event, or the OR gate, where at least one of input event occurrences is required for the output event , or the K/N gate, where at least K input event occurrences are required for the output event. In theory, other logical gates can be used, such as NOR or NAND, but they are usually excluded from practical use. Negated gates are not desired because of assumptions used at evaluation of the fault trees.

Gate G1 represents the failure of line 1 to deliver water to point B.

Gate G2 represents the failure of line 2 to deliver water to point B.

The AND gate of the top event shows that both lines has to fail (line 1 has to fail and line 2 has to fail) in order that the system fails.
Gate G3 represents failures of automatic actions of pump B3 and valve B4 in order to provide water to point B.
Gate G4 represents failures of automatic actions of pump B5 and valve B6 in order to provide water to point B.

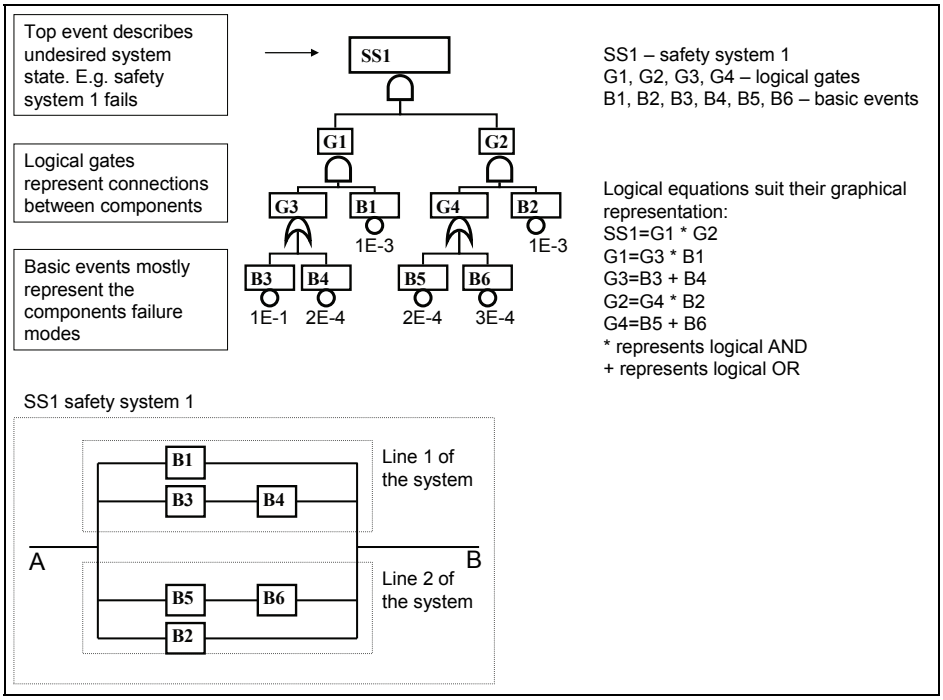


Fig. 1. Fault tree example

Basic events are the ultimate parts of the fault tree, which represent undesired events, such as component failure modes, missed actuation signals, human errors (NUREG/CR-1278, 1983), contributions of testing and maintenance activities and common cause contributions. Basic events on Fig. 1 are represented with abbreviations B_i (e.g. B1, B2, B3, B4, B5 and B6). They are identified by name code and they include description of the failure mode and identification of the component under investigation.
Basic event B3 represents failure of pump B3 to start and run for specified period of time at specified capacity. Basic event B4 represents failure of valve B4 to open and stay open for the specified period of time. Basic event B1 represents failure of operator to establish water flow if automatic action was not successful. Similarly is with basic events B2, B5 and B6 on the other line.
The fault tree is mathematically represented by a set of Boolean equations or by the fault tree figure itself. The Boolean equations and the fault tree for the example system are presented on Fig. 1.

Numbers below the basic events represent their failure probabilities, which are either obtained from data bases or they are calculated with the probabilistic models based on data about the previous experience with those or similar components and their failure modes that are defined in the respective basic events.
The qualitative fault tree analysis is the process of Boolean reduction of a set of Boolean equations. The rules of Boolean algebra are presented on Table 1. The sign for product suits the AND logic and the sign for sum suits the OR logic.

Boolean Law	Expressions		
Commutative Law	X+Y=Y+X	XY=YX	
Associate Law	(X+Y)+Z=X+(Y+Z)	(XY)Z=X(YZ)	
Distributive Law	X(Y+Z)=XY+XZ	(X+Y)Z=XZ+YZ	
Identity Law	XX=X	X+X=X	
Redundancy Law	X(X+Y)=X	X+XY=X	(X')'=X
Complementary Law	X+X'=1	XX'=0	
De Morgan's Theorem	(XY)'=X'+Y'	(X+Y)'=X'Y'	

Table 1. Rules of Boolean algebra

For the fault tree example from Fig. 1 it is needed that all five logical equations are inserted one to another in order to have one logical equation starting from top event and consisting of basic events as its parameters.

$$SS1 = ((B3+B4)*B1) * ((B5+B6)*B2) \quad (1)$$

Qualitative fault tree analysis identifies the minimal cut sets, which are the combinations of the smallest number of component faults that may cause the system fault. In other words, the minimal cut sets are combinations of the smallest number of basic events, which, if occur simultaneously, may lead to the top event.
The logical equation representing the fault tree has to be written as the sum of products. The rules of the Boolean algebra are used for rewriting of the equation. For example fault tree from Fig. 1 , eq. 2 represents such required reformulation of eq. 1.

$$SS1 = B3*B1*\ B5*B2+B4*B1*B5*B2+\ B3*B1*B6*B2+\ B4*B1*\ B6*B2 \quad (2)$$

The general expression for the minimal cut sets is the following.

$$SS = \sum_{i=1}^{n} MCS_i \quad (3)$$

SS - top event,
MCS_i - minimal cut set i,
n - number of minimal cut sets.

$$MCSi = \prod_{j=1}^{m} Bj \tag{4}$$

m - number of basic events in minimal cut set i.
For the example fault tree from Fig. 1, the qualitative results indicate four minimal cut sets. Each includes four basic events. This means that the safety system 1 fails if basic events B3 and B1 and B5 andB2 occur or if basic events B4 and B1 and B5 and B2 occur or if basic events B3 and B1 and B6 and B2 occur or if basic events B4 and B1 and B6 and B2 occur.
Minimal cut set can be a single minimal cut set, if one basic event occurrence causes the top event, or in other words: one component failure causes the system failure. Minimal cut set can be a double minimal cut set, if two basic events occurrences cause the top event, or in other words: two component failures cause the system to fail. Minimal cut set can be a triple minimal cut set, if three basic events occurrences cause the top event. The example fault tree evaluation shows that four quadruple minimal cut sets are qualitative result of fault tree evaluation of the example fault tree.
Quantitative fault tree analysis includes the following results.
- Calculation of the system unavailability, which is one of the main risk measures at the system and component level, which is based on probability of failure of safety system components and which is obtained through calculation of the top event probability.
- Calculation of Risk Increase Factor (RIF, sometimes interpreted also as Risk Achievement Worth, RAW), which identifies components, which in case of their failure (failure probability assumed as 1), impact significantly the system (or plant) risk increase. For those components it is worth to maintain them well in order that the reliability of the system is not reduced (i.e. in order that the risk is not increased).
- Calculation of Risk Decrease Factor (RDF, sometimes interpreted also as Risk Reduction Worth, RRW), which identifies components, which in case of their complete success (failure probability is assumed as 0) impact significantly the system (or plant) risk decrease. For those components it is worth to improve their reliability in order that the reliability of the system is increased (i.e. in order that the risk is decreased).
The fault tree top event probability is calculated according to eq. 5.

$$Q_S = \sum_{i=1}^{n} Q_{MCSi} - \sum_{i<j} Q_{MCSi \cap MCSj} + \\ + \sum_{i<j<k} Q_{MCSi \cap MCSj \cap MCSk} - \ldots + (-1)^{n-1} Q_{\bigcap_{i=1}^{n} MCSi} \tag{5}$$

Q_{SS} - top event probability
Or, it can be approximated with the following equation - for Q_{mcsi} less than 0.1, the approximate results stay in 10% of accuracy in the conservative side (Čepin, 2005). If the negated events are considered in the fault tree analysis, the care should be taken about the use of approximations.

$$Q_{SS} = \sum_{i=1}^{n} Q_{MCSi} \tag{6}$$

For the assumption that the basic events are mutually exclusive, the following can be used.

$$Q_{MCSi} = \prod_{j=1}^{m} Q_{Bj} \tag{7}$$

Q_{Bj} - probability of occurrence of basic event B_j

$$Q_{Bj} = Q_{Bj}(\lambda_j, \lambda_{oj}, q_j, T_{ij}, T_{tj}, T_{rj}, T_{pj,\ldots}) \tag{8}$$

Q_{Bj} - probability of occurrence of basic event B_j
λ_j - operating failure rate of the equipment modeled in the basic event B_j,
λ_{oj} - standby failure rate of the equipment modeled in the basic event B_j,
q_j - probability of failure per demand of equipment modeled in basic event B_j,
T_m – mission time,
T_{ij} - test interval of standby equipment modeled in basic event B_j,
T_{tj} - test duration time of standby equipment modeled in basic event B_j,
T_{rj} - repair time (i.e. mean time to repair or mean time to restore) of standby equipment modeled in basic event B_j,
T_{pj} - test placement time of standby equipment modeled in basic event B_j (it specifies the timing of test).
Probability of occurrence of basic event is calculated according to selected equation. Simple example of probabilistic model for a component, which should actuate on a demand is shown on the following equation.

$$q = n_s / n \tag{9}$$

q - probability of failure per demand,
n_s – number of failed operations,
n – number of all operations.
Other probabilistic models are in more details presented in references (NUREG-0492, 1981; Vesely et al., 2002).
Risk Increase Factor is calculated according to the following equation (NUREG/CR-3385, 1983; NEI 00-04, 2005).

$$RIFj = \frac{Q_{SS}(Q_{Bj} = 1)}{Q_{SS}(Q_{Bj})} \tag{10}$$

RIF_j … Risk Increase Factor for equipment modeled in basic event B_j,
$Q_{SS}(Q_{Bj})$ - top event probability,
$Q_{SS}(Q_{Bj}=1)$ - top event probability considering $Q_{Bj}=1$ (component B_j certainly fails).
Risk Decrease Factor is calculated according to the following equation.

$$RDFj = \frac{Q_{SS}(Q_{Bj})}{Q_{SS}(Q_{Bj} = 0)} \tag{11}$$

$Q_{SS}(Q_{Bj}=0)$ - top event probability considering $Q_{Bj}=0$ (component B_j cannot fail).

3.2 Event Tree Analysis

The event tree analysis is a method used to represent potential accident sequences or scenarios associated with a particular undesired initiating event (Papazoglou, 1998; Swaminathan & Smidts, 1999; PRA NASA Guide, 2002).

The initiating event is an event, which may lead to the accident consequences. The event tree model describes the logical interrelationships between potential safety system function successes and failures in a timely manner after the initiating event.

Safety system functions are the means to prevent the accident or to mitigate its consequences. Human actions can also be considered similarly as the safety system functions. Each separate safety system function can be further analysed with the fault tree analysis.

The end states of the accident scenarios are plant damage states.

Fig. 2 shows a generalised example of the event tree. Initiating event can be event such loss of offsite power or important pipe break of specified size for example if nuclear power plant is the object of investigation.

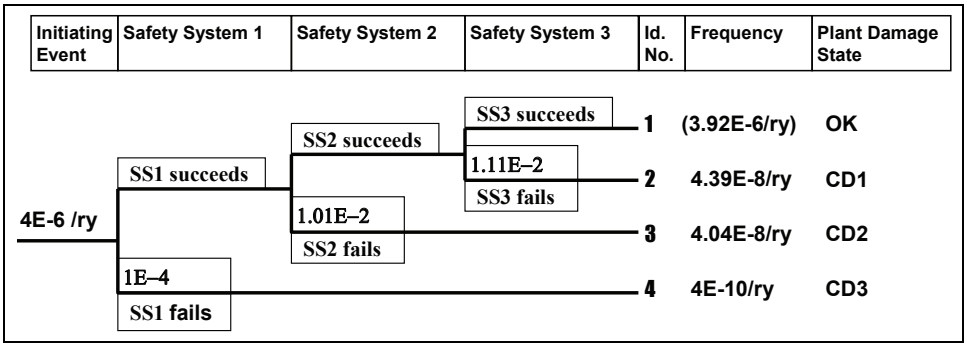


Fig. 2. Event tree – generalised example

After the initiating event, the safety system 1 should operate in sense that undesired plant damage states are reached. If the system succeeds the scenario goes upwards the event tree, if it fails, downwards at the node of safety system 1.

For all safety systems consecutively one after another as their operation follows the time and listing sequence, their success is shown in the event tree upwards from the previous node and failure is shown downwards from the node. The branches of the event tree which refer to safety system failure can be linked to a fault tree model of that safety system.

At the end, the plant damage states are identified. Code OK on the Fig. 2 means that the state of the plant is without the damage. The codes CD1, CD2 and CD3 are the codes for plant damage states. Universal plant damage state can be defined as core damage in the case of nuclear power plants.

The qualitative results of the event tree analysis include minimal cut sets for accident sequences. Accident sequence is a set of events, which result in a particular plant damage state. Example for the event tree on Fig. 2 is plant damage state 2, which ends with the CD1 plant damage state and includes initiating event, success of safety system 1, success of safety

system 2 and failure of safety system 3. If the fault trees for safety systems failures are linked to the event tree, the qualitative results of the event tree are similar as to results of the joined fault trees with the difference of presence of initiating event.
The quantitative results include accident sequences frequencies. Each accident sequence frequency is simplified as a product of initiating event frequency and safety system failure or success probabilities. If the event tree is linked with the fault trees for safety systems the initiating event frequency is multiplied with the results of the respected fault trees.

3.3 Fault Tree and Event Tree Integration

For the analysis of a nuclear power plant, several event trees are developed and each is linked with many fault trees. The results are then combined together through all respective scenarios and through all the event trees developed for the plant level analysis.
Fig. 3 shows the fault tree and event tree integration.
Probabilistic safety assessment includes tenths of event trees and hundredths of fault trees linking together thousands of gates and thousands of basic events.
If the plant damage state is core damage, the core damage frequency is the respective risk measure for the analysis at the plant level. Analyses up to the state of the reactor core are the subject of level 1 of the probabilistic safety assessment.
If the containment and its safety systems are considered in addition, the damage state can be radioactive releases to the environment. Analyses up to the state of the radioactive releases are the subject of level 2 of the probabilistic safety assessment. The large early release frequency is the respective risk measure for level 2.
Both risk measures: core damage frequency and large early release frequency are the indicators of the plant safety although the qualitative aspects of the results, which are the most important sets of component failures, which can lead to accident sequences, should not be forgotten. They have been the primary objective of the first probabilistic safety assessments.
The described procedures help to confront with risk analyses, which objectives are written in answers to three questions.
1. What can go wrong? Accident scenarios of the event trees give the answer. They can be at the level of the event tree or the can be at the level of linking with the fault trees, where each accident sequence is further represented by minimal cut sets.
How likely is it? The probabilities of failures of safety systems and the frequencies of initiating events together give the quantitative results and rank more likely and less likely accident sequences.
What are the consequences? Consequences are defined at the end states of the event trees and can be at the level of the state of the core for the level 1 of the probabilistic safety assessment, or they can be at the level of the state of the radioactive releases for the level 2 of the probabilistic safety assessment or they can be at the level 3 of the probabilistic safety assessment, which is oriented to the assessment to the dispersion of radioactive substances in the environment, where the weather conditions play the most important role.

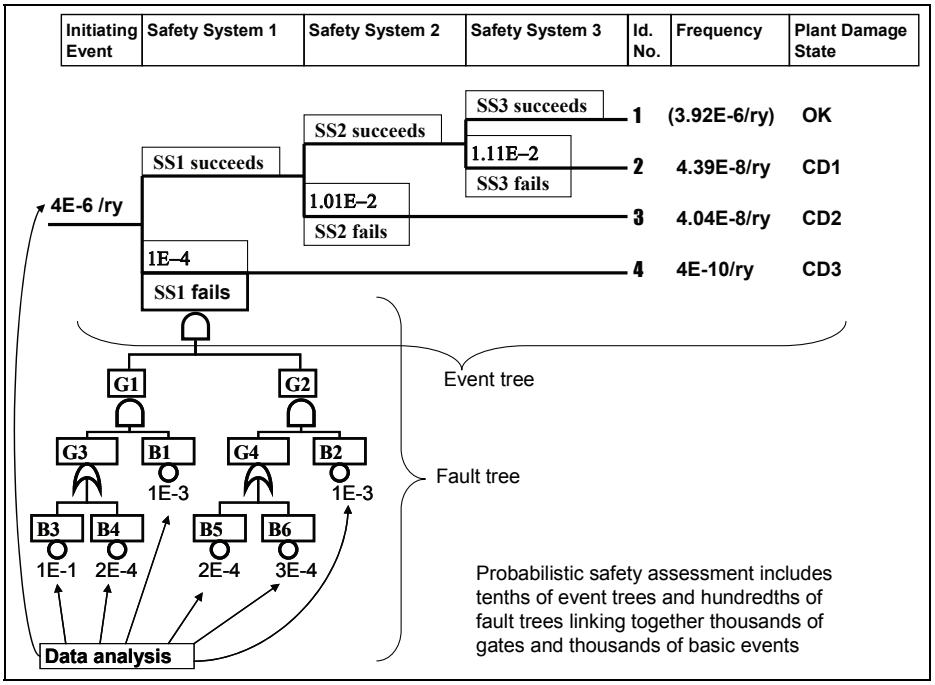


Fig. 3. Fault tree and event tree integration

The analyses show in general, that the risk of nuclear power plants is small compared to other risks to which we are exposed.

Probabilistic safety assessments provide a technique for assessing the safety of a particular facility and also an information base that is applicable to a wide variety of issues and decisions. Probabilistic safety assessment is far wider than only the presented fault tree and event tree integration. The probabilistic safety assessment includes the following main topics.

Information collection include collection of large amount of information including systems design descriptions with drawings, operating procedures, technical specifications, manufacturer requirements and recommendations for the testing and maintenance, other studies about the plant and standards about the equipment.

Analysis of human reliability and analysis of plant procedures includes the behaviour of operators during testing and maintenance and during routine operations and the diagnosis and actions of the operator teams after the occurrence of undesired initiating events.

Data-base development includes collection, classification and evaluation of generic reliability data when the specific data is not yet available and collection, classification and evaluation of plant specific data as a support for quantitative risk analyses.

Accident sequence quantification and systems quantification includes application of powerful computer codes for probabilistic safety assessment. Consideration of truncation or cut off is an important issue. Namely, the models are so large that it is not possible analytically solve the models. Approximations are made and negligible contributions are neglected (Čepin, 2005).

External event analysis includes consideration of earthquakes, fires, floods and other applicable external events for which it is necessary evaluate the plant response.
Uncertainty analysis is important as many of probabilistic models include parameters, for which is difficult to get accurate data. Approximations are done and uncertain models are used, which propagate to the results. The risk-informed decision-making has to consider the uncertainties of the evaluations.
Analysis of physical processes in materials exposed to high temperatures and pressures in normal and accident conditions is a difficult issue, which has to be performed. Many of those analyses are highly uncertain due to very demanding mathematical models of unknown processes.
Analysis of radionuclide release and transport in the environment is largely connected with weather conditions, which may impact the spread of the radionuclide materials in the environment.
Special section of the probabilistic safety assessment is its application for other modes than the full plant power operation, e.g. plant shutdown (Kiper, 2002; NUREG/CR-6144, 1995; NUREG-1449, 1992; IAEA-TECDOC-1144, 2000). Conduction of the analysis is focused to several time windows. One after another, each time window and each configuration is considered and in each time window the risks are assessed. The configuration with reactor head open for the refuelling is the most important configuration in terms of shutdown risk in nuclear power plants with pressurized water reactors.

3.4 Risk Criteria

The risk criterion is a term, which distinguishes between what is considered as an acceptable level of safety and what it is not (Čepin, 2007b).
The national approaches about risk criteria differ notably from country to country, so no commonly accepted international agreement exists (NKS-44, 2001; GS-1.14, 2002; Berg et al., 2003).
Quantitative risk objectives in United States of America consider individual and societal risk:
- The mean risk of an individual near a nuclear power plant (living within 1 mile radius) to receive an acutely lethal dose through a reactor accident is not to exceed 5E-7/year (this corresponds roughly to 0,1% of the risk from all fatal accidents).
- The risk for the general population within ten-mile-radius around a nuclear power plant to die of cancer as a result of the reactor operation should not exceed 2E-6/year (this corresponds to about 0,1% of the total cancer risk conditional on industrial activities).
In spite of the fact that no common criteria exist internationally, one can conclude that the production of electrical energy from nuclear power should not contribute notably to the overall risk is common to the national approaches.
The ALARA (As Low As Reasonably Achievable) principle is mostly acceptable, which states that the risk should be as low as it is reasonably achievable.
In addition, a common position exists that the future power plants should be better and safer than the current ones, which is the position of International Atomic Energy Agency.
Namely, the existing and future plants are distinguished in sense that the criteria are stricter in case of future plants for an order of magnitude.
The objective for core damage frequency for existing plants is 1E-4/reactor-year and for future plants it is 1E-5/ reactor-year.

The objective for large early release frequency for existing plants is 1E-5/ reactor-year and for future plants it is 1E-6/ reactor-year.

3.5 Risk-Informed Decision-Making

In addition to the risk criteria for the nuclear power plant operation, the risk criteria in some countries are developed in two aspects considering the acceptability of changes.

- The first aspect includes permanent changes; e.g. assessment of acceptability of plant modifications.
- The second aspect includes temporary changes; e.g. consideration about the on-line maintenance.

Plant modification is a permanent change in the plant, which may be a physical change (e.g. an upgrade of a system, an addition of redundant equipment, a replacement of some components) or a non-physical change (e.g. improved plant operating procedure or improved testing and maintenance procedure, a change connected with certain requirement). An assessment of acceptability of plant modifications requires the risk criteria for permanent changes in the plant, because modification is a permanent change and it represents a potential for permanent change in risk.

On-line maintenance is a wide process of planning, analysing, preparation and implementation of the testing and maintenance of the plant equipment (mostly equipment, which is in stand-by), when the plant is operating, instead of performing those activities in the outage period, when the plant is shut down for refuelling. Consideration about on-line maintenance requires the risk criteria for temporary changes in the plant, because each activity of the on-line maintenance represents a temporary change and it represents a potential for temporary change in risk. In addition, consideration about on-line maintenance may require the risk criteria for permanent changes in the plant, because the approval of the overall concept of the on-line maintenance represents a potential for permanent change in risk.

The risk-informed decision-making is a term describing the process of assessing risks connected with technical decisions and considering of the risk results together with other means or with safety analyses to reach the most appropriate decisions.

The main and the most general rule is that the activities, which results in decrease of risk, are appreciated and mostly approved. Further, the activities, for which a small increase of risk is evaluated, can be considered acceptable, if the risk increase is small and if there are benefits of the change, which overrule the increase of risk, or if there are no methods and tools to evaluate completely the proposed change in terms of positive and negative aspects in terms of risk. Namely, sometimes it is difficult to evaluate quantitatively all the positive and negative aspects of proposed change in such extent that risk models qualitatively and quantitatively include all the positive and negative aspects of the proposed change.

Finally, if a large increase of risk is connected with proposed change, such change is not acceptable.

The risk of testing and maintenance of standby safety equipment with consideration of single configuration change can be represented by the core damage frequency or by the large early release frequency. Fig. 4 shows the increased risk as a result of outage of standby equipment i where the core damage frequency is the selected risk measure.

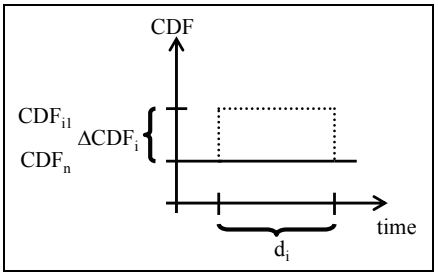


Fig. 4. The risk of testing and maintenance

The nominal risk is increased in an amount due to inoperable standby safety equipment at the time duration of testing and maintenance of equipment i. The increased risk ($Risk_i$) should be lower than the acceptance criteria, e.g. $Risk_{criteria}$=1E-6 (PSA Applications Guide, 1995; Čepin, 2007b), as it is in equation 15 below.

$$Risk_i = \Delta CDF_i \cdot d_i \tag{12}$$

where:

$$\Delta CDF_i = CDF_{i1} - CDF_n \tag{13}$$

ΔCDF_n - increase of core damage frequency due to outage of equipment i,
CDF_n - core damage frequency for the nominal conditions of the plant,
CDF_{i1} - core damage frequency with equipment i unavailable due to testing or maintenance,
d_i … time duration of testing or maintenance of equipment i.
If testing and maintenance is performed more frequently than yearly, the frequency of tests is considered in addition.

$$Risk_i = \Delta CDF_i \cdot d_i \cdot f_i \cdot T \tag{14}$$

f_i - frequency of testing and maintenance activities,
T - time interval considered (e.g. 1 year).

$$Risk_i < Risk_{criteria} \tag{15}$$

$Risk_{criteria}$ – limit of risk criteria.
The criteria may be different for one temporary change and for a cumulative impact of more temporary changes over certain time interval (Čepin, 2007b).
Examples of testing of standby safety equipment are diesel generators in a nuclear power plant. Diesel generators in a nuclear power plant are standby equipment, which should operate in the case if other sources of power system are lost. In such case, they provide power to the safety systems in order to cool the reactor, even if the reactor is in shutdown.
Table 2 shows the results of the risk evaluation, if the diesel generator 1 would be the candidate for the on-line maintenance in a nuclear plant.

The results include the core damage frequency of specific plant, its sensitivity to a specific change and the calculated increase of risk considering the risk increase due to inoperable equipment and the time duration of this inoperability.
The first column from the left identifies the status and the equipment, which may be subjected to the on-line-maintenance, which is diesel generator 1. The second column gives the core damage frequency for nominal conditions of the plant, which is the same for all on-line-maintenance activities of the same plant. The third column gives the allowed outage time, which is determined in technical specifications of the plant for the respective equipment and it is the longest possible time duration of testing and maintenance without shutting the plant down. The fourth column gives the core damage frequency with diesel generator 1 unavailable due to testing or maintenance. The fifth column gives the difference between the fourth and the second column, which represents the increase of core damage frequency with diesel generator 1 unavailable due to testing or maintenance. The sixth column gives the risk of on-line-maintenance for diesel generator 1, which is unavailable due to testing or maintenance. The risk is obtained by multiplying the increased core damage frequency with its duration, which is considered as the largest possible time duration, i.e. as the complete allowed outage time. The real risk is normally lower because the testing or maintenance is performed quicker than the complete allowed outage time. The seventh column gives the identification of the analyzed plant.
The risk results in table 2 show that on-line-maintenance of standby diesel generator 1 of plant NPP_S does not exceed the criteria (e.g. $Risk_i=Risk_{DG1}<1E-6$) even if it is performed for the complete allowed outage time.

Equipment status	CDF_n (/ry)	AOT_i (h)	CDF_{i1} (/ry)	ΔCDF_i (/ry)	$Risk_i$	NPP ID
DG1 inoperable	3,48E-05	72	5,11E-05	1,63E-05	1,34E-07	NPP_S

Table 2. Results of risk evaluation

4. Analyses, Results and Applications

Applications of probabilistic safety assessment differ at the utility and at the regulatory body. Regulatory applications of probabilistic safety assessment include monitoring and assessing the effectiveness of rules and requirements, training of the regulatory body staff, risk follow-up, risk-based safety indicators, analysis of operational events, assessment of deviations, response to emergency conditions, ranking of safety issues, ranking of importance of plant equipment, risk-informed inspection, safety guidance and prioritisation of regulatory research. Utility applications of probabilistic safety assessment include:
- optimizations of technical specifications, including surveillance requirements optimization, changes and exemptions to technical specifications (Yang et al., 2000; Čepin & Martorell, 2002),
- support for modification of licensing basis and assessment of plant changes,
- management of in-service inspection and testing, optimization of maintenance, which includes preventive and corrective maintenance (Martorell et al., 2000; Čepin, 2002),
- configuration control and planning of maintenance at outages, prioritization of activities and scheduling of the activities (Harunuzzaman & Aldemir, 1996),
- improving training for operators and operational support stuff (Čepin, 2007a; Čepin, 2008),
- improving of plant procedures (Prošek & Čepin, 2008),

- improving plant vulnerability and security questions (Čepin et al., 2006; Čepin, 2009).
In addition, probabilistic safety assessment is used for the design of new plants and it represents a chapter of the final safety report.

5. Conclusion

Probabilistic safety assessment is a standardized tool for assessing and improving nuclear power plant safety. Its primary methods are the fault tree analysis and event tree analysis. The fault tree analysis is oriented to analyses of systems, while the event tree analysis is oriented to connections between the systems.
Qualitative fault tree analysis identifies the combinations of component faults that may cause the system fault. Quantitative fault tree analysis includes calculation of the system unavailability, calculation of risk increase factor, which identifies components, for which it is worth to maintain them well in order that the risk is not increased, calculation of risk decrease factor, which identifies components, for which it is worth to increase the redundancy or to improve their reliability in order that the risk is decreased.
The results of the event tree analysis include accident sequences and their frequencies. The core damage frequency and the large early release frequency are among the most common risk measures in probabilistic safety assessment of nuclear power plants.
Quantitative risk objectives vary from country to country. The common principle says that the production of electrical energy from nuclear power should not contribute notably to the overall risk. The risk criteria are stricter in case of future plants compared to existing plants.
The risk-informed decision-making evaluates risks connected with technical decisions and helps to reach the most appropriate decisions. The applications of the risk-informed decision-making include evaluations of temporary changes such as on-line maintenance and permanent changes such as procedural changes or plant modifications in a nuclear power plant.

6. References

50-P-12 (1996). Procedures for Conduction Probabilistic Safety Assessments of Nuclear Power Plants (Level 3), Safety Series No. 50-P-12, IAEA

50-P-4 (1992). Procedures for Conduction Probabilistic Safety Assessments of Nuclear Power Plants (Level 1), Safety Series No. 50-P-4, IAEA

50-P-8 (1995). Procedures for Conduction Probabilistic Safety Assessments of Nuclear Power Plants (Level 2), Safety Series No. 50-P-8, IAEA

60 FR 42622 (1995). Use of Probabilistic Risk Assessment Methods in Nuclear Activities: Final Policy Statement, Federal Register, Vol. 60, p. 42622, USNRC

Apostolakis G. E. (2004). How Useful Is Quantitative Risk Assessment?, Risk Analysis, Vol. 24, pp. 515-520

ASME RA-S-2002 (2002). Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications. The American Society of Mechanical Engineers. ASME, 2002; Addendum, 2005

Berg H.P., R. Gortz, E. Schimetschka (2003). Quantitative Probabilistic Safety Criteria for Licensing and Operation of Nuclear Plants, BFS-SK-03/03

Brisbois J., J.M. Lanore, A. Villemeur, J.P. Berger, J.M. De Guio (1990). Les etudes probabilistes de surete des centrales nucleaires francaises de 900 et 1300 MWe (Probabilistic Safety Assessments of French 900 and 1300 MWe Nuclear Power Plants).

Čepin M. (2002). Optimization of Safety Equipment Outages Improves Safety, Reliability Engineering and System Safety, Vol. 77, pp.71-80

Čepin M. (2005). Analysis of Truncation Limit in Probabilistic Safety Assessment. Reliability Engineering and System Safety, Vol. 87 (3), pp. 395-403

Čepin M. (2007a). Importance of Human Contribution within the Human Reliability Analysis (IJS-HRA). Journal of Loss Prevention in the Process Industries, vol. 21, no. 3, pp. 268-276

Čepin M. (2007b). The risk criteria for assessment of temporary changes in a nuclear power plant, Risk analysis, Vol. 27, no. 4, pp. 991-998

Čepin M. (2008). DEPEND-HRA-A method for consideration of dependency in human reliability analysis, Reliability Engineering and System Safety, Vol. 93, no. 10, pp. 1452-1460

Čepin M. (2009). Applications of the Fault Tree Analysis for Vulnerability Studies, Chapter 8 of: Nuclear Fuels: Manufacturing Processes, Forms and Safety, Nova Science Publishers

Čepin M., B. Mavko (1997). Probabilistic Safety Assessment Improves Surveillance Requirements in Technical Specifications, Reliability Engineering and Systems Safety, Vol. 56, pp. 69-77

Čepin M., B. Mavko (2002). A Dynamic Fault Tree, Reliability Engineering and System Safety, Vol. 75, No. 1, pp. 83-91

Čepin M., Cizelj L., Leskovar M., Mavko B. (2006). Vulnerability Analysis of a Nuclear Power Plant Considering Detonations of Explosive Devices, Journal of Nuclear Science and Technology, Vol. 43, No. 10, pp. 1258-1269

Čepin M., Martorell S. (2002). Evaluation of Allowed Outage Time Considering a Set of Plant Configurations, Reliability Engineering and System Safety, Vol. 78, pp. 259-266

Farmer F. (1967). Reactor safety and siting: a proposed risk criterion, Nuclear Safety, pp. 539–548

GL 88-20 (1988). Individual Plant Examination for Severe Accident Vulnerabilities--10CFR 50.54(f), Generic Letter, US NRC

GRS (1980). Deutsche Risikostudie Kernkraftwerke, GRS

GS-1.14 (2002). Criteria for the Performance of Probabilistic Safety Assessment Applications, CSN

Harunuzzaman M., T. Aldemir (1996). Optimization of Standby Safety System Maintenance Schedules in Nuclear Power Plants, Nuclear Technology, Vol. 113, pp. 354-367

HSE (1992). Safety Assessment Principles for Nuclear Plants, Health & Safety Executive, UK, London

IAEA-TECDOC-1144 (2000). Probabilistic Safety Assessment of Nuclear Power Plants for Low Power and Shutdown Modes, IAEA

IEC 61025 (2006). Fault Tree Analysis (FTA), IEC

Keller W., M. Modarres (2005). A Historical Overview of Probabilistic Risk Assessment Development and its Use in the Nuclear Power Industry: A Tribute to the Late Professor Norman Carl Rasmussen, Reliability Engineering & System Safety, Vol. 89 (3), pp. 271-285

Kiper K. L. (2002). Insights from an All-Modes PSA at Seabrook Station, International Topical Meeting on Probabilistic Safety Assessment, Detroit, Proceedings, pp. 429-434, ANS

Kumamoto H., E. J. Henley (1996). Probabilistic Risk Assessment and Management for Engineers and Scientists, IEEE Press, New York

Maggio G. (1996). Space Shuttle Probabilistic Risk Assessment: Methodology & Application, Proceedings Annual Reliability and Maintainability Symposium, IEEE, pp. 121-132

Martorell S., S. Carlos, A. Sanchez, V. Serradell (2000). Constrained Optimization of Test Intervals Using a Steady-State Genetic Algorithm, Reliability Engineering and System safety, Vol. 67, pp. 215-232

Martorell, S., Carlos, S., Villanueva, J. F., Sánchez, A. I., Galvan, B., Salazar, D., Čepin, M. (2006). Use of Multiple Objective Evolutionary Algorithms in Optimizing Surveillance Requirements, Reliability Engineering and System Safety, Vol. 91 (9), pp. 1027-1038

NEI 00-04 (2005). 10 CFR 50.69 SSC Categorization Guideline, NEI

NKS-44 (2001). J. Holmberg, U. Puikkinen, T. Rosquist, K. Simola, Decision Criteria in PSA Applications

NUREG/CR-1150 (1989). Severe Accident Risks: An Assessment for Five US Nuclear Power Plants, US NRC

NUREG/CR-1278 (1983). Handbook for Human Reliability Analysis with Emphasis on Nuclear Power Plants Application, US NRC

NUREG/CR-2300 (1982). Probabilistic Risk Assessment Procedures Guide, US NRC

NUREG/CR-2728 (1983). Interim Reliability Evaluation Program Procedures Guide, US NRC

NUREG/CR-2815 (1985). Probabilistic Safety Analysis Procedures Guide, US NRC

NUREG/CR-3385 (1983). Measures of Risk Importance and their Applications, US NRC

NUREG/CR-4550 (1990). Analysis of Core Damage Frequency, USNRC

NUREG/CR-6141 (1995). Handbook of Methods for Risk-Based Analyses of Technical Specifications, US NRC

NUREG/CR-6144 (1995). Evaluation of Potential Severe Accident During Low Power and Shutdown Operations at Surry, Unit 1, NRC

NUREG-0492 (1981). Fault Tree Handbook, US NRC

NUREG-1449 (1992). Shutdown and Low Power Operation at Commercial Nuclear Power Plants in the United States, NRC

Papazoglou I. A. (1998). Mathematical Foundations of Event Trees, Reliability Engineering and System Safety, Vol. 61, pp. 169-183

PRA NASA Guide (2002). Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, NASA

Prošek A., M. Čepin (2008). Success criteria time windows of operator actions using RELAP5/MOD3.3 within human reliability analysis, Journal of Loss Prevention in the Process Industries, Vol. 21, no. 3, 260-267

PSA Applications Guide (1995). Electric Power Research Institute, EPRI, TR-105396

RA-S-2008 (2008). Standard for Level 1 / Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME

RG 1.174 (2002). An approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis, US NRC

RG 1.177 (1998). An approach for Plant-Specific, Risk-Informed Decisionmaking: Technical Specifications, US NRC

RG 1.200 (2007). An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities, Rev. 1, US NRC

RG 1.201 (2006). Guidelines for Categorizing Structures, Systems, and Components in Nuclear Power Plants According to their Safety Significance, Rev. 1, US NRC

S-294 (2005). Probabilistic Safety Assessment (PSA) for Nuclear Power Plants, Regulatory Standard, Canadian Nuclear Safety Commission

Swaminathan S, C. Smidts (1999). The Mathematical Formulation for the Event Sequence Diagram Framework, Reliability Engineering and System Safety, Vol. 65, pp. 103-118

Vaurio J. K. (1995). Optimization of Test and Maintenance Intervals Based on Risk and Cost, Reliability Engineering and System Safety, Vol. 49, pp. 23-36

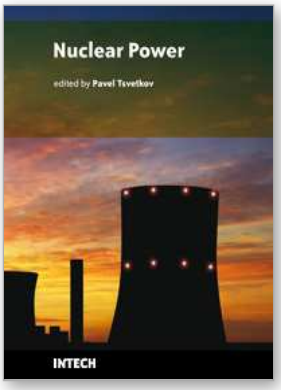
Vesely W., J. Dugan, J. Fragola, J. Minarick, J. Railsback (2002). Fault Tree Handbook with Aerospace Applications, National Aeronautics and Space Administration, NASA

WASH-1400 (1975). Reactor Safety Study: An Assessment of Accident Risks in US Commercial Nuclear Power Plants, NRC

WASH-740 (1957). Theoretical possibilities and consequences of major accidents in large nuclear power plants (The Brookhaven Report), US AEC

Yang J. E., T. Y. Sung, Y. Yin (2000). Optimization of the Surveillance Test Interval of the Safety Systems at the Plant Level, Nuclear Technology, Vol. 132, pp. 352-365

YVL-2.8 (2003). Probabilistic safety analysis in safety management of nuclear power plants, STUK



Nuclear Power

Edited by Pavel Tsvetkov

ISBN 978-953-307-110-7
Hard cover, 388 pages
Publisher Sciyo
Published online 17, August, 2010
Published in print edition August, 2010

The world of the twenty first century is an energy consuming society. Due to increasing population and living standards, each year the world requires more energy and new efficient systems for delivering it. Furthermore, the new systems must be inherently safe and environmentally benign. These realities of today's world are among the reasons that lead to serious interest in deploying nuclear power as a sustainable energy source. Today's nuclear reactors are safe and highly efficient energy systems that offer electricity and a multitude of co-generation energy products ranging from potable water to heat for industrial applications. The goal of the book is to show the current state-of-the-art in the covered technical areas as well as to demonstrate how general engineering principles and methods can be applied to nuclear power systems.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821