LES CAHIERS DE LA SÉCURITÉ INDUSTRIELLE

2012-07

RISK ANALYSIS

Uncertainty Characterization in Risk analysis for Decision-making Practice

Enrico Zio

Nicola Pedroni

FonCSI
FONDATION POUR UNE CULTURE DE SÉCURITÉ INDUSTRIELLE

The *Foundation for an Industrial Safety Culture* (FonCSI) is a french public-interest research foundation created in 2005. It aims to:

- undertake and fund research activities that contribute to improving safety in hazardous organizations (industrial firms of all sizes, in all industrial sectors);
- work towards better mutual understanding between high-risk industries and civil society, aiming for a durable compromise and an open debate that covers all the dimensions of risk;
- foster the acculturation of all stakeholders to the questions, tradeoffs and problems related to risk and safety.

In order to attain these objectives, the FonCSI works to bring together researchers from different scientific disciplines with other stakeholders concerned by industrial safety and the management of technological risk: companies, local government, trade unions, NGOs. We also attempt to build bridges between disciplines and to promote interaction and cross-pollination between engineering, sciences and the humanities.

The work presented in this document is the result of research funded by the FonCSI. The opinions presented are those of the authors.

FONCSI
Fondation pour une culture de sécurité industrielle

Foundation for an Industrial Safety Culture
A public-interest research foundation

http://www.FonCSI.org/

6 allée Émile Monso – BP 34038
31029 Toulouse cedex 4
France

Telephone: +33 534 32 32 00
Twitter: @TheFonCSI
Email: contact@FonCSI.org

Résumé

Titre	Caractérisation de l'incertitude dans l'analyse de risque pour améliorer la prise de décision
Mots-clefs	incertitude, analyse de risque, QRA, caractérisation, prise de décision
Auteurs	Enrico Zio et Nicola Pedroni
Date de publication	mai 2012

Ce document fournit une synthèse des sources d'incertitude pouvant affecter une analyse de risque probabiliste. Pour chaque étape du processus d'analyse de risque (modélisation du système considéré, identification des dangers, estimation de la probabilité et la gravité des conséquences de séquences accidentelles, évaluation du risque), les auteurs décrivent et classifient les types d'incertitude qui peuvent survenir.

Le document propose :

- ▷ une description de la démarche d'analyse de risque, telle que mise en œuvre dans des industries à forts potentiels de dangers, comme le nucléaire et l'extraction pétrolière et gazière ;
- ▷ une classification des sources d'incertitude (épistémique et aléatoire) ainsi qu'une description de techniques qui peuvent être employées pour modéliser ces sources d'incertitude ;
- ▷ une description des différentes étapes impliquées dans une étude probabiliste des risques (ou QRA, pour *Quantitative Risk Assessment*, en anglais), ainsi qu'une analyse des types d'incertitude qui peuvent survenir à chaque étape ;
- ▷ des annexes donnant une introduction à différents outils utilisés pendant les analyses probabilistes des risques, comme le HAZID, les arbres de fautes et arbres de défaillances.

D'autres documents à venir dans cette série décriront les techniques qui peuvent être utilisées pour représenter ces différentes formes d'incertitude, pour les propager au sein de l'analyse de risques, et pour présenter à des décideurs des métriques de risque incluant une information sur l'incertitude pesant sur les résultats de l'analyse.

À propos des auteurs

Enrico Zio est Professeur de Fiabilité et Analyse de Risque au Politecnico di Milano, et Directeur de la Chaire *Systèmes complexes et défis énergétiques* de l'École Centrale Paris & Supelec. Il est également chairman du *European Safety and Reliability Association* (ESRA).

Nicola Pedroni est maître de conférences au département Énergie du Politecnico di Milano. Sa recherche concerne les méthodes calculatoires avancées pour l'évaluation de la sécurité des systèmes industriels, en présence d'incertitude.

Pour citer ce document

Zio et Pedroni (2012). *Uncertainty characterization in risk analysis for decision-making practice*, numéro 2012-07 des *Cahiers de la Sécurité Industrielle*, Fondation pour une Culture de Sécurité Industrielle, Toulouse, France (ISSN 2100-3874). Disponible à l'adresse http://www.FonCSI.org/fr/.

Abstract

Title	Uncertainty characterization in risk analysis for decision-making practice
Keywords	uncertainty, QRA, probabilistic risk analysis, decision-making
Authors	Enrico Zio and Nicola Pedroni
Publication date	May 2012

This document provides an overview of sources of uncertainty in probabilistic risk analysis. For each phase of the risk analysis process (system modeling, hazard identification, estimation of the probability and consequences of accident sequences, risk evaluation), the authors describe and classify the types of uncertainty that can arise.

The document provides:

- ▷ a description of the risk assessment process, as used in hazardous industries such as nuclear power and offshore oil and gas extraction;
- ▷ a classification of sources of uncertainty (both epistemic and aleatory) and a description of techniques for uncertainty representation;
- ▷ a description of the different steps involved in a Probabilistic Risk Assessement (PRA) or Quantitative Risk Assessment (QRA), and an analysis of the types of uncertainty that can affect each of these steps.
- ▷ annexes giving an overview of a number of tools used during probabilistic risk assessment, including the HAZID technique, fault trees and event tree analysis.

Future documents in this series will describe techniques for representing these different forms of uncertainty (using mathematical techniques), for propagating them through the risk assessment process, and for presenting the resulting uncertainty-enhanced risk measures to decision-makers.

About the authors

Enrico Zio is Professor of Reliability, Safety and Risk Analysis at Politecnico di Milano and Director of the Chair in Complex Systems and the Energetic Challenge of École Centrale Paris & Supelec. He is also chairman of the *European Safety and Reliability Association* (ESRA).

Nicola Pedroni is an associate professor in the Energy Department of the Politecnico di Milano. His research concerns advanced computational methods for the reliability assessment of industrial systems in presence of uncertainties.

To cite this document

Zio and Pedroni (2012). *Uncertainty characterization in risk analysis for decision-making practice*, number 2012-07 of the *Cahiers de la Sécurité Industrielle*, Foundation for an Industrial Safety Culture, Toulouse, France (ISSN 2100-3874). Available at http://www.FonCSI.org/en/.

Contents

1

Introduction

Context

Although the use of risk assessment and uncertainty analysis for decision making may take different perspectives, there is a shared and common understanding that these tools provide useful **decision support**, in the sense that their outcomes inform decision makers, insofar as the technical risk side of the problem is relevant for the decision **[Aven 2010b]**.

The actual decision outcome for a critical situation involving a potential for large consequences typically derives from a thorough process which combines:

- an **analytic evaluation** of the situation (*i.e.*, the risk assessment) by rigorous, replicable methods evaluated under agreed protocols of an expert community and peer-reviewed to verify the assumptions underpinning the analysis;
- a **deliberative group exercise** in which all involved stakeholders and decision makers collectively consider the decision issues, look into the arguments for their support, scrutinize the outcomes of the technical analysis and introduce all other values (*e.g.* social and political) not explicitly included in the technical analysis.

This way of proceeding allows the technical analysis to remain manageable, while being complemented by deliberation to ensure coverage of the non-modelled issues. In this way, the analytic evaluation (*i.e.*, the risk assessment) *supports* the deliberation by providing numerical outputs[1] and also all the argumentations behind the analysis itself, including the assumptions, hypotheses, parameters and their uncertainties **[Nilsen and Aven 2003]**.

With respect to the latter issue, the key point is to guarantee that uncertainties are taken into account in *each* step of the risk assessment procedure in a manner which ensures that the information and knowledge relevant for the problem are represented in the most faithful manner. In particular, uncertainties have to be

1. systematically identified and classified;
2. represented and described by rigorous mathematical approaches;
3. propagated through the steps of the risk assessment procedure onto the risk measures until the decisions.

The bottom line concern with respect to uncertainty in decision making is to provide the decision makers with a **clearly informed picture** of the problem upon which they can confidently reason and deliberate **[Zio 2009; Aven and Zio 2011]**.

For more than 30 years, probabilistic analysis has been used as the basis for the analytic process of risk assessment or hazardous systems and the treatment of associated uncertainties. The common term used is *Probabilistic Risk Assessment* (PRA, also referred to as Quantitative Risk Assessment, QRA). Its first application to large technological systems (specifically nuclear power plants) dates back to the early 1970s **[USNRC 1975]**, but the basic analysis principles have not significantly changed since.

However, the purely probability-based approaches to risk and uncertainty analysis can be challenged under the common conditions of limited or poor knowledge on the **high-consequence risk problem**, for which the information available does not provide a strong

[1] Point estimates and distributions of the relevant safety parameters, possibly to be compared with predefined numerical safety criteria for further guidance to the decision.

basis for a specific probability assignment: in such a decision making context, many stakeholders may not be satisfied with a probability assessment based on subjective judgments made by a group of analysts. In this view, a broader risk description is sought where all the uncertainties are laid out 'plain and flat', with no additional information inserted in the analytic evaluation in the form of assumptions and hypotheses which cannot be proven right or wrong. This concern has sparked a number of investigations in the field of uncertainty representation and analysis, which has led to the developments of frameworks alternative to the probabilistic one (*e.g.*, probability bounds analysis **[Ferson and Ginzburg 1996]**, imprecise probability **[Walley 1991]**, random sets **[Dempster 1967; Shafer 1976]** and possibility theory **[Dubois and Prade 1988; Dubois 2006]**).

Finally, decision-makers commonly seek further protection in the implementation of the decision by adding conservatisms and performing traditional engineering approaches of 'defense-in-depth' to bound the uncertainties and in particular the 'unknown unknowns' (completeness uncertainty).

defense in depth

Objectives of this document

In this wide framework of uncertainty identification, representation and propagation, the objective of the present document is twofold:

1. analyzing and describing in detail the (traditional) steps of the risk assessment procedure;
2. systematically identifying and classifying the sources of uncertainty affecting *each* step of the risk assessment procedure.

The technical details about risk assessment will be exposed for clarity to analyze and judge how each step is affected by uncertainty and how this impacts the communication of risk to decision makers, in the typical settings of high-consequence risk analysis of complex systems with limited knowledge on their behaviour. The driver of the critical analysis is really the decision making and the need to feed it with representative information derived from the risk assessment, to robustly support the decision.

The problem of uncertainty representation and propagation will be described in future documents in this collection.

Document structure

The remainder of the document is structured as follows:

- ▷ Chapter 2 presents the concepts of risk and risk analysis;
- ▷ In chapter 3, the problems of uncertainty and uncertainty analysis are presented within the framework of risk assessment;
- ▷ In chapter 4, the different steps of the risk assessment procedure are analyzed in detail and the sources of uncertainty affecting each of these steps are highlighted and briefly described.

Three annexes provide more detail on specific tools used during a probabilistic risk assessment:

- ▷ Annex A provides a description of the **HAZID** technique;
- ▷ Annex B describes the **fault tree** technique;
- ▷ Annex C describes the construction and evaluation of an **event tree**.

2

Risk and risk analysis

2.1 From defence in depth to probabilistic risk assessment

The subject of risk nowadays plays a relevant role in the design, development, operation and management of components, systems and structures in many types of industry. In all generality, the problem of risk arises wherever there exists a **potential source of damage or loss**, *i.e.* a *hazard* (threat) to a "target", such as people or the environment. Under these conditions, **safeguards** are typically devised to prevent the occurrence of the hazardous conditions, and protections are put in place to protect from and **mitigate** its associated undesired consequences. The presence of a hazard does not suffice itself to define a condition of risk; indeed, inherent in the latter there is the uncertainty that the hazard translates from potential to actual damage, bypassing safeguards and protections. In summary, the notion of risk involves some kind of loss or damage that might be received by a target and the uncertainty of its transformation into an actual loss or damage.

hazard

One classical way to defend a system against the uncertainty of its failure scenarios has been to:

1. identify the group of failure event sequences leading to credible **worst-case accident scenarios** S_i (design-basis accidents);
2. predict their **consequences** x_{S_i};
3. accordingly design proper **safety barriers** for preventing such scenarios and for protecting against, and mitigating, their associated consequences **[Zio 2009]**.

design-basis accident

Within this approach (often referred to as a **structuralist defense-in-depth** approach), safety margins against these scenarios are enforced through conservative regulations of system design and operation, under the creed that the identified worst-case, credible accidents would envelop all credible accidents for what regards the challenges and stresses posed on the system and its protections. The underlying principle has been that if a system is designed to withstand all the worst-case credible accidents, then it is 'by definition' protected against any credible accident **[Apostolakis 2006]**.

worst-case accident

This approach has been the one classically chosen – and for many technologies is still the leading approach – to protect a system from the uncertainty of the unknown failure behaviors of its components, systems and structures, without directly quantifying the uncertainty, to provide reasonable assurance that the system can be operated without undue risk. However, the practice of referring to "worst" cases implies strong elements of **subjectivity** and arbitrariness in the definition of the accidental events, which may lead to the consideration of scenarios characterized by really catastrophic consequences, although highly unlikely. This may lead to the imposition of unnecessarily stringent regulatory burdens and thus excessive conservatism in the design and operation of the system and its protective barriers, with a penalization of the industry. This is particularly so for those high-consequence industries, such as the nuclear, aerospace and process ones, in which accidents may lead to potentially large consequences.

For this reason, an alternative approach has been pushed forward for the design, regulation and management of the safety of hazardous systems. This approach, initially motivated by the growing use of nuclear energy and by the growing investments in aerospace missions in the 1960s, is based on the principle of **quantifying the reliability** of the accident-preventing and consequence-limiting protection systems which are designed and implemented to intervene

in protection against all potential accident scenarios. This approach no longer differentiates between credible and incredible, or large and small accidents [Farmer 1964]. Initially, a number of studies were undertaken to investigate the merits of a quantitative approach based on probability for the treatment of the uncertainty associated with the occurrence and evolution of accident scenarios [Garrick and Gekler 1967]. The findings of these studies motivated the first complete and full-scale probabilistic risk assessment of a nuclear power installation [USNRC 1975]. This extensive work showed that, indeed, the dominant contributors to risk need not be necessarily the design-basis accidents, a "revolutionary" discovery which undermined the fundamental creed underpinning the structuralist, defense-in-depth approach to safety [Apostolakis 2006].

Following these lines of thought, and after several "battles" for their demonstration and valorisation, the probabilistic approach to risk analysis (PRA) has arisen as an effective technique for analysing system safety, not limited only to the consideration of worst-case accident scenarios but extended to looking at **all feasible scenarios** and their related consequences. The probability of occurrence of such scenarios becomes an additional key aspect to be quantified in order rationally and quantitatively to handle uncertainty [USNRC 1975; NASA 2002; Aven 2003; Bedford and Cooke 2001; Henley and Kumamoto 1992; Kaplan and Garrick 1981; McCormick 1981; USNRC 1983].

Selecting the worst case scenario is a somewhat subjective process, and can lead to excessively strong safety requirements

From the view point of safety regulations, this has led to the introduction of new criteria which account for both the consequences of the scenarios and their probabilities of occurrence under a now rationalist, defense-in-depth approach. Within this approach to safety analysis and regulation, **reliability engineering** takes on an important role in the assessment of the probability of occurrence of the accident scenarios as well as the probability of the functioning of the safety barriers implemented to hinder the occurrence of hazardous situations and mitigate their consequences if such situations should occur [Zio 2009].

reliability engineering

2.2 The framework of PRA

The basic analysis principles used in a PRA can be summarized as follows. A PRA systemizes the knowledge and uncertainties about the phenomena studied by addressing three fundamental questions [USNRC 1983]:

- Which sequences of undesirable events transform the hazard into an actual damage?
- What is the **probability** of each of these sequences?
- What are the **consequences** of each of these sequences?

This leads to a widely accepted, technical definition of risk in terms of a set of triplets [Kaplan and Garrick 1981] identifying the sequences of undesirable events leading to damage (the accident scenarios), the associated probabilities and the consequences. In this view, the outcome of a risk analysis is a list of scenarios quantified in terms of probabilities and consequences, which collectively represent the risk. On the basis of this information, the designer, the operator, the manager and the regulator can act effectively so as to manage (and possibly reduce) risk (*cf.* figure 2.1).

In the PRA framework, the knowledge on the problem and the related uncertainties are systematically manipulated by rigorous and replicable probability-based methods to provide representative risk outcomes such as the expected number of fatalities[1], the probability that a specific person shall be killed due to an accident (individual risk) and frequency-consequence ($f - n$) curves expressing the expected number of accidents (frequency f) with at least n fatalities.

In spite of the maturity reached by the methodologies used in PRA, a number of new and improved methods have been developed in recent years to better meet the needs of the analysis, in light of increasing system complexity and to respond to the introduction of new technological systems. Many of the methods introduced allow increased levels of detail and precision in the modelling of phenomena and processes within an **integrated framework of analysis**

[1] The expected number of fatalities due to the operation of a plant or equipment is the mathematical expectation of the number of fatalities per year due to accidents on the plant. Anticipated fatalities are commonly expressed in terms of indices such as PLL (Potential Loss of Lives) and FAR (Fatal Accident Rate).

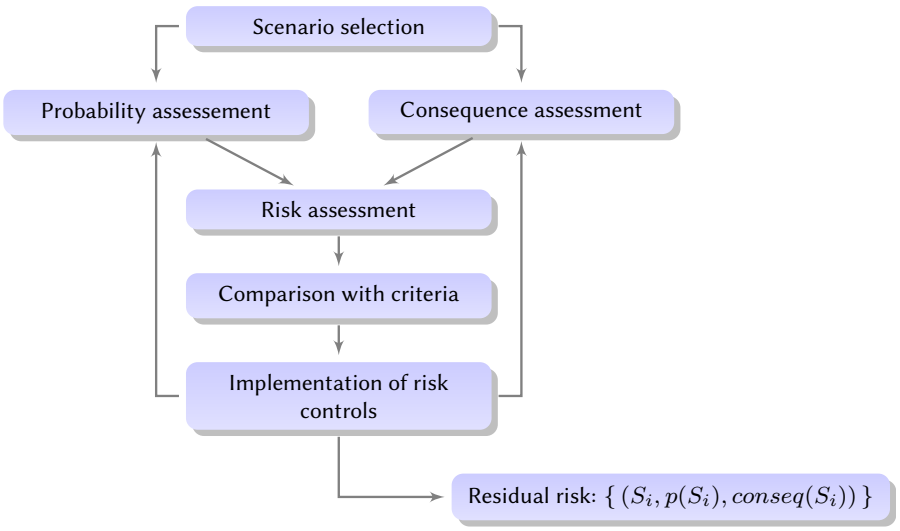

Figure 2.1 – The risk analysis process, which leads to a set of triplets comprising the accident scenarios S_i and their estimated probability and consequences.

covering physical phenomena, human and organisational factors as well as software dynamics (*e.g.* **[Mohaghegh et al. 2009]**). Other methods are devoted to the improved representation and analysis of risk and related uncertainties, in view of the decision making tasks that the outcomes of the analysis are intended to support. Examples of newly introduced methods are *Bayesian Belief Networks (BBNs), Binary Digit Diagrams (BDDs), multi-state reliability analysis, Petri Nets and advanced Monte Carlo simulation tools*. For a summary and discussion of some of these models and techniques, see **[Bedford and Cooke 2001; Zio 2009]**.

The probabilistic analysis underpinning PRA stands on two lines of thinking: the traditional frequentist approach and the Bayesian approach **[Bedford and Cooke 2001; Aven 2003]**. The **frequentist approach** is typically applied in the presence of a large amount of relevant data; it is founded on well-known principles of statistical inference, the use of probability models, the interpretation of probabilities as relative frequencies, point values, confidence intervals estimation and hypothesis testing.

The **Bayesian approach** is based on the use of **subjective probabilities**. It is applicable in cases where data is scarce. The steps in the Bayesian approach are:

1. Establish adequate probability models representing the **aleatory uncertainties**, *i.e.* the variabilities in the phenomena studied, such as *the lifetimes of a type of unit*.
2. Establish probability models for the **epistemic uncertainties** (due to incomplete knowledge or lack of knowledge) about the values of the parameters of the models. They are represented by prior subjective probability distributions. When new data on the phenomena studied become available, Bayes' formula is used to update the representation of the epistemic uncertainties in terms of the posterior distributions.
3. The predictive distributions of the quantities of interest (the *observables*, for example *the lifetime of new units*) are derived by applying the law of total probability. The predictive distributions are epistemic but they also reflect the inherent variability represented by the underlying probability models.

Subjective probability

Subjective probability is a measure of a person's **degree of belief** concerning the plausibility of an event. From a conceptual viewpoint, a subjective probability is commonly linked to the betting interpretation that goes back to the foundational literature on subjective probabilities (see *e.g.* **[?Singpurwalla 2006]**). In this interpretation, one's degree of belief in E is p if and only if p units of utility is the price at which one would buy or sell a bet that pays 1 unit of utility if E, and pays 0 if not E.

However, to avoid a mixture between uncertainty assessments and value judgments, many analysts prefer to use the comparison with a standard interpretation, for example drawing a ball from an urn **[Lindley 2000; Aven 2003]**. The term "subjective probability" is also debated, since it gives the impression that the probability and the associated assessment are non-scientific and arbitrary; it is often replaced by terms such as "judgmental probability" and "knowledge-based probability" **[Singpurwalla 2006; Aven 2010a]**.

3

Uncertainty and uncertainty analysis in risk assessment

In all generality, the quantitative analyses of the phenomena occurring in many engineering applications are based on mathematical models which are then turned into operative computer codes for simulation. A model provides a representation of a real system dependent on a number of hypotheses and parameters. The model can be deterministic (*e.g. Newton's dynamic laws or Darcy's law for groundwater flow*) or stochastic (*e.g.* the *Poisson model for describing the occurrence of earthquake events*).

In practice, the system under analysis can not be characterized exactly – the knowledge of the underlying phenomena is incomplete. This leads to *uncertainty* on the analysis which can be defined as a *state* of the analyst who cannot describe or foresee a phenomenon due to i) an intrinsic variability of the phenomenon itself or ii) lack of knowledge and information. This leads in practice to uncertainty on both the **values of the model parameters** and on the **hypotheses supporting the model** structure. Such uncertainty propagates within the model and causes **variability in its outputs**: for example, when many values are plausible for a model parameter, the model outputs associated to the different values of the uncertain parameter will be different; the quantification and characterization of the resulting output uncertainty is of paramount importance, and it defines the scope of the uncertainty analysis.

Uncertainty analysis

DEFINITION

An uncertainty analysis aims at determining the uncertainty in analysis results that derives from uncertainty in analysis inputs **[Helton and Oberkampf 2004]**. We may illustrate the ideas of the uncertainty analysis by introducing a model $f(x)$, which depends on the input quantities x and on the function f; the quantity of interest x is computed by using the model $y = f(x)$. The uncertainty analysis of y requires an assessment of the uncertainties about x and a propagation through the model f to produce an assessment of the uncertainties about y.

Typically, the uncertainty about x and the uncertainty related to the model structure f, *i.e.*, uncertainty due to the existence of alternative plausible hypotheses on the phenomena involved, are treated separately. While the first source of uncertainty has been widely investigated and more or less sophisticated methods have been developed to deal with it, research is still ongoing to obtain effective and agreed methods to handle the uncertainty related to the model structure **[USNRC 2009]**. See also **[Aven 2010b]** who distinguishes between *model inaccuracies* (the differences between y and $f(x)$), and *model uncertainties* due to alternative plausible hypotheses on the phenomena involved.

Uncertainty is thus an unavoidable component affecting the behavior of systems and more so with respect to their limits of operation. Despite all the dedicated effort put into improving the understanding of systems, components and processes through the collection of representative data, the appropriate characterization, representation, propagation and interpretation of uncertainty remains a fundamental element of the risk analysis of any system. Following this view, uncertainty analysis is considered an integral part of PRA, although it can also exist independently in the evaluation of a model.

In what follows, the main causes (§ 3.1) and types (§ 3.2) of uncertainty are discussed within a risk assessment framework.

3.1 Causes of uncertainty

Different *causes* of uncertainty can be recognized in risk analysis **[Armacosta and Pet-Edwards 1999; Zimmermann 2000]**:

- **Lack of information (or knowledge)**: Lack of information, knowledge and/or data on the phenomena, systems and events to be analyzed is the main source of uncertainty: it can be of *quantitative* (*e.g.*, the analyst does not know the precise value of the probability of a given event of interest) or *qualitative* (*e.g.*, the analyst knows the probabilities of the events of interest but the available information does not allow a *deterministic* description of the problem to be analyzed) nature.
  Another situation characterized by lack of knowledge is called *approximation*: it takes place when the analyst does not have enough information to describe exhaustively the phenomenon of interest or when he/she deliberately uses a lower level of detail than the one achievable. In some cases, the approximation is declared explicitly, while in other cases it is hidden.
  Obviously, this cause of uncertainty can be reduced by gaining more notions, information and data about the problem at hand.
- **Abundance of information (or knowledge)**: This kind of uncertainty is due to the human incapacity of assimilating and elaborating many pieces of data and information at the same time. In this situation, the analyst usually focuses his attention only on those parameters and those pieces of data and information that he/she considers more important, neglecting the others. The identification of a rigorous (and possibly automated) procedure to select (among hundreds or thousands) the relevant data, information and parameters for the application at hand is the most critical issue.
  The analyst has to face this kind of uncertainty when, for example, he/she has to choose among different models for simulating a given phenomenon.
- **Conflicting nature of pieces of information/data**: It may happen that some pieces of available information and data suggest a given behavior of the system, while others suggest a different one. In this case, increasing the amount of available information and data would not decrease the uncertainty, but rather it would increase the conflict among different pieces of information and data. This conflict can be due to the fact that i) some pieces of information are affected by errors, but the analyst cannot identify them, ii) some of the available pieces of data are not relevant to the problem at hand or iii) the model of the system used by the analyst is not correct (*e.g.*, it is characterized by bias). Again, in order to reduce this source of uncertainty, the analyst has to make an accurate choice among the available pieces of information and data and possibly discard some of them to reduce the conflict.
- **Measurement errors**: The measurement of a physical quantity (*temperatures, weights, lengths, ...*) is always affected by uncertainty due to i) the imprecision of the analyst who performs the measurement or ii) the mechanical tolerance of the instrument adopted.
- **Linguistic ambiguity**: All languages contain words that have different meanings depending on the context of analysis. Note that this source of uncertainty can be considered as due to "lack of information" because providing more details about the context of analysis would help to reduce the associated uncertainty.
- **Subjectivity of analyst opinions**: Uncertainty may derive from the subjective interpretation of the available pieces of information and data by the analyst: different analysts may provide different interpretations of the same piece of information and data depending on their cultural background and competence in the field of analysis. This source of uncertainty can be reduced by resorting to the elicitation of *multiple* opinions from *different* experts.

3.2 Types of uncertainty

In the context of PRA, uncertainty is conveniently distinguished into two different *types*: "aleatory" and "epistemic" **[Apostolakis 1990; Helton and Oberkampf 2004; USNRC 2009]**. The former refers to phenomena occurring in a random way: probabilistic modeling offers a sound and efficient way to describe such occurrences. The latter captures the analyst's confidence in the PRA model by quantifying the degree of belief of the analysts on how well it represents the actual system; it is also referred to as *state-of-knowledge* or *subjective* uncertainty and can be *reduced* by gathering information and data to improve the knowledge on the system behavior.

aleatory uncertainty

Aleatory uncertainties concern, for instance, the occurrence of the events that define the various possible accident scenarios, the *time to failure of a component* or the *random variation of the actual geometrical dimensions and material properties of a component or system (due to differences between the as-built system and its design upon which the analysis is based)* **[USNRC 1990; Helton 1998; USNRC 2002]**. Two examples of classical probabilistic models used to describe this kind of uncertainties in PRAs are the Poisson model for events randomly occurring in time (*e.g.*, *random variations of the operating state of a valve*) and the binomial model for events occurring "as the immediate consequence of a challenge" (for instance, *failure of a safety valve when the pressure in a vessel increases rapidly*[1]) **[USNRC 2005; Hofer et al. 2002; Krzykacz-Hausmann 2006]**.

epistemic uncertainty

Epistemic uncertainty is associated to the lack of knowledge about the properties and conditions of the phenomena underlying the behavior of the systems. This uncertainty manifests itself in the model representation of the system behavior, in terms of both (*model*) uncertainty in the hypotheses assumed and (*parameter*) uncertainty in the (fixed but poorly known) values of the parameters of the model **[Helton and Oberkampf 2004]**. Both model and parameter uncertainties associated to the current state of knowledge of the system can be represented by subjective probability distributions within a Bayesian approach to PRA **[Apostolakis 1990, 1995, 1999]**.

Whereas epistemic uncertainty can be reduced by acquiring knowledge and information on the system, aleatory uncertainty cannot be reduced in this way, and for this reason is sometimes called *irreducible uncertainty*.

[1] Called *failure on demand* of a safety equipment.

4

Risk analysis: main steps and corresponding sources of uncertainty

Risk analysis comprises two parts: the first one aims at identifying malfunctioning, operative errors and external events that may cause accidents in the system/plant of interest; the second one aims at analyzing in detail the accidents that are more critical from the point of view of their frequency and/or their consequences. The final objective is to identify and quantify the impact of accidents and malfunctions (*e.g., failures, operation errors, maintenance errors, external events*) on the system/plant, production, assets and operators, the population and the environment. This evaluation allows to provide indications about the design of the system/plant (*e.g., the installation of prevention/mitigation systems, the modification of the operation/maintenance procedures, ...*) in order to reduce the risk for production, assets, operators, population and environment.

Within this framework, the analytic process of risk assessment for a system is traditionally divided into five steps:

1. system description and modeling (described in § 4.1);
2. identification of the hazards related to the system functioning (§ 4.2);
3. selection of the events that may initiate accident sequences (or scenarios), hereafter called Initiating (or Initiator) Events (IEs) (§ 4.3);
4. quantitative analysis of the accident sequences deriving from the selected IEs (*i.e.*, estimation of their probabilities/frequencies and consequences) (§ 4.4);
5. evaluation of risk and decision making (or deliberative) process (*i.e.*, identification, planning and implementation of the most effective actions to reduce risk) (§ 4.5).

The uncertainties associated with each of these steps are described in the following sections.

4.1 STEP 1 System description and modeling

The main features of the first step of the risk assessment procedure (namely, system description and modeling) are described in § 4.1.1, whereas the corresponding sources of uncertainty are summarized in § 4.1.2.

4.1.1 Description

The construction of the model of a system requires the following steps:

i. comprehension of the *hierarchical*, *logical* and *functional* relations linking the physical elements of the system at any level of detail (*e.g., representation of series/parallel logic relations between components, identification of the main functions performed by single components or groups of components, construction of block diagrams, ...*);

ii. construction of a **parametric model** of the system, *i.e.*, a mathematical representation of the behavior of the system dependent on the values of both known and unknown *internal parameters*;

iii. **calibration** of the mathematical model by means of data (*component, software and human failure data, maintenance record data* and so on) collected (when possible) from the *real* system under analysis **[NPRD 1995]**. Crudely put, calibration is the activity of adjusting the internal parameters of the models until the outputs of the model fit the available data **[Kennedy and O'Hagan 2001]**.

4.1.2 Sources of uncertainty

The sources of uncertainty corresponding to STEP 1 of risk analysis (namely, system description and modeling) can be summarized as follows:

- models are always **approximate** and **simplified** representations of reality, which bears a significant amount of uncertainty to the overall analysis: this type of uncertainty is often referred to as **model inadequacy** **[Kennedy and O'Hagan 2001]**. In order to reduce this uncertainty, the analyst has to capture *all* the *important* features of the system (*i.e.*, all the hierarchical, logical and functional relations linking the physical elements of the system at any level of detail) such that the quality of the analysis is not jeopardized.

model inadequacy

- the successful performance of steps *i.* – *iii.* of § 4.1.1 relies on the competence and **subjective judgment** of the analyst;
- the quantity and quality of the data employed in the calibration phase of step *iii.* of § 4.1.1 can be low, due to:
  - **scarce availability**, because of the possibly scarce operating experience of the system over a wide range of conditions encountered during operation[1];
  - **imprecision** of the data/information available on the system;
  - **measurement errors**.

4.2 STEP 2 Hazard identification

The second step into the analysis of the risk of a given system is that of identifying the hazards associated to its operation.

Hazard

DEFINITION

A hazard is any real or potential condition that may result in injury, illness, death to personnel, damage to the environment, business interruption or loss of assets. Therefore, hazards are not necessarily events, but are threats to safety, assets and production that if triggered by specific initiator events have negative effects on the exposed system, but if opportunely managed do not lead to any accident.

The aim is then that of identifying effective methods for assisting engineers in coping with the hazards, *i.e.* in identifying, classifying, eliminating and/or controlling them **[Zio 2007]**.

The methods developed for performing the hazard identification task consist, in general, in a qualitative analysis of the system and its functions, within a systematic framework of procedures. The methods strongly rely on the expertise of the designers, analysts and personnel who have designed, operated and maintained the system **[Henley and Kumamoto 1992]**.

The main features and steps characterizing the hazard identification procedure are described in § 4.2.1, whereas the corresponding sources of uncertainty are summarized in § 4.2.2.

[1] This is particularly relevant for systems employing new technologies.

4.2.1 Description

The hazard identification procedure consists of three basic steps **[USDoD 1980, 1993; ECSS 1999, 2003]**, described in further detail below:

1. preliminary **historical analysis** of past accidents which occurred in systems similar to that of interest;
2. **functional analysis** aimed at highlighting those functions performed by the system at hand that are relevant to the risk assessment task;
3. **hazard identification** using HAZard IDentification (HAZID) techniques.

Historical analysis

Historical analysis is aimed at a preliminary identification of the safety problems related to a given typology of system, on the basis of past accidents happened to similar systems. This research is carried out by resorting to the available literature specialized in the field and to data bases recording accident events of interest **[USDoD 1993; NPRD 1995]**.

This analysis is used to provide a preliminary, rough indication of the most *important* and *critical* components and functions of the system under analysis in order to drive the subsequent steps of functional analysis and hazard identification.

Functional analysis

The main functions performed by the system are first identified; then, each main function is decomposed in the elementary functions necessary to perform the main one, according to a **hierarchical tree structure**. In other words, a breakdown of the system functions is provided through different hierarchical levels of detail, *i.e.*, functions at level n are decomposed into functions at level $n + 1$. Further details can be found in **[ECSS 1999]**.

An example of this approach is reported in Table 4.1 with reference to a system for the compression and storage of hydrogen **[Carpiognano et al. 2007]**.

Level	Function
1.	Hydrogen production
1.1	Water demineralization
1.1.1	Storage of demineralized water
...	
1.2	Hydrogen generation
1.3	Hydrogen purification
...	...
2.	Hydrogen compression
...	...

Table 4.1 – Example of functional analysis based on a hierarchical tree structure, with reference to a system for the compression and storage of hydrogen **[Carpiognano et al. 2007]**

Hazard identification using HAZID techniques

HAZID is a *qualitative*, *structured* and *iterative* methodology which combines **deductive** aspects (search for causes) and **inductive** aspects (consequence analysis) with the objective of identifying hazards in the functioning of a given system (and, as a final outcome, the initiating events of undesired accident sequences). HAZID looks at the *functions* which are performed in the system: indeed, the method proceeds through the compilation of tables (such as table 4.2) which highlight possible **functional anomalies** and their associated causes and consequences **[USNRC 1983; USDoD 1993; ECSS 2003; Zio 2007]**.

In extreme synthesis, HAZID comprises the following steps **[Henley and Kumamoto 1992]**:

1. consider the *elementary* functions emerged from the functional analysis described in the previous § 4.2.1 (*i.e.*, those at the "lower" levels of the hierarchical tree) and decompose the system into **functionally independent units** (*reaction unit, storage unit, pumping unit, etc.*);
2. for each elementary function (and corresponding functionally independent unit) considered in STEP 1 above, identify the potential *deviations* from nominal behavior. In order to do so, it is necessary to:
   - ▷ specify all the unit *incoming* and *outgoing* fluxes (*energy, mass, control signals, etc.*) and the characteristic (corresponding) *process variables* (*temperature, flow rate, pressure, concentration, etc.*);
   - ▷ apply *guide words* such as "low", "high", "no", "more", "less", "reverse" to the previously identified process variables and unit functions, so as to generate deviations from the nominal process regime (*"high gas temperature", "more gas flow", "no control signal", "low gas pressure", "reverse mass flow", ...*);
3. for each functional deviation identified at STEP 2 above, qualitatively identify its possible *causes*, *consequences* and the associated *hazard* (for instance, *"more gas flow" may be* due to *a valve jammed open or to a pump trip and may* cause *overpressure in a storage tank*);
4. for each functional deviation identified at STEP 2 above and the corresponding causes and consequences identified at STEP 3 above, provide a *qualitative* estimate of the associated Frequencies (F), Damages (D) and Risk (R): these qualitative estimates reflect the analysts' and operators' experience, knowledge and lessons learnt. An example of the qualitative classification of Frequencies (F) and Damages (D) for a given functional deviation of interest is reported in Table 4.2.

Further details about the HAZID technique are reported in Appendix A.

Function	Deviation	Causes	Consequences	Hazard	F	D	R	Recommendations

Table 4.2 – Example of HAZID table

4.2.2 Sources of uncertainty

The sources of uncertainty associated with STEP 2 of risk analysis (namely, hazard identification) are related to the possibly *incomplete* identification of the hazards due to:

- ▷ historical analysis performed using data bases that are not reliable, not updated or not specific to the typology of system of interest;
- ▷ not rigorous and systematic use of HAZID techniques, *e.g.* due to:
  - application limited only to portions of the system;
  - coarse level of detail adopted;
  - incomplete analysis of all the operative functional phases;
  - superficial treatment of human and software errors;

Frequency		
F	**Qualitative estimate**	**Description**
1	Extremely unlikely	Not expected during the system lifetime
2	Remote	It should not happen during the system lifetime
3	Not likely	Expected at most once during the system lifetime
4	Likely	Expected few times during the system lifetime
5	Occasional	Expected many times during the system lifetime

Damage		
D	**Qualitative estimate**	**Description**
1	Safe	No relevant damage to humans, safety functions available
2	Marginal	Partial damage to humans and/or partial loss of the safety functions
3	Severe	Serious damage to humans and/or complete loss of the safety functions
4	Critical	Deaths among the plant operators and/or complete loss of the safety functions
5	Catastrophic	High number of deaths, even among the population, and destruction of the system

Table 4.3 – Qualitative classifications of Frequencies (F) and Damages (D) for hazards identified through the HAZID technique

  - incomplete evaluation of external events (*earthquakes, tornadoes, etc.*) that may act as initiators of accident sequences;

- ▷ imprecise definition of the qualitative classes of frequency and damage (*cf.* table 4.3 for an example);
- ▷ imprecise (or even wrong) assignment of the identified functional deviations to the corresponding qualitative classes of frequency and damage.

4.3 STEP 3 Selection of Initiating Events (IEs)

After the hazards are identified, the corresponding Initiating Events (IEs) (*i.e.*, events that unleash the potential inherent cause of the hazard and, either directly or indirectly, result in damage to the system, the plant operators, the environment or in a loss of production) are selected. Thus, the output of this task consists of a list of the IEs (*component failures and defects, process deviations, external events, operator errors, etc.*) which have a probability of occurrence not equal to zero and which can give rise to significant consequences. Experts' experience, lessons learnt and collection of failure data are again the knowledge sources that feed this part of the study. Notice that a hazard could be triggered by different initiator events leading to identical or different consequences.

The identification of the accident initiators is obviously a key aspect of the overall safety analysis and great care must be put into its completeness since those accident events not included at this stage are very unlikely to enter in the analysis at a later stage **[USNRC 1983; NASA 2002; ECSS 2003]**.

The main features of this step of the risk assessment procedure are described in brief in § 4.3.1, whereas the corresponding sources of uncertainty are summarized in § 4.3.2.

5					
4					
3					
2					
1					
F/D	1	2	3	4	5

Unacceptable: more detailed investigations and changes to the system design and/or management are **recommended**

ALARP (As Low As Reasonably Practicable) or **almost acceptable**: changes to the system design and/or management are **suggested**

Acceptable: the current system design guarantees an adequate control of risk

Figure 4.1 – Exemplary qualitative Risk Matrix for the identification of Initiating Events (IEs)

4.3.1 Description

The following steps have to be undertaken **[USNRC 1983; NASA 2002; ECSS 2003]**:

i. for each hazard resulting from STEP 2 (§ 4.2), identify the corresponding Initiating Events (IEs) (*i.e.*, those events that unleash the potential inherent cause of the hazard and result in damage for the system, the population or the environment): IEs should be hunted out among the possible failures and defects of components, software errors, human errors, *etc.*;

ii. classify the *criticality* of the events identified in STEP 1 above on the basis of the associated level of *risk* by resorting to a qualitative Risk Matrix. In particular, the level of risk associated to an event can be classified as "acceptable" (*i.e.*, the current system design guarantees an adequate control of risk), "almost acceptable" or "As Low As Reasonably Practicable" (ALARP) (*i.e.*, changes to the system design and/or management are suggested) and "unacceptable" (*i.e.*, more detailed investigations and changes to the system design and/or management are recommended). An exemplary qualitative Risk Matrix is shown in figure 4.1;

iii. on the basis of the classification performed at step *ii.* above, select the most *critical* events;

iv. among the most critical events, select those that have the potential for becoming initiators of accident sequences (*i.e.*, Initiating Events-IEs);

v. group similar IEs (*i.e.*, those requiring the intervention of the same safety functions, involving the same area of the system, leading to similar accident evolutions and consequences, ...) into homogeneous classes;

vi. for each class, select *one* reference IE representative of *all* the IEs belonging to the same class.

4.3.2 Sources of uncertainty

The sources of uncertainties corresponding to STEP 3 of risk analysis (namely, selection of the initiating events) can be summarized as follows:

- the successful performance of steps *i.* – *vi.* of § 4.3.1 relies on the *competence*, *experience* and *subjective judgment* of the analyst;
- some of the IEs may have been erroneously left out in STEP 1;
- the *grouping* of the IEs performed at step *v.* of § 4.3.1 may be *rough* and *approximate*.

4.4 STEP 4 Quantitative analysis of the accident sequences

The analysis of the accident sequences (or scenarios) represents the quantitative phase of risk assessment. In synthesis, the accident sequences deriving from each of the Initiating Events (IEs) identified in the previous STEP 3 of the procedure (§ 4.3) are determined; then, the probability (or frequencies) of occurrence of such sequences and the corresponding consequences (*i.e.*, the associated damage) are quantified.

A few details about the methods employed for the quantitative analysis of the accident sequences are reported in § 4.4.1, whereas the corresponding sources of uncertainty are summarized in § 4.4.2.

4.4.1 Description

The quantitative analysis of accident sequences is usually performed by resorting to the Event Tree (ET) methodology.

Event tree method

DEFINITION

Event trees are *inductive* logic methods for identifying the various accident sequences which can result from a single Initiating Event (IE). The approach is based on the discretization of the real accident evolution in few macroscopic events.

Once an initiating event is defined, the events delineating the accident sequences must be defined and organized according to the *time* and *logic* of occurrence. The events delineating the accident sequences are usually characterized in terms of: i) the intervention (or not) of protection systems which are supposed to take action for the mitigation of the accident; ii) the fulfillment (or not) of safety functions; iii) the occurrence or not of physical phenomena. These events are structured in the form of headings in the event tree. For each event, the set of possible states (success or failure of safety systems, occurrence or not of phenomenological events, ...) must be defined and enumerated: each state gives rise to a *branching* of the tree.

Event tree concerning rupture of a pipe in a hydrogen storage facility

In figure 4.2, if the IE is the rupture of a pipe with release of gas in a plant for the compression and storage of hydrogen, the first function required would be that of blocking the released flow rate (event E_1), followed by the possible ignition of hydrogen (event E_2) and finally the quenching of the fire (event E_3). By way of example, referring to figure 4.3, sequence $S_2 = IE, \overline{E_1}, \overline{E_2}$ denotes the accident scenario in which the initiating event IE occurs, the blocking safety system is called upon and does not succeed ($\overline{E_1}$) and hydrogen ignition does not occur ($\overline{E_2}$).

Fault tree analysis

DEFINITION

Fault tree analysis is a *systematic*, *deductive* technique which allows to develop the causal relations leading to a given undesired event. It is deductive in the sense that it starts from a defined system failure event and unfolds backward its causes down to the primary (basic) independent faults, also called Basic Events (BEs). The method focuses on a single system failure mode and can provide qualitative information on how a particular event can occur and what consequences it leads to, while at the same time allowing the identification of those components which play a major role in determining the defined system failure. Moreover it can be solved in quantitative terms to provide the probability of events of interest starting from knowledge of the probability of occurrence of the Basic Events (BEs) which cause them.

The interested reader can find further details concerning fault tree analysis in Appendix B at the end of this document.

The accident sequences which derive are then quantified in terms of their probability (or frequency) of occurrence. This requires the determination of the probability (or frequency) of occurrence of the IE and of the *conditional* probabilities of occurrence of the events composing the sequence. Each event (branch) in the tree can be interpreted as the **top event** of a **fault tree** which allows the evaluation of the probability of the occurrence of such event. The value thus computed represents the conditional probability of the occurrence of the event, given that the events which precede on that sequence have occurred.

top event

Fault tree used to estimate the probability of an event in the fault tree above

Figure 4.3 shows the schematics of the event tree of figure 4.2 with an exemplary fault tree used to evaluate the probability $p(E_1|IE)$ of event E_1 conditional on the occurrence of the Initiating Event (IE). Notice that probability $(E_1|IE)$ is computed as a function of the probabilities $p(BE_1)$, $p(BE_2)$ and $p(BE_3)$ of the Basic Events BE_1, BE_2 and BE_3 which cause E_1: in particular, $p(E_1|IE) = 1 - (1 - p(BE_1) \cdot p(BE_2) \cdot (1 - p(BE_3)))$. The multiplication of the conditional probabilities (or frequencies) for each branch in the sequence gives the probability (or frequency) of that sequence. For example, still referring to figure 4.3, the probability $p(S_4)$ of sequence $S_4 = IE, \overline{E_1}, E_2, \overline{E_3}$ is given by

$$p(S_4) = p(IE) \cdot p(\overline{E_1}|IE) \cdot p(E_2|\overline{E_1}) \cdot p(\overline{E_3}|E_2)$$

Finally, the estimation of the **consequences** $x_{S_i}, i \in \{1, 2, ...\}$, of each accident sequence requires the simulation of the physical phenomena included in the event tree branches (*gas release, dispersion, ignition, fire propagation, natural circulation of fluids, heat radiation* and so on) by means of properly built **mathematical models** that are usually translated into deterministic **computer codes**.

Further details about event tree and fault tree techniques are not reported here for brevity; the interested reader is referred to **[Zio 2007]** and references therein and to Appendices B and C, respectively, at the end of the report.

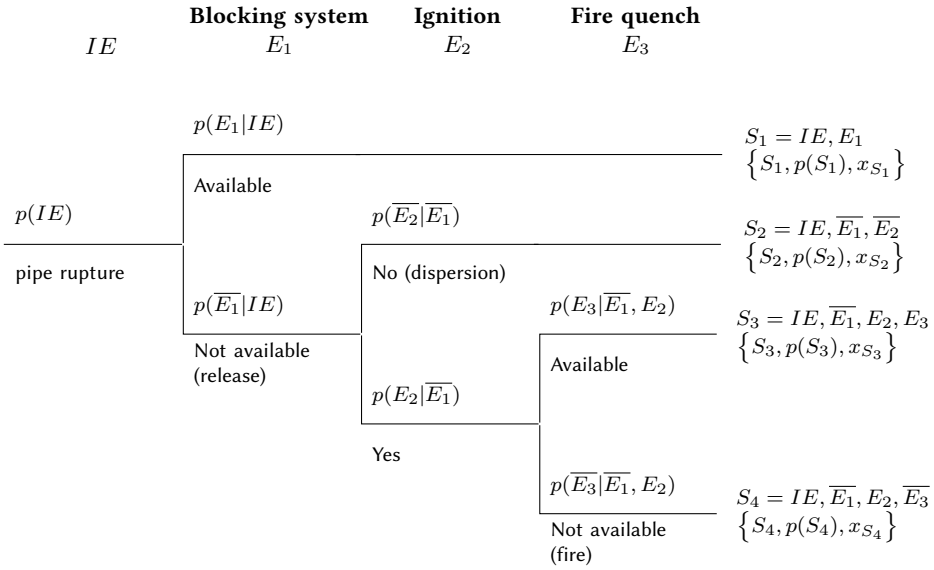

Figure 4.2 – Example of event tree in which the Initiating Event (IE) is a pipe rupture in a hydrogen compression and storage system

4.4.2 Sources of uncertainty

Uncertainty corresponding to STEP 4 of risk assessment (namely, quantitative analysis of the accident sequences) typically affects:

- ▷ the values of the **conditional probabilities** of occurrence of the events composing the accident scenarios;
- ▷ the **modeling of the accident scenarios** by means of traditional event tree and fault tree methodologies;
- ▷ the **consequences of the accident scenarios** (*i.e.*, in practice, the mathematical models and the computer codes simulating the phenomenological events included in the accident scenarios).

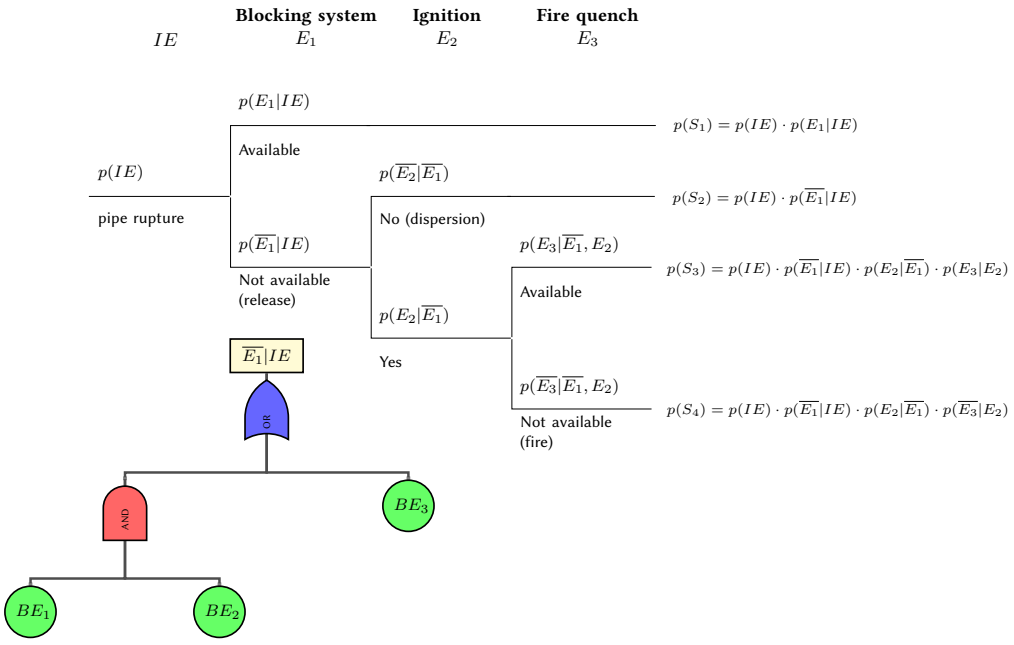

Figure 4.3 – Schematics of the event tree shown in figure 4.2 with an exemplary fault tree used to evaluate the probability $p(E_1|IE)$ of event E_1 conditional on the occurrence of the Initiating Event.

Uncertainties affecting the probabilities of the events included in the accident scenarios

Epistemic uncertainties typically affect the values of the probabilities and frequencies of the events included in the accident scenarios of interest: for example, *failure and repair rates of mechanical components, probabilities of failure on demand of safety systems, probabilities of human errors, probabilities and frequencies of phenomenological and external events* are typically affected by **epistemic uncertainty** due to lack of knowledge and/or data on the physical phenomena involved and/or to limited or (possibly) null operating experience of the corresponding component or system over the wide range of conditions encountered during operation[2]; then, the uncertainties in the probabilities of the branching events obviously propagate onto the probabilities of the accident scenarios. By way of example, referring to figures 4.2 and 4.3 of § 4.2.1, the values of probabilities $p(IE)$, $p(E_1|IE)$, $p(\overline{E_3}|E_2)$, $p(BE_1)$, $p(BE_3)$, *etc.*, and consequently $p(S_1)$, $p(S_2)$, ..., $p(S_4)$ are typically affected by epistemic uncertainty.

However, it is useful to consider different practical cases that may be encountered in the tasks of estimating the probability of events included in the accident scenarios and representing the corresponding epistemic uncertainty:

- ▷ in case of events dominated by hardware failures (*i.e.*, failures of mechanical components), a sufficient amount of (failure) data is usually available to the analysts for statistical manipulation and estimation; this quantitative information is then frequently combined with expert judgment to build probability distributions, within a subjective view of probability **[Huanga et al. 2001; Baraldi and Zio 2008]**;
- ▷ in case of events dominated by human failures, the analyst may not have sufficiently refined knowledge or opinion to characterize the associated relevant epistemic uncertainty in terms of probability distributions because i) the amount of (failure) data is limited or even null, ii) the collection and treatment of (failure) data is difficult or even impossible and/or iii) the available information/data is often of qualitative nature (*i.e.*, it is expressed in terms of fuzzy linguistic rules) **[Huanga et al. 2001; Baraldi and Zio 2008]**. In such cases, theories alternative to the probabilistic one (*e.g.*, fuzzy, evidence or possibility theories) have to be sought to represent the corresponding epistemic uncertainty **[Zadeh 1965; Dempster 1967; Shafer 1976; Dubois and Prade 1988; Dubois 2006]**;

[2] This issue is particularly relevant for systems employing new technologies.

- in case of phenomenological events (*gas release, dispersion, ignition, fire propagation, natural circulation of fluids, ...*) and external events (*earthquakes, floods, etc.*), epistemic uncertainty is due to lack of knowledge on the physical phenomena involved and to scarce or null experience over a wide range of operative conditions (*e.g.*, because they are difficult to reproduce and study through laboratory experiments). In such cases, an estimate of the probability of the phenomenological event is usually obtained by *simulating* the physical phenomena of interest by means of a **mathematical model** translated into a — often, rather complex — **computer code** [Fong et al. 2009].

Uncertainty of heat transfer coefficients

The epistemic uncertainty associated to the values of the heat transfer coefficients for fluids in natural convection is much larger than in forced convection: thus, evaluating the failure probability of a safety system relying on naturally circulating water (e.g., a passive decay heat removal system in a nuclear reactor) is more difficult than estimating the failure probability of a safety system based on mechanical pumps [Burgazzi 2007].

Uncertainties affecting the modeling of the accident scenarios

The modeling of the accident scenarios and of the system behavior introduces an additional source of epistemic uncertainty into the analysis because it typically requires a **simplification** and **approximation of reality**. Thus, uncertainty is typically related to:

- the capability of the available modeling techniques to provide an effective and realistic representation of the behavior of the system during an accidental transient. For example, whereas event tree and fault tree methodologies typically undertake the classical binary success/failure logic, the performance of real systems may settle on different levels depending on the operative conditions and on the degradation state of the constitutive multi-state components [Zio and Podofillini 2003]. In addition, event tree and fault tree techniques are essentially static and cannot take into account time-dependent physical evolutions typical of real systems [Siu 1994];
- the heavily approximate nature of the models describing **human behavior**: in particular, the difficult and incomplete identification of the possible factors influencing human performance and of the corresponding interactions and effects, the unavoidable variability of the behavior of different individuals in the same situations and the difficult description and modeling of interactions/relationships in work teams [Chang and Mosleh 2007];
- the lack of well-founded models to describe the (failure) behavior of software and digital instrumentation and control systems [Zhu et al. 2007].

Uncertainties affecting the consequences of the accident scenarios

The estimation of the consequences of each accidental scenarios requires the *simulation* of the physical phenomena included in the event tree branches (*e.g.*, *gas release, dispersion, ignition, fire propagation, natural circulation of fluids, heat radiation* and so on) by means of properly built **mathematical models** that are usually translated into deterministic **computer codes**. Thus, the uncertainties associated to the consequences of the accident scenarios are related to those affecting the simulation of the phenomenological events included in the event tree branches and the corresponding mathematical models and computer codes.

The classification provided here is by no means complete or even unique, but is intended only to illustrate some of the dominant sources of uncertainty in simulation models. Excepting some changes in terminology, the following classification scheme that we have adopted is consistent with that provided by [Kennedy and O'Hagan 2001]:

- **Aleatory parametric uncertainty**: Because models are idealizations of some real phenomena, they frequently allow for greater control over the input parameter values than can actually be realized. However, it may not be possible to specify, or control, the values of some of these inputs in the real system. Moreover, the system may interact with its environment in a complicated and dynamic manner so that some of the inputs are effectively random. The distinguishing feature of these parameters is that their values could conceivably change each time the code is run. For instance, if the computational model must repeatedly call a subroutine that contains an aleatory variable, a new value

must be randomly selected from its distribution for each call to this subroutine. Consequently, repeated runs of the code under identical input configurations will lead to different outputs, and the output of the code will be a random variable **[Langewisch 2010]**.

Random loads on a structure

Typical examples of aleatory parametric uncertainty are represented by the random variation of the geometrical dimensions and material properties of a simulated component or system (due to differences between the as-built system and its design upon which the analysis is based) or by the random loads and resistances of structures in structural reliability simulation codes.

▷ **Epistemic parametric uncertainty**: Not all the inputs to the model will be random in the sense described above. Nevertheless, when attempting to simulate some phenomena, it is necessary to specify these remaining parameters in a manner that is consistent with the actual system being simulated. In practice, however, the appropriate values of many of these parameters may not be precisely known due to a lack of data concerning the phenomena under consideration. As described previously, this type of uncertainty is one instance of epistemic uncertainty. More specifically, we refer to this uncertainty as epistemic parametric uncertainty. Epistemic parametric uncertainty is distinguished from aleatory parametric variability in that, in the case of the former, the input parameter takes some fixed, albeit unknown, value. Thus, the value does not change each time the model is run.

Power level of a nuclear reactor

Typical examples of epistemic parametric uncertainty are represented by the parameters used to describe the system (e.g., power level, pressure, temperature, material conductivity, mass flow rate, ...), e.g. owing to errors in their measurement or insufficient data and information. For example, according to industry practice and experience, an error of 2% is usually considered in the determination of the power level in a nuclear reactor, due to uncertainties in the measurements. As a consequence, the power level is usually known only to a certain level of precision, i.e., epistemic parametric uncertainty is associated with it **[Pagani et al. 2005]**.

▷ **Epistemic model uncertainty** (or model inadequacy): this form of uncertainty arises because mathematical models are simplified representations of real systems and, therefore, their results may be affected by error or bias. Model uncertainty (or inadequacy) also includes the fact that the model could be too simplified and therefore would neglect some important phenomena affecting the final result: this latter type of uncertainty is sometimes identified independently from model uncertainty and is known as **completeness uncertainty [USNRC 2009]**. In practice, even if there was no (aleatory or epistemic) parameter uncertainty (so that we knew the *true* values of the parameters and variables required to make a particular estimate of the state of the system being modeled), the *estimated* value would not equal the *true* value of the system state: this discrepancy is due to model inadequacy.

Model uncertainty

Model uncertainty (or inadequacy) may for example involve the correlations adopted to describe Thermal-Hydraulic (T-H) phenomena, which are subject to errors of approximation. Such uncertainties may for example be captured by multiplicative ($z = c(x) \cdot \varepsilon$) or additive models ($z = c(x) + \varepsilon$) **[Zio and Apostolakis 1996]**, *where z is the real value of the quantity to be predicted (e.g. heat transfer coefficients, friction factors, Nusselt numbers or thermal conductivity coefficients), $c(\bullet)$ is the mathematical model of the correlation (i.e., the result of the correlation as computed by the T-H code), x is the vector of correlating variables and ε is the associated multiplicative or additive error factor: as a result, the uncertainty in the quantity z to be predicted is translated into an uncertainty in the multiplicative or additive error factor ε. This error is commonly classified as representing model uncertainty.*

As a final remark, notice that the simulation of complex accident sequences requires the concatenation of several simulation models, each one introducing an amount of uncertainty in the analysis; thus, long and complex accident sequences may produce an "explosion" of the associated uncertainty.

4.5 STEP 5 Risk evaluation and decision making process

The main features of the last step of the risk assessment procedure (namely, risk evaluation and decision making process) are described in § 4.5.1, whereas the corresponding sources of uncertainty are summarized in § 4.5.2.

4.5.1 Description

The conclusive phase of risk analysis consists of the **evaluation of the risk** associated to the accident scenarios identified and quantified in the previous step (§ 4.4). In practice, the risk associated to the accident scenarios is usually classified as "acceptable" (*i.e.*, the current system design guarantees an adequate control of risk), "almost acceptable" or "As Low As Reasonably Practicable" (ALARP) (*i.e.*, changes to the system design and/or management are suggested) and "unacceptable" (*i.e.*, more detailed investigations and changes to the system design and/or management are recommended).

A possible approach for classifying the accident scenarios $S_i, i \in \{1, 2, ...\}$, is represented graphically in figure 4.4, where the probabilities $p(S_i), i \in \{1, 2, ...\}$ of the scenarios are plotted against their consequences $x_{S_i}, i \in \{1, 2, ...\}$[3]. Then, each scenario is represented in the diagram as a point: for example, referring to figure 4.4, scenario S_1 would be classified as "unacceptable", scenario S_2 as "ALARP" and scenario S_3 as "acceptable".

On the basis of this classification and visual representation, the decision maker first identifies the most effective strategy to reduce risk (*e.g.*, **prevention**, *i.e.* reduction of the probability of the accident, or **mitigation**, *i.e.* reduction of the consequences of the accident); then, a detailed risk-informed analysis of the system leads to the choice of the practical design and/or management modifications to prevent and/or mitigate the accident.

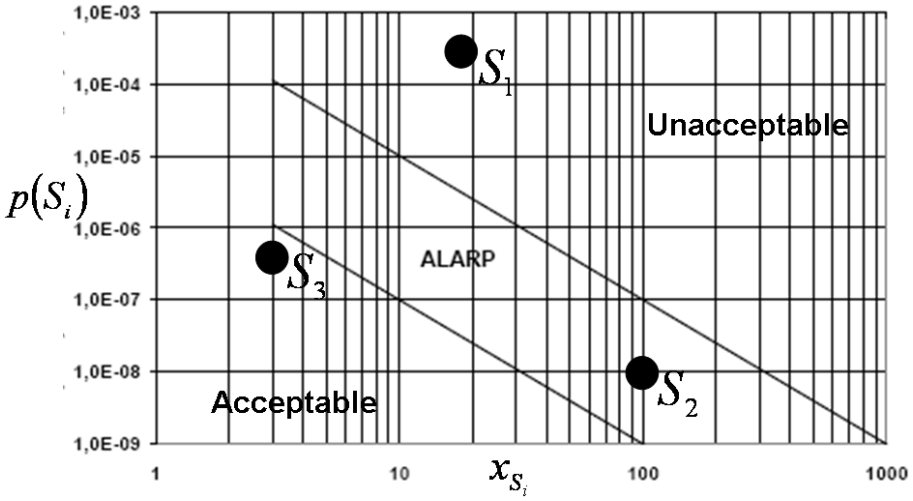

Figure 4.4 – Possible criteria for risk classification: scenario S_1 is "unacceptable", scenario S_2 is "ALARP" and scenario S_3 is "acceptable". The horizontal axis is the consequence of scenarios, on a logarithmic scale. The vertical axis is the probability of the scenarios, on a log scale.

[3] Consequences could be expressed for instance in terms of *number of fatalities*

4.5.2 Sources of uncertainty

This phase of risk quantification and evaluation is affected by all the types of uncertainties introduced in the previous phases of the analysis, which therefore impact the outputs of the risk assessment procedure.

From the modeling and methodological viewpoint, the phase of risk estimation and evaluation is affected by the lack of well-sounded and rigorous criteria for the evaluation of **risk acceptability**. Indeed, risk estimation is known to be affected by a number of factors:

risk acceptability

- ▷ heuristics used by people when dealing with complex, probabilistic problems (also known as *cognitive biases*) which affect risk perception **[Kahneman et al. 1982]**), such as:
  - the **availability heuristic** (the probability of an event is estimated by the ease with which examples of the event come to mind), which studies have for instance shown leads to underestimation of the frequency of common causes of death **[Lichtenstein et al. 1978]**;
  - **anchoring and adjustment effects**, which lead people to place too much importance on the first information one obtained on a subject (the "anchor"), operating by incremental adjustments with respect to that anchor instead of weighting new evidence in the same way as the initial estimate;
  - overconfidence or **optimism bias**, which is a tendency for people to be overly optimistic about the outcome of planned actions (including overestimating the probability of positive events and underestimating that of negative events) **[Oskamp 1965]**;
  - **illusion of control**, the tendency for people to overestimate their ability to control events **[Langer 1975]**.
- ▷ heuristics used in individual decision-making under risk and uncertainty, such as irrational escalation[4], loss aversion, and endowment effects[5];
- ▷ group decision biases, such as conformity and **group polarization** (the tendency for people in group situations to form opinions and reach decisions which are more extreme, or more risky, than when they decide alone), **groupthink [Janis 1982]** and possibly cyclic preferences in group decisions[6].

Beyond the objective level of risk generated by a project, a number of aspects are known to influence people's judgment as to the acceptability of an activity (*cf.* for instance **[Sandman 1989]**):

- ▷ is the origin of the risk natural or industrial/technological?
- ▷ is the nature of the hazard familiar to people, or unfamiliar?
- ▷ are the possible effects memorable or easily forgotten, dreaded or not?
- ▷ is the hazard of a catastrophic or a chronic nature?
- ▷ is exposure to the risk perceived to be fair, or unfair (issues related to equity)?
- ▷ is the activity perceived to be morally relevant?
- ▷ are sources of information concerning the risk and the activity perceived to be trustworthy?
- ▷ is the governance of the industrial activity and the risk management process perceived to be open and responsive?

Finally, this operation is strongly influenced by the social, economic and cultural context of a given country: thus, the level of risk acceptability associated to the operation of the same

[4] Irrational escalation, also known as the *sunk cost fallacy*, is a phenomenon where people justify maintaining a decision by prior investment, despite new evidence suggesting that the cost, starting today, of continuing the decision outweighs the expected benefit.

[5] The endowment effect, also known as *status quo bias*, is the observation that people often demand much more to give up an object than they would be willing to pay to acquire it.

[6] Condorcet's voting paradox, a situation noted by the Marquis de Condorcet in the 18^{th} century, is a situation where collective preferences can be cyclic, even if the preferences of individual voters are not. This shows that majority voting in a group of people may fail to yield a stable outcome. The paradox was generalized by the economist Arrow, leading to Arrow's impossibility theorem **[Arrow 1950]**, proving the absence of a social choice rule that respects a number of plausible requirements.

typology of system (*e.g.*, nuclear, chemical, ...) will be different in different countries. An example of this variability is shown in figure 4.5, concerning a system for the compression and storage of hydrogen.

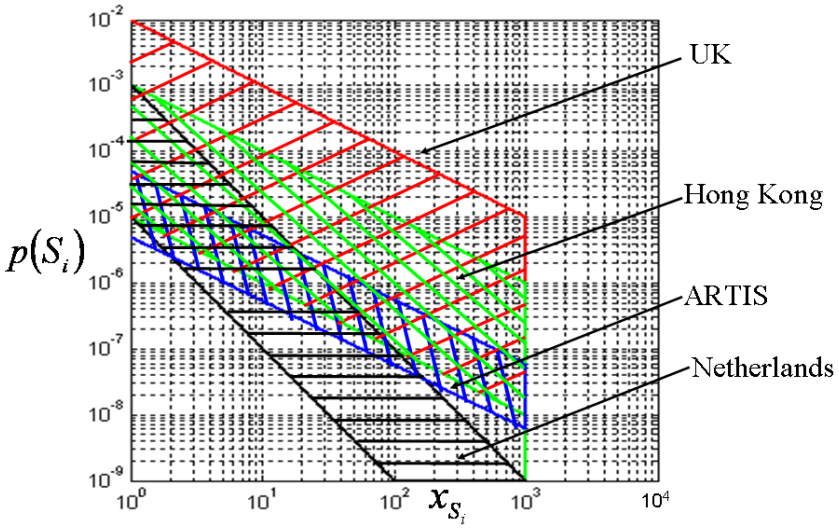

Figure 4.5 – Different criteria for classification of risk in different countries, with reference to a system for the compression and storage of hydrogen

A

The HAZID technique

A.1 Definitions

Hazard analysis is defined as a systematic and iterative process of the identification, classification and reduction of hazards[1]. Hazard Identification (HAZID) is aimed at assessing all hazards that could directly and indirectly affect the safe – correct operation of the plant – system.

A.2 Main concepts

Figures A.1 and A.2 sketch the concepts which HAZID is based on: hazards reveal themselves through hazard manifestations and are activated if initiating events occur (the combination of a hazard and an initiating event is a *mishap*, *i.e.*, an unplanned event or series of events resulting in death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment). The causes of the events that activate hazards, the sequence of the events that may occur in consequence of this activation and their effects define the Hazard Scenario (figure A.2). Notice that different hazard scenarios can originate from the same hazard and different hazard scenarios can lead to the same consequence (dashed arrows in figure A.2). The impact that the final effects have on properties and safety is evaluated and the probability of occurrence of these effects provide the basis for making the final decision about the risk acceptability.

A HAZID study is carried out by a team of competent engineers from a mixture of disciplines, led by an analyst who is experienced in the HAZID technique. Each area, or zone, of the installation is considered against a **checklist of hazards**. Where it is agreed that a hazard exists in a particular area, the risk presented by the hazard is considered, and all possible means of either eliminating the hazard or controlling the risk and/or the necessity for further study are noted on a HAZID worksheet. Actions are assigned to either discipline groups or individuals to ensure the mitigating control, or further study is completed.

A.3 Essentials

A.3.1 HAZID Objectives

- ▷ Identify hazards to host facilities due to design, and evaluate potential consequences should the hazards be realized;
- ▷ Establish safeguards to manage hazards; identify areas where further understanding of safeguard effectiveness is needed;
- ▷ Make recommendations to reduce the likelihood of hazard occurrence or mitigate the potential consequences.

The HAZID method, accepted as one of the best techniques for identifying potential hazards and operability problems, involves the following:

- ▷ Assembly of a team of experienced project personnel;

[1] A hazard is any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment or property; or damage to the environment. Notice that hazards are not events, but the prerequisite for the occurrence of hazard scenarios with their negative effects on safety and properties.

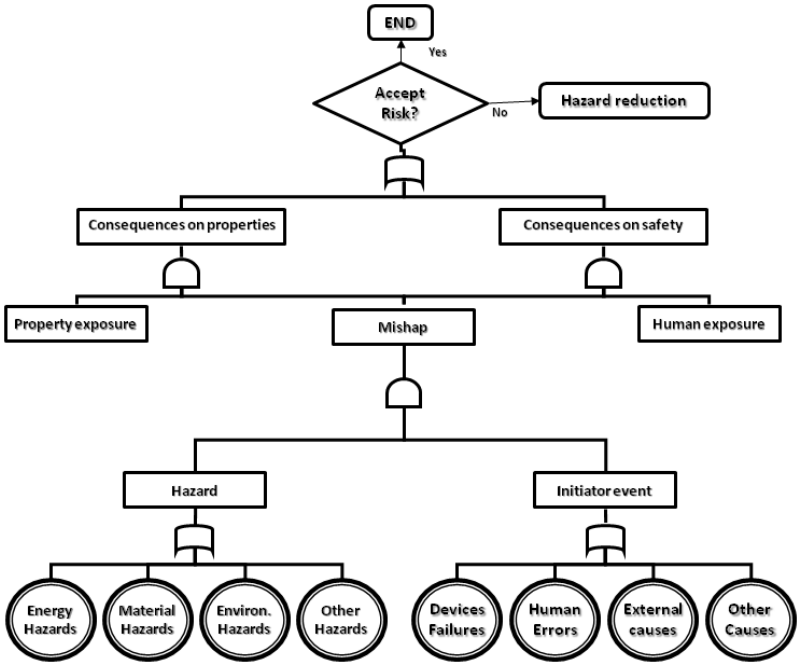

Figure A.1 – Concepts underlying HAZID

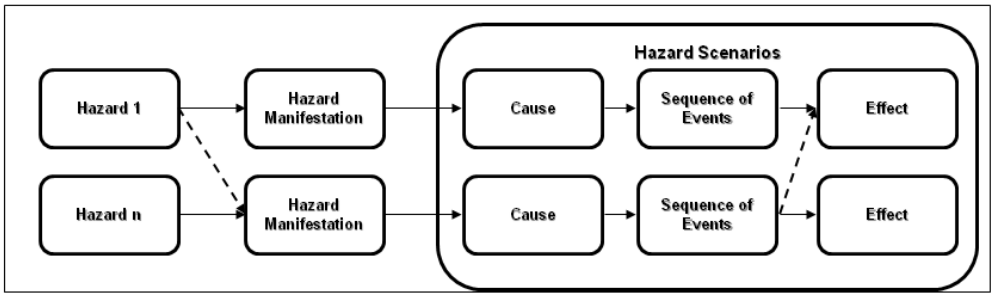

Figure A.2 – Hazards and hazard scenarios

- ▷ Presentations detailing the scope of the HAZID;
- ▷ Identify hazards, causes, consequences and safeguards. Notice that the main "sources" used for this task are:
  - analysis of similar systems;
  - preliminary Hazard Lists (provided by reference standards);
  - expert knowledge;
  - lessons learnt;
  - analysis of environmental constraints, including the operating environment (*drop, shock, vibration, extreme temperature, noise, confined space, fire, electrostatic discharge, lightning, etc.*);
  - analysis of operating test, maintenance, and emergency procedures.
- ▷ Make recommendations to address hazards, as appropriate;
- ▷ Risk ranking of hazardous events.

A.3.2 Key Benefits to Client

- ▷ Existing design knowledge is efficiently captured relative to client's projects;
- ▷ Numerous procedural, equipment design, testing, and process control recommendations allow expedited development of standardized equipment.

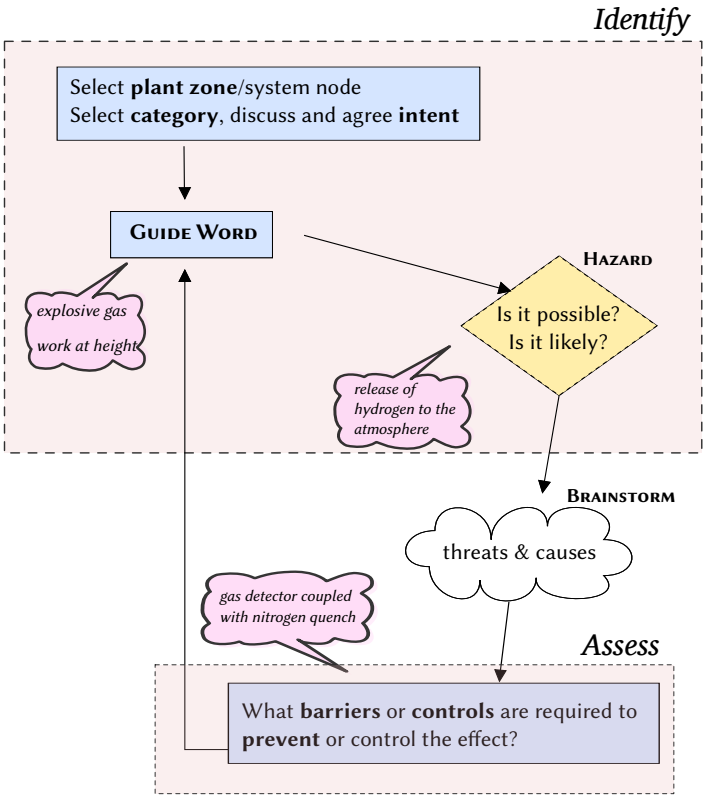

Figure A.3 – The HAZID process (*cf.* § 4.2.1 for definitions)

A.3.3 Process steps

1. Define the purpose, objectives, and scope of the study;
2. Select the team;
3. Prepare for the study;
4. Carry out the team review;
5. Record the results.

B

Fault-tree analysis

B.1 Introduction

For complex multi-component systems, for example such as those employed in the nuclear, chemical, process and aerospace industries, it is important to analyze the possible mechanisms of failure and to perform probabilistic analyses for the expected frequency of such failures. Often, each such system is unique in the sense that there are no other identical systems (same components interconnected in the same way and operating under the same conditions) for which failure data have been collected: therefore a statistical failure analysis is not possible. Furthermore, it is not only the probabilistic aspects of failure of the system which are of interest but also the initiating causes and the combination of events which can lead to a particular failure.

The engineering way to tackle a problem of this nature, where many events interact to produce other events, is to relate these events using simple logical relationships (intersection, union, *etc.*) and to methodically build a logical structure which represents the system.

In this respect, fault tree analysis is a systematic, deductive technique which allows to develop the causal relations leading to a given undesired event. It is deductive in the sense that it starts from a defined system failure event and unfolds backward its causes down to the primary (basic) independent faults. The method focuses on a single **system failure mode** and can provide qualitative information on how a particular event can occur and what consequences it leads to, while at the same time allowing the identification of those components which play a major role in determining the defined system failure. Moreover it can be solved in quantitative terms to provide the probability of events of interest starting from knowledge of the probability of occurrence of the basic events which cause them.

In the following, we shall give only the basic principles of the technique. The interested reader is invited to look at the specialized literature for further details, *e.g.* **[Zio 2007]** and references therein from which the material herein contained has been taken.

B.2 Fault tree construction

A fault tree is a graphical representation of causal relations obtained when a system failure mode is traced backward to search for its possible causes. To complete the construction of a fault tree for a complex system, it is necessary to first understand how the system functions. A system flow diagram (such as a reliability block diagram) is used for this purpose, *e.g.* to depict the pathways by which materials are transmitted between components of the system.

The first step in fault tree construction is the selection of the **system failure event** of interest. This is called the **top event**; every following event will be considered in relation to its effect upon it.

The next step is to identify **contributing events** that may directly cause the top event to occur. At least four possibilities exist **[Henley and Kumamoto 1992]**:

1. no input to the device;
2. primary failure of the device (under operation in the design envelope, random, due to aging or fatigue);
3. human error in actuating or installing the device;

4. secondary failure of the device (due to present or past stresses caused by neighboring components or the environments: for instance common cause failure, excessive flow, external causes such as earthquakes).

If these events are considered to be indeed contributing to the system fault, then they are connected to the top event logically via an OR function and graphically through the OR gate (*cf.* figure B.1).

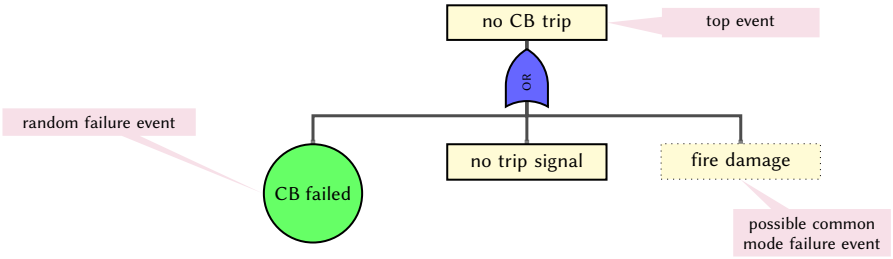

Figure B.1 – Top and first level of a fault tree for a circuit breaker (CB) failing to trip an electrical circuit, after **[GE 1974]**

Once the first level of events directly contributing to the top has been established, each event must be examined to decide whether it is to be further decomposed in more elementary events contributing to its occurrence. At this stage, the questions to be answered are:

- ▷ is this event a primary failure?
- ▷ is it to be broken down further in more primary failure causes?

In the first case, the corresponding branch of the tree is terminated and this primary event is symbolically represented by a circle. This also implies that the event is independent of the other terminating events (circles) which will be eventually identified and that a numerical value for the probability of its occurrence is available if a quantitative analysis of the tree is to be performed.

On the contrary, if a first level contributing event is not identified as a primary failure, it must be examined to identify the sub-events which contribute to its occurrence and their logical relationships (*cf.* figure B.2).

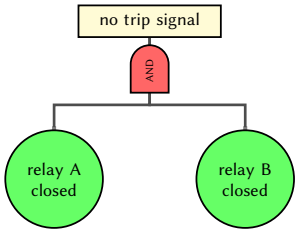

Figure B.2 – AND function example for the circuit breaker of the electrical system with the top event of Figure B.1, after **[GE 1974]**

The procedure of analyzing every event is continued until all branches have been terminated in independent primary failures for which probability data are available. Sometimes, certain events which would require further breakdown can be temporarily classified as primary at the current state of the tree structure and assigned a probability by rule of thumb. These underdeveloped events are graphically represented by a diamond symbol rather than by a circle.

A fault tree can be described by a set of Boolean algebraic equations, one for each gate of the tree. For each gate, the input events are the independent variables and the output event is the dependent variable. Utilizing the rules of Boolean algebra it is then possible to solve these equations so that the top event is expressed in terms of sets of primary events only.

Finally, the quantitative analysis of the fault tree consists of transforming its logical structure into an equivalent probability form and numerically calculating the probability of occurrence

of the top event from the probabilities of occurrence of the basic events. The probability of the basic event is the failure probability of the component or subsystem during the mission time of interest. The corresponding mathematical details can be found in **[Zio 2007]**.

C

Event tree analysis

Event trees are inductive logic methods for identifying the various accident sequences which can originate from a single initiating event. The approach is based on the discretization of the real accident evolution in a small number of macroscopic events. The accident sequences derived are then quantified in terms of their **probability of occurrence**.

The events delineating the accident sequences are usually characterized in terms of:

1. the intervention (or not) of protection systems which are supposed to take action for the mitigation of the accident (*system event tree*);
2. the fulfillment (or not) of safety functions (*functional event tree*);
3. the occurrence or not of physical phenomena (*phenomenological event tree*).

Typically, the functional event trees are an intermediate step to the construction of system event trees: following the accident-initiating event, the safety functions which need to be fulfilled are identified; these will later be substituted by the corresponding safety and protection systems.

The system event trees are used to identify the accident sequences developing within the plant and involving the protection and safety systems.

The phenomenological event trees describe the accident phenomenological evolution outside the plant (*fire, contaminant dispersion, ...*).

In the following, we shall give only the basic principles of the technique. The interested reader is invited to consult the specialized literature for further details, *e.g.* **[Zio 2007]** and references therein from which most of the material herein has been taken.

C.1 Event tree construction

An event tree begins with a defined accident-initiating event which could be a component or an external failure. It follows that there is one event tree for each different accident-initiating event considered. This aspect obviously poses a limitation on the number of initiating events which can be analyzed in details. For this reason, the analyst groups similar initiating events and only one representative initiating event for each class is investigated in details. Initiating events which are grouped in the same class are usually such to require the intervention of the same safety functions and to lead to similar accident evolutions and consequences.

Once an initiating event is defined, all the safety functions that are required to mitigate the accident must be defined and organized according to their time of intervention. For example (*cf.* figure C.1) if the initiating event (IE) is the rupture of a pipe with release of flammable liquid and the sparking of jet-fire, the first function required would be that of interception of the released flow rate, followed by the cooling of adjacent tanks and finally the quenching of the jet. These functions are structured in the form of headings in the functional event tree. For each function, the set of possible success and failure states must be defined and enumerated. Each state gives rise to a branching of the tree (*cf.* figure C.1). For example, in the typical binary success/failure logic it is customary to associate to the top branch the success of the function and to the bottom branch its failure.

Figure C.1 shows a graphical example of a system event tree: the initiating event is depicted by the initial horizontal line and the system states are then connected in a stepwise, branching fashion: system success and failure states have been denoted by S and F, respectively.

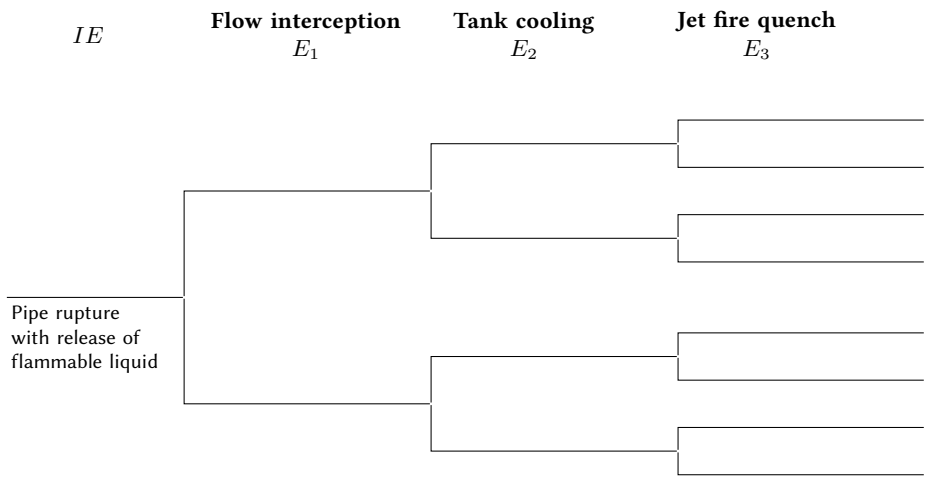

Figure C.1 – Example of functional event tree, after **[Zio 2007]**

The accident sequences that result from the tree structure are shown in the last column. Each branch yields one particular accident sequence; for example, IS_1F_2 denotes the accident sequence in which the initiating event *IE* occurs, system 1 is called upon and succeeds (S_1), and system 2 is called upon but fails to perform its defined function (F_2). For larger event trees, this stepwise branching would simply be continued. Note that the system states on a given branch of the event tree are conditional on the previous system states having occurred. With reference to the previous example, the success and failure of system 1 must be defined under the condition that the initiating event has occurred; likewise, in the upper branch of the tree corresponding to system 1 success, the success and failure of system 2 must be defined under the conditions that the initiating event has occurred and system 1 has succeeded.

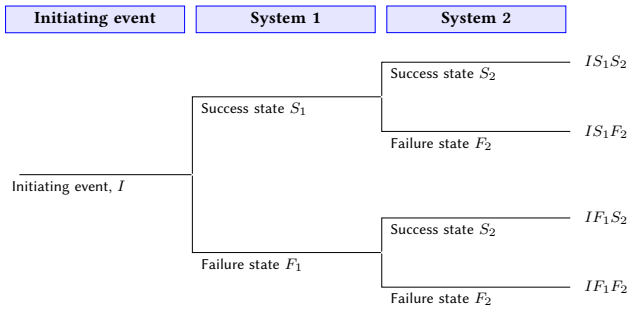

Figure C.2 – Illustration of system event tree branching, after **[USNRC 1975]**

C.2 Event tree evaluation

Once the final event tree has been constructed, the final task is to compute the probabilities of system failure. Each event (branch) in the tree can be interpreted as the top event of a fault tree which allows the evaluation of the probability of the occurrence of such event. The value thus computed represents the conditional probability of the occurrence of the event, given that the events which precede on that sequence have occurred. Multiplication of the conditional probabilities for each branch in a sequence gives the probability of that sequence (*cf.* figure C.3).

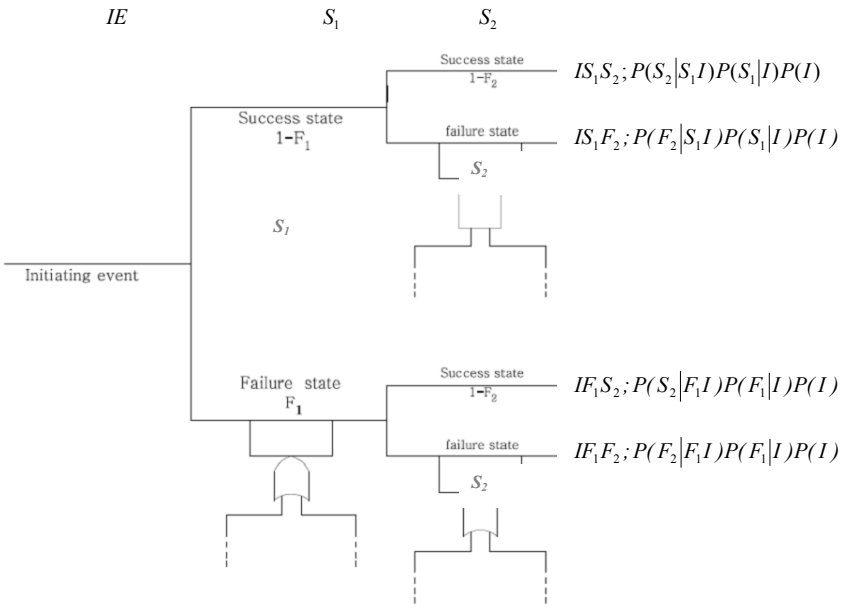

Figure C.3 – Schematics of the event tree shown with the fault trees used to evaluate the probabilities of different events

Bibliography

Apostolakis, G. E. (1990). The concept of probability in safety assessment of technological systems. *Science*, 250(4986):1359–1364. DOI: 10.1126/science.2255906.

Apostolakis, G. E. (1995). A commentary on model uncertainty. In *Proceedings of the Workshop on Model Uncertainty: its Characterization and Quantification*, 13–22 pages, Center for Reliability Engineering, University of Maryland, College Park, Maryland. Also published as NUREG/CP-0138, U.S. Nuclear Regulatory Commission.

Apostolakis, G. E. (1999). The distinction between aleatory and epistemic uncertainties is important: an example from the inclusion of ageing effects into PSA. In *Proceedings of the International Topical Meeting on Probabilistic Safety Assessment (PSA'99)*, 135–142 pages, Washington, D.C.

Apostolakis, G. E. (2006). PRA/QRA: an historical perspective. In *2006 Probabilistic/quantitative risk assessment workshop*, Taiwan.

Armacosta, R. L. and Pet-Edwards, J. (1999). Integrative risk and uncertainty analysis for complex public sector operational systems. *Socio-Economic Planning Sciences*, 33(2):105–130. DOI: 10.1016/S0038-0121(98)00004-4.

Arrow, K. J. (1950). A difficulty in the concept of social welfare. *Journal of Political Economy*, 58(4):328–346. Available at http://gatton.uky.edu/Faculty/hoytw/751/articles/arrow.pdf.

Aven, T. (2003). *Foundations of Risk Analysis: A Knowledge and Decision-Oriented Perspective*. Wiley. ISBN: 978-0471495482, 206 pages.

Aven, T. (2010a). On the need for restricting the probabilistic analysis in risk assessments to variability. *Risk Analysis*, 30(3):354–360. DOI: 10.1111/j.1539-6924.2009.01314.x.

Aven, T. (2010b). Some reflections on uncertainty analysis and management. *Reliability Engineering & System Safety*, 95(3):195–201. DOI: 10.1016/j.ress.2009.09.010.

Aven, T. and Zio, E. (2011). Some considerations on the treatment of uncertainties in risk assessment for practical decision making. *Reliability Engineering & System Safety*, 96(1):64–74. DOI: 10.1016/j.ress.2010.06.001.

Baraldi, P. and Zio, E. (2008). A combined Monte Carlo and possibilistic approach to uncertainty propagation in event tree analysis. *Risk Analysis*, 28(5):1309–1325. DOI: 10.1111/j.1539-6924.2008.01085.x.

Bedford, T. and Cooke, R. (2001). *Probabilistic Risk Analysis. Foundations and Methods*. Cambridge University Press, Cambridge. ISBN: 978-0521773201, 414 pages.

Burgazzi, L. (2007). Addressing the uncertainties related to passive system reliability. *Progress in Nuclear Energy*, 49(1):93–102. DOI: 10.1016/j.pnucene.2006.10.003.

Carpiognano, A., Ganci, F., and Ponte, E. (2007). Methods of evaluation of uncertainties in the risk assessment of complex technological systems: application to an hydrogen refuelling station. Technical report, Politecnico di Milano.

Chang, Y. H. J. and Mosleh, A. (2007). Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents: Part 1: Overview of the IDAC model. *Reliability Engineering & System Safety*, 92(8):997–1013.

Dempster, A. P. (1967). Upper and lower probabilities induced by a multivalued mapping. *The Annals of Mathematical Statistics*, 38(2):325–339. DOI: 10.1214/aoms/1177698950.

Dubois, D. (2006). Possibility theory and statistical reasoning. *Computational Statistics and Data Analysis*, 51:47–69. DOI: 10.1016/j.csda.2006.04.015.

Dubois, D. and Prade, H. (1988). *Théorie des possibilités: application à la représentation des connaissances en informatique*. Masson, Paris. ISBN: 978-2225805790.

ECSS (1999). Space engineering: functional analysis (ECSS-E-10-05A). Technical report, European Cooperation on Space Standardization (ESA/ESTEC), Noordwijk, Netherlands.

ECSS (2003). Hazard analysis (ECSS-Q-40-02A). Technical report, European Cooperation on Space Standardization (ESA/ESTEC), Noordwijk, Netherlands.

Farmer, F. R. (1964). The growth of reactor safety criteria in the United Kingdom. In *Proceedings of the Anglo-Spanish power symposium*, Madrid.

Ferson, S. and Ginzburg, L. R. (1996). Different methods are needed to propagate ignorance and variability. *Reliability Engineering & System Safety*, 54(2):133–144. DOI: 10.1016/S0951-8320(96)00071-3.

Fong, C. J., Apostolakis, G. E., Langewish, D. R., Hejzlar, P., Todreas, N. E., and Driscoll, M. J. (2009).

Reliability analysis of a passive cooling system using a response surface with an application to the flexible conversion ratio reactor. *Nuclear Engineering and Design*, 239(12):2660–2671.

Garrick, B. J. and Gekler, W. C. (1967). Reliability analysis of nuclear power plant protective systems (HN-190). Technical report, US Atomic Energy Commission, Los Angeles, California. Available at http://www.osti.gov/bridge/servlets/purl/4568767-q8QGlL/4568767.pdf.

GE (1974). Reliability manual for liquid metal fast reactor (LMFBR) safety programs. Technical report, General Electric Company. SRD-74-113.

Helton, J. C. (1998). Uncertainty and sensitivity analysis results obtained in the 1996 performance assessment for the waste isolation power plant (SAND98-0365). Technical report, Sandia National Laboratories.

Helton, J. C. and Oberkampf, W. L. (2004). An exploration of alternative approaches to the representation of uncertainty in model predictions. *Reliability Engineering & System Safety*, 85(1):39–71. Special issue on Alternative Representations of Epistemic Uncertainty. DOI: 10.1016/j.ress.2004.03.025.

Henley, E. J. and Kumamoto, H. (1992). *Probabilistic risk assessment: Reliability Engineering, Design, and Analysis*. IEEE Press, New York. ISBN: 978-0879422905, 568 pages.

Hofer, E., Kloos, M., Krzykacz-Hausmann, B., Peschke, J., and Woltereck, M. (2002). An approximate epistemic uncertainty analysis approach in the presence of epistemic and aleatory uncertainties. *Reliability Engineering & System safety*, 77(3):229–238. DOI: 10.1016/S0951-8320(02)00056-X.

Huanga, D., Chenb, T., and Wang, M. J. (2001). A fuzzy set approach for event tree analysis. *Fuzzy Sets and Systems*, 118(1):153–165. DOI: 10.1016/S0165-0114(98)00288-7.

Janis, I. L. (1982). *Groupthink: Psychological studies of political decisions and fiascos*. Cengage Learning. ISBN: 978-0395317044, 349 pages.

Kahneman, D., Slovic, P., and Tversky, A. (1982). *Judgment under uncertainty: Heuristics and biases*. Cambridge University Press, Cambridge, UK. ISBN: 978-0521284141, 544 pages.

Kaplan, S. and Garrick, B. J. (1981). On the quantitative definition of risk. *Risk Analysis*, 1(1):11–27. DOI: 10.1111/j.1539-6924.1981.tb01350.x.

Kennedy, M. C. and O'Hagan, A. (2001). Bayesian calibration of computer models. *Journal of the Royal Statistical Society B*, 63(3):425–464. Available at http://www.stat.lsa.umich.edu/pdfs/KA2001.pdf, DOI: 10.1111/1467-9868.00294.

Krzykacz-Hausmann, B. (2006). An approximate sensitivity analysis of results from complex computer models in the presence of epistemic and aleatory uncertainties. *Reliability Engineering & System safety*, 91:1210–1218. DOI: 10.1016/j.ress.2005.11.019.

Langer, E. J. (1975). The illusion of control. *Journal of Personality and Social Psychology*, 32(2):311–328. DOI: 10.1037/0022-3514.32.2.311.

Langewisch, D. R. (2010). *Uncertainty and sensitivity analysis for long-running computer codes: a critical review*. PhD thesis, Massachusets Institute of Technology. Also published as technical report MIT-NSP-TR-024 in the Nuclear Systems Enhanced Performance (NSP) Program. Available at http://hdl.handle.net/1721.1/58285.

Lichtenstein, S., Slovic, P., Fischhoff, B., Layman, M., and Combs, B. (1978). Judged frequency of lethal events. *Journal of Experimental Psychology: Human Learning and Memory*, 4(6):551–578. DOI: 10.1037/0278-7393.4.6.551.

Lindley, D. V. (2000). The philosophy of statistics. *The Statistician*, 49(3):293–337. DOI: 10.1111/1467-9884.00238.

McCormick, N. J. (1981). *Reliability and risk analysis: methods and nuclear power applications*. Academic Press, New York. ISBN: 978-0124823600, 466 pages.

Mohaghegh, Z., Kazemi, R., and Mosleh, A. (2009). Incorporating organizational factors into probabilistic risk assessment (PRA) of complex socio-technical systems: A hybrid technique formalization. *Reliability Engineering & System Safety*, 94(5):1000–1018. DOI: 10.1016/j.ress.2008.11.006.

NASA (2002). Probabilistic risk assessment procedures guide for NASA managers and practitioners. Technical report, NASA. Available at http://www.hq.nasa.gov/office/codeq/doctree/praguide.pdf.

Nilsen, T. and Aven, T. (2003). Models and model uncertainty in the context of risk analysis. *Reliability Engineering & System Safety*, 79(3):309–317. DOI: 10.1016/S0951-8320(02)00239-9.

NPRD (1995). Nonelectronic parts reliability data (NPRD-95). Technical report, Reliability Analysis Center, Rome, NY.

Oskamp, S. (1965). Overconfidence in case-study judgments. *Journal of Consulting Psychology*, 29(3):261–265. DOI: 10.1037/h0022125.

Pagani, L. P., Apostolakis, G. E., and Hejzlar, P. (2005). The impact of uncertainties on the performance of passive systems. *Nuclear Technology*, 149(2):129–140. Available at http://pbadupws.nrc.gov/docs/ML0527/ML052790021.pdf.

Sandman, P. M. (1989). Chapter *Hazard versus Outrage in the Public Perception of Risk* in *Effective Risk*

Communication (Covello, V., McCallum, D., and Pavlova, M., Ed.), 45–49 pages. Plenum Press, New York.

Shafer, G. (1976). *A Mathematical Theory of Evidence*. Princeton University Press, Princeton, NJ. ISBN: 978-0691081755, 297 pages.

Singpurwalla, N. D. (2006). *Reliability and risk: a Bayesian perspective*. Wiley. ISBN: 978-0470855027, 396 pages.

Siu, N. (1994). Risk assessment for dynamic systems: An overview. *Reliability Engineering & System Safety*, 43(1):43–73. DOI: 10.1016/0951-8320(94)90095-7.

USDoD (1980). MIL-STD-1629: Procedures for performing a failure mode, effects and criticality analysis. Technical report, US Department of Defense, Washington, D.C.

USDoD (1993). MIL-STD-882C: System safety program requirements. Technical report, US Department of Defense, Washington, D.C.

USNRC (1975). NUREG-75/014 (WASH-1400) Reactor safety study, an assessment of accident risks. Technical report, US Nuclear Regulatory Commission, Washington, D.C. a.k.a. "the Rasmussen Report" (superseded by NUREG-1150).

USNRC (1983). PRA procedures guide: A guide to the performance of probabilistic risk assessments for nuclear power plants (NUREG/CR-2300). Technical report, US Nuclear Regulatory Commission, Washington, D.C. Available at http://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr2300/.

USNRC (1990). Severe accident risks: an assessment for five U.S. nuclear power plants (NUREG-1150). Technical report, US Nuclear Regulatory Commission. Available at http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1150/.

USNRC (2002). An approach for using probabilistic risk assessment in risk-informed decisions on plant-specific changes to the licensing basis (NUREG-1.174). Technical report, US Nuclear Regulatory Commission, Washington, D.C. Available at http://www.nrc.gov/reading-rm/doc-collections/reg-guides/power-reactors/rg/01-174/.

USNRC (2005). Fire PRA methodology for nuclear power facilities (NUREG/CR-6850). Technical report, US Nuclear Regulatory Commission, Washington, D.C. Available at http://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6850/.

USNRC (2009). Guidance on the treatment of uncertainties associated with PRAs in risk-informed decision making (NUREG-1855). Technical report, US Nuclear Regulatory Commission, Washington, D.C. Available at http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1855/v1/sr1855v1.pdf.

Walley, P. (1991). *Statistical Reasoning with Imprecise Probabilities*. Chapman and Hall. ISBN: 978-0412286605, 720 pages.

Zadeh, L. A. (1965). Fuzzy sets. *Information and Control*, 8(3):338–353. DOI: 10.1016/S0019-9958(65)90241-X.

Zhu, D., Mosleh, A., and Smidts, C. (2007). A framework to integrate software behavior into dynamic probabilistic risk assessment. *Reliability Engineering & System Safety*, 92(12):1733–1755. DOI: 10.1016/j.ress.2006.09.024.

Zimmermann, H. J. (2000). An application-oriented view of modeling uncertainty. *European Journal of operational research*, 122(2):190–198. DOI: 10.1016/S0377-2217(99)00228-3.

Zio, E. (2007). *An introduction to the basics of reliability and risk analysis*. World Scientific. ISBN: 978-9812706393, 180 pages.

Zio, E. (2009). Reliability engineering: Old problems and new challenges. *Reliability Engineering & System Safety*, 94(2):125–141. DOI: 10.1016/j.ress.2008.06.002.

Zio, E. and Apostolakis, G. E. (1996). Two methods for the structured assessment of model uncertainty by experts in performance assessments of radioactive waste repositories. *Reliability Engineering & System Safety*, 54(2):225–241. DOI: 10.1016/S0951-8320(96)00078-6.

Zio, E. and Podofillini, L. (2003). Monte Carlo simulation analysis of the effects of different system performance levels on the importance of multi-state components. *Reliability Engineering & System Safety*, 82:63–73. DOI: 10.1016/S0951-8320(03)00124-8.

Vous pouvez extraire ces entrées bibliographiques au format BibTeX en cliquant sur l'icone de trombone à gauche.

Reproducing this document

You can download this document, and others in the *Cahiers de la Sécurité Industrielle* collection, from FonCSI's web site. Documents are available in PDF, EPUB (for tablets and e-readers) and MOBI (for Kindle e-readers). Paper versions can be ordered online from a print-on-demand service.

Foundation for an Industrial Safety Culture
a public interest research foundation
http://www.FonCSI.org/

6 allée Émile Monso – BP 34038
31029 Toulouse cedex 4
France

Telephone: +33 534 32 32 00
Twitter: @TheFonCSI
Email: contact@FonCSI.org

ISSN 2100-3874

6 allée Émile Monso
ZAC du Palays — BP 34038
31029 Toulouse cedex 4

www.foncsi.org