
Space systems — Probabilistic risk assessment (PRA)

Systèmes spatiaux — Évaluation du risque probabiliste (PRA)

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO 11231:2019

<https://standards.iteh.ai/catalog/standards/iso/e3f56f20-b5db-4d90-aa23-c53c5a38614d/iso-11231-2019>



iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO 11231:2019

<https://standards.iteh.ai/catalog/standards/iso/e3f56f20-b5db-4d90-aa23-c53c5a38614d/iso-11231-2019>



COPYRIGHT PROTECTED DOCUMENT

© ISO 2019

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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	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	4
4 Principles of probabilistic risk assessment	4
4.1 General	4
4.2 Mission success and system safety risk assessment concept	4
4.3 PRA general process	7
5 Objectives, uses and benefits of probabilistic risk assessment	8
5.1 Objectives of a probabilistic risk assessment	8
5.2 Probabilistic risk assessment results usage	8
5.3 Benefits of a probabilistic risk assessment	9
6 PRA requirements and detailed process	9
6.1 Probabilistic risk assessment requirements	9
6.2 Overview of the probabilistic risk assessment process	9
6.3 Probabilistic risk assessment basic tasks	10
6.3.1 General	10
6.3.2 Task 1: Objectives and approach definition	10
6.3.3 Task 2: System familiarization	11
6.3.4 Task 3: Initiating event identification	11
6.3.5 Task 4: Scenario modelling	12
6.3.6 Task 5: Failure modelling	12
6.3.7 Task 6: Quantification	13
6.3.8 Task 7: Uncertainty analysis	13
6.3.9 Task 8: Sensitivity analysis	14
6.3.10 Task 9: Ranking	14
6.3.11 Data analysis	15
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
Annex A (informative) Example of space systems unit-value/mission-criticality category definitions	17
Annex B (informative) Capability-based PRA process tailoring guidance	18
Bibliography	22

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.