# INTERNATIONAL STANDARD

# ISO 11231

First edition
2010-08-01

## Space systems — Probabilistic risk assessment (PRA)

*Systèmes spatiaux — Évaluation du risque probabiliste (PRA)*



Reference number
ISO 11231:2010(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

# Contents

Page





## Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 11231 was prepared by Technical Committee ISO/TC 20, *Aircraft and space vehicles*, Subcommittee SC 14, *Space systems and operations*.

## Introduction

Structured risk management processes use qualitative and quantitative risk assessment techniques to support optimal decisions regarding safety and the likelihood of mission success, as provided for in ISO 17666. The most systematic and comprehensive methodology for conducting these evaluations is probabilistic risk assessment (PRA).

Probabilistic risk assessment has, over the past three decades, become the principal analytic method for identifying and analysing risk from project and complex systems. Its utility for risk management (RM) has been proven in many industries, including aerospace, electricity generation, petrochemical and defence. PRA is a methodology used to identify and evaluate risk, in order to facilitate RM activities by identifying dominant contributors to risk, so that resources can be effectively allocated to address significant risk drivers and not wasted on items that contribute insignificantly to the risk. In addition to analysing risk, PRA provides a framework to quantify uncertainties in events and event sequences that are important to system safety. By enabling the quantification of uncertainty, PRA informs decision makers on the sources of uncertainty and provides information on the worth of investment resources in reducing uncertainty. In this way, PRA supplements traditional safety analyses that support safety-related decisions. Through the use of PRA, safety analyses are capable of focussing on both the likelihood and severity of events and consequences that adversely impact safety.

PRA differs from reliability analysis in two important respects:

a) PRA allows a more precise quantification of uncertainty both for individual events and for the overall system;

b) PRA applies more informative evaluations that quantify metrics related to the occurrence of highly adverse consequences (e.g. fatalities, loss of mission), as opposed to narrowly defined system performance metrics (e.g. mean-time-to-failure).

PRA also differs from hazard analysis, which identifies and evaluates metrics related to the effects of high-consequence and low-probability events, treating them as if they had happened, i.e. without regard to their likelihood of occurrence. In addition, the completeness of the set of accident scenarios cannot be assured in the conduct of a hazard analysis. PRA results are more diverse and directly applicable to resource allocation and other RM decision-making based on a broader spectrum of consequence metrics.

Through the PRA process, weaknesses and vulnerabilities of the system that can adversely impact safety, performance and mission success are identified. These results in turn provide insights into viable RM strategies to reduce risk and direct the decision maker to areas where expenditure of resources to improve design and operation might be more effective.

The most useful applications of PRA have been in the risk evaluation of complex systems that can result in low-probability and high-consequence scenarios, or the evaluation of complex scenarios consisting of chains of events that collectively may adversely impact system safety more than individually.

# Space systems — Probabilistic risk assessment (PRA)

## 1 Scope

This International Standard supports and complements the implementation of the risk management process defined in ISO 17666 in situations when application of quantitative risk assessment is deemed necessary.

This International Standard defines the principles, process, implementation and requirements for conducting a quantitative risk assessment, and explains the details of probabilistic risk assessment (PRA) as applied to safety. While PRA can be applied to project risk management involving cost and schedule, this application is outside the scope of this International Standard.

This International Standard provides the basic requirements and procedures for use of PRA techniques to assess safety or mission risk and success in space programmes and projects. This International Standard is applicable to all international space projects involving:

- the design of space vehicles for the transportation of personnel in space;
- the design of space and non-terrestrial planetary stations inhabited by human beings;
- the design of space and launch vehicles powered by, or carrying, nuclear materials;
- other projects as directed by authorities or clients.

These types of projects generally involve scenarios, chains of events or activities that could result in the death of, or serious injury to, members of the public, astronauts or pilots, or the workforce, or the loss of critical or high-value equipment and property. For other types of projects, it is intended that PRA be performed at the discretion of the project management.



## 2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 17666, *Space systems — Risk management*

## 3 Terms, definitions and abbreviated terms

### 3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 17666 and the following apply.

**3.1.1**
**acceptable risk**
safety risk, the severity and the probability of which may be reasonably accepted by humanity, without durable or irreversible foreseeable consequences on health, Earth, and the environment, at the present time and in the future

[ISO 14620-2:2000, definition 3.1]

**3.1.2**
**expert judgment**
systematic and structured elicitation of likelihood data through estimation and assessment by specialists

NOTE 1 "Structured" implies the use of a method; "systematic" means regularly.

NOTE 2 Mathematical aggregation of individual judgments is generally preferred over behavioural or consensus aggregation.

**3.1.3**
**likelihood**
probability of occurrence or measure for the occurrence rate or frequency of an event, a hazard scenario or consequence

**3.1.4**
**likelihood reference frame**
relative indicator against which the likelihood is expressed

NOTE The likelihood reference frame is linked to the structure of the analysis. A typical reference frame in use in space projects is "per mission".

**3.1.5**
**risk**
quantitative or qualitative measure for the severity of a potential damage and the probability of incurring that damage

[ISO 14620-2:2000, definition 3.27]

NOTE Risks arise from uncertainty due to a lack of predictability or control of events. Risks are inherent to any project and can arise at any time during the project life cycle; reducing these uncertainties reduces the risk.

**3.1.6**
**risk contributor**
single event or particular set of events upon which the risk depends

NOTE Risk contributors can be ranked relative to each other by their **risk contribution** (3.1.7).

**3.1.7**
**risk contribution**
measure of the decrease of the likelihood of a top consequence, when the events associated with the corresponding risk contributor are assumed not to occur

NOTE 1 Risk contribution indicates (and is directly proportional to) the "risk reduction potential" of the risk contributor. Important risk contributors are events, which have a high-risk contribution and risk reduction potential.

NOTE 2 Risk contribution provides a systematic measure that makes it possible to rank design and operation constituents of a system from a safety risk point of view. It allows the identification of high risk or vulnerable areas in the system, which can then serve as drivers for safety improvements.

**3.1.8**
**safety risk**
measure of the potential consequences of a hazard (e.g. expected number of casualties) considering the probability of the associated mishap, the harm caused to people, and the damage caused to public and private property and the environment

[ISO 14620-2:2000, definition 3.30]

NOTE 1 Safety risk is always associated with a specific hazard scenario or a particular set of scenarios. The risk posed by a single scenario is called "individual scenario risk". The risk posed by the combination of individual risks and their impact on each other is called "overall risk".

NOTE 2 The magnitude of safety risk is represented by the severity and the likelihood of the consequence.



**3.1.9**
**(risk) scenario**
sequence or combination of events leading from the initial cause to the unwanted consequence

[ISO 17666:2003, definition 2.1.13]

NOTE The cause can be a single event or something activating a dormant problem.

**3.1.10**
**stakeholder**
individual or organization that stands to gain or to lose as a result of risk consequences

**3.1.11**
**uncertainty**
lack of certitude resulting from inaccuracies of input parameters, analysis process, or both

[ECSS-P-001B:2004, definition 3.216]

NOTE Uncertainty can be represented as an interval with an upper and lower value or as an uncertainty distribution.

**3.1.12**
**uncertainty contributor**
single event or particular set of events upon which the uncertainty of the top consequence depends

NOTE Uncertainty contributors can be ranked relative to each other by their **uncertainty contribution** (3.1.13).

**3.1.13**
**uncertainty contribution**
measure of the decrease of the uncertainty of a top consequence, when the likelihoods of the events associated with the corresponding uncertainty contributor are assumed to be without uncertainty

NOTE 1 Uncertainty contribution indicates (and is directly proportional to) the "uncertainty reduction potential" of the uncertainty contributor. Important uncertainty contributors are events, which have a high uncertainty contribution and uncertainty reduction potential.

NOTE 2 Uncertainty contribution provides a systematic measure that makes it possible to rank data and information sources.

## 3.2 Abbreviated terms

| | |
|---|---|
| FMEA | Failure Modes and Effects Analysis |
| IE | Initiating Event |
| MLD | Master Logic Diagrams |
| PRA | Probabilistic Risk Assessment |
| P(A) | probability of event A |
| P(A/B) | conditional probability of event A given event B has occurred |
| RM | Risk Management |

# 4 Principles of probabilistic risk assessment

## 4.1 General

Probabilistic risk assessment assists engineers and managers in including risk results in management and engineering practices and in the decision-making process throughout a project life cycle, for such aspects as design, construction, testing, operation, maintenance and disposal, together with their interfaces, management, cost and schedule (see ISO 17666).

Probabilistic risk assessment supports and interfaces with the risk management process by providing the required relevant risk data. Risk assessment is an important task within the risk management process.

The steps in the risk management process, as described in ISO 17666, are as follows:

— step 1: define risk management implementation requirements;

— step 2: identify and assess the risks;

— step 3: decide and act;

— step 4: monitor, communicate and accept risks;

— step 5: control of residual risks.

Step 2 constitutes a process and is also referred to as "risk assessment". Once step 1 is completed, risk assessment provides the information used to conduct the remainder of the risk management process. Risk assessment provides the data upon which to base decisions concerning the design and implementation of controls used to prevent or mitigate risks.

Step 3 includes the opportunity to decide whether the assessed risk is acceptable to programme/project management and the stakeholders. If the risk is unacceptable, measures shall be taken to bring it down to an acceptable level. If it is acceptable, management measures shall be taken (steps 4 and 5) to monitor the evolution of risk and to ensure that it will not grow to unacceptable levels.

Risk assessment can be performed qualitatively or quantitatively or both. Qualitative risk assessment is performed by categorizing the likelihoods and consequences of risk as discussed below, where it applies to safety problems. In this context, it is called safety risk assessment.

In many cases, likelihoods and consequences need to be evaluated quantitatively. If sufficient statistical data do not exist for this purpose, modelling techniques are used.

For rare (very low probability) events, where sufficient statistical data do not exist, the significance of important risk drivers is assessed through probabilistic risk assessment. See Clause 6 for PRA requirements and process.

In the rest of this International Standard, PRA methodology primarily intended for safety applications is discussed. Another form of risk assessment, called "programmatic risk assessment", is used to assess the risks of not performing within pre-defined programme schedule and cost estimates. In this process, schedule profiles based on uncertainties in the originally defined schedule are modelled using simulation or Monte Carlo methods. These uncertainties can occur due to a number of technical or management reasons. Subsequently, the effects of schedule changes and of other technical or management impacts on cost are evaluated. Programmatic risk is then evaluated in the form of distributions of probabilities of exceeding given schedule milestones and costs.



### 4.2 Safety risk assessment concept

The application of PRA to safety problems is discussed here. The safety risk assessment concept is derived from PRA. Safety risk assessment complements deterministic hazard analysis by adding a probabilistic dimension to the evaluation of hazards in support risk informed decision-making. The probabilistic dimension is expressed in terms of likelihoods.

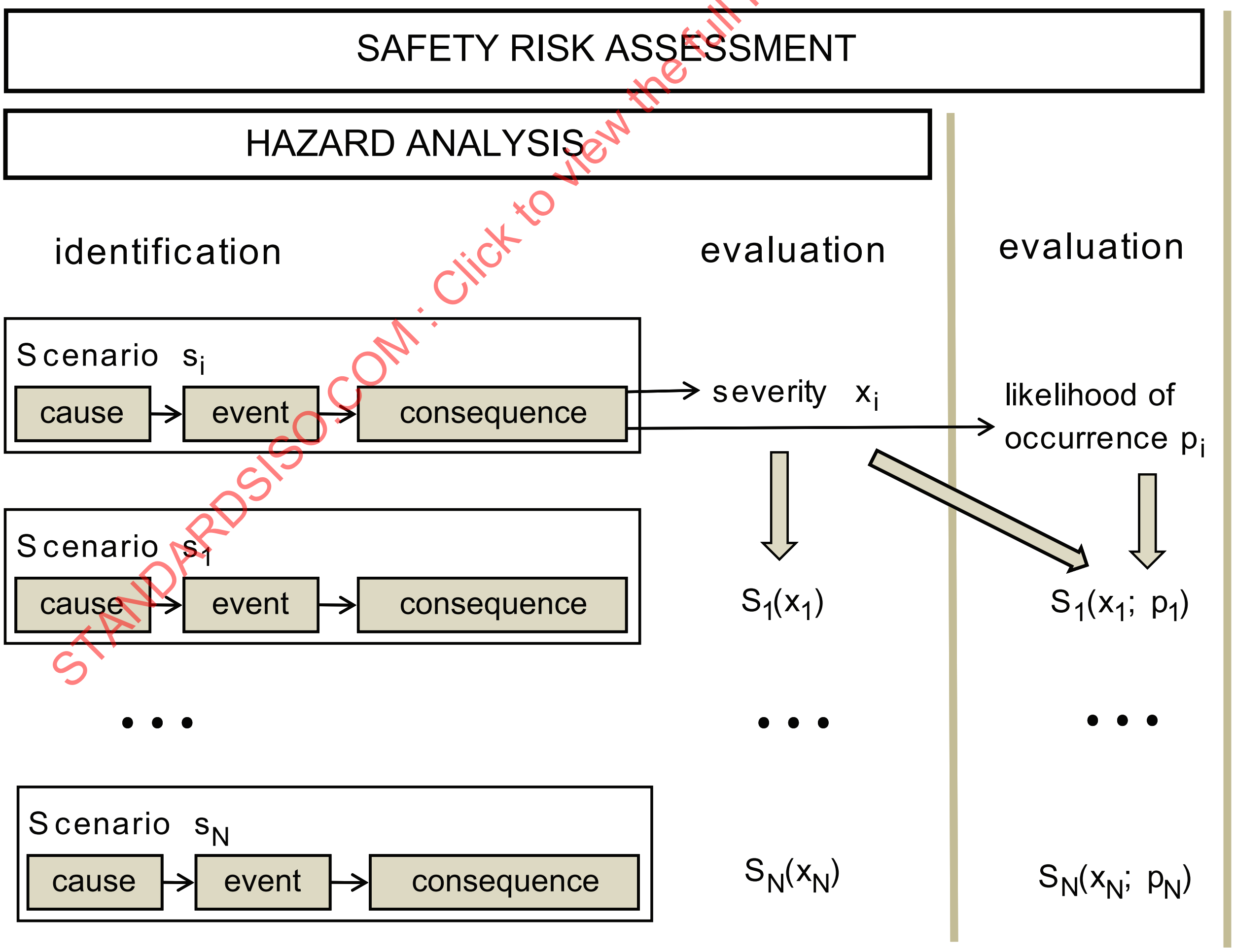
The interface between safety risk assessment and hazard analysis is shown in Figure 1.

Safety risk assessment can be used to either assess the risks posed by individual hazard scenarios separately, or assess sets of scenarios collectively, in the form of the overall risk posed by those scenarios.

The assessment of individual scenarios can be performed using consequence severity and scenario likelihood categorization schemes by applying risk grids or risk matrices and risk indexes, as described in ISO 17666. However, these risk matrix and index methods cannot be used to combine individual components of risk within a scenario, or to combine scenarios to evaluate overall risk. These methods do not constitute combinatorial computational tools.

Assessment of the overall risk posed by a particular set of scenarios requires the rigor of the PRA approach. This assessment provides the basis for identifying and ranking risk contributors. Important contributors can then be used for driving and optimizing the system design or operation from a safety performance point of view. The calculated overall risk can also be compared to probabilistic safety targets or acceptance criteria. Acceptable risks are defined by authorities or clients in step 1 of the risk management process. Risk can also be used as a metric for quantifying safety in decision models.






NOTE $S_i$ = Scenario i; $S_1$ = Scenario 1; $S_N$ = Scenario N: with severity = $x_i$ and likelihood = $p_i$: Therefore $S_1(x_1)$ = the severity of Scenario 1 and $S_1(x_1;p_1)$ = risk of Scenario 1; and $S_N(x_N)$ = the severity of Scenario N and $S_N(x_N;p_N)$ = risk of Scenario N.

**Figure 1 — Interface between safety risk assessment and hazard analysis**

A representation of the assessment of overall safety risk is shown in Figure 2. As indicated in the figure, safety risk assessment uses hazard scenarios to model individual sequences of events that are necessary and sufficient for an undesired system level consequence to occur. A scenario can be represented as a “logical intersection” of the initial cause or initiating event and the necessary conditional intermediate events leading to the associated consequence. The overall risk is then the logical union of the risk of the individual scenarios that lead to same consequence.

Probabilistic risk assessments of complex systems identify scenarios typically using event trees, or event sequence diagrams and fault trees, to derive the logical models that lead to particular undesired safety consequences of interest. As described above, in order to quantify scenarios, the likelihood of the initiating events (i.e. causes) and the probability of each subsequent intermediate event, conditional on the occurrence of the previous events in the sequence, are combined to determine the probability that the end state (i.e. consequences) will occur. For each scenario, the severity (i.e. magnitude) of the consequences is usually determined based on the physical characteristics and nature of the scenario being evaluated. The overall consequences are determined by summing overall scenarios in a process that is analogous to that used to determine the overall probability.

An estimation of event likelihoods is usually based on different sources of data. Typical data sources include previous experience with the particular system [i.e. measured or directly observed relevant test or experience data and lessons learned (see ISO 16192)], data from other systems or projects (i.e. extrapolation from generic data, similarity data, or physical models) and expert judgment (i.e. direct estimation of likelihoods by domain specialists). Events are quantified in the context of the corresponding hazard scenario, i.e. the likelihood of an event is assessed conditionally on the previous events in the sequence.

Systematic identification and treatment of uncertainties is characteristic of the assessment of the overall risk and conducted in two ways. The likelihood estimates of scenario events are produced with their associated uncertainties and presented in the form of probability distributions or intervals. These uncertainties are then propagated in the calculations of the likelihoods of the consequence(s).

Quantification of the overall risk is obtained by calculating the likelihoods and magnitudes of the consequences. This calculation can be achieved through the use of point values or probability (uncertainty) distributions. An uncertainty distribution is characterized by representative point values, e.g. the mean or a specific quintile value in the upper part of the distribution. A representative point value in the upper part of the uncertainty distribution associated with the overall risk, at a confidence level accepted by the decision maker, tends to be used to implement the precautionary principle for risk acceptance decisions and for risk comparisons. The precautionary principle implies that conservative assumptions with respect to the risk value are preferred to optimistic ones, in order to ensure that a system is not considered to satisfy an agreed risk target or an acceptance criterion falsely, or that one option is not falsely preferred to another one in the comparisons. Higher uncertainty regarding the overall risk value transfers a higher representative point value to be used for risk acceptance or comparisons.

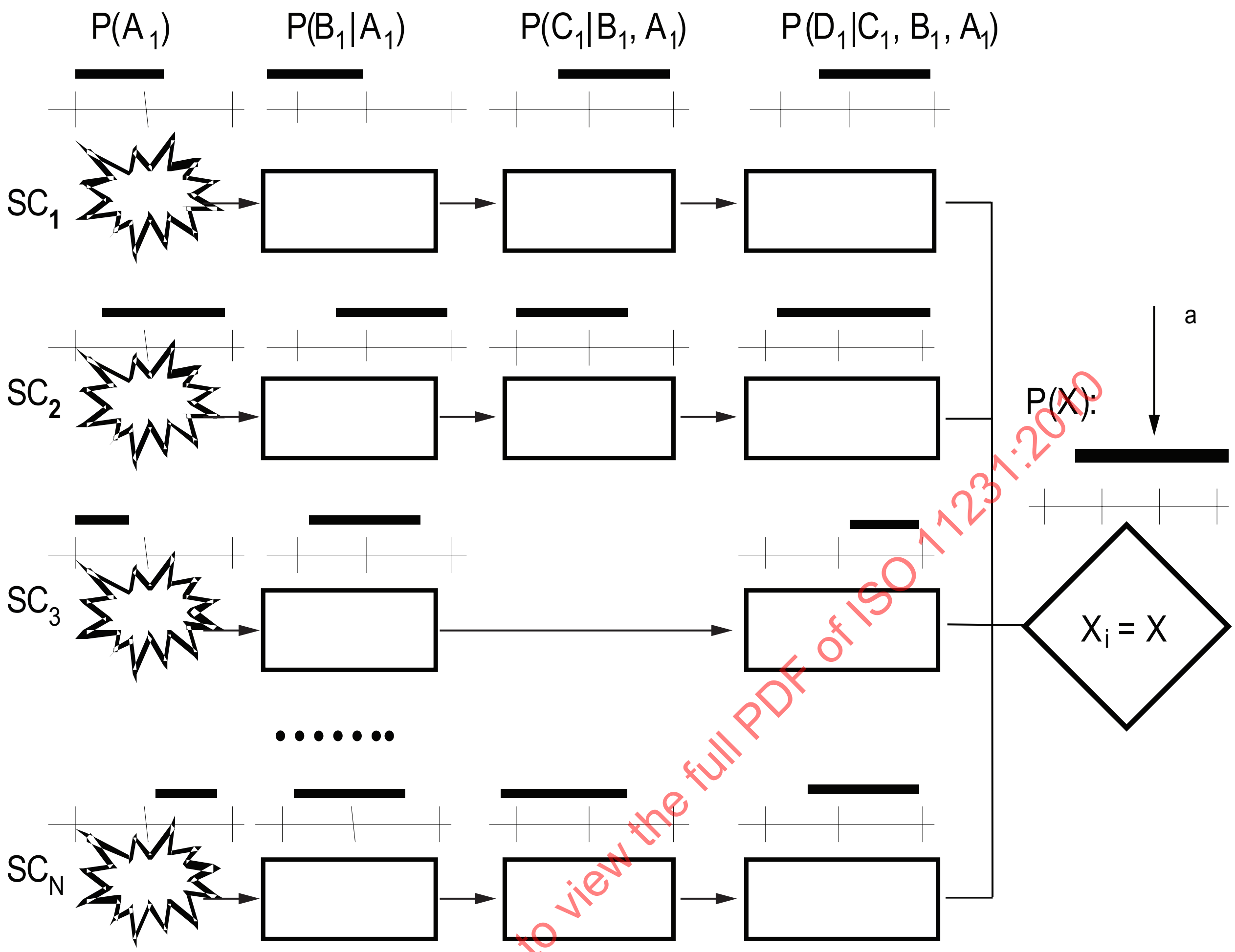
The relative importance of an event or a scenario to the overall risk is measured by its risk contribution. The risk contribution provides information on the potential for safety improvement, i.e. potential for reducing the overall risk associated with the event or scenario. Similar to individual events, design and operation constituents can also be ranked from a risk reduction point of view by accumulating the risk contributions of the events associated with the particular constituents.

The relative importance of the uncertainty of an event or a scenario to the uncertainty of the overall risk is measured by its uncertainty contribution. Uncertainty contribution values indicate and rank those events, which are the main sources of uncertainty for the consequence likelihood and have the highest potential for reducing this uncertainty. Reduction of consequence uncertainties directly transfers to the use of lower representative point values of the consequence likelihoods.

Risk and uncertainty contributors are identified based on their ranking. Important risk and uncertainty contributors are those events, or their corresponding system constituents, that have high-risk reduction and uncertainty reduction potential.






a "Representative point value".

NOTE $SC_1$ = scenario 1, $SC_2$ = scenario 2, $SC_3$ = scenario 3, $SC_N$ = scenario N; $P(A_1)$ = probability of $A_1$, the initiating event; $P(B_1 | A_1)$ = conditional probability of $B_1$ given $A_1$; $P(C_1 | B_1, A_1)$ = conditional probability of $C_1$ given $B_1$ and $A_1$; $P(D_1 | C_1, B_1, A_1)$ = conditional probability of $D_1$ given $C_1$, $B_1$ and $A_1$; P(x) = total probability, the logical sum of the probability of all scenarios 1 to N

**Figure 2 — Example of the assessment of the overall risk**



## 4.3 Concept of risk and probabilistic risk assessment

The concept of risk includes both undesirable consequences, e.g. the number of people harmed, and the probability of occurrence of the consequences. Sometimes risk is defined as the expected value of consequence occurrence. This representation of risk results in a summary measure and not a general definition. Understanding how the system fails and producing probability distributions for the consequences affords a much more complete description of risk.

A common definition of risk is represented by a set of triplets. Determining risk generally amounts to answering the questions below.

a) What can go wrong? (the scenario)

b) How likely is it? (likelihood)

c) What are the consequences? (severity of the consequences)

The answer to the first question is a set of accident scenarios. The answer to the second question requires evaluating the probabilities that the scenarios will occur, and the answer to the third question requires estimating associated consequences. In addition to probabilities and consequences, the triplet definition emphasizes the development of accident scenarios and makes them part of the definition of risk. These scenarios are indeed one of the most important results of a risk assessment. Figure 3 illustrates the implementation of these concepts in PRA.

The PRA process begins by identifying a set of "initiating events" (IEs) that perturb the system, i.e. adverse triggers that cause it to change its operating state or configuration. For each IE, the analysis proceeds by determining the subsequent events (failures) that can lead to undesirable consequences. The magnitudes of the consequences of these scenarios are then determined, as well as their occurrence frequencies (probabilities). Finally, frequencies and consequences are integrated into a representation of the risk profile of the system. This risk profile is then used to support risk management decisions.

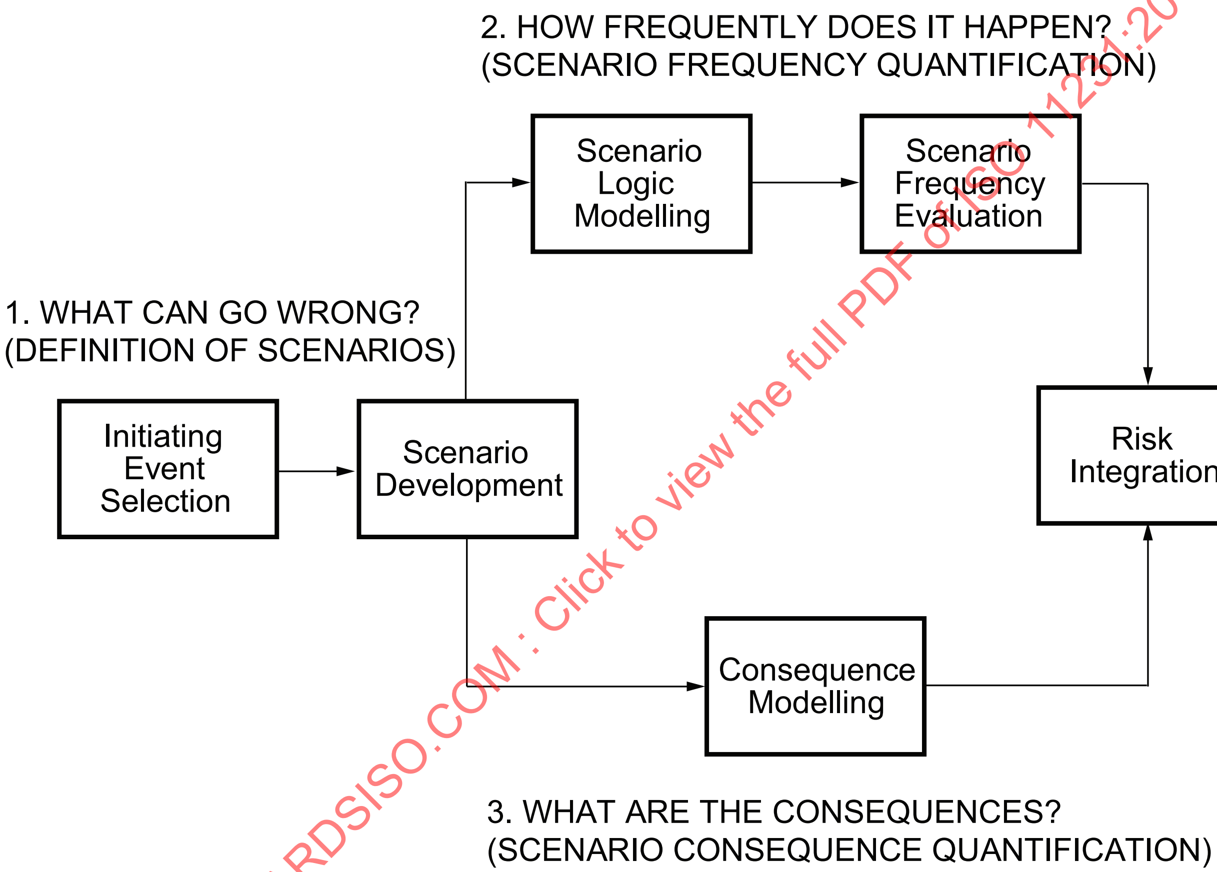





**Figure 3 — Implementation of the Triplet Definition of Risk in PRA**

## 5 Objectives, uses, and benefits of probabilistic risk assessment

**5.1** The objectives of a probabilistic risk assessment are the following:

— to identify and assess the (safety or mission) risks posed by individual identified scenarios, or to identify and assess the overall risk posed by sets of scenarios collectively;

— to identify risk and uncertainty contributors, as well as corresponding risk areas in system design and operation;

— to rank risk and uncertainty contributors in a decreasing order of importance;

— to identify and prioritise options for risk reduction.

**5.2** Probabilistic risk assessment results are used for the following:

- to assess the level of safety or mission risk and success in a quantitative (probabilistic) manner;
- to decrease the level mission risk and increase the level of safety or mission success of a system through risk reduction;
- to drive the definition and implementation of design and operational requirements, specifications, concepts, procedures, etc.;
- to provide a quantitative basis for defining safety and mission requirements by:
  - determining the applicability of safety and mission requirements,
  - implementing safety and mission requirements;
- to verify PRA results implementation and to demonstrate compliance or non-compliance;
- to support safety and mission-related project decisions;
- to support safety submissions and reviews through documented evidence;
- to support safety certification of a system through documented evidence;
- to support risk communication and tracking;
- to provide input to overall project risk management.

**5.3** The benefits of a probabilistic risk assessment are the following:

- to provide a quantitative framework for assessing risks and determining which are acceptable and which are not;
- to apportion safety responsibilities among teams more realistically;
- to allocate safety improvement expenditures in proportion with the impact of these improvements on risk reduction;
- to build safety into the system in an efficient and consistent way;
- to display quantitatively the significance of accident scenarios;
- to identify quantitatively system and component weaknesses;
- to assess phase related system or subsystem safety levels;
- to compare quantitatively the efficiency of risk reduction actions.

**5.4** The specific objectives of risk assessment with respect to a project specific application are determined under task 1 of the risk assessment process.

# 6 PRA requirements and process

## 6.1 Probabilistic risk assessment requirements

The following probabilistic risk assessment requirements are defined:

a) probabilistic risk assessment shall follow the process as defined in 6.3;

b) probabilistic risk assessment shall be documented in accordance with the requirements of Clause 8.

## 6.2 Overview of the probabilistic risk assessment process

The tasks of a probabilistic risk assessment described in 6.3 are used to address step 2 of the risk management process, as outlined in 4.1 and illustrated in Figure 4.

## 6.3 Probabilistic risk assessment tasks

### 6.3.1 General

The PRA task flow is shown in Figure 4. A brief description of each task is provided in 6.3.2 to 6.3.11.

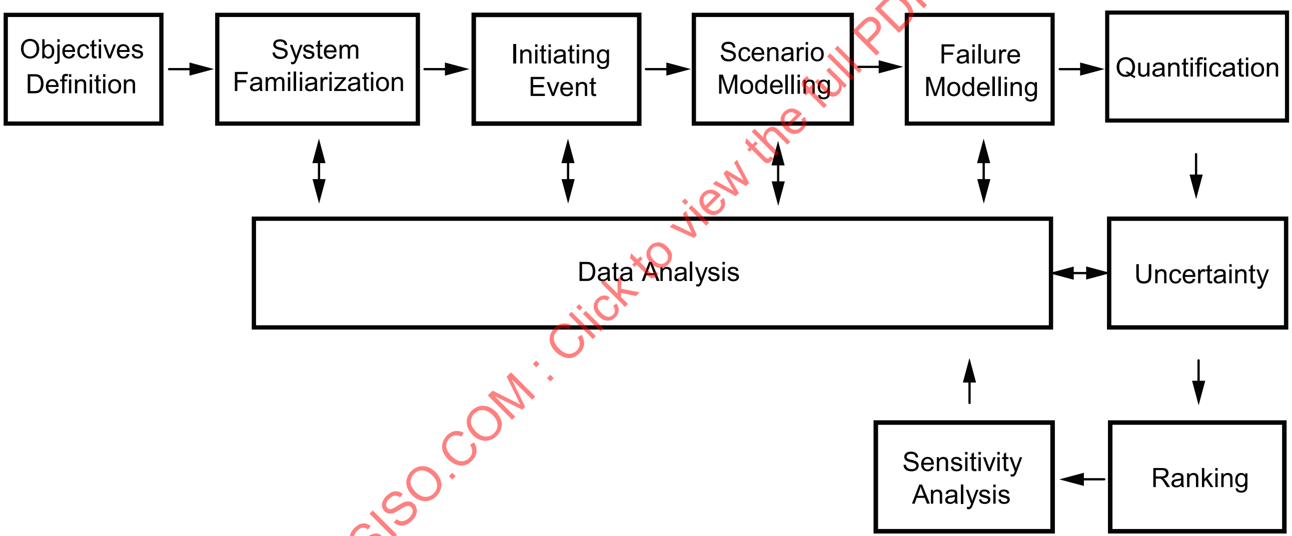



**Figure 4 — Task flow in a typical PRA**

### 6.3.2 Task 1: Objectives definition

The initial task of a PRA is to define the objectives and scope of the analysis. The objectives of the risk assessment provide clear statements of the purpose and expected end uses for the results. The scope defines the mission profile and system(s) or portion thereof that will be included in the analysis. These two elements provide the basis for identifying and selecting the consequence(s) metrics of interest. These consequence metrics can include harm to humans (e.g. injury, illness or death), degradation of mission capabilities, loss of mission, property damage and losses or other undesired outcomes.

Depending on the objectives and scope of the PRA, applicable system configurations and time frame, guidelines for considering initiating events should be defined, i.e. whether to include external events such as micrometeoroids. The results of task 1 should be completely reviewed by the appropriate project management and responsible safety and mission assurance organizations prior to commencing with the assessment.

The activities below are included in task 1.

a) Identify the objectives of the probabilistic risk assessment, by defining the intended purpose and use(s) of the analytical results.

b) Identify the scope and depth of the analysis, by defining the mission envelope, applicable systems boundaries (which part of systems design and operations will be analysed) and the level of detail for accident scenarios and the associated analyses.

c) Identify the consequence metric(s) for the analysis, including the consequence types and whether risks are required for individual hazard scenarios, or overall risks of specific undesired consequence types, or both (i.e. loss of mission, loss of vehicle, loss of crew):

   1) identify the risk grid, index scheme or risk matrix to be used (based on consequence severity and scenario likelihood categories), and

   2) identify specified overall risk targets or acceptance criteria (based on probabilistic targets and criterion for a specific consequence).

d) Identify associated information and data sources.



### 6.3.3 Task 2: System familiarization

Familiarization with the system under analysis is the next step. Familiarization covers all relevant design and operational information, including engineering and process drawings, as well as operating and emergency procedures. If the PRA is being performed on an existing system that has been operated for some time, the engineering information shall be on an as-built or as-operated basis. If the PRA is being conducted during design, the engineering information needed for the assessment is based on the as-designed configuration with considerations for system operations. Examination and, if possible, visual inspection of the system(s) being analysed, are recommended. The purpose of this effort is to become thoroughly familiar with the mission and systems involved and to gain an understanding of the success states and success criteria needed for proper overall mission completion. System familiarization identifies how the systems operate, their interdependencies, the role of the human in operations (command and control, maintenance) and any system configuration changes that may occur during applicable mission stages, phases or regimes. Mission and system success criteria provide the basis for developing functional and systemic models.

The activities below are included in task 2.

a) Identify and describe the analytical scope, systems configuration and operation (functional and physical architecture and layout vis-à-vis the mission timeline), including mission phases and operating configurations, system constituents and functions, and physical zones, etc.

b) Define the mission success criteria along with contributions from and the success criteria of each system required for completion of the mission.

### 6.3.4 Task 3: Initiating event identification

Next, a complete set of initiating events that triggers subsequent accident scenarios shall be identified and analysed. These events initiate accident sequences leading to defined end states (consequence metrics). There are several ways to identify initiating events. If the PRA is being performed on an existing system that has been operated for some time, a review of past experiences, incidences and operating history can help identify initiating events. If the analysis is being conducted on new designs, past experience of similar systems in similar environments or with similar mission envelopes can be used. Along with experience data, systematic methods, e.g. Master Logic Diagrams (MLD) and Failure Modes and Effects Analysis (FMEA), are recommended for identifying initiating events. An MLD is a hierarchical, top-down tree display, showing general types of undesired events at the top, proceeding to increasingly detailed event descriptions at lower tiers and displaying postulated initiating events at the bottom. An FMEA systematically assumes component failures and evaluates their effects on system performance.

When multiple initiating events leading to scenarios with the same end state are identified, those events having very low probabilities can be screened out. Independent initiating events can be grouped according to the similarity of challenges they pose to the system, i.e. initiated events that result in the same system response. When initiating events are treated as a group, their frequencies can be summed to derive the group initiator frequency.

The activities below are included in task 3.

a) Identify and evaluate initiating events that can trigger subsequence accident scenarios using experience data and systematic methods (use relevant input from existing hazard analysis produced in accordance with MLDs and FMEAs).

b) Evaluate the occurrence probabilities of the identified initiating events and screen out those events with very low relative probabilities (or frequencies).

c) Combine initiating events with similar effect on the system into groups and determine group occurrence probabilities (frequencies).

### 6.3.5 Task 4: Scenario modelling

Modelling of accident scenario is an inductive process that usually involves tools called event trees. An event tree starts with the initiating event and progresses through the scenario, a series of successes or failures of intermediate events (also called pivotal events or top events), until end states are reached. Event trees generally take into account the time sequence of pivotal or top events that represent the functional or systemic behaviour of the overall system. Sometimes a graphical tool called an event sequence diagram (ESD) is used to describe an accident scenario, because this type of diagram lends itself better to engineering thinking than does an event tree. An ESD is logically equivalent to an event tree and shall then be converted to an event tree for quantification. Another type of inductive modelling tool that can also be employed is a reliability block diagram.



The activities below are included in task 4.

a) For each initiating event (or combined group of events), model the approximate time sequence and conditional response (success or failure) of the pivotal events (i.e. human actions, structure, systems, components) needed to prevent the initiating event from causing potential consequences.

b) For those accident sequences that are postulated to lead to potential consequences, evaluate the conditional physical (mechanistic) response of the system to the physical impacts of the initiating events as modified by identified preventative controls (i.e. human actions, structures, systems, components) and determine the magnitude and characteristics of the ensuing physical response (i.e. detonation, deflagration, loss of control, loss of oxygen, etc.).

c) For those physical system responses that can lead to potential consequences, model the conditional response (success or failure) of the controls (i.e. human actions, structures, systems, components) available or designed to mitigate the potential consequences that can be caused by the physical system responses.

### 6.3.6 Task 5: Failure modelling

The modelling of failure causes and faults (or their complements, successes) of each pivotal or event tree top event is a deductive process. There are several deductive modelling tools that can be employed to evaluate the failure of top events such as Markov chains, reliability block diagrams, and fault trees, among others. Fault tree analysis is the most common method. A fault tree consists of three parts. The top part is the top event, which corresponds to the failure of a pivotal event (or event tree top event) in the accident scenario. The middle part consists of intermediate events (faults) that, in combination, cause failure of the event immediately above it. These events are linked through logic gates (e.g. AND gates and OR gates) to the events both above and to events at the bottom part of the fault tree, called the basic events. There can be many layers of intermediate events to describe the failure of the pivotal (or top event). The occurrence of the basic events will ultimately lead to the occurrence of the top events through the logic of the fault tree. The fault trees are then linked to the accident scenarios and simplified (using Boolean reduction rules) to support quantification.

The activities below are included in task 5.

a) For each pivotal or event tree top event, identify and record the associated initiating event and previous events in the accident scenario. These events provide the initial and boundary conditions needed to evaluate their failure (or their complements, successes). In addition, record the success criteria (defined in task 2) for the functioning of the pivotal or top events that are also needed for the evaluation.

b) For each pivotal or event tree top event, develop the failure (i.e. fault tree) model, the logical combination of intermediate faults that can cause the top event. Dependent on the function or system being modelled, there may be several layers of intermediate events.

c) Identify the basic events (failures or faults), along with their success criteria, for the initial and boundary conditions associated with the top event.

d) Link the fault tree models for the pivotal or event tree top events to the associated portion of the event tree model.

### 6.3.7 Task 6: Quantification

Quantification refers to the process of estimating the frequency of occurrence and the magnitude of the consequences of the undesired end states for the accident scenarios. The frequency of occurrence of each end state is calculated using the fault tree linking approach, resulting in the logical product of the initiating event frequency and the (conditional) probabilities of each pivotal event along the event sequence path from the initiating event to the end state. The failure models [fault tree(s)] for the pivotal events provide the logical combinations of basic events needed for the quantification of the pivotal events (through the linking process). The magnitudes of the undesired end states (consequences) for the accident sequences are usually evaluated through deterministic calculations taking into account the physical response of the system being evaluated and the functioning of the systems identified or designed to mitigate the consequences. All sequences with like end states are then grouped, i.e. their probabilities are logically summed into the probability of the representative end state.

The activities below are included in task 6.

a) Perform the Boolean evaluation of the linked event sequence [event tree(s)] and failure models [fault tree(s)] for each initiating event. This evaluation will result in sets of basic events (called minimal cut sets) leading to the undesired end states. These minimal cut sets represent the accident sequences in terms of the basic events.

b) Estimate the frequency of occurrence of each minimal cut set by logically combining the initiating event frequency with the failure probabilities for the associated basic events. Typical data sources for the failure probabilities include previous experience with the particular system (i.e. measured or directly observed relevant test or experience data and lessons learned), data from other systems or projects (i.e. extrapolation from generic data bases, similarity data or physical models) and expert judgment (i.e. direct estimation of likelihoods by domain specialists).

c) Estimate the type and magnitude of the consequences.

d) Group the sequences with the same end state and logically sum their probabilities to estimate an overall probability that each representative end state will occur.

### 6.3.8 Task 7: Uncertainty analysis

One purpose of a PRA is to develop realistic models that take into account the uncertainty in events. Therefore, the probabilistic risk model is effectively an uncertainty analysis model. Recognizing that uncertainty analysis is a main constituent of the probabilistic risk model and assessment provides the foundation to the proper application of the PRA results in the RM decision-making process. It is incumbent on

