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

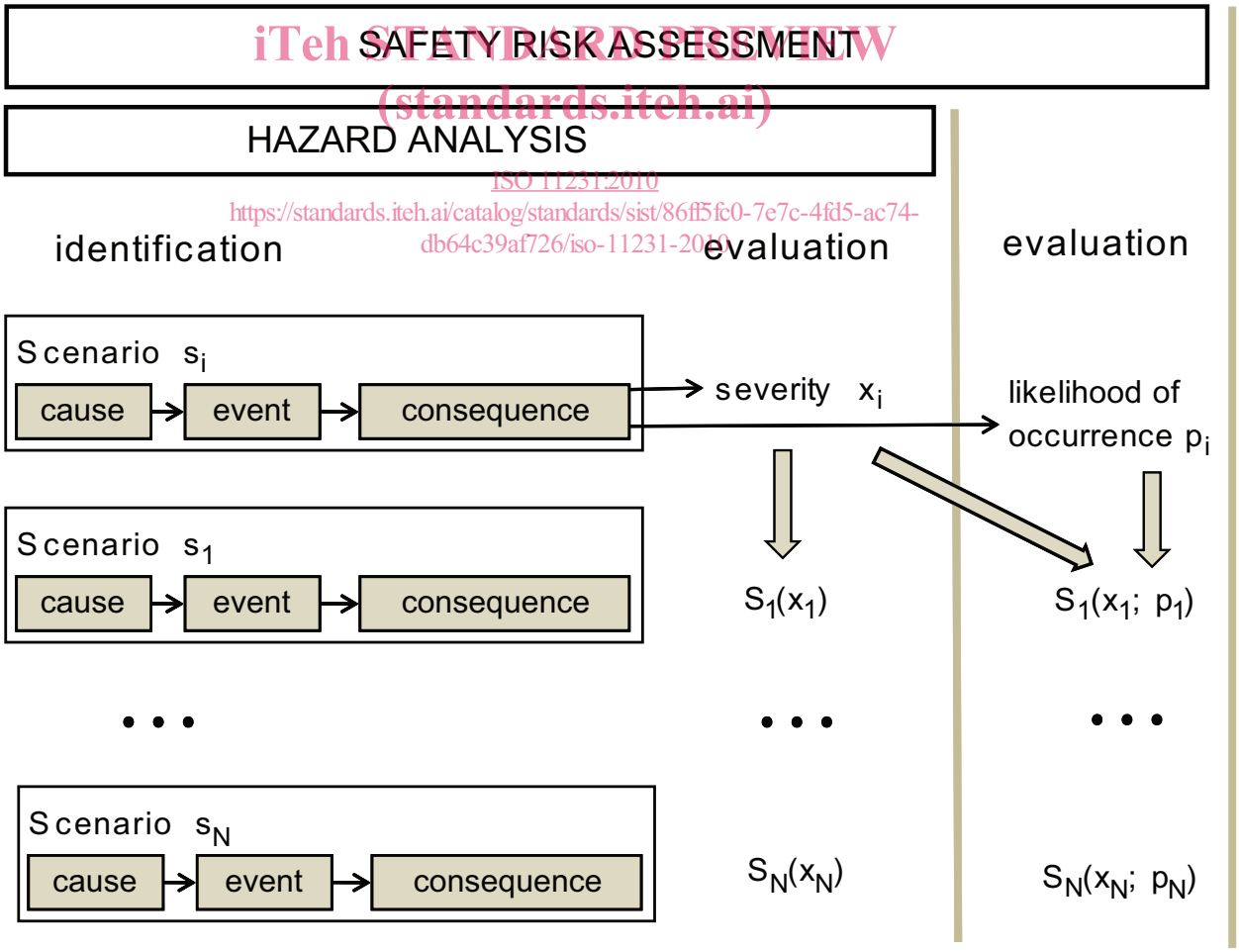
The application of PRA to safety problems is discussed here. The safety risk assessment concept is derived from PRA. Safety risk assessment complements deterministic hazard analysis by adding a probabilistic dimension to the evaluation of hazards in support risk informed decision-making. The probabilistic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