INTERNATIONAL STANDARD

ISO 17666

Second edition
2016-11-15

Space systems — Risk management

Systèmes spatiaux — Management des risques

Reference number
ISO 17666:2016(E)

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

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 on 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 the following URL: www.iso.org/iso/foreword.html.

The committee responsible for this document is ISO/TC 20, *Aircraft and space vehicles*, Subcommittee SC 14, *Space systems and operations*.

This second edition cancels and replaces the first edition (ISO 17666:2003), of which it constitutes a minor revision. Annex B has been added in this edition and contains a DRD for consideration when preparing the risk management plan.

Introduction

Risks are a threat to the project success because they have negative effects on the project cost, schedule and technical performance, but appropriate practices of controlling risks can also present new opportunities with positive impact.

The objective of project risk management is to identify, assess, reduce, accept, and control space project risks in a systematic, proactive, comprehensive, and cost-effective manner, taking into account the project's technical and programmatic constraints. Risk is considered tradable against the conventional known project resources within the management, programmatic (e.g. cost, schedule), and technical (e.g. mass, power, dependability, safety) domains. The overall risk management in a project is an iterative process throughout the project life cycle, with iterations being determined by the project progress through the different project phases, and by changes to a given project baseline influencing project resources.

Risk management is implemented at each level of the customer-supplier network.

Known project practices for dealing with project risks, such as system and engineering analyses, analyses of safety, critical items, dependability, critical path, and cost, are an integral part of project risk management. Ranking of risks according to their criticality for the project success, allowing management attention to be directed to the essential issues, is a major objective of risk management.

The project actors agree on the extent of the risk management to be implemented into a given project depending on the project definition and characterization.

Space systems — Risk management

1 Scope

This document defines, extending the requirements of ISO 14300-1, the principles and requirements for integrated risk management on a space project. It explains what is needed to implement a project-integrated risk management policy by any project actor, at any level (i.e. customer, first-level supplier, or lower-level suppliers).

This document contains a summary of the general risk management process, which is subdivided into four (4) basic steps and nine (9) tasks. The implementation can be tailored to project-specific conditions.

The risk management process requires information exchange among all project domains and provides visibility over risks, with a ranking according to their criticality for the project; these risks are monitored and controlled according to the rules defined for the domains to which they belong.

The fields of application of this document are all the space project phases. A definition of project phasing is given in ISO 14300-1.

When viewed from the perspective of a specific programme or project context, the requirements defined in this document are tailored to match the genuine requirements of a particular profile and circumstances of a programme or project.

NOTE Tailoring is a process by which individual requirements or specifications, standards, and related documents are evaluated and made applicable to a specific programme or project by selection, and in some exceptional cases, modification and addition of requirements in the standards.

2 Normative references

There are no normative references in this document.

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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

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

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

3.1.1
acceptance of risk
decision to cope with consequences, should a risk scenario materialise

Note 1 to entry: A risk can be accepted when its magnitude is less than a given threshold, defined in the risk management policy.

Note 2 to entry: In the context of risk management, acceptance can mean that even though a risk is not eliminated, its existence and magnitude are acknowledged and tolerated.

3.1.2
risk communication
all information and data necessary for risk management addressed to a decision maker and to relevant actors within the project hierarchy

3.1.3
risk index
combined score used to measure the likelihood of occurrence, magnitude, and severity of risk

3.1.4
individual risk
risk identified, assessed, and mitigated as a distinct risk items in a project

3.1.5
risk management
systematic and iterative optimisation of the project resources, performed according to the established project risk management policy

3.1.6
risk management policy
organisation's attitude towards risks, how it conducts risk management, the risks it is prepared to accept and how it defines the main requirements for the risk management plan

3.1.7
risk management process
all project activities related to the identification, assessment, reduction, acceptance, and feedback of risks

3.1.8
overall risk
risk resulting from the assessment of the combination of individual risks and their impact on each other, in the context of the whole project

Note 1 to entry: Overall risk can be expressed as a combination of qualitative and quantitative assessment.

3.1.9
risk reduction
implementation of measures that leads to reduction of the likelihood or severity of risk

Note 1 to entry: Preventive measures aim at eliminating the cause of a problem situation, and mitigation measures aim at preventing the propagation of the cause to the consequence or reducing the severity of the consequence or the likelihood of the occurrence.

3.1.10
residual risk
risk remaining after implementation of risk reduction measures

3.1.11
resolved risk
risk that has been rendered acceptable

3.1.12
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.

3.1.13
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.

3.1.14
risk trend
evolution of risks throughout the life cycle of a project

3.1.15
unresolved risk
risk for which risk reduction attempts are not feasible, cannot be verified, or have proven unsuccessful

Note 1 to entry: It can also be defined as a risk remaining unacceptable.

4 Abbreviated terms

The following abbreviated terms are defined and used within this document.

ECSS European Cooperation for Space Standardization

IEC International Electrotechnical Commission

5 Principles of risk management

5.1 Risk management concept

Risk management is a systematic and iterative process for optimising resources in accordance with the project's risk management policy. It is integrated through defined roles and responsibilities into the day-to-day activities in all project domains. Risk management assists managers and engineers when including risk aspects in management and engineering practices and judgement throughout the project life cycle. It is performed in an integrated, holistic way, maximising the overall benefits in areas such as:

— design, construction, testing, operation, maintenance, and disposal, together with their interfaces,

— control over risk consequences, and

— management, cost, and schedule.

This process adds value to the data that is routinely developed, maintained, and reported.

5.2 Risk management process

The entire spectrum of risks is assessed. Trade-offs are made among different, and often competing, goals. Undesired events are assessed for their severity and likelihood of occurrence. The assessments of the alternatives for mitigating the risks are iterated, and the resulting measurements of performance and risk trend are used to optimise the tradable resources.

Within the risk management process, available risk information is produced and structured, facilitating risk communication and management decision making. The results of risk assessment and reduction and the residual risks are communicated to the project team for information and follow-up.

5.3 Risk management implementation into a project

Risk management requires corporate commitment in each actor's organisation and the establishment of clear lines of responsibility and accountability from corporate level downwards. Project management

has the overall responsibility for the implementation of risk management, ensuring an integrated, coherent approach for all project domains.

Risk management is a continuous, iterative process. It constitutes an integral part of normal project activity and is embedded within the existing management processes. It utilises the existing elements of the project management processes to the maximum extent possible.

5.4 Risk management documentation

The risk management process is documented to ensure that the risk management policies are established, understood, implemented, and maintained, and that they are traceable to the origin and rationale of all risk-related decisions made during the life of the project.

6 The risk management process

6.1 Overview of the risk management process

The iterative four-step risk management process of a project is illustrated in Figure 1. The tasks to be performed within each of these steps are shown in Figure 2.

Step 1 comprises the establishment of the risk management policy (Task 1) and risk management plan (Task 2), and is performed at the beginning of a project. The implementation of the risk management process consists of a number of "risk management cycles" over the project duration comprising Steps 2 to 4, subdivided into seven: Tasks 3 to 9.

The period designated in the illustration with "Risk management process" comprises all the project phases of the project concerned. The frequency and project events at which cycles are required in a project (only three are shown in Figure 1 for illustration purposes) depend on the needs and complexity of the project and need to be defined during Step 1. Unforeseen cycles are required when changes to, for example, the schedule, technologies, techniques, and performance of the project baseline occur.

Risks at any stage of the project are controlled as part of the project management activities.

