1

Applications and practices of modelling, risk and uncertainty

This chapter reviews classical practice in various domains involving modelling in the context of risk and uncertainty and illustrates its common and distinguishing features. In particular, the distinct model formulations, probabilistic settings and decisional treatments encountered are reviewed in association with the typical regulatory requirements in the areas of natural risk, industrial design, reliability, risk analysis, metrology, environmental emissions and economic forecasting. This will help to introduce the notation and concepts that will be assembled within the generic modelling framework developed in Chapter 2. It will also lead to a review of the associated challenges discussed in other chapters. Although unnecessary to an understanding of the rest of the book, Chapter 1 can thus be read as an overview of the areas motivating the book’s applications and as an analysis of the corresponding state of the art.

In order to facilitate reading, the following sections group the review of methods and practices under subsections that refer to given classes. Obviously, some of the methods introduced in association with one field are in fact used elsewhere, but this would not be the dominant practice. Industrial risk denotes risks affecting industrial facilities as the consequence of internal initiators such as reservoir failure, pipe break and so on; on the other hand, natural risk covers risks triggered by natural aggressions (e.g. seism, flood, ...) and impacting on either industrial facilities or domestic installations. At the crossroads lies the so-called natech risk amongst which the Fukushima/Sendai event is a recent example.

1.1 Protection against natural risk

Natural risk, an important concern for industrial or domestic facilities, has triggered an extensive field of risk research for which the ultimate goal is generally the design of protection for infrastructures or the reduction of the level of vulnerability in existing installations. Probabilistic approaches have permeated to a various extent both regulation and engineering practice, for example with regard to nuclear or hydro power facilities. Here are some notable examples of natural risk addressed:
flood protection,
maritime aggressions, such as waves or storm surges coupled with extreme tides,
low flows or high temperatures (threatening the cooling of energy facilities),
extremely cold temperatures, or associated phenomena (ice blocking, . . .),
seism.

The typical situation is depicted in Figure 1.1. The box called ‘local risk situation’ summarises all phenomena according to which a flood, seism, cold wave or any type of aggression may impact locally on the installation and generate undesired consequences. It is determined both by:

- the natural hazard events (flood, seism, wind series . . . ) that constitute initiators of the risk phenomenon;
- the local configuration of the installation, that is its vulnerability depending on the local mechanics of the natural event and its consequences depending on the assets of all kinds that are at stake (plant operation, integrity of equipments, resulting pollution or damage to the environment, potential injuries or fatalities, . . . ) and the level of protection insured by the design choices and protection variables (e.g. dike height).

Natural initiators can be generally described by a few variables such as wind speed, seismic acceleration, flood flow and so on: they will be subsequently gathered inside a vector $x^m$. Similarly, all protection/design variables will be formally gathered inside a vector $d$. Additionally, official regulations or design

---

1 Dimension can be very large, even infinite if the time dynamics or spatial extension of the initiator are relevant to the design (e.g. flood hydrogram, seismic accelerogram, seismic acceleration 3D field): without loss of generality the vector notation is kept at this stage, and is also understood as the result of discretisation of the associated functions.
guidelines generally specify *risk or design criteria* that drive the whole study process. The definition of such criteria combines the following elements:

- A given undesirable *event of interest* (e.i.) which will be denoted as $E$. Think of dike overflow caused by flood or marine surge, structural collapse, cooling system failure and so on. Such an event of interest is technically defined on the basis of critical thresholds for one or several *variables of interest* (v.i.) characterizing the *local risk situation*: they are represented in Figure 1.1 by vector $z$. Think of the flood water level, a margin to mechanical failure, a critical local temperature and so on.
- A maximal *acceptable level of risk*: for instance, the undesired event should not occur up to the 1000-yr flood, or for the seism of reference; or else, structural collapse should occur less than $10^{-3}$ per year of operation and so on.

The type of structure shown in Figure 1.1, linking variables and risk criteria, is similar to that mentioned in the book’s introduction. Beyond natural risk, it will be repeated with limited variations throughout the areas reviewed in this chapter and will receive a detailed mathematical definition in Chapter 2.

### 1.1.1 The popular ‘initiator/frequency approach’

A considerable literature has developed on the issues raised by protection against natural risk: this includes advanced probabilistic models, decision theory approaches or even socio-political considerations about the quantification of acceptable risk levels (e.g. Yen and Tung, 1993; Duckstein and Parent, 1994; Apel et al., 2004; Pappenberger and Beven, 2006). The most recent discussions have focused on the cases of major vulnerability, uncertainty about the phenomena, reversibility or the precautionary principle (Dupuy, 2002). Notwithstanding all these research developments, it is useful to start with the state of the practice in *regulatory* and *engineering* matters. Most of the time, emphasis appears to be given to a form of *‘initiator/frequency approach’* which consists of attaching the definition of the risk criterion to a reference level prescribed for the initiator, for instance:

- ‘overspill should not occur for the 1000-yr flood’,
- ‘mechanical failure margin should remain positive for the reference seism’.

As will be made clear later, this consists essentially of choosing to focus on a single initiator $x^m$ as the dominant *alea* or source of randomness controlling the hazards and the risk situation. Good examples are the extreme wind speed, the flood flow, the external seismic scenario and so on. Nevertheless, a closer look into the realisation of the undesired event $E$ usually leads to identifying other potentially important sources of uncertainties or risk factors. Yet, those additional uncertain variables (which will be noted $x^m$) may be separated and given an ancillary role if they are mentioned at all. Think of:

- the riverbed elevation which conditions the amount of overspill for a given level of flood flow;
- the soil conditions around the industrial facility that modify the seismic response;
- the vulnerability of the installations, or conversely the conditional efficiency of protection measures.

At most, the two former types of variability would be studied in the context of local sensitivity to the design, if not ignored or packed within an additional informal margin (e.g. add 20 cm to design water level, add 20% to seismic loading, etc.). The latter type is seldom mentioned and is even less often included in the regulatory framework.

This has a strong impact on the probabilistic formulation of the approach. Consider the undesired event $E$ characterised by the variables of interest $z$ (e.g. flood level, peak temperature, peak wind velocity,
mechanical margin to failure). Event $E$ is often schematised as a mathematical set stating that a certain threshold (e.g. dike level, critical temperature, critical wind, zero margin) is exceeded for a real-valued variable of interest:

$$E = \{z | z > z_s \}$$  \hspace{1cm} (1.1)

It could more generally involve several thresholds to be exceeded by several components of interest during the same event (see Section 1.2.1 on structural reliability). Supposing that there is a model quantifying the phenomena involved in the local risk situation, the undesired event will be modelled as one of the following mathematical relationships:

$$e = 1_{z \in E} = G(x^{in}, x^{en}, d)$$  \hspace{1cm} (1.2)

$$z_s - z = G(x^{in}, x^{en}, d)$$  \hspace{1cm} (1.3)

whereby the model function $G(\cdot)$ predicts either the event $E$ itself, through an indicator variable $e$ ($e = 1$ when event $E$ is realized, $e = 0$ otherwise), or through a margin to failure $z_s - z$ that should stay positive in order to remain safe. It may be as simple as a subtraction between a scalar $x^{in}$ (e.g. natural flood level) and the protection level $d$ (e.g. dike elevation). It could also be a more complex model involving integral-differential equations to be solved to quantify the impact of a given natural event $x^{in}$ (say a reference seism) on the event or variable of interest. It should depend also on the design variables $d$ as well as on other salient environmental or system conditions $x^{en}$.

Hence, what was called an ‘initiator frequency approach’ consists formally in estimating a level $x^{in}$ for the initiator corresponding to a given annual frequency (or probability) of $x$. When modelling $x^{in}$ as a random variable $X^{in}$, such a level corresponds to the following quantile:

$$P(X^{in} > x^{in}) = \alpha$$  \hspace{1cm} (1.4)

where, for instance, $\alpha = 10^{-2}$ (respectively $10^{-3}$) if $x^{in}$ denotes the hundred-year (resp. the thousand-year) storm wind speed or flood flow. It may be hard to compute meaningful probabilities in some cases, such as rare seism: then $x^{in}$ may alternatively denote a conventional level that is thought to be ‘reasonably maximally plausible’ without quantifying the level of risk. Either way, the approach subsequently consists in checking the following risk criterion:

$$c_Z(d) = G(x^{in}, x^{en}, d) \geq 0$$  \hspace{1cm} (1.5)

or equivalently:

$$c_Z(d) = P[G(x^{in}, X^{en}, d) > 0 | X^{en} = x^{en}] < \alpha$$  \hspace{1cm} (1.6)

---

2 See Chapter 4 for comments on the theoretical differences between the two notions; differences can be neglected in practice for rare events, for which frequencies and probabilities are numerically very close.

3 Note that while $x^{in}$ can be defined straightforwardly as the quantile in dimension 1 for $x^{in}$, things become more complex when considering a vector initiator. This may be seen as another limit on the simplicity of the initiator-frequency approach, circumvented in practice through the consideration of an ‘equivalent’ event.
where $c_Z(d)$ denotes a first example of what will be called the \textit{risk measure} throughout the book. The risk criterion is defined in comparing the risk measure to a prescribed threshold. Fulfilling such a criterion can be reformulated as:

\begin{quote}
‘up to the $z$ - initiator (i.e. 1000-yr flood, reference seism etc.) at least, installation is safe under design $d$’.
\end{quote}

Such a risk measure has more of a \textit{conditional deterministic} nature than a fully probabilistic one. Indeed, two important remarks can be made. Note firstly that a \textit{monotonous} relationship of the underlying physics is implicitly assumed in order to give credit to the fact that such a criterion \textit{covers} all initiators $x^{in}$ lower than $x^z$. This gives a first example of the type of \textit{physical} consideration involved in risk assessment, to which the book will come back to in detail (see Chapters 4 and 7).

Although \textit{physically intuitive} in many natural risk situations (the stronger the windgust, the thinner the covering material, the lower the dike and so on the riskier), this hypothesis may not be certain in some cases. Secondly, the criterion may not cover satisfactorily the other sources of uncertainty affecting $x^{en}$, for it does not formally define what values should be taken for those leftover variables. Sensible engineering practice would usually fix so-called ‘penalised’ values (noted $x^{en}_{pn}$) for those variables, meaning that some coefficients or safety margins are incorporated to multiply (or add up to) the ‘best-estimate’ values noted $x^{en}$. Note that this effort to cover the unknowns presupposes in turn the monotonicity of the alternative relationship $x^{en} \rightarrow G(...,x^{en})$. This type of approach, which will be called ‘initiator-frequency + margins’, is sometimes used in the field of natural risk protection. It has inspired greater developments in a number of standards or regulations in the field of industrial safety as will be shown in Section 1.2.

### 1.1.2 Recent developments towards an ‘extended frequency approach’

A more complete ‘\textit{extended frequency approach}’ has also been considered in the literature for a long time, although the names differ (cf. review by de Rocquigny, 2010). It involves an alternative risk criterion that tries to remedy the two above-mentioned shortcomings. The risk measure incorporates an extended probabilistic description of the uncertainties affecting not only the initiator but also other influential variables, as follows:

\begin{equation}
P(G(X^{in}, d, X^{en}) = 0) \geq 1 - \alpha \quad \text{or} \quad P(G(X^{in}, d, X^{en}) > 0) \geq 1 - \alpha \tag{1.7}
\end{equation}

Fulfilling this alternative risk criterion can be reformulated as:

\begin{quote}
‘except in less than $\alpha\%$ of the risk situations, installation is safe under design $d’$.
\end{quote}

This extended approach should be seen as a rather rare and mostly recent alternative (see the Dutch regulations on flood). In natural risk, the initiator/frequency approach remains as standard practice (Table 1.1). Admittedly, this is not disconnected from some practical aspects of natural risk assessment. Indeed, concentrating on an \textit{initiator frequency approach} enables the studies to be carried out in two distinct steps involving contrasting types of expertise:

\begin{enumerate}
\item \textit{Statistics and/or physical expertise}: estimation of the initiator characteristics $x^z$ for a target frequency $z$, for example the 1000-yr flood, the 100-yr storm or the ‘reference maximal’ seism, and so on;
\end{enumerate}

\footnote{See Section 4.2.2 for more details.}
(ii) **engineering**: deterministic modelling and design of the consequences conditional to a documented target level.

**Step (i)** covers the probabilistic dimension of the risk criterion, and involves a typically extreme value statistical estimation of sample records for $x^a$ (cf. Chapters 4 and 5). Samples, that will be referred to as $X_n$ with size $n$, may require rather elaborate statistical modelling, all the more so when $x^a$ is a multivariate time series. In many cases, sample size $n$ is small enough compared to $1/a$ for the statistical fluctuations affecting the estimation of a rare quantile $x^a$ not to be negligible: those estimation uncertainties may be quantified explicitly within the definition of the risk criterion. For instance, the French risk criterion applicable to the nuclear power criterion incorporates the upper bound of the 70% bilateral confidence interval affecting the $x^a = 1000$-yr flood estimate within an initiator-frequency approach (Equation (1.3)); on the contrary, the corresponding one for hydropower does not incorporate it in a quantitative manner. In later sections we will return frequently to the critical issue of integrating the various layers of uncertainty involved in risk assessment:

- The frequency or return period (here $1/1000 \text{yr}$) measures the likelihood of the initiator, covering mostly-irreducible uncertainty due to the spatial-temporal variability of natural events. Some authors refer to it as encompassing the risk, or aleatory uncertainty or variability. Technically-speaking, it will also be called level-1 uncertainty in subsequent chapters, as it will be modelled by random variables directly representing the unknown physical state of the event.

- The confidence level (here 70%) refers to the imprecision of the frequency estimation due to data limitations, and possibly also the modelling errors or imprecision regarding the description of the local phenomena and consequences. It covers uncertainty that is – theoretically at least – reducible. Some authors refer to it as the epistemic uncertainty or simply uncertainty about the risk level. Technically-speaking, it will be called ‘level-2’ uncertainty as it will materialise in uncertain parameters affecting the level-1 random variables, not directly tied to the physical states.

Conversely, it may not be considered legitimate or practical to work within a probabilistic approach for **step (i)**. This is either because samples may not be significant enough, or because of a lingering epistemological controversy about the quantification of return frequencies for very rare catastrophic

<table>
<thead>
<tr>
<th>Type of hazard</th>
<th>Initiator (yr$^{-1}$)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flood</td>
<td>$1/100 - 1/500$ for residential areas</td>
<td>Additional margins are set up on power plants</td>
</tr>
<tr>
<td></td>
<td>$&lt;1/1000$ for nuclear power plants</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$1/10000$ for large dams</td>
<td></td>
</tr>
<tr>
<td>Storm/extreme winds</td>
<td>$1/100$ for power infrastructure network</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$1/50$ to $1/100$ for more standard buildings</td>
<td></td>
</tr>
<tr>
<td>Earthquake</td>
<td>$1/450$ (Eurocodes)</td>
<td></td>
</tr>
<tr>
<td>Sea levels</td>
<td>$1/1000$ for nuclear power plants</td>
<td>Variations may be found according to the conjunction of multiple hazards (tide, storm surge, estuarine flood, tsunami...</td>
</tr>
</tbody>
</table>
events. By convention, ‘reference maximal plausible events’ would then replace the \(z\)-initiator level, as is the case for earthquakes in France.

The deterministic nature of Step (ii) has the practical advantage of simplifying the studies and reducing the computational burden. Checking that the risk criterion is fulfilled involves essentially one run of the model \(G(.)\) representing the consequences of a given initiator for each design scenario. As will be developed in Chapter 7, managing the computational load is essential when drawing in elaborate numerical models to represent the physical phenomena involved in the risk situation. However elaborate the step (i) statistical modelling of \(x^{\text{en}}\) may be, the proposed simplification relies on the fact that the risk criterion involves a probabilistic target for just one real-valued initiator variable, excluding any probabilistic representation of the other sources of uncertainties. More elaborate probabilistic computations are required when the full probability of the undesired event (Equation (1.7)) replaces the deterministic checking of the undesired event for a given initiator quantile (Equations (1.5) and (1.6)). As a matter of fact, most engineers already carry out a few computations on the consequence models \(G(x^a,.)\) within deterministic sensitivity studies: testing, to some limited extent, the above-mentioned informal margins in components involving the potentially influential unknowns \(x^{\text{en}}\).

Much research work has provided evidence of the utility, if not the necessity, of formally integrating other sources of uncertainty so as to get a fairer picture of the risk and hence optimise the risk management strategies in a more comprehensive risk-informed approach. This has been done in extensive Bayesian settings, for instance, which offer a natural and solid foundation for a double-level probabilistic representation of aleatory/epistemic uncertainty. Bayesian settings have been advocated for hydrological and natural risk applications for years (de Groot, 1970; Krzysztofowicz, 1983; Duckstein and Parent, 1994) and in particular developed within the GLUE (generalised likelihood uncertainty estimation, Beven and Binsley, 1992) methodology and MUCM (managing uncertainty in complex models, http://mucm.group.shef.ac.uk Sheffield University program). Subsequent chapters will come back to the subject with more elaborate methods that will mostly integrate statistics and engineering steps into approaches with a higher computational cost.

It is noteworthy that, to a large extent, industrial practice retains an ‘initiator/frequency + margins’ approach. Such an approach will also be referred to as mixed deterministic-probabilistic in the rest of this book. In the nuclear industry, it is traditional to call it simply ‘deterministic’, since the largest part of the computational and design studies are treated conditionally with a given initiator and hence exclude any direct probabilistic treatment. More fundamentally perhaps than the computational issues, cultural limitations in acceptability often restrict probabilities to describing the natural hazards themselves rather than the more complete risk and uncertainty picture.

Note that the subject of natural risk assessment, particularly in its hydrological applications, is also a rich area of application for forecasting techniques targeting short- or mean-term predictions (e.g. for early-warning systems, flood routing or crisis management) rather than risk assessment involving extreme events. While the present section is dedicated to the latter, comments regarding the former can be found in section Section 1.5.

### 1.2 Engineering design, safety and structural reliability analysis (SRA)

This section concentrates on the issues associated with risks incurred by industrial facilities as the result of internal initiating failures or adverse events. In contrast, the preceding section involved natural initiators, hence external aggressions. The division between the two domains is very much a matter of tradition, and later chapters will offer generic approaches that show a common theoretical foundation.
Practices in industrial safety have nevertheless led to greater use and development of probabilistic risk assessment methods, such as structural reliability analysis (as reviewed below) or systems reliability (see Section 1.3).

1.2.1 The domain of structural reliability

Design of industrial structures, be they nuclear, aerospace, offshore, transport, and so on, has generated the need for some rules or codes to prevent failure mechanisms and secure reliability levels in the face of highly diverse sources of uncertainty affecting the operating systems (variability of material properties, of operational loads, fabrication tolerances, ...). Beyond empirical design margins, a whole range of methods is usually referred to as the structural reliability analysis (SRA) (Madsen, Kenk, and Lind, 1986). This domain is not disconnected from the previous considerations regarding protection against natural risk: in fact, much emerged from the design issues related to external events such as offshore sea waves upon oil facilities or extreme winds upon buildings and so on. However the research and engineering practices are somewhat different. Beyond the fact that the communities have generally distinct backgrounds – statisticians and geosciences for natural risk, reliability and mechanics for SRA – a more fundamental difference is that ‘modern’ SRA readily couples the system model with a more extensive probabilistic uncertainty model.

SRA considers a structure characterised by an event of interest or more generally a group of events leading to failure ($E_f$) Figure 1.2. Failure is a matter of structural definition: it may include a number of so-called failure modes, physical phenomena such as brutal collapse or just crack initiation. Those failures may occur under a certain number of conditions regarding two types of variables affecting system behaviour, namely the design variables (again noted $d$) and the physical variables (denoted as $x = (x_i)_{i=1...p}$). A failure function $G(x,d)$ – denoted as $G(x)$ in SRA whereby design options are implicitly included in $G(.)$ – encapsulates this knowledge of the different phenomena leading to failure. Be it a single mechanical model for one failure mode of a simple component, or more generally a series of sub-models describing each failure mode of each component of the system assembled through Boolean operators, it always consists of a deterministic

$$z_{pn}=G(z_{pn},d)>0$$

Failure probability below a threshold

$$P_f=P(E_f)=10^{-b}$$

Failure probability below a threshold

$$E_f=z|z=G(x,d)<0$$

Failure function $G(.)$

Risk (or design) criterion

Figure 1.2 Structural reliability analysis – schematisation.
relationship between $x$, $d$ and the failure event of interest with the following convention:

$$E_f = \{x | z = G(x) < 0\}$$  \hspace{1cm} (1.8)

For a given design $d$, the failure set (or failure domain) thus defines a set of values of $x$ leading to the event of interest $E_f$. It is a subset of the space of variation of the uncertain variables (noted $\Omega_x$). Associated definitions are given to the safe set or domain $E_s = \{x | G(x) > 0\}$ and to the limit state (or failure surface) $E_l = \{x | G(x) = 0\}$. The latter, representing a zero probability in non-degenerated cases, is essentially of mathematical/algorithmic interest.

Consider, for instance, the simplified example of the reactor vessel in nuclear safety. Failure could theoretically occur as a result of the abnormal pressure-temperature of the primary fluid, itself subjected to an internal initiator such as the drop in pressure following a pipe break elsewhere in the circuit. Stress upon a pre-existing flaw inside the vessel width could then exceed the resilience margin of the material resulting in a failure event either defined as the sudden rupture or, more conservatively, as the triggering of flaw propagation. Failure modelling involves a complex finite-element thermo-mechanical model $m = M(.)$ predicting stress and temperature fields as a function of numerous uncertain variables (properties of materials, flaw characteristics, the thermodynamics of accidental transients, the radiation received over time and the resulting fragilising, etc.) as well as design or operational conditions $d$ (such as temperature and pressure limits, prescribed recovery times, etc.). Hence a failure margin $z$ is computed by subtracting a stress intensity factor (noted $K_1$) from a toughness function (noted $K_{1c}$), both functions of $m$, defining altogether the following failure function $G(.)$:

$$m = M(x^1, \ldots x^p, d) = M(x, d)$$

$$z = K_{1c}(m, x, d) - K_1(m, x, d) = g(m, x, d) = g(M(x, d), x, d) = G(x, d)$$  \hspace{1cm} (1.9)

### 1.2.2 Deterministic safety margins and partial safety factors

As a matter of fact, the field of structural reliability has a long history of standards and regulations (Ellingwood, 1994), notably in risky industries such as the nuclear or aerospace industry. Regulatory criteria typically specify reliability requirements, namely an absence of failure over the system and/or per component. These are prescribed during a given period and for a given scenario, such as a conventional accident or stress history under hypotheses $d$ concerning the structure. Traditional regulations resemble to a certain extent the ‘initiator-frequency + margins’ approach mentioned above. Design is studied under conventional scenarios (such as pipe break, explosion, etc.) to which typical occurrence frequencies may be given, although generally on a more limited statistical analysis than for the natural initiators considered in the preceding section. A risk criterion then involves ‘penalising’ with safety margins the remaining uncertain variables $x$, that is to say applying coefficients or safety factors $f^i$ to their ‘best-estimate’ values $x_{be}$ and verifying reliability by deterministic calculation:

$$x_{pn} = (x_{be}^1 \cdot f^1, \ldots, x_{be}^p \cdot f^p)$$

$$z_{pn} = G(x_{pn}, d) > 0$$  \hspace{1cm} (1.10)

This approach is generally referred to in the industry – notably in nuclear design – as a deterministic approach or as an approach through ‘penalised scenarios’: it involves an elementary form of deterministic treatment of sources of uncertainty pre-supposing again that the function $x \rightarrow G(x,.)$
considered component per component $x^i$ is monotonous. This is a mostly intuitive situation in fracture mechanics (e.g. the greater the load, the greater the risk), but is less straightforward in fluid mechanics (where competing phenomena may trigger irregular bifurcations). As mentioned in the preceding section, it has the considerable advantage of limiting the number of computations to one or a few runs in potentially complex mechanical models. It also requires the identification of an upper limit (or a lower one, according to the sign of monotony) of plausible uncertain variation for every component $x^i$, both physically realistic and consensual amongst stakeholders. In practice, aside from informal physical expertise, that certain limit $x^i_{pn}$, noting the penalised value for $x^i$, can correspond approximately to the quantile $x^i_{a_i}$ for the component implicitly modelled as a random variable $X^i$ whereby:

$$P(X^i > x^i_{a_i}) = \alpha^i$$

(1.11)

A resistance property would be taken at its lower 5% value accounting for the variability of materials, while a loading variable would be taken at its upper 95% value accounting for lack of knowledge or partial randomness in the operating conditions. This is also referred to as a ‘partial safety factor’ approach (Ellingwood, 1994; Melchers, 1999), whereby safety factors are defined for each partial component $x^i$ of the vector $x$, altogether conditioning overall safety.

Important literature continues to argue about the interest and inherent conservatism of this kind of approach which aggregates potentially heterogeneous margins, reflected by the quantiles $\alpha^i$, in a barely controllable manner (cf. de Rocquigny, Devictor, and Tarantola, 2008 for a review). Remember that there are some distinctive operational advantages with this kind of approach: it enables one to reduce the often enormous number of scenarios down to a selection of hopefully conservative (if not representative) ones which are more carefully studied and given margins. It also leads to design codes which are much easier to enforce over, for example, large and heterogeneous sets of industrial products/installations than direct probabilistic targets leaving each single designer free to craft probabilistic distributions and possibly calibrate each system differently. Conversely, experience shows that it is quite difficult to translate partial safety factors or related partially deterministic approaches into an overall probabilistic risk level that could be compared to other risk situations. Chapter 4 will return to the underlying dependence issues and the interpretation of probability as a means to rank the relative likelihood of risks for decision-making.

### 1.2.3 Probabilistic structural reliability analysis

To circumvent those shortcomings, modern structural reliability has come to move from the partial safety to an extended randomisation of vector $x$, in a trend comparable to the extended frequency approach exposed for natural risk. Formally, the risk criterion (or design limit) defined in Equations (1.10) and (1.11) could be understood as a mixed deterministic-probabilistic criterion based on the conditioning of all components of $X$, as a distribution conditional to everything is simply a deterministic level:

$$z = G((x^i_{a_i})_{i=1,...,p}, d) > 0 \iff P\left[G(X, d) > 0 | (X^i = x^i_{a_i})_{i}\right] = 1$$

(1.12)

If $G(.)$ is not monotonous, an optimisation algorithm becomes necessary, thus multiplying considerably the number of required calculations. Such a ‘strongly deterministic’ approach is rarely applied in practice because of its tremendous computational challenges.
For some years now this approach has been compared with approaches known as ‘probabilistic’ that model explicitly all sources of uncertainty as random variables $X_i$. Probabilistic uncertainty modelling is developed upon the input space with the delineation of a joint probability density function $f_X$ for vector $x$, provided that all corresponding sources of uncertainties may be acceptably randomised. Hence, the risk measure is generally taken as the following failure probability:

$$p_f = P(E_f) = \int_{E_f} f_X(x) dx = \int_{\Omega_x} 1_{g(x,d) < 0} f_X(x) dx$$  \hspace{1cm} (1.13)$$

which should be kept close to zero. In fact, it is frequently found that only a part of the vector $x$ is randomised, say the first $m$ components $(x_i)_{i=1,...,m}$ out of the total vector of $p$ inputs. This comes down to a partial conditioning into penalised values of remaining variables such as internal initiators (e.g. reference accidents in nuclear safety). Furthermore, $p_f$ is compared to a threshold of $10^{-b}$, or at least the probability of a reference scenario $d^o$ considered as reliable enough if the specification of an absolute probabilistic threshold is too controversial. While these approaches are known as ‘probabilistic’, they may again be formalised as mixed deterministic-probabilistic where any of the two following risk criteria replaces that of Equation (1.12):

$$p_f(d) = P\left[G(X,d) < 0 \mid (X' = X_{pm}^{i=m+1:p}) \right] < 10^{-b}$$  \hspace{1cm} (1.14)$$

or:

$$p_f(d) = P\left[G(X,d) < 0 \mid (X' = X_{pm}^{i=m+1:p}) \right] < p_f(d^o)$$  \hspace{1cm} (1.15)$$

A key difficulty is related to the fact that SRA generally involves a rare failure event (now defined as the conditional event $E_f = \{x \mid (x_i = x_{pm}^{i=m+1:p}) \cap G(x,d) < 0\}$, that is to say the tail-end of the $Z$ distribution, together with rather CPU-intensive failure functions $G(.)$. The risk measure, a very complex multiple integral (Equation (1.13)), thus constitutes a great computational challenge which has generated considerable numerical research. Aside from efforts to reduce the variance of Monte-Carlo Sampling (MCS) through importance sampling techniques, specific strategies were developed to evaluate the probability of exceeding a threshold. For example, the First (resp. Second) Order Reliability Methods (FORM resp. SORM) may considerably reduce the number of $G(.)$ model runs in evaluating a very low $p_f$. As will be developed in Chapter 7, underlying approximations do rely crucially on the strong physical-mathematical properties of the failure function such as convexity or monotony: yet another example of the importance of combining physical and probabilistic knowledge in order to undertake accountable risk modelling, as will be discussed throughout the book. Last but not least, these methods also generate importance factors that is indices ranking the uncertain inputs $X'$ with respect to their contribution to the failure probability. More than the absolute value of the risk measure, this type of information may be contemplated in order to ameliorate the designs.

### 1.2.4 Links and differences with natural risk studies

Note the similarities between Figures 1.1 and 1.2: both approaches focus on a given event of interest (failure or the undesired/critical event in natural risk respectively), occurring in the system (the structure or the risk situation resp.) and represented by a system model function $G(.)$ (the failure function or the phenomenological model resp.). $G(.)$ depends on some uncertain variables $x$ corresponding to the former $(x''', x''')$ as well as to controllable design variables $d$ to be adjusted according to a given risk measure (the failure probability or the frequency of the event of interest resp.).
SRA goes into the full coupling of the system model and probabilistic uncertainty modelling, enabling the computation of an integrated probabilistic risk measure. While the corresponding computational difficulties may explain why most natural risk studies are restricted to the initiator/frequency approach, they have led to more enthusiastic developments in SRA with advanced numerical thinking. Yet some challenges and limitations remain:

- Unlike the previous domain, truly statistical modelling of the sources of uncertainties is often limited; accordingly, the statistical significance of the very low probability figures computed for \( p_f \) is still of concern although it was identified early on (Ditlevsen and Bjerager, 1986).
- Randomising of all sources of uncertainties, much beyond the practices in natural risk, has often the disadvantage of staying elusive as to the proper understanding of the underlying random experiments or sample space required to theoretically settle the setting. Frequentist interpretations being generally much trickier than with natural initiators, some authors interpret the results more as subjective probabilities for relative design comparison.
- Physical hypotheses (e.g. monotony, convexity) that underlie reliability approximations or the definition of risk criterion often remain insufficiently documented.

Beyond the mere checking of an absolute risk criterion, SRA lays large emphasis on importance factors, that is the ranking of uncertain inputs regarding their contribution to reliability, as well as on the relative comparison of contrasted designs through a risk measure (the failure probability).

1.3 Industrial safety, system reliability and probabilistic risk assessment (PRA)

Reliability and risk associated with industrial facilities are highly affected by their complexity, as those systems comprise numerous physical components organised into a wealth of functional chains. It may be hard to identify a modern elementary object which cannot be seen as a system in itself (e.g. a temperature captor); but think about the hundreds of thousands of such elementary pieces included in industrial facilities such as power plants, nuclear waste repositories or in industrial products such as airplanes, cars, and so on. SRA covers systems to a certain extent and has developed structural systems safety extensions to account for multiple-failure events such as those occurring in multiple-component mechanical structures (Ditlevsen and Bjerager, 1986). Nonetheless, practices in systems reliability have traditionally involved other approaches, denominated alternatively as Quantitative Risk Analysis (QRA), Probabilistic Risk Analysis (PRA) or even Probabilistic Safety analysis (PSA) in the nuclear sector (Bedford and Cooke, 2001). Similar to what was suggested in linking formally natural risk to structural reliability studies, subsequent sections will develop the theoretical continuum relating QRA to SRA, as already advocated in the literature, for instance by Aven and Rettedal (1998).

1.3.1 The context of systems analysis

The overall context (Figure 1.3) can be analysed in a similar framework to that of Figures 1.1 and 1.2. System reliability identifies one or several undesired event(s) of interest (or top event, noted again \( E \)) characterising the failure of the key functions of the system: severe reactor damage, airborne electrical shutdown, process unavailability and so on. This(ese) event(s) of interest affecting the system can be explained by a number of internal or external initiating elementary events (formally gathered inside the large vector \( E^{in} \)), as well as conditional disruption events representing system components or processes that fail to contain the initiating failure (vector \( E^{sy} \)). A quantitative system model, typically
based on fault trees or event trees, will predict the event of interest as a function of those inputs as well as of the decision or design variables \(d\). The undesired event of interest \(E\) thus becomes a logical function of all elementary events, a basic algebraic result of those trees, such as:

\[
E = \bigcup_i \left[ E_i^{\text{in}} \cap \bigcap_{j_i(d)} E_j^{\text{sy}} \right] = G(E_i^{\text{in}})
\]  

(1.16)

where, as a non-exclusive illustration, failure of the system is assumed to occur upon at least one of a set of initiator events \(i\) associated with a series \(j_i\) of conditional disruption events that could be mitigated by design (protection) choices \(d\). More comprehensively, complex events would actually involve a recursive use of Equation (1.16) as each of those \(j_i\) disruption events would themselves be the result of a sub-chain of ancillary initiators or sub-component disruptions.

The formula has a variety of equivalent formal interpretations: (a) it can be seen as a relationship between the events defined as subsets of states of nature; (b) it can be translated straightforwardly into a relationship between the probabilities (or frequencies) associated with those events; and (c) it can also be translated into a deterministic function between the indicator variables (now noted \(e\), in lowercase) representing each precise elementary state of the system components or initiators \((e = 1\) in the case of initiator realisation or component failure, \(e = 0\) otherwise):

\[
e = \sum_i \left[ e_i^{\text{in}} \cdot \prod_{j_i(d)} e_j^{\text{sy}} \right] = G(e_i^{\text{in}}, e_j^{\text{sy}}, d)
\]  

(1.17)

In that latter case, the system model \(G(.)\) represents the deterministic causality – or at least a presumably-strong dependence – between all sub-events or states of the system components and the final state regarding the undesired event. It constitutes the output of a functional analysis of the system. In real studies, Equation (1.17) may be much more complex than a simple sum of products, either because it is a
conservative approximation of the exact Poincaré formula (see Annex Section 10.2), or even more so because of the complexity of sub-systems. In general, it will appear as a deterministic function of elementary states (initiators or conditional processes), however numerous those may be. Think in the thousands at least for the nuclear PSA.

Starting from that functional description, probabilistic analyses assign to all elementary events their corresponding frequencies or conditional probabilities, according to whether they are initiator or conditional failures (see Chapter 4):

\[
P(E^{in\ i}) = P(1_{Ein\ i} = 1) = f^i \quad P(E^{sy\ k}) = P(1_{E_{sy\ k}} = 1) = p^k
\]

Such figures are estimated either through component failure statistics or expert opinion. Note that the dependence phenomena between elementary events are additional key features to be estimated through probabilities of common modes. Equation (1.17) yields a relationship between all those elementary values and the frequency of the undesired event \( f^e \), which represents the risk measure of the QRA:

\[
c_r(d) = f^e = G(\{f^i\}, (p^k)_k, d)
\]

That risk measure can then be compared to a risk acceptance criterion such as ‘system failure should be less frequent than \(10^{-9}\) per flight-hour in the aerospace industry, or \(10^{-6}\) per plant-year of operation in the nuclear’, as illustrated in Table 1.2.

Note that the wording ‘risk acceptance criterion’ should be used within a limited perspective of a prescribed regulation or standard, notwithstanding the much broader and largely debated topic of risk acceptability. Though it largely exceeds the modelling scope of this book, Chapter 2 will return to some extent to the issue in the sense that a risk criterion should always be considered as a means to rank relative options, costs and benefits, never as an absolute statement. Even if very small, the residual risk of large radioactive release due to nuclear plant failure is never acceptable as such. Though risk perception and a larger societal debate have their say beyond purely technical measures, the residual risk could become less unacceptable perhaps from the perspective of the alternative residual risks of equivalent power production: think of a dam break in a hydropower plant or of the unpredictable effects of climate change due to the major CO\(_2\) release of thermal power plants. In some cases indeed the risk measure may be formulated explicitly as a relative index so as to compare design choices or operation and maintenance modifications to a standard design or operating process. This is the case in the US nuclear field, where the Nuclear Regulatory Commission allows for changes in operational procedures provided the following risk measure does not deviate from that of the reference design.

### 1.3.2 Links and differences with structural reliability analysis

A simple reformulation can closely link this formula to the fully probabilistic risk measures mentioned in preceding sections, viz. the extended frequency approach of natural risk or the failure probability in SRA. Consider the system model as a deterministic function of the vector of elementary states \( x = (e^{in}, e^{sy}) \) characterizing the overall system state. A set of elementary probabilities for each component \( e^i \), which are two-state Bernoulli random variables, plus a dependence structure consisting of, for example, common modes by pairs, is read as a discrete joint probability density upon the vector \( x \) of discrete random variables. The frequency of the undesired event (Equation (1.19)) appears then as the equivalent of the SRA failure probability:

\[
f^e = P[G(e^{in}, e^{sy}, d) = 1] = P[G(X, d) = 1]
\]
**Table 1.2** Risk acceptance criteria (in yearly frequency) in various industries.

<table>
<thead>
<tr>
<th>Industry</th>
<th>Targets (yearly frequency per plant)</th>
<th>Targeted individual risk per person per year</th>
<th>Observed Accident Rate (frequency of fatal accidents per year)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nuclear plants - present (future)</td>
<td>Internal failure (core damage) $10^{-4}$ ($10^{-5}$) (^i)</td>
<td>$10^{-6}$ (Netherlands)</td>
<td>$\sim 10^{-4}$ internal system failure, but $2-4.10^{-5}$ fatalities</td>
<td>Considering about 10 000 plant-years and a conservative figure of 2000 deaths in all civil accidents, amongst 5000–10 000 average close inhabitants to plants</td>
</tr>
<tr>
<td></td>
<td>External release of RN (LERF) $10^{-5}$ ($10^{-6}$ to negligible)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aerospace</td>
<td></td>
<td>$\sim 10^{-6}$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Car</td>
<td>$10^{-4}$ if large exc., or $10^{-3}$ if normal (USA)</td>
<td>$10^{-6}$ (^m)</td>
<td>$1.10^{-4}$ (^f) to $2.10^{-4}$ (^h)</td>
<td></td>
</tr>
<tr>
<td>Bridges or civil structures</td>
<td></td>
<td>$&lt; 10^{-6}$ (UK) (^m, h)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traffic accidents</td>
<td></td>
<td>$1.10^{-4}$ (^j) to $3.10^{-4}$ (^h)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>All accidents</td>
<td></td>
<td>$3.10^{-4}$ (^j) (Japan) to $5.10^{-4}$ (USA)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>All deaths</td>
<td></td>
<td>$\sim 8.10^{-3}$ (^j) to $1.10^{-2}$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\(^a\)One decade less when excluding external hazard initiator.  
Source: \(^m\) (Menzies, 1995); \(^i\) (Nuclear Safety Commission of Japan, 2004); \(^j\) (IAEA, 2005); \(^h\) (Madsen, Kenk, and Lind, 1986); \(^f\) French car statistics.
where:
\[ X \sim f_x = \{ (f^i)_j, (p^j)_i \} \]  \hspace{1cm} (1.21)

In that respect, QRA appears as formally similar to SRA. Key practical differences remain however:

- In QRA, the Boolean nature of the system model \( G(.) \) and of model inputs \( x \) simplify considerably the computation of the risk measure, since the complex multiple-integral of SRA (Equation (1.14)) becomes here a closed-form expression (Equation (1.17)).
- Conversely, the size of \( x \) and the associated dependence structure, reflected in the logical model (fault/event tree building) and the common mode probabilities, are generally much more complex in QRA than in SRA.

Chapters 7 and 5 respectively will discuss in more detail those two essential remarks which bear an importance beyond the mere comparison of QRA and SRA. Boolean discretisation is a powerful tool to simplify the computation of risk measures such as failure probabilities even in phenomenological models departing from the logical reliability models. Functional analysis through fault trees and common mode quantification is also a powerful tool to help model complex phenomenological dependence in a tractable way.

1.3.3 The case of elaborate PRA (multi-state, dynamic)

Systems analysis involves other methods than fault trees and event trees. These basic tools do not represent the dynamic reliability phenomena, and become tricky to use if elementary events behave closer to multi-state than to simple Boolean variables. Yet, much of the observations made above remain unchanged.

Multi-state static models such as Bayesian Belief Networks (BBN) (cf. for example Kurowicka and Cooke, 2006) generalise the deterministic functional dependence coined in Equation (1.17), insofar as they link the undesired event \( e \) to multi-state indicator variables \( e^{i\text{in}} \) and \( e^{i\text{sy}} \) representing the state of initiator events or conditional processes:

\[ e = G (e^{i\text{in}}, e^{i\text{sy}}, d) \]  \hspace{1cm} (1.22)

Accordingly, the computation of the risk measure \( f^e \) involves discrete probability distributions and conditional dependence structures generalising Bernoulli distributions and common modes. This can still be interpreted as a failure probability being the image of a joint pdf on the vector \( x \) of multi-state events through \( G(.) \). Closed-form expressions still result in general, albeit of large dimension because of the multi-state features.

Dynamic reliability approaches (e.g. under Markov chains, Petri networks, etc.) are developed to account for the temporal variation of reliability characteristics as well as the time-dependent combinations of causalities. Think of the contrasted consequences of the failure of the \( i \)-th component occurring before or after failure of the \( j \)-th; or of emergency system actions with uncertain response delays, which modify the subsequent event tree. Then the prediction of \( e \), at time \( t \) draws in a time-dependent stochastic operator to the dynamic system: Equation (1.22) is replaced by Piecewise Deterministic Markov Processes (PDMP), stochastic differential equations (SDE) and so on. The probabilistic description of time-dependent elementary states of the system \( e^{i\text{in}}, e^{i\text{sy}} \) involves time series instead of standard random variables. Risk measures, such as the expected time to failure or expected dependability of the system, are not closed-form anymore. They still appear however as elaborated integral functions of the system model, depending on the uncertain model inputs represented by time series \( X \), as well as on the possibly time-dependent design actions or maintenance strategies \( d \)
such as the following expectation:

\[ R = E[G(X_t, D_t)] = \int g[X_t, D_t] dW_s \]  

(1.23)

Note that more sophisticated mathematical tools may then be necessary, such as the use of stochastic integration over the entire trajectory \( s \in [0, t] \) of the stochastic processes \( W_t \), representing the sources of uncertainties perturbing the time-dependent system state represented by \( X_t \).

Although this domain is specific to a large extent, it has, like the previous situations, the risk measure appearing as an integral of the system model along random distributions, so it may theoretically use Monte-Carlo simulation similarly to SRA. Practical approximations have to be made generally due to computational costs of the system model over a large time interval and hence a large number of discretised time steps: those may be quite different to that of SRA owing to the stochastic nature of the time-dependent integral (Equation (1.23)). This may include the complete replacement of the system model by dedicated mathematical formulations allowing for closed-form integration to avoid the excessively costly convergence of Monte-Carlo.

### 1.3.4 Integrated probabilistic risk assessment (IPRA)

Consider now the elaborate risk studies within which several of the previously introduced layers are being put together, such as:

- a central (logical) system model with some functional complexity described by QRA, denoted as: 
  \[ e = G_s(e^{in}, e^{sy}, d^{f}) \],
- an ‘upstream’ natural risk component plugged in as a more detailed description of one of the initiating events \( e^{in} = G_n(x^{in}, x^{en}, d^{n}) \) affecting the central system,
- a ‘downstream’ consequence phenomenological model further describing the impact of undesired functional failure of the system \( e \) into variables of interest \( z = G_c(e, x^c, d^c) \) quantifying the detrimental consequences (such as plant unavailability costs, large release of pollutants, number of fatalities . . .) as a function of supplementary variables \( x^c \) modifying the detriment for a given \( e \) (meteorological conditions, vulnerability, etc.).

This is the case for some of the most elaborate American nuclear risk assessments, such as the Waste Isolation Power Plant performance assessment (Helton et al., 1996), or the NUREG-1150 studies (NRC, 1990). It is also the setting of the ARAMIS European project (Salvi and Debray, 2006), cf. (Figure 1.4), whereby that central logical system model is thought of as a chaining of a fault tree from initiators to the central undesired event and an event tree predicting the consequences from the central undesired event. Consequence prediction could couple a logical model, viz. an event tree, and a phenomenological model, typically a physical-chemical or environmental model predicting the extension of the explosion or the accidental pollutant spill.

A further refinement could be to plug inside the central QRA system model an SRA-type model. This would mean detailing one of the QRA conditional failure events, such as the breaking of the vessel, as a result of the initiating event plus some system failures. By considering a similar structure for each layer, the global approach can be viewed as a simple chaining of each:

- the final variables of interest are defined as those of the consequence model \( z \),
- the vector of uncertain inputs (resp. of design actions) consists in concatenating all vectors of input states or variables of the three models \( x = (e^{in}, e^{sy}, x^{in}, x^{en}, x^c) \) (resp. \( d = (d^f, d^n, d^c) \)).
a compound deterministic function represents the overall system model as follows:

\[
z = G_c \circ G_s \circ G_n (e^{in}, e^{sy}, \chi^{in}, \chi^{co}, d^{ii}, d^{in}, d^{co}) = G (x, e, d) \tag{1.24}
\]

The single (output) undesired event of interest is replaced by a whole spectrum of consequences, hence described by a vector of variables of interest \( z \). The associated risk measures are multifold:

- (discrete level-based) a discrete collection of probabilities (or frequencies) corresponding to a set of selected representative levels of consequences,
- \((ccdf)\) a curve of probabilities to exceed a continuous level of \( z \) for a given type of consequences.

The second option does correspond to the formal consideration of the cumulative distribution function (cdf) of the variable of interest \( z \), or rather it’s complementary which is traditionally preferred under the denomination of ccdf (Helton, 1993). This can be understood as equivalent to one of the options available to formalise the well-known Farmer curve (or risk profile) relating to severity and frequency (Figure 1.5-right). Note that assessing consequences for various aspects such as cost, number of fatalities, cumulated dose emitted and so on, generates a set of ccdf for each component \( z^k \). Practice, inspired by regulations, tends to focus eventually on a discrete level-based risk measure. While the whole risk curve may be simulated, risk criteria generally refer to the exceedance of one or a few thresholds, such as that associated with the Large Early Release Frequency (LERF) in the nuclear field. This comes down to considering the likelihood of a discrete set of consequences \( (z_1, z_2, \ldots) \) or equivalently a discrete set of undesired consequence events defined as \( E_1 = \{z \mid z > z_1\} \), \( E_2 = \{z \mid z > z_2\} \) and so on.

Both options require a probabilistic model to be set up to describe the amount of uncertainty in each input of the chain: distribution of the initiating events or hazard variables, elementary failure probabilities of the internal system components, conditional probabilities and variability of uncertain consequences and so on. Hence, computing the ccdf of the consequences or the probability of exceeding a given

---

**Figure 1.4** ARAMIS Risk model for IPRA, adapted from (Salvi and Debray, 2006).
undesired threshold involves the following global integral:

\[ c_z(d) = P(z > z_s) = 1 - F_Z(z_s) = P(G(X, E, d) > z_s) \] (1.25)

Given the mix of continuous and discrete variables involved, computation typically resembles that of a chaining of SRA and QRA. Simplifications of the inner integral, similar to QRA involving the logical models, bring it down to closed-form conditional probabilities, leaving an SRA-type integration for the part that includes phenomenological models (see Chapter 7).

Yet a complete picture of the risk measures and computations involved requires raising the issue of the level-2 uncertainty affecting the risk components. As already mentioned in Section 1.1.2, data and expertise limitations raise the issue of the accuracy of failure probabilities of components (with respect to the potential common modes, that is non-independent behaviour of component failure), of frequencies of extreme initiator events, or of rare conditional consequences. This issue appeared rather early in the history of nuclear probabilistic risk analysis, as the famous first full-scale IPRA ever undertaken in a nuclear plant (Rasmussen et al., 1975) – the Reactor Safety Study, also known as the WASH report – was quickly criticised on these grounds (Lewis et al., 1979). Hence, models of level-2 epistemic uncertainty in the parameters of the core probabilistic model were developed. A long debate took place on the subsequent classification of the large variety of uncertainties encountered in large industrial systems into two types, namely the aleatory (or irreducible, variability) and epistemic (or reducible, lack of knowledge) categories. The rationale for explicitly separating those two categories into two levels inside the decision-making criteria has been discussed accordingly (Apostolakis, 1999; Oberkampf et al., 2002; Aven, 2003). Subsequent chapters will return to that key concept. Note that computations depend critically on the choice made at that level and incorporated into compound risk measures. A level-2 uncertainty model transforms the ccdf curve illustrated in Figure 1.5 into an uncertain curve, or in other words into a set of ccdf indexed by the level-2 confidence level as illustrated in Figure 1.6.

Indeed, denoting \( \theta_{XE} \) as the vector of parameters of all input distributions of the global model, the ccdf depends on its value:

\[ 1 - F_Z(z_s) = 1 - F_Z(z_s | \theta_{XE}) = P(G(X, E, d) > z_s | \theta_{XE}) \] (1.26)

so that the ccdf becomes a random function when a level-2 uncertainty model transforms those parameters in a random vector \( \Theta_{XE} \sim \pi(\Theta_{XE} | \zeta) \). A variety of compound level-2 risk measures have been contemplated in IPRA practice and discussed in the literature. The expected ccdf (expected over the
level-2 distribution \( \pi(\cdot) \) may be the most popular one, possibly because of its simplicity:

\[
c_z(\mathbf{d}) = E_\pi[1 - F_Z(z_j | \Theta_{XE})] = E_\pi[P(G(\mathbf{X}, \mathbf{d}) > z_j | \Theta_{XE})]
\]  

(1.27)

Another common one is the (level-2) probability or confidence that the (level-1) frequency will exceed a given threshold of consequence while remaining below a risk target \( z \) (say \( z = 10^{-6} \)):

\[
c_z(\mathbf{d}) = P[1 - F_Z(z_j | \Theta_{XE}) < z]
\]  

(1.28)

Both involve elaborate integration of the chained model \( G(.) \) with significant computational consequences (see Chapter 7). Those two risk measures exhibit different decision-theory properties and associated protection margins and costs (see Chapter 4). The kind of chained model involved in such elaborate risk studies and the variety of associated risk measures will also be illustrated by the pedagogical example in Chapter 3.

Although beyond the scope of the book, note also that the continued debate in the 2000s also suggested some extra-probabilistic extensions whereby the second level (or epistemic uncertainty layer) is modelled through Dempster-Shafer or evidence theory (see review in de Rocquigny, Devictor, and Tarantola, 2008), possibilistic distributions or fuzzy sets (see Helton and Oberkampf, 2004) on top of a probabilistic layer for aleatory (level-1) uncertainty.

### 1.4 Modelling under uncertainty in metrology, environmental/sanitary assessment and numerical analysis

The concept of uncertainty was already an essential part of the domains reviewed previously: every type of risk analysis comprises some statement about uncertainty . . . or else the risky event becomes a certainty. It is not the purpose of the present section to discuss in epistemological terms the specificities of uncertainty as differentiated from risk: Chapters 2 and 4 will return to that point. Observe so far that, beyond the domain of risk analysis as such, the study of uncertainty affecting the results of any modelling or measurement effort has involved some dedicated approaches. Those are referred to as uncertainty and
sensitivity analysis (UASA). They stand beyond the explicit risk analysis as they do not model risky events and consequences in the sense of serious accidents. Consider for instance:

- Metrology;
- quality control in industrial processes;
- qualification and calibration of numerical codes;
- environmental or sanitary impact analysis;
- quantitative project management;
- climate studies;
- and so on.

### 1.4.1 Uncertainty and sensitivity analysis (UASA)

Notwithstanding the variable terminologies in sub-domains, several authors have pointed to a generic underlying methodological structure to the UASA studies (Helton et al., 1996; de Rocquigny, Devictor, and Tarantola, 2008). Figure 1.7 sketches the conceptual framework advocated by de Rocquigny, Devictor, and Tarantola (2008) in a format comparable to the previous Figures presented in this chapter. UASA studies involve considerable similarities: a pre-existing model – anything from the simple analytical operations describing a basic measurement chain to the complex finite element model of air pollution transfer – is the central object of interest. It is studied as to how sources of uncertainties affecting its inputs affect the outputs. UASA studies tend to privilege output variables of interest rather than events of interest in the absence of risky events. In the UASA studies, it is also useful to distinguish between:

- full decision criteria, which correspond to risk acceptance criteria. For instance: the metrological chain should issue a measurement with a maximum of 3% uncertainty (generally a given multiple of the coefficient of variation); pollutant discharge should not exceed the licence threshold with 95% confidence (or 95% of the time variability) and so on.
quantities of interest, which correspond to risk measure. For instance: a coefficient of variation representing the output variability or inaccuracy; a quantile; or a maximal deterministic range of variation and so on.

In many studies, particularly in the numerical modelling activity or other upstream stages, there are no (or not yet clear) external regulatory or formal decision-making processes to abide by and hence no predetermined criterion for the question: ‘how much uncertainty affects my predictions?’ Assessing uncertainty in terms of some given quantity is however inevitable, although sometimes implicit. The question ‘how much uncertainty?’ is often answered on the basis of the variance or coefficient of variation of the output. However, it is sometimes forgotten that the appropriate approach and answers given could be quite different if one referred to the maximal deterministic range or a one-sided confidence interval: this is where the choice of a quantity of interest comes up.

On the input side, UASA also distinguish uncertain model inputs (vector $x$) from fixed ones (vector $d$). Note that the allocation of the model inputs between ‘uncertain’ and ‘fixed’ ones is often a matter of choice rather than theoretical discussion. It can change over the course of the study and of the decision-making process. Importance ranking/sensitivity analysis and model calibration steps do play key roles with respect to that choice, as will be commented upon later.

An uncertainty model is built upon the uncertain inputs, through various probabilistic or non-probabilistic settings. Central practice consists in the classical one-level probabilistic setting: this means randomising all sources of uncertainty – be they temporal, spatial or population variability, lack of knowledge on model parameters, measurement errors, and so on – affecting vector $x$. This is summarised into a pdf with independent or dependent inputs if appropriate, provided information is available to quantify them. The variety of settings already mentioned previously on natural risk, structural safety or integrated PRA can also be found: mixed deterministic-probabilistic settings (e.g. with some penalised fixed inputs) or even double-level probabilistic settings distinguishing so-called aleatory from epistemic components. Indeed, double-level probabilistic settings materialise naturally when undertaking an uncertainty study on the parameters of a pre-existing QRA or IPRA model. As mentioned above, the risk measure of a QRA is expressed as the following deterministic relation between the frequency of the output event and those of the elementary input events:

$$c_z(d) = f^o = G_i(f^i), (p^k)_k, d$$

Hence, an uncertainty study of its parameters results in developing a probabilistic model upon the frequencies and probabilities $(f^i), (p^k)_k$ themselves, the resulting quantities of interest being, for instance, confidence levels on the frequency of the undesired event. Research work (Helton and Oberkampf, 2004; Limbourg,) has also explored the use of extra-probabilistic settings for these kinds of applications, such as Dempster-Shafer Theory (DST).

A formal distinction is drawn classically between two types of study: uncertainty analysis (or uncertainty propagation) denoting the quantification of the uncertainty in the outputs inside the appropriate quantities of interest; and sensitivity analysis denoting the apportioning of that output uncertainty into each component of the uncertain inputs and the ranking of importance of those with respect to a given quantity of interest. Such interpretation of the terms is not always as clear-cut, so that sensitivity analysis may less appropriately designate elementary treatments such as the one-at-a-time variations of the inputs of a deterministic model or the partial derivatives; elsewhere, it may denote the entire UASA effort of understanding and managing a model in the context of uncertainty.
1.4.2 Specificities in metrology/industrial quality control

In the domain of metrology or quality control, uncertainty analysis is a basic requirement associated with the qualification of any measurement device, chain of devices or production process. Through sensitivity analysis (although the term is less classical there), it is also a forcible means to optimise costs and productivity of monitoring and quality control investments. It may sometimes be officially regulated, such as in nuclear maintenance, radiological protection or environmental control. For instance, in the application of European undertakings relating to the section of the Kyoto protocol concerning industrial emissions, a system of CO₂ emission permits has been established; it requires an explicit uncertainty declaration in order to secure fairness between real emissions and emission rights (Figure 1.8).

A metrological UASA study consists typically in aggregating the uncertainties associated with each variable \( x^i \) representing the result associated with each \( i \)-th operation or elementary sensor (e.g. flow metering of fuel, analysis of carbon content, net emission factor...) within the generally simple analytical function \( z = G(x) \) expressing the final measurand \( z \), for example the annual tonnage of CO₂.

In the field of metrology of industrial processes, the use of a probabilistic uncertainty model is rather common and quite standardised by the ‘Guide to the expression of uncertainty in measurement’ (ISO, 1995). Rather than aggregate elementary uncertainties in a deterministic manner, it assumes that uncertainty associated with each sensor or measurement operation in comparison with a reference value has an aleatory character that is modelled efficiently by probability calculations. Such uncertainty includes: noises affecting the operation of the sensor, local fluctuation of the measurement point around the average physical quantity sought, error in reading a counter or in rounding the measurement displayed, and so on.

The quantity of interest mostly involved is the so-called ‘enlarged uncertainty’, defined either as the ratio of the half-extension of a 95%-confidence interval around the expectation of \( z \):

\[
\% \text{unc}_z = \frac{1}{2} \frac{E(Z)}{E(Z)} \left( z_{\text{up}} - z_{\text{low}} \right)
\]  

(1.30)

or, more approximately, as a multiple of its coefficient of variation:

\[
\% \text{unc}_z \approx k \cdot \frac{\sqrt{\text{var}(Z)}}{E(Z)} = k \cdot c_V(Z)
\]  

(1.31)

Figure 1.8 Thermal power plant emissions (left) and metrological steps (right), (de Rocquigny, 2006).
where \( z_\beta = F_Z^{-1}(\beta) \) designates a quantile, \( F_Z \) standing for the cumulative distribution function of \( Z \). The so-called enlargement factor \( k \) is being taken as 2, 3 or an intermediate value depending on the case. A typically associated decision criterion requires it should not exceed a given threshold, such as 3% maximal uncertainty in the declared value.

Uncertainty modelling is generally simple in metrology. While correlation coefficients represent dependences, fully Gaussian uncertainty models are selected: this is sometimes supported by an argument based on the symmetry of errors and the existence of multiple underlying additive physical phenomena. The fact that the uncertainties are bounded (for example because of a command and control mechanism) may nevertheless lead to the choice of a uniform or even triangular pdf.

Note, however, that the level-2 uncertainty associated with the estimation of the uncertainty of elementary devices is sometimes included explicitly in metrological uncertainty modelling. Think of the fluctuation of a sampling statistic \( s^2_X \) in small samples around the real unknown variance \( \sigma^2_X \). For instance, repeatable data-based empiric variances can be multiplied by a factor greater than 1, decreasing with the number of measures \( n \) used to estimate it, instead of simply taking the gross estimated value. This accounts for the possibility, through the effect of sampling fluctuation, of under-estimating the unknown true variance. The practice is heterogeneous, because \( n \) is not always known to the industrial end-user. This question becomes particularly important when the cost of determining sources of uncertainty is high, because of the necessary tests involving burdensome basic operations. Consider the reception of nuclear fuel assemblies before reloading in a power plant: the measurement process is very demanding, but the risk associated with too great a level of uncertainty is serious, since mistaken acceptance of a fuel assembly too large for the core grid would result in the costly unavailability of the plant.

Propagation, that is the computation of the quantities of interest, involves mostly the so-called ‘uncertainty propagation law’, which is a Taylor-first order approximation of the variance of the variable of interest:

\[
E(Z) \approx G(E(X))
\]

\[
\text{Var } Z \approx \sum_{i=1}^{p} \left( \frac{\partial G}{\partial x^i} \right)^2 \text{Var } X^i + \sum_{i \neq j}^{p} \frac{\partial G}{\partial x^i} \frac{\partial G}{\partial x^j} \text{Cov } (X_i, X_j)
\]

Chapter 7 will discuss the fact that it constitutes indeed an elementary propagation method. Such an approximation relies essentially on the linearity of the system model, well suited to the purpose when the uncertainties are generally small enough with regard to the scale of potential non-linearities of \( G(.) \).

### 1.4.3 Specificities in environmental/health impact assessment

Environmental or sanitary impact assessments comprise numerous modelling layers, such as: emission analysis, physical-chemical reactions and local or regional transport through one or multiple media (air – gaseous or aerosol, water – dissolved or suspended, soil, . . .), bio-exposition models, dose-effect, toxicological models, epidemiology, external costs and so on. UASA studies have been developed for decades to understand and contain with better confidence the uncertain impact of emissions or activities (Granger Morgan and Henrion, 1990; Frey and Rhodes, 2005). As a matter of fact, the area is fraught with a wide range of sources of uncertainty: either due to the hard task of modelling complex coupled systems and sometimes poorly known phenomenologies, discrepancies between expert opinions, the lack of data, or simply the fundamental variability characterising environmental or biological systems and populations.
In reference to the previous areas, the following features and specificities can be noted:

- Risk measures are typically quantiles: 95% quantile of concentration of a pollutant in the discharge, $10^{-3}$ received dose of a potentially harmful compound and so on.
- The choice of distinguishing or not variability from uncertainty is an important point: this results in single or double-level probabilistic settings which are theoretically very similar to those encountered in the aleatory/epistemic debate in IPRA.
- Highly numerous uncertain model inputs are encountered, with a comparatively low amount of data. This implies an extended use of expert elicitation and of Bayesian settings which are much more developed than elsewhere.
- The absence of unique or well-defined pre-existing models, the widely-recognised need for calibration (Beck, 1987) and the interest for machine learning or data mining-inspired techniques (e.g. (Gauthier et al., 2011) on cancer risk score).

The latter two points might be the more challenging with regard to modelling. This may be understood in the context of the intrinsic complexity and variability of the mineral or organic environment: this happens in the geological, hydrological or sedimentology fields, or with even greater complexity at the biological, ecological or health levels. The phenomenology is generally less controlled than in man-made structures or systems. The dissemination of chemical compounds in a river environment, for instance, involves many types of transfer between water-borne dissolved or suspended, sediment-borne, or living matter-borne compartments, each of which may be modelled with variable levels of geographical or phenomenological detail. Only a handful of sample measurements may be available to inform and calibrate such models. Moreover, in the absence of data, quite controversial ranges may be found for the plausible variability of the environmental coefficients which additionally depend on the type of model to which the coefficient is an input. Besides standard uncertainty treatments such as the use of Monte-Carlo simulation, the issue of model building, selection and calibration has seen greater development than elsewhere. The following section and Chapter 6 will discuss that important issue.

1.4.4 Numerical code qualification (NCQ), calibration and data assimilation

The prevalence of uncertainty considerations has grown considerably in the field of numerical analysis in the 2000s. In fact, they may be traced back to the late 1970s in nuclear thermal-hydraulic codes (Cacuci et al., 1980), or indirectly to the very beginning of computer science after World War II. Monte-Carlo Sampling may be viewed as the very historical origin of computing: recall that Von Neumann’s ENIAC machine in 1946 was designed essentially for Monte-Carlo neutronics. Yet, probabilistic sampling was fundamentally thought of as a solver of the neutron equations for given (fixed) input conditions owing to the underlying statistical physics; which does not represent the type of macroscopic uncertainty now prevalent in risk and uncertainty analysis.

The above-mentioned structure of UASA encompasses the typical issues raised: $G(.)$ represents a complex numerical function resulting from numerical solvers of physics-based integral-differential operators (e.g. a neutron calculation in a nuclear core). It often takes in large-dimension vectors of continuous inputs $x$ and outputs $z$ that discretise multi-variate functional inputs/outputs representing variable fields or time transients. Typical examples are fluid velocities or temperatures, stress fields and so
on. Input parameters are affected by all sorts of uncertainties and what is looked for is, by order of subjective priority:

- ranking sensitivities of the outputs to the numerous inputs,
- rating an ‘order of magnitude’ of output variability, the quantities of interest being mostly variance or coefficient of variation and, more rarely, quantiles,
- calibrating a code against experimental data and testing facilities,
- updating the code prediction with new data to be assimilated.

Owing to the strong numerical background, derivatives have been playing a key role in the uncertainty and sensitivity techniques considered. They were firstly involved in ‘one-at-a-time’ deterministic sensitivity analysis and later through Taylor-first order approximations of the output variance. Although completely identical to metrological techniques from a probabilistic point of view, the numerical strategies deployed to obtain the least costly calculation of derivatives appearing in the formula led to the use of a variety of names: by direct derivative = Direct Sensitivity Method (DSP), or by adjunct derivative = Adjoint Sensitivity Method (ASM), (see Cacuci et al., 1980), or else the ‘method of perturbations’ or the ‘method of moments’. These appellations sometimes refer to the deterministic propagation of uncertainties or alternatively the estimation of other probabilistic moments through differential developments of an order higher than one. Since the year 2000, sensitivity ranking has incorporated more sophisticated sensitivity analysis techniques such as polynomial chaos expansions, which develop the input/output joint distributions on a much more powerful basis than Taylor series (Ghanem, 1990; Sudret, 2008). In general, these developments refer implicitly to variance as a quantity of interest. Gaussian or Uniform uncertainty models are used with comparatively less effort devoted to statistically estimating those models from real field data. Indeed, from a numerical analysis point of view, probabilistic sensitivity analysis may be seen as a powerful exploration tool over spaces of possible values for systems which may not yet exist, as is the case with upstream design stages (de Rocquigny, Devictor, and Tarantola, 2008).

Unlike the area of risk analysis, environmental or metrological studies, there is a virtually-unanimous consensus on sticking to simple probabilistic models mixing all sources of uncertainty within a single layer. Yet, in the particular domain of nuclear thermal-hydraulics which has considerable historical significance, it is traditional to account for a second probabilistic level in order to cover the numerical sampling limitations placed upon the (computational) estimation of an output quantile. The so-called Wilks method, based on (Wilks, 1941) though well beyond the scope of his initial work, implies the estimation of a ‘95 95’ level for the output variable of interest. As will be discussed in Chapter 7, it is in fact a very robust technique to cover propagation uncertainty or error that is generated by a low number of Monte-Carlo runs on a costly numerical code. On the contrary, such sampling uncertainty is not accounted for in the mechanical models that were historically behind the structural reliability techniques mentioned above. Indeed, thermal-hydraulics models provide evidence of a response that is far more irregular for inputs in general and hence amenable to potentially rougher output distributions and slower resulting convergence.

An essential area of historical development has been with regard to the issue of experimental calibration (or qualification, or Verification and Validation) and data assimilation; the former typically in nuclear code building (Boyack, 1990) and the latter in meteorology (Talagrand, 1997). Closely related are the fields of parameter identification (Beck and Arnold, 1977; Walter and Pronzato, 1997) or model identification already mentioned in the environmental domain (Beck, 1987). All involve the comparison between model outputs and experimental data resulting in the calibration of input parameters that are more or less unknown, the estimation (and generally reduction) of model-measurement residual error, and possibly the dynamically-updated prediction of outputs (in the case of dynamic data assimilation). These are, for example, initial conditions and resulting atmospheric indicators in meteorology. It is necessary at
this stage to complete the modelling structure by introducing a second category of model outputs that becomes essential in this case: within the high-dimensional outputs $m$ of numerical codes, observations can be made available on output components $y$ that are different to those on $z$ that are later involved in predicting the quantity of interest. Hence, this family of inverse techniques generally consists in translating the information obtained on a sample of experimental measurements $(y_j)$ into the calibrated value of the uncertain inputs $x$. In a dynamic approach, generally best interpreted in a Bayesian statistical framework, there may thus be a prior uncertainty model with the associated predicted quantity of interest, followed by a posterior description and prediction after incorporation of assimilated data (Figure 1.9).

Chapter 6 will further develop this topic which proves essential for sound modelling in the context of risk and uncertainty. Substantial extensions of the algorithms developed in classical numerical analysis are needed: indeed, those algorithms mostly stick to Gaussian and/or linear contexts and are unnecessarily limited to a description of epistemic uncertainty in the sense that code inputs are generally considered to be unknown but physically fixed (de Rocquigny and Cambier, 2009).

1.5 Forecast and time-based modelling in weather, operations research, economics or finance

An essential area of application of modelling under uncertainty with considerable practical value and ongoing research involves the prediction of variables of interest under uncertainty over future times of interest. Think of meteorological forecast, operations research and stochastic optimisation be it in econometrics (micro-economic market forecast or macro-economic growth forecast), energy or asset management, financial market forecast and portfolio analysis and so on (see, e.g. the survey of Tay and Wallis, 2000 or Elliott, Granger, and Timmermann, 2006).

This area shares essential common features with the framework developed above (in particular IPRA or UASA). Again, the decision-maker is interested in the prediction of given variables of interest characterising an underlying system, process, portfolio or market, which is itself impacted by a number of uncertain events, behaviours or mechanisms, in order to typically select the best actions to take (the
controllable variables) such as operational actions best suited to the likely weather or market demand or portfolio allocations. A quantity of interest or risk measure is set to optimise performance or control the risk budget. For instance, the power supply-demand balance would be controlled over a future time period through a prescribed maximal frequency of events with negative balance. Otherwise, the value of asset portfolios over a particular holding period would be controlled over its future quantiles (denominated Value-at-Risk in finance) or alternative risk measures such as the expected value of loss conditional to exceeding a given quantile (expected shortfalls).

A core difference with the practices reviewed above concerns the time basis of this kind of analysis. The decision-maker would generally look for predictions for the variables of interest at possibly-multiple and generally short-term future times of interests; the time dynamics carry essential information in the sense that the correlation between recent, present and future states of the system are substantial so that the underlying models benefit from involving dedicated time series and probabilistic dynamics. This leads to using probabilistic and statistical modelling techniques distinct from those used for the estimation of extreme events or industrial safety although connections exist with the area of dynamic reliability (Section 1.3.3) and natural risk assessment. Particularly in hydrology, complementary types of flood models are being developed either for the day or week-ahead predictions of likely flows (e.g. for hydro-power, early-warning, flood routing or crisis management) or for extreme event flood risk assessment (e.g. for the design of dam safety or protection dike). Eventually, the area of forecasting often involves events frequent enough to be observable.

Though not central in the scope of this book, a number of comments will be addressed to the specificities required regarding time-explicit risk measures (in Chapter 4), forecast models as distinguished from risk models (in Chapter 6) and time-based decision-making possibly involving the essential concept of options (in Chapter 8).

1.6 Conclusion: The scope for generic modelling under risk and uncertainty

1.6.1 Similar and dissimilar features in modelling, risk and uncertainty studies

Practice shows both similar and dissimilar features, as summarised in Table 1.3. Firstly, the general structure is similar in most modelling studies (Figures 1.1–1.3 and 1.7): it incorporates a system model, representing the system studied under risk and/or uncertainty, and a number of associated inputs and outputs of interest for decision-making. Furthermore, most risk or uncertainty studies incorporate a probabilistic representation of at least some of the inputs. Hence the outputs of interest are assessed from the perspective of a probabilistic quantity which is called the risk measure or quantity of interest (or design criterion, etc.). From a theoretical perspective, such measures mostly involve a generic format, namely multiple integrations of the system model over the uncertainty model.

Yet, a closer look into the various practices evidences some dissimilarity:

- The nature of system models: clearly phenomenological for natural risk or SRA; mostly logical for QRA; of a mixed nature within IPRA; and viewed as numerical in UASA or code qualification.
- The type of inputs/outputs: discrete events are considered for some (in QRA or SRA for the output side) while continuous variables are involved for others (such as UASA or SRA for the input side). Probability distributions thus vary from discrete laws, such as Bernoulli r.v. for simple events, to continuous laws, such as Gaussian r.v. for uncertain input variables.
### Table 1.3 Overview of domain generics and specificities.

<table>
<thead>
<tr>
<th>Natural risk protection (NRA)</th>
<th>SRA</th>
<th>QRA</th>
<th>IPRA</th>
<th>UASA - metrology</th>
<th>UASA - environmental</th>
<th>NCQ, data assimilation</th>
<th>Forecasting/time-based in weather, asset management, finance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System model</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local risk situation</td>
<td>Failure function</td>
<td>Event tree, fault tree, BBN...</td>
<td>A combination of the NR, SRA and QRA</td>
<td>Pre-existing model (metrological chain)</td>
<td>Pre-existing model (numerical model)</td>
<td>Numerical code</td>
<td>Pre-existing model (numerical model)</td>
</tr>
<tr>
<td>Critical event</td>
<td>Failure event</td>
<td>Undesired event (or top event)</td>
<td>Continuous consequence variables or set of consequence events</td>
<td>Variables of interest: continuous and often scalar</td>
<td>Variables of interest: continuous and often vector</td>
<td>Variables of interest: continuous and often vector</td>
<td>Variables of interest: continuous and time series</td>
</tr>
<tr>
<td><strong>Event/variables of interest</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>aleatory variables (mostly continuous)</td>
<td>uncertain variables (mostly continuous)</td>
<td>Elementary events</td>
<td>A combination of NR, SRA, QRA</td>
<td>uncertain variables (measurement errors)</td>
<td>uncertain variables (mostly continuous)</td>
<td>uncertain inputs (mostly continuous)</td>
<td>Uncertain inputs and recent states (static and/or time-series)</td>
</tr>
<tr>
<td><strong>Model inputs</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Frequency of undesired event or quantile of variable of interest</td>
<td>Failure probability (undesired event)</td>
<td>Frequency of undesired event</td>
<td>Frequencies of a set of consequences or cdf of variables of interest</td>
<td>Quantity of interest: $C_V$ or c.i.</td>
<td>Quantity of interest: $C_V$ or c.i.</td>
<td>Quantity of interest: variance or $C_V$</td>
<td>Expected value, c.i., variance or quantiles at short-term future times</td>
</tr>
<tr>
<td><strong>Risk measure/quantity of interest</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Remarks</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Careful statistical modelling, often involving extreme value theory</td>
<td>CPU challenge due to low probabilities</td>
<td>Very large vector of inputs and dependence</td>
<td>‘Epistemic’ and ‘aleatory’ components may be distinguished</td>
<td>Level-2 uncertainty (estimation of input uncertainty)</td>
<td>Large uncertain models and large use of expert opinion</td>
<td>CPU challenge due to large input dimension</td>
<td>Specificities due to the importance of temporal correlation structure and stochastic processes</td>
</tr>
</tbody>
</table>
• The type of risk measures/quantities of interest considered and associated with the decision criteria: failure probabilities or frequencies, output variance or confidence intervals, expected consequence and so on.
• The probabilistic settings and their specification: some studies clearly differentiate ‘risk or vulnerability or aleatory’ components (quantified in a frequency) from ‘uncertainty or epistemic’ components (quantified in an associated confidence interval); others aggregate overall probabilities or expectations without making an explicit distinction between the variability or levels of imprecision involved. In many cases deterministice penalisation of some inputs is kept, along with probability distribution for others.
• The main objectives of the study: to demonstrate compliance with a regulatory criterion, to optimise a design, or simply to facilitate importance ranking and deeper phenomenological understanding.
• The biggest challenges encountered: for some studies, statistical estimation may involve large resources and complex models while, in others, informal expert judgement is considered satisfactory; the computation of risk measures may be a real limiting factor in SRA, NCQ or some large UASA while it is only a minor step in QRA or natural risk; model building and validation and associated uncertainties are of key concern in environmental or biological modelling, though much less elsewhere.

1.6.2 Limitations and challenges motivating a unified framework

Previous sections have already evidenced some limitations in given domains, and the restricted permeability between them. In summary:

• Distinction of practices between NRA and SRA tends to prevent a fruitful use of the relative advances of each, such as detailed statistical modelling for the former, or performing coupled probabilistic-numerical computation for the latter.
• Careful specification of the meaning of the probabilistic models (the nature of underlying uncertainty) is not as developed in SRA or NCQ as it is in IPRA.
• The potential of high-performance computing is largely investigated in SRA or NCQ, but is insufficiently accounted for in NRA which is often limited to unnecessarily simplified risk description.
• Formalized model identification and selection techniques, largely developed in data analysis and statistical modelling, have only permeated into environmental or biological modelling, and only to a limited extent into numerical code qualification and data assimilation.
• The time basis for the variables of interest is fundamental in forecasting, time-based risk analysis in finance or data assimilation techniques owing to the crucial role of temporal correlations inside the model; yet, other domains such as NRA or IPRA also implicitly define the time basis of their measures, though not necessarily requiring a complete stochastic process as the correlations can be less tractable for, for example, extreme events.
• Rather than opposing them violently, a careful understanding of the mixed deterministic-probabilistic settings helps describe more accountably the plausible extent of lack of knowledge. This could avoid over-trusting either: deterministic design assumptions disregarding the extent of uncertainty; or conversely fully probabilistic computations based on vaguely justified pdf in the absence of data, credible expertise or simply by not specifying the meaning of the randomised quantities.

Complex industrial systems require an increasing blend of all such approaches as the search for operational margins and the regulatory control processes intensifies. For instance, the investigation of vulnerability to natural risk initiators addresses jointly: a careful specification of the meaning of the
quantity of interest or risk measure regarding the underlying type of uncertainty covered, as well as the
time basis; a finer modelling of the climate statistical series; a better calibration of physical-numerical
models representing the local phenomenology; and a finer understanding of protection system reliability.
This suffers from insufficient consistency between the reliability, statistical and physical modelling
components and expertise.

In spite of their apparent diversity, there is much to share and integrate. As mentioned above, QRA
may be formally presented similarly to SRA, itself linkable to the ‘extended frequency approach’ in NRA.
The comments on advanced IPRA or UASA have demonstrated the opportunities associated with unifying
frameworks explicitly: Chapter 2 will generalise them into a generic modelling approach. For instance,
the computation of most of the risk measures or quantities of interest involves essentially the integration of
a deterministic function (the system model) over the uncertainty model (a more or less elaborate density
function); the nature of the inputs or outputs involved (discrete events or continuous variables) merely
facilitates some integration techniques while conserving the theoretical issue (see Chapter 7). Moreover,
the estimation needs of the various types of models, as well as those of calibration, and assimilation of
identification, mostly taken on similar statistical techniques, although coming with partial variants owing to
the continuous, discrete or temporal nature of the variables (see Chapter 5), or to the input/output position
of the variables that can be observed directly or indirectly through a numerical model (see Chapter 6).
These facts, all too often hidden by domain boundaries in the literature or engineering practices,
constitutes the key starting point for the use of the generic numerical tools that will be developed in the
subsequent chapters.

References

and Earth System Sciences, 4, 295–308.

Apostolakis, G. (1999) The distinction between aleatory and epistemic uncertainties is important; an
example from the inclusion of aging effects in the PSA. Proceedings of PSA’99, Washington DC.


Structural Safety, 20, 155–165.

Sons, Ltd.

Research, 23(8), 1393–1442.

University Press.

Beven K.J. and Binley A.M. (1992) The future of distributed model: model calibration and uncertainty
prediction, Hydrological Processes, 6, 279–298.

Boyack, B.E. (1990) Quantifying reactor safety margins-part I: an overview of the code scaling,

Science and Engineering, 75.


de Rocquigny, E. (2010) An applied framework for uncertainty treatment and key challenges in


