
**Space systems — Safety
requirements —**

**Part 1:
System safety**

*Systèmes spatiaux — Exigences de sécurité —
Partie 1. Sécurité système*

Dit document mag slechts op een stand-alone PC worden geïnstalleerd. Gebruik op een netwerk is alleen toestaan als een aanvullende licentieovereenkomst voor netwerkgebruik met NEN is afgesloten. This document may only be used on a stand-alone PC. Use in a network is only permitted when a supplementary license agreement for us in a network with NEN has been concluded.

Preview



Reference number
ISO 14620-1:2018(E)

© ISO 2018

Copyright
Preview



COPYRIGHT PROTECTED DOCUMENT

© ISO 2018

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	vii
Introduction	viii
1 Scope	1
1.1 General.....	1
1.2 Field of application.....	2
1.3 Tailoring.....	2
2 Normative references	2
3 Terms, definitions and abbreviated terms	2
3.1 Terms and definitions.....	2
3.2 Abbreviated terms.....	5
4 System safety programme	6
4.1 Scope.....	6
4.2 Safety organization.....	6
4.2.1 General.....	6
4.2.2 Safety representative.....	6
4.2.3 Reporting lines.....	6
4.2.4 Safety integration.....	6
4.2.5 Coordination with others.....	6
4.3 Safety representative access and authority.....	6
4.3.1 Access.....	6
4.3.2 Delegated authority to reject — stop work.....	7
4.3.3 Delegated authority to interrupt operations.....	7
4.3.4 Conformance.....	7
4.3.5 Approval of reports.....	7
4.3.6 Review.....	7
4.3.7 Representation on boards.....	7
4.4 Safety risk management.....	7
4.4.1 Safety risks.....	7
4.4.2 Hazard assessment.....	7
4.4.3 Preferred measures.....	8
4.5 Project phases and safety review cycle.....	8
4.5.1 Progress meetings.....	8
4.5.2 Project reviews.....	8
4.5.3 Safety programme review.....	10
4.5.4 Safety data package.....	10
4.6 Safety programme plan.....	11
4.6.1 Implementation.....	11
4.6.2 Safety activities.....	11
4.6.3 Definition.....	11
4.6.4 Description.....	11
4.6.5 Safety and project engineering activities.....	11
4.6.6 Supplier and sub-supplier premises.....	11
4.6.7 Conformance.....	11
4.7 Safety certification.....	12
4.8 Safety training.....	12
4.8.1 Overall training.....	12
4.8.2 Participation.....	12
4.8.3 Detailed technical training.....	12
4.8.4 Product specific training.....	12
4.8.5 Records.....	12
4.8.6 Identification.....	12
4.9 Accident/incident reporting and investigation.....	13
4.10 Safety documentation.....	13

	4.10.1	General	13
	4.10.2	Customer access	13
	4.10.3	Supplier review	13
	4.10.4	Documentation	13
	4.10.5	Safety data package	13
	4.10.6	Safety deviations and waivers	14
	4.10.7	Verification tracking log	14
	4.10.8	Lessons-learned file	14
5		Safety engineering	15
	5.1	Safety engineering objectives	15
	5.1.1	General	15
	5.1.2	Elements	15
	5.1.3	Lessons learned	15
	5.2	Safety design principles	15
	5.2.1	Human life consideration	15
	5.2.2	Design selection	15
	5.2.3	System safety order of precedence	15
	5.2.4	Environmental compatibility	16
	5.2.5	Safe without services	16
	5.2.6	Fail safe design	16
	5.2.7	Hazard detection — Signalling and safing	17
	5.2.8	Access	17
	5.2.9	Safety risk reduction and control	17
	5.3	Failure tolerance requirements	19
	5.3.1	Basic requirements	19
	5.3.2	Software	20
	5.3.3	Payload interface	20
	5.3.4	Redundancy separation	20
	5.3.5	Failure propagation	20
	5.3.6	Design for minimum risk	21
	5.3.7	Probabilistic safety targets	21
	5.4	Identification and control of safety critical functions	22
	5.4.1	Identification	22
	5.4.2	Inadvertent operation	22
	5.4.3	Provisions	22
	5.4.4	Shutdown and failure tolerance requirements	22
	5.4.5	Electronic, electrical, electromechanical	22
6		Safety analysis requirements and techniques	23
	6.1	General	23
	6.2	Assessment and allocation of requirements	23
	6.2.1	Safety requirements	23
	6.2.2	Additional safety requirements	23
	6.2.3	Define safety requirements — functions	23
	6.2.4	Define safety requirements — subsystems	23
	6.2.5	Justification	23
	6.2.6	Functional and subsystem specification	24
	6.3	Safety analysis	24
	6.3.1	General	24
	6.3.2	Mission analysis	24
	6.3.3	Feasibility	24
	6.3.4	Preliminary definition	24
	6.3.5	Detailed definition, production and qualification	24
	6.3.6	Utilization	24
	6.3.7	Disposal	24
	6.4	Specific safety analysis	25
	6.4.1	General	25
	6.4.2	Hazard analysis	25

6.4.3	Safety risk assessment.....	25
6.4.4	Safety analysis for hardware-software systems.....	26
6.5	Supporting assessment and analysis.....	27
6.5.1	General.....	27
6.5.2	Warning time analysis.....	27
6.5.3	Caution and warning analysis.....	27
6.5.4	Common cause and common mode failure analysis.....	27
6.5.5	Fault tree analysis.....	28
6.5.6	Human dependability analysis.....	28
6.5.7	Failure modes, effects and criticality analysis.....	28
6.5.8	Sneak analysis.....	28
6.5.9	Zonal analysis.....	29
6.5.10	Energy trace analysis.....	29
7	Safety verification.....	30
7.1	General.....	30
7.2	Tracking of hazards.....	30
7.2.1	Hazard reporting system.....	30
7.2.2	Status.....	30
7.2.3	Safety progress meeting.....	30
7.2.4	Review and disposition.....	30
7.2.5	Documentation.....	30
7.2.6	Mandatory inspection points.....	30
7.3	Safety verification methods.....	31
7.3.1	Verification engineering and planning.....	31
7.3.2	Methods and reports.....	31
7.3.3	Verification requirements.....	31
7.3.4	Analysis.....	31
7.3.5	Inspections.....	31
7.3.6	Tests.....	31
7.3.7	Verification and approval.....	31
7.4	Qualification of safety critical functions.....	32
7.4.1	Verification.....	32
7.4.2	Qualification.....	32
7.4.3	Failure tests.....	32
7.4.4	Verification of design or operational characteristics.....	32
7.4.5	Safety verification testing.....	32
7.5	Hazard close-out.....	32
7.5.1	Safety assurance verification.....	32
7.5.2	Safety approval authority.....	32
7.6	Residual risk reduction.....	33
8	Operational safety.....	33
8.1	General.....	33
8.2	Basic requirements.....	33
8.3	Flight operations and mission control.....	33
8.3.1	Launcher operations.....	33
8.3.2	Contamination.....	33
8.3.3	Flight rules.....	33
8.3.4	Hazardous commanding control.....	34
8.3.5	Mission operation change control.....	34
8.3.6	Safety surveillance and anomaly control.....	34
8.4	Ground operations.....	34
8.4.1	Applicability.....	34
8.4.2	Initiation.....	35
8.4.3	Review and inspection.....	35
8.4.4	Hazardous operations.....	35
8.4.5	Launch and landing site requirements.....	35
8.4.6	GSE requirements.....	35

Preview
Copyright

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 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 the following URL: 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 14620-1:2002), which has been technically revised.

The main changes compared to the previous edition are as follows:

- definitions have been revised; and
- the document has been aligned with the ISO/IEC Directives Part 2, 2016 edition.

A list of all parts in the ISO 14620 series can be found on the ISO website.

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

This document is one of the series of space standards intended to be applied together for the management, engineering and product assurance in space projects and applications.

ISO 14620-1:2018(E)
Preview

Space systems — Safety requirements —

Part 1: System safety

1 Scope

1.1 General

This document defines the safety programme and the technical safety requirements that are implemented in order to comply with the safety policy as defined in ISO 14300-2. It is intended to protect flight and ground personnel, the launch vehicle, associated payloads, ground support equipment, the general public, public and private property, and the environment from hazards associated with space systems. Launch site operations are described by ISO 14620-2 and flight safety systems in ISO 14620-3.

The safety policy is applied by implementing a system safety programme, supported by risk assessment, which can be summarized as follows.

- a) Hazardous characteristics (system and environmental hazards) and functions with potentially hazardous failure effects are identified and progressively evaluated by iteratively performing systematic safety analyses.
- b) The potential hazardous consequences associated with the system characteristics and functional failures are subjected to a hazard reduction sequence whereby:
 - 1) hazards are eliminated from the system design and operations;
 - 2) hazards are minimized; and
 - 3) hazard controls are applied and verified.
- c) The risks that remain after the application of a hazard elimination and reduction process are progressively assessed and subjected to risk assessment, in order to:
 - 1) show compliance with safety targets;
 - 2) support design trades;
 - 3) identify and rank risk contributors;
 - 4) support apportionment of project resources for risk reduction;
 - 5) assess risk reduction progress; and
 - 6) support the safety and project decision-making process (e.g. waiver approval, residual risk acceptance).
- d) The adequacy of the hazard and risk control measures applied are formally verified in order to support safety validation and risk acceptance.
- e) Safety compliance is assessed by the project and safety approval obtained from the relevant authorities.

ALTIJD DE ACTUELE NORM IN UW BEZIT HEBBEN?

Nooit meer zoeken in de systemen en uzelf de vraag stellen:
“Is ISO 14620-1:2018 en de laatste versie?”™

Via het digitale platform NEN Connect heeft u altijd toegang tot de meest actuele versie van deze norm. Vervallen versies blijven ook beschikbaar. **U en uw collega's** kunnen de norm via NEN Connect makkelijk raadplagen, online en offline.

Kies voor slimmer werken en bekijk onze mogelijkheden op www.nenconnect.nl.

Heeft u vragen?

Onze Klantenservice is bereikbaar maandag tot en met vrijdag, van 8.30 tot 17.00 uur.

Telefoon: 015 2 690 391

E-mail: klantenservice@nen.nl

