

This is a preview of "ISO 11231:2010". [Click here to purchase the full version from the ANSI store.](#)

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 2010

This is a preview of "ISO 11231:2010". [Click here to purchase the full version from the ANSI store.](#)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.



COPYRIGHT PROTECTED DOCUMENT

© ISO 2010

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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

This is a preview of "ISO 11231:2010". [Click here to purchase the full version from the ANSI store.](#)

Contents

Page

Foreword	iv
Introduction.....	v
1 Scope	1
2 Normative references	1
3 Terms, definitions and abbreviated terms	1
3.1 Terms and definitions	1
3.2 Abbreviated terms	3
4 Principles of probabilistic risk assessment	4
4.1 General	4
4.2 Safety risk assessment concept	5
4.3 Concept of risk and probabilistic risk assessment	7
5 Objectives, uses, and benefits of probabilistic risk assessment.....	8
6 PRA requirements and process	10
6.1 Probabilistic risk assessment requirements	10
6.2 Overview of the probabilistic risk assessment process	10
6.3 Probabilistic risk assessment tasks.....	10
7 Peer review.....	15
7.1 General	15
7.2 Internal peer reviews.....	15
7.3 External peer reviews.....	15
8 Probabilistic risk assessment report — data content requirements	16
Bibliography.....	17

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*.

This is a preview of "ISO 11231:2010". [Click here to purchase the full version from the ANSI store.](#)

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.