INTERNATIONAL STANDARD

ISO 11231

Second edition
2019-05

Space systems — Probabilistic risk assessment (PRA)

Systèmes spatiaux — Évaluation du risque probabiliste (PRA)

Reference number
ISO 11231:2019(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: 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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

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

This second edition cancels and replaces the first edition (ISO 11231:2010), which has been technically revised.

The main changes compared to the previous edition are as follows:

— updated definitions of terms;

— simplification of Clause 4;

— updated figures and tables;

— addition of capability-based safety, reliability and quality assurance.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

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

PRA has, over the past three decades, become the principal analytic method for identifying and analysing risk from projects 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 are 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 focusing on both the probability 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 analyses, 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 probability 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 document supports and complements the implementation of the risk management process defined in ISO 17666 in situations when the application of a quantitative risk assessment is deemed necessary.

This document 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 document.

This document provides the basic requirements and procedures for the use of PRA techniques to assess safety or mission risk and success in space programmes and projects. This document 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 the 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 documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 purpose of this document, the terms and definitions given in ISO 17666 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1.1
acceptable risk
safety risk, the severity, and the *probability* (3.1.3) 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

[SOURCE: ISO 14620-2:2011, 3.1, modified — The EXAMPLE has been removed]

3.1.2
expert judgment
systematic and structured elicitation of probability data through the estimation and assessment by specialists

Note 1 to entry: "Structured" implies the use of a method; "systematic" means regularly.

Note 2 to entry: Mathematical aggregation of individual judgments is generally preferred over behavioural or consensus aggregation.

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

3.1.4
probability reference frame
relative indicator against which the *probability* (3.1.3) is expressed

Note 1 to entry: The probability 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
undesirable situation or circumstance that has both a likelihood of occurring and a potentially negative consequence on a project

Note 1 to entry: 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.

[SOURCE: ISO 17666:2016, 3.1.12]

3.1.6
risk contribution
measure of the decrease of the *probability* (3.1.3) of a top consequence, when the events associated with the corresponding risk contributor are assumed not to occur

Note 1 to entry: 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 to entry: 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.

3.1.7
risk contributor
single event or particular set of events upon which the risk depends

Note 1 to entry: Risk contributors can be ranked relative to each other by their *risk contribution* (3.1.7).

3.1.8
risk management
systematic and iterative optimisation of the project resources, performed according to the established project risk management policy

[SOURCE: ISO 17666:2016, 3.1.5]

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

Note 1 to entry: The cause can be a single event or something activating a dormant problem.

[SOURCE: ISO 17666:2016, 3.1.13]

3.1.10
safety risk
measure of the potential consequences of a hazard considering the *probability* (3.1.3) of the associated mishap, the harm caused to people, and the damage caused to public and private property and the environment

EXAMPLE Expected number of casualties.

Note 1 to entry: 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 to entry: The magnitude of safety risk is represented by the severity and the *probability* (3.1.3) of the consequence.

[SOURCE: ISO 14620-2:2011, 3.30, modified — NOTE 1 and 2 have been removed; new Note 1 and 2 to entry have been added; EXAMPLE has been added]

3.1.11
interested party
stakeholder
person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity

EXAMPLE Customers, owners, people in an organization, providers, bankers, regulators, unions, partners or society that can include competitors or opposing pressure groups.

[SOURCE: ISO 9000:2015, 3.2.3, modified — Note 1 to entry has been removed]

3.1.12
uncertainty
lack of certitude resulting from inaccuracies of input parameters, analysis process or both

Note 1 to entry: Uncertainty can be represented as an interval with an upper and lower value or as an uncertainty distribution.

3.1.13
uncertainty contributor
single event or particular set of events upon which the uncertainty of the top consequence depends

Note 1 to entry: Uncertainty contributors can be ranked relative to each other by their *uncertainty contribution* (3.1.13).

3.1.14
uncertainty contribution
measure of the decrease of the uncertainty of a top consequence, when the probabilities of the events associated with the corresponding uncertainty contributor are assumed to be without uncertainty

Note 1 to entry: 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 to entry: Uncertainty contribution provides a systematic measure that makes it possible to rank data and information sources.

3.2 Abbreviated terms

FMECA	Failure Mode, Effects, and Criticality 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

PRA 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).

In this document, the PRA methodology is intended for technical risk assessments involving mission success and system safety.

4.2 Mission success and system safety risk assessment concept

The application of PRA to mission success and system safety risks is discussed here. Mission success and system safety risk assessments complement deterministic failure modes and effects analysis (FMEA) and hazard analysis (HA) by adding a probabilistic dimension to the deterministic evaluation in the form of failure mode, effects, and criticality analysis (FMECA) in the case of the former and hazard risk assessment in the case of the latter. These probabilistic evaluations support risk informed decision-making.

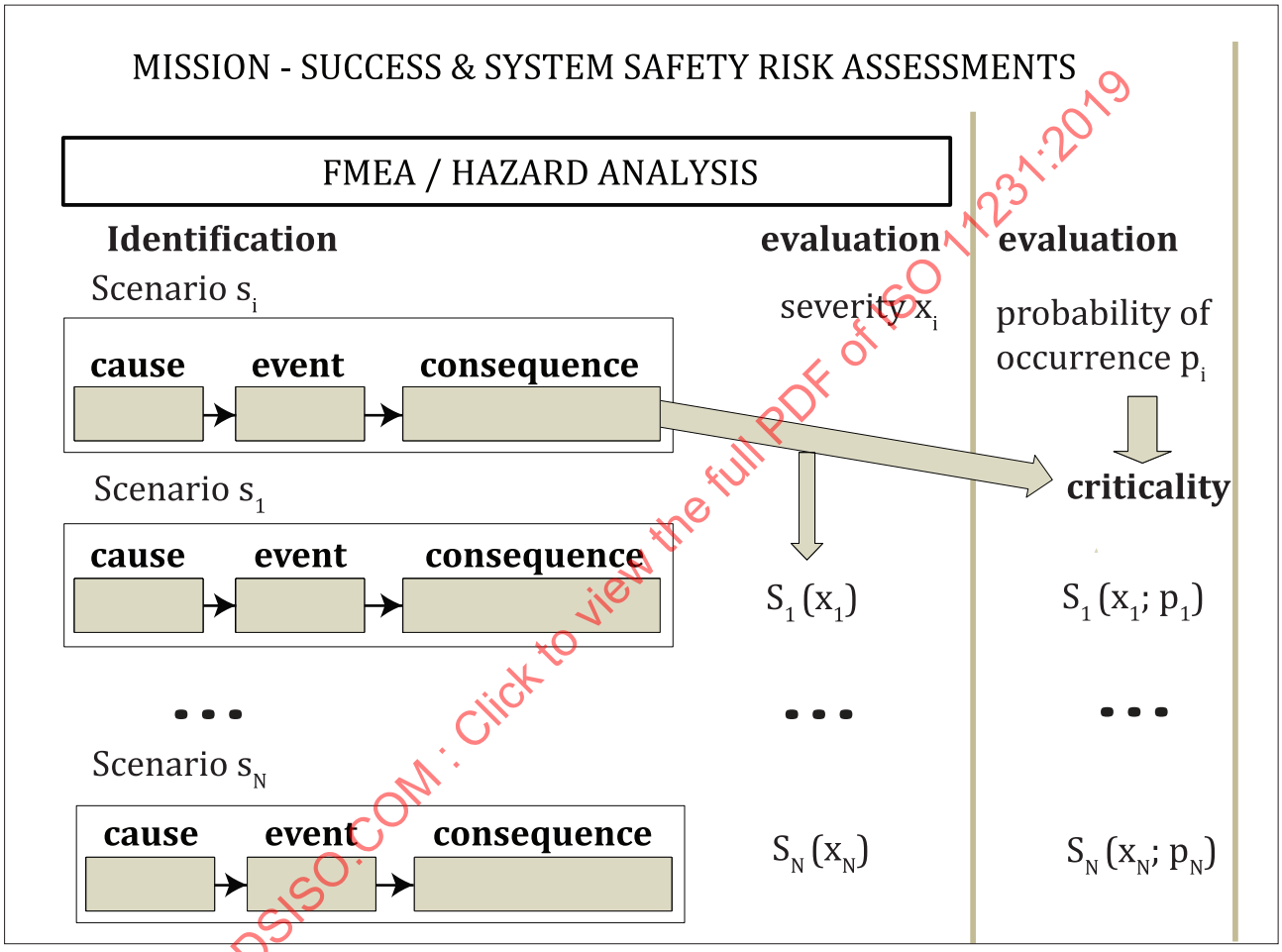
The relationship between the deterministic and probabilistic failure modes/hazards evaluation methods is shown in Figure 1.

Mission-success and system safety risk assessments can be used to either assess the risks posed by individual risk scenarios separately, or assess sets of risk scenarios collectively, in the form of the overall risk posed by those scenarios.

The assessment of individual risk scenarios can be performed using consequence severity and scenario probability categorization schemes by applying risk grids or risk matrices and risk indexes, as described in ISO 23460 and ISO 14620-1. However, these risk matrixes 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 the 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.



Key

S_i	scenario i	$S_1(x_1;p_1)$	risk of scenario 1
S_1	scenario 1	$S_N(x_N)$	severity of scenario N
S_N	scenario N: with severity = x_i and probability = p_i	$S_N(x_N;p_N)$	risk of scenario N
$S_1(x_1)$	severity of scenario 1		

Figure 1 — Relationship between the deterministic and probabilistic failure modes/hazard evaluation methods

A representation of the assessment of the overall mission-success or system safety risk is shown in Figure 2. As indicated in the figure, the risk assessment uses the failure mode or 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 the 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 probability 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 probabilities 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 probabilities by domain specialists). Events are quantified in the context of the corresponding hazard scenario, i.e. the probability of an event is assessed conditionally on the previous events in the sequence.

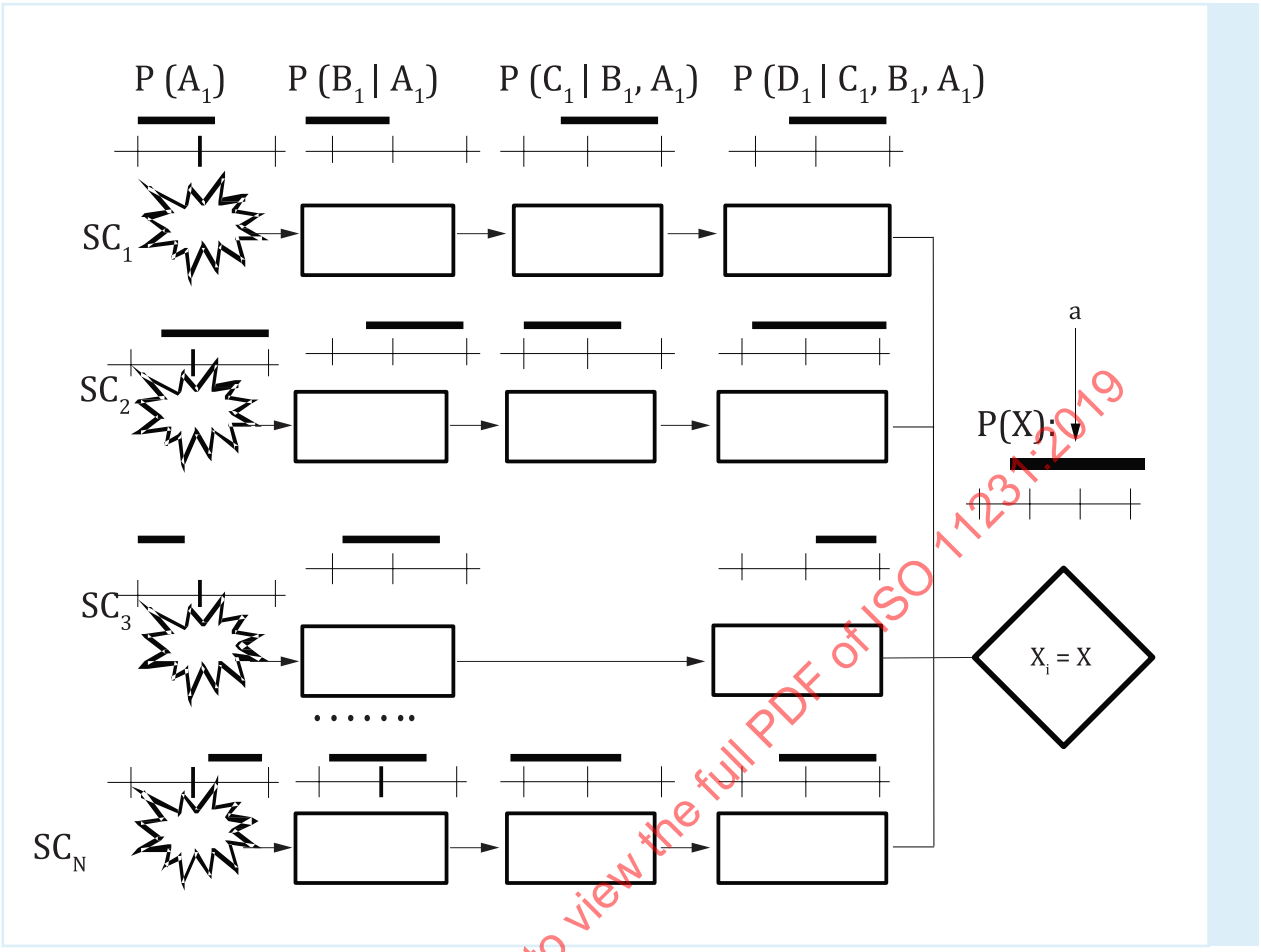
Systematic identification and treatment of uncertainties is characteristic of the assessment of the overall risk and conducted in two ways. The probability estimates of scenario events are produced with their associated uncertainties and presented in the form of probability distributions or intervals.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

Quantification of the overall risk is obtained by calculating the probabilities 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 in the comparisons. A 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 probability and have the highest potential for reducing this uncertainty. The reduction of consequence uncertainties directly transfers to the use of lower representative point values of the consequence probabilities.

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.



Key

SC_1	scenario 1	$P(A_1)$	probability of A_1, the initiating event
SC_2	scenario 2	$P(B_1 \mid A_1)$	conditional probability of B_1 given A_1
SC_3	scenario 3	$P(C_1 \mid B_1, A_1)$	conditional probability of C_1 given B_1 and A_1
SC_N	scenario N	$P(D_1 \mid C_1, B_1, A_1)$	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	a	Representative point value

Figure 2 — Example of the assessment of the overall risk

4.3 PRA general process

As illustrated in Figure 3, the PRA general 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). Frequencies and consequences are integrated into a representation of the risk profile of the system. This risk profile is evaluated for uncertainties and then used to support risk management decisions.

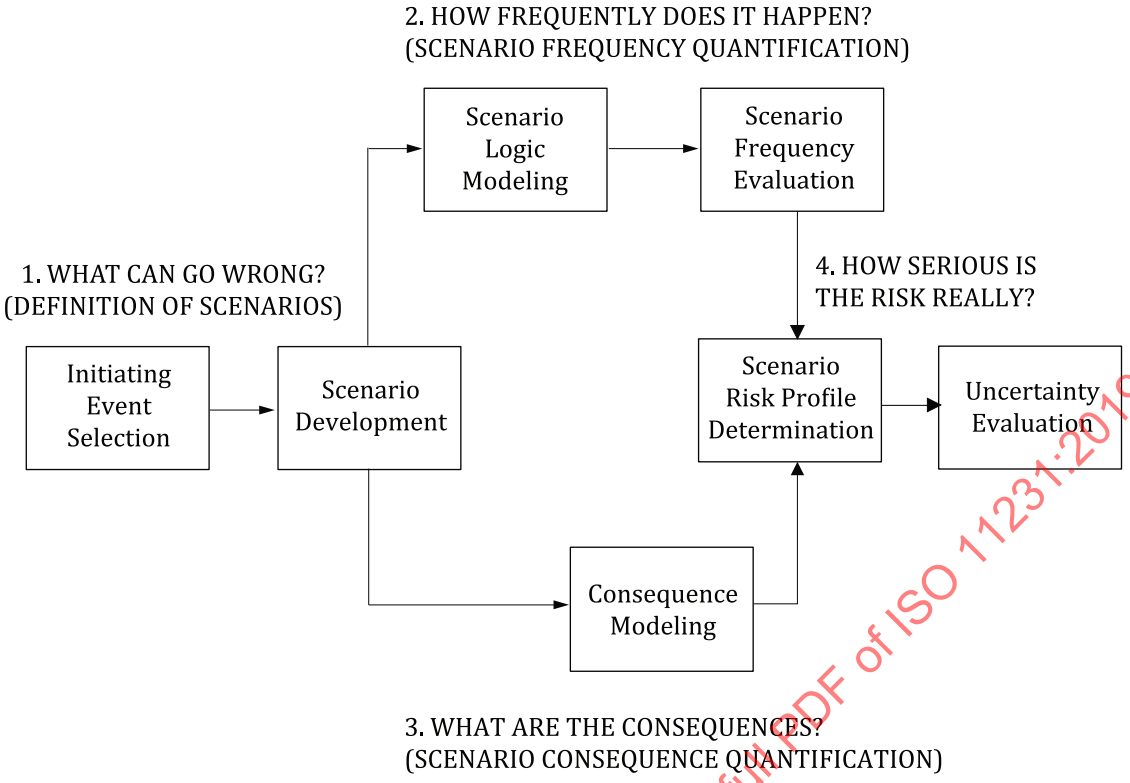


Figure 3 — PRA general process flow steps

5 Objectives, uses and benefits of probabilistic risk assessment

5.1 Objectives of a probabilistic risk assessment

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 prioritize options for risk reduction.

5.2 Probabilistic risk assessment results usage

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 evidences;

— to support safety certification of a system through documented evidences;

— to support risk communication and tracking;

— to provide input to overall project risk management.

5.3 Benefits of a probabilistic risk assessment

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.

6 PRA requirements and detailed process

6.1 Probabilistic risk assessment requirements

The probabilistic risk assessment requirements in this document are defined as follows:

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

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

6.2 Overview of the probabilistic risk assessment process

The basic tasks of a probabilistic risk assessment are described in 6.3. These basic tasks are used to implement steps 1 through 4 of the PRA general process flow, as outlined in 4.3 and illustrated in Figure 3. The PRA planning should result in a set of activities that are commensurate with the system's unit-value/mission-criticality and life cycle technical data content/maturity. This planning is sometimes referred to as a capability-based process tailoring (see ISO/TS 18667). An example of space systems unit-value/mission-criticality category definitions is provided in Annex A (sourced from ISO/TS 18667). Guidance for capability-based PRA process tailoring is provided in Annex B (sourced from ISO/TS 18667).

6.3 Probabilistic risk assessment basic tasks

6.3.1 General

The detailed PRA process flow diagram is illustrated in Figure 4. A brief description of each of the nine basic tasks in this process is provided in 6.3.2 to 6.3.10.

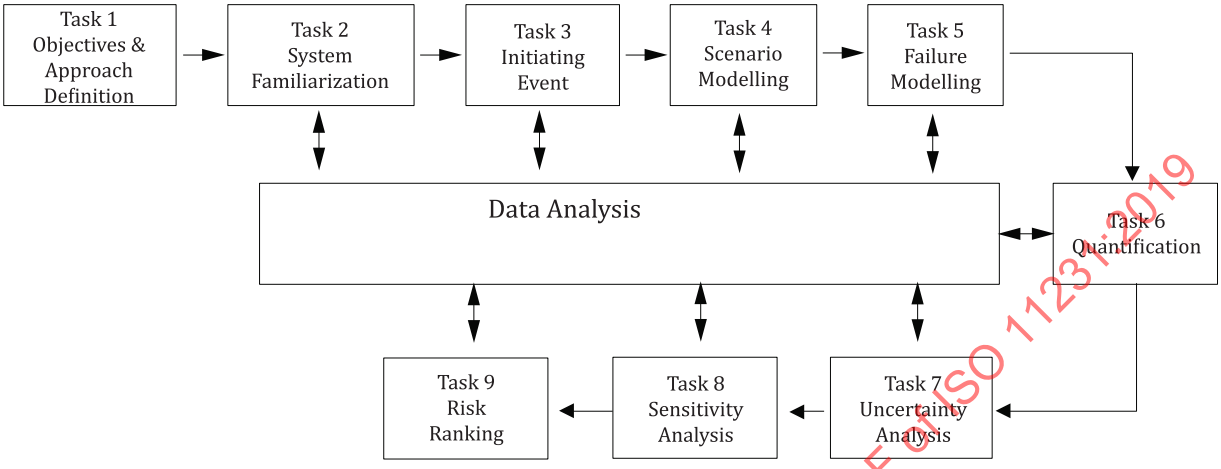


Figure 4 — Detailed PRA process flow basic tasks

6.3.2 Task 1: Objectives and approach definition

The initial task of a PRA is to define the objectives, scope and approach of the analysis, i.e. plan the PRA. 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 probability 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.

e) Document the approved PRA plan.

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 a 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 the 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 Mode, Effects, and Criticality Analysis (FMECA), 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 FMECA systematically assumes component failures and evaluates their effects on the 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 FMECAs).

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 effects on the system into groups and determine the 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 failures (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 the same 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 probabilities 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 the PRA analyst to find ways to quantify and present uncertainties associated with analytical inputs, models and degree of knowledge in a manner that will make the risk results understandable and usable to the decision-makers. All PRA insights reported to decision-makers should include an appreciation of the overall degree of uncertainty involved and provide insights concerning which sources of uncertainty are critical to the results. Monte Carlo simulation methods are generally used to perform uncertainty analysis.

The activities below are included in task 7.

a) When estimating the frequency of occurrence of each minimal cut set, the uncertainty in the data should be included. Develop appropriate uncertainty distributions or representations for the basic events in the minimal cuts sets.

b) Logically combine the uncertainty distribution for the initiating event with the uncertainty distributions for the failure probabilities associated basic events. There are a number of methods available for performing these calculations, including analytical methods and Monte Carlo simulation.

c) Determine uncertainties in the magnitude of the undesired end states (consequences).

d) Evaluate the uncertainty contribution of individual basic events to the uncertainty in the overall results.

e) Record the results with their uncertainty bounds including insights concerning which sources of uncertainty are critical to the results.

6.3.9 Task 8: Sensitivity analysis

Sensitivity analysis is a type of uncertainty analysis that focuses on evaluating the effects of variations (due to uncertainties) in assumptions, modelling, physical parameters and basic events. These analyses are frequently performed in a PRA to indicate those analytical inputs or elements whose changes in value cause the greatest changes in partial or final risk results. Sensitivity analyses are also used to assess the sensitivity of the PRA results to dependencies among basic event failures.

The activities below are included in task 8.

a) List the assumptions concerning mission, structure, system and component success criteria, modelling, and physical parameters. In addition, identify those structures, systems and components contained in single accident sequences (minimal cut sets) that have a common property, which could render them susceptible to dependent failures.

b) For the assumptions, systematically and independently vary the success criteria, modelling and parametric values, and change the PRA models and data by adjusting the event sequence [event tree(s)] and event failure models [fault tree(s)] appropriately. Re-evaluate the overall PRA model for changes in the accident sequences, ranking and quantitative risk results.

c) For potentially dependent structures, systems and components within a single cut set, combine them into a single basic event and assign it the highest probability among the coupled events. Independently re-evaluate the overall PRA model for changes that occur to the accident sequences, ranking and quantitative risk results from each adjusted cut set.

6.3.10 Task 9: Ranking

In some PRA applications, special techniques are used to identify the lead, or dominant, contributors to risk in accident sequences or scenarios. The ranking of these lead, or dominant, contributors in decreasing order of importance is called importance ranking. The ranking process is usually performed using the event sequence [event tree(s)] and event failure models [fault tree(s)]. There are several quantitative importance measures that typically determine the change in the quantified risk (probability) due to the change in the probability of a basic event or measure the contribution of a basic event to the overall risk. Some of these quantitative important measures include Fussell-Vesely (F-V), risk reduction worth (RRW), and risk achievement worth (RAW).

The activities below are included in task 9.

a) Identify the main risk contributors.

b) Evaluate the overall risk model for the selected importance measures and rank order individual accident scenarios and basic events accordingly.

c) Determine the contributions to the overall risk and uncertainty from these accident sequences and basic events.

6.3.11 Data analysis

Data analysis refers to the process of collecting and analysing information and data. Data collection and analysis proceeds in parallel or in conjunction with the nine PRA tasks described above, so it is not addressed as a separate task in this document. One of the uses of data analysis in PRA is to estimate various parameters of the initiating events and the basic events used in the PRA models. These parameters are normally organized into a database and used to obtain probabilities for structures, systems and component failure rates, initiator frequencies, human failure probabilities and common cause factors. In cases where there are no statistically significant data to support PRA parameter estimation, the PRA analyst may need to rely on expert judgment and elicitation.

PRA data analysis includes but is not limited to the activities below:

a) Identify the data needed from the initiating events and the basics events in the PRA model.

b) Collect probability information and data for the events from objective data (measured or directly observed from relevant test or experience), semi-objective data (extrapolation from generic data, similarity data or physical models) and subjective data (expert judgment by domain specialists).

c) Estimate event probabilities using statistical methods and develop uncertainty distributions.

d) Develop a PRA database containing collected information and data, parameter estimates and probabilities including uncertainties.

7 Peer review

7.1 General

In order to enhance the quality and credibility of a PRA, internal and external peer reviews should be conducted. In general, these reviews concentrate on the appropriateness of methods, information, sources, judgments and assumptions, as well as their application to the project being evaluated and its objective(s).

The purpose of these reviews is to verify the correct application of the methodology and the accuracy of the analytical results. Peer reviews should be conducted for all PRAs.

7.2 Internal peer reviews

Internal peer reviews are conducted by team members composed of subject matters experts to cross-check each other's models and results. These reviews also involve the examination and discussions of the models and results with individuals most knowledgeable with the systems being evaluated, including designers, builders and operators.

7.3 External peer reviews

This type of review is carried out by independent peers, i.e. people who are not involved in the study and have no stake in it, but who have capabilities that are better than those of the individuals who performed the study. The peers' expertise should span the range of disciplines and experience required for the study.

The use of a participatory peer review should be considered. The participatory peer review process begins early in the assessment and proceeds in parallel with the project, involving frequent, periodic contact and interactions with the PRA team. This type of review is conducted in order to identify problems and to recommend corrective actions early, instead of waiting to begin the peer review when the PRA is virtually complete. While this approach may sacrifice some independence in the peer review,

it is likely to result in a PRA being performed correctly the first time, thereby saving the expenditure of time and resources in the correction of problems at the end of the project.

8 Probabilistic risk assessment report — Data content requirements

Table 1 establishes the data content requirements for a probabilistic risk assessment report. A PRA report shall be established according to the content given in this table. The safety risk assessment report may be combined with a hazard analysis report, as appropriate.

Table 1 — Probabilistic risk assessment report contents

Main clause	Description
Title page	The title page shall include: — document title; — document number and release date; — name and affiliation of author(s); — release signatures.
Document change record	The document change record shall be completed in accordance with project configuration management requirements.
Table of contents	Self-explanatory.
Introduction/Scope/Summary	This clause shall provide a brief introduction of the report, its scope and a summary of the main findings.
Documents	This clause shall provide a list of all applicable (normative) and reference (informative) documents used to establish the report.
Terms, definitions and acronyms	Terms, definitions and acronyms shall be explained. Unless they are unique to the report, this may be by reference to other documents.
Scope, mission profile and systems	This clause shall provide the scope, the mission profile and system(s), or portion thereof, included in the analysis.
Requirements	This clause shall provide a summary of the relevant requirements on the system(s) under consideration and on the performance of the assessment, including consequence severity and scenario probability categorizations.
Assumptions	This clause shall provide a description of any assumptions made in performing the assessment, including, where necessary, any limitations on the performance of the assessment (e.g. not all tasks performed).
Description of the system/functions	This clause shall provide a description of the systems and functions in sufficient detail to support the modelling and findings of the assessment.
Description of the methods, models and analytical techniques	This clause shall provide a description of the methods and models used in performing the analysis, including, where applicable, the analytical techniques for systems response and consequence quantification.
Data analysis	This clause shall provide a description of the data, data reduction techniques and uncertainty models used in the assessment.
Summary of results and recommendations	This clause shall summarize the results of the assessment and provide recommendations.

Annex A
(informative)

Example of space systems unit-value/mission-criticality category definitions

Table A.1 — Example space systems unit-value/mission-criticality category definitions

High III unit-value/ mission-criticality category 5	High II unit-value/ mission-criticality category 4	High I unit-value/ mission-criticality category 3	Medium unit-value/ mission-criticality category 2	Low unit-value/ mission-criticality category 1
— Defence spacecraft — Launch vehicles — Long-range missiles — Nuclear powered spacecraft — Flight termination hardware/ software components — Radiation/ high-energy emitting equipment — Commercial /military manned spacecraft & space stations	— Commercial/ communications spacecraft — Experimental manned spacecraft — Short-range missiles/ rockets — Low Earth orbit passenger spacecraft — Human or environment safety-critical hardware/ software components — Military satellite control stations — Radiation hardened spacecraft electronics — Spacecraft explosive devices	— Science/ Research spacecraft — Small satellites — CubeSats (debris threat) — Non-human & non-environment safety-critical hardware/ software components — Commercial satellite control stations — Military computers/ peripherals — Military grade spacecraft electronics — Spacecraft structures/ mechanisms — Spacecraft pressure vessels — Landers on comet/planet	— CubeSats & micro satellites (non-debris threat) — Industrial grade spacecraft electronics — Industrial computers/ peripherals — Industrial computers/ peripherals — Space experiment equipment — Spacecraft status monitoring hardware/ software components — Computer operating system software programs — Prototype spacecraft systems/ components — Satellite data relay stations	— Motorized/ manual spacecraft assembly tools — Spacecraft insulation materials — Computer application software programs

Annex B
(informative)

Capability-based PRA process tailoring guidance

B.1 The capability-level 1 PRA process activities

B.1.1 Authorization of the contractor's PRA function and assigning it responsibility and authority for meeting the PRA requirements of this document, the contract and the supplier's enterprise-level command media. The implementation of an appropriately tailored PRA process by appropriately trained personnel should be authorized as needed.

— Assignment of qualified management and technical personnel to perform PRA, and provide them with the tools they need to plan and implement a cost-effective PRA process.

— Use of validated methods to identify, assess and eliminate or control unacceptable mission success and system safety risks.

B.1.2 Identification of the applicable PRA requirements. The identified PRA requirements should be consistent with this document and the contract. The supplier should flow down the PRA requirements to all subordinate suppliers that provide inputs to the PRA. The basic PRA tasks are:

— Objectives & approach definition

— System familiarization

— Initiating event assessment

— Scenario modelling

— Failure modelling

— Quantification

— Uncertainty analysis

— Sensitivity analysis (using engineering judgement)

— Risk ranking (using engineering judgement)

B.1.3 Documentation of an internally approved PRA plan that is consistent with this document, the contract and the supplier's enterprise-level command media.

B.1.4 Coordination of PRA activities and data items with subordinate suppliers.

B.1.5 Application of appropriate engineering best practices to perform the PRA basic tasks.

B.1.6 Implementation of a qualitative risk assessment process that is consistent with this document and ISO 17666.

B.1.7 Utilization of formal and informal methods to verify PRA requirements are met. The formal verification methods involve review and concurrence by the customer. Verification of hazardous materials risk mitigation is typically performed in a formal manner. The informal verification methods involve review and concurrence by internal management only.