Chapter 12
Engineering Risk Assessment

Daniel Straub

Engineers must make decisions or advise decisions makers in problems involving uncertainty and risk. Engineering risk assessments support engineers and scientists in this task, by providing a structured approach to understanding and modeling the risks. Such risk assessments are based on a quantitative engineering modeling approach, which differs from the actuarial approach to risk modeling. Because of limited data, engineers must utilize all available information from multiple sources, including physical and logical models, observed data and expert knowledge. This information is uncertain and often contradicting. The methods presented in this chapter help engineers to consistently combine this information to come up with best estimates of risk and optimal decision support. They also help the engineer in understanding the limitations and sensitivity of risk estimates and facilitate the communication and comparison of risks. Finally, they enable the definition of clear criteria for assessing the acceptability and optimality of engineering solutions to reducing risk.

Keywords Reliability · Decision making · Risk acceptance · Structural reliability · Bayesian networks

Mathematics Subject Classification (2010) 60K10 · 62C10 · 62P30 · 90B25

The Facts

- Risk assessment is a formalized way of identifying feasible and optimal actions in situations involving uncertainty and risk.
- Risk assessment includes the identification of risks, the analysis of risks and the assessment of optimality and acceptability of risks.

D. Straub (✉)
Engineering Risk Analysis Group, Faculty of Civil, Geo and Environmental Engineering, Technische Universität München, Theresienstr. 90, 80333 Munich, Germany
e-mail: straub@tum.de

C. Klüppelberg et al. (eds.), *Risk – A Multidisciplinary Introduction*,
DOI 10.1007/978-3-319-04486-6_12,

- In engineering, risk is often associated with systems for which no or limited data is available. An actuarial approach to risk analysis (based purely on failure/damage statistics) is thus not feasible and alternative methods are needed.
- Engineering risk analysis combines physical, chemical and other models with probabilistic models of uncertainty, which are derived from both data and expert knowledge.
- Because data is limited, inclusion of in-service observations is an important part of engineering risk analysis (e.g. using Bayesian methods).

1 Introduction

The single most important responsibility of the engineer is to make decisions or to provide advice on decision making related to technology and the environment. Examples of decisions that engineers are concerned with include:

– the selection of the height of a concrete slab in a building;
– the choice of a traffic regime at a road intersection;
– the choice of soil remediation measures at the site of an industrial facility;
– the selection of the structural system and material for a skyscraper;
– the choice of an inspection and monitoring regime for an aircraft;
– the decision on the location of a new railway line;
– the choice of a site and a concept for a nuclear waste deposit.

The above examples range from seemingly minor decisions to decisions that have a major impact on a society. In all these decision problems, the engineer aims at identifying the decision alternative that is the optimal one in accordance with a set of objectives, such as cost minimization and minimization of environmental impact. Ideally, the engineer can define an objective function and all the variables entering the objective function are known with certainty. In this case, the identification of the optimal decision becomes a trivial matter. An example of such a decision problem is the design of a column that should lead to the minimum cost under the condition that it complies with the relevant codes.

In most real situations, however, the engineer must consider different, often contradictory, objectives, and she must make the decisions under conditions of uncertainty. For example, in the case of the column design, the minimization of the cost might not be the only objective, but additionally a minimization of the environmental impact might be desirable. Furthermore, the column might be subject to blast loads that are not specified by the code and which are highly uncertain. In general, the larger the impact of the decision, the more it will be required to address conflicting objectives and uncertainty. In order to make rational choices under such circumstances and to be able to justify and communicate these choices, the engineer needs to be able to formalize the problem, in a similar way as she formalizes a structural design using the rules of mechanics. This is the aim of engineering risk analysis and assessment.

Risk assessment can be seen as a special case of general decision analysis that involves uncertain, adverse consequences. Even though it is possible to merely compute the risks without considering any decisions, it is important to realize that an effective risk assessment can only be carried out in the context of the decisions to be taken (by the engineer, her client and society). The formulation of the scope of a risk analysis strongly depends on the potential decisions to be made by the decision maker. As an example, an earthquake risk analysis for a building will be different if the client is an insurance company merely interested in setting a premium, in which case it might be sufficient to determine the expected value of the annual loss in economic terms with limited accuracy, or if the client is an owner interested in a safe home, in which case it might be desired that the analysis determines the expected loss of life and property damage for different alternative seismic retrofitting options.

2 Definition of Risk

Risk arises whenever there is uncertainty on potentially adverse system outcomes, such as the failure of a structural system, the contamination of ecological systems, traffic accidents, monetary losses. The risk associated with an event increases with increasing probability of the event and/or increasing consequences. This is intuitively understood.

Here, the following mathematical definition of risk is used:

$$\text{Risk} = \text{Expected adverse consequences}.$$

The term "expected" refers to the mathematical concept of the expected value. For the case of a single adverse event E, e.g. the event of a car crash, the risk $R(E)$ is computed as the product of the probability of the event $\Pr(E)$ with the consequences of the event $c(E)$:

$$R(E) = \Pr(E) \cdot c(E). \tag{1}$$

In most risk assessments, more than one possible adverse event (scenario) needs to be considered. The total expected risk is then computed by integration or summation over all possible scenarios and risk contributions. As an example, consider the risk due to flooding in an area A. The flood hazard is commonly described by the annual maximum discharge Q in the relevant river. Let $f_Q(q)$ be the probability density function (PDF) of Q, and let $c(q, x)$ be the economic consequences of a flood with discharge q at location x. The total economic risk in the area is then calculated by integrating over all possible values of Q (the scenarios) and by integrating over the total area A:

$$R = \int_{x \in A} \int_0^\infty c(q, x) f_Q(q) \mathrm{d}q \mathrm{d}x. \tag{2}$$

As obvious from these definitions, risk is expressed in the same dimension as the consequences, e.g., monetary values, number of fatalities, amount of toxic material. In many instances, it will be necessary or preferable to convert these consequences

into an abstract utility value, to allow for a more consistent expression of the decision maker's preferences under uncertainty (see Chap. 3, [47] for an introduction to utility theory).

In engineering applications, probability (as in Eqs. (1) and (2)) is generally a subjective value, following the Bayesian interpretation of probability. In some instances, the terms likelihood or belief are used instead of probability, but to avoid confusion we will always use the term probability here. The reason for the subjective interpretation is that in real engineering applications the conditions for the frequentist (sometimes falsely termed "objective") interpretation of probability are not met. However, since decisions *must* be made, the engineer has no alternative to using her best estimate of the probabilities of events, which of course should be based on all available data and information. For this reason, Bayesian methods, which enable the combination of information from different sources, have a central role in engineering risk analysis.

3 Risk Assessment Procedure

A risk assessment is a formalized approach to determining and assessing the risk. When combined with the planning of actions, it is denoted risk-based decision making (or risk management). A procedure for risk analysis and management is illustrated in Fig. 1, adapted from Stewart and Melchers [4], and briefly outlined in the following.

Any risk assessment should commence with a definition of the context in which the analysis takes places. The risk analyst should state who the decision makers and the involved stakeholders are (client, society, governmental organizations, individuals) and it should be identified what their objectives and preferences are. Constraints and potentially influencing factors, including legal, financial, political, cultural and organizational aspects, should be determined. On this basis, the goals and the constraints of the risk analysis should be clearly stated. In particular, the criteria against which the risk is to be assessed must be defined at this stage (see Sect. 6 for examples) and agreed upon with the client.

In a next step, the investigated system must be clearly defined, as it is commonly done in a proper engineering analysis. The system is defined in terms of its physical extension (e.g. the area included in an environmental risk assessment), in terms of the potential hazards (which types of hazard are not included?) and in terms of its societal dimensions (e.g. the types of consequences that are to be considered). This definition should be established in collaboration with, and must be approved by, the client.

In a third step, a hazard scenario analysis is performed, aimed at identifying all relevant scenarios contributing to the risk. This includes an initial assessment of the risks associated with the scenarios. This crucial part of the analysis, which provides the basis for all the later analysis, is presented in more details in Sect. 4.

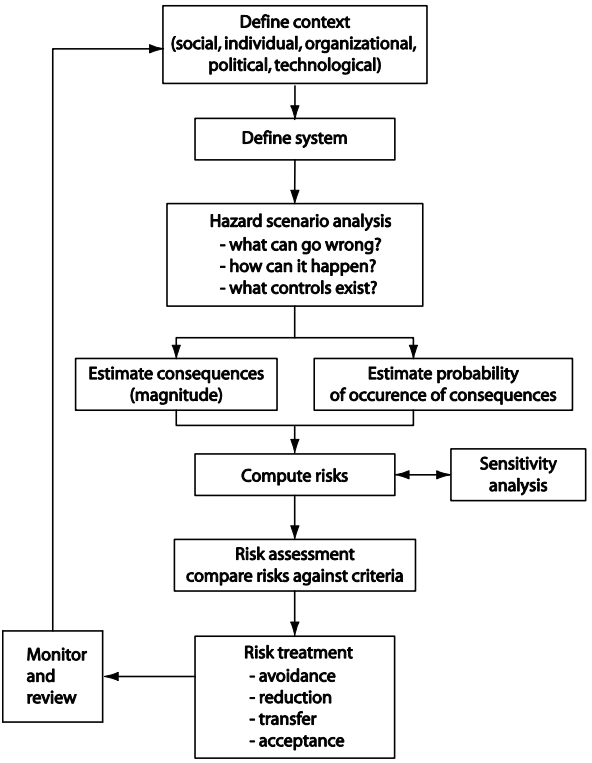

Fig. 1 Risk-based decision making/risk management procedure (adapted from Stewart and Melchers [4])

The hazard scenario analysis is followed by the quantitative risk analysis, which consists of estimating the probability of the identified adverse events as well as their consequences, by means of a variety of probabilistic modeling and analysis tools, which will be outlined in Sect. 5. These computations must generally be based on a number of assumptions. For this reason, it is essential that the computed risks are subject to a sensitivity analysis, in order to understand the influence of the assumptions on the final results. This may be followed by further analysis of crucial assumptions and a re-evaluation of the risks.

Finally, the risks are assessed, i.e. they are compared against the previously defined risk acceptance criteria (outlined in Sect. 6). At this stage, the results of the analysis are presented to the decision makers and, in some instances, to the stakeholders. On the basis of the risk assessment, strategies for treating the non-acceptable risks must be identified. Four different strategies are distinguished in Fig. 1:

- *Avoidance*: The system, or parts of the system, is no longer operated, thus reducing the associated risk to zero. In many instances, this is not an option.
- *Reduction*: The risks are reduced by introducing appropriate mitigation measures, which reduce the probability of events or their consequences. Examples

include modifications of the system itself, controlling the system through monitoring/inspection and early warning/evacuation procures.
- *Transfer*: Financial risks can be transferred through insurance or related financial instruments.
- *Acceptance*: In some instances, risks that do not comply with risk acceptance criteria must be accepted. Such acceptance should always be a temporary solution until other measures are adopted.

Following the implementation of the measures, it is required to monitor the efficiency of the measures and to review the risks after their implementation. If necessary, adjustments to the risk treatment strategy must be made.

Most elements of the risk assessment are changing with time, and ideally the risk analysis is set up in a dynamic manner, i.e. it is revised at regular intervals. Thereby, it is of importance that all the assumptions and computations made in the assessment are well documented, and that all information, including data, is well organized. This will highly facilitate an update of the risk assessment at future times, since a major portion of the budget for risk assessments is typically allocated to the collection and organization of data and information.

A set of application examples of engineering risk analyses can be found in Stewart and Melchers [4].

4 Hazard Scenario Analysis

A central part of any risk analysis is the hazard scenario analysis. In this phase of the analysis, all potential hazards and scenarios leading to damages must be identified, and suitable strategies to reach this goal must be implemented. These can vary strongly depending on the type of system and risks considered, on whether or not similar risk assessments were previously performed and on whether or not standardized procedures for the risk assessment of the considered system exist. An example of such a standardized procedure is the Probabilistic Safety Assessment methodology (PSA) developed for nuclear power plants (e.g. Beckjord et al. [11]; Apostolakis [7]).

4.1 Risk Screening

A key element of the hazard scenario analysis is a procedure for collecting the knowledge of relevant experts, which is typically achieved by organizing a meeting that includes engineers with relevant system-specific knowhow, personnel with field experience and risk analysts. Such meetings, which are sometimes termed risk screening meetings, can be understood as an organized brain-storming. In a first round, the participants are asked to envision everything that could possibly go

wrong, however unlikely the scenario. It is important that the organizers of the meeting (the moderators) ensure that no scenarios are discarded at this point. In particular experienced practitioners tend to make arguments such as "this has never happened before", and the moderators must make sure that no participant is discouraged by such comments. At this point in the process, even the highly unlikely scenarios can be of relevance. Clearly, such a meeting must be well structured and the moderators must be well prepared with background knowledge and all potentially relevant information (e.g. plans, maps, photographs, etc.).

4.2 Qualitative and Semi-quantitative Assessment of Risks

In conjunction with the risk screening, a first semi-quantitative estimation of the probability and the consequences of scenarios is made. To this end, it is common to define so-called risk matrixes, as illustrated in Fig. 2. The colors indicate the risk category. Since risk is the product of probability and consequence (Eq. (1)), the diagonals correspond to equi-risk lines if consequences and probability are plotted in log-log-scale, as is commonly done.

Here, the probability (or frequency) of events is grouped into classes (e.g., >0.1, $0.1–10^{-2}$, $10^{-2}–10^{-3}$, $10^{-3}–10^{-4}$, $<10^{-4}$), as is the consequences of events. Often, separate risk matrixes are defined for different consequence categories (fatalities, financial consequences, ecological consequences). It is noted that many industrial companies and government agencies have such risk matrixes, but these are confidential in most cases, due to legal concerns.

To each scenario, as identified in the risk screening, is assigned a probability and a consequence class (or several consequence classes, one for each category). A useful strategy to facilitate this assignment is to illustrate each consequence class by some example scenarios. This is particularly relevant when the assignments are made by experts with limited experience in estimating probabilities.

At the end of the hazard scenario analysis, it must be determined, which of the scenarios are to be further studied in the detailed analysis. This is achieved by considering all identified scenarios and excluding those that are considered to be of acceptable risk (e.g. those that fall into the green area in the matrix of Fig. 2). In this process it is important that all the assumptions made are well documented. Furthermore, when deciding which risks to accept, the limited accuracy of the initial hazard scenario analysis must be accounted for; i.e., only those risks that cannot become relevant even with a more detailed analysis can be excluded.

In this context, often the so-called ALARP principle is invoked, which stands for "As low as reasonably possible". It is common practice to divide the risk matrix into three regions: a region of acceptable risk, a region of inacceptable risk and in-between is the ALARP region, as shown in Fig. 2. All risks that are in the ALARP region should be reduced to a level "as low as reasonably possible". This signifies that for all risk scenarios falling into this region, the risks should be optimized, typically through a cost-benefit analysis. This is further discussed in Sect. 6.

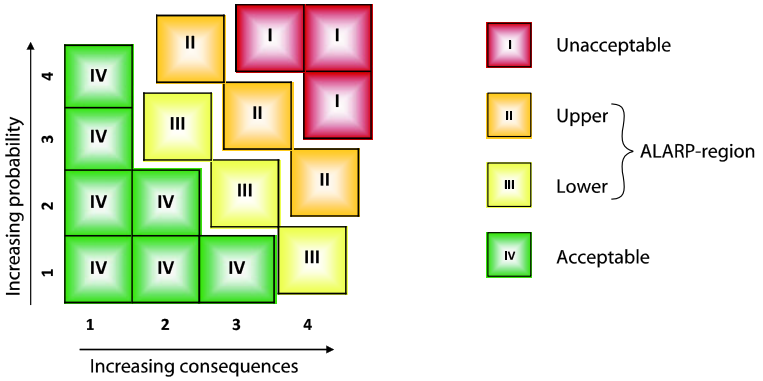

Fig. 2 Risk matrix

4.3 Logic Tree Analysis

As part of the initial assessment, as well as in detailed quantitative risk assessments, logic trees are often used for system representation. These are typically binary system representations; the most well-known are *fault trees* and *event trees*. Fault trees establish the relation between component failures and system failure events (the latter are called top-events). Event trees establish the consequences of system failures (top events) by laying out all possible event sequences following the system failure. These tools, their applications and their limitations are described in Chap. 13, [50].

5 Quantitative Risk Assessment

Quantitative risk assessment should be based on probabilistic methods. However, in risk analysis of anthropogenic systems, typically not enough data is available to determine a useful failure statistics. The reasons are

(a) that the number of such systems is often limited and failure rates are low;
(b) that the systems are subject to unique design, loading and operation conditions;
(c) that the systems are subject to common factors, introducing strong dependence among observations.

As an example, the rate of fatal accidents of European and US commercial airlines is in the order of 10^{-7}–10^{-8} per hour of flight (NTSB [33]), and accidents can reasonably well be modeled by a Poisson process. However, the failure rate varies depending on aircraft age, operator, and various other factors. Assume that our aim is to determine the probability of failure for a specific aircraft of Lufthansa during the next flight hour and compare it with the acceptable value of 10^{-8}. Within the Lufthansa fleet, in the past 10 years, no fatal accident of an aircraft in service occurred, and in the past 20 years, one fatal accident occurred. Even if all the other

specific factors of this aircraft were neglected, any statistical estimate of the failure rate is highly uncertain. More importantly, the estimate of the failure rate will not provide us with useful information on how to reduce probability of failure, since the influence of the various factors that can be modified (inspection/maintenance procedures, flight operation procedures, aircraft design) is not and cannot be quantified using statistical methods alone. It is therefore necessary to combine statistical data with engineering models of the process. This is a central part of quantitative methods in engineering risk analysis.

The following sections outline a number of techniques available in engineering risk analysis for combining engineering models with stochastic models and data, all of which aim at providing the most accurate prediction of the probability of adverse events with the given information.

5.1 Statistics

Despite the fact that there is typically not sufficient data available, statistics remains an essential tool in engineering risk analysis. In particular, probabilistic models of input parameters must be determined; as an example, the statistics of rainfall precipitation are a required input to a flood risk analysis. In this and many other examples, an estimate of the extreme behavior is essential, i.e. extreme value statistics are of importance (see Chap. 6, [23]). Special focus must be put on an accurate assessment of the uncertainties involved, since the data basis is often insufficient; an excellent example of such uncertainty is given by Coles et al. [15].

When data is limited and statistical uncertainty is relevant, Bayesian statistics enables to consistently account for this uncertainty and to include it in the assessment. An introduction to Bayesian statistics is given in Chap. 8, [17]. In addition, it is often useful to combine the data with expert opinion, which is facilitated by Bayesian statistics, whereby the prior distributions are selected following the experts. However, care is needed in order not to use the information contained in the data twice, which can happen when the experts' opinions are based on the same data that are used to determine the posterior statistics.

5.2 Probabilistic Analysis of Engineering Models

In engineering, physical, chemical or logical models of the relevant processes are typically available. These are used to make predictions of the performance of given systems. Any model can be considered as a function g that establishes a relationship between inputs $\mathbf{X}$ and outputs $\mathbf{Y}$:

$$\mathbf{Y} = g(\mathbf{X}). \tag{3}$$

In many instances (and those are the situations of interest to us), all or some of the input variables $\mathbf{X} = [X_1; X_2; \ldots]$ are random. As a result, the outcome variables

$\mathbf{Y} = [Y_1; Y_2; \ldots]$ become random as well, even if the model (the function) is known with certainty. We are thus dealing with functions of random variables.

In addition, the function g itself can also be random, i.e. for a given $\mathbf{X}$, the vector of outcome variables $\mathbf{Y} = [Y_1; Y_2; \ldots]$ is random. This situation commonly occurs in the analysis of problems involving stochastic processes, e.g. in the analysis of dynamic systems with random excitation (e.g. cars, aircraft, structures under wind or earthquake excitation). Introductions to the analysis of such systems can be found in Lutes and Sarkani [31]. Here, we will restrict ourselves to problems in which g is a deterministic function. This does not imply that we assume the model to be perfect: model uncertainty can be included through additional random variables in $\mathbf{X}$.

Ideally, we compute the full probability distribution of $\mathbf{Y}$ exactly. However, this is only possible in few cases, as discussed below. In some instances, it is sufficient to compute moments of the distribution of $\mathbf{Y}$ instead of the full distribution, which significantly simplifies the problem. For most problems, however, it will be necessary to use approximation methods. These include Monte Carlo Simulation (MCS) and the class of Structural Reliability Methods (SRM), which also include advanced sampling techniques such as adaptive importance sampling and subset simulation. These SRM are presented in Sect. 5.3.

It should be noted that applied physical models are often numerical, e.g. Finite Element (FE) models. This implies that no analytical solution for $\mathbf{Y} = g(\mathbf{X})$ exists, and that obtaining values of $\mathbf{Y}$ can be costly (in terms of computation time). This has implications on the applicable methods for evaluating the characteristics of $\mathbf{Y}$.

Illustration 5.1 (Fatigue Model) For illustrational purposes, we consider the Palmgren-Miner model for material fatigue, which occurs in dynamically loaded structures such as aircraft, trains, cars, bridges and buildings. One of the tragic failures caused by material fatigue was the accident of the ICE train at Eschede, Germany in 1998, causing 101 fatalities. Fatigue damage can be measured in terms of a normalized damage D, which in the simplest form of the model is computed as

$$D = n \frac{1}{C} S^m. \tag{4}$$

Here, C and m are material parameters, S are the stress ranges due to constant cyclic loading and n are the number of stress cycles. Failure occurs when the damage exceeds 1, i.e. when $D \geq 1$.

We consider the case where C and S are random variables, i.e. we have $\mathbf{X} = [C; S]$ and $\mathbf{Y} = [D]$. We will use this model to illustrate the different concepts and solution strategies below.

The simplest class of models is the one of linear models, which can be generically written as

$$\mathbf{Y} = g(\mathbf{X}) = \mathbf{a}_0 + \mathbf{a}\mathbf{X}, \tag{5}$$

where $\mathbf{X}$ is a vector of length n_X, $\mathbf{Y}$ and $\mathbf{a}_0$ are vectors of length n_Y, and $\mathbf{a}$ is a $n_Y \times n_X$ matrix of coefficients. As is well known, for linear models, the mean and

covariance of $\mathbf{Y}$ can be computed exactly (Papoulis and Pillai [34]). In the special case that the random variables $\mathbf{X}$ are multinormal (Gaussian) distributed, the random variables $\mathbf{Y}$ also have a multinormal distribution. This explains the popularity of linear Gaussian models: for these models, the full distribution of $\mathbf{Y}$ is readily obtained, since it is fully described by its mean and covariance.

It is noted that many non-linear models can be transformed into linear models, as illustrated in the following.

Illustration 5.2 (Fatigue Model) The non-linear model for material fatigue of Eq. (4) can be transformed into a linear model of C and S by taking the logarithm:

$$\ln D = \ln n - \ln C + m \ln S. \tag{6}$$

It follows that the mean of the logarithm of the fatigue damage is

$$\mathrm{E}[\ln D] = \ln n - \mathrm{E}[\ln C] + m\mathrm{E}[\ln S] \tag{7}$$

and its variance is

$$\mathrm{Var}[\ln D] = \mathrm{Var}[\ln C] + m^2 \mathrm{Var}[\ln S]. \tag{8}$$

If C and S are lognormal distributed, then $\ln D$ is normal distributed and the probability of failure, $\Pr(D \geq 1) = \Pr(\ln D \geq 0)$ can be computed analytically.

In the case of non-linear engineering models, a common strategy in probabilistic analysis is to approximate the models by a linear or quadratic model, so-called first- and second-order approximations (e.g. Papoulis and Pillai [34], Straub [5]). Rarely, higher order approximations are also chosen. However, in risk analysis, it is commonly the extreme events that are of interest. In this case, the approximation of the function $g(\mathbf{X})$ around the expected value $\mathbf{M_X}$ is generally not suitable. An alternative is to approximate $g(\mathbf{X})$ in the tail of the distribution, corresponding to the region of interest. Such an approach is pursued by structural reliability methods introduced in Sect. 5.3 below.

In theory, it is also possible to compute the exact distribution of $\mathbf{Y} = g(\mathbf{X})$. As is well known, when Y is a scalar one-to-one function of a single random variable X, then the distribution of $Y = g(X)$ is readily obtained as

$$f_Y(y) = f_X\left[g^{-1}(y)\right] \left| \frac{\mathrm{d}g^{-1}(y)}{\mathrm{d}y} \right|, \tag{9}$$

where g^{-1} is the inverse function of g. Solutions for general functions of one or more random variables are described in Papoulis and Pillai [34]. However, for most realistic models of engineering systems with several random variables, these solutions are not practical and approximate methods, such as the Monte Carlo simulation, are necessary.

5.2.1 Monte Carlo Approximation

With the availability of computers, a simple, intuitive and often effective approach to analyzing functions of random variables is Monte Carlo Simulation (MCS). It

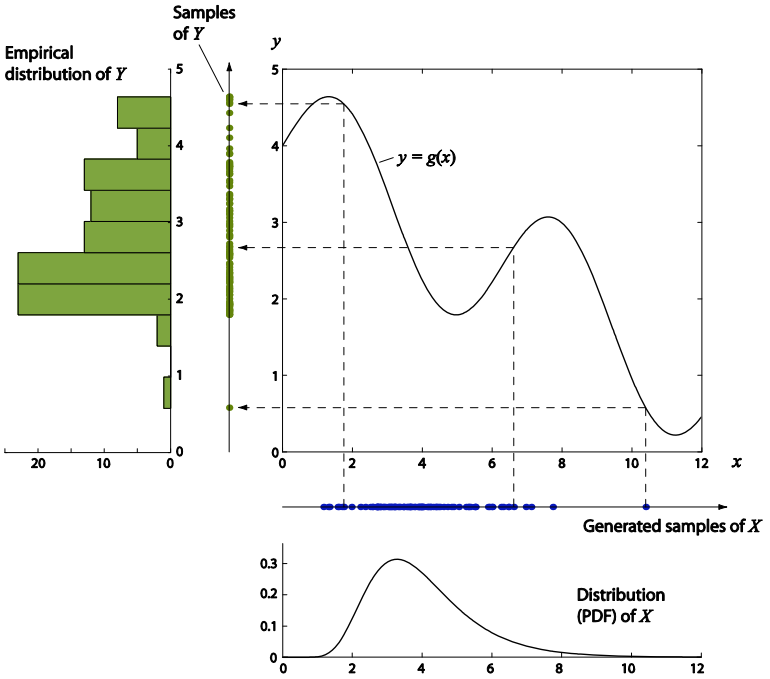

Fig. 3 Illustration of the Monte Carlo simulation approach to evaluating functions of random variables (from Straub [5])

proceeds by artificially generating samples $\mathbf{x}_i, i = 1, \ldots, n_s$ from the distribution of the input variables $\mathbf{X}$ and then evaluating the functions $\mathbf{y}_i = g(\mathbf{x}_i)$ for each sample value $\mathbf{x}_i$ separately. In this way, a set of samples $\mathbf{y}_i, i = 1, \ldots, n_s$ of the function values $\mathbf{Y}$ are generated, which provide an empirical estimate of the distribution of $\mathbf{Y}$. The principle of the MCS method is illustrated in Fig. 3 for the case of a scalar input variable X and a scalar output variable Y.

The MCS method is particularly useful when the function $\mathbf{Y} = g(\mathbf{X})$ must be evaluated numerically and when it is difficult or impossible to obtain the inverse function $g^{-1}(\mathbf{Y})$. In MCS, evaluation of the inverse function is not required.

A main advantage of MCS is its simplicity. For a given function $g(\mathbf{X})$, it consists of only three steps, which are readily performed with a few lines of computer code (in addition to the code required for evaluating $g(\mathbf{X})$). These are:

1. Generation of (pseudo-)random samples $\mathbf{x}_i$, $i = 1, \ldots, n_s$, of the input variables $\mathbf{X}$.
2. n_s evaluations of the function to $\mathbf{y}_i = g(\mathbf{x}_i)$.
3. Analysis of the generated samples $\mathbf{y}_i$ of $\mathbf{Y}$.

A more detailed introduction can be found e.g. in Rubinstein and Kroese [40] or Straub [6]. Here we only note that MCS is inefficient when computing the probability of rare events. When applying MCS with n_s samples to calculate the probability

p_F of an event F, the coefficient of variation of the MCS estimation error is approximately $(\sqrt{n_s p_F})^{-1}$. As an example, to compute a probability $p_F = 10^{-6}$, we need $n_s = 25 \times 10^6$ samples to achieve an accuracy of 20 %.

A variant of MCS, which is often more efficient, is importance sampling (IS), as described e.g. in Engelund and Rackwitz [21]. Instead of sampling randomly from the distribution of $\mathbf{X}$, IS allows to concentrate samples of $\mathbf{X}$ in the region of interest. In risk analysis, this region typically corresponds to the values of $\mathbf{X}$ for which failure of the system occurs. The identification of this region is a non-trivial matter, which, however, is facilitated by structural reliability methods outlined in the next section.

5.3 Structural Reliability Methods

In risk analysis, we are mostly concerned with failure events that have small probabilities and for which the MCS approach is not efficient. For this reason, a class of methods called Structural Reliability Methods (SRM) have been developed since the 1970s (e.g. Rackwitz and Fiessler [39]; Der Kiureghian and Liu [18]). The following provides a brief outline of SRM, detailed introductions can be found e.g. in Ditlevsen and Madsen [20], Melchers [32] or Straub [6].

In SRM, the event of interest is described in terms of a so-called limit state function $g(\mathbf{X})$, where $\mathbf{X} = [X_1; X_2; \ldots; X_n]$ is the vector of random variables of the problem (the uncertain model input). By definition, the (failure) event F corresponds to

$$F = \big\{ g(\mathbf{X}) \leq 0 \big\}. \tag{10}$$

In this formulation, $\{g(\mathbf{X}) \leq 0\} = \Omega_F$ corresponds to a domain in the outcome space of $\mathbf{X}$, whose surface is described by $\{g(\mathbf{X}) = 0\}$. The probability of the event F is thus identical to the probability of $\mathbf{X}$ taking a value within this domain. It can be computed by integrating the joint probability density function of $\mathbf{X}$, denoted by $f(\mathbf{x})$, over Ω_F:

$$\Pr(F) = \int_{g(\mathbf{x}) \leq 0} f(\mathbf{x}) \mathrm{d}x_1 \mathrm{d}x_2 \cdots \mathrm{d}x_n. \tag{11}$$

The problem is illustrated in Fig. 4. For the case of two random variables, as in Fig. 4, numerical integration is straightforward, e.g. using quadrature rules. However, most methods for numerical integration have computation times that increase exponentially with the number of dimensions (one exception being MCS). Therefore, they are not suitable to solve the integral in Eq. (11) when the number of random variables is larger than 3 to 5.

All structural reliability methods aim at solving Eq. (11). All of these methods are approximations, and each method has its own advantages and disadvantages. Here, only the first-order reliability method (FORM) is briefly introduced, followed by a short outline of other methods.

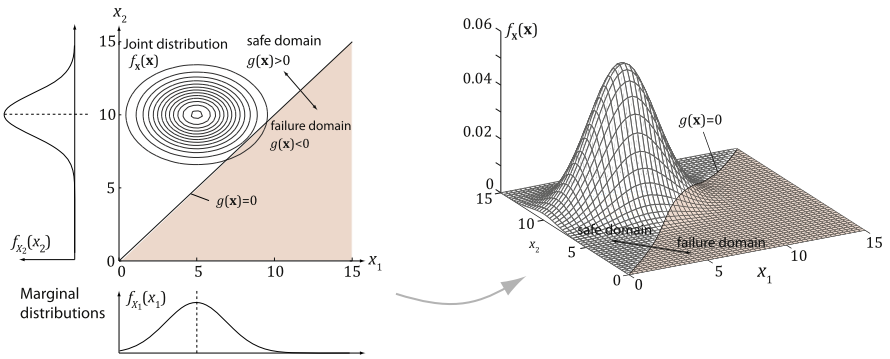

Fig. 4 Illustration of the general reliability problem, for the case of two random variables; *left*: contour plot of the joint PDF, *right*: 3D plot of the same joint PDF

Illustration 5.3 (Fatigue Failure) With the fatigue model introduced in Eq. (4), fatigue failure is modeled as the event of the damage D reaching or exceeding 1, i.e. $F = \{1 - D \leq 0\}$. It follows that the fatigue failure can be described by the following limit state function:

$$g(C, \Delta S) = 1 - n\frac{1}{C}S^m. \tag{12}$$

5.3.1 First-Order Reliability Method (FORM)

The method starts by transforming the problem from the original space of the random variables $\mathbf{X}$ to the space of standard normal random variables $\mathbf{U}$. If the joint distribution of $\mathbf{X}$ is of the Gaussian copula class, the Nataf transformation can be applied (Der Kiureghian and Liu [18]), if the joint distribution of $\mathbf{X}$ is of any arbitrary form, the Rosenblatt transformation can be used (Rackwitz and Fiessler [39]). The reader is referred to Ditlevsen and Madsen [20], Melchers [32] or Straub [6] for details. In the following, we let T denote this transformation, i.e.:

$$\mathbf{U} = \mathrm{T}(\mathbf{X}), \tag{13}$$

$$\mathbf{X} = \mathrm{T}^{-1}(\mathbf{U}). \tag{14}$$

The first basic idea of FORM is to transform the limit state function g to the space of standard normal random variables. Let G denote the new limit state function in standard normal space:

$$G(\mathbf{U}) = g\left(\mathrm{T}^{-1}(\mathbf{U})\right). \tag{15}$$

The transformation T is probability conserving, therefore we have that $\Pr(F) = \Pr(g(\mathbf{X}) \leq 0) = \Pr(G(\boldsymbol{U}) \leq 0)$. In analogy to Eq. (11), the probability of the failure event F is now computed by

$$\Pr(F) = \int_{G(\mathbf{u})\leq 0} \phi(\mathbf{u}) \mathrm{d}u_1 \mathrm{d}u_2 \cdots \mathrm{d}u_n, \tag{16}$$

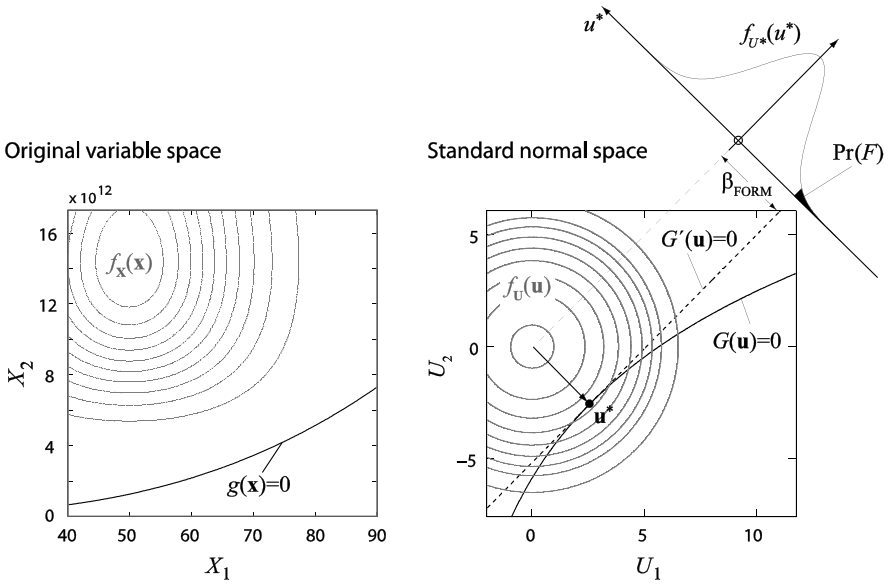

Fig. 5 Design point and linear approximation of the limit state surface. *Left side*: original random variable space; *right side*: standard normal space

where ϕ is the standard multivariate normal PDF.

The second basic idea of FORM is to approximate the limit state function $G(\mathbf{U})$ by a first-order Taylor expansion at the expansion point $\mathbf{u}^*$, denoted by $G'(\mathbf{U})$. To limit the approximation error, the expansion point is selected as the point in the failure domain with the highest probability content, the so-called Most Likely Failure Point (MLFP). Because the standard multivariate normal PDF ϕ is rotation-symmetric around the origin, the MLFP is equal to the point on the failure surface $G(\mathbf{U}) = 0$ that is the closest to the origin (provided that $\Pr(F) < 0.5$). The identification of the expansion point therefore corresponds to a constrained minimization problem:

$$\mathbf{u^*} = \arg\min \|\mathbf{u}\| \quad \text{subject to} \quad G(\mathbf{u}) = 0, \tag{17}$$

where $\|\mathbf{u}\| = \sqrt{\mathbf{u}^{\mathrm{T}}\mathbf{u}}$ is the Euclidian norm of the vector $\mathbf{u}$, which corresponds to the distance of u from the origin. The notation arg min stands for "the argument that gives the minimum value of".

Figure 5 illustrates the transformation of the limit state surface and the approximation by a hyperplane at the MLFP for the case of two random variables (in which case the hyperplane reduces to a line).

With this approximation, the limit state surface is approximated by its tangent at the design point, see Fig. 5. In FORM, the integration over the domain $\{G(\mathbf{u}) \leq 0\}$ is thus replaced by the integration over a half space defined by the tangent $\{G'(\mathbf{u}) = 0\}$.

Every marginal distribution of the standard multivariate normal distribution is a standard normal distribution. Therefore, the marginal probability distribution of $\mathbf{U}$

in the direction perpendicular to the linearized limit state surface is also a standard normal distribution, as illustrated in Fig. 5. It should be clear from the illustration that the probability of failure is fully defined by the distance $\beta_{\text{FORM}} = \|\mathbf{u}^*\|$ between the origin and the MLFP as

$$\Pr(F) \approx \Pr\big(G'(\mathbf{U}) \leq 0\big) = \Phi(-\beta_{\text{FORM}}). \tag{18}$$

Here, Φ is the standard normal cumulative distribution function (CDF). β_{FORM} is known as the FORM reliability index.

The FORM solution is independent of the problem dimension, i.e. the n-dimensional integration always reduces to an evaluation of the standard normal CDF. The difficulty in FORM is the identification of the MLFP, $\mathbf{u}^*$ i.e. the solution of the optimization problem of Eq. (17). Optimized algorithms exist for this purpose. Furthermore, specialized response surface methods have been developed to limit the number of calls of the function $g(\mathbf{X})$, e.g. Bucher and Bourgund [14] or Sudret [49].

FORM is surprisingly accurate for a wide range of problems, but the accuracy is obviously dependent on how strongly non-linear the limit state function is. For this reason, it is recommended to check improve the accuracy of FORM by performing an additional importance sampling, in which the sampling density is centered around the MLFP, e.g. Rackwitz [37]. Many other strategies exist, e.g. a second-order approximation (Breitung [13]) or a novel efficient simulation technique based on Markov Chain Monte Carlo (Au and Beck [8]), and the interested reader is referred to the literature provided in the bibliography.

Illustration 5.4 (Fatigue Failure) The fatigue failure is described by the limit state function in Eq. (12), $g(C, S) = 1 - nC^{-1}S^m$. We assume the following model for the parameters (all random variables are independent).

Because C and S are statistically independent, they can be transformed separately from $\mathbf{X}$ to $\mathbf{U}$-space, by requiring that $F_{Xi}(x_i) = \Phi[\mathrm{T}(x_i)]$. It follows that the inverse transformation T^{-1} from standard normal space is:

$$\begin{aligned} C &= \exp(U_C \sigma_{\ln C} + \mu_{\ln C}), \\ S &= U_S \sigma_S + \mu_S. \end{aligned}$$

Consequently, the limit state function in standard normal space is obtained by inserting the above expressions in Eq. (12):

$$G(\mathbf{U}) = 1 - \frac{n}{\exp(U_C \sigma_{\ln C} + \mu_{\ln C})}(U_S \sigma_S + \mu_S)^m. \tag{19}$$

The original and the transformed limit state functions are those shown earlier in Fig. 5, where $X_1 = S$ and $X_2 = C$.

With the parameters of Table 1, the MLFP is found according to Eq. (17) as

$$\mathbf{u}^* = [2.59; -2.55].$$

(This can be verified graphically in Fig. 5.) The corresponding FORM reliability index is $\beta_{\text{FORM}} = \|\mathbf{u}^*\| = 3.63$ and the FORM estimate of the probability of failure

Table 1 Parameters of the fatigue model

Variable	Distribution	CDF[a]	Parameters[b]
C	lognormal	$\Phi\left[(\ln c - \mu_{\ln C})/\sigma_{\ln C}\right]$	$\mu_{\ln C} = 30.5$, $\sigma_{\ln C} = 0.45$
S	normal	$\Phi\left[(s - \mu_S)/\sigma_S\right]$	$\mu_S = 50$, $\sigma_S = 12.5$
m	deterministic	–	$m = 3$
n	deterministic	–	$n = 10^7$

[a] Φ is the standard normal CDF

[b] All dimensions are corresponding to mm and N

is found as:

$$\Pr(F) \approx \Phi(-\beta_{\text{FORM}}) = 1.4 \times 10^{-4}.$$

For comparison, the exact solution found by direct numerical integration is $\Pr(F) = 1.3 \times 10^{-4}$. (By observing the shape of the linear approximation in Fig. 5, it should be clear that FORM slightly overestimates the reliability.)

5.4 System Reliability

In the above sections it was assumed that the event of interest is described by a parametric function of a number of random variables $\mathbf{X}$. In many instances, however, the event of interest corresponds to a system failure event that can be described by a logical function of component failure events. As a simple example, consider the failure of an aircraft with four engines. The aircraft is still operational with one engine, and the system failure F_S can thus be expressed as the intersection of the component failures F_i : $F_S = \bigcap_{i=1}^{4} F_i$. (Such a system is known as a parallel system.)

The probability of component failure can often be determined from data, either from experimental tests or—preferably—from in-service failure data. The probability of the system failure is then determined based on the component failure probability and the logical model of the system.

If the components as well as the system are expressed by binary states (failure/survival), then the relation between component states and system state can be modeled by reliability block diagrams, an example of which is given in Fig. 6. The system fails whenever there is no path between the beginning and the end of the block diagram. It is noted that other logic trees, in particular fault trees (Chap. 13, [50]), can be converted into such reliability block diagrams.

The analysis of binary systems is commonly done by identifying the so-called minimal cut sets. A cut set is a set of components that leads to system failure (it "cuts" the diagram in two) and a minimum cut set is one in which no subset is a cut set (i.e. all components must fail to cause failure of the system). For the example of Fig. 6, there are two minimal cut sets: $\{1, 3, 4\}$ and $\{2, 3, 4\}$.

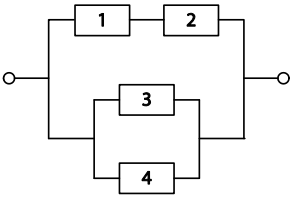

Fig. 6 Example of a reliability block diagram for a system with four components

The dual to cut sets are link sets: a link set is a set of components that ensure the system to work, and a minimum link set is one where no subset is a link set (i.e. all components are necessary for the system to function). The minimum link sets of the system in Fig. 6 are: $\{1, 2\}$, $\{3\}$ and $\{4\}$. It is pointed out that the identification of minimal link sets or cut sets is non-trivial, and can become computationally infeasible for large and complex systems.

There are two basic types of systems: the parallel system and the series system. In the parallel system, all components are set in parallel, i.e. the system fails only if all components fail: $F_S = \bigcap_{i=1}^{n} F_i$. In the series system, all components are set in series, i.e. the system fails as soon as one components fails: $F_S = \bigcup_{i=1}^{n} F_i$. For a general system, failure can be described by considering each minimal cut set as a parallel system (all components must fail for failure to occur), and the system as a series system of its minimal cut sets (the system fails as soon as one cut set fails). It follows that system failure is:

$$F_S = \bigcup_{k=1}^{n_k} \bigcap_{i \in Ck} F_i, \tag{20}$$

wherein n_k is the number of minimal cut sets and C_k is the index set describing the kth minimal cut set. For the example of Fig. 6, it is: $F_S = (F_1 \cap F_3 \cap F_4) \cup (F_2 \cap F_3 \cap F_4)$. By applying the distributive law, this can be reformulated to $F_S = (F_1 \cup F_2) \cap F_3 \cap F_4$. (Alternatively, this formulation can be obtained directly from the minimal link set formulation.)

For known cut sets, the system failure probability $\Pr(F_S)$ can be computed as a function of the individual component failure probabilities $\Pr(F_i)$, $i = 1, \ldots, n$ when component failure events are statistically independent. (As an example, if all components of the system shown in Fig. 6 are independent and have identical failure probability $\Pr(F_i) = 0.1$, then the probability of system failure is $\Pr(F_S) = 0.0019$.) This assumption of independence does not hold for most applications, and it is then necessary to know the probabilities of intersections, such as $\Pr(F_i \cap F_j)$. In this case, exact computation is only possible for small systems or when the dependence structure can be expressed in a simple form (e.g. when dependences are caused by common influencing factors). However, approximate solutions based on simulation (e.g. MCS) exist, or bounds can be computed (e.g. Song and Der Kiureghian [42]).

The computation of system reliability is a broad discipline, in particular when including also non-binary (i.e. multi-state) systems. The interested reader is referred to the monographs on system reliability by Barlow and Proschan [10] and Høyland and Rausand [26].

5.5 Bayesian Updating

Bayesian analysis is an important tool in engineering risk analysis, since it facilitates the consistent combination of information from various sources, which is crucial when the amount of data is limited. As an example, there is large uncertainty associated with tunnel construction because of random geology, but prior to and during the construction information is gathered from the site, e.g. by observing deformations or measuring groundwater flow. These allow the experienced engineer to adjust the project to minimize risks. Bayesian updating can formalize this process of assessing the risk conditional on such observations (e.g. Straub [44], Papaioannou and Straub [3]).

Bayesian updating of the probability of an event F with an observation event Z is based on the rule of Bayes:

$$\Pr(F \mid Z) = \frac{1}{\Pr(Z)} \Pr(Z \mid F) \Pr(F). \tag{21}$$

Here, $\Pr(F)$ is the a-priori probability of F (i.e. before the observation Z); $\Pr(F \mid Z)$ is the conditional a-posteriori probability of F (i.e. conditional on the observation Z); the conditional probability $\Pr(Z \mid F)$ is the so-called likelihood, which describes the information content of Z with respect to F; $\Pr(Z)$ is the a-priori probability of making the observation Z, which is obtained by normalization. Bayesian updating can be performed repetitively. Consider the case where we make two observations Z_1 and Z_2 sequentially. Firstly, the probability of F is updated with the observation Z_1 following Eq. (21). Secondly, the updated probability $\Pr(F \mid Z_1)$ becomes the new prior probability, and the conditional $\Pr(F \mid Z_1 \cap Z_2)$ is calculated from Eq. (21) where $\Pr(F)$ is replaced with $\Pr(F \mid Z_1)$.

Bayes' rule is at the heart of Bayesian statistics, as introduced in Chap. 8, [17]. The reader is referred to that chapter for details on the practical implementation of Eq. (21) in that context. There are two practical differences between the application in Bayesian statistics and in engineering risk assessment: (a) Unlike in Bayesian statistics, where the prior probability distribution is often weakly informative, in risk assessment the prior probability $\Pr(F)$ is generally informative, as it is based on the available models of the process. (b) In engineering risk assessment, the event F is often described by complex probabilistic models (often based on engineering models, as outlined earlier). Therefore, different computational approaches are required than in Bayesian statistics (e.g. the use of MCMC is often inefficient). The methods are often based on structural reliability methods, but other methods like Bayesian networks are also becoming popular. The reader is referred to Straub [43, 44] for examples of such methods.

Illustration 5.5 (Updating of Fatigue Reliability and Risk) A common strategy to reduce the risk due to fatigue failures is to perform regular inspections of the fatigue-sensitive structural details. Trains, aircrafts, turbines, bridges and many other structures undergo regular inspection, which are costly due to the inspection cost and the

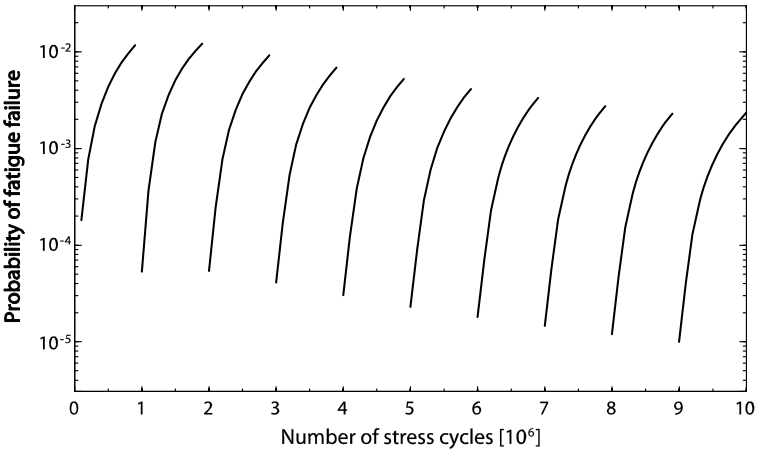

Fig. 7 Bayesian updating of the probability of fatigue failure with inspection results: inspections are performed in intervals of 10^6 stress cycles, all inspections result in no-identification of defects; taken from Straub [43]

downtime of the system. (As an example, basic checks of commercial aircrafts are performed approximately every 500–800 flight hours.) For these reasons, there is a strong interest in optimizing these inspections, which requires quantifying the effect of inspections on the probability of failure (e.g. Straub and Faber [46]).

Fatigue inspections check whether or not cracks are present in the material. When defects are found, they are repaired. When no defects are found, the probability of failure is decreased, purely due to the reduction of the uncertainty. The quality of the inspection is described by so-called Probability of Detection (PoD) functions, which describe the probability of detecting a defect as a function of the defect size. To update the probability of failure, the likelihood function is constructed by combining this PoD function with physical models describing crack growth. The latter are a function of multiple random variables. In this way, Bayes' rule can be used to update the probability of failure after every inspection that results in not finding a defect. An exemplarily result is shown in Fig. 7.

5.6 Bayesian Networks

Bayesian networks (BNs), also known as Bayesian belief networks, are probabilistic models that facilitate efficient representation of the dependence structure among random variables by graphical means. BNs have been developed since the 1980s, mostly in the field of artificial intelligence, for representing probabilistic information and reasoning (Russell and Norwig [41]). They have found applications in many fields such as statistical modeling, language processing, image recognition and machine learning, and have increasingly been applied in engineering risk analysis. Recent applications in this field are reported, e.g., in Fris-Hansen [24], Faber et al. [22],

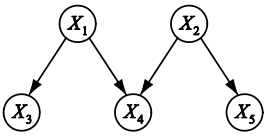

Fig. 8 A simple Bayesian network

Grêt-Regamey and Straub [25], Straub [43], Bensi et al. [12]. A general introduction to BN can be found in the textbook by Jensen and Nielsen [28].

In a nutshell, BNs model a joint probability distribution of a set of random variables $\mathbf{X} = [X_1, \ldots, X_n]$. Each random variable is represented by a node in the BN, and the links between them represent the dependence structure among the variables. If all $\mathbf{X}$ are discrete, they are fully described by their joint probability mass function (PMF), $p(\mathbf{x})$. The size of the joint outcome space of $\mathbf{X}$ for which $p(\mathbf{x})$ must be defined increases exponentially with the number of variables, but the BN enables an efficient modeling by factoring the joint probability distribution into conditional (local) distributions for each variable given its *parents*. Parents of a variable X_i are all random variables that have links pointing to X_i. A simple BN with five variables is illustrated in Fig. 8, where X_1 is a parent of X_3 and X_4, and X_2 is a parent of X_4 and X_5.

The joint PMF for this network is given as

$$p(\mathbf{x}) = p(x_1, x_2, \ldots, x_5) = p(x_1)p(x_2)p(x_3 \mid x_1)p(x_4 \mid x_1, x_2)p(x_5 \mid x_2) \tag{22}$$

which can be written in the compact and general form

$$p(\mathbf{x}) = \prod_{i=1}^{n} p\big[x_i \mid pa(X_i)\big] \tag{23}$$

where $pa(X_i)$ denotes the set of parents of X_i.

The decomposition of the joint PMF into the conditional PMFs of each variable given its parents, $p[x_i \mid pa(X_i)]$, is motivated by the *d-separation* rules (Pearl [36]), which describe the independence assumptions encoded in the graphical structure of the BN. However, the BN definition of the joint PMF according to Eq. (23) is quite intuitive even to the lay engineer with little understanding of the theory. To understand the efficiency of the BN representation, consider the case where each variable in the BN of Fig. 8 has 10 outcome states. To directly represent the joint PMF $p(\mathbf{x})$, it is necessary to specify 10^5 probability values (the size of the outcome space of $\mathbf{X}$). However, with the decomposition according to Eq. (22), it is sufficient to specify $10 + 10 + 10^2 + 10^3 + 10^2 = 1220$ probability values (e.g. for specifying $p(x_5 \mid x_2)$ for all combinations of X_2 and X_5, 10^2 values are required). Therefore, even for this simple example, the required information for specifying the problem is reduced by two orders of magnitude.

To efficiently compute marginal and conditional probabilities of variables in the network (the *inference* process), the conditional independence properties can also be exploited. Global computations involving $p(\mathbf{x})$ can be replaced by local computations. For the case that all random variables are discrete and/or linear combinations of Gaussian random variables, exact inference algorithms exist, but finding

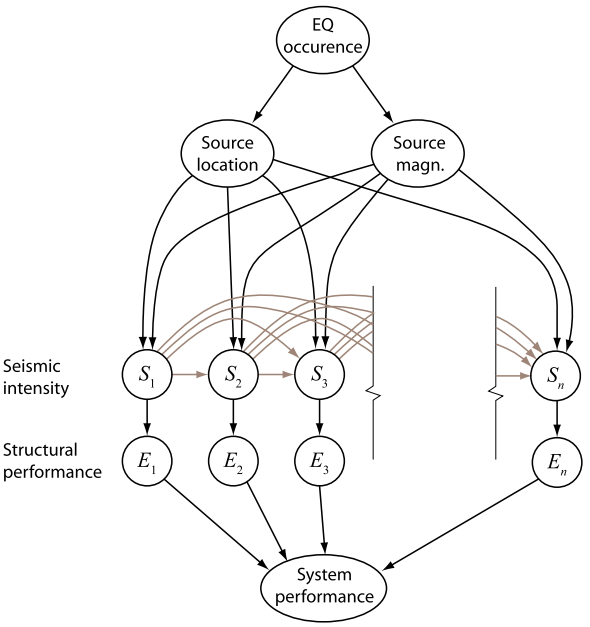

Fig. 9 BN model for seismic risk analysis of an infrastructure system (Straub et al. [48])

optimal computation strategies in a specific BN is a NP-hard task. Alternatively, sampling methods can be used to evaluate BNs. The latter can also be applied to BNs with continuous random variables. An accessible introduction to all these inference algorithms is provided by Jensen and Nielsen [28]. It is noted that a variety of software exists for constructing and evaluating BNs, many of which are available for free (e.g. the Genie software, developed at the University of Pittsburgh: http://genie.sis.pitt.edu/).

The BN has several features that make it highly useful in engineering risk analysis:

(a) Its graphical form provides a concise representation of statistical dependence that can be understood also by non-experts.
(b) The decomposition of the problem into local conditional distributions corresponds to the way complex risk analyses are performed. Combining different probabilistic models within one single BN model is often straightforward.
(c) As its name suggests, the BN is efficient for Bayesian updating when new information becomes available.

BNs are a powerful modeling framework when it is possible to exploit conditional independence among random variables. This is the case for most applications of engineering risk analysis, where the relation among random variables is often characterized by causal relations (A causes B). One example of such a dependence structure is given in Fig. 9. The dependence between the seismic intensities S_i at multiple sites i due to common earthquake source characteristics can be modeled efficiently with the BN. It also captures the assumption that the performance E_i of

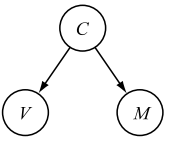

Fig. 10 The causal network for the corrosion inspection problem

infrastructure elements (bridges, pipelines, etc.) depend only on the seismic intensity at their site. However, in the example given in Fig. 9 it is also observed that, when including spatial correlation between the seismic intensity at different locations, a large number of links are needed (indicated in grey). This is one example of a dependence that is not efficiently represented by a BN. In most instances, suitable modeling strategies can avoid such types of dependences (e.g. Straub and Der Kiureghian [45]).

BN can directly be extended to decision graphs, to assess the effect of mitigation actions on the risk, and to optimize decisions following the classical decision theory (Chap. 3, [47]).

Illustration 5.6 (Corrosion Inspection) To determine the risk due to corrosion of the reinforcement in a reinforced concrete structure, a so-called "half-cell potential measurement" is performed to identify corrosion activity, together with a visual inspection of the concrete surface. Let us denote the condition of the element by C, with $\{C = 0\}$ being the event of no corrosion and $\{C = 1\}$ the event of corrosion. V is the visual inspection, with $\{V = 0\}$ the event of no visible corrosion and $\{V = 1\}$ the event of visible corrosion. M is the outcome of a half-cell potential measurement with $\{M = 0\}$ being the event of no-indication and $\{M = 1\}$ the event of indication.

It is reasonable to assume that for given condition of the element, the outcome of the measurement is independent of the visual inspection. Therefore, the causal network for this problem is shown in Fig. 10.

The conditional probability mass functions required for the specification of the network can be summarized in so-called conditional probability tables:

Event	Probability
$\{C = 0\}$	0.8
$\{C = 1\}$	0.2

Event	Probability conditional on	
	$\{C = 0\}$	$\{C = 1\}$
$\{V = 0\}$	1	0.5
$\{V = 1\}$	0	0.5

Event	Probability conditional on	
	$\{C = 0\}$	$\{C = 1\}$
$\{M = 0\}$	0.8	0.15
$\{M = 1\}$	0.2	0.85

These probability models can be obtained from deterioration models and past experience with the inspections. With these specifications, it is possible to compute

the probability of corrosion conditional on different measurement/observation outcomes. It is:

Event	Probability conditional on			
	$\{V=0\}, \{M=0\}$	$\{V=0\}, \{M=1\}$	$\{V=1\}, \{M=0\}$	$\{V=1\}, \{M=1\}$
$\{C=0\}$	0.977	0.653	0	0
$\{C=1\}$	0.023	0.347	1	1

For this simple example, the computations are trivial and can easily be performed by hand. As an example, it is:

$$\begin{aligned}\Pr(C=1 \mid V=0 \cap M=1) &= \frac{\Pr(C=1 \cap V=0 \cap M=1)}{\Pr(V=0 \cap M=1)} \\ &= \frac{\Pr(C=1)\Pr(V=0 \mid C=1)\Pr(M=1 \mid C=1)}{\sum_{i=0}^{1}\Pr(C=i)\Pr(V=0 \mid C=i)\Pr(M=1 \mid C=i)} \\ &= \frac{0.2 \times 0.5 \times 0.85}{0.8 \times 1.0 \times 0.2 + 0.2 \times 0.5 \times 0.85} = 0.347.\end{aligned}$$

Note that this corresponds to the application of Bayes' rule.

5.7 Sensitivity Analysis

One of the most important parts of any risk analysis is the investigation of the sensitivity of the computed risks to changes in the model parameters and assumptions. In engineering risk analysis, it is often necessary to make relatively crude assumptions on certain model parameters, due to the lack of detailed information or models. It is therefore essential that the sensitivity of the computed risks to these assumptions is quantified.

A sensitivity analysis essentially consists in re-running the risk computations for different input parameters. If the number of parameters is large and/or the risk model is computationally demanding, these re-runs must be limited to a few cases, which have to be selected using engineering judgment. Also, sensitivity measures from probabilistic calculations (e.g. using FORM or MCS) can be used (e.g. Cooke and van Noortwijk [16]), but it must be considered that these measures are local, i.e. for non-linear models they reflect only the effect of small changes in the assumptions.

It is also noted that many risk analyses are notional, which means that they do not compute the real risks, but compute the risk conditional on certain idealized assumptions. In particular, the effect of human error is often excluded from quantitative risk computations, due to the difficulty in modeling such errors. In this case, the computed value cannot be compared against absolute risk criteria, but the model it is still useful to assess the sensitivity of the risk to influencing factors and model assumptions. By means of sensitivity analyses, it is possible to pre-evaluate different mitigation strategies.

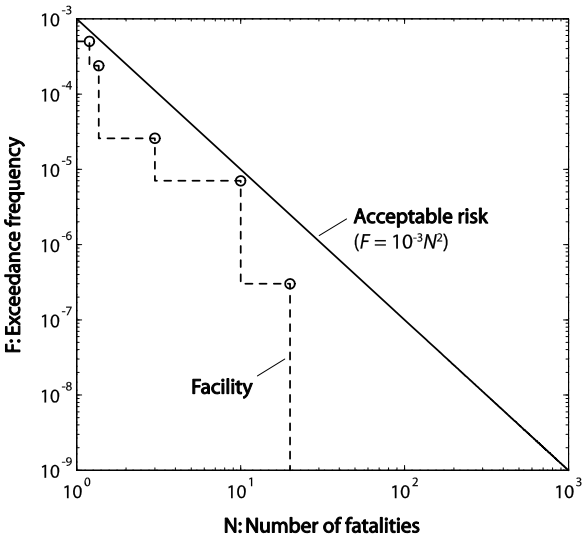

Fig. 11 Acceptable risks for chemical plants in the Netherlands, together with an exemplary F–N curve for a facility (with acceptable risk)

6 Risk Acceptance and Optimization

Once risks are computed, they must be compared against acceptance criteria. Often, multiple risk acceptance criteria (RAC) must be considered. On the one hand, criteria may be defined separately for different consequence classes (fatalities and health effects, economical, environmental). Also, it is often distinguished between individual risk (i.e. the risk accrued by one specific individual), and societal risk (the average risk in a society). The former applies e.g. to the workers in a facility or to inhabitants nearby, the latter to a member of the general public who is exposed only infrequently. On the other hand, RAC may be defined separately by the different stakeholders involved. The operator of the facility and the regulatory bodies may each have their own RAC, whereby the latter are mostly concerned with life and health risks, and increasingly with environmental risks.

RAC can be expressed in different formats, depending on the type of risk considered. It is common to express the acceptable *individual* safety risk in terms of the probability of an individual dying due to an accident during a reference time period. The acceptable *societal* safety risk is often expressed in terms of so-called F–N diagrams, where F stands for exceedance frequency and N stands for the number of fatalities. Figure 11 shows the acceptable societal risk for chemical and process plants in the Netherlands (Jongejan [29]), together with a fictitious curve for a facility. To understand this diagram, consider the point ($N = 10^1$, $F = 6 \times 10^{-6}$): this point signifies that events with $N = 10$ or more are estimated to occur with an annual frequency of 6×10^{-6}. The risk of an activity is acceptable when the entire curve is to the left of the acceptability criterion.

Risk acceptance criteria can be derived by means of different fundamental principles. It is often distinguished between:

(a) Expressed preferences: with this approach, RAC are obtained directly by asking the relevant stakeholders. The difficulty with this approach is that risk levels are often abstract values that are difficult to understand by most individuals and organizations.
(b) Revealed preferences: RAC are derived from the risk that is implicitly accepted by current activities. As an example, when assessing a new system, it can be stated that any risk that is lower or equal to the risk of the present system is acceptable. This is the most commonly applied approach in engineering.
(c) Optimization: RAC can be derived by identifying optimal risk levels, as discussed in Sect. 6.1 below. This allows regulators to require that risks are reduced to a level that can be achieved with reasonable efforts (the ALARP principle outlined in Sect. 4.2).

Existing RAC are often obtained by a combination of the above principles. For example, it is common to derive acceptance criteria from current practice, but then adjust the criteria using optimization principles, e.g. using more stringent criteria for risks where mitigation costs are low. (This approach was followed in deriving the target reliability values provided in Annex B of Eurocode 0 (DIN [19]).) Furthermore, RAC from the public (such as the one shown in Fig. 11) often represent a public consensus, and are derived based on processes involving scientists and engineers, but also representatives of governmental bodies and politicians.

For further examples and details on risk acceptance criteria, the reader is referred to Paté-Cornell [35], Aven and Vinnem [9] and Jongejan [29].

6.1 Optimization

When making decisions involving risk, one should aim at making *optimal* decisions. On the one hand, it is desirable to reduce risks as much as possible; on the other hand, one should use as little resources (money, material, time) as possible for risk reduction. This leads to a classical optimization problem, aiming at finding the optimal trade-off between risk and resources spent for risk reduction, which is illustrated in Fig. 12. The optimal decision is the one minimizing the expected cost, the optimal risk is the one associated with the decision leading to the minimal total expected cost.

Optimization principles can be used to derive absolute RAC (e.g. Rackwitz [38]), or they can be invoked by requiring that risks are reduced to an optimal level, following the ALARP principle. Such an approach is pursued by the UK Health and Safety Executive, which is the regulatory body in the UK (HSE [27]).

The optimization approach requires that all consequences and costs are expressed in the same unit, which is typically a monetary unit. If safety risks are involved, this requires quantifying the value of a statistical life (e.g. Lentz [30]). While this is not without controversy, such an approach is necessary if it is to be ensured that resources are distributed optimally among different activities within a society (for further discussion see Sect. 2.4 in Chap. 3, [47]).

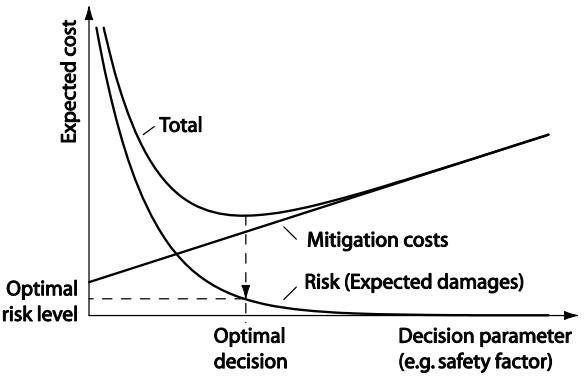

Fig. 12 Trade-off between risk and mitigation cost

7 Food for Thought

- How can we combine an engineering model, which is based on physical principles, with observed data?
- An open question in many risk analyses is how to quantify the effect of human and organizational factors.
- Discuss the context and the system definition of a risk assessment for a nuclear waste depository.
- Why do we differentiate between individual risks and societal risks?
- Engineers must often make decisions involving potentially large consequences and fatalities on the basis of limited information. How can the engineer sleep well at night?
- What is the principle of FORM?
- Why is a linear or quadratic approximation of the performance function around the mean value not suitable to compute the risk of fatigue failure of an aircraft?
- If you need to advise on which of two alternative designs for a train axle should be selected, how would you proceed?
- Often, the most difficult part of an engineering risk assessment is to explain the methods and the results to lay people and even other engineers, due to their difficulties in understanding probability. How can one approach this?

8 Summary

This chapter outlines a framework for engineering risk assessment, with a particular emphasis on quantitative methods. A general procedure is introduced, including system definition, hazard identification, risk analysis, sensitivity analysis, risk assessment and mitigation. Thereafter, it is focused on the quantitative modeling of risk in engineering, which differs from the actuarial approach by combining probabilistic engineering models (typically physical and/or chemical models) with empirical data and sometimes expert knowledge. This is illustrated by brief examples. A brief

outline of risk acceptance and optimality in the context of engineering applications concludes the chapter.

References

Selected Bibliography

1. T. Aven, *Foundations of Risk Analysis. A Knowledge and Decision-Oriented Perspective* (Wiley, Chichester, 2005)
2. J.R. Benjamin, C.A. Cornell, *Probability, Statistics, and Decision for Civil Engineers* (McGraw-Hill, New York, 1970)
3. I. Papaioannou, D. Straub, Reliability updating in geotechnical engineering including spatial variability of soil. Comput. Geotech. **42**, 44–51 (2012)
4. M.G. Stewart, R.E. Melchers, *Probabilistic Risk Assessment of Engineering Systems* (Chapman & Hall, London, 1997)
5. Straub, Lecture notes in engineering risk analysis. TU München (2011)
6. Straub, Lecture notes in structural reliability methods. TU München (2011)

Additional Literature

7. G.E. Apostolakis, How useful is quantitative risk assessment? Risk Anal. **24**(3), 515–520 (2004)
8. S.-K. Au, J.L. Beck, Estimation of small failure probabilities in high dimensions by subset simulation. Probab. Eng. Mech. **16**, 263–277 (2001)
9. T. Aven, J.E. Vinnem, On the use of risk acceptance criteria in the offshore oil and gas industry. Reliab. Eng. Syst. Saf. **90**(1), 15–24 (2005)
10. R.E. Barlow, F. Proschan, *Mathematical Theory of Reliability*. Classics in Applied Mathematics, vol. 17 (SIAM, Philadelphia, 1996)
11. E.S. Beckjord, M.A. Cunningham, J.A. Murphy, Probabilistic safety assessment development in the United States 1972–1990. Reliab. Eng. Syst. Saf. **39**(2), 159–170 (1993)
12. M.T. Bensi, A. Der Kiureghian, D. Straub, A Bayesian network methodology for infrastructure seismic risk assessment and decision support. PEER Report 2011/02, Pacific Earthquake Engineering Research Center, University of California, Berkeley (2011)
13. K. Breitung, Asymptotic approximations for multinormal integrals. J. Eng. Mech., Trans. ASCE **110**(3), 357–366 (1984)
14. C.G. Bucher, U. Bourgund, A fast and efficient response surface approach for structural reliability problems. Struct. Saf. **7**(1), 57–66 (1990)
15. S. Coles, L.R. Pericchi, S. Sisson, A fully probabilistic approach to extreme rainfall modeling. J. Hydrol. **273**(1–4), 35–50 (2003)
16. R.M. Cooke, J.M. van Noortwijk, Local probabilistic sensitivity measures for comparing FORM and Monte Carlo calculations illustrated with dike ring reliability calculations. Comput. Phys. Commun. **117**(1–2), 86–98 (1999)
17. C. Czado, E.C. Brechmann, Bayesian risk analysis, in *Risk – A Multidisciplinary Introduction*, ed. by C. Klüppelberg, D. Straub, I. Welpe (2014)
18. A. Der Kiureghian, P.-L. Liu, Structural reliability under incomplete probability information. J. Eng. Mech., Trans. ASCE **112**(1), 85–104 (1986)
19. DIN, Eurocode 0—basis of structural design (EN 1990:2002). Deutsches Institut für Normung e.V. (2001)

20. O. Ditlevsen, H.O. Madsen, *Structural Reliability Methods* (Wiley, New York, 1996)
21. S. Engelund, R. Rackwitz, A benchmark study on importance sampling techniques in structural reliability. Struct. Saf. **12**(4), 255–276 (1993)
22. M.H. Faber, I.B. Kroon, E. Kragh, D. Bayly, P. Decosemaeker, Risk assessment of decommissioning options using Bayesian networks. J. Offshore Mech. Arct. Eng. **124**(4), 231–238 (2002)
23. V. Fasen, C. Klüppelberg, A. Menzel, Quantifying extreme risks, in *Risk – A Multidisciplinary Introduction*, ed. by C. Klüppelberg, D. Straub, I. Welpe (2014)
24. A. Friis-Hansen, Bayesian networks as a decision support tool in marine applications. PhD thesis, DTU, Lyngby, Denmark (2000)
25. A. Grêt-Regamey, D. Straub, Spatially explicit avalanche risk assessment linking Bayesian networks to a GIS. Nat. Hazards Earth Syst. Sci. **6**(6), 911–926 (2006)
26. A. Høyland, M. Rausand, *System Reliability Theory. Models and Statistical Methods*. A Wiley-Interscience Publication (Wiley, New York, 1994)
27. HSE, *Reducing Risks, Protecting People. HSE's Decision-Making Process*. JHSE Books (Health and Safety Executive, Liverpool, 2001)
28. F.V. Jensen, T.D. Nielsen, *Bayesian Networks and Decision Graphs*. Information Science and Statistics (Springer, New York, 2007)
29. R.B. Jongejan, How safe is safe enough? The government's response to industrial and flood risks. PhD thesis, TU, Delft, NL (2008)
30. A. Lentz, Acceptability of civil engineering decisions involving human consequences. PhD thesis, TU München (2007)
31. L.D. Lutes, S. Sarkani, *Random Vibrations. Analysis of Structural and Mechanical Systems* (Elsevier/Butterworth/Heinemann, Amsterdam, 2004)
32. R.E. Melchers, *Structural Reliability Analysis and Prediction* (Wiley, New York, 1999)
33. NTSB, Aviation accident statistics. National Transportation Safety Board, US (2010). Retrieved June 19, 2011
34. A. Papoulis, S.U. Pillai, *Probability, Random Variables, and Stochastic Processes* (McGraw-Hill, Boston, 2009)
35. M.E. Paté-Cornell, Quantitative safety goals for risk management of industrial facilities. Struct. Saf. **13**(3), 145–157 (1994)
36. J. Pearl, *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*. The Morgan Kaufmann Series in Representation and Reasoning (Morgan Kaufmann, San Mateo, 1988)
37. R. Rackwitz, Reliability analysis—a review and some perspectives. Struct. Saf. **23**(4), 365–395 (2001)
38. R. Rackwitz, Optimal and acceptable technical facilities involving risks. Risk Anal. **24**(3), 675–695 (2004)
39. R. Rackwitz, B. Fiessler, Structural reliability under combined load sequences. Comput. Struct. **9**, 489–494 (1978)
40. R.Y. Rubinstein, D.P. Kroese, *Simulation and the Monte Carlo Method* (Wiley-Interscience, New York, 2007)
41. S.J. Russell, P. Norvig, *Artificial Intelligence: A Modern Approach* (Prentice-Hall, Englewood Cliffs, 2003)
42. J. Song, A. Der Kiureghian, Bounds on system reliability by linear programming. J. Eng. Mech., Trans. ASCE **129**(6), 627–636 (2003)
43. D. Straub, Stochastic modeling of deterioration processes through dynamic Bayesian networks. J. Eng. Mech., Trans. ASCE **135**(10), 1089–1099 (2009)
44. D. Straub, Reliability updating with equality information. Probab. Eng. Mech. **26**(2), 254–258 (2011)
45. D. Straub, A. Der Kiureghian, Bayesian network enhanced with structural reliability methods. Part A: theory. J. Eng. Mech., Trans. ASCE **136**(10), 1248–1258 (2010)
46. D. Straub, M.H. Faber, Risk based inspection planning for structural systems. Struct. Saf. **27**(4), 335–355 (2005)

47. D. Straub, I. Welpe, Decision-making under risk: a normative and behavioral perspective, in *Risk – A Multidisciplinary Introduction*, ed. by C. Klüppelberg, D. Straub, I. Welpe (2014)
48. D. Straub, M.T. Bensi, A. Der Kiureghian, Spatial modeling of earthquake hazard and infrastructure performance through Bayesian networks, in *Proc. ASCE Engineering Mechanics '08 Conference*, University of Minnesota, Minneapolis (2008)
49. B. Sudret, Meta-models for structural reliability and uncertainty quantification, in *Proc. Asian-Pacific Symposium on Structural Reliability and Its Applications*, Singapore (2012)
50. B. Vogel-Heuser, S. Rösch, Integrated modeling of complex production automation systems to increase dependability, in *Risk – A Multidisciplinary Introduction*, ed. by C. Klüppelberg, D. Straub, I. Welpe (2014)