Chapter 7 Quantitative Risk Assessment with Structural Reliability Analysis

7.1 Introduction and concepts
SRA (Structural Reliability Analysis) is a tool for calculating failure probabilities of structure. QRA (Quantitative Risk Assessment) is a more extensive safety analysis than SRA. QSRA (Quantitative Structural Risk Assessment) is, in a word, an extension of assessment of structure reliability. On the basis of SRA, in order to do QSRA, the only important work is to establish relevant standards of risk analysis and to assess it. In this chapter, QRA and SRA will be introduced in detail.

7.1.1 General
Risk analysis is a relatively new subject in comparison with most branches of engineering and new subjects take time for terminology to be agreed between specialists and even longer for wider application. A further difference is that, unlike most engineering calculations, the results of risk studies tend to be of direct concern to the general public and it is often necessary to present the results of assessments and predictions to a wide and critical audience.

Several examples can be found in the literature where structural reliability analysis (SRA) has been utilized in parts of quantitative risk analysis (QRA), (e.g., Soares, 1995). However, in most cases where SRA is applied the objects of the analysis are various types of structures exposed to different kinds of loading or wear mechanisms, and the analysis is carried out by scientists and engineers with background from structural design and the SRA tradition. Recently, efforts have been taken to assess to what extent methods of SRA is fit to model other systems appearing in the context of QRA, (e.g., Nilsen et al., 1998). The expression ‘structural reliability’ certainty indicates that the technique is restricted to analyses concerning structures, where load and capacity parameters are essential. This is however not the case, even though the theory behind the technique is developed for systems of this kind. Traditional SRA calculates the probability of failure related to the variability of geometrical and material quantities as well as of the loading under operating conditions. However, for using SRA methods it is not necessary to restrict attention to operating conditions, and when speaking about methods of SRA no constraints are put on the cause or consequence of failure. Refer to Nilsen et al. (1998) for a further discussed on the applicability of SRA methods, and some examples of use of SRA methods outside the traditional context.

Integrating SRA methods with QRA requires the establishment of a unified stochastic framework, to treat uncertainties consistently and obtain useful results for decision-making. Looking at the alternative probabilistic approaches it is not obvious how to formulate such a framework. The purpose of this guide is to discuss the alternatives and give recommendations with respect to which approach to be used.
Risk is an abstract notion, relating to the occurrence of undesired events in the immediate, intermediate or distant future. The term combines the two separate notions of the likelihood of one or more undesired events and the severity of consequences resulting from them. In the risk analysis of an engineering system the following are necessary, as far as is possible:

a) To identify all the undesired events that could occur
b) To assess their likelihood of occurrence or frequency, and
c) To estimate the nature and severity of the resulting consequences.

The wider subject of risk management involves these steps together with decision-making, control and auditing. The following concepts are essential in discussing safety and risk.

### 7.1.2 Concepts

**Physical hazard**: This is the concept that there are substances or objects with the potential for causing harm to people, the environment, or other objects. Physical hazards can be grouped under a number of types, as shown in table 7.1.1.

<table>
<thead>
<tr>
<th>Physical Hazard Type</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Toxic materials</td>
<td>Chlorine, methyl iso-cyanate</td>
</tr>
<tr>
<td>Carcinogens</td>
<td>Asbestos, vinyl chloride</td>
</tr>
<tr>
<td>Flammable materials</td>
<td>Petroleum, methane</td>
</tr>
<tr>
<td>Explosive materials</td>
<td>Ammonium nitrate, trinitrotoluene</td>
</tr>
<tr>
<td>Radioactive materials/ sources</td>
<td>Radon, X-rays</td>
</tr>
<tr>
<td>Objects with high potential energy</td>
<td>Pressure vessel, charged capacitor</td>
</tr>
<tr>
<td>Objectives with high kinetic energy</td>
<td>Moving ship, dropped object</td>
</tr>
<tr>
<td>Dangerous microbiological substances</td>
<td>Anthrax, HIV virus</td>
</tr>
</tbody>
</table>

**Table 7.1.1 Physical Hazard Types**

**Physical failure**: This is the concept that, as the result of the release of some hazard potential, an engineering or other system suffers some degree of damage.

**Failure consequences**: As the result of the failure of an engineering or other system, there is likely to be a range of undesired consequences. Some of these may be a direct result of the hazard that induced the physical failure; others may result from additional hazards. The consequences may include death and injury of people (the workforce and members of the general public), permanent disablement and long-term health effects, physical damage to the engineering system itself, loss of use of the facility, loss of professional reputation, etc.

**Risk**: The word risk is used and defined in many ways. However, the intended meanings are often closer than the words imply. The rather imprecise definition given in BS 4778 is: ‘A risk is the combination of the probability or frequency of occurrence of a defined hazard and the magnitude of the consequences of the occurrence’. A somewhat
different definition is given in a recent publication by the Health and Safety Executive (HSE, 1992) where risk is defined in simple language as ‘the chance that something adverse will happen’ and then more precisely as ‘the probability that a specified undesirable event will occur in a specified period or as a result of a specified situation’. In the latter, the word ‘risk’ is used as a synonym for ‘probability’ in relation to some specified undesired event (e.g., death), whereas in the BS4778 definition something different is implied.

The other concepts are used in this Chapter as defined in the previous chapters in this report.

7.1.3 Objectives of risk analysis

It is important to realize what the objectives of carrying out a risk analysis are. Obviously legal or authority requirements need to be met, but it is more important to utilize this tool in an effective effort to enhance safety as far as possible.

The most important objectives for use of risk analyses are (Soares, 1998):

a) Identification of significant risk contributions as basis for improvement
b) Identification of conditions and premises of single failures and failure sequences that may cause threat to personnel, environment and material investments, in order to find the basis for effective risk reduction measures
c) Provide the basis for later emergency preparedness analysis

It is important to stress that analysis is virtually useless, unless the following activities are carried out when the analysis is finalized:

a) Evaluation of risk analysis results in relation to risk acceptance criteria to decide what extent of risk reduction that is required
b) Consideration of the most effective ways and means to reduce risk

7.2 QRA and SRA

In a quantitative risk analysis (QRA), risk is quantified in an absolute sense or a relative sense, often in relation to some kind of risk acceptance criteria. The analysis identifies critical activities and systems, and predicts the effect of implementing risk-reducing measures. Conducting a QRA also gives understanding of hazards causation and potential escalation pathways. The purpose of the analysis is to provide a basis for making decisions concerning choice of solutions and measures. Such decisions could be specified as for example design loads. It is usual to distinguish between risks threatening human lives and health, the environment, and those which threaten assets or financial interests.

Risk may be expressed by the consequence spectrum \((K_i, F_i)\), \((K_2, F_2)\), …… where \(F_i\) designates the frequency of undesirable events leading to the consequence \(K_i\), or possibly the probability that an undesirable event shall occur which gives the consequence \(K_i\), (Figure 7.2.1).
Let $C$ denote the loss due to accidental events during a specific period of time. As a risk measure (index) we often use the statistical expected value of $C$, $Ec$. For the above risk model we have

$$Ec = C_1 \cdot F_1 + C_2 \cdot F_2 + \cdots$$

If $C$ counts the number of fatalities (per year) we refer to this value as PLL (Potential Loss of Lives). The FAR (Fatal Accident Rate) is closely linked to PLL. It is defined as the statistically expected number of accidental deaths per 100 million ($10^8$) exposed hr. The expected value has the advantage that there is only one value, so that evaluations and comparisons of risk can easily be performed. Risk expressed by statistically expected loss should normally be reported in addition to the consequence system.

More generally, we may use expected utility, $E_r(C)$, as a measure of risk, where $r$ is a given utility function.

As to the quantification of probability, it seems that most risk analyses being conducted in the offshore petroleum industry today are based on the classical approach, in the sense that the risk analysts see the analyses as a tool for producing estimates of true, unobservable quantities such as probabilities and expected values. A probability is interpreted in the classical statistically sense as the relative fraction of times the events occur if the situation analysed were hypothetically ‘repeated’ an infinite number of times. The parameters of the models (such as the basic event probabilities in the fault trees and the branching probabilities in event trees) are however not estimated purely by means of hard data. In practice these parameters are estimated by integrating hard data and expert opinions. This integration is usually carried out without using a well structured procedure. However, the interpretation of probabilities and frequencies is classical – there exists a true (unobservable) risk, and using risk analyses, we generate this true risk.

![Figure 7.2.1 General risk model](attachment:image.png)

This approach, which will be referred to as the common practice, is conceptually quite similar to the classical Bayesian approach as described in Aven (1997). Also in the classical Bayesian approach the purpose of the analysis is to say something about true, unobservable quantities (probabilities and statistically expected values). The main difference is related to the treatment of uncertainty. Common practice allows for subjective point estimates (‘best estimates’) of parameters, but the uncertainty associated with these estimates are seldom quantified. In the classical Bayesian
approach uncertainty related to the true parameter values and model should be expressed by subjective probability distributions, which then also generate uncertainty distributions for the output risk indices. Bayes formula is the tool for systematically updating the uncertainty distributions when new information is available.

An alternative approach, which has been drawn attention to quite recently in the offshore QRA community, is the ‘fully Bayesian approach’ where focus is on observable quantities such as the occurrence of accidental events, the number of fatalities, etc. and the use of subjective probabilities to express the uncertainty related to the values of these quantities. This approach is conceptually different from the above approaches since there exist no true risk/ probability. Probability is a way of expressing uncertainty.

The main difference between the classical Bayesian approach (also incorporating the common practice) and the fully Bayesian approach has to do with uncertainty: in the former approach uncertainty is related to the value of \( F_i \), whereas in the fully Bayesian approach uncertainty is related to the consequences \( K_i \) and losses \( c_i \).

As described in Chapters 2 and 3 in this report, the methods of structural reliability analysis (SRA) represent a tool for calculating probabilities of the form

\[
P_f = P(g(X) \leq 0)
\]

where \( X = (x_1, x_2, \cdots, x_n) \) is a set of random variables called the basic variables

\( g \) is the so-called limit state function.

Often a set of limit state function is logically connected as unions and intersections, leading to probabilities such as:

\[
P(g_1(X) \leq 0 \cup g_2(X) \cap g_3(X) \leq 0 \cup \cdots \cap \cdots)
\]

If \( X \) has distribution function \( F \), \( P_f \) can be written:

\[
P_f = \int_{\{X:g(X)\leq 0\}} dF(X)
\]

If \( F \) has a density \( f \), this integral takes the form

\[
P_f = \int_{\{X:g(X)\leq 0\}} f(X)dX
\]

Methods of SRA are used to calculate the probability \( P_f \), and to study the sensitivity of the failure probability to variations of the model parameters. Often Monte Carlo simulation is used, but this is a very time consuming technique in case of small probabilities. By utilising the approximate methods FORM and SORM sufficiently accurate results are normally found. These and related methods are described in Chapters 2 and 3.

The Bayesian approach seems to be the dominant probabilistic framework for SRA methods (Soares, 1995). Updating of probabilities within the classical Bayesian framework is very common, but also elements from the fully Bayesian approach are often seen in structural reliability analyses. As for the QRA community, the probabilistic basis for the analyses is seldom precisely specified.
7.3 Integrating QRA and SRA methods

Methods of SRA are tools for calculating probability. Thus the methods used in this type of analysis are standing in line with other reliability models, like lifetime models for mechanic and electronic equipment, reliability models for software, availability models for supply systems and models for calculating the reliability of human actions. All models of this kind can be used to calculate single probabilities that are inputs in different methods used in QRA, such as for the basic events in fault tree analysis (FTA) and the branching points in event tree analysis (ETA). A special feature of methods of SRA is however, that the influence from several random variables and failure modes may be taken into account in a single analysis. Thus, using methods of SRA, the splitting of events into detailed subevents is often not necessary to the same extent as in FTA and ETA. This makes it possible for a whole section of a fault or event tree to be replaced by a single analysis based on the SRA methods. Compared to models traditionally applied in QRA, SRA methods enable the analyst to obtain more knowledge from the analysis. Refer to Nilsen et al. (1998) for a further discussion on this and related issues. Note that a fault tree itself can be viewed as a SRA, defining the basic variable \( x_i \) as the indicator variable associated with the occurrence of the basic event \( i \) in the fault tree. The use of continuous variables is however more common in SRA, and the ability to deal with continuous variables is considered to be one of the main attractions of this technique.

The Bayesian approach is probably the most suitable basis for integrated QRA and SRA modelling. It is necessary to include whatever relevant information is available, and the Bayesian approach provides a consistent tool for combining ‘hard data’ and subjective information (expert opinions, engineering judgements etc). The classical statistical approach to risk analysis is not considered suitable for QRA and SRA. There are not sufficient ‘hard’ data available to accurately estimate unknown parameters of the methods.

In the following two subsections integrated approaches are presented for SRA methods and QRA, based on the classical Bayesian approach and the fully Bayesian approach, respectively.

7.3.1 Classical Bayesian approach and integration of SRA methods

In risk analyses we are interested in probabilities of accidental events. For this purpose a model is developed, for example a fault tree, with the basic event probabilities as parameters. We can formalise this by writing \( p = u(Q) \), where \( p \) denotes the probability of the accidental event, \( u \) the model and \( Q = (q_1, q_2, \cdots) \) the parameters of the model. Consider as an example a fault tree with two basic events \( B_1 \) and \( B_2 \), such that the occurrence of A is connected to \( B_1 \) and \( B_2 \) by an AND-gate. Then

\[
p = P(A) = P(B_1)P(B_2|B_1) = q_1q_2
\]
where \( q_1 = P(B_1) \) and \( q_2 = P(B_2|B_1) \) denotes the conditional probability of \( B_2 \) given \( B_1 \). If \( q_2 = P(B_2) \), then the event \( B_2 \) is independent of the event \( B_1 \).

It is assumed that there exist true values of \( p, u \) and \( Q \). These values of \( p \) and \( Q \) can be interpreted in the classical statistically sense as the relative fraction of times the events occur if the situation analysed were hypothetically ‘repeated’ an infinite number of times. The true model \( u \) produces the true value of \( p \) when the input \( Q \) is true.

The true values of \( p, u \) and \( Q \) are uncertain (unobservable and unknown), and we use probabilities to express this uncertainty. We start with initial information \( I \) about \( Q \), including engineering judgements, that exists before the data are observed. This initial information is expressed by a prior probability distribution \( H(Q|I) \), which reflects our initial knowledge concerning the parameters \( Q \), after having observed the experience data \( D \), we derive the posterior distribution \( H(Q|I,D) \) (using Bayes Theorem), which expresses the updated knowledge of the parameters \( Q \) after the data have been observed.

Due to the functional relationship between \( p \) and \( Q \) we can also establish the posterior distribution \( q_0 \) of \( p \). This uncertainty analysis is very often done with Monte Carlo simulation, a technique that is applied in many risk analysis codes. Mathematically we can write

\[
H_0(p') = P(p \leq p') = \int_{\{Q|Q \leq p'\}} dH(Q)
\]

where \( H \) is either the prior or the posterior distribution of \( Q \), similarly we can take into account our uncertainty related to the model \( u \). The produced distribution \( H_0 \) reflects our uncertainty related to the true value of \( p \).

This classical Bayesian approach deals with analysis / inference related to true, unobservable quantities, which is also the basis of classical statistics.

To predict \( Q \) parametric models are often used, e.g., exponential life time models. Consider the fault tree example and let \( \lambda = (\lambda_1, \lambda_2) \) with \( \lambda_i \) equal to the failure rate in the exponential model associated with event \( i \). Then \( q_i = q_i(\lambda) = 1 - e^{-\lambda_i t} \), where it is the point in time of interest. An uncertainty analysis with respect to \( \lambda \) will then produce a distribution on \( Q \), and from this a distribution can be established on \( p \).

In this set-up, the uncertainty has two elements; the stochastic (aleatory) uncertainty related to the failure time (expressed by the probability distributions \( 1 - e^{-\lambda t} \)) and the state-of-knowledge (epistemic) uncertainty related to the parameters \( \lambda \) (expected by \( H(\lambda) \)). If the exponential model \( 1 - e^{-\lambda t} \) is used, additional information will change the epistemic uncertainty distribution only.

Now to incorporate SRA methods in this setting, consider for example a case where one of the \( q_i \) is obtained by SRA methods, say \( q_1 \). Then \( q_1 \) is:

\[
q_1 = P(g_1(X) \leq 0)
\]

for a limit state function \( g_1 \) and basic variables \( X \). Denoting by \( F \) the distribution function of \( X \), it can be written:
\[ q_i = \int_{\{x \mid g(x) \leq 0\}} dF(X) \]

Assuming the existence of a theoretical, true (but unknown) distribution function \( F \) and limit state function \( g_1 \), there will also be a true (unknown) value of \( q_i \). The uncertainty related to the distribution \( F \) and the limit state function \( g_1 \), generates the uncertainty distribution on \( q_i \). Consider first a situation where uncertainty is ignored related to \( g_1 \) and assume that the uncertainty related to \( F \) is restricted to specifying a parameter (parameter vector) \( \lambda \in \Lambda \). Thus

\[ F(X) = F(X|\lambda) \]

There exists a true, but unknown, value of \( \lambda \).

\( q_i \) and \( P_\lambda \) are written to show the dependency on the parameter \( \lambda \).

Hence

\[ q_i(\lambda) = P_\lambda( g_i(X) \leq 0) = \int_{\{x \mid g(x) \leq 0\}} dF(X|\lambda) \]

and it is seen that the uncertainty distribution \( H_1 \) of \( q_i \) can be written

\[ H_1(q'_1) = P(q_1 \leq q'_1) = \int_{\{\lambda \mid q_1(\lambda) \leq q'_1\}} dH(\lambda) \]

where \( H \) denotes the prior or posterior distribution function of \( \lambda \). Thus a formula has been established for the uncertainty distribution of \( q_i \) based on SRA methods. Here \( F(X|\lambda) \) expresses the aleatory uncertainty, whereas \( H \) expresses the epistemic uncertainty.

Not all the basic variables need to depend on \( \lambda \). We might for example have a situation where \( X_1 \) is independent of \( \lambda \), and independent of the other basic variables (given \( \lambda \)), so that we can write

\[ P(X \leq \overline{X}|\lambda) = P(X_1 \leq x_1)P(\{X_i \leq x_i, i \geq 2\}|\lambda) \]

To incorporate uncertainty related to the limit state function \( g_1 \), consider the following approach. Assume, as an example, that the uncertainty related to \( g_1 \) is reflected by a random variable \( X \), such that the true limit state function \( g_1^* \) is given by \( g_1^* = Xg_1 \). Now including the variable \( X \) into the set of basic variables \( X \), we have again a special case of the standard model.

Above, SRA methods have been used to say something about one of the \( q_i \), only. However, the same type of arguments can be used when two or more \( q_i \)'s are studied using SRA methods. Consider the fault tree example with two basic events \( B_1 \) and \( B_2 \) connected by an AND-gate, and \( P(B_1 \cap B_2) = P(B_1)P(B_2|B_1) = q_1q_2 \). Suppose we have established two limit state functions \( g_1 \) and \( g_2 \) linked to \( B_1 \) and \( B_2 \) such that

\[ P(B_1 \cap B_2) = P(g_1(X) \leq 0 \cap g_2(X) \leq 0) \]

Then it can be proceed as in the one-dimensional case noting that

\[ P(g_1(X) \leq 0 \cap g_2(X) \leq 0) = \int_{\{x \mid g_1(x) \leq 0, g_2(x) \leq 0\}} dF(X) \]
7.3.2 Fully Bayesian approach and integration of SRA methods

The alternative to the classical Bayesian approach is the ‘fully Bayesian approach’, which is characterised by a focus on observable quantities, like the occurrence or not of an accidental event, the number of accidental events in a given period of time, lost production in a period of time, etc. Subjective probabilities are used to express the uncertainty of these quantities. So for the example considered above, the number of accidental events is focussed on in the given period of time, or simply the occurrence or not of an accidental event (when it is unlikely that two or more accidental events occur during the time period of interest).

As above let A denote the occurrence of the accidental event. The uncertainty involved is related to whether the event A will occur or not. Using various risk analysis methods a functional relationship between the occurrence of A and events \( B = (B_1, B_2, \cdots) \) on a more detailed level. Then

\[
I(A) = v(I(B_1), I(B_2), \cdots)
\]

where \( I() \) denotes the indicator function, which equals 1 if the argument is true and 0 otherwise. The uncertainty of the analyst regarding the occurrence of the event \( B_i \) is expressed by a subjective probability \( q_i = P(B_i) \). Using the relationship \( v \) and probability calculus, the subjective probability \( P(A) \) can be computed, which then expresses the uncertainty related to whether the event A will occur or not. Usually then

\[
P(A) = v(Q)
\]

Consider again the fault tree example with two basic events \( B_1 \) and \( B_2 \), such that the occurrence of A is connected to \( B_1 \) and \( B_2 \) by an AND-gate, i.e., \( I(A) = I(B_1)I(B_2) \). Then

\[
P(A) = P(B_1)P(B_2 | B_1) = P(B_1)P(B_2)
\]

assuming that the events \( B_1 \) and \( B_2 \) are independent, i.e., the knowledge of the outcome of \( B_1 \) does not make us change the degree of belief concerning the occurrence of \( B_2 \). Then

\[
v(Q) = q_1q_2
\]

In this approach, the meaning of uncertainty is completely different from uncertainty in the classical Bayesian approach. What is uncertain is the occurrence of the event A, and the probability \( P(A) \) expresses this uncertainty. The fact that there could be faults and weakness of the model used does not change this interpretation of \( P(A) \). There is no sense in speaking about uncertainty of the probability \( P(A) \), because such a reasoning would presuppose the existence of a true value of \( P(A) \).

Now suppose that we use a parametric model to quantify the uncertainty whether the event A will occur or not, e.g., an exponential lifetime model. Let \( \lambda \) be the model parameter, e.g., the failure rate the exponential model. Then by the Bayesian approach and according to the Law of Total Probability, we can calculate \( P(A) \) by

\[
P(A) = \int P(A | \lambda) dH(\lambda)
\]
where \( P(A|\lambda) \) denotes the conditional probability of \( A \) given \( \lambda \), and \( H(\lambda) \) is a distribution function of \( \lambda \) -- prior or posterior depending on the availability of experience data. Denoting \( q_1(\lambda) = P(B_1|\lambda) \) and \( q(\lambda) = (q_1(\lambda), q_2(\lambda), \ldots) \), we would usually have \( P(A|\lambda) = v(q(\lambda)) \), and hence

\[
P(A) = \int v(q(\lambda))dH(\lambda)
\]

Consider again the fault tree example. Assuming the events \( B_1 \) and \( B_2 \) are judged independent given \( \lambda \), it is follows that

\[
P(A|\lambda) = P(B_1|\lambda)P(B_2|\lambda) = q_1(\lambda)q_2(\lambda) = v(q(\lambda))
\]

Now, how should we interpret \( H(\lambda) \) and \( q(\lambda) \)? Does the use of the distribution \( H \) mean that we believe in a true value of \( \lambda \)? No, \( H \) gives weights to the different \( \lambda \) values according to the confidence we have in the different values (for predicting observable quantities); there exist no true value. Similarly, we can give weight to different models \( v \) according to the confidence we have in the different models (for predicting observable quantities). Another way of expressing this is to say that we give them weight according to the confidence we have in the assumptions underpinning the model (Zio et al., 1996).

Is it consistent with the fully Bayesian approach to assume a true value of \( \lambda \)? No, because, if we believe in a true value of \( \lambda \), we should also believe in a true value of \( q \), and consequently also in a true value of \( p \), but that is not possible in a fully Bayesian setting where \( P(A) \) is a total measure of uncertainty.

In a fully Bayesian setting all probabilities quantify epistemic uncertainty. The probabilities \( P(B_i|\lambda) \) and \( P(A|\lambda) \) (where \( \lambda \) is varying) represent alternative models (mathematical expressions) which we consider suitable for expressing our degree of belief concerning the occurrence of \( B_i \) and \( A \). It is a way of standardizing the probability considerations. By introducing these conditional probabilities we simplify the probability considerations by reducing the dimensions of the background information (Singpurwalla, 1988). It is not essential that the parameter \( \lambda \) has a physical interpretation; allowing different values of \( \lambda \) is just a way of generating a class of appropriate uncertainty distributions for \( B_i \) and \( A \).

Incorporation of SRA methods in this setting is straightforward. Now \( q_1 = P(g_1(X) \leq 0) \) is a measure of uncertainty, a degree of belief, concerning the occurrence of the event \( g_1(X) \leq 0 \). The values of the quantities \( X \) are uncertain (unknown) and the uncertainty is expressed by the subjective probability distribution \( F \), giving

\[
q_1 = \int_{\{X: g_1(X) \leq 0\}} dF(X)
\]

If we consider alternative models \( F(X|\lambda) \), we obtain \( P(A) \) using

\[
P(A) = \int v(q(\lambda))dH(\lambda)
\]

with
\[ q_i(\lambda) = \int_{\{x: f_i(x) \leq 0\}} dF(X|\lambda) \]

If SRA methods replaces more than one of the \(q_i\), we can proceed along the same lines.

### 7.3.3 Conclusions and discussions of the Bayesian approaches

It is possible to integrate SRA methods in QRA using both a classical Bayesian approach and a fully Bayesian approach. The classical Bayesian approach provides a framework which allows for uncertainty analysis of unknown quantities. These quantities are either parameters in the QRA model and/or parameters of the distribution function of the basic variables. The uncertainty of the parameters is propagated through the models to the output quantities.

The fully Bayesian approach will provide the probabilities of the uncertain events that are relevant in the specific situation of decision-making. These probabilities are total in the sense that they incorporate all types of uncertainty. Thus the result itself is a total measure of uncertainty, and does not require any further discussion of ‘uncertainty of the probabilities’.

When evaluating alternative approaches we should always ask ourselves whether the model and the interpretation serve the purpose of the analysis. How can the analysis provide the best possible basis for making decisions concerning choice of solutions and measures? Typically, the questions to be addressed by a risk analysis are:

- a) Is the level of danger high (relative to other activities and possible criteria)?
- b) What are the main risk contributions?
- c) What is the difference between alternative solutions?
- d) What risk reducing effect will certain measures have?

The answers to these questions give the message of the analysis and a basis for decisions.

We believe that this message is best presented using the fully Bayesian approach. This approach means that we consider risk analysis as a tool for argument and debate over safety, rather than an attempt to say something about objective risk values (Watson, 1994). Using the fully Bayesian approach the message of the analysis is not ‘disturbed’ by a discussion of uncertainty of the output probabilities / frequencies, as in the classical Bayesian approach. In our opinion it is often difficult to use the classical Bayesian approach in decision-making as the resulting uncertainty intervals are so large. What are the conclusions if two options are compared and the uncertainty bands are (0.001, 0.01) and (0.002, 0.10), respectively? The risk analysis group is consulted as an expert team to help the decision maker, but the message when adopting this approach is not very informative and gives the impression that risk analysis results are extremely uncertain. The use of SRA methods can reduce this problem, but not remove it. If the fully Bayesian approach is adopted, the output results are expressing the analysis group’s total uncertainty related to observable quantities, and it is possible to present a clear message.
It is also difficult to perform a consistent analysis within the classical Bayesian setting: in theory, an uncertainty distribution on the total model and parameter space should be established, which is of course impossible to do in practice. So, in applications only a few marginal distributions for some selected parameters are normally specified, and as a consequence the uncertainty distributions on the output probabilities / frequencies are just reflecting some aspects of uncertainty. This makes it difficult to interpret the uncertainties produced. If all uncertainties could have been included, the total uncertainty would become very large. A clear analysis is then not available. Regardless of the approach taken, the use of sensitivity analysis and importance analysis is required to establish the message of the analysis. The information basis of the analysis, and the presuppositions and assumptions made in the analysis, should be incorporated into the message. To eliminate unwanted variability in results from one analysis to another, guidelines / standards related to methods and data are required. Such guidelines / standards should however not reduce the flexibility and freedom of choice of the analysis group too much. Remember that, in a Bayesian setting, the results of the analysis express the best judgements of the analysis group. Of course, all elements of the analysis must be properly documented.

7.4 Risk analysis methodology

7.4.1 Preliminary hazard analysis – PHA
Preliminary Hazard Analysis (PHA) and Failure Mode and Effect Analysis (FMEA) are almost identical analysis techniques, when it comes to the practical execution of a study. The formats are similar, and the terms are often used synonymously. This presentation starts with the PHA which is often preferred in a safety context, and continues with FMEA.

7.4.1.1 Introduction
The preliminary Hazard Analysis (PHA) is a method for identifying potential hazards and evaluating the associated risks.
A potential hazard is in these terms the identified energy source which, if not controlled, may cause an unwanted event. Examples of hazards energy sources may be heavy loads and so on.
Having identified the possible unwanted events, further use of the PHA method guides us through a systematic concept review evaluating probable causes and consequences, and also preventive and corrective actions required to obtain a satisfactory level of safety.
The PHA may in the detail design phase be followed up by a HAZOP study (HAZard and OPerability study)

7.4.1.2 Procedure
The procedure to be followed throughout the PHA is described as shown below:
a) Definition of subsystems and operational modes
b) Identification of potential hazards
c) Definition of unwanted events
d) Evaluation in the PHA sheet
e) Identification of critical and subcritical events
f) Corrective Action Recommendation Forms (CARFs)
g) Evaluation of combined failure effects
h) Evaluation of common cause events

At this stage, SRA is used.

7.4.1.3 Probability and consequence classes
The following are the categories that may be used in the PHA analysis (Soares, 1998). The interpretations of these categories are only for illustrative purposes. Others may be used, depending on circumstances, systems analysed, etc.

7.4.1.3.1 Probability classes

<table>
<thead>
<tr>
<th>Probability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/H High</td>
<td>An unwanted event likely to occur during the operational phase being analysed.</td>
</tr>
<tr>
<td></td>
<td>i.e. probability of occurrence over 50%</td>
</tr>
<tr>
<td>3/M Marginal</td>
<td>An unwanted event which may occur during the operational phase, but most likely not.</td>
</tr>
<tr>
<td></td>
<td>i.e. probability of occurrence between 50% and 10%</td>
</tr>
<tr>
<td>2/L Low</td>
<td>An unwanted event which is likely to occur during the operational phase.</td>
</tr>
<tr>
<td></td>
<td>i.e. probability of occurrence between 10% and 1%</td>
</tr>
<tr>
<td>1/LL Low low</td>
<td>An unwanted event which is very unlikely to occur during the operational phase and may be considered as insignificant.</td>
</tr>
<tr>
<td></td>
<td>i.e. probability of occurrence below 1%.</td>
</tr>
</tbody>
</table>

7.4.1.3.2 Consequence classes

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/CAT Catastrophic</td>
<td>System totally out of control, i.e. personnel killed, uncontrolled pollution / explosion / fire or loss of full production or start-up delay for more than 50 days</td>
</tr>
<tr>
<td>3/SEV Severe</td>
<td>Situation controllable by system isolation, i.e. personnel injured, minor pollution / explosion / fire or loss of full production or start-up delay for between 7 and 50 days</td>
</tr>
<tr>
<td>2/MARG Marginal</td>
<td>System under operator control, i.e. no personnel injury or detectable pollution / fire and reduced production or partial start-up delay for up to 7 days.</td>
</tr>
</tbody>
</table>
Totally safe situation, i.e. no personnel injury or detectable pollution / fire and reduced production or partial start-up delay not more than what can be regained within short time. (No cost impact)

7.4.2 Failure mode and effect analysis
A simple illustration of the FMEA approach is included in order to demonstrate how similar the two approaches are. The FMEA was conducted for a multiswivel system on a production vessel.

7.4.2.1 Approach and methodology
The approach with subdivision in subsystems, etc. is entirely similar to the PHA methodology. The FMEA form is almost identical with the PHA form. The focus in FMEA is often on technical systems.
The use is illustrated through the following case study for a complex coupling. The focus in this demonstration is on results and presentation of these. Each identified failure mode in the FMEA is evaluated semi-quantitatively with respect to frequency and consequence. The frequency is assessed according to the following scale:

<table>
<thead>
<tr>
<th>Frequency Cat.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Very unlikely</td>
</tr>
<tr>
<td>II</td>
<td>Not probable</td>
</tr>
<tr>
<td>II</td>
<td>Seldom</td>
</tr>
<tr>
<td>IV</td>
<td>Probable</td>
</tr>
</tbody>
</table>

The consequences are categorized according to three criteria:

A Effect on production (which is usually the main concern of an FMEA)
B Potential pollution
C Effect on personnel

The following list describes the consequence categories used for assessing the effects on the production.

<table>
<thead>
<tr>
<th>Consequence Cat.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>No or minor consequence on the production</td>
</tr>
<tr>
<td>II</td>
<td>Small and local consequences. Short production delay.</td>
</tr>
<tr>
<td>III</td>
<td>Local damage or failure requiring medium restoration time. Production delay until the damage is repaired or new equipment is installed.</td>
</tr>
<tr>
<td>IV</td>
<td>Serious failure requiring long repair or restoration time.</td>
</tr>
</tbody>
</table>
Production delay until repair or replacement of equipment is performed.

The listing below describes the consequence categories used for assessing the pollution potential:

<table>
<thead>
<tr>
<th>Consequence Cat.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>Not relevant</td>
</tr>
<tr>
<td>I</td>
<td>No pollution (minor gas leaks or leaks from hydraulic systems).</td>
</tr>
<tr>
<td>II</td>
<td>Pollution handled by drain system. Small oil leaks.</td>
</tr>
<tr>
<td>III</td>
<td>Local pollution. Moderate leaks.</td>
</tr>
<tr>
<td>IV</td>
<td>Severe pollution. Large leaks (blowouts).</td>
</tr>
</tbody>
</table>

The listing below describes the consequence categories used for assessing the effect on personnel:

<table>
<thead>
<tr>
<th>Consequence Cat.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>Not relevant</td>
</tr>
<tr>
<td>I</td>
<td>No injuries. Effect on working environment.</td>
</tr>
<tr>
<td>II</td>
<td>Injuries may occur.</td>
</tr>
<tr>
<td>III</td>
<td>Injuries are likely to occur. Escape from the area may be required.</td>
</tr>
<tr>
<td>IV</td>
<td>Fatalities are likely to occur.</td>
</tr>
</tbody>
</table>

The effects and consequences of failures are not deterministic. This means that one specific failure may in some circumstances have very limited consequences, which in other circumstances the same failure may have rather severe consequences. To be on the conservative side, a ‘worst case’ (within reasonable limits) is considered for all failure modes in the FMEA. This does however not imply consideration of all consequences caused by an unfavourable ‘domino effect’ initiated by the particular failure. The evaluation of consequences is limited to the direct effects of the failure.

The risk related to each of the failure modes considered in the FMEA should be regarded as the product of the frequency and the consequence. The resulting risk picture is therefore expressed by a critically matrix having frequency category as dimension on one axis, and consequence category on the other. Thus, a particular critically category refers to one cell in the critical matrix.

7.4.2.2 FMEA sheets
The primary objectives of an FMEA are to identify all components in the system and to consider relevant failure modes for these components. The likely effect of the identified failure modes is evaluated.

The FMEA presented includes other aspects and further evaluation of the failure modes. This is, however, only supplementary information, as most emphasis has been put on the primary objectives of the FMEA. The following explains the terminology applied in the FMEA Sheet.

FMEA sheet (sample)

<table>
<thead>
<tr>
<th>FMEA OF TRANSFER OPTION WITH MULTI-SWIVEL</th>
<th>PAGE .. OF ..</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description of unit</td>
<td>Description of failure</td>
</tr>
<tr>
<td>Identification</td>
<td>Function (operation)</td>
</tr>
</tbody>
</table>

*Description of unit* includes identification of the components to consider as well as description of the function or operational mode for each component.

*Description of failure* includes a listing of all relevant failure modes and the possibility for detection of the failures. Probable cause of failure is also given for each failure mode. The ‘detection’ and ‘probable cause of failure’ columns are only supplementary information and should be regarded as such.

*Effect of failure* includes evaluation of the likely effect on the component itself (on unit) or on the primary function of the component. Possible effects on other components or systems are also given. Only the most important and severe effects are listed.

Generally, *risk* is the product of frequency and consequence. Therefore, the risk column includes a semi-quantitative assessment of the frequency (Fr) and consequences (C) of each failure mode. The consequences are related to three criteria: effect on production (A), potential pollution (B) and effect on personnel (C).

In case there are several identical items (for instance values), the frequency assessment is intended to reflect the total occurrence probability of each failure mode. It should be noted that the frequency and consequence assessments are only indicative, and no extensive research has been performed in order to categorize the failure mode.

The supplementary column *Corrective actions* lists possible measures to repair or restore the system when a failure has occurred. This column is related to the ‘Probable cause of failure’ column. There is however no direct link between them, which means that there is not necessarily a corrective action listed for every cause of failure, and vice versa.
7.4.3 Event tree analysis methodology

7.4.3.1 Introduction
An event tree is a visual model for description of possible event chains which may develop from a hazardous situation. Top events are defined and associated probabilities of occurrence are estimated. Possible outcomes from the event are determined by a list of questions where each question is answered yes or no. The questions will often correspond to safety barriers in a system such as ‘isolation failed?’, and the method therefore reflects the designer’s way of thinking. The events are portioned for each question, and a probability is given for each branching point. The end events (terminal events) can be gathered in groups according to their consequence to give a risk picture. A simple way to carry out a fatality risk assessment is to assign a number of fatalities to the branching points (in case of branching one way), and these are summed to find the number of fatalities for the end events.

From event trees the following are often performed:

a) Frequency calculation for consequence classes
b) Simulation of uncertainty in input data
c) Sensitivity analysis (effect of variations of some parameters)
d) Identification of major contributions to each consequence class

7.4.3.2 Event tree for escape and evacuation
The event tree which is being considered is a tree for an evaluation of evacuation from a platform. The top event in the event tree is assumed to be an event which required evacuation from the platform, e.g. a blowout, a large fire etc. From this top event, different scenarios may develop, depending on the circumstances. The different circumstances are described to the right of the event tree, in the form of a number of questions.
The first question considered in the event tree is whether precautionary escape from the platform has been performed. If this is the case, then we move to the left along the first branch of the event tree, otherwise we move to the left.
The second question is whether escape has been performed prior to ignition. Obvious, if precautionary escape has been performed, this question is superfluous. For the left branch from the first question, this second question is therefore not considered. However, for the right branch it is relevant. In this way, we can continue through the event tree, splitting the scenarios into more and more new scenarios, depending on a variety of conditions.
The event tree can be also be used for quantification of the likelihood of different scenarios. Probability values can be assigned to each branch and in this way we build up a tree of conditional probabilities.
If we return to the example with evacuation again, we may assume that the probability of precautionary evacuation being performed is 0.6. This means that the probability that
precautionary evacuation is not performed will be 0.4. Secondly, given that precautionary evacuation not has been performed, we may assume that the probability of escape before ignition is 0.8. The total probability of escape before ignition given no precautionary escape becomes $0.4 \cdot 0.8 = 0.32$.

By continuing this logic through the tree, we can arrive at probabilities for the terminal events in the event tree. If we also multiply using the frequency of the top event, we arrive at the frequency for each terminal event.

### 7.4.3.3 Major hazard scenarios

The event tree shown above is a relevant example, but does not reflect the main use of event trees in offshore QRA, namely for modelling of accident sequences from hydrocarbon leaks and other major hazards.

The following are the main categories of event trees often considered:

- **a)** Structural and marine accidents
- **b)** Blowouts
- **c)** Hydrocarbon leak events from process equipment
- **d)** Hydrocarbon leak events from riser
- **e)** Fires in utility systems, mud process and quarters

Figure 7.4.1 presents the structure of event trees for M30 module on a gas production platform, where separate trees are developed for each piece of equipment:

Trees are now developed separately for the relevant leak categories for each piece of equipment. The number of trees may therefore be quite substantial for a large platform. It is therefore necessary to eliminate trees and parts thereof that are not really required, in order to avoid overweight.

### 7.4.3.4 Initiating event frequency and nodes in event trees

The frequencies for each leak (top event) are presented on the same sheets as the event tree (Soares, 1998). Frequency for initiating events are calculated separately for each equipment or system based on either on system or equipment values.

Event tree probabilities are provided for each branching point (node) in the event trees. It is stressed that not all safety systems need to be reflected in the tree as separate nodes.
It will in many circumstances be most efficient to combine several systems into one
node, to avoid that the event tree increase to an unmanageable size.

7.5 Conclusions
Risk analysis is a relatively new subject in comparison with most branches of
engineering. In the risk analysis of an engineering system it is necessary, as far as the
following is possible:
   a) To identify all the undesired events that could occur
   b) To assess their likelihood of occurrence or frequency, and
   c) To estimate the nature and severity of the resulting consequences.

The most important objectives for use of risk analyses are:
   a) Identification of significant risk contributions as basis for improvement
   b) Identification of conditions and premises of single failures and failure sequences
      that may cause threat to personnel, environment and material investments, in
      order to find the basis for effective risk reduction measures
   c) Providing the basis for later emergency preparedness analysis

In a quantitative risk analysis (QRA), risk is quantified in an absolute sense or a relative
sense, often in relation to some kind of risk acceptance criteria. The analysis identifies
critical activities and systems, and predicts the effect of implementing risk-reducing
measures. Conducting a QRA also gives understanding of hazards causation and
potential escalation pathways. The purpose of the analysis is to provide a basis for
making decisions concerning choice of solutions and measures.

Methods of SRA are tools for calculating probability. Thus the methods used in this
type of analysis are standing in line with other reliability models, like lifetime models
for mechanic and electronic equipment, reliability models for software, availability
models for supply systems and models for calculating the reliability of human actions.
All models of this kind can be used to calculate single probabilities that are inputs in
different methods used in QRA, such as for the basic events in fault tree analysis (FTA)
and the branching points in event tree analysis (ETA). A special feature of methods of
SRA is however, that the influence from several random variables and failure modes
may be taken into account in a single analysis. Thus, using methods of SRA, the
splitting of events into detailed subevents is often not necessary to the same extent as in
FTA and ETA. This makes it possible for a whole section of a fault or event tree to be
replaced by a single analysis based on the SRA methods. Compared to models
traditionally applied in QRA, SRA methods enable the analyst to obtain more
knowledge from the analysis. The use of continuous variables is however more common
in SRA, and the ability to deal with continuous variables is considered to be one of the
strengths of this technique.

In this chapter, the integrated approaches for SRA methods and QRA are presented on
the basis of the classical Bayesian approach and the fully Bayesian approach,
respectively. It is possible to integrate SRA methods in QRA using both a classical
Bayesian approach and a fully Bayesian approach. The classical Bayesian approach provides a framework which allows for uncertainty analysis of unknown quantities. These quantities are either parameters in the QRA model and/or parameters of the distribution function of the basic variables. The uncertainty of the parameters is propagated through the models to the output quantities.

The fully Bayesian approach will provide the probabilities of the uncertain events that are relevant in the specific situation of decision-making. These probabilities are total in the sense that they incorporate all types of uncertainty. Thus the result itself is a total measure of uncertainty, and does not require any further discussion of ‘uncertainty of the probabilities’.

In addition to the above, Risk Analysis methodology is introduced. Preliminary Hazard Analysis (PHA) and Failure Mode and Effect Analysis (FMEA) are almost identical analysis techniques, when it comes to the practical execution of a study. The formats are similar, and the terms are often used synonymously. This presentation starts with the PHA which is often preferred in a safety context, and continues with FMEA.

The procedure to be followed throughout the PHA is described as shown below:

- Definition of subsystems and operational modes
- Identification of potential hazards
- Definition of unwanted events
- Evaluation in the PHA sheet
- Identification of critical and subcritical events
- Corrective Action Recommendation Forms (CARFs)
- Evaluation of combined failure effects
- Evaluation of common cause events

The FMEA with subdivision in subsystems, etc. is entirely similar to the PHA methodology. Each identified failure mode in the FMEA is evaluated semi-quantitatively with respect to frequency and consequence.

An event tree is a visual model for description of possible event chains which may develop from a hazardous situation. Top events are defined and associated probabilities of occurrence are estimated. The events are portioned for each question, and a probability is given for each branching point. The end events (terminal events) can be gathered in groups according to their consequence to give a risk picture. A simple way to carry out a fatality risk assessment is to assign a number of fatalities to the branching points (in case of branching one way), and these are summed to find the number of fatalities for the end events.

From event trees the following are often performed:

- Frequency calculation for consequence classes
- Simulation of uncertainty in input data
- Sensitivity analysis (effect of variations of some parameters)
- Identification of major contributions to each consequence class

QRA with SRA is a useful tool for structure design, maintenance and service.