Risk Assessment in Advanced Engineering Design

M. Holický

Traditional methods for designing of civil engineering structures and other engineering systems are frequently based on the concept of target probability of failure. However, this fundamental quantity is usually specified on the basis of comparative studies and past experience only. Moreover, probabilistic design methods suffer from several deficiencies, including lack of consideration for accidental and other hazard situations and their consequences. Both of these extreme conditions are more and more frequently becoming causes of serious failures and other adverse events. Available experience clearly indicates that probabilistic design procedures may be efficiently supplemented by a risk analysis and assessment, which can take into account various consequences of unfavourable events. It is therefore anticipated that in addition to traditional probabilistic concepts the methods of advanced engineering design will also commonly include criteria for acceptable risks.

Keywords: hazard, risk, assessment, advanced design, structure, engineering system.

1 Notation

A_i	States of node A
B_j	States of node B
D_k	States of node D
C_{ij}	Consequences of events E_{ij} (utility, cost, damage, injuries)
C_{tot}	Total expected cost
E_{ij}	Events
H_i	Hazard situation i
H_1	Hazard situation under normal conditions
H_2	Hazard situation due to fire
H_3	Hazard situation due to fire without flashover
H_4	Hazard situation due to fire with flashover
$\mathrm{P}(F/H_i)$	Probability of failure F given situation H_i
$\mathrm{g}(\boldsymbol{x})$	Performance (limit state) function
p_F	Probability of failure F
p_{d}	Target probability of failure
p_{f}	Probability $\mathrm{P}(F\|H_2)$ of structural failure during fire
$p_{\mathrm{fi,s}}$	Probability of fire start $\mathrm{P}(H_2)$
$\boldsymbol{x}$	Generic point of the vector of basic variables
$\boldsymbol{X}$	Vector of basic variables
β	Reliability index
$\varphi_X(\boldsymbol{x})$	Probability density function of the vector of basic variables $\boldsymbol{X}$
$\Phi_{\mathrm{N}}^{-1}(p_F)$	Inverse distribution function of standardized normal variable

2 Introduction

Present standards for design of civil structures [1, 2, 3] are mostly based on the concept of the target probability of failure p_{d}. However, it is well recognised that the reliability of structures and other engineering systems suffers from a number of uncertainties, that can hardly be analysed [4, 5, 6] and well described [7] by probabilistic methods. Moreover, traditional probabilistic concepts consider the significance of failure and other adverse events only very vaguely [1, 2]. That is why probabilistic methods are often supplemented by recently developing methods of risk assessment [5, 6, 8, 9]. In some countries, risk assessment even becomes compulsory by law in the case of complex technical systems (power stations, tunnel routes) by law.

With regard to probabilistic concepts, it should be noted that civil engineering structures and other engineering systems suffer from a number of uncertainties, which can hardly be entirely described by available theoretical tools. These uncertainties include [8]:

- natural randomness of basic variables,
- statistical uncertainties caused by a limited amount of available data,
- model uncertainties caused by deficiencies of computational models,
- uncertainties caused by inaccuracy in definitions of limit states,
- gross errors caused by human faults,
- lack of understanding of the actual behaviour of materials and structures.

The above uncertainties are listed in an order corresponding to their increasing effect on the frequency of failures and the decreasing possibility of describing them theoretically. Traditional probability methods usually deal with the first three types of uncertainties only. The fourth uncertainty could be partly described using the theory of fuzzy sets [10]. Theoretical tools for the description of gross errors are insufficient [5], while no tools are available to describe lack of understanding of the actual behaviour of new materials and structures. The theoretical tools obviously have a limited capability to describe all types of uncertainties [7, 8]. This fact may partly explain the observed proportions of failure causes indicated in [8].

In general, structural failures and other adverse events occus primarily under hazard (accidental) situations (due to impact, explosion, fire and extreme climatic actions) and partially under normal (persistent) design situations due to common load effects. Obviously, further developments in advanced engineering design should be focussed on the most important causes, including the effects of various hazard situations due to human activity and extreme environmental

effects. Probabilistic concepts constitute the most important theoretical tool.

3 Probabilistic design methods

Probabilistic methods are commonly based on the assumption that an event (failure) F given a certain condition (hazard situation) H, is unequivocally described by inequality $g(\boldsymbol{x}) < 0$, where $g(\boldsymbol{x}) = 0$ is the so called limit state function and $\boldsymbol{x}$ is a realisation of the vector of basic variables $\boldsymbol{X}$. If the joint probability density $\varphi_X(\boldsymbol{x}|H)$ of basic variables $\boldsymbol{X}$ given the situation H is known, then the conditional probability $p_F = P(F|H)$ can be determined as

$$p_F = P(F|H) = \int_{g(\boldsymbol{x})<0} \varphi_{\boldsymbol{X}}(\boldsymbol{x}|H)\, d\boldsymbol{x} \,. \qquad (1)$$

Instead of the probability p_F the reliability index $\beta = -\Phi_N^{-1}(p_F)$ is often used. It is well recognised [4] that the described concept has several deficiencies. Important deficiencies originate from uncertainties in the definition of the limit state function $g(\boldsymbol{x})$ and in probabilistic models of basic variables $\boldsymbol{X}$ given the conditions H. However, the most significant and essential deficiency of probabilistic design methods based solely on equation (1) is the lack of consideration for all hazard situations H_i and the relevant consequences of unfavourable events. To reduce this drawback, methods of risk analysis and assessment have recently been developed [5, 6] and applied (e.g., [6]).

4 Basic concepts of risk assessment

The risk assessment of a system attempts to cover all possible hazard situations that might lead to unfavourable events related to the considered system. The hazard situations include gross errors in human activity and accidental actions such as impact, explosion, fire and extreme climatic loads. Identified hazard situations (including accidental and common design situations), designated generally as H_i, are assumed to occur with a certain probability $P(H_i)$. If the failure F of a structure due to a particular situation H_i occurs with the conditional probability $P(F|H_i)$, then the total probability of failure p_F is given as [11]:

$$p_F = \sum_i P(F|H_i)\, P(H_i) \,. \qquad (2)$$

The conditional probabilities $P(F|H_i)$ must usually be found by a separate analysis of the respective situations H_i. Equation (2) can be used for harmonisation of the partial probabilities of failure $P(F|H_i)\,P(H_i)$ corresponding to the situations H_i, and for the following risk consideration.

In general, the hazard situations H_i may lead to a number of events E_{ij} (e.g., collapse, excessive deformations, full development of the fire, impact). The consequences of the events E_{ij} are expressed by one-dimensional utility components C_{ij} (e.g., by the costs expressed in a certain currency). If the consequences C_{ij} are uniquely related to the events E_{ij} then the total utility (risk) C related to the hazard situations H_i is given as [8]:

$$C = \sum_{ij} C_{ij}\, P(E_{ij}|H_i)\, P(H_i) \,. \qquad (3)$$

It is sometimes necessary to describe the consequences of an unfavourable event E_{ij} by a quantity having several components, denoted as $C_{ij,k}$ (describing for example costs, injuries or casualties). The components C_k of the resultant risk are then given as

$$C_k = \sum_{ij} C_{ij,k}\, P(E_{ij}|H_i)\, P(H_i) \,. \qquad (4)$$

If it is possible to specify the acceptable limit $C_{k,d}$ for the components C_k, then the structure can be designed on the basis of the condition for acceptable risks $C_k < C_{k,d}$, which supplements the probability condition $p_f < p_d$.

Several methods have been developed to analyse risk (fault tree, event tree, causal networks). A promising method seems to be provided by Bayesian decision analysis using decision trees or Bayesian (believe) causal networks.

5 Decision tree

In general a decision tree has three basic nodes, as indicated in Fig. 1: a decision node representing alternative actions or options, a chance node representing the random outcome of the decision, and a utility node representing utility or risk outcomes of the decision [9].

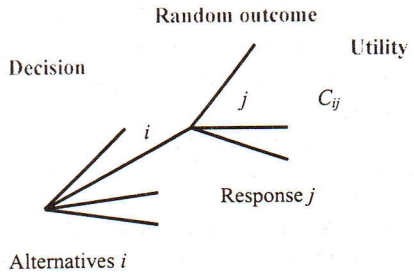

Fig. 1: Decision tree for prior and posterior analysis

The simplest form of decision analysis is so-called prior--analysis of the risk (utility) when the basic statistical and probabilistic information is available prior to any decision or activity. Prior analysis is an assessment of the risk associated with different decisions; it is commonly used for comparing the risks corresponding to different decisions. Posterior decision analysis differs from prior analysis by considering possible changes in the branching probabilities and/or the consequences due to risk reducing measures, risk mitigating

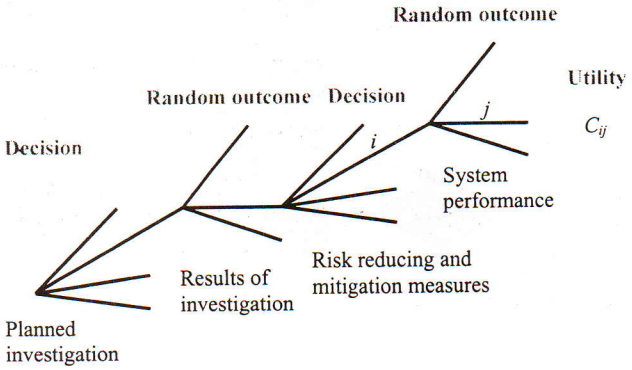

Fig. 2: Decision tree for pre-posterior decision analysis

measures and collection of additional information. Posterior decision analysis may be used to evaluate different additional activities affecting the total risk.

Another important modification of the described approaches, known as pre-posterior decision analysis, may be illustrated by the decision tree shown in Fig. 2. The aim of pre-posterior decision analysis is to identify the optimal decisions with regard to activities that may be performed in the future, e.g., planning of risk reducing activities and/or collection of new information. An important pre-requisite for pre-posterior decision analysis is consideration of future actions that may be applied taking into account the results of the planned activities.

6 Bayesian network

Bayesian networks or influence diagrams (Bayesian networks supplemented by utility nodes) [12, 13] provide an important generalization of various decision trees. The main features of this method are illustrated by the following two examples. Fig. 3 shows a simplified network extracted from influence diagrams developed for risk analysis of buildings under a fire design situation [14, 15, 16]. The network consists of seven chance nodes numbered 1, 2, 3, 4, 5, 12 and 14, four decision nodes 6, 7, 15 and 16, and six utility nodes 8, 9, 10, 11, 13 and 17. The utility nodes represent the costs of various fire safety measures (nodes 8, 10, 17), damage to the building (nodes 9, 11), and injuries (node 13).

Nodes are interconnected by directional arrows indicating causal links between parent and children nodes. All the causal links must, however, be described by appropriate input data (conditional probabilities or utility units) linked to assumed states of the nodes. For example the utility nodes (except utility node 13) are directly dependent on the size of a building (node 15). Utility node 13, describing the cost of injury, is affected by the size of the building through the number of endangered persons represented by chance node 14. This data is sometimes difficult to specify, and expert judgement often has to be used.

Chance nodes 1, 2, 3, 4, 5, 12 and 14 represent alternative random variables having two or more states. The node 1-Situation describes the probability of fire start $p_{\mathrm{fi,s}} = \mathrm{P}(H_2)$ and the complementary probability $1 - p_{\mathrm{fi,s}}$ of normal situation H_1. Chance node 2-Sprinklers describes the functioning of sprinklers provided that the decision (node 6) is positive; the probability of the active state of the sprinklers given at fire start is assumed to be very high, for example 0.999. Chance node 3-Flashover has two states: the design situation H_3 (fire design situation without flashover) and H_4 (fire design situation with flashover when the fire is fully developed).

If sprinklers are installed, the flashover in a compartment of 250 m^2 has the positive state with the conditional probability 0.002; if sprinklers are not installed then $P\{H_4|H_2\} = 0.066$ [14, 15, 16]. It is assumed that with probabilities equal to squares of the above values the fire will flash over the whole building, thus the values 0.000004 and 0.0044 are considered for chance node 3. Chance node 4–Protection (introduced for formal computational reasons) has identical states as decision node 7–Protection. Chance node 5–Collapse represents structural failure that is described by the probability distribution linked to three children nodes (1, 3, 4). This situation can hardly be modelled using a decision tree. Note that the probability of collapse in the case of fire but not flashover may be smaller than in a persistent situation, due to the lower imposed load.

In order to describe the basic principle of probability calculation used when analysing Bayesian networks, consider the fundamental task indicated in Fig. 4. The simple example in Fig. 4 is taken out of the diagram shown in Fig. 3. One child node D (Node 1 – Fire flashover) is dependent on two parent

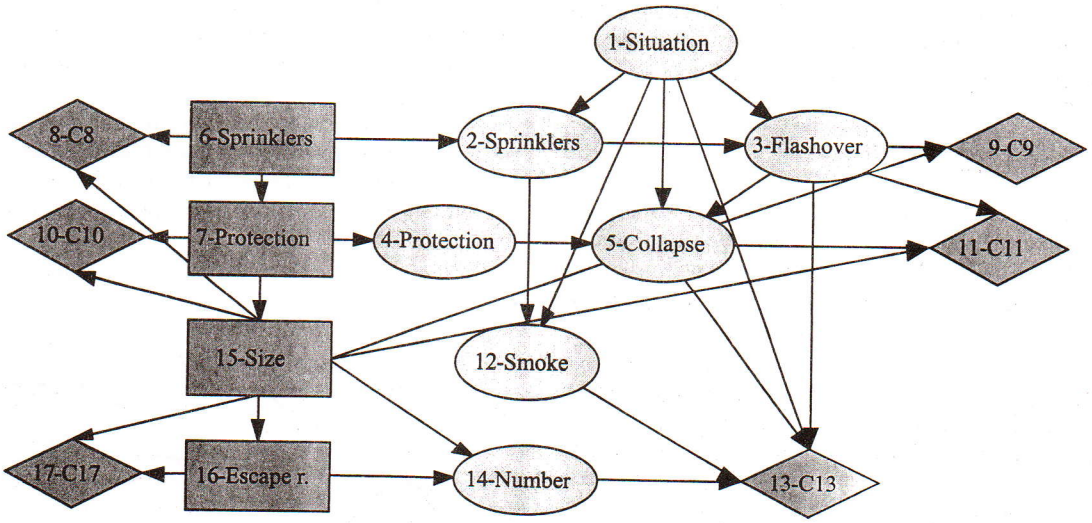

Fig. 3: Bayesian network describing a structure under normal and fire design situations

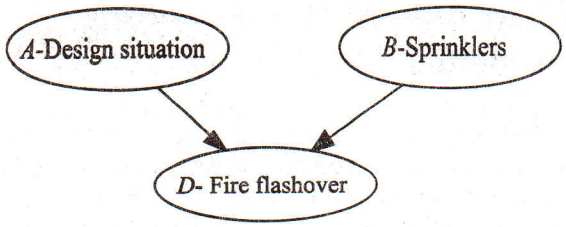

Fig. 4: A fundamental case of a Bayesian network

nodes: A (Node 1 Design situation) and B (Node 2 Sprinklers), each of them having a number of discrete states A_i and B_j.

If the children nodes A and B have a discrete state A_i and B_j then the probability of event D_k (a particular state of node D) is given by the formula

$$P(D_k) = \sum P(D_k|A_iB_j)\,P(A_i)\,P(B_j)\,. \qquad (4)$$

In addition to the general relationships (2) and (3), equation (4) represent the fundamental theoretical tool for analyzing Bayesian network or influence diagrams. The input data consists of the conditional probabilities $P(D_k|A_iB_j)$, which are sometimes difficult to specify.

Another example of an influence diagram recently used for risk analysis of tunnel routes in Prague is indicated in Fig. 5 (unpublished study of the author). It shows the most important nodes describing safety in tunnels. It contains six decision nodes representing important factors (1 to 6), seven chance nodes (7 to 13) and six utility nodes (14 to 19). Arrows indicating causal links connect relevant nodes. All the causal links must again be characterized by appropriate input data.

It is interesting to note that in this case the network includes six decision nodes describing important factors affecting the safety of a tunnel, which might be adjusted at the design stage. The utility nodes represent the economic factors and adverse consequences (nodes 14 to 19).

A more detailed description of the nodes is provided by the following list, which also indicates difficulties in input data specification.

Decision nodes (1 to 6)

1. **Structure**. The decision node describes the structural arrangement of the tunnel (length, slope, number of lanes, etc.), which might be adjusted at the design stage.
2. **Traffic**. Describes the traffic arrangements in the tunnel (curves, ingoing and outgoing lanes) that are alternatively considered in the design.
3. **E_routes**. Describes the distance of the escape routes and their capacity that are considered in the design.
4. **F-safety**. Describes extent of fire safety measures applied in the tunnel, which may be adjusted in the design.
5. **Ventilation**. Describes the probability that the ventilation system applied in the tunnel will actually be functioning.
6. **T_equipm**. Describes the extent of the technological equipment that is activated in case of an accident.

Chance nodes (7 to 13)

7. **N_accid**. This chance node describes the number of accidents per year.
8. **N_pers**. Describes the number of persons endangered during traffic accidents in the tunnel.
9. **F_starts**. Describes the probability that a fire will start.
10. **Function**. Describes the efficiency of the fire safety equipment.
11. **Fire**. Describes the probability of a fully developed fire.
12. **Function**. Describes the efficiency of the ventilation system.

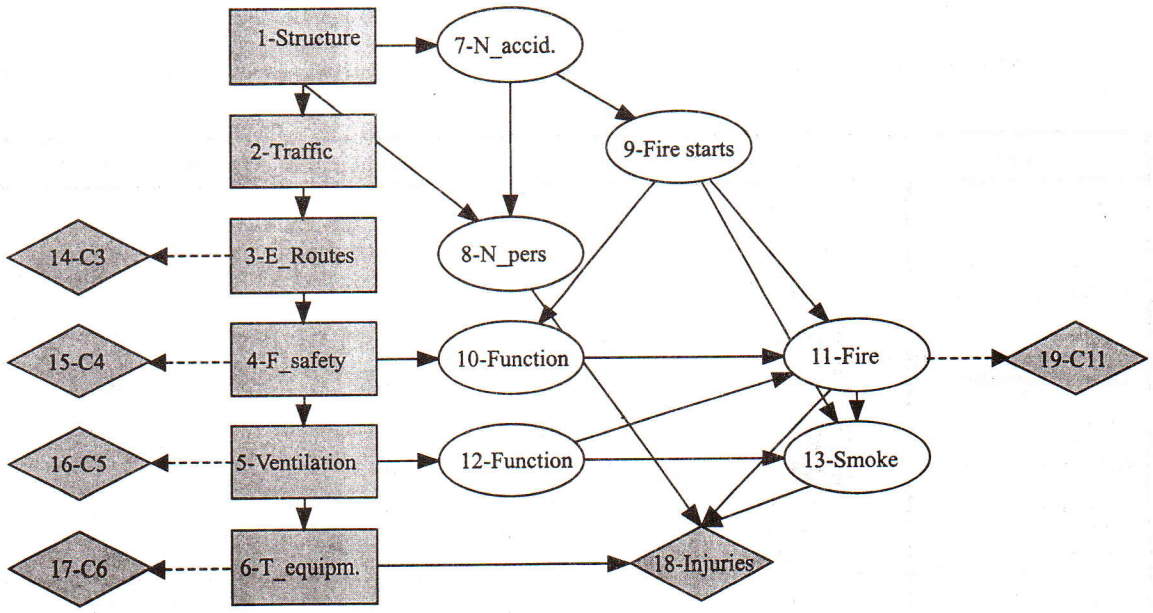

Fig. 5: Bayesian network for risk analysis in tunnels

13. **Smoke.** Describes the intensity of smoke developed in the tunnel.

Utility nodes (14 to 19)

14. **C3.** Cost of the decision described in node 3.
15. **C4.** Cost of the decision described in node 4.
16. **C5.** Cost of the decision described in node 5.
17. **C6.** Cost of the decision described in node 6.
18. Injuries. Cost due to injuries.
19. **C11.** Cost of a fully developed fire.

Probabilistic and risk analysis is very similar to that described in detail above for the case of a fire situation. Without going into technical details Fig. 5 shows the effect of the ventilation system and technological equipment on the expected risk of one tunnel in the city route circle in Prague, taking into account fatal injuries only.

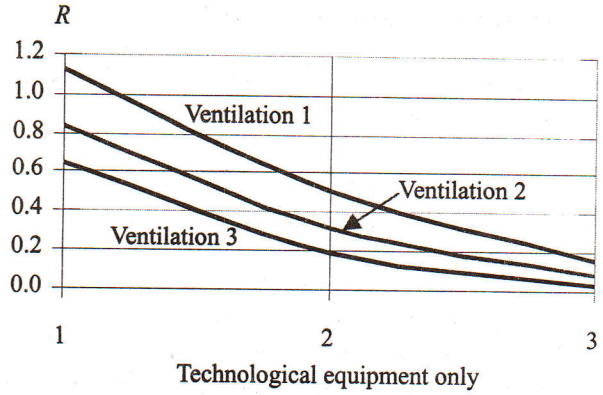

Fig. 6: Effect of ventilation level and technological equipment on expected risk in a tunnel

7 The implied cost of averting a fatality

The utility nodes may generally describe economic as well as social and environmental costs [17, 18, 19]. In order compare all possible damages it is necessary to express all consequences in terms of a single unit. This seems to be an extremely difficult task. Table 1 indicates that the cost of one life is estimated to about 1 to 3 million of USD (data presented in [19]). The so-called Implied Cost of Averting a Fatality *ICAF* can be expressed as

$$ICAF(\Delta e) = g\left(1-\left(1+\frac{\Delta e}{e}\right)^{1-\frac{1}{w}}\right)\Delta e\,, \qquad (5)$$

where symbols g, e and w are defined in Table 1. However, the data indicated in Table 1 remains a subject for further investigation and should be considered as indicative values only.

8 Criteria for social risks

An important question concerning risk assessment is what happens when we compare obtained results with acceptable limits. The criteria for social limits shown in Fig. 7 are taken from [8].

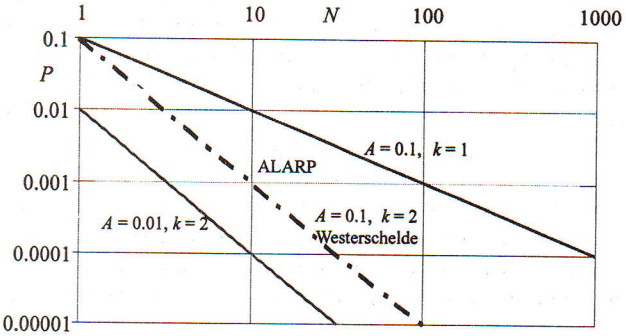

Fig. 7: Acceptable level of social risks

Table 1: The Implied Cost of Averting a Fatality – ICAF(Δe), financial data in PPP US$ (1999) obtained from UN-HDR 2001, World Bank

Country	g - annual income	e - life time	$2w$ - working part of e	ICAF(Δe) [$\times 10^6$]
US	34000	77	0.15	2.6
Japan	26000	81	0.15	2.1
Germany	25000	77	0.125	1.9
UK	22000	77	0.125	1.7
Czech Republic	**8000**	**75**	**0.15**	**0.6**
Mexico	8800	72	0.15	0.6
South Africa	9100	55	0.15	0.5
Colombia	5900	70	0.15	0.4
China	3900	70	0.15	0.3
India	2400	63	0.15	0.1
Nigeria	800	47	0.18	0.04

International standard ISO 2394 (1998) provides a limit for an individual risk of fatal injury per year by the value 10^{-6}. If there are more endangered persons in one accident, the acceptable risk is usually expressed [8] as

$$P(R > N) < A\, N^{-k}, \qquad (6)$$

where R is the assessed risk (number of fatal injuries), N denotes the acceptable number of fatal injuries, and A and k are suitable parameters. Fig. 5 shows three variants of these criteria:

- upper bound for $A = 0.1$ and $k = 1$,
- middle level for $A = 0.1$ and $k = 2$,
- lower bound for $A = 0.01$ and $k = 2$.

The upper bound indicates the uttermost (most benevolent) acceptable limit, while the lower (more severe) bound shows generally acceptable limits. The region between the lower and upper limits is often denoted by the known abbreviation ALARP (As Low As Reasonably Possible). If the assessed values are within the ALARP region, it is recommended to decrease the assessed risk as much as possible. It is interesting to note that the middle level of the limit for $A = 0.1$ and $k = 2$ (indicated in Fig. 7 by the dashed and dotted line) has been accepted as an accepted risk level for the road tunnel in Westerschelde in the Netherlands [8].

It should be emphasized that the above-described criteria include casualties (social consequences) only and do not consider any other (economic or political) consequences. Combination of different type of adverse consequences remain an open question.

9 Concluding remarks

Traditional approaches to engineering design of civil engineering structures and other technical systems are frequently based on the concept of target probability. This fundamental quantity is usually based on comparative studies and past experience only. Moreover, probabilistic design methods suffer from several deficiencies, including lack of consideration for accidental and other hazard situations. However, more and more frequently both these extreme conditions are becoming the causes of serious failures and other adverse events. For this reason, the specification of the target probability of failure remains an open question (how safe is safe enough?).

The most important contribution of risk analysis and assessment consists in systematic consideration of various consequences. Several techniques are available at present: decision trees, the Bayesian belief networks and influence diagrams. Available experience indicates that the Bayesian belief networks provide a transparent, logical and effective tool for analysing engineering systems. It should however be underlined that any analysis of an engineering system is always dependent on assumed input data, often of a very uncertain nature. The input data should be estimated with due regard to the specific technological and economic conditions of a given system. In particular, the economic , social and environmental consequences of adverse events should be further investigated.

It appears that methods of risk analysis and assessment may significantly contribute to further improvement of current engineering design. The remarkable fact that the public is better prepared to accept certain risks than to stand for specified probabilities of failure will make the application of risk assessment easier. It is therefore anticipated that in the near future probabilistic methods in engineering will be supplemented by criteria for acceptable risks.

Acknowledgement

This research has been conducted at the Klokner Institute of the Czech Technical University in Prague, as a part of research project CEZ: J04/98/210000029 "Risk Engineering and Reliability of Technical Systems".

References

[1] EN 1990. 2002: *Basis of Structural Design*. (Transformation ENV 1991-1, 1994) Brussels, 2002.

[2] EN 1991-1-2. 2002: *Actions on Structures Part 1–2, General Actions – Action on Structures Exposed to Fire*. (Transformation of ENV 1991-2-2: 1995), Brussels, 2002.

[3] ISO 2394: *General Principles on Reliability for Structures*. ISO, Geneva, 1998.

[4] Ellingwood, B. R.: *Probability-Based Structural Design: Prospect for Acceptable Risk Bases*. Application of Statistics and Probability. Icasp 8. Balkema Rotterdam, 1999, p. 11–18.

[5] Melchers, R. E.: *Structural Reliability Analysis and Prediction*. Chichester: John Wiley & Sons, 1999, p. 437.

[6] Steward, M. S., Melchers, R. E.: *Probabilistic Risk Assessment of Engineering System*. London: Chapman & Hall, 1997, p. 274.

[7] Holický, M., Schneider, J.: *Structural Design and Reliability Benchmark Study*; Safety, Risk and Reliability – Trends in Engineering; Zürich: IABSE, 2001, p. 929–938.

[8] Holický, M.: *Prospects For Advanced Engineering Design Based On Risk Assessment*. Acta Polytechnica, Vol. 41, No. 4–5, 2001, p. 8–12.

[9] Vrouwenvelder, A., Holicky, M., Tanner, C. P., Lovegrove, D. R., Canisius, E. G.: *Risk Assessment and Risk Communication in Civil Engineering*. CIB Report. Publication 259, Rotterdam, 2001.

[10] Holický, M.: *Fuzzy Probabilistic Optimisation of Building Performance*. Automation in Construction, Vol. 8, No. 4, 1999, p. 437–443.

[11] Ang, A. H-S., Tang, W. H.: *Probabilistic Concepts in Engineering Planning and Design*. Volume I - Basic Principles. London: John Wiley, 1975, p. 409.

[12] Jensen, Finn V. (1999): *Introduction to Bayesian Networks*. Aalborg University, Denmark, 1996.

[13] Hugin System: *Version 5.7, Professional*. Hugin Expert A/S, Niels Jernes Vej 10, DK-9220 Aalborg, Denmark, 2001.

[14] Holický, M., Schleich, J.-B.: *Probabilistic Risk Analysis of a Structure in Normal and Fire Situation Including Life Safety*. ICOSSAR 2001, Newport Beach (USA): A. A. Balkema Publishers, 2001, p. 127.

[15] Holický, M., Schleich, J.-B.: *Modelling of a Structure under Permanent and Fire Design Situation*. Proc. of Safety, Risk and Reliability – Trends in Engineering. International

Conference, Malta, 21/23.3.01, Rotterdam: A. A. Balkema Publishers, 2001, p. 789–794.

[16] Holický, M.: *Risk Assessment of Steel Buildings and Occupants under Fire Situation*. ICASP 9, Berkeley, 2003, to be published.

[17] Lewis, R.: *The Public Perception of Risk*. RSA Journal, November 1995, p. 52–63.

[18] Schneider, J.: *Safety – A Matter of Risk, Cost and Consensus*. Structural Engineering International, No. 4, November 2000, p. 266–269.

[19] Rackwitz, R.: *New LQI-developments*. JCSS Workshop on Reliability Based Calibration, Zürich, 2002.

Prof. Ing. Milan Holický, DrSc.
phone: +420 224 353 842
e-mail: holicky@vc.cvut.cz

Czech Technical University in Prague
Klokner Institute
Šolínova 7
166 08 Prague 6, Czech Republic