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.

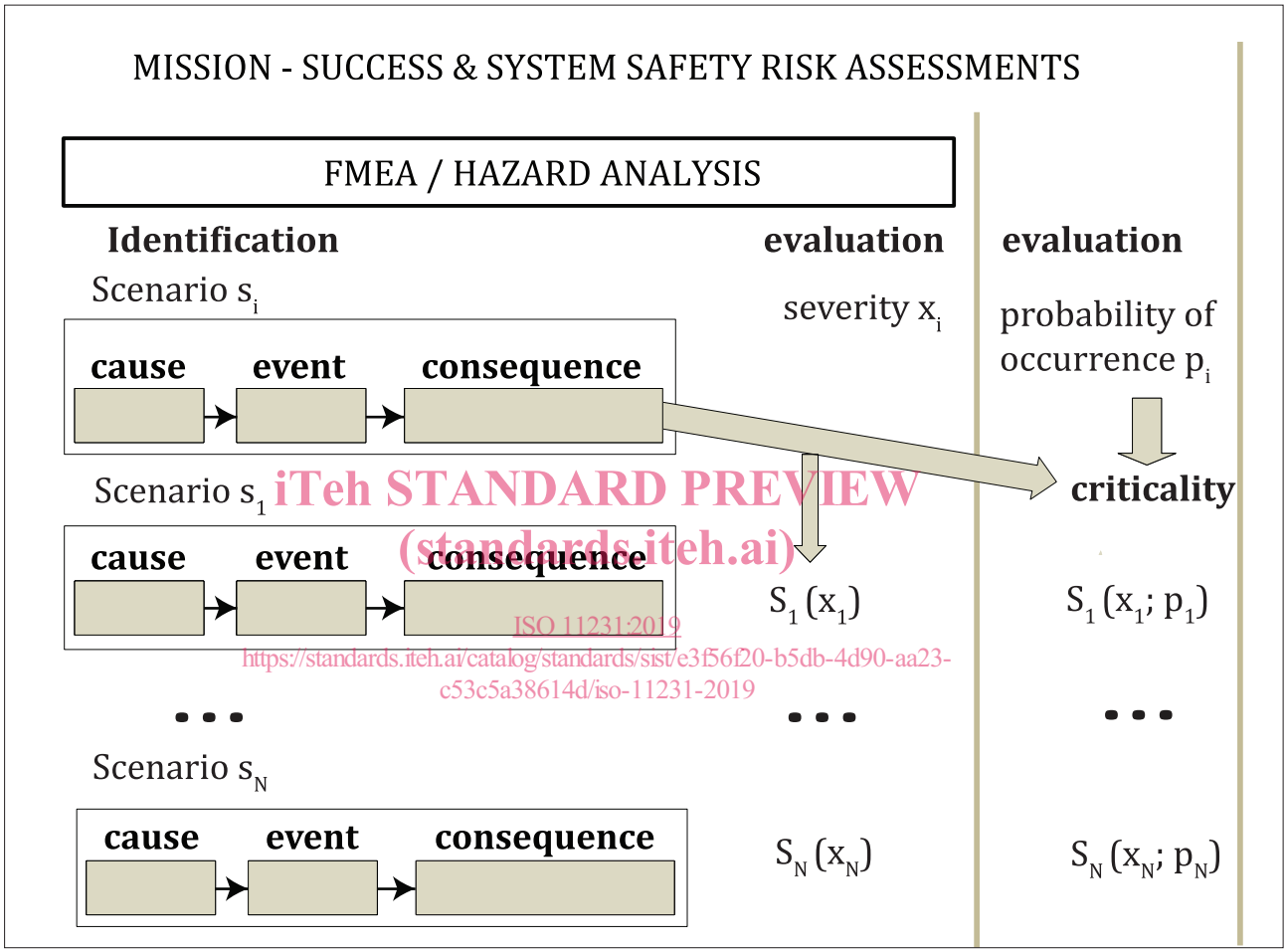
The relationship between the deterministic and probabilistic failure modes/hazards evaluation methods is shown in Figure 1.

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.