Available online at www.sciencedirect.com

SCIENCE DIRECT®

ELSEVIER

Reliability Engineering and System Safety 80 (2003) 173–184

RELIABILITY ENGINEERING & SYSTEM SAFETY

www.elsevier.com/locate/ress

Risk assessment for civil engineering facilities: critical overview and discussion

M.H. Faber[a,*], M.G. Stewart[b]

[a]Risk and Safety Group, Institut für Baustatik und Konstruktion, ETH-Hönggerberg, HIL E 32.3, CH-8093 Zurich, Switzerland
[b]Centre for Infrastructure Performance and Reliability, The University of Newcastle, Newcastle, NSW 2308, Australia

Received 28 March 2002; revised 24 July 2002; accepted 3 January 2003

Abstract

The present paper should be seen as a basis for discussion of important aspects of risk analysis and assessment, as well as attempting to describe risk assessment in accordance with the present state of the art. Risk assessment is thus presented in an overview form from the viewpoint of being a means for decision-making and thus within the formal framework of decision theory. First the motivation for risk analysis is given and the theoretical basis together with the practical aspects, methodologies and techniques for the implementation of risk assessment in civil engineering applications are explained and discussed. The paper furthermore addresses the problems associated with risk acceptance criteria, risk aversion and value of human life and attempts to provide suggestions for the rational treatment of these aspects. Finally a number of problem areas are highlighted and the needs for further education, research and dissemination are stressed.

Keywords: Risk; Risk analysis; Decision theory; Uncertainty; Probability; Consequences; Risk averseness; Risk acceptance; Optimality

1. Introduction

During the last decade there has been an increasing societal concern on sustainable developments focusing on the conservation of the environment, the welfare and safety of the individual and at the same time the optimal allocation of available natural and financial resources. As a consequence the methods of risk and reliability analysis in civil engineering, mainly developed during the last three decades, are increasingly gaining importance as decision support tools in civil engineering applications. However, their value in connection with the quantification and documentation of risks and the planning of risk reducing and mitigating measures is not fully appreciated in the civil engineering profession at large, although it is in some specialist areas and interest in risk management, asset management, etc. is increasing rapidly. Risk and reliability analysis is in fact a multidisciplinary engineering field requiring a solid foundation in one or several classical civil engineering disciplines in addition to a thorough understanding of probability, risk analysis and decision analysis. There are no signs that the focus on risks will decrease in the future. The future development and the preservation and maintenance of the infrastructure of society will even more likely demand an intensified focus on risk.

As a consequence of the tremendous demand for risk-based decision analysis in engineering applications and an apparent lack of recognition of risk analysis as a distinct discipline, a rather broad range of practices for risk analysis has developed through the years. Practical experience as well as several benchmark studies has clearly shown that risk analysis may in reality stand for very different things depending on the 'professionals' performing the analysis and the clients requesting them. This situation is not a satisfactory one and the risk engineering profession should make an effort to define risk analysis, to identify a best engineering practice for risk analysis and furthermore to set up an framework for the categorisation and standardisation of risk analysis.

The present paper attempts to provide a critical overview and discussion of risk analysis in general but with a view to the special problems arising in civil engineering facilities in particular. Emphasis is given to the need of establishing a formal basis for risk analysis taking into account decision

[*] Corresponding author.
E-mail address: michael.faber@ethz.ch (M.H. Faber).

0951-8320/03/$ - see front matter © 2003 Elsevier Science Ltd. All rights reserved.
doi:10.1016/S0951-8320(03)00027-9

theory and to identify and discuss the various shortcomings from this point of view.

2. The definition of risk

Risk is a rather commonly used notion and is used interchangeably with words like chance, likelihood and probability to indicate that we are uncertain about the state of the item, issue or activity under discussion. However, even though we may understand from the context of discussion what is meant by the different words it is necessary in the context of engineering decision making that we are precise and consistent in our understanding of risk (e.g. Elms [29]).

As we shall see later, technical risk is typically defined as the expected consequences associated with a given activity. Considering an activity with only one event with potential consequences risk R is thus the probability that this event will occur P multiplied with the consequences given the event occurs C, i.e.

$$R = P \times C \tag{1}$$

This definition is consistent with the interpretation of risk used in the insurance industry (expected losses) and risk may, e.g. be given in terms of EUROs, dollars, the number of human fatalities, exposure limits to toxic substances, etc. However, the definition, analysis, treatment and regulatory requirements of 'risk', as well as the associated nomenclature, have evolved for different civil engineering disciplines, although the underlying theoretical and philosophical frameworks are similar.

3. The practical implementation of risk analysis

3.1. Overview

Risk analyses may be represented in a generic format, which is largely independent from the application or whether the risk analysis is performed in order to document that the risks associated with a given activity are acceptable or is performed to serve as a basis for a management decision. Fig. 1 shows a generic representation of a risk analysis, in this case, a flow chart based on the Australia/New Zealand code on Risk Management [1]. Clearly, Fig. 1 shows that a risk analysis is not a 'one-off' process, but one that may well require regular monitoring and review due to changes in system needs, increased operating experience, accidents and other new information relevant to system performance. The individual steps in the flow chart are described in Stewart and Melchers [2].

3.2. Hazard identification

One of the first tasks in risk analysis of civil engineering facilities is to identify the potential hazards, i.e. the sources of risk. This process plays a crucial part of the risk analysis due to the fact that only the identified potential hazards, which are subjectively and objectively known, can be taken into account. If all the relevant hazards are not identified then the risk analysis will result in biased decision-making, which in general will be cost inefficient and ultimately could lead to unacceptably high risks to people and the environment.

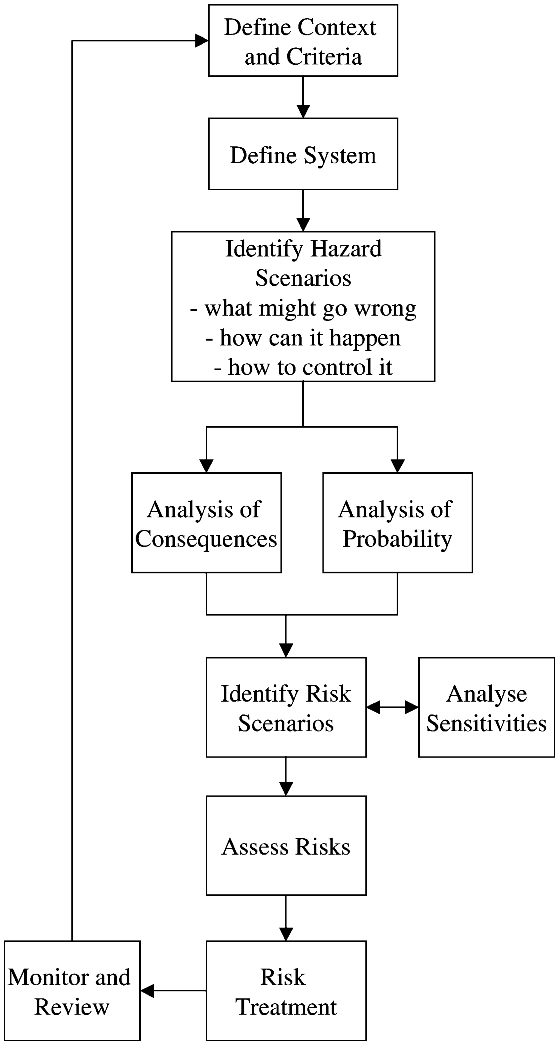

Fig. 1. Generic representation of the flow of risk-based decision analysis.

Different techniques for hazard identification have developed from various engineering application areas such as the chemical, nuclear power and aeronautical industries. See e.g. Stewart and Melchers [2] for a comprehensive review. Among these are

- Preliminary Hazard Analysis (PHA)
- Failure Mode and Effect Analysis (FMEA)
- Failure Mode Effect and Criticality Analysis (FMECA)
- Hazard and Operability Studies (HAZOP)
- Risk Screening (Hazid sessions)

A complementary approach is that hazards may also be identified on the basis of past experience as reported in so-called incident data banks containing a systematic documentation of events leading to or almost leading to (near misses) system failure.

A large proportion of failures of civil engineering facilities are due to human error (e.g. Hauser [3], Eldukair and Ayyub [4], Stewart [5]) yet hazard scenarios for many civil engineering facilities ignore the influence of human error, in design, construction, use or maintenance. The main exceptions being the operation of nuclear power plants, offshore platforms, ships and chemical process plants (i.e. operator errors). This casts some doubt over the utility of risk analyses, particularly if the risk analysis is the only method to ensure system safety.

3.3. Logic tree analysis

Having identified the different sources of risk for an engineering system and analysed these in respect to their chronological and causal components, logic trees may be formulated and used for the further analysis of the overall risk as well as for the assessment of the risk contribution from the individual components. Seen in relation to the theoretical formulation of risk analysis described later the analysis of logic trees provides the tools for assessing the various branching probabilities in the event decision trees as well as the corresponding consequences.

The current practice in risk analysis is to use the following types of logic trees (e.g. Lee et al. [30]; Villemeur [31]:

- Fault trees
- Event trees
- Cause/consequence charts

Due to the fact that fault trees cannot directly accommodate dependent basic events they are not appropriate for the assessment of probabilities of scenarios involving so-called common cause failures. For civil engineering applications this limitation is a serious one as dependency is a common feature rather than the exception for the events contributing to the risks. In principle, event-trees can deal with such dependencies; however in practice, this requires great care during event-tree construction. This limitation is, however, not present for Bayesian Probabilistic Nets, which seem to be a very promising tool for risk analyses in general, see e.g. Jensen [40], Faber et al. [6], Faber [7] and Friis-Hansen [8]. Considering the analysis of hazards for structural systems the methods of structural systems reliability theory may be applied, see e.g. Ditlevsen and Madsen [9]. These methods have been developed specifically to take into account the effect of dependency between the events ultimately leading to system failure.

The integral analysis of hazard scenarios involving the combined effect of human errors, failure of technical systems such as pumps and valves and failures of structural components and systems is an area where more progress is needed before a consistent basis for risk analysis is achieved. Whereas the methodological basis for such analysis might be found in the application of modern risk analysis tools (e.g. Bayesian Probabilistic Networks) more problems are related to the choice of detail in the representation of the hazard scenarios as well to the matter of standardization in regard to the uncertainty modelling.

3.4. Uncertainty modelling

Risk analyses are typically made on the basis of information, which at least partly is subject to uncertainty or just incomplete. In fact the variables influencing a decision/risk analysis may be subject to several sources of uncertainty; these can be broadly categorized as

- Inherent or natural variability of the phenomenon itself (aleatory or type 1 uncertainty).
- Modelling uncertainty: (i) uncertainty as to whether all factors that influence the model are included, or (ii) uncertainty in how the model describes the relationship between these factors (epistemological or type 2 uncertainty).
- Statistical uncertainty (epistemological or type 2 uncertainty).

It is likely that modelling and statistical parameter uncertainties will be reduced as the understanding of the variable increases, e.g. through the collection and analysis of additional data and the development of improved predictive models. However, future events are not always directly related to historical data and difficulties may be encountered when trying to predict the occurrence of events beyond this data range.

The sources of uncertainty, even for the same facility, are very dependent on the purpose of the risk analysis. For example, for design of a new facility the uncertainties may be based on analysis of historical data (i.e. past experience) covering a range of existing facilities. However, these predicted uncertainties may fail to capture the actual uncertainties of this new 'as built' facility (e.g. the quality of concrete or the operating environment might be different from that predicted). Thus, a posterior risk analysis will provide for more accurate results.

The reference period of the risk-decision analysis is also very important when modelling stochastic or non-stationary processes. For example, it is often assumed that an ergodic stochastic process may model the occurrence of events; however, the influence of long-term or other effects (e.g. El Nino phenomenon) may also need to be considered. Further, uncertainties for short reference periods might appear reasonable but when predictive models are extrapolated for long reference periods then uncertainties can easily propagate and increase to possibly unrealistic levels. Such a situation might occur, for instance, in the stochastic modelling of deterioration processes where the accuracy of long-term predictions may be limited, see e.g. Stewart [10].

Finally, in many cases it is not possible to include all sources of uncertainty in the probabilistic models used in a risk analysis. These sources of uncertainty are essentially non-quantifiable and are normally associated with say bias of analysts preferences for particular probability models, expertise of system representation study team, inclusion of all failure events, human error, unforeseen modes of failure, etc. Nonetheless, 'best practice' requires that quality assurance measures and peer reviews be conducted so as to enhance the credibility and accuracy of the analysis by ameliorating these and other sources of uncertainty. The widespread adoption of the JCSS Probabilistic Model Code [11] or other standardized probabilistic guidelines or databases would also greatly reduce the scope for analyst-to-analyst variability, again leading to more credible risk analyses.

3.5. Evaluation of risk

The simplest form of risk analysis is the so-called prior-analysis. In the prior-analysis the risk (expected utility) is evaluated on the basis of statistical information and probabilistic modelling available prior to any decision and/or activity. In practice, this would typically occur for the design of new facilities. A simple decision tree in Fig. 2 illustrates the prior analysis. In a prior analysis the risk (expected utility) for each possible activity/option is evaluated as

$$R = E[U] = \sum_{i=1}^{n} P_i C_i \tag{2}$$

where R is the risk, U the utility, P_i is the ith branching probability and C_i the consequence of the event of branch i.

A posterior analysis is in principle of the same form as the prior analysis, however, changes in the branching probabilities and/or the consequences in the decision tree reflect that the considered problem has been changed as an effect of risk reducing measures, risk mitigating measures and/or collection of additional information. A posterior analysis may thus be used to evaluate the effect of activities, which factually have been performed (e.g. Diamantidis [39]). For example, for assessment of existing facilities the testing and inspection of the 'as built' facility would be expected to reveal many gross design and construction errors, leading to a more accurate reliability analysis.

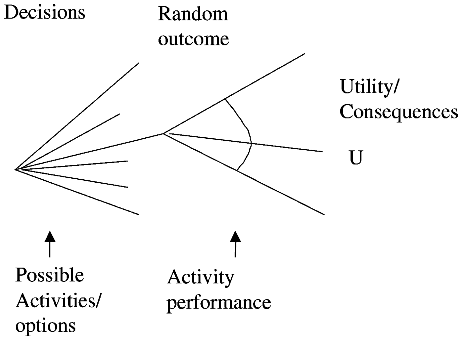

Fig. 2. Decision tree for prior and posterior decision analysis.

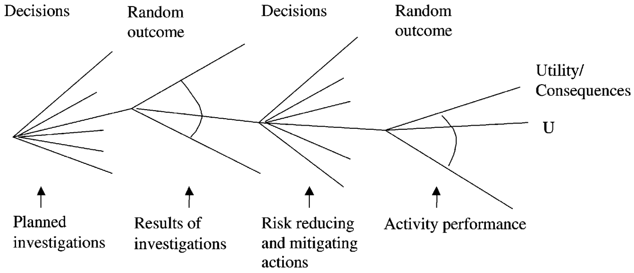

Fig. 3. Decision tree for pre-posterior decision analysis.

A pre-posterior analysis [41] may be illustrated by the decision tree shown in Fig. 3. Using pre-posterior analysis optimal decisions in regard to activities, which may be performed in the future, e.g. the planning of risk reducing activities and/or collection of information may be identified. An important prerequisite for pre-posterior analysis is that decision rules need to be formulated specifying the future actions which will be taken on the basis of the results of the planned activities. Pre-posterior analyses form a strong decision support tool and have been intensively used for the purpose of risk based inspection planning, see e.g. Faber et al. [12]. However, so far pre-posterior decision analysis has been grossly overlooked in risk assessments.

It is important to note that the probabilities for the different events represented in the prior or posterior decision analyses may be assessed by logic tree analysis, classical reliability analysis and structural reliability analysis or any combination of these. The risk analysis thus in effect includes all these aspects of systems and component modelling in addition to providing the framework for the decision-making. The following sections will now discuss the two components needed for the evaluation of risk: analysis of consequences and analysis of probabilities.

3.5.1. Analysis of consequences

The consequences of a failure event are generally measured in terms that directly affect people and their environment such as loss of life or injury and economic losses. Consequences of most contention are those that tend to result from catastrophic low probability/high consequence events. For example, Meyer [13] estimates that the consequences of core melt-down at a nuclear power plant may cause property damage of approximately $14 billion and over 48,000 deaths over a thirty year period (early and latent fatalities).

A major difficulty in estimating consequences is how to compare direct economic losses (building damage, production losses), indirect losses (user delay or inconvenience, impact on economic growth, unemployment) and non-monetary losses resulting from loss of life or injury, damage to the environment, social disruption, etc. The problem of establishing a common denominator for these different attributes is far from trivial. As an example it was for a long period of time not considered good practice to discuss—at least in public—the value of a human life. As a matter of fact several techniques have been developed to provide a means of comparing the different consequences of different activities by e.g. assessing the decision makers preferences in terms pair wise comparisons between different attributes. In the end of course this amounts to the same as establishing a common denominator for the considered consequences, a fact, which is often overlooked behind the complex numerical evaluations.

Various attempts have been made to quantify the economic value of a human life; these include (i) forgone earnings due to premature death—$450,000 [14]; (ii) 'value of a statistical life' (equal to $$D\cdot x$ where $$D$ is the amount an individual is prepared to pay to reduce their fatality risk by 1^{-x}, hence a group of x people would average one death less per year)—$1.6 to $8.5 million, see Fisher et al. [15]; (iii) money spent on government programmes per life saved—$100,000 for steering column protection to $90 million for asbestos removal [16]; or (iv) government compensation payable for death by accident. However, perhaps a more meaningful approach is to use a social indicator that reflects the quality of life in a society or group of individuals in terms of an individuals contribution to GNP, life expectancy, time for enjoyment of life, etc., such as the Human Development Index or Life Quality Index, Lind [17] and Nathwani et al. [18], which can be optimised to determine an acceptable implied cost of averting a fatality—$2 to $3 million, see Rackwitz [19].

Considering the enormous economic impact on society originating in political wishes related to the preservation of the environment, such as e.g. the decommissioning of offshore oil production facilities, cleaning of polluted ground water and exploitation of solar energy it is of utmost importance that a consistent framework be established, based on generally non-political values allowing for the quantification of environmental qualities. In the end this amounts to establishing the relations between environmental qualities and cost consequences or perhaps in terms of relations between the environmental qualities and the quality of life.

Traditionally, the emphasis on consequence modelling has been on the consequences of loss of safety, i.e. damages and loss of life or injury. However, recent work has begun to focus on the service life extension of existing facilities where the main concern is the high inspection, maintenance and repair costs necessary to keep ageing facilities functioning. In such cases, indirect costs such as those due to user delays or downtime may be considerable; for example, an analysis of cost data suggest that user delay and additional vehicle operating costs due to traffic diversions associated with closing a bridge for 5 days is approximately 25% of initial construction costs, see Ehlen [20].

The influence of time is an important consideration; benefits and costs seldom occur simultaneously. Future consequences may be discounted to represent equivalent current consequences. The standard measure of equivalent current consequences is the 'net present value' which uses a discount rate as the expected real rate of return (net of inflation) on future interest-bearing investments. Note that a high discount rate implies that the decision is generally not sensitive to long-term consequences (say over 30–40 years); in which case, the large uncertainty of long-term predictions expected with some risk analyses may not be an important consideration in decision analyses.

3.5.2. Analysis of probabilities

Classical reliability theory was developed for systems consisting of a large number of components of similar type under similar loading and for all practical matters statistically independent. This has found wide application in the aeronautical, nuclear, chemical, building and process industries. The theoretical basis for reliability analysis is thus the theory of probability and statistics developed for disciplines such as operations research, systems engineering and quality control. The probability of failure of such components can be interpreted in terms of relative failure frequencies observed from operational experience. Furthermore, due to the fact that failure develops as a direct consequence of an accumulating deterioration process the main focus was directed towards the formulation of probabilistic models for the estimation of the statistical characteristics of the time until component failure. Having formulated these models the observed relative failure frequencies can be applied as the basis for their calibration.

In structural and other demand-capacity reliability analyses the situation is fundamentally different due to the fact that structural failures are very rare and tend to occur as a consequence of an extreme event such as an extreme loading exceeding the load carrying capacity where the resistance might possibly be reduced due to deterioration such as corrosion or fatigue. In addition to this no useful information can be collected in regard to relative failure frequencies as almost all structural components and systems are unique either due to differences in the choice of material and geometry or by differences in the loading and exposure characteristics. When considering the estimation of failure probabilities for structural components it is thus necessary to establish probabilistic modelling of both the resistances and the loads and to estimate the probability of failure on the basis of these. In this process due account must then be given to the inclusion of all available spatial and temporal statistical information concerning the material, dimensional and other strength related properties and the load characteristics

3.5.2.1. Classical reliability analysis. As mentioned previously the classical reliability analysis was developed to estimate the statistical characteristics of the lives of technical components in order to be able to predict the characteristics, which are important for, the design and operation of systems build up by such components. These characteristics include the expected failure rate, the hazard function, the expected life and the mean time between failures, see e.g. Klaassen and van Peppen [32]. Modelling the considered system by means of logic trees where the individual components are represented by the decision nodes it is possible to evaluate various quantitative measures of performance such as the probability that a system will fail during a specified period, the positive effect of introducing redundancy into the system and its cost consequences or the effect of inspections and maintenance activities.

The failure rate for most technical systems is known as the bath-tub curve illustrated in Fig. 4 (e.g. Daniels [33]). The bath-tub curve is typical for many technical components where in the initial stages of the life the birth defects, production errors, etc. are a significant source of failure. When the component has survived a certain time it implies that birth defects were not present and the reliability increases. Thereafter a period of steady state performance occurs followed by ageing. For components exhibiting a constant failure rate function inspections are of little use since the component does not exhibit any degradation. However, for components with a slowly increasing failure rate function inspections may be useful and can be planned such that the failure rate does not exceed a certain critical level. If the failure rate function is at first quasi-constant and then followed by an abrupt increase inspections are also of little use, however, in this case a replacement strategy is more appropriate. The validity of the bath-tub curve to all types of components has been questioned widely and cannot be considered always to be valid (e.g. Lees [34]).

Clearly, Fig. 4 shows that the failure rate is not constant with time. In such cases, the time-dependent failure rate is known as the hazard function. This is a conditional failure rate defined as the probability that the component or system will fail at time t, given that the component or system has not failed prior to time t.

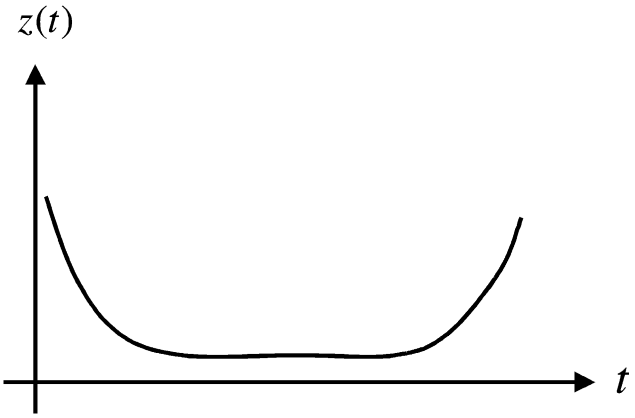

Fig. 4. The failure rate function—bath-tub curve.

An important issue is the assessment of failure rates on the basis of observations. As mentioned previously data on observed failure rates may be obtained from databanks of failures from different application areas. Care must be exercised when evaluating failure rates. If the components are not new in the beginning of the observation period the failure rates may be over estimated and if the observed interval is too short no observed failures may be present. For such cases different approaches to circumvent this problem may be found in the literature, see e.g. Lees [34]. Alternatively the failure rates may also be assessed by means of e.g. Maximum-Likelihood estimation where the parameters of the selected probability distribution function for the time till failure are estimated on the basis of observed times to failure.

Due to the lack of data and general uncertainties associated with the applicability of the available data failure rates may themselves be modelled as uncertain. The basis for the a priori assessment of the uncertainty associated with the failure rates may be established subjectively or preferably as a byproduct of the Maximum-Likelihood estimation of the distribution parameters of the probability distribution function for the time to failure. Having established an a priori model for the failure rate for a considered type of component another important issue is how to update this estimate when new or more relevant information about observed failures become available. In general, Bayes theorem is used to establish the a posterior probability density function for the failure rate [35].

3.5.2.2. Structural reliability analysis/demand-capacity reliability analysis. Concerning the reliability of structural components or other demand-capacity systems such as dams, pipelines, mechanical components, etc. the situation is different in comparison to that of e.g. electrical components; namely, failure events are very rare even for time intervals of many years and the mechanism behind individual failures are in most cases different. Structural failure predominantly occurs as a result of extreme events, such as extreme winds, avalanches, snowfall, earthquakes, or combinations hereof, rather than due to ageing or system degradation. However, other forms of ‘failure’ such as loss of functionality or lost production are increasingly sources of concern to asset owners, particularly for ageing or deteriorating civil engineering facilities.

For reliability analysis it is thus necessary to establish probabilistic models for loads and resistances including all available information about the statistical characteristics of the parameters influencing these. Such information might include data regarding the annual extreme wind speeds, experimental results of concrete compression strength, etc. Due to the fact that a significant part of the uncertainties influencing the probabilistic modelling of loads and resistances are due to lack of knowledge the failure probabilities, which may be assessed on this basis must be understood as nominal probabilities, i.e. not reflecting the true probability of failure for the considered structure but rather reflecting the uncertainty about the performance of the structure.

For a structural component for which the uncertain resistance R and load S are modelled by random variables with probability density functions $f_R(r)$ and $f_S(s)$, respectively, the probability of failure may be determined by

$$P_{\mathrm{f}} = P(R \leq S) = P(R - S \leq 0) = \int_{-\infty}^{\infty} F_R(x) f_S(x) \mathrm{d}x \quad (3)$$

assuming that the load and the resistance variables are statistically independent. The cumulative distribution function of resistance may also be termed a 'fragility curve'. A fragility curve is not dependent on load modelling and so helps separate and identify the effect of resistance and load uncertainty on a structural reliability calculation. This is particularly pertinent for systems with high load uncertainty and variability such as earthquakes, cyclones, floods, etc. (e.g. Ellingwood [36]).

In general, the resistance and the load cannot be described by only two random variables but rather by functions of random variables. Hence, a general formulation for the probability of failure may be determined through the following n-dimensional integral

$$P_{\mathrm{F}} = \int_{g(x) \leq 0} f_{\mathbf{x}}(\mathbf{x}) \mathrm{d}\mathbf{x} \quad (4)$$

where $f_{\mathbf{x}}(\mathbf{x})$ is the joint probability density function for the vector of basic random variables $\mathbf{X}$ and the integration is performed over the failure domain (e.g. Melchers [26]; Ditlevsen and Madsen [9]). The solution of the integral in Eq. (4) is by no means a trivial matter except for very special cases and in most practical applications numerical approximate approaches must be pursued. Practical methods for the approximate solution of Eq. (4) may be found in Ditlevsen and Madsen [9], STRUREL [21] and Proban [22]. A description of the basic principles of structural reliability theory may also be found in the JCSS Probabilistic Model Code [11].

3.6. Optimality and risk acceptance criteria

The decision-making process is a complex one, and one that is often entwined with political processes. A number of issues that risk assessment attempt to resolve include: "Who is to bear what level of risk, who is to benefit from risk-taking and who is to pay? Where is the line to be drawn between risks that are to be managed by the state, and those that are to be managed by individuals, groups or corporations? What information is required for 'rational' risk management and how should it be analysed? What actions make what difference to risk outcomes? Who evaluated success or failure in risk management and how? Who decides what should be the desired trade-off between different risks?" [23].

These matters are not easily resolved, are not for risk assessment to solve alone and are all related to risk acceptance criteria; namely, what risks are acceptable? The development and implementation of risk acceptance criteria involves:

- *perception of risk*: ensure that level of system risk is acceptable (or tolerable);
- *formal decision analysis*: analytical techniques to balance or compare risks against benefits (e.g. risk-cost-benefit analysis, life-cycle cost analysis); and/or
- *regulatory safety goals*: legislative and statutory framework for the development and enforcement of risk acceptance criteria.

The risk acceptance criteria generally adopted by the US Nuclear Regulatory Commission, UK Health and Safety Executive and other regulatory authorities is that risks and hazards should be 'As Low As Reasonably Possible' (ALARP) or 'As Low As Reasonably Attainable' (ALARA), e.g. Melchers [27] and Sharp et al [28]. The definition for such terms as 'low', 'reasonably', 'possible' and 'attainable' are highly subjective and prone to being interpreted in a conservative manner. Some attempts have been made to define this criteria in more tangible (and verifiable) terms-this often means in terms of risks, see Fig. 5.

3.6.1. Individual and societal risks

It is worthwhile to recognise that the problem concerning risk acceptance has a fundamental and philosophical bearing to the rights of human beings. The United Nations Office of the High Commissioner of Human Rights regulates the rights of humans by the 'Universal Declaration of Human Rights' UNOHCHR [24]. Here three of the relevant articles are given for easy reference.

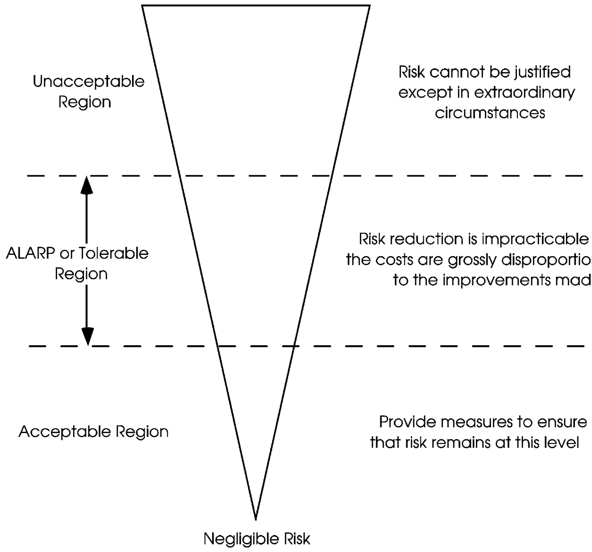
Unacceptable Region
Risk cannot be justified except in extraordinary circumstances
ALARP or Tolerable Region
Risk reduction is impracticable or the costs are grossly disproportionate to the improvements made
Acceptable Region
Provide measures to ensure that risk remains at this level
Negligible Risk

Fig. 5. Levels of Risk and ALARP (adapted from Ref. [27]).

> *Article 1.* All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood.
>
> *Article 3.* Everyone has the right to life, liberty and security of person.
>
> *Article 7.* All are equal before the law and are entitled without any discrimination to equal protection of the law. All are entitled to equal protection against any discrimination in violation of this Declaration and against any incitement to such discrimination.

The articles emphasises both the moral and legal obligation to consider all persons as being equal and furthermore underlines the rights to personal safety for all individuals. Therefore whatever criteria we formulate in regard to the acceptable risks we should always bear in mind that the abovementioned fundamental principles of these human rights are not violated thereby.

Safety has a cost—as we already know and shall discuss more in the following—therefore the level of safety to be guaranteed for the individual member of society is a societal decision with a strong bearing to what the society can afford. However, with reference to the 'Universal Declaration of Human Rights' representatives of society have a general moral obligation to consider all investments and expenditures in the light of the question 'could the resources have been better spent' in the attempt to meet the aim of this declaration.

When discussing the issue of 'acceptable risks' the issue is often confused by the fact that some individuals might have a different viewpoint to what is acceptable as compared to the viewpoint of the society. Each individual has their own perception of risk, or as expressed in decision theoretical terms, their own 'preferences'. Considering the acceptability of activities related to civil engineering or any other activities with possible implications to third parties for that matter the main question is not the preferences of the individual member of society but rather the preference of the society as expressed by the 'Universal Declaration of Human Rights' or some other generally agreed convention. It is important to appreciate the difference. The preferences of individuals may in fact be in gross contradiction with the preferences of society and it is necessary to view acceptability from a societal angle, yet at the same time ensuring that the basic human rights of individuals are safeguarded.

3.6.2. Societal risks and risk aversion

A distinction is often made between individual and societal risks. Individual risks are expressed in terms of fatalities per year, fatalities per year of exposure, etc., whilst societal risks are typically represented in terms of an $F-N$ curve which is a plot of cumulative frequency (F) of n or more fatalities versus number of fatalities (N). The ways that risk is presented can well affect risk perception. For example, an individual fatality risk of 10^{-5} is equivalent (in a statistical sense) to a societal risk of 10^{-8} of killing 1000 people. Yet, society seems more concerned about catastrophic events that harm large numbers of people rather than a series of lesser failure events that collectively harm a similar number of people. This preference is reflected in a typical $F-N$ curve, where for example Fig. 6 shows that an individual annual fatality risk of 10^{-4} has the same preference as an event killing 10 people with a frequency of 10^{-6} per year. This shows an increasingly risk-averse behaviour as the consequences increases; however, from a purely rational viewpoint this may be viewed as a somewhat illogical approach to increasing life-safety and it is severely doubtful if such an approach can lead to efficient and rational decisions. Despite the long tradition for using *FN*-diagrams in risk analysis it should be noted that these do not provide a consistent means for comparing the risks between different activities.

A rational basis for avoiding the introduction of risk aversion is readily available if it is recognised that the reason for being risk averse is that the events involving high consequences often are associated with 'follow-on' events which themselves may contribute significantly to the risk. The follow-on consequences for an offshore operator who in one event will lose an entire production facility with maybe a 100 fatalities are e.g. a significant loss of reputation leading to declining sales figures, expensive investigations of safety procedures by the authorities, reduced chances of obtaining new oil production concessions and reduced government/tax

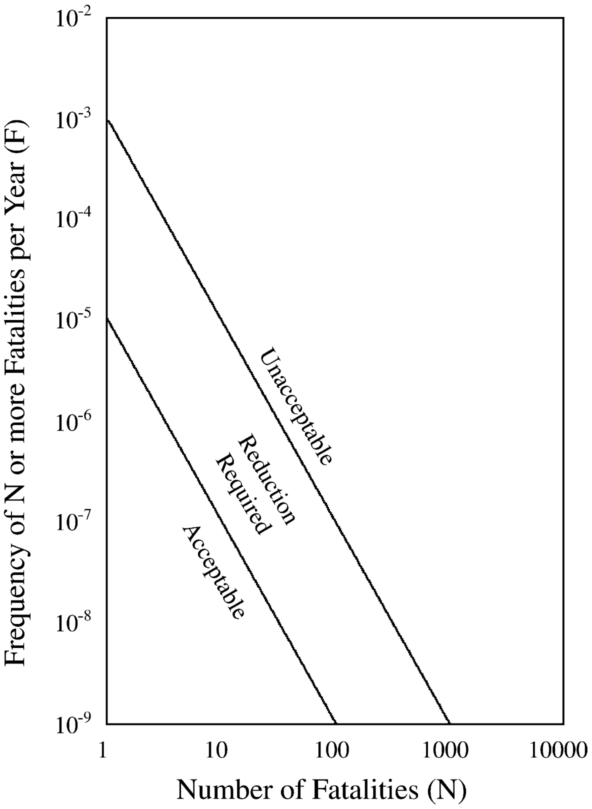

Fig. 6. Safety targets for societal risks in The Netherlands.

revenue. If all such ‘follow-on’ consequences are taken into account in the risk analysis then there is indeed no need to introduce any degree of risk averseness and the decision basis will be more transparent.

3.6.3. Multi-attribute and multi-objective risk-based decision analysis

Decision-making often leads to situations where different attributes need to be considered simultaneously, e.g. costs, loss of life, community disturbances and/or damages to the environment. Furthermore different interest groups may have different objectives or preferences and thus in effect value the combined effect of the attributes differently. Such situations are sometimes referred to as multi-attribute/multi-objective decision-making and represent a complex problem in risk analysis. Theoretically and methodically such problems might easily be treated within the framework of decision theory using multi-attribute/multi-objective decision-making techniques (e.g. Keeney and Raiffa [37]). However, it should be clearly understood that these techniques do not themselves provide any answer as to how the different attributes and/or different objectives should be weighted. This problem must be addressed regardless and there can be little chance of a rational approach if preferences between interested parties are irreconcilable. A fundamental necessity prior to the commissioning of any decision analysis is that the decision maker(s) are identified and that their preferences are assessed.

Care must always be taken to attempt to establish insight into the considered decision problems-the use of ‘black box’ decision tools may diverge the focus from this. It is also contentious converting some attributes to a common denominator that all interested parties could agree to, particularly when the values under consideration are subjective, e.g. converting noise disruption caused by a proposed heliport into monetary units. Ultimately, however, weighting preferences and establishing a common denominator present challenges to existing decision theory. What is of importance is that decision theory is more than just a ‘one-off’ numerical analysis, but should be a dynamic and transparent process involving on-going consultation with interested parties that may result in changes in preferences, trade-offs, new insights and hopefully at the end of such a process a decision that most interested parties can live with.

3.6.4. Optimisation of expected utility and the Life Quality Index

Formal or quantitative decision analyses provide decision-makers with analytical techniques to assess risk preferences; in particular, to compare or balance risks against benefits. A decision may therefore be based on activities that maximize expected monetary benefits, the expected utility or another index of performance such as the Life Quality Index, see e.g. Nathwani et al. [18].

A large variety of risk reduction measures may be considered for a particular activity. An example concerning risks to persons on offshore production facilities is gas detection systems, firewalls, sprinkler systems and separation of housing and production modules. Each of these risk reduction measures has its own efficiency. The question, however, remains how much should be invested in safety for a given activity. This question may be answered by a decision analysis by considering the expected total benefit associated with the considered activity $E[B]$

$$\begin{aligned} E[B] &= I(1 - P_F(C_R)) - C_R - C_F P_F(C_R) \\ &= I - C_R - (I + C_F)P_F(C_R) \end{aligned} \quad (5)$$

where I is the benefit from the activity, C_F is the cost consequence in case of failure, C_R is the cost of the risk reducing measures and where the probability of failure is a function of the costs invested in the risk reduction. The optimal investment in risk reducing measures may then be determined. Ultimately, however, decisions based on rational or formal analyses may be overruled (or at least delayed) by such political considerations as electoral pressure, national security implications, or lack of funds.

Losses from catastrophic system failure cannot always be remunerated from available corporate assets, insurance cover or even government resources. It is also likely that high consequence/low risk facilities could not operate if all costs were borne by the designers, owners and operators of the facility causing the risk. Accordingly, regulatory authorities have enacted liability limits for some facilities. For example, the liability of all nuclear plants for property damage and personal injury resulting from an accident (in the United States) is limited by the Price-Anderson Act to \$9.43 billion in 1998. Given that up to \$300 billion in damages could occur if core melt occurred at an existing nuclear power plant in the US it is readily apparent that this liability limit would not adequately compensate the victims of catastrophic system failure. Hence a significant proportion of expected losses, in the event of catastrophic system failure, will be borne by the victims and society as a whole, hence it appears that in some cases the benefits and risks will not be shared equitably.

Time is an important factor that may influence decisions since psychological studies show that the preferences of a decision-maker will increase with the postponement of adverse consequences. This is an important consideration when decision-makers consider the long-term consequences to future generations of a decision. Preferences may also change over time; for example, the public are more aware and concerned about environmental issues than two decades ago. Therefore, it is not unexpected that uncertainties will arise over future preferences.

3.6.5. Regulatory safety goals and calibration of acceptable risks

An alternative to using results from a risk analysis in a quantitative decision analyses is to use the results more directly for regulatory purposes. The safety goals (risk acceptance criteria) tend to be surrogates for the risks and hazards, which are considered to be acceptable (or tolerable) to society (see e.g. Paté-Cornell [25] and Stewart and Melchers [2]). This explains, in part, why most regulatory safety goals are legislated for potentially hazardous facilities as nuclear plants, offshore platforms, chemical process plants, waste facilities, transportation of hazardous goods, commercial aircraft and dams.

Risk acceptance criteria based on regulatory safety goals or analytical decision models tend to contain the inherent belief by analysts, decision-makers and the public that the calculated risks are actual risks. Clearly, this is a crucial assumption given that the precision of risk analyses is not necessarily high. This means that risks may have little objective meaning, except in a comparative or relative sense. It follows that a decision analysis such as a risk-cost-benefit or life-cycle cost analysis that sums actual (known) costs such as design or construction costs with predicted risks (expected costs or losses) may not be rational and so may produce decisions that are not optimal.

In some risk analyses it is possible to propagate uncertainties through the analysis so that the overall system risk can be represented in a probabilistic manner, such as a probability distribution or upper and lower confidence limits. This will help the decision-maker understand the variability and sensitivity of risk estimates, which would not be so obvious if results of a risk analysis were presented as single point estimates only. However, it is then unclear whether regulatory safety goals should be compared with the mean, median or some upper confidence limit of system risk. Some decision-makers may want to exercise 'prudent pessimism' by using an upper confidence limit of system risk resulting in the conservative use of risk acceptance criteria. Such an approach may not always be rational, but it does mean that the decision-maker needs to make a conscious decision and so the degree of conservatism is readily apparent.

The structural engineering profession is one of the few disciplines concerned with civil engineering facilities that are, in a sense, self-regulated with respect to public safety. With the exception of unusual, specialist or new technology structures, most structures are designed to codes developed to ensure that use of code-specified design equations will result in nominal probabilities of structural collapse that are (i) relatively constant for a range of structural materials and loading conditions and (ii) do not exceed a 'target' value of approximately 1×10^{-4} and 1×10^{-5} failures per year, see e.g. Melchers [26]. This process is termed 'calibration'. Probabilities of failure are termed 'nominal' because they are obtained from relatively simple methods, target values are derived from previously accepted technology and are used simply to compare one project against another. So no attempt is made to compare these 'nominal' risks with regulatory or societal based tolerable risk levels. Thus these probabilities of failure have no validity outside the framework in which they have been employed [27]. Such an approach also avoids the large uncertainties associated with modelling uncertainties.

3.6.6. Other considerations

Understandably, the focus on this paper has been on the quantification of risk and how this can be used as a decision-making tool. The knowledge of the system and its performance accrued during a risk analysis can also reveal new insights (in a qualitative sense) into system performance and how this might be improved. This is possible because a risk analysis generally incorporates a logical, systematic and rigorous approach to system modelling, leading to an increased understanding of system performance well before any quantitative results are available. This is an important observation because it is very easy to criticise risk analyses for their limitations, selection of data and models, uncertainties, bias, etc. As long as the purpose of a risk analysis is to understand system performance, and not a 'numbers game' such as used solely to satisfy quantitative risk acceptance criteria, then a risk analysis can be a very effective tool to improve system safety and performance.

4. Conclusions and discussions

Risk analysis is generic and thus the underlying principles and philosophy are identical and independent of the problem type-meaning that e.g. the optimal design of a power plant facility as a problem is very similar to that of asset management for the owner of 1000 bridges. This discussion paper has provided a brief overview of these principles, as well as highlighting and discussing the uncertainties and limitations of existing practices.

It would be comforting to believe that risk analysts are largely aware of these issues, and perhaps more importantly, convey this type of information to their clients who ultimately are the decision-makers. Experience suggests that this is not always the case. Hence, in broad terms, there is a need for increased understanding of risk analysis and that this understanding will need to be tailored for the following individuals or groups:

- Risk analysts—provide for better consistency in terms of methods, models and data so as to increase the credibility of risk analysis.
- Civil engineers—be capable of providing pertinent information to the risk analyst and critically review the outcomes of a risk analysis.
- Decision-makers (owners, government, community)—be informed about the rationality of their decisions and their impact on the interested parties.

The following conclusions and recommendations (in no particular order) are complementary and may be appropriate to one or more of the above individuals or groups:

1. There appears to be a significant proportion of engineers who are suspicious of risk analysis. Reasons cited might include “too difficult”, “too mathematical”, “can’t imagine such low frequencies”, “has little physical meaning”, etc. Some of these comments are simply ill-informed and might reflect the lack of exposure to probability theory and risk analysis in their formal engineering education. Traditionally, engineering courses have a strong emphasis on statistical theory (e.g. concrete quality, hydrology) but less on probability theory, which is more useful for predicting failure probabilities. More emphasis also needs to be placed on risk analysis and assessment and its relationship to code development, asset management, etc.
2. There is clearly a need for the adoption of standardised risk analysis techniques and probabilistic models as this will decrease analyst-to-analyst variability of outcomes. Significant analyst-to-analyst variability might well be perceived by engineers, decision-makers and the public to indicate an inexact and immature ‘science’ not capable to providing accurate predictions of risk.
3. It should be recognised that information used in a risk analysis should all be treated in the same manner. For example, a risk analysis must be able to accommodate judgemental and frequentistic information.
4. Human error is an important source of risk. Risk analyses incorporating human error (Human Reliability Analysis—e.g. Kirwan [38]) are restricted to errors that may be quantified but it is inherently difficult to include errors involving diagnosis, high-level decision-making or management of organisations. The omission of human error from a risk analysis results in the assumption that the design, construction and operation of facilities are ‘error-free’. Whether this is appropriate depends on the context of how the risk assessment results will be used. It may be acceptable, in some cases, if the risk analyst recommends quality assurance and control programmes for the civil engineering facility under consideration that will help ameliorate the incidence or consequences of human error.
5. Risk averseness is a matter treated with great inconsistency. If $F-N$ curves, ‘prudent pessimism’ or other risk adverse criteria is a characteristic of the risk assessment then this should be clearly stated when describing the risk acceptance criteria. This will lead to a more transparent decision-making process. However, it would be more rational to avoid risk adverse behaviour by considering ‘follow-on’ consequence modelling.
6. There is a general tendency and a long practice for letting the available and or preferred computational tools govern the type and usefulness of the performed risk analysis, i.e. standardisation has been strongly dominated by the available ‘traditional tools’. In principle standardisation is not a bad thing, however, focus should be directed more closely to the identification of the tools and where their use is appropriate.
7. At the present time and for sure in the years to come a large proportion of the available resources of society will continue or increasingly be spend on various activities aimed at preserving or benefiting the environment. Examples hereof are the decommissioning of obsolete structures and facilities, reduction of CO_2 emissions, exploitation of non-polluting energy and many others. These enormously important issues are presently being dealt with in a rather arbitrary manner governed by active interest groups and agenda driven politicians. Two important aspects should be noted in this context, namely that the decision basis for this kind of problem does not yet exist since we still have no commonly agreed and consistent measure by which we can value environmental qualities, and secondly that decisions of this kind are often performed on the basis of uninformed preferences. Important and difficult work still lies ahead.
8. Risk analyses involving worker or public safety or public resources should be subject to mandatory quality assurance and peer review. Quality assurance procedures can focus on the review of internal procedures and practices. Peer review should consist of an independent and critical review, conducted by recognised experts in risk analysis and assessment.

Acknowledgements

This paper is based on a shortened version of a discussion paper presented by the authors to the Joint Committee of Structural Safety. The full text of the JCSS discussion paper, which includes more extensive discussion of the issues raised in the present paper, may be obtained from the JCSS http://www.jcss.ethz.ch/.

References

[1] AS/NZS 4360. Risk Management. Standards Australia, Sydney; 1999.
[2] Stewart MG, Melchers RE. Probabilistic risk assessment of engineering systems. London: Chapman & Hall; 1997.
[3] Hauser R. Lessons from European failures. Concr Int 1979;21–5.
[4] Eldukair ZA, Ayyub BM. Analysis of recent U.S. structural and construction failures. J Perform Constr Facilities, ASCE 1991;5(1): 57–73.
[5] Stewart MG. Structural reliability and error control in reinforced concrete design and construction. Struct Safety 1993;12:277–92.
[6] Faber MH, Kroon IB, Kragh E, Bayly D, Decosemaeker P. Risk assessment of decommissioning options using Bayesian networks. J Offshore Mech Arctic Engng, ASCE 2002;124:231–8.
[7] Faber MH. Lecture notes on risk and safety in civil engineering. An introduction to Bayesian Probabilistic Net’s, http://www.ibk.baug.ethz.ch/Fa/; 2001.
[8] Friis-Hansen A. Inspection planning for offshore jacket structures using Bayesian networks. In: Faber MH, editor. Proc. to International Workshop on Risk Based Inspection and Maintenance Planning. IBK Bericht Nr. 266; 2001. p. 139–54.
[9] Ditlevsen O, Madsen HO. Structural reliability methods. Chichester: Wiley; 1996.

[10] Stewart MG. Ongoing issues in time-dependent reliability of deteriorating concrete bridges. In: Das P, editor. Management of highway structures. London: Thomas Telford; 1999. p. 241–53.

[11] JCSS. Probabilistic Model Code. The Joint Committee on Structural Safety; 2001. http://www.jcss.ethz.ch/.

[12] Faber MH, Kroon IB, Sorensen JD. Sensitivities in structural maintenance planning. Reliab Engng Syst Safety 1996;51(3):317–30.

[13] Meyer MB. Catastrophic loss risks: an economic and legal analysis, and a model state statute. In: Waller RA, Covello VT, editors. Low-probability high-consequence risk analysis. New York: Plenum Press; 1984. p. 337–60.

[14] Marin A. Costs and benefits of risk reduction. Risk: analysis perception and management, London: The Royal Society; 1992. p. 192–201.

[15] Fischer A, Chestnut LG, Violette DM. The value of reducing risks of death: a note of new evidence. J Policy Anal Mgmt 1989;8(1):88–100.

[16] Lind NC, Nathwani JS, Siddall E. Management of risk in the public interest. Can J Civil Engng 1991;18:446–53.

[17] Lind NC. Target reliability levels from social indicators. In: Schueller GI, Shinozuka M, Yao JTP, editors. Sixth International Conference on Structural Safety and Reliability, vol. 3.; 1993. p. 1897–904.

[18] Nathwani JS, Lind NC, Pandey MD. Affordable safety by choice: the life quality method. Institute for Risk Research, University of Waterloo, Canada; 1997.

[19] Rackwitz RA. New approach for setting target reliabilities. Proc. Safety, Risk and Reliability—Trends in Engineering, Malta. Zürich: IABSE; March 21–23, 2001. p. 531–6.

[20] Ehlen MA. Life-cycle costs for fibre-reinforced-polymer bridge decks. J Mater Civil Engng 1999;11(3):224–30.

[21] STRUREL, Version 6.1, Theoretical, Technical and Users manual. Munich: RCP-GmbH; 1998.

[22] DNV, Sesam. PROBAN Version 4, Theory Manual. DNV Research Report no. 93-2056.

[23] Hood CC, Jones DKC, Pidgeon NF, Turner BA, Gibson R, Bevan-Davies C, Funtowicz SO, Horlick-Jones T, McDermid JA, Penning-Rowsell EC, Ravetz JR, Sime JD, Wells C. Risk management, risk: analysis, perception and management. London: The Royal Society; 1992. p. 135–92.

[24] United Nations High Commissioner for Human Rights, 1945: http://www.unhchr.ch/udhr/lang/eng.htm.

[25] Paté-Cornell ME. Quantitative safety goals for risk management of industrial facilities. Struct Safety 1994;13:145–57.

[26] Melchers RE. Structural reliability: analysis and prediction. New York: Wiley; 1999.

[27] Melchers RE. Society, tolerable risk and the ALARP principle. In: Melchers RE, Stewart MG, editors. Probabilistic risk and hazard assessment. Netherlands: Balkema; 1993. p. 243–52.

[28] Sharp JV, Kam JC, Birkinshaw M. Review of criteria for inspection and maintenance of North Sea structures. In Proc. 12th Int. Conf. on Offshore Mechanics and Arctic Engineering (OMAE'93), vol. 2. New York: ASME; 1993. p. 363–8.

[29] Elms D, editor. Owning the future: integrated risk management in practice. Christchurch, NZ: Centre for Advanced Engineering; 1998.

[30] Lee WS, Grosh DL, Tillman EA, Lie CH. Fault tree analysis, methods and applications—a review. IEEE Trans Reliab 1985;R-34(3): 194–203.

[31] Villemeur A. Reliability, availability, maintainability and safety assessment. Chichester, UK: Wiley; 1991.

[32] Klaassen KB, van Peppen JCL. System reliability: concepts and applications. London: Edward Arnold; 1989.

[33] Daniels BK. Data banks for events, incidents, and reliability. In: Green AE, editor. High risk safety technology. Chichester: Wiley; 1982. p. 259–91.

[34] Lees FP, Loss prevention in the process industries, vols. 1/2. London: Butterworths; 1980.

[35] Ang AHS, Tang WH. Probability concepts in engineering planning and design. Volume 1. Basic principles. New York: Wiley; 1975.

[36] Ellingwood BR. Earthquake risk assessment of building structures. Reliab Engng Syst Safety 2001;74:251–62.

[37] Keeney RL, Raiffa H. Decisions with multiple objectives: preferences and value tradeoffs. New York: Wiley; 1976.

[38] Kirwan B. A guide to practical human reliability assessment. London: Taylor & Francis; 1994.

[39] Diamantidis D, editor. Probabilistic Assessment of Existing Structures. France: JCSS, RILEM; 2001.

[40] Jensen JV. An introduction to Bayesian networks. UCL Press, London; 1996.

[41] Lindley DV, Introduction to probability and statistics from a Bayesian viewpoint, vols. 1/2. Cambridge: Cambridge University Press; 1976.