APPORTS DE LA RECHERCHE

Risk-informed decision-making processes

An overview

Enrico Zio and Nicola Pedroni

n° 2012-10

THEME

Risk analysis

Les Cahiers de la sécurité industrielle

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

www.FonCSI.org

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

@TheFonCSI
contact@FonCSI.org

Résumé

Titre	Panorama des processus décisionnels tenant compte du risque
Mots-clefs	incertitude, analyse de risque, prise de décision, arbitrage, RIDM
Auteurs	Enrico Zio et Nicola Pedroni
Date de publication	Décembre 2012

Les auteurs présentent les concepts généraux, définitions et enjeux de la mise en œuvre de processus décisionnels tenant compte du risque (mieux connus sous leur dénomination en anglais, *Risk-informed decision-making* ou RIDM). Il s'agit de démarches structurées qui visent à aider les décisionnaires confrontés à des décisions complexes à fort enjeux, impliquant des objectifs multiples, en présence d'incertitude. Elles visent à s'assurer que le choix entre les alternatives soit fait en étant informé des risques de chaque option, et que l'ensemble des attributs d'une décision soient considérés dans un cadre intégré. Des motivations de l'utilisation de ces techniques en complément d'approches déterministes traditionnelles d'analyse de risque sont fournies.

Les processus de RIDM adoptés par la NASA et par la Nuclear Regulatory Commission, autorité de tutelle du nucléaire aux États-Unis d'Amérique, sont décrits en détail. Le document se termine par une analyse des similitudes et des différences d'approche de mise en œuvre de ces démarches entre ces deux organismes.

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). *Panorama des processus décisionnels tenant compte du risque*. Numéro 2012-10 des *Cahiers de la Sécurité Industrielle*, Fondation pour une Culture de Sécurité Industrielle, Toulouse, France (ISSN 2100-3874). DOI : 10.57071/539rdm. Disponible à l'adresse www.foncsi.org/fr/.

Abstract

Title	Overview of risk-informed decision-making processes
Keywords	risk, uncertainty, decision-making, RIDM, arbitration, PRA
Authors	Enrico Zio and Nicola Pedroni
Publication date	December 2012

The authors introduce the general concepts, definitions and issues related to the use of Risk-informed decision-making (RIDM). These are structured processes which assist decision-makers when faced with high impact, complex decisions involving multiple objectives and the presence of uncertainty. They aim to ensure that decisions between competing alternatives are taken with an awareness of the risks associated with each option, and that all attributes of a decision are considered in an integrated manner. Motivations for the use of these techniques as a complement to more traditional deterministic approaches to risk assessment are provided.

The RIDM processes adopted by NASA and by the US Nuclear Regulatory Commission are described in detail, with an analysis of commonalities and differences in approach.

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). *Overview of risk-informed decision-making processes.* Number 2012-10 of the *Cahiers de la Sécurité Industrielle*, Foundation for an Industrial Safety Culture, Toulouse, France (ISSN 2100-3874). DOI: 10.57071/539rdm. Available at www.foncsi.org/en/.

Foreword

The past two decades have seen an evolution from *risk-based* to *risk-informed* safety management approaches, in which quantitative outcomes of risk assessment are only one component of the decision-making process, being combined with other criteria (such as social preferences, political concerns and budgetary constraints). This change in the relationship between risk assessment and decision-making has been driven by several factors:

- Better awareness that real decisions (in the fields of industrial safety, environmental management, urban development) must integrate **multiple concerns**, and that outputs from risk assessment procedures often comprise **significant uncertainty**, and thus cannot be used "mechanically" to derive a well-founded decision.
- Ongoing debate on the role of technical knowledge and expertise in public decision-making, in which the "technical rationality" of scientists and engineers is seen by some critics as disregarding the social context and citizens' concerns (a "cultural rationality") in their analyses **[Plough et Krimsky 1987]**. This has led to greater **stakeholder participation** in decision-making, in which technocratic decision processes, driven purely by rational technical considerations, are modified to integrate the concerns and the perceptions of stakeholders.
- From a more technical viewpoint, a recognition that both **deterministic** approaches to risk assessment (which focus on the ability of engineering principles such as safety margins, redundancy and diversity to prevent and reduce the impact of catastrophic failures) and **probabilistic** methods (which integrate estimations of the likelihood of accident scenarios and which allow operators and regulators to determine which barriers would provide the most benefit in risk reduction) provide useful insights into safety management, and that a framework for combining their inputs is needed.

The present document provides an introduction to risk-informed decision-making, along with a description of the manner in which the technique has been implemented by the NASA for management of risk in space programmes, and by the US NRC for the regulation of nuclear activities. The authors also document the respective advantages and disadvantages of deterministic and probabilistic approaches to risk assessment.

Eric Marsden, FonCSI
November 20, 2012

We welcome your feedback! Please send your comments on suggestions for improvement of this document by email to `cahiers@FonCSI.org`.

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 the decision-makers insofar as the technical risk side of the problem is relevant for the decision [Aven 2010].

Further, the actual decision outcome for a critical situation involving a potential for large consequences typically derives from a thorough process which combines i) 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, and ii) 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 makes it possible to keep the technical analysis manageable by complementation with deliberation for ensuring coverage of the non-modelled issues. In this way, the analytic evaluation (*i.e.*, the risk assessment) supports the deliberation by providing numerical outputs (point estimates and distributions of the relevant safety parameters, possibly to be compared with predefined numerical safety criteria for further guidance to the decision) and also all the arguments behind the analysis itself, including the assumptions, hypotheses, parameters and their uncertainties [Nilsen et 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 whilst ensuring 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 et Zio 2011].

For more than 30 years, probabilistic analysis has been used as the basis for the analytic process of risk assessment 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 changed significantly since that period.

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 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 **[Ferson et Ginzburg 1996; Walley 1991; Dempster 1967; Shafer 1976; Dubois et Prade 1988; Dubois 2006]**.

Notice that in the implementation of the decision it is common for decision-makers to seek for further protection by adding conservatisms and performing traditional engineering frameworks of "defense-in-depth" (typical of a *deterministic* approach to risk assessment) to bound the uncertainties and in particular the "unknown unknowns" (completeness uncertainty).

In general, the insights provided by the probabilistic approach *complement* those provided by the deterministic approach. In view of this, the trend is to move towards a much more *risk informed* approach in which the insights from the risk information provided by the PRA is used formally as part of an integrated decision-making process. When this *integrated* process is applied to making decisions about *safety issues*, this is sometimes referred to as Risk Informed Decision-Making (RIDM).

Objectives of this document

In this wide framework of decision-making in risk assessment practice in presence of uncertainties, the present document aims to:

1. introduce the general concepts, definitions and issues related to Risk-Informed Decision-Making (RIDM) processes in presence of uncertainties;
2. describe in detail the RIDM processes adopted by two organizations in the complex, safety-critical fields of aerospace and nuclear engineering, *i.e.*, the *National Aeronautics and Space Administration* (NASA) and the *United States Nuclear Regulatory Commission* (USNRC).

Document structure

The document is structured as follows:

- In chapter 2, the definitions of risk and risk analysis are briefly recalled, after which the general concepts, motivations and issues related to Risk-Informed Decision-Making (RIDM) processes are outlined;
- Chapters 3 and 4 present in detail how the RIDM process is implemented respectively at NASA and by the USNRC;
- Annexes A to C provide detail on the derivation of performance measures, the ordering of performance measures and the establishment of risk tolerances on the performance measures in the NASA RIDM process.

2

Risk-informed decision-making

2.1 Risk and risk assessment

In the past, a **deterministic** approach was chosen as the basis for making decisions on safety issues. In particular, the approach was to:

worst-case scenarios

1. identify a group of failure event sequences leading to credible worst-case accident scenarios $\{S_i\}$ called design-basis accidents;
2. predict their consequences $\{x_{S_i}\}$;
3. design appropriate safety barriers which prevent such scenarios and protect from, and mitigate, their associated consequences **[Zio 2009]**.

safety margins

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. These regulations operate under the assumption that the challenges and stresses caused to the system and its protections by any credible accident, are less than those caused by the worst-case, credible accidents. 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]**.

However, in recent years, a *probabilistic* approach to risk analysis (PRA) has arisen as an effective way for analyzing system safety, not limited only to the consideration of worst-case accident scenarios but extended to examining all feasible scenarios and their related consequences, with the probability of occurrence of such scenarios becoming an additional key aspect to be quantified in order rationally and quantitatively to handle uncertainty. In particular, the move has been towards an *integrated* approach that combines the insights provided by the deterministic approach and those from the probabilistic approach with any other requirements in making decisions on a safety issue **[USNRC 1975; NASA 2002; Aven 2003; Bedford et Cooke 2001; Henley et Kumamoto 1992; Kaplan et Garrick 1981; McCormick 1981; USNRC 1983]**.

Risk in PRA

Within the Probabilistic Risk Assessment framework, risk is operationally defined as a **set of triplets [USNRC 1983]**:

- ▷ the scenario(s) leading to degraded performance with respect to one or more performance measures (*e.g.*, scenarios leading to injury, fatality, destruction of key assets);
- ▷ the likelihood(s) (qualitative or quantitative) of those scenarios;
- ▷ the consequence(s) (qualitative or quantitative severity of the performance degradation) that would result if those scenarios were to occur.

Uncertainties are included in the evaluation of likelihoods and consequences.

Defining risk in this way supports risk management, because **[NASA 2010]**:

- ▷ the definition distinguishes high-probability, low-consequence outcomes from low-probability, high-consequence outcomes;

- it points the way to proactive risk management controls, for example by supporting identification of risk drivers and the screening of low-probability, low-consequence outcomes;
- it can point the way to areas where investment is warranted to reduce uncertainty.

The document **[Zio et Pedroni 2012]**, available in the same collection as the present document, provides more information on the way in which uncertainty arises and can be managed in a PRA.

2.2 The Risk-Informed Decision-Making (RIDM) process

In this section, general concepts related to Risk-Informed Decision-Making (RIDM) processes are presented. In particular, the following questions are answered:

- What is RIDM? (§ 2.2.1)
- When is RIDM invoked? (§ 2.2.2)
- How does RIDM help? (§ 2.2.3)

2.2.1 What is RIDM?

A *risk-based* decision-making process provides a defensible basis for making decisions and helps to identify the greatest risks and prioritize efforts to minimize or eliminate them. It is based primarily on a narrow set of model-based risk metrics, and generally does not lead much space for interpretation. Considerations of cost, feasibility and stakeholder concerns are generally not a part of risk-based decision-making, which is typically conducted by technical experts, without public consultation or stakeholder involvement.

In contrast, *risk-informed* decision-making (RIDM) is a **deliberative process** that uses a **set of performance measures**, together with other considerations, to "inform" decision-making. The RIDM process acknowledges that **human judgment** has a relevant role in decisions, and that technical information cannot be the unique basis for decision-making. This is because of inevitable *gaps* in the technical information, and also because decision-making is an intrinsically *subjective*, *value-based* task. In tackling complex decision-making problems involving *multiple*, *competing* objectives, the *cumulative knowledge* provided by experienced personnel is essential for integrating technical and nontechnical elements to produce dependable decisions **[NASA 2008, 2010]**.

2.2.2 When is RIDM invoked?

RIDM is invoked for key decisions (*e.g.*, design decisions, make-buy decisions, budget reallocation, ...), which typically require setting or rebaselining of requirements **[NASA 2010]**. It is invoked in many different venues, including boards and panels, safety review boards, risk reviews, engineering design decision forums and configuration management processes, among others **[NASA 2010]**.

RIDM is applicable for decisions that typically have one or more of the following characteristics **[NASA 2010]**:

- **high financial stakes**: significant costs and significant potential safety impacts are involved in the decision;
- **complexity**: the actual ramifications of alternatives are difficult to understand without detailed analysis;
- presence of **uncertainty**: uncertainty in key inputs creates substantial uncertainty in the outcome of the decision alternatives and points to risks that may need to be managed;
- **multiple objectives**: large numbers of objectives require detailed formal analyses;
- **diversity of stakeholders**: high accuracy is needed to define objectives and derive the corresponding performance measures when the set of stakeholders represents a wide variety of preferences and perspectives.

RIDM typically requires detailed, quantitative analyses, which are expensive to undertake, and is thus not suited to small, low budget projects which are in their operational phase.

2.2.3 How does RIDM help?

RIDM is a structured process that **[NASA 2008]**:

- ▷ aims at achieving "project" success by risk-informing the selection of decision alternatives;
- ▷ ensures that decisions between competing alternatives are taken with an awareness of the risks associated with each, thus helping to avoid late design changes, which can be relevant sources of risk, cost overshoot, schedule delays, and cancellation;
- ▷ tackles some of the following issues: namely,
  1. the possible "incongruence" between stakeholder expectations and the resources required to address the risks to achieve those expectations;
  2. possible misunderstanding of the risk that a decision-maker is accepting when making commitments to stakeholders;
  3. the miscommunication in considering the respective risks associated with competing alternatives.
- ▷ tries to foster development of a **robust technical basis for decision-making** by:
  - *coupling* the *attributes* of the proposed decision alternatives to the *objectives* that define "project" success;
  - considering *all* attributes (that are important to the stakeholders) in an integrated manner;
  - helping ensure that a **broad spectrum of decision alternatives** are considered;
  - performing quantitative assessment of the **advantages and drawbacks of each decision alternative** relative to the identified objectives;
  - taking into account the **uncertainties** related to each proposed decision alternative to quantify their impact on the achievement of the identified objectives;
  - *communicating* the quantitative assessment of the proposed decision alternatives into the decision environment, where it is deliberated along with other considerations to form a comprehensive, risk-informed basis for alternative selection.

The next chapter illustrates the manner in which RIDM is used at NASA.

3

NASA Risk-Informed Decision-Making process

Within the NASA organizational hierarchy **[NASA 2010]**, top-level objectives (NASA Strategic Goals, such as mission success), flow down in the form of progressively more detailed **performance requirements**, whose achievement guarantees that the top-level objectives are met. Each operational/organizational unit within NASA discusses with the unit(s) at the next lower level in the hierarchy a series of objectives, performance measures and requirements, resources, and schedules that characterize the tasks to be performed by the unit(s). At each step, the lower level operational/organizational unit manages its own risks and reports risks and elevates decisions for managing risks to the next higher level. Employing the Risk-Informed Decision-Making (RIDM) process in support of key decisions as requirements flow down through the operational/organizational hierarchy ensures that objectives remain intertwined to NASA Strategic Goals **[NASA 2010]**.

Throughout this process, interactions take place between the following actors **[NASA 2008]**:

1. the **stakeholders** (*i.e.*, individuals or organizations that are affected by the outcome of a decision but are outside the organization doing the work or making the decision);
2. the **risk analysts** (*i.e.*, individuals or organizations that apply probabilistic methods to the quantification of risks and performances);
3. the **subject matter experts** (*i.e.*, individuals or organizations with expertise in one or more topics within the decision domain of interest);
4. the **Technical Authorities**;
5. the **decision-maker**.

Figure 3.1 illustrates these roles and interfaces within the NASA RIDM process. It can be seen that it is fundamental that the analysts conducting the risk analysis of alternatives take into account the objectives of the various stakeholders in their analyses. These analyses are performed by subject matter experts in the domains spanned by the objectives. The completed risk analyses are deliberated and the decision-maker selects a decision alternative for implementation (with the agreement of the Technical Authorities).

The NASA RIDM process involving the above mentioned actors consists of three parts, namely Part 1, 2 and 3, briefly summarized below and described in detail in the following Sections 3.1, 3.2 and 3.3, respectively **[Dezfuli et al. 2010; NASA 2008, 2010]**:

▷ **Part 1 – Identification of decision alternatives**

Objectives are decomposed into their constituent objectives, each of which reflects an individual issue that is significant to the stakeholders. At the lowest level of decomposition are *performance objectives*, each of which is associated with a *performance measure* that quantifies the degree to which the performance objective is addressed by a given decision alternative. In general, a performance measure has a "direction of goodness" that indicates the direction of increasingly good performance measure values. A complete set of performance measures is considered for decision-making, that reflects stakeholder interests and spans the mission execution domains of i) safety, ii) technical, iii) cost and iv) schedule **[NASA 2010]**. Objectives whose performance measure values are required to lie within predefined limits (for *all* decision alternatives) give rise to *imposed constraints*

performance measures

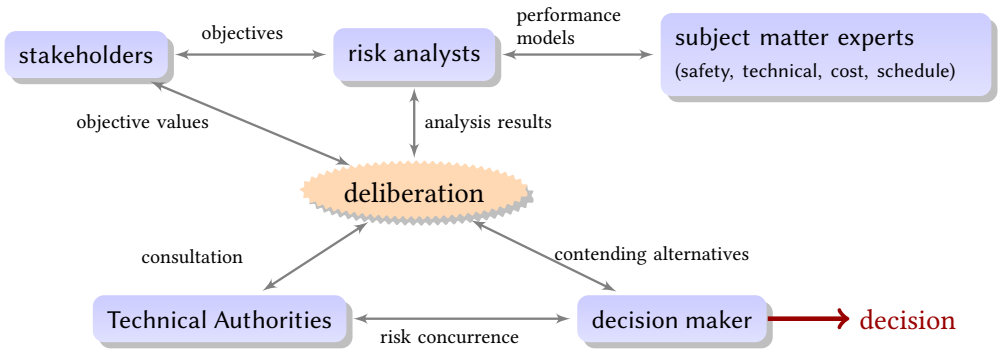


Figure 3.1 – *Roles and interfaces in the NASA RIDM process*

reflecting those limits. Objectives and imposed constraints constitute the basis on which decision alternatives are compiled, and performance measures are the means by which their ability to meet imposed constraints and achieve objectives is quantified (§ 3.1).

▷ **Part 2 – Risk analysis of decision alternatives**

The performance measures of each alternative are quantified; given the presence of *uncertainty*, the actual outcome of a particular decision alternative will be only one of a (possibly) broad spectrum. Therefore, it is incumbent on risk analysts to model all possible outcomes of interest, accounting for their probabilities of occurrence, in terms of the scenarios that produce it: this produces a *probability distribution* of outcomes for each alternative.

If the uncertainty in one or more performance measures prevents the decision-maker from assessing important differences between alternatives, then the risk analysis may be *iterated* in order to reduce uncertainty. The iterative analysis stops when the level of uncertainty does not preclude a *robust decision* from being taken.

Robust decision

DEFINITION

A robust decision is based on sufficient technical evidence and characterization of uncertainties to determine that the selected alternative best reflects the decision-maker's preferences and values given the state of knowledge at the time of the decision, and is considered insensitive to credible modeling perturbations and realistically foreseeable new information **[NASA 2010]**.

TBfD

The principal product of the risk analysis is the *Technical Basis for Deliberation (TBfD)*, a document that lists the set of candidate alternatives, summarizes the analysis methodologies used to quantify the performance measures, and presents the results. The TBfD is the input that risk-informs the deliberations that support decision-making (§ 3.2).

▷ **Part 3 – Risk-informed alternative selection**

Deliberation takes place among the stakeholders and the decision-maker who either i) prunes the set of alternatives and asks for further analysis of the remaining alternatives or ii) selects an alternative for implementation or iii) asks for new alternatives.

To facilitate deliberation, a set of **performance commitments** is associated with each alternative. Performance commitments identify the performance that an alternative is capable of, at a given probability of exceedance, or risk tolerance. By establishing a **risk tolerance** for each performance measure independent of the alternative, comparisons of performance among the alternatives can be made on a **risk-normalized basis**. In this way, stakeholders and decision-makers can deliberate the performance differences between alternatives at common levels of risk, instead of having to choose between complex combinations of performance and risk (§ 3.3).

The NASA RIDM process has just been described as a *linear* sequence of steps: however,

this representation is used only for the sake of simplicity. Actually, in reality, some steps of the processes may be conducted in parallel, and others may be iterated multiple times before moving to subsequent steps. In particular, Part 2 (namely, Risk analysis of decision alternatives) is internally iterative as analyses are refined to meet decision needs; in addition, Part 2 is iterative with Part 3 (namely, Risk-informed alternative selection), as stakeholders and decision-makers iterate with the risk analysts in order to produce sufficient technical basis for taking a robust decision.

The following sections provide details concerning Parts 1, 2 and 3 of this decision process.

3.1 Part 1 – Identification of decision alternatives

Decision alternatives have to be identified in the context of the objectives that have to be achieved. Thus, the identification of the alternatives starts with the process of understanding stakeholders' expectations (Step 1.A, described in § 3.1.1); then, stakeholders' expectations are decomposed into quantifiable objectives and performance measures in order to allow comparison among the candidates (Step 1.B in § 3.1.2); finally, a set of feasible alternatives is compiled that addresses the quantified objectives (Step 1.C in § 3.1.3).

3.1.1 Step 1.A – Understand stakeholders' expectations

Stakeholder expectations result when they i) specify what is desired as a final outcome or as a thing to be produced and ii) establish bounds on the achievements of goals (these bounds may for example include costs, time to delivery, performance objectives, organizational needs). In other words, the stakeholder expectations that are the outputs of this step consist of i) *top-level objectives* and ii) *imposed constraints*. Top-level objectives state what the stakeholders want to achieve from the activity: these are frequently *qualitative* and *multifaceted*, reflecting competing sub-objectives (*e.g.*, increase reliability *vs.* decrease cost). Imposed constraints represent the top-level success criteria outside of which the top-level objectives are not achieved.

Planetary Science Mission example

The hypothetical "Planetary Science Mission example" described in **[NASA 2010]**, supposes that the objective of the RIDM process is to place a scientific platform in orbit around a given planet in order to collect data and send it back to earth. Stakeholders' expectations may include:

- ▷ the launch date must be within the next 55 months due to the launch window;
- ▷ the scientific platform should provide at least 6 months of data collection;
- ▷ the mission should be as inexpensive as possible, with a cost upper limit of $500 M;
- ▷ the probability of radiological contamination of the planet should be minimized, with a goal of no greater than 0.1%.

3.1.2 Step 1.B – Derive performance measures

Although the top-level objectives state that the goal has to be accomplished, they may be too complex and/or vague for operational purposes; thus, in general, decision alternatives cannot be directly compared only on the basis of the (multifaceted and/or qualitative) top-level objectives. To overcome this issue, top-level objectives are decomposed, using an **Objective Hierarchy** (OH), into a set of different *lower-level* objectives describing (in more detail) the complete set of necessary and/or desirable characteristics that any feasible alternative should have. Each of these lower-level objectives is then associated to a *performance measure*, that quantifies the extent to which a decision alternative meets the corresponding objective and, thus, provides a mathematical basis for comparing the different alternatives.

Construct an Objective Hierarchy

An **Objective Hierarchy** (OH) is built by subdividing an objective into lower-level objectives of more detail. Figure 3.2 shows an example OH. At the first level of decomposition the top-level objective of interest is declined into the *general execution domains* of Safety, Technical, Cost and Schedule. Below each of these general domains the objectives are further decomposed into *sub-objectives*, which themselves are iteratively decomposed until appropriate quantifiable *performance objectives* are generated. The decomposition of objectives stops when the set of performance objectives is *operationally useful* and *quantifiable*.

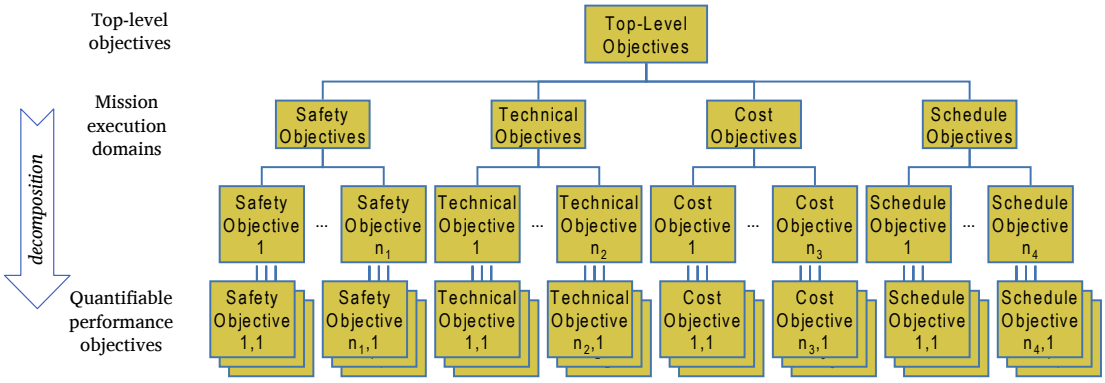


Figure 3.2 – *An example objective hierarchy*

Planetary Science Mission example OH

By way of example, the figure below shows the objective hierarchy built from the top-level objective "Project success" for the Planetary Science Mission example introduced in § 3.1.1 **[NASA 2010]**. It can be seen that the top-level objective of interest, *i.e.*, Project success, is successively decomposed through the general execution domains of Safety, Technical, Cost and Schedule, producing a set of performance objectives at the leaves.

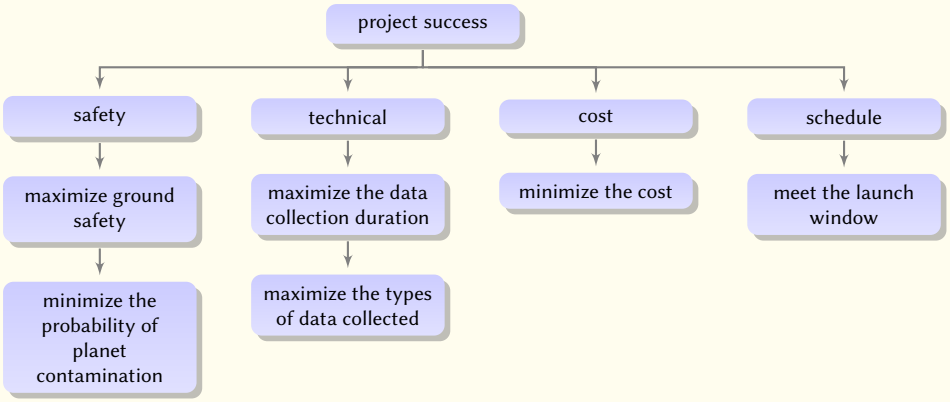


Figure 3.3 – *Example objective hierarchy for a NASA planetary science mission*

Derive performance measures for the performance objectives

Once an OH is built that decomposes each top-level objective into a complete set of performance objectives, a **performance measure** is assigned to each as a quantitative measure of its degree of fulfillment. In most cases, the appropriate performance measure to use is evident from the objective (*e.g.*, the objective "Minimize cost" is naturally associated with the performance measure "Total cost"); in other cases, the choice is not so clear, and work must be done in order to assure that the objective is not only quantifiable, but that the performance measure used to quantify it is adequately representative of the objective of interest.

Further technical details about this issue are not reported here for brevity; the interested reader is referred to **[NASA 2010]** and to Appendix A at the end of this document.

By way of example, refer to the Planetary Science Mission example that is briefly presented in § 3.1.1 and whose OH (built for the top-level objective "Project success") is reported in figure 3.3. The performance measures associated to the four performance objectives derived from the top-level objective "Project success" are reported in table 3.1 together with the corresponding *imposed constraints*[1].

Performance objective	**Performance measure** [unit of measure]	**Imposed constraint**
Minimize cost	Project cost [$M]	None
Minimize development time	Months to completion [months]	55 months
Minimize the probability of planet Pu contamination	Probability of planet contamination by Pu [/]	0.1%
Maximize data collection	Months of data collection [months]	6 months

Table 3.1 – *Performance measures and imposed constraints associated to the performance objectives derived from the top-level objective "Project success" (figure 3.3) for the Planetary Science Mission example introduced in § 3.1.1* **[NASA 2010]**

3.1.3 Step 1.C – Compile a set of alternatives

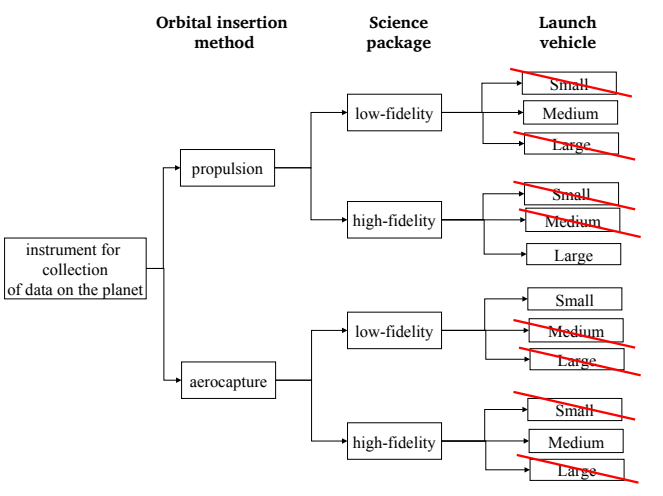
One of the possible ways to compile and represent the decision alternatives under consideration is by a *trade tree* **[NASA 2010]**. Initially, the trade tree contains a number of high-level decision alternatives representing high-level differences in the strategies used to address objectives. The tree is then developed in greater detail by determining a general *category* of options that are applicable to each strategy. Trade tree development continues iteratively until the leaves of the tree contain alternatives that are sufficiently well defined to allow quantitative evaluation through risk analysis.

Along the way, branches of the trade tree containing unattractive categories can be pruned, as it becomes evident that the alternatives contained therein are either *unfeasible* (*i.e.*, they are incapable of satisfying the imposed constraints) or just *inferior* to alternatives on other branches. An alternative that is inferior to some other alternative with respect to every performance measure is said to be *dominated* by the superior alternative. At this point in the RIDM process, assessment of performance is high-level, depending on simplified analysis and/or expert opinion, *etc.*: in particular, when performance measure values are quantified, they are done so as *point estimates*, using a *conservative* approach to estimation in order to be inaccurate on the side of inclusion rather than elimination.

[1] Notice that some performance measures have *imposed constraints*, whereas others are unconstrained but still have a desirable *direction of goodness*.

Trade tree for Planetary Science Mission example

For instance, consider the Planetary Science Mission example of § 3.1.1. A trade tree was used to compile potential alternatives for the mission to a planet of interest. As shown below, the three (decision alternative) attributes that were considered for developing the tree were i) the orbital insertion method (propulsive deceleration *vs.* aerocapture), ii) the science package (lighter, low-fidelity instrumentation vs. heavier, high-fidelity instrumentation), and iii) the launch vehicle (small, medium, and large). However, initial estimates of payload mass indicated that there was only one appropriately matched launch vehicle option to each combination of insertion method and science package. Thus, eight of the twelve initial options were screened out as being "unfeasible", leaving four alternatives to be forwarded to risk analysis.



3.2 Part 2 – Risk analysis of decision alternatives

Risk analysis consists of performance assessment supported by probabilistic modeling. It is used here to propagate the uncertainties inherent in a particular decision alternative to uncertainty in the achievement of objectives, were that decision alternative to be pursued. Performance is assessed in terms of the performance objectives developed in Step 1 (§ 3.1). The performance measures established for these objectives provide the means of quantifying performance so that alternatives can be effectively compared.

Part 2 of the NASA RIDM process (namely, Risk analysis of decision alternatives) comprises two steps: in Step 2.A, the risk analysis framework is structured for *each* decision alternative identified at Step 1.C of § 3.1.3 (in other words, risk analysis methodologies are selected for each analysis domain represented by the objectives and coordination among the analysis activities is established to ensure a consistent, integrated evaluation of each alternative) (§ 3.2.1); in Step 2.B, the risk analysis is conducted, which entails probabilistic evaluation of each alternative's performance measure values (§ 3.2.2). On the basis of the quantitative results of the risk analysis process, in Step 2.C the Technical Basis for Deliberation (TBfD) is developed, which provides the primary means of risk-informing the subsequent alternative selection process (§ 3.2.3).

3.2.1 Step 2.A – Structure the (alternative specific) risk analysis framework

This step of the NASA RIDM process is concerned with how domain-specific analyses, conducted in accordance with existing methodological practices, are integrated into a multi-disciplinary framework to support **decision-making under uncertainty**. In general, the challenge for the risk analysts is to establish a framework that:

1. operates on a common set of (potentially uncertain) *performance parameters*[2] for a given alternative;

[2] A performance parameter is any *value* needed to execute the *models* that quantify the performance measures. Unlike performance measures, which are the same for all decision alternatives, performance parameters typically vary among alternatives, *i.e.*, a performance parameter that is defined for one alternative might not apply to another

2. consistently addresses *uncertainties* across alternatives;
3. preserves *correlations* between performance measures and between parameters (see § 3.2.2 for details).

In practice, in order to structure the risk analysis framework for a given decision alternative, the relationships between performance measures and the analyses needed to quantify them have to be established and illustrated. By way of example, figure 3.4 traces Performance Parameter 2 through the risk analysis framework, showing how it is used by multiple risk analyses in multiple execution domains (*e.g.*, Safety, Technical, Cost and Schedule).

Performance Parameter 2 is a direct input to a risk analysis in the Safety and Technical domains. This analysis produces outputs that are used as inputs to two other Safety and Technical risk analyses. Some of these risk analyses produce values for Performance Measures 1 and *m*, whereas others produce an output that is needed by a risk analysis in the Cost & Schedule domain. This Cost & Schedule risk analysis ultimately supports quantification of Performance Measure 2. Each of the *m* performance parameters that define Alternative *i* can be similarly traced through the risk analysis framework.

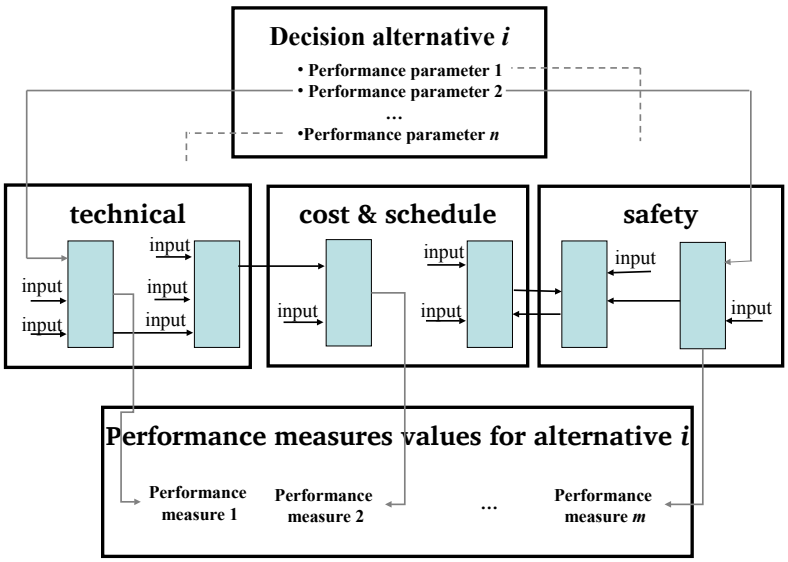
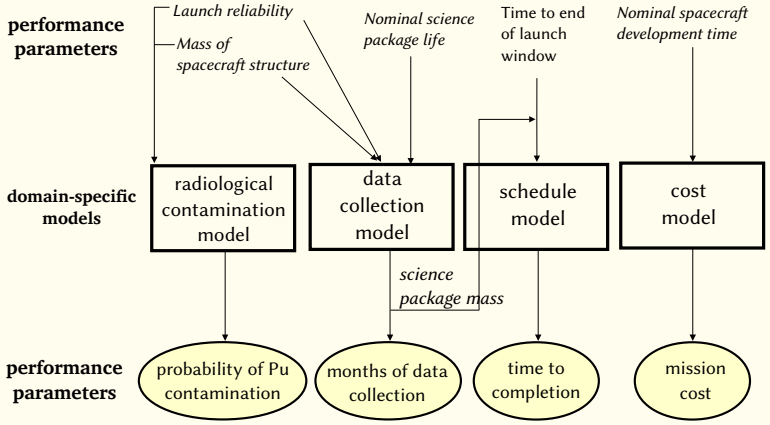


Figure 3.4 – *Risk analysis framework: conceptual relationship between performance parameters and performance measures in each decision alternative*

alternative. Example performance parameters related to the performance objective of sending a satellite into earth orbit might include propellant type, propellant mass, engine type/specifications, *etc.*; additionally, performance parameters also include relevant environmental characteristics such as meteorological conditions. Performance parameters may be *uncertain*: indeed, risk has its origins in performance parameter uncertainty, which propagates through the risk analysis, resulting in performance measure uncertainty.

Risk analysis framework for the Planetary Science Mission example

Each alternative is characterized by its performance parameters, some of which are uncertain (in italic) and others of which have definite, known deterministic values (Time to end of launch window). In order to calculate the performance measures previously selected for illustrative purposes, four separate performance models are developed for radiological contamination, data collection, schedule and cost. Some performance parameters (such as spacecraft structure mass and launch reliability) are used in multiple models; some models (*e.g.*, the data collection model) produce outputs (*e.g.*, science package mass) that are inputs to other models (*e.g.*, the schedule model).



3.2.2 Step 2.B – Risk quantification via probabilistic modeling of performance

If there were no uncertainty, the question of performance assessment would be one of quantifying point value performance measures for each decision alternative. In the real world, however, uncertainty is unavoidable, and the consequences of selecting a particular decision alternative cannot be known with absolute precision.

For decision-making under uncertainty, risk analysis is necessary, in which uncertainties in the values of each alternative's performance parameters are identified and propagated through the analysis to produce uncertain performance measures. Moreover, since performance measures might not be independent, possible **correlations** must be considered.

One possible way to propagate uncertainties while preserving correlations is to conduct all analysis by Monte Carlo Simulation (MCS) that amounts to:

1. sampling possible values of the n uncertain performance parameters (*i.e.*, the uncertain inputs) $\{p_{1,k}, p_{2,k}, ..., p_{n,k}\}$ from the corresponding Probability Density Functions (PDFs), whilst respecting correlations;
2. propagating them through the suite of analyses;
3. collecting the resulting m performance measures (*i.e.*, the uncertain outputs) as a vector of performance measure values $\{PM_{1,k}, PM_{2,k}, ..., PM_{m,k}\}$.

As the Monte Carlo procedure iterates (for $k = 1...N_T$), these performance measure vectors accumulate and, at the end of the iteration process, the probability distributions of the performance measures can be expressed, *e.g.*, in the form of a histogram. Figure 3.5 illustrates the MCS procedure as it would be applied to a single decision alternative (namely, Decision Alternative i)[3].

Referring to the Planetary Science Mission example introduced in § 3.1.1, figure 3.6 shows the PDFs resulting from the propagation of the uncertainties onto the four performance measures (*i.e.*, probability of Pu contamination, data volume, cost and time to completion) employed

[3] Uncertainties are distinguished by two categorical groups: aleatory and epistemic. Aleatory uncertainties are random or stochastic in nature and cannot be reduced by obtaining more knowledge through testing or analysis. On the other hand, epistemic uncertainties are not random in nature and can be reduced by obtaining more knowledge through testing and analysis. Further details can be found in **[USNRC 2002, 2009, 2005; NASA 2010]**. **[Zio et Pedroni 2012]**, in the same collection as this document, provides an overview of sources of uncertainty in a probabilistic risk analysis.

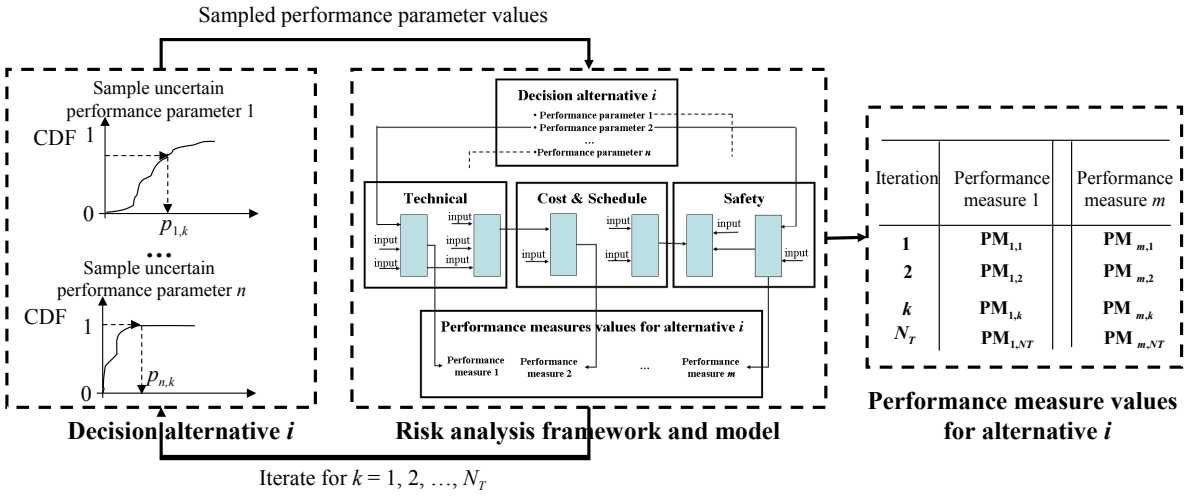


Figure 3.5 – *Monte Carlo Simulation for propagating uncertainties onto the performance measures in the analysis of the generic Decision alternative i*

to evaluate and compare four different decision alternatives; the corresponding imposed constraints are also shown as dashed lines.

It can be seen that there is substantial overlap among the PDFs. In practice, consideration is given to performing additional analysis to resolve such overlap in cases where doing so is expected to illuminate the decision. Statistical techniques such as *sensitivity analysis* allow analysts to identify the uncertain inputs which contribute the most to uncertainty in the outputs which impact the decision; additional effort can then be made to reduce the level of uncertainty in these inputs. In some cases however, additional analysis cannot help to distinguish among alternatives, especially when the underlying uncertainties are common to them.

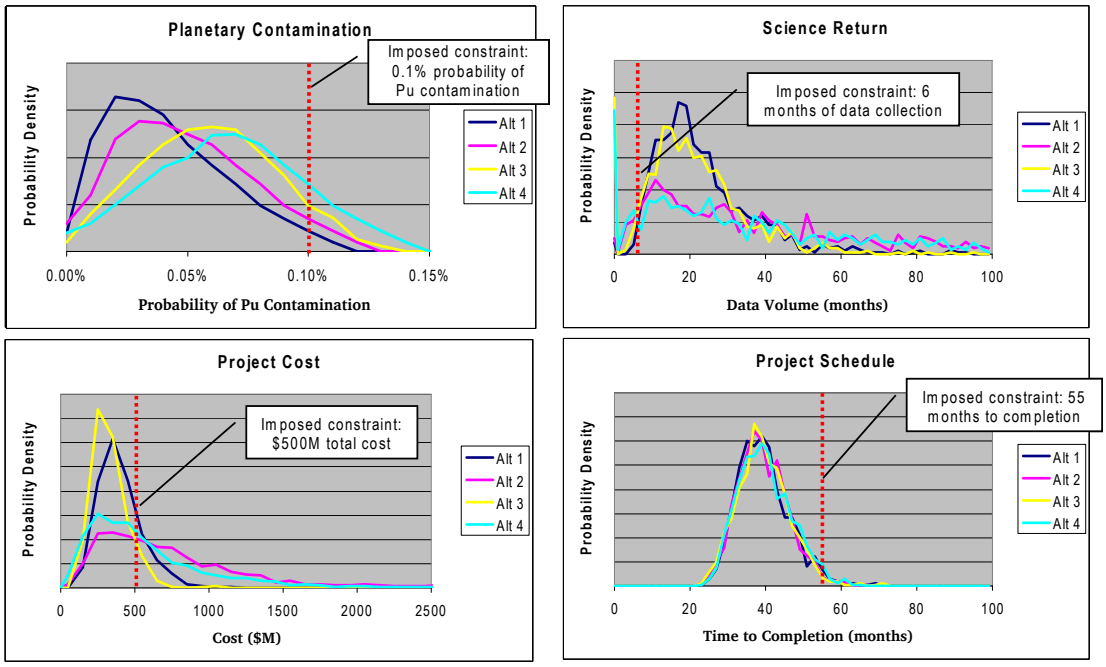


Figure 3.6 – *Propagation of uncertainty onto the performance measures for four decision alternatives of the Planetary Science Mission example introduced in § 3.1.1 (from* **[NASA 2010]***)*

3.2.3 Step 2.C – Produce the Technical Basis for Deliberation (TBfD)

On the basis of the results of the uncertainty propagation obtained at the previous Step 2.B (§ 3.2.2), the Technical Basis for Deliberation (TBfD) is produced. The TBfD specifies the minimum information needed to risk-inform the selection of a decision alternative. The content of the TBfD is driven by the question: "What information do the deliberators and decision-makers need in order for their decision process to be fully risk-informed?".

Different methods can be adopted to communicate risk results:

- **charts** can be produced where the competing alternatives are compared in terms of the probability that the corresponding performance measures violate the constraints imposed on the problem;
- **statistics** (such as the mean, the median, the 5^{th} and 95^{th} percentiles) of the probability density functions of the performance measures can be provided for each competing alternative;
- the **entire probability density functions** of all the performance measures of the competing alternatives can be represented.

Further technical details about the TBfD are far beyond the scope of the present document; the interested reader is referred to **[NASA 2010]**.

3.3 Part 3 – Risk-informed alternative selection

The risk-informed alternative selection process within RIDM provides a method for integrating risk information into a *deliberative* process for decision-making, relying on the *judgment* of the decision-makers to make a risk-informed decision.

> The decision-maker does not necessarily base his or her selection of a decision alternative *solely* on the results of the risk analysis. Rather, the risk analysis is just *one* input to the process, in recognition of the fact that it may not model everything of importance to the stakeholders.

Part 3 (namely, Risk-informed alternative selection) is structured as follows. In Step 3.A, *performance commitments* are developed, representing consistent levels of risk tolerance across alternatives (§ 3.3.1). In Step 3.B, stakeholders, risk analysts, and decision-makers *deliberate* the relative merits and drawbacks of each alternative, *given* the information in the TBfD. This step is *iterative*, and may involve additional risk analysis or other information gathering. The decision-maker may also be involved at this stage to help *prune* the number of alternatives. Once a set of contending alternatives has been identified, the decision-maker integrates the issues raised during deliberation into a *rationale* for the selection of an alternative (§ 3.3.2).

3.3.1 Step 3.A – Develop risk-normalized performance commitments

Performance commitments

A performance commitment is a performance measure *value* set at a particular *percentile* of the performance measure's PDF, in order to *anchor* the decision-maker's perspective to that performance measure value as if it were her commitment, were she to select that alternative. For a given performance measure, the performance commitment is set at the *same percentile* for all decision alternatives, so that the probability of failing to meet the different alternative commitment values is the same across alternatives.

Performance commitments support a *risk-normalized* comparison of decision alternatives, in that a *uniform level of risk tolerance* is established prior to deliberating the merits and drawbacks of the various alternatives. Put another way, risk-normalized performance commitments show what each alternative is capable of with an *equal likelihood* of achieving that capability, given the state of knowledge at the time. Figure 3.7 shows a Performance Commitment *C* for Performance Measure PM. Performance Measure PM is characterized by a Probability Density Function (PDF), due to uncertainties that affect the analyst's ability to forecast a precise value.

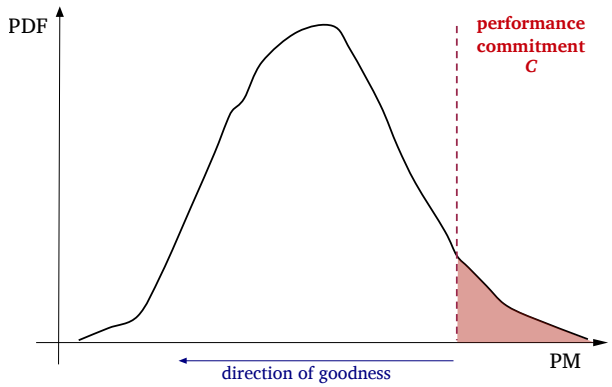


Figure 3.7 – *Example of performance commitment C for a generic performance measure PM*

The decision-maker's *risk tolerance* level for not meeting Performance Commitment C is represented by the shaded area.

The inputs to performance commitment development are:

1. the performance measure PDFs for each decision alternative (which are generated at step 2.B of § 3.2.2);
2. an *ordering* of the performance measures[4];
3. a *risk tolerance* for each performance measure, expressed as a percentile value[5].

For each alternative, performance commitments are established by *sequentially* determining, based on the performance measure *ordering*, the value that corresponds to the stated *risk tolerance*, *conditional* on meeting previously-defined performance commitments. This value becomes the performance commitment for the current performance measure, and the process is repeated until all performance commitments have been established for all performance measures. In figure 3.8, there are only two performance measures, PM_1 and PM_2. Then, the risk analysis results can be shown as a scatter plot on the PM_{1-2} plane (figure 3.8, top left), where each point represents the output from a single iteration of Monte Carlo Simulation. If the ordering of the performance measures is PM_1 first and PM_2 second, PM_1 would be the first performance measure to have a performance commitment established for it (figure 3.8, top right). This is done by determining the value of PM_1 whose probability of exceedance equals the defined risk tolerance. That value becomes the PM_1 performance commitment. The process is repeated for cost, conditional on the PM_1 performance commitment being met. Thus, the points on the scatter plot that exceed the PM_1 performance commitment have been removed from consideration and the PM_2 performance commitment is established solely on the basis of the remaining data (figure 3.8, bottom left). The result is a set of performance commitments for PM_1 and PM_2 that reflects the risk tolerances of the deliberators and decision-maker (figure 3.8, bottom right).

Once the performance commitments are developed, each alternative can be compared to every other alternative in terms of their performance commitments, with the deliberators understanding that the risk of not achieving the levels of performance given by the performance commitments is the same across alternatives. Additionally, the performance commitments can be compared to any imposed constraints to determine whether or not the possibility that they will not be satisfied is within the risk tolerance of the deliberators, and ultimately, the decision-maker.

For the sake of clarity, table 3.2 reports the results of the development of risk-normalized performance commitments for the Planetary Science Mission example. Risk-normalized performance commitments were developed for four alternatives, for the performance measures of time to completion, project cost, data volume, and planetary contamination. The table shows the risk tolerance given to each: for example, because of the importance of meeting the

[4] Suggestions on how to order performance measures can be found in Appendix B.

[5] Suggestions on how to establish risk tolerances on performance measures can be found in Appendix C at the end of the report.

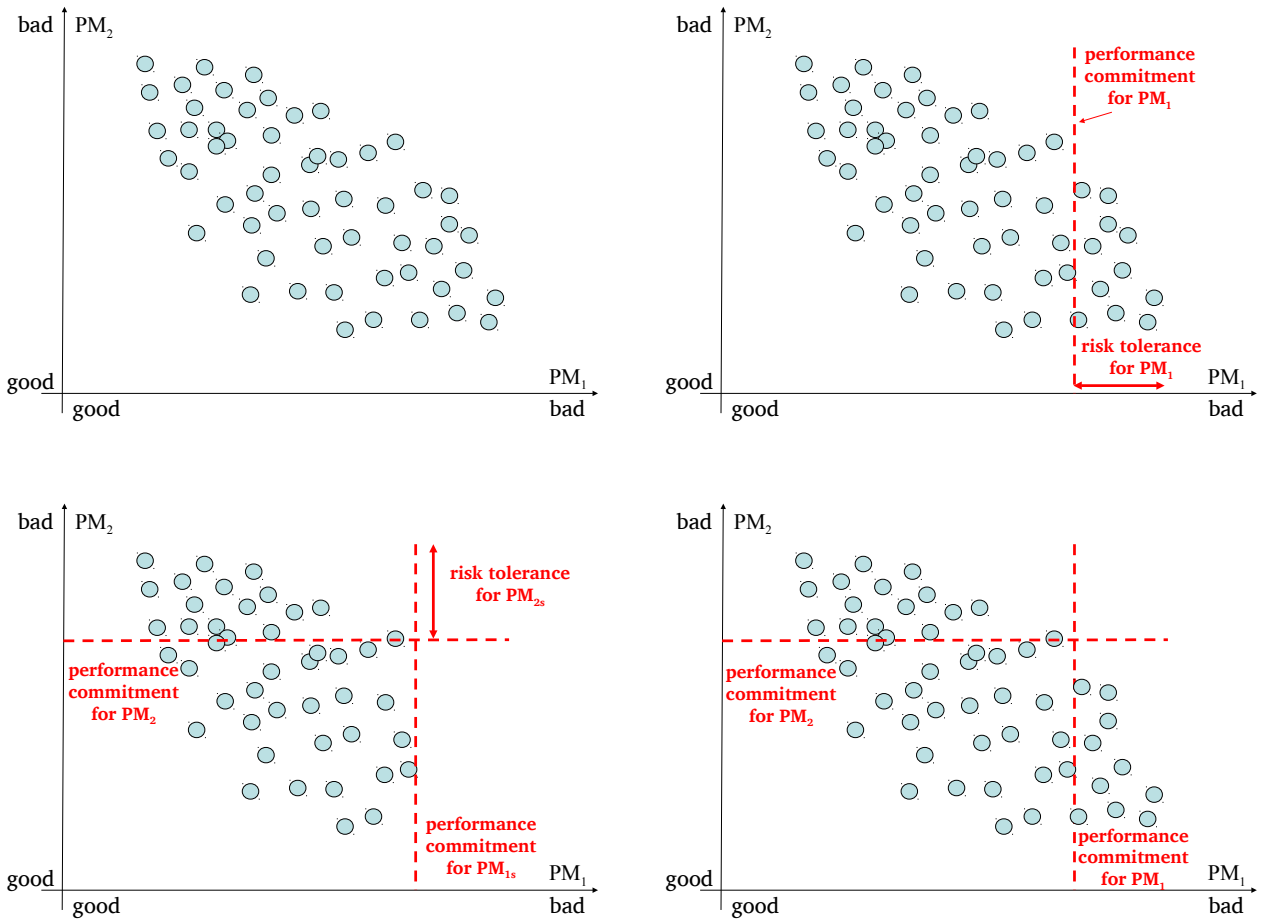


Figure 3.8 – *Conditional establishment of performance commitments*

55 month launch window, a low risk tolerance of 3% is given to time to completion; instead, the 10% data volume risk tolerance is reasonably low, but reflects the belief that minor shortfalls will not significantly erode the success of the mission.

The table also shows the ordering of the performance measures that was used to develop performance commitments. Time to completion was chosen first due to its critical importance; project cost was chosen next, due to its importance in an environment of scarce resources; data volume was chosen third, due to its prominence among the technical objectives.

In addition, the table shows the levels of performance that are achievable at the stated risk tolerances. It is evident that Alternative 4 does not meet the 6 month data volume imposed constraint. However, the deliberators recognize that a different risk tolerance might produce a data volume performance commitment that is in line with the imposed constraint, so they are reluctant to simply discard Alternative 4. Instead, they determine the risk that would have to be accepted in order to produce a data volume performance commitment of at least 6 months: this turns out to be 12%, which the deliberators consider to be within the range of reasonable tolerances (indeed, it is not significantly different from 10%).

Performance measure	Risk tolerance	Performance measure ordering
Time to completion	3%	1
Project cost	27%	2
Data volume	10%	3
Planet contamination	15%	4

Alternative	Time to completion	Project cost	Data volume (12%)	Planet contamination
1	54	576	11 (11)	0.07%
2	53	881	9.9 (11)	0.08%
3	55	413	6.8 (7.8)	0.1%
4	54	688	4.9 (6.0)	0.11%

Table 3.2 – *Performance commitments for the Planetary Science Mission example of § 3.1.1*

3.3.2 Step 3.B – Deliberate, select an alternative and document the decision rationale

The decision-maker has the authority and responsibility for critical decisions. While ultimate responsibility for alternative selection rests with the decision-maker, alternative evaluations can be performed within a number of deliberation forums which may be held before the final selection is made. As partial decisions or "down-selects" may be made at any one of these deliberation forums, they are routinely structured around a team organizational structure identified by the decision-maker. It is important to have a team with broad-based expertise to perform sufficient analysis to support a recommendation or decision. At the top of the structure may be the decision-maker or a deliberation lead appointed by the decision-maker. If a deliberation lead is appointed this individual should be an experienced manager, preferably one with an analytical background.

diversity of experience

Carrying out this step requires:

1. the identification of the competing alternatives;
2. the communication of the competing alternatives to the decision-maker;
3. the selection of a decision alternative and the documentation of the decision rationale.

Identify competing alternatives

After the performance commitments have been generated, they are used to reduce the set of decision alternatives to those that are considered to be the final "competitors" for selection by the decision-maker: this part of the process continues the pruning activity begun in § 3.1.3. Reasons for elimination of non-contending alternatives include: i) infeasibility (performance commitments are exceeded by the imposed constraints); ii) dominance (other alternatives exist that have superior performance commitments on every performance measure, and substantially superior performance on some); iii) inferior performance in key areas (in any decision involving multiple objectives, some objectives will be of greater importance to deliberators than others, *e.g.*, crew safety; alternatives that are inferior in terms of their performance commitments in key areas can be eliminated on that basis).

The guidance above for identifying contending alternatives is primarily focused on comparisons of performance commitments. However, performance commitments do not capture all potentially relevant aspects of performance, since they indicate the performance at only a single percentile of each performance measure PDF. Therefore, alternatives identified as contenders on the basis of their performance commitments are further evaluated on the basis of additional *uncertainty considerations* relating to their performance at other percentiles of their performance measure PDF. In particular, performance uncertainty may give rise to alternatives with the following characteristics:

- ▷ they offer superior *expected* performance: in many decision contexts, the decision-maker's preference for an alternative with uncertain performance is equivalent to his or her preference for an alternative that performs at the mean value of the performance

measure PDF. When this is the case, expected performance is valuable input to decision-making, as it reduces the comparison of performance among alternatives to a comparison of point values. However, in the presence of performance *thresholds*, over-reliance on expected performance in decision-making has the potential to: i) introduce potentially significant probabilities of falling short of imposed constraints, thereby putting objectives at risk, even when the mean value meets the imposed constraints; ii) contribute to the development of derived requirements that have a significant probability of not being achievable;

- ▷ they offer the potential for *exceptionally high* performance: for a given performance measure PDF, the percentile value at the decision-maker's risk tolerance may be unexceptional relative to other contending alternatives. However, at higher risk tolerances, its performance may exceed that of other alternatives, to the extent that it becomes attractive relative to them. An example of this is shown in figure 3.9. In this figure, Alternative 2's performance commitment is at a worse level of performance than Alternative 1's; however, Alternative 2 offers a possibility of performance that is beyond the potential of Alternative 1. In this case, decision-makers have several choices. They can:
  1. choose Alternative 1 on the basis of superior performance at their risk tolerance;
  2. choose Alternative 2 on the basis that its performance at their risk tolerance, though not the best, is acceptable, and that it also has the potential for far superior performance;
  3. set their risk tolerance such that the performance commitment for both alternatives is the same thus making this performance measure a non-discriminator between the two options.
- ▷ they present a risk of *exceptionally poor* performance: this situation is the reverse of the situation above. In this case, even though the likelihood of not meeting the performance commitment is within the decision-makers' risk tolerance, the consequences may be severe, rendering such an alternative potentially unattractive.

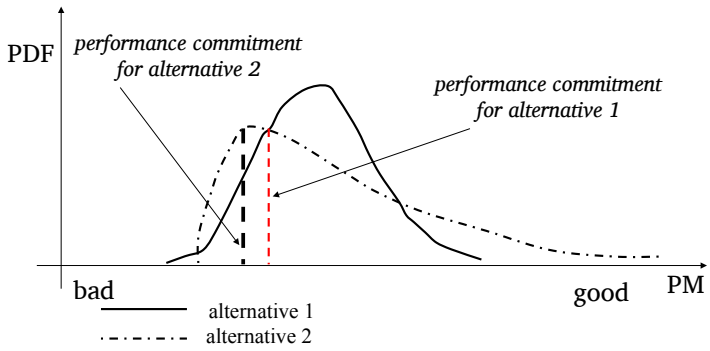


Figure 3.9 – *Uncertainties in performance measures: inferior expected performance, but potential for exceptionally high performances*

A final remark is in order with respect to the **iterative nature** of the deliberation process required for identifying competing alternatives. For example, one or more performance measures might be uncertain enough to significantly overlap, thereby inhibiting the ability to make a robust decision. Moreover, large uncertainties will, in general, produce poor performance commitments, particularly when risk tolerance is low: it would be unfortunate to discard an alternative on this basis if additional analysis could be undertaken to reduce uncertainty. Therefore, before a set of contending alternatives can be chosen, it is important that the deliberators are satisfied that particular uncertainties have been reduced to a level that is as low as reasonably achievable given the scope of the effort. It is expected that the risk analysis will be *iterated*, under the direction of the deliberators, to address their needs.

Alternative	Probability of not meeting constraint [%]			
	Time to completion (< 55 months)	**Cost** (<500M$)	**Data volume** (> 6 months)	**Planet contamination** (< 0.1% probability)
1	2.8	22	4.1	1.1
2	2.4	57	6.4	3.2
3	3.0	9.7	8.7	5.5
4	2.3	47	12	12

Table 3.3 – *Contending alternatives (and corresponding probabilities of not meeting the imposed constraints) for the Planetary Science Mission example of § 3.1.1*

Communicate the competing alternatives to the decision-maker

In this phase, the remaining alternatives all have positive attributes that make them attractive in some way and that make them all contenders. The next step is to find a way to clearly state for the decision-maker the *advantages* and *disadvantages* of each remaining alternative, especially how the alternatives address imposed constraints and satisfy stakeholder expectations.

In addition, information produced during deliberation should be summarized and forwarded to the decision-maker. This includes: i) *risk tolerances* and *performance commitments*; ii) *pros* and *cons* of each contending alternative (*e.g.*, a table); iii) *risk lists*: each alternative will have different contributors to its performance commitment risks; correspondingly, each contending alternative will have a risk list written for it that identifies the major *scenarios* that contribute to risk. For example, each risk is articulated in a *risk statement*, which identifies an existing *condition* that indicates a possibility of some future *consequence* that contributes to one or more performance commitments not being met.

Further details are not given here for brevity; the interested reader is referred to **[NASA 2010]**.

Select a decision alternative and document the decision rationale

Once the decision-maker has been presented with enough information for risk-informed decision-making, he or she is ready to select a decision alternative for implementation. The RIDM process is concerned with assuring that decisions are risk-informed, and does not specify a particular process for selecting the decision alternative itself: these may be qualitative or quantitative, structured or unstructured.

Regardless of the method used for making the decision, the decision-maker finally formulates and documents the decision rationale in light of the risk analysis: technical information on documenting the decision rationale are beyond the scopes of the present report: details can be found in Appendix E of **[NASA 2010]**.

With reference to the Planetary Science Mission example of § 3.1.1, table 3.3 reports four possible decision alternatives together with the corresponding probabilities of not meeting the imposed constraints. The first objective of the deliberators is to see whether or not the set of alternatives can be pruned down to a smaller set of contending alternatives to present to the decision-maker. Table 3.3 shows that the risk of not meeting the $500 M cost constraint is high for Alternatives 2 and 4 compared to the risk tolerance of 27%. Specifically, Alternatives 2 and 4 are infeasible given the combination of the cost constraint and the NASA policy which specifies that the project be budgeted at the 70^{th} percentile or greater. The 70^{th} percentile cost estimates are $860 M for Alternative 2 and $650 M for Alternative 4. Thus, the deliberators prune these alternatives from contention.

Finally, the decision-maker confers with selected deliberators and stakeholders, chooses the alternative that he believes best balances the pros and cons of each contending alternative, and documents his/her decision rationale.

4

USNRC Risk-Informed Decision-Making process

The US Nuclear Regulatory Commission

The US NRC is an independent agency of the United States government that oversees reactor safety and security, reactor licensing and renewal, radioactive material safety, and spent fuel management (storage, security, recycling, and disposal).

In the past, the United States Nuclear Regulatory Commission (USNRC) (together with other regulatory bodies) has used a deterministic approach as the basis for making decisions on safety issues and organizing the activities that they carry out. This was done by applying high-level criteria such as the need to provide defence-in-depth and adequate safety margins **[USNRC 2002]**. The need to meet these deterministic requirements is the basis for most of the regulations, safety standards, guidance, *etc.* that are currently being used by regulatory bodies.

However, in recent years, PRAs have been developed for most of the nuclear facilities and the information provided by these PRAs is increasingly being used to *complement* and *integrate* the deterministic approach. In particular, there is explicit consideration of both the likelihood of events and their potential consequences together with such factors as good engineering practice and sound managerial arrangements.

In more detail, the USNRC integrated decision-making approach, hereafter also referred to as Risk-Informed Decision-Making (RIDM) process, is a structured process in which all the insights and requirements relating to a safety or regulatory issue are considered in reaching a decision. It includes the recognition of any *mandatory requirements*, the insights from the *deterministic analysis*, the insights from the *probabilistic analysis* and any *other applicable insights*: all these elements have to be considered and properly *weighed* to take a decision. In addition, once the decision has been made, there is a need to *implement* it and *monitor* it in order to determine how effective it has been and whether there is a need to revise the decision. These concepts are synthesized in figure 4.1 and detailed below **[IAEA 2005]**:

- **Mandatory requirements**: These typically concern legal requirements, regulations and plant technical specifications; in addition, one of the mandatory requirements is that the risk be kept at a level that is as low as reasonably achievable.
- **Deterministic requirements**: At a high level, they relate to whether the defense-in-depth requirement is met and adequate safety margins are maintained: in particular, defense-in-depth philosophy has traditionally been applied in reactor design and operation to provide *multiple* means/barriers to accomplish safety functions and prevent the release of radioactive material; instead, the rationale for adopting safety margins is to design the plant and the safety systems in such a way as to provide a *large margin* between how the plant would behave in fault conditions and failure of any of the barriers to the release of radioactive material.
  At a lower level, this relates, *e.g.*, to whether there are sufficient levels of *redundancy* and *diversity* in the safety systems.

- **Probabilistic risk insights**: The emerging trend is to carry out a PRA that addresses all initiating events and hazards. The PRA provides an estimate of the level of risk from the plant and the results are used to determine where there are weaknesses in the design or operation of the plant.
- **Other factors**: These may include the costs and the benefits that would arise from making the change, the remaining lifetime of the plant, doses to workers that would arise from implementing the proposed decision and so on.

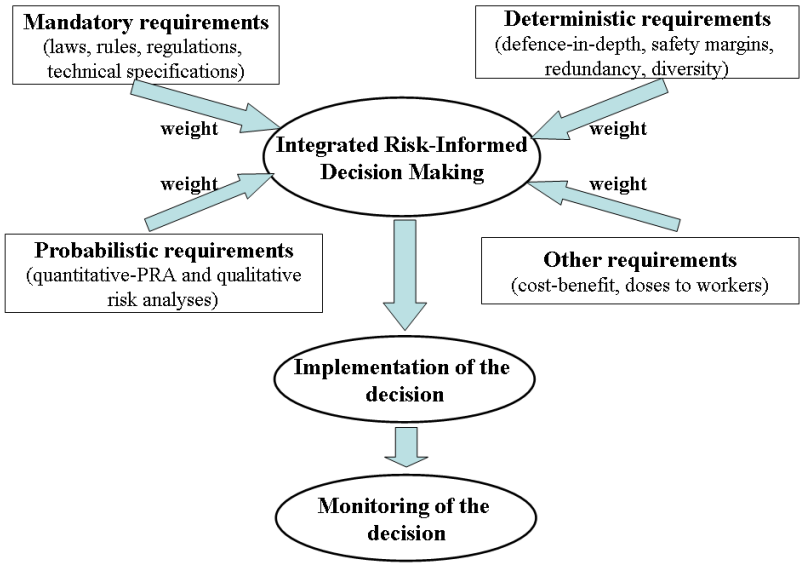


Figure 4.1 – *Elements of the NRC integrated decision-making process* **[IAEA 2005]**

The integrated RIDM process (whose elements are presented in figure 4.1) may be applied to different issues that need to be addressed by a regulatory body, that is:

1. decisions on **plant safety issues** that require regulatory approval (*i.e.*, whether to make *changes* to the *design* and/or *operation* of the nuclear power plant: for example, the plant technical specifications and conditions for normal operation, the frequency of in-service inspection and maintenance, the combinations of safety systems that may be removed from service control during operation and shutdown modes, the way in which maintenance activities are carried out which could include carrying out more maintenance during power operation, the frequency of statutory outages, the emergency operating procedures and accident management measures, the quality assurance arrangements, ...);
2. decisions on *how* the regulatory body itself *operates* (*e.g.*, whether to make changes to regulations, whether to initiate and coordinate safety related research and so on).

In this document, only the integrated RIDM process for deciding on plant safety issues is considered for brevity; the interested reader is referred to **[IAEA 2005]** for details about the integrated RIDM process as applied to decisions on how the regulatory body operates.

The sequential steps of the USNRC integrated RIDM process for plant safety issues are (*cf.* figure 4.1):

1. Define the plant safety issue to be addressed by the regulatory body (described in § 4.1);
2. Identify the applicable mandatory, deterministic, probabilistic and other requirements and criteria (§ 4.2);
3. Carry out quantitative and qualitative assessments to identify how the plant safety issue affects the requirements identified (§ 4.3);
4. Weight the results obtained from the assessments carried out (§ 4.4);
5. Make the decision (§ 4.5);
6. Implement the decision (§ 4.6);
7. Monitor the effect of the decision (§ 4.7).

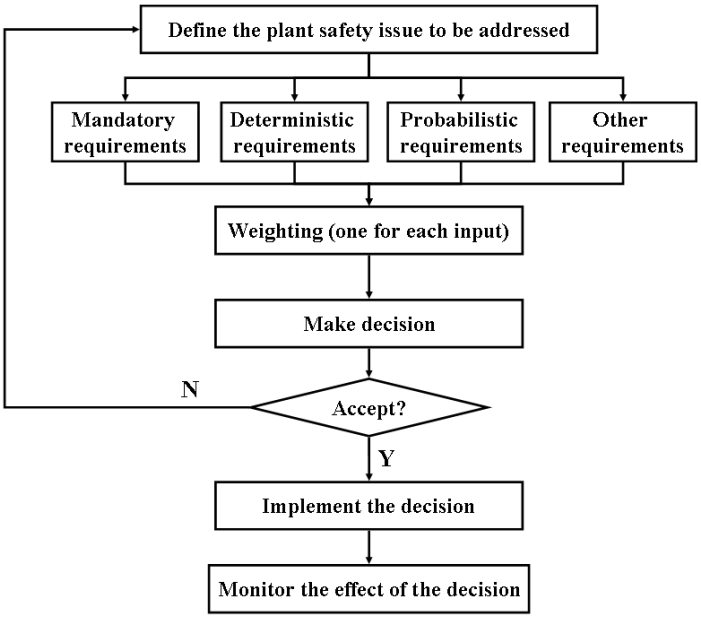


Figure 4.2 – *Sequential steps of the USNRC RIDM process for deciding on plant safety issues* [IAEA 2005]

4.1 Step 1 – Define the plant safety issue to be addressed

The first step in the process is to define the safety issue to be addressed by the regulatory body: this could include requests by the plant operators to make *changes* to i) the *design* of the plant or ii) the *way* in which the plant is *operated*:

1. **Changes to the design of the plant**: The need for such changes may arise as a result of a Periodic Safety Review to determine whether the plant is safe for continued operation: this usually requires a review of the level of safety of the plant by resorting to deterministic analyses and/or PRAs to identify areas where improvements need to be considered. Modifications that are made to *improve* plant *safety* may include: i) improving components, systems, structures to increase their capability to resist to external hazards (*e.g.*, seismic events); ii) increasing the level of separation and segregation of safety systems to protect them against internal hazards (*e.g.*, fire and flood); iii) include additional safety systems to provide diverse means for performing the corresponding safety functions. On the other hand, modifications may be considered that may result in a small *increase* of *risk*, such as changing the fuel so that the power level of the reactor is increased or increasing the quantity of radioactive material stored at the facility.
2. **Changes to the way the plant is operated**: The plant Technical Specifications give limits and conditions for normal operation and they are traditionally formulated such that the deterministic requirements are met; however, plant operators often consider them too restrictive and tend to relax these specifications. This relaxation may be accepted if i) the increase in risk associated to the proposed change is low or it is outweighed by other changes that reduce risk and/or ii) financial benefit is gained by the change. Examples where plant operators have changed the way a plant is operated in order to gain financial benefit include: increasing the standard test intervals or allowed outages for components; testing diesel generators less frequently to reduce the wear arising from repeated starts; increasing the period between refueling outages, from 2 to 3 years for instance; carrying out more maintenance while the reactor is working and allowing more components to be removed from service at the same time, which would reduce the duration of plant shutdown.

4.2 Step 2 – Identify the applicable requirements and criteria

At this stage, requirements related to the specific issue addressed have to be identified; these include mandatory (further described in § 4.2.1), deterministic (§ 4.2.2), probabilistic (§ 4.2.3) and other requirements (§ 4.2.4).

4.2.1 Step 2.A – Identify the mandatory requirements

Mandatory requirements depend on the type of issue, but in general they will include legal requirements, governmental decrees, current regulations, and plant technical specifications. One of the mandatory requirements is the need to ensure that the risk is reduced to a level that is *As Low As Reasonably Practicable* (ALARP). In many cases, the test of reasonable practicability is to show that the costs of making the change are not excessive when compared to the benefits that would be obtained: this is often addressed by carrying out benefit-cost analyses.

The expectation is that the plant would remain within the licensed domain after the changes have been made.

4.2.2 Step 2.B – Identify the deterministic requirements

The aim of this step is to define and apply a set of *conservative* rules and *deterministic* requirements for the design and operation of a nuclear plant. If these rules are met, they are expected to provide a high degree of confidence that the level of risk is acceptably low. This conservative approach has provided a way of taking into account uncertainties in the performance of equipment and humans.

At a higher level, the deterministic requirements relate to i) providing defense-in-depth and ii) maintaining sufficient safety margins **[IAEA 2005]**:

1. **Providing defense-in-depth**: The defense-in-depth philosophy has traditionally been applied in reactor design and operation to provide multiple means to accomplish safety functions and prevent the release of radioactive material. In other words, the aim of addressing defense-in-depth is to ensure that focus is given to preventing initiating events, providing safety systems to prevent core damage, avoiding containment failure and mitigating the consequences of any releases of radioactive material; this means that multiple barriers are maintained intact to prevent the release of radioactive material from the plant.
   According to USNRC, defense in depth philosophy is maintained if **[USNRC 2002]**:
   (a) a reasonable balance is preserved among prevention of core damage, prevention of containment failure, and consequence mitigation;
   (b) over-reliance on programmatic activities or operator actions to compensate for weaknesses in plant design is avoided: for example, maintenance and surveillance activities should be intended to *complement* and *not replace* proper plant design;
   (c) system redundancy, independence, and diversity are preserved commensurate with the expected frequency and consequences of challenges to the system, and associated uncertainties (*e.g.*, no risk outliers);
   (d) defenses against potential common cause failures are preserved, and the potential for the introduction of new common cause failure mechanisms is assessed;
   (e) independence of barriers is not degraded;
   (f) defenses against human errors are preserved.

2. **Ensuring safety margins**: The aim is to design the plant and the safety systems in such a way as to provide a large margin between how the plant would behave in fault conditions and failure of any of the barriers to the release of radioactive material. These margins should be sufficient to take account of any uncertainties in the analysis methods and data **[IAEA 2003]**. For example, the operation of the containment systems needs to ensure that during an accidental transient there is a large margin between the temperature and pressure conditions reached in the containment and those that would lead to failure so that there is a high degree of confidence that damage of the containment cannot occur.

The lower level principles relate to i) the single failure requirement, ii) preventing common cause failure, iii) providing equipment qualification, iv) limiting the claims made on the plant operating staff **[IAEA 2005]**:

- **Applying the single failure requirement**: For safety systems provided to ensure any safety functions, the requirement is that they be designed in such a way that no single failure prevents them from carrying out their safety function. Therefore, the safety systems usually have more than one train of equipment that is capable of carrying out the safety function. The single failure requirement is normally applied to the active components that are required to operate in order to perform the safety function; in some cases it may also be applied to passive components **[IAEA 1990]**.
- **Preventing common cause failure**: The reliability of the safety systems that have a number of similar/redundant trains is limited by common cause failures. When a high level of reliability is required, diverse means of carrying out the safety function need to be incorporated. Diversity can be provided by:
  (a) carrying out the safety function by using a different physical process;
  (b) using different equipment to carry out a given safety function;
  (c) using equipment of the same type but from different manufacturers in the two different systems.
- **Providing equipment qualification**: The design aim is to ensure that structures, systems and components are able to withstand the environmental conditions and loadings that they would experience following accident conditions and different initiating events. This is done by defining design basis events, such as the *Design Basis Earthquake* (DBE). Analysis needs to be carried out to demonstrate that structures would not fail, and systems and components would be able to carry out their safety functions where required following the DBE. The way in which the DBE needs to be defined is often prescribed in regulatory guidance.
- **Limiting the claims made on the plant operators**: The design aim is to ensure that the demands made on the plant operators in fault conditions are achievable. This is done by applying deterministic requirements, which, for example, require that no operator actions should need to be carried out in the very short term (for instance, within the first 10 to 30 minutes) in the main control room or in the short term (*e.g.*, within the first two hours) in any plant area following any initiating event.

4.2.3 Step 2.C – Identify the probabilistic requirements

For nuclear power plants probabilistic requirements are typically given in terms of two risk metrics:

- the *Core Damage Frequency* (CDF), expressed in $[\text{reactor} \cdot \text{year}]^{-1}$, is an expression of the likelihood that, given the way a reactor is designed and operated, an accident could cause the fuel in the reactor to be damaged;
- the *Large Early Release Frequency* (LERF), expressed in $[\text{reactor} \cdot \text{year}]^{-1}$, is an expression of the likelihood of those core damage accidents that can lead to large, unmitigated releases from containment before effective evacuation of the nearby population have the potential to cause prompt fatalities.

A possible framework for the definition of probabilistic criteria was given in **[IAEA 1999]**. This defines a "threshold of tolerability" above which the level of risk would be intolerable and a "design target" below which the risk would be broadly acceptable. Between these two levels there is a region where the risk would only be acceptable if all reasonable achievable measures have been taken to reduce it **[IAEA 2005]**. Based on current experience with nuclear power plant design and operation, numerical values were proposed that could be achieved by current and future designs. For the CDF, the objective is 10^{-4} per reactor-year for existing plants and 10^{-5} per reactor-year for future plants. For a large release of radioactive material, the objective is 10^{-5} per reactor-year for existing plants and 10^{-6} per reactor-year for future plants.

Following these general objectives, in the USA the probabilistic requirements for accepting changes in the design or operation of a plant are provided in **[USNRC 2002]**:

- changes that lead to a reduction in the risk (CDF and LERF) would normally be allowed;

- changes that lead to a small increase in the risk ($< 10^{-6}$ per reactor year for CDF and $< 10^{-7}$ per reactor year for LERF) would normally be allowed unless the *overall* risk is high (*i.e.*, *considerably* larger than 10^{-4} per reactor year for CDF or *considerably* larger than 10^{-5} per reactor year for LERF), in which case the focus would need to be on finding ways to reduce the risk (area C in figure 4.3);
- changes that lead to a moderate increase in the risk (in the range 10^{-6} to 10^{-5} per reactor year for CDF or 10^{-7} to 10^{-6} per reactor year for LERF) would normally be allowed only if it can be shown that the overall risk is small (that is CDF < 10^{-4} per reactor year and LERF $< 10^{-5}$ per reactor year) (area B in figure 4.3);
- changes that would lead to a large increase in the risk ($> 10^{-5}$ per reactor year for CDF or $> 10^{-6}$ per reactor year for LERF) would not be allowed (area A in figure 4.3).

These guidelines are intended for comparison with the results obtained by using a PRA to determine the change in the CDF or LERF for the proposed change to the design or operation of the plant (§ 4.3.3).

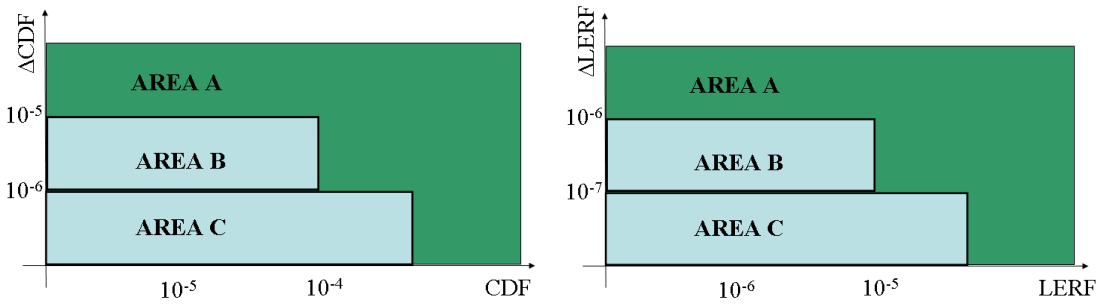


Figure 4.3 – *Probabilistic acceptance criteria for CDF (left) and LERF (right)* [USNRC 2002]

4.2.4 Step 2.D – Identify other requirements

The aim of this step is to ensure that any other relevant factors that have not already been addressed are included in the decision-making process. These factors could include the following:

- **Costs**: the cost of making modifications to the design or operation of the plant. This would include the costs of producing the design, procuring the hardware, installation, commissioning, and any losses in revenue that would be incurred if the plant needs to be shut down to make the changes.
- **Radiation doses**: the radiation doses that would be incurred by workers in making the modifications to the design of the plant.
- **Operating experience**: this would include experience from the plant operation and the findings from regulatory inspections. Any adverse findings would need to be taken into account in the decision-making process.
- **Economic benefits**: many of the modifications that are proposed by plant operators would lead to a benefit — that is, a higher rate of income from the plant or lower maintenance costs. For example, if the issue relates to increasing the power level for a nuclear power plant or increasing the throughput of a fuel reprocessing plant, this would result in an increase in the revenue for the plant. This needs to be recognized in the decision-making process, although economic benefits would not usually have a significant influence on the decision.
- **Remaining lifetime**: it is often the case that the need to make modifications is identified as part of a Periodic Safety Review that has been carried out for an older nuclear facility and the remaining lifetime of the plant needs to be taken into account in the decision-making process. If the remaining lifetime is short, it may not be reasonably practicable to make a change and consideration needs to be given to whether it would be acceptable for the plant to continue operation without improvements being made.

▷ **Cost-benefit ratio**: it is often the case that the costs and benefits of making a plant modification are compared by carrying out a formal cost-benefit analysis.

4.3 Step 3 – Evaluate how the plant safety issue affects the requirements

The change to the design or operation of the plant needs to be reviewed in order to determine how it affects the mandatory (§ 4.3.1), deterministic (§ 4.3.2), probabilistic (§ 4.3.3) and other (§ 4.3.4) requirements.

4.3.1 Step 3.A – Evaluate how the change affects the mandatory requirements

Although some of the mandatory requirements (identified at Step 2.A of § 4.2.1) may be overriding, the integrated decision-making process would still be followed to ensure that this was done in the optimum way. The areas where any of the applicable mandatory requirements are not met would need to be taken into account in the decision-making process. This would need to be the case for all the issues addressed apart from those that related to a request for an exemption to the existing licensing requirements/regulations.

4.3.2 Step 3.B – Carry out the assessment to get deterministic insights

In this step, an assessment is carried out by comparing with the applicable deterministic requirements identified in Step 2.B (§ 4.2.2): the aim would be to identify any areas where these requirements are not met.

For defence-in-depth requirements, the aim would be to determine if there were any shortfall in the provisions made for preventing initiating events from occurring, for coping with initiating events, for containment so that radioactive material is not released to the environment and for protecting the public if a release should occur. The aim would be to determine whether any of these provisions fell short of the defined standard.

For safety systems, the aim would be to determine whether sufficiently diverse equipment had been incorporated to provide protection against frequent initiating events, whether sufficient redundancy had been provided by applying the single failure criterion to safety systems, *etc.*

It is widely recognized that there are **uncertainties** in many of the issues addressed by the assessments of the deterministic insights. For example, there are uncertainties in i) the analytical models, computer codes and data used to predict the behavior of the plant in operational/accident conditions, and ii) the hazard curves that are used to define different hazardous events and the capability of structures, systems and components to withstand such events.

The traditional way in which these uncertainties are treated in the assessment of deterministic insights is to make *conservative assumptions* and use conservative *models* and *data*. For example, for *design basis accidents*, the analysis assumes that: a) the postulated initiating event has occurred, b) the event occurs at a time when the initial conditions are at the worst end of their range, c) no credit is taken for the operation of the control systems (unless they aggravate the situation), d) the worst single failure occurs in the protection systems and e) conservative damage criteria are used for the aspects of plant safety challenged by the initiating event. The aim of using these assumptions is to ensure that **safety margins** are available and that there is a *high level of confidence* that failure conditions are not reached.

Design Basis Accident

A design basis accident (DBA), or maximum credible accident, is a combination of postulated challenges and failure events against which nuclear power plants are designed to ensure adequate and safe plant response. They are the set of accidents for which system designers make explicit provision, ensuring that their design is able to withstand their effects. Different DBA subtypes include design-basis earthquakes, floods and fires.

The current trend is to use best estimate codes for deterministic accident analyses provided that they are either combined with a reasonably conservative selection of input data or are associated with the evaluation of the uncertainties of the results. A good level of conservatism is still expected to be built into the deterministic analysis needed to demonstrate to the regulatory body that sufficient safety margins exist **[IAEA 2005]**.

4.3.3 Step 3.C – Carry out the assessment to get probabilistic insights

For a nuclear power plant, the normal approach is to carry out a PRA. The PRA can be used in two ways:

- to provide an estimate of the risk from the plant (usually the CDF and sometimes LERF) and to use this analysis to determine whether there are weaknesses in the design or operation;
- to determine the change in the risk that would arise from proposed changes to the design or operation of the plant.

For purposes of implementation, the licensee[6] should assess the expected change in CDF and LERF. The necessary sophistication of the evaluation, including the scope of the PRA (*e.g.*, internal events only, full power only), depends on the contribution the risk assessment makes to the integrated decision-making, which depends to some extent on the magnitude of the potential risk impact. For changes that may have a more substantial impact, an in-depth and comprehensive PRA analysis, appropriate to derive a quantified estimate of the total impact of the proposed change, will be necessary to provide adequate justification. In other applications, calculated risk-importance measures or bounding estimates will be adequate. In still others, a qualitative assessment of the impact of the plant change on the plant's risk may be sufficient.

The remainder of this section discusses the use of quantitative PRA results in decision-making. This discussion has two parts:

1. A fundamental element of USNRC's risk-informed regulatory process is a PRA of sufficient scope, level of detail, and technical acceptability for the intended application. We discuss below the expectations with respect to the needed PRA's *scope*, *level of detail*, and *technical acceptability*.
2. One of the strengths of the PRA framework is its ability to characterize the impact of *uncertainty* in the analysis, and it is essential that these uncertainties be recognized when assessing whether the principles are being met. We present guidelines on how the uncertainty is to be addressed in the decision-making process.

Quality of the PRA analysis

One overall requirement is that the scope, level of detail and quality of the PRA needs to be consistent with its intended applications and the role that the probabilistic input plays in the decision-making process **[USNRC 2002; IAEA 2005]**:

is the analysis comprehensive?

- **PRA scope**: The goals and scope of the PRA, and its intended applications need to be clearly defined at the start of the analysis. The emerging standard for PRAs currently produced is to aim for completeness so that all the contributions to the risk are addressed in the analysis. This includes all internal and external initiating events and hazards and addresses all the modes of operation of the plant. However, the scope of the PRA used may sometimes be less than this and, if this is the case, the limitations in its use will need to be recognized.
- **Level of detail of the PRA**: This needs to be sufficient to allow the impact of the proposed changes in the design or operation of the plant to be modeled. The emerging standard is for PRAs to be carried out to a detailed component level, which would normally allow the change in the CDF or LERF to be estimated for the majority of the proposed changes. For some applications, the required risk information can be generated by developing a very simple probabilistic model. However, for other applications, such as configuration risk management, a very detailed PRA model is required. In general, the more detailed the PRA model produced, the wider will be the range of applications for which the PRA will be suitable.
- **PRA technical acceptability**: The methods used in the analysis need to be consistent with the state of the art and current best practices as defined in national and international

[6] The licensee of a nuclear power plant is the organization which has obtained a license from the US NRC to operate the plant.

PRA standards and guidance. In recent years, there have been a number of activities to develop PRA standards **[Mosleh et al. 1989]**. The aim has been to improve the accuracy, consistency and usability of the PRAs produced **[USNRC 1978]**.

Comparison of PRA results with acceptance guidelines, including uncertainties

This section provides guidance on comparing the results of the PRA with the acceptance guidelines described in § 4.2.3. In the context of integrated decision-making, the acceptance guidelines should *not* be interpreted as being *prescriptive*: instead, they are intended to provide an indication, in numerical terms, of what is considered acceptable. As such, the numerical values defining the areas in figure 4.3 (☞ page 28) are approximate values that provide an indication of the changes that are generally acceptable. Furthermore, the uncertainties associated with PRA calculations preclude a definitive decision with respect to which area the application belongs to based purely on the numerical results **[USNRC 1998c, 2002]**[7].

The different acceptance guidelines reported in § 4.2.3 require different depths of analysis. Changes resulting in a decrease in the CDF and LERF estimates do not require an assessment of the calculated baseline CDF and LERF. Generally, it should be possible to argue on the basis of an understanding of the contributors and the changes that are being made that the overall impact is indeed a decrease, without the need for a detailed quantitative analysis.

If the calculated values of CDF and LERF are very small (area C in figure 4.3), a detailed quantitative assessment of the baseline value of CDF and LERF will not be necessary. However, if there is an indication that the CDF or LERF could considerably exceed 10^{-4} and 10^{-5} respectively, in order for the change to be considered the licensee may be required to present arguments as to why steps should not be taken to reduce CDF or LERF. Such an indication would result, for example, if i) the calculated contribution to CDF or LERF significantly exceeds 10^{-4} and 10^{-5} respectively, ii) there has been an identification of a potential vulnerability from a margins-type analysis, or iii) historical experience at the plant in question has indicated a potential safety concern.

For larger values of ΔCDF and ΔLERF (area B in figure 4.3) an assessment of the baseline CDF and LERF is required **[USNRC 2002]**.

To demonstrate compliance with the numerical guidelines, the *level of detail* required in the assessment of the values and the analysis of uncertainty related to *model* and *incompleteness* issues will depend on what follows **[USNRC 1998c]**: in area C of figure 4.3, the closer the estimates of ΔCDF or ΔLERF are to their corresponding acceptance guidelines, the more detail will be required. Similarly, in Area B of figure 4.3, the closer the estimates of ΔCDF or ΔLERF and CDF and LERF are to their corresponding acceptance guidelines, the more detail will be required. On the contrary, if the estimated value of a particular metric is very small compared to the acceptance goal, a simple bounding analysis may suffice with no need for a detailed uncertainty analysis.

Because of the way the acceptance guidelines are developed, the appropriate numerical measures to use in the initial comparison of the PRA results to the acceptance guidelines are mean values. The mean values referred to are the *means* of the probability distributions that result from the propagation of the uncertainties on the input parameters and those model uncertainties explicitly represented in the model. While a formal propagation of the uncertainty is the best way to correctly account for state-of-knowledge uncertainties that arise, *e.g.*, from the use of the same *parameter* values for several basic event probability models, under certain circumstances, a formal propagation of uncertainty may not be required if it can be demonstrated that the state-of-knowledge correlation is unimportant. This will involve, for example, a demonstration that the bulk of the contributing scenarios (cut sets or accident sequences) do not involve multiple events that rely on the same parameter for their quantification **[USNRC 2002]**.

[7] There are two facets to uncertainty that, because of their natures, must be treated differently in PRA applications. As mentioned earlier (note 4 of § 3.2.2). They have been termed *aleatory* and *epistemic* uncertainty. In addition, it is useful to identify three classes of epistemic uncertainty that are addressed in and impact the results of PRAs: *parameter* uncertainty, *model* uncertainty, and *completeness* uncertainty **[Helton 1998; USNRC 1990, 2005, 2002, 2009]**.

While the analysis of *parametric* uncertainty is fairly mature, and is addressed adequately through the use of mean values, the analysis of the *model* and *completeness* uncertainties cannot be handled in such a formal manner. Whether the PRA is complete or only partial, and whether it is only the change in metrics or both the change and baseline values that need to be estimated, it will be incumbent on the licensee to demonstrate that the choice of reasonable *alternative* hypotheses, *adjustment factors*, or modeling *approximations* or *methods* to those adopted in the PRA model would not significantly change the assessment. This demonstration can take the form of well formulated sensitivity studies or qualitative arguments. It is not the intent that the search for alternatives should be exhaustive and arbitrary. For the decisions that involve only assessing the change in metrics, the number of model uncertainty issues to be addressed will be smaller than for the case of the baseline values, when only a portion of the model is affected. The alternatives that would drive the result toward unacceptableness should be identified and sensitivity studies performed or reasons given as to why they are not appropriate for the current application or for the particular plant. In general, the results of the sensitivity studies should confirm that the guidelines are still met even under the alternative assumptions (*i.e.*, change generally remains in the appropriate region). Alternatively, this analysis can be used to identify candidates for compensatory actions or increased monitoring. The licensee should pay particular attention to those assumptions that impact the parts of the model being exercised by the change **[USNRC 2002]**.

One alternative to an analysis of uncertainty is to design the proposed change such that the major sources of uncertainty will not have an impact on the decision-making process. For example, in the region of the acceptance guidelines where small increases are allowed regardless of the value of the baseline CDF or LERF, the proposed change to the plant could be designed such that the modes of operation or the initiating events that are missing from the analysis would not be affected by the change. In these cases, incompleteness would not be an issue. Similarly, in such cases, it would not be necessary to address all the model uncertainties, but only those that impact the evaluation of the change.

4.3.4 Step 3.D – Carry out the assessment to get insights from other relevant factors

The aim is to carry out the assessment to get insights from the relevant factors listed in § 4.2.4:

- the doses to workers that would be incurred while carrying out the work to make any changes required to the design of the plant;
- the costs and timescales for carrying out the work, which would include an identification of any periods for which the plant would need to be shut down;
- any benefits that would arise (such as an increase in the revenue from the plant);
- a benefit-cost analysis to compare the costs of making the modifications to the benefits that would be obtained from it;
- any adverse factors that could arise in making the change: for a nuclear power plant, this could include an increase in the operational complexity of the plant and any additional burden on the plant operators;
- insights from the operational experience data or inspection findings that are relevant to the issue.

4.4 Step 4 – Weight the inputs from the assessments carried out

The manner in which the mandatory requirements and the deterministic, probabilistic and other insights are weighted depends on the particular issue being addressed. Therefore it is not possible to give definitive guidance on how this should be done: much of this weighting is subjective and relies on engineering judgments **[IAEA 2005]**.

Where the insight relates to mandatory national legal requirements or to the need to meet established national practices, these would normally carry the highest weight and will have to be observed (unless, of course, the issue being considered relates to a change in rules or regulations or a request for regulatory exemption).

The relative weights given to the deterministic and probabilistic insights reflects the confidence that the regulatory body has in the PRA. Although a higher weight has traditionally been

given to deterministic analyses, the current trend is for high quality PRAs to be produced and for PRA insights to be used effectively in the regulatory decision-making process.

The degree to which the risk insights play a role, and therefore the need for detailed staff review, is application dependent. **Quantitative risk results** from PRA calculations are typically the most useful and complete characterization of risk, but they are generally supplemented by **qualitative risk insights** and **traditional engineering analysis**. Qualitative risk insights include generic results that have been learned from the numerous PRAs that have been performed in the past decades and from operational experience. For example, if one is deciding which motor-operated valves in a plant can be subject to less frequent testing, the plant-specific PRA results can be compared with results from similar plants. This type of comparison can give support to the licensee's analysis and reduce the reliance of the staff review on the technical acceptability of the licensee PRA. However, as a general rule, applications that impact large numbers of systems, structures and components (SSCs) will benefit from a PRA of high quality.

In addition, the weight given to the probabilistic analysis will take account of the type of probabilistic input that was provided — that is, whether it is based on a full PRA analysis or whether only less formal risk insights are available. If a full scope PRA has been used, the weight of the PRA insights will further depend on the quality of the analysis carried out. This will also take account of the results of sensitivity studies and uncertainty analysis, where these have been carried out.

It is often the case that the deterministic and probabilistic insights are in agreement. For example, a modification that improves the deterministic position (for example, it increases the level of redundancy or diversity in the safety systems) will also lead to a reduction in the risk. In this case, the relative weighting of the deterministic and probabilistic insights may be less important and the outcome of the decision may depend on other factors such as the dose to workers or the results of the benefit-cost analysis.

If the deterministic and probabilistic insights are not in agreement, it is often the case that greater weight is given to the more conservative insight — that is, the one that indicates a need for improvement.

The weighting that would be applied to the need for a modification would be greater if the results of the probabilistic analysis showed that the overall risk from the plant was approaching a level that was not acceptable or if the change to the plant removed one of the weaknesses in the design or operation of the plant that has been identified from the PRA.

Finally, the weighting would also be expected to take account of the outcome of any benefit-cost analysis that had been carried out; if this has shown that the costs of making the changes are excessive when compared to the benefits that would be obtained, this would lead to a low weighting for the change to be made.

4.5 Step 5 – Make the decision

In making the decision, the regulatory body will need to take account of all the requirements and insights identified from the preceding steps, combine them taking account of the different weights assigned to them and reach a decision on whether the proposed change should be accepted or rejected. However, there is a fundamental difficulty in doing this because the requirements and insights obtained from the preceding steps are not expressed in the same units.

It is good practice for the regulatory body to involve **multidisciplinary teams** in the decision-making process where the members of the team are able to deal with the diverse inputs with different weights. The team normally includes members who can cover all the disciplines involved (transient analysis, radiological analysis, human factors task analysis, severe accident analysis, PRA, *etc.* as required for the issue being addressed) and are familiar with the plant (which would include the design, operation, operational experience, *etc.*). In addition, due account will need to be taken of the **uncertainties** associated with the deterministic and probabilistic analyses, and the other factors taken into account in the decision-making process. Finally, other factors that the multidisciplinary teams may wish to take into account in making the decision include the cumulative impact of previous changes and the **overall performance** of

the plant as reflected by inspection findings, operational data and plant performance indicators **[USNRC 2002; IAEA 2005]**.

The inputs provided by the multidisciplinary team experts in each of the areas would include:

- the methods and data used, and the assumptions made, in carrying out the analysis, identifying also limitations that might impact the use of the results;
- the conclusions drawn from the analysis carried out;
- an understanding of any uncertainties in the analysis and the results of any sensitivity studies that have been carried out;
- the relationship between the input that they are providing and that are being provided by the other experts.

Decision-making benefits of a multidisciplinary team

Inputs in the field of maintenance actions and policies have a close connection and dependence with inputs in the fields of human factors (*e.g.* in the modeling of possible operator errors) and, for instance, with the study and quantification of the radiation doses that would be incurred by workers and operators in making the modifications to the design of the plant.

Each member of the multidisciplinary team would be expected to have a high level of expertise in at least one of the areas that provide a significant input into the decision-making process. They would need to be able to explain their input also to non-specialists. They would also need to have a broad perspective on nuclear safety issues so that they would be able to understand and take account of the inputs being provided by the other experts. The level of expertise of the members of the multidisciplinary team would need to be consistent with the importance of the decision being made.

If more than one issue arises at the same time, it is recommended that the regulatory body consider them individually and make a separate decision made on each of them. If two or more issues are considered together, it is possible that one of the issues may lead to a relatively large increase in the risk, which would be masked by a relatively large decrease in the risk from the others. This needs to be avoided and each of the issues should be considered on its own. However, if a number of proposals arise within a short period to make changes that would lead to the risk being increased, it is advisable that the regulatory body take account of the **combined effect** of these changes to make sure that this is also acceptable **[IAEA 2005]**.

4.6 Step 6 – Implement the decision

Decisions concerning the implementation of changes should be made in light of the uncertainty associated with the results of the traditional and probabilistic engineering evaluations. Broad implementation within a limited time period may be justified when uncertainty is shown to be low (data and models are adequate, engineering evaluations are verified and validated, *etc.*), whereas a slower, phased approach to implementation (or other modes of partial implementation) would be expected when uncertainty in evaluation findings is higher and where programmatic changes are being made that could impact SSCs[8] across a wide spectrum of the plant, such as in in-service testing and in-service inspection. In such situations, the potential introduction of common cause effects must be fully considered and included in the submission.

The way in which changes towards risk informed regulations would be implemented depends on the respective national legislative system and the legal status of the regulations **[IAEA 2005]**.

Impact of the legislative context on decision-making

Filtered containment venting systems and other equipment such as hydrogen re-combiners have been incorporated to increase the level of defence-in-depth against severe accident scenarios in some US states but not in others, due to the greater significance that has been placed on providing protection for the containment.

[8] Systems, structures and components.

4.7 Step 7 – Monitor the effect of the decision

It is good practice that the consequences of any decisions made be monitored and feedback provided on their effectiveness. The aim of monitoring is to determine whether the change has been made effectively and whether there are any adverse effects. Such monitoring is usually performance based.

For changes to the design or operation of a nuclear facility, a monitoring process would usually be agreed with the plant operators and this would be included in inspection activities by the regulatory body.

Performance-monitoring strategies should be considered carefully to ensure that no safety degradation occurs because of the changes to the plant. The main concern is the possibility that the cumulative impact of changes that affect a large class of SSCs could lead to an unacceptable increase in the number of failures due to degradation, including possible increases in common cause mechanisms. Therefore, a monitoring plan should be established to make sure that the engineering evaluation used to analyze the impact of the proposed changes continues to reflect the actual reliability and availability of the SSCs involved. Further details of acceptable processes for implementation in specific applications are discussed in **[USNRC 1998c,a,d,b]**.

The proposed monitoring programs should include a means to adequately *track* the performance of equipment that, when degraded, can affect the conclusions of the engineering evaluations and integrated decision-making that support the change to the plant. The program should be capable of trending equipment performance after a change has been implemented to demonstrate that performance is consistent with that assumed in the traditional engineering and probabilistic analyses that were conducted to justify the change. The program should be such that

1. SSCs are monitored in relation to their safety significance (*e.g.*, monitoring for SSCs categorized as having low safety significance may be less rigorous than that for SSCs of high safety significance);
2. feedback of information and corrective actions are put into effect promptly;
3. degradation in SSC performance is detected and corrected before plant safety is compromised.

As part of the monitoring program, measures for specific *cause determination*, *trending* of degradation and failures, and *corrective actions* should be considered. Such measures should be applied to SSCs relative to their safety significance as determined by the engineering analyses that support the plant change. A determination of cause is needed when performance expectations are not being met or when there is a functional failure of an application-specific SSC that poses a significant condition adverse to performance. The cause determination should identify the cause of the failure or degraded performance to the extent that corrective action can be identified that would preclude the problem or ensure that it is anticipated prior to becoming a safety concern. It should address failure significance, the circumstances surrounding the failure or degraded performance, the characteristics of the failure, and whether the failure is isolated or has generic or common cause implications **[Mosleh et al. 1989]**.

Finally, the monitoring program should identify any **corrective actions** to preclude the recurrence of unacceptable failures or degraded performance. The circumstances surrounding the failure may indicate that the SSC failed because of adverse or harsh operating conditions (for instance, operating a valve dry, or over-pressurization of a system) or failure of another component that caused the SSC failure. Therefore, corrective actions should also consider SSCs with similar characteristics with regard to operating, design, or maintenance conditions. The results of the monitoring need not be reported to the regulator, but should be retained onsite for inspection.

5

Conclusions

In the past, regulatory bodies have used a *deterministic* approach as the basis for making decisions on safety issues and organizing the activities that they carry out. This was done by applying high level criteria such as the need to provide defence-in-depth and adequate safety margins. These were developed into lower level requirements, which were aimed at ensuring that the risk to workers and members of the public was adequately controlled. The need to meet these deterministic requirements is the basis for most of the regulations, safety standards, guidance, *etc.* that are currently being used by regulatory bodies. The main strength of the deterministic approach is that it is *well developed* and that there is a *very large body of experience* in applying this approach. However, there are a number of shortcomings in the deterministic approach that need to be recognized and these include the following **[IAEA 2005]**:

- in the past, the deterministic approach has tended to look at *infrequent, bounding* fault conditions rather than less severe faults that are more frequent and often give a greater contribution to the risk;
- the deterministic approach only takes initiating event frequencies and component failure probabilities into account in an *approximate* way, so that it is not possible to determine whether the design of the safety-critical system is balanced, *i.e.*, whether any group of initiating events makes a contribution to the risk that is much larger than the others (for example, in most situations, greater levels of redundancy and diversity need to be provided for frequent initiating events than for infrequent initiating events). It has often been the case that the deterministic approach has led to a very high level of protection being provided for some initiating events but not for others;
- when a review against deterministic principles has been carried out for a safety-critical system and shortfalls have been identified, it is not possible to determine which of the possible improvements would give the greatest reduction in risk and hence which of them need to be given the highest priority for implementation.

Although the deterministic approach has been refined over the years, it is widely recognized that the reliance on a deterministic approach on its own is unlikely to be sufficient to demonstrate that high levels of safety have been achieved in a way that is balanced across initiating events and safety systems. This has been seen from the PRAs that have been carried out and have demonstrated that some of the contributions to the risk have not been adequately controlled by the deterministic approach. Actually, in recent years, PRAs has been developed and the information provided by these PRAs is increasingly being used to *complement* the deterministic approach. The move has been towards an **integrated approach** that combines the insights provided by the deterministic approach and those from the probabilistic approach with any other requirements in making decisions on a safety issue or in deciding on the priorities for the activities to be carried out by the regulatory body. When this integrated process is applied to making decisions about safety issues in safety-critical systems, this is sometimes referred to as **Risk Informed Decision Making** (RIDM). When it is applied to making decisions about the way in which a regulatory body carries out its activities, this is sometimes referred to as **Risk informed Regulation**.

In this framework, in order to exemplify the general concepts, definitions and issues related to RIDM, the present document has described in detail the RIDM processes adopted by two American regulatory bodies in the complex, safety-critical fields of aerospace and nuclear

engineering: the National Aeronautics and Space Administration (NASA) and the United States Nuclear Regulatory Commission (US NRC), respectively. Although both regulatory bodies employ RIDM approaches, their interpretation of RIDM seems slightly different: the NRC implementation (as in the nuclear area in general) seems to be more focused on *increasing* the impact that PRA have on regulatory decisions: the focus is thus on how to *resolve* possible conflicts between deterministic analyses and PRA. The NASA focus seems to be a combination of a better decision structure crossing internal organizational boundaries (following the objective hierarchy) and support for multi-criteria decisions under uncertainty. In spite of this slightly different interpretation, from a detailed analysis of the two RIDM processes it can be concluded that in general the main strengths of the use of a probabilistic approach to inform decisions related to safety-critical systems are the following **[IAEA 2005]**:

- the analysis starts from a comprehensive list of initiating events and sets out to identify all the fault sequences that could lead to system damage;
- initiating event frequencies and system/component failure probabilities are included *explicitly* and not *approximately* in the PRA model: thus, through PRA it is possible to determine whether the design is balanced;
- the analysis provides a **quantitative estimation of the level of risk** from the system;
- the PRA models *all* initiating events, hazards and structures/systems/components in a **single model**. Hence:
  - It is possible to derive the *relative importance* of each of them explicitly. Such an explicit ranking is not possible in the deterministic approach since it treats each of the initiating events and hazards separately. Modern PRA software provides calculations of a number of **importance functions** that can be used to determine the risk significance of all the initiating events, fault sequences and structures/systems/components included in the PRA model. At the NRC, for instance, some rules related to equipment deemed to be safety related have changed **[Collins 2001]**:

    > *With insights provided from PRAs, the NRC now realizes that some equipment that has historically been categorized and treated as safety related, and thus subject to special restrictions, in fact only makes a limited contribution to risk and is therefore eligible for relief from regulatory requirements. Conversely, other equipment that was not previously categorized as safety related is now understood to have safety significance and is therefore eligible for enhanced treatment.*

  - The analysis can be used to identify also *where* improvements to the design and operation of the system are needed to give the greatest reduction in risk.
  - The PRA provides a very good means of **comparing relative risks**.
- Modern PRA software allows some of the **parameter uncertainties** to be addressed explicitly.

On the other hand, shortcomings in the probabilistic approach arise from the *scope* or *level of detail* (and quality) of the PRA, which make the use of PRA for regulatory relief still **controversial** and challenge further developments and applications of risk-informed decision-making and performance-based regulation **[IAEA 2005]**:

- A main obstacle to the implementation of risk-informed decision-making is the fact that **quantitative risk acceptance criteria** for all categories of regulatory objectives do not exist in the most countries. Risk-informed decision-making is not possible without **general probabilistic safety goals** as well as **detailed quantitative acceptance criteria** on the level of safety function, system and components reliability. The top level safety goals, which give answers to the question "How safe is safe enough", have to be defined by the policy and society. If such a definition is not provided, the elaboration of detailed quantitative acceptance criteria on the safety function, system and component levels by technical expertise is without normative foundation and therefore meaningless **[Hahn 2002]**.
- It is important to ensure that the results of a PRA analysis are not **used outside their range of validity** (*i.e.*, outside the range of validity of the models employed for the analysis itself). This shortcoming relates to the use of a particular PRA for a *particular application* (rather than of PRAs in general) and needs to be recognized by the user of the PRA when providing an input into the risk informed process.

- ▷ It is not possible to fully demonstrate that the PRA model is *complete*, in that all the initiating events and fault sequences that could contribute to the risk have been identified.
- ▷ There are very large (orders of magnitude) **uncertainties** in some areas of the PRA so that the results are difficult to use in the decision-making process.
- ▷ There are modeling difficulties and a high degree of **subjectivity** in some areas of the PRA — for example, modeling human errors of commission and dependency between individual human errors.
- ▷ Potentially risk-relevant factors such as the influence of organization, management and safety culture are normally not considered in current PRAS.

Owing to the reasons mentioned, it has often been difficult to compare the PRAs that have been carried out for similar systems due to differences in methodology and data. It should be stressed that this is a limitation for the potential application of the PRA rather than the PRAs themselves. However, this has led to reluctance by some regulatory bodies to accept the use of PRA to the extent that they are able to move towards a risk-informed approach.

Finally, it should be noted that, in risk informed decision-making and risk informed regulation, the PRA provides *only one of the inputs* into the decision-making process — the others being related to factors such as the degree to which any mandatory requirements are met, the insights from the deterministic analysis, the results of any cost benefit analysis, special considerations, *etc.* A risk-based approach in which the input from the PRA (or other risk analysis) is the sole input into the decision-making process is not advisable.

A

Deriving performance measures in the NASA RIDM process

The following practical cases can be considered when deriving performance measures for performance objectives (see § 3.1.2):

1. The performance objective of interest can be *easily* and *directly* represented by an appropriate performance measure: for example, the objective "Minimize cost" is naturally associated with the performance measure "Total cost". In addition, within the class of objectives that can be directly represented by a performance measure, the following two sub-classes can be identified:
   - ▷ objectives that are **empirically quantifiable** (*e.g.*, "Minimize cost", "Maximize payload mass", "Minimize development time", ...) have an obvious *natural* unit scale (*e.g.*, "Minimize cost" [$],"Maximize payload mass" [kg], "Minimize development time" [months]);
   - ▷ objectives that are not empirically quantifiable require the development of a so-called **constructed scale**. A constructed scale is typically appropriate for measuring objectives that are essentially *subjective*, or for which subjective or linguistic assessment is more appropriate. An example of this kind of objective could be "Maximize Stakeholder Support". In this case, "stakeholder support" is the attribute being measured, but there is no natural measurement scale by which an objective assessment of stakeholder support can be made. Instead, it might be reasonable to construct a scale that supports subjective/linguistic assessment of stakeholder support: for example, position 1 in the scale may be associated to "Action-oriented opposition", position 3 to "Neutrality", position 4 to "Support" and so on **[NASA 2010]**.
2. The performance objective of interest cannot be easily and directly represented by an appropriate performance measure; in such cases, a **proxy performance measure** can be identified. For example, the "Probability of Loss Of Crew" is a *natural* performance measure as applied to "astronaut life safety", but it may be a proxy for "overall astronaut health", particularly in situations where astronaut injury and/or illness are not directly assessable.

A remark is in order with respect to the classification reported above. Although it is preferable that a performance measure be directly measurable, this is not always possible, even for objectives with natural measurement scales. For example, a safety-related risk metric such as "Probability of Loss of Crew" is typically used to quantify the objective "Maintain Astronaut Health and Safety". This performance measure is the product of *modeling* activities as opposed to *direct measurement*, involving the integration of numerous parameters within an *analytical model* of the alternative under analysis. In such cases, the modeling protocols become part of the performance measure definition, which assures that performance measures are calculated consistently.

B

Ordering the performance measures in the NASA RIDM process

Because of possible correlations between performance measures, performance commitments are developed sequentially (*cf.* § 3.3.1). Thus, in general, performance commitments depend on the order in which they are developed. Qualitatively, the effect that performance measure order has on performance commitment values is as follows **[NASA 2010]**:

- If performance measures are **independent**, then the order is not important and the performance commitments will be set at the defined risk tolerances of the performance measures' marginal PDFs.
- If performance measures are **positively correlated** (in terms of their directions of goodness), then the performance commitments that lag in the ordering will be set at higher levels of performance than would be suggested by their marginal PDFs alone. This is because lagging performance measures will have already been conditioned on good performance with respect to leading performance measures. This, in turn, will condition the lagging performance measures on good performance, too, due to the correlation.
- If performance measures are **negatively correlated** in terms of their directions of goodness, then the performance commitments that lag in the ordering will be set at lower levels of performance than would be suggested by their marginal PDFs alone. Figure 3.8 (page 18) shows this phenomenon. In the bottom left of the figure, the PM_2 performance commitment is set at a slightly lower performance than it would have been if the data points that exceed the PM_1 performance commitment were not "conditioned out".
- The lower the risk tolerance, the lower the effect of conditioning on subsequent performance commitments. This is simply because the quantity of data that is "conditioned out" is directly proportional to risk tolerance.

These general effects of performance measure ordering on performance commitments suggest the following ordering guidelines:

- Order performance measures from low risk tolerance to high risk tolerance. This assures a minimum of difference between the risk tolerances as defined on the conditioned PDFs versus the risk tolerances as applied to the marginal PDFs.
- Order performance measures in terms of the desire for specificity of the performance measure's risk tolerances. For example, the performance commitment for the first performance measure in the ordering is precisely at its marginal PDF. As subsequent performance commitments are set, dispersion can begin to accumulate as conditioning increases.

C

Establishing risk tolerances on the performance measures in the NASA RIDM process

The RIDM process calls for the specification of a risk tolerance for each performance measure, along with a **performance measure ordering**, as the basis for performance commitment development (*cf.* § 3.3.1). These risk tolerance values have the following properties:

- the risk tolerance for a given performance measure is the same across all alternatives;
- risk tolerance may vary across performance measures, in accordance with the stakeholders' and decision-maker's attitudes towards risk for each performance measure.

Risk tolerances, and their associated performance commitments, play multipurpose roles within the RIDM process:

1. uniform risk tolerance across alternatives normalizes project/program risk;
2. the risk tolerances that are established during the RIDM process indicate the levels of acceptable initial risk that the CRM process commits to managing during implementation;
3. performance commitments based on risk tolerance enable point value comparison of alternatives in a way that is appropriate to a situation that involves thresholds (*e.g.*, imposed constraints): by comparing a performance commitment to a threshold, it is immediately clear whether or not the risk of crossing the threshold is within the established risk tolerance; in contrast, if a value such as the distribution mean were used to define performance commitments, the risk with respect to a given threshold would not be apparent.

Issues to consider when establishing risk tolerances include:

- relationship to imposed constraints (*e.g.*, in general, deliberators have a low tolerance for noncompliance with imposed constraints);
- high-priority objectives (*e.g.*, in general, it is expected that the deliberators will have a low risk tolerance for objectives that have a high priority, but for which imposed constraints have not been set);
- low-priority objectives and "stretch goals" (*e.g.*, in general, some decision situations might involve objectives that are not crucial to program/project success, but which provide an opportunity to take risks in an effort to achieve high performance).

Bibliography

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

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

Aven, T. (2010). *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.

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

Collins, S. J. (2001). Risk informed safety and regulatory decision making: an NRC perspective. In *Proceedings of the 2001 IAEA international conference on Topical issues in nuclear safety*. IAEA.

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.

Dezfuli, H., Stamatelatos, M., Maggio, G., and Everett, C. (2010). Risk-informed decision making in the context of NASA risk management. In *Proceedings of the PSAM 10 Conference*.

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. ISBN: 978-2225805790.

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.

Hahn, L. (2002). Impediments for the application of risk-informed decision making in nuclear safety (IAEA-CN-82/49). In *International Conference on Topical Isues in Nuclear Safety*. www-pub.iaea.org/MTCD/publications/PDF/pub1120/CD/PDF/Issue1/CN-82-49.pdf.

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.

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

IAEA (1990). *Application of the single failure criterion. IAEA safety series n°50-P-1*. Technical report, IAEA. ISBN: 92-0-123790-1.

IAEA (1999). *Living probabilistic safety assessment (LPSA), (IAEA-TECDOC-1106)*. Technical report, IAEA. www-pub.iaea.org/MTCD/Publications/PDF/te_1106_prn.pdf.

IAEA (2003). *Safety margins of operating reactors – analysis of uncertainties and implications for decision making (IAEA-TECDOC-1332)*. Technical report, IAEA. ISBN: 92-0-118102-7. www-pub.iaea.org/MTCD/publications/PDF/te_1332_web.pdf.

IAEA (2005). *Risk-informed regulation of nuclear facilities: overview of the current status (IAEA-TECDOC-1436)*. Technical report, IAEA. ISBN: 92-0-100105-3. www-pub.iaea.org/MTCD/Publications/PDF/TE_1436_web.pdf.

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.

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

Mosleh, A., Fleming, K., Parry, G., Paula, H., Worledge, D., and Rasmuson, D. (1989). *Procedures for treating common cause failures in safety and reliability studies: analytic background and techniques (NUREG/CR-4780)*. Technical report, US Nuclear Regulatory Commission. See also NUREG-5485.

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

NASA (2008). *Agency risk management procedural requirements (NPR 8000.4A)*. Technical report, NASA. nodis3.gsfc.nasa.gov/displayDir.cfm?Internal_ID=N_PR_8000_004A_.

NASA (2010). *Risk-informed decision making handbook (NASA/SP-2010-576)*. Technical report, NASA. standards.nasa.gov/documents/viewdoc/3315763/3315763.

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.

Plough, A. L. and Krimsky, S. (1987). *The emergence of risk communication studies: Social and political context.* Science, Technology & Human Values, 12:4–10.

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

USNRC (1975). *NUREG-75/014 (WASH-1400) Reactor safety study, an assessment of accident risks.* Technical report, US Nuclear Regulatory Commission. a.k.a. "the Rasmussen Report" (superseded by NUREG-1150). DOI: 10.2172/7134131.

USNRC (1978). *Quality assurance program requirements. Regulatory guide 1.33.* Technical report, US Nuclear Regulatory Commission. Revision 2.

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. 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. www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1150/.

USNRC (1998a). *An approach for plant-specific, risk-informed decision-making: Graded quality assurance. Regulatory guide 1.176.* Technical report, US Nuclear Regulatory Commission.

USNRC (1998b). *An approach for plant-specific, risk-informed decision-making: Inservice inspection of piping, Regulatory guide 1.178.* Technical report, US Nuclear Regulatory Commission.

USNRC (1998c). *An approach for plant-specific, risk-informed decision-making: Inservice testing. Regulatory guide 1.175.* Technical report, US Nuclear Regulatory Commission.

USNRC (1998d). *An approach for plant-specific, risk-informed decision-making: Technical specifications, Regulatory guide 1.177.* Technical report, US Nuclear Regulatory Commission.

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. 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. 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. 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.

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 Pedroni, N. (2012). *Uncertainty characterization in risk analysis for decision-making practice.* Cahier de la Sécurité Industrielle 2012-07, Fondation pour une culture de sécurité industrielle. www.foncsi.org/, DOI: 10.57071/155chr.

You can save these bibliographic entries in BibTeX format by clicking on the paper clip icon to the left.

Reproducing this document

FONCSI
Fondation pour une culture de sécurité industrielle

Foundation for an Industrial Safety Culture
a public interest research foundation

www.FonCSI.org

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

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