



BSI Standards Publication

**Space systems — Capability-based Safety,
Dependability, and Quality Assurance
(SD&QA) programme management**

National foreword

This Published Document is the UK implementation of ISO/TS 18667:2018.

The UK participation in its preparation was entrusted to Technical Committee ACE/68, Space systems and operations.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2018
Published by BSI Standards Limited 2018

ISBN 978 0 580 95241 8

ICS 49.140

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 March 2018.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

TECHNICAL
SPECIFICATION

ISO/TS
18667

First edition
2018-02-15

**Space systems — Capability
based Safety, Dependability,
and Quality Assurance (SD&QA)
programme management**

*Systèmes spatiaux — Management de programmes de sécurité, de
sûreté de fonctionnement et d'assurance de la qualité (SD&QA), axé
sur les capacités*



Reference number
ISO/TS 18667:2018(E)

© ISO 2018



COPYRIGHT PROTECTED DOCUMENT

© ISO 2018. Published in Switzerland

All rights reserved. Unless otherwise specified, 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
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	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms, definitions and abbreviated terms	1
3.1 Terms and definitions.....	2
3.2 Abbreviated terms.....	4
4 Objectives, policy and principles — General	5
4.1 Objectives.....	5
4.2 Policy.....	5
4.3 Principles.....	6
5 Instructions	9
5.1 General.....	9
5.2 Authorize SD&QA programme.....	9
5.2.1 General.....	9
5.2.2 Safety programme.....	10
5.2.3 Dependability programme.....	10
5.2.4 Quality Assurance (QA) programme.....	10
5.2.5 Assign qualified managers, leads, engineers, and technicians to SD&QA programme.....	10
5.2.6 Continuously improve the SD&QA processes.....	10
5.3 Define/identify, assess, and flow down the SD&QA requirements.....	10
5.3.1 Flow down the essential SD&QA requirements.....	11
5.3.2 Conflicting SD&QA requirements disposition criteria.....	12
5.4 Planning the SD&QA programme.....	12
5.4.1 General.....	12
5.4.2 Select SD&QA processes based on Product Unit-Value/Criticality Categories.....	16
5.4.3 Define SD&QA process implementation phasing based on systems engineering life cycle phases/milestones.....	16
5.4.4 Identify the SD&QA guidance sources.....	19
5.4.5 Establish the Technical Performance Metrics.....	19
5.5 Coordinate the SD&QA processes with other product assurance processes.....	19
5.5.1 General.....	19
5.5.2 Coordinate Project's and Subcontractor's SD&QA Activities.....	19
5.5.3 Establish, utilize, and maintain a project SD&QA database system.....	20
5.6 Apply engineering and evaluation methods to identify system and process deficiencies.....	20
5.6.1 General.....	20
5.6.2 Define the system failure criteria and identify failure modes.....	20
5.6.3 Assess maturity of key input data, constraints, ground rules, and analytical assumptions.....	22
5.7 SD&QA risk assessment and control.....	23
5.7.1 Integrate SD&QA with programme-wide technical risk management processes.....	23
5.7.2 SD&QA risk management responsibilities.....	23
5.7.3 SD&QA Programme Self-Inspections.....	24
5.7.4 SD&QA risk identification.....	25
5.7.5 Qualitative SD&QA risk likelihood assessment.....	27
5.7.6 Quantitative SD&QA risk likelihood assessment.....	30
5.7.7 SD&QA risk mitigation assessment.....	30
5.7.8 SD&QA risk tracking.....	30
5.7.9 SD&QA risk level assessment.....	31

5.7.10	Separate ESOH/system safety risk management.....	32
5.7.11	Present SD&QA risk status using a single risk matrix format.....	32
5.7.12	Perform structured SD&QA reviews.....	35
5.7.13	Apply SD&QA lessons learned.....	36
5.8	Verify SD&QA requirements are met.....	36
Annex A (informative) Fundamental SD&QA Processes.....		37
Annex B (informative) Capability-based Safety, Dependability and Quality Assurance Programme tailoring requirements template.....		39
Annex C (informative) Safety, Dependability and Quality Assurance (SD&QA) programme and Process Definitions.....		44
Annex D (informative) Space systems safety-critical and mission-critical unacceptable conditions checklist (Cont.).....		63
Bibliography.....		66

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*.

Introduction

This document is intended for use in the engineering community.

The terms Safety, Dependability, and Quality Assurance (SD&QA) are often used interchangeably, but they have very different meanings. *Safety* is the system state with acceptable levels of risk for conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. *Dependability* is the ability of an item or system to perform as and when required. *Quality Assurance* is the part of quality management focused on providing confidence that quality requirements are fulfilled.

This document defines the “*what to do’s*” at depths that facilitate consistency in planning and implementing SD&QA programme which identify, assess, and eliminate or mitigate technical risks using levels of effort commensurate with the product’s unit-value/criticality and systems engineering life cycle data content/maturity.

The fundamental building blocks of the capability-based SD&QA programme consists of the SD&QA processes identified in [Annex A](#) and described in [Annex C](#). The fundamental SD&QA processes are grouped programmatically according to separate SD&QA domains, and functionally according to documented management, engineering, and testing approaches. [Annex B](#) defines the tiered criteria used for rating the SD&QA risk management capability of existing SD&QA programme or for planning the desired SD&QA risk management capability of new SD&QA programme. The unique provisions of this document include the following:

- Consistent criteria (see [Annex B](#)) for rating the capability of SD&QA programme to identify, analyse, and mitigate or control, potential and existing, product and process deficiencies in a manner that is commensurate with the product’s unit-value/criticality (see [Table 1](#)) and systems engineering life cycle data content/maturity (see [Table 3](#));
- Structured planning to achieve a predefined level of SD&QA risk management capability for the overall SD&QA programme or any individual SD&QA process through a statement of work (SOW) or memorandum of agreement (MOA);
- Collecting, reviewing, and applying existing lessons learned for rating the maturity of input data used for performing SD&QA analyses;
- Creating and disseminating new lessons learned to sustain continuous improvement of the SD&QA programme through the enterprise.

Space systems — Capability-based Safety, Dependability, and Quality Assurance (SD&QA) programme management

1 Scope

This document applies to the design, development, fabrication, test, and operation of commercial, civil, and military space and ground control systems, sites/facilities, services, equipment, and computer software. Criteria is provided for rating the capability of the entire SD&QA programme or an individual SD&QA process to identify, assess, and eliminate or mitigate risks that threaten safety or mission success. The predefined capability rating criteria define the sequence of activities necessary to achieve a measurable improvement in the effectiveness of SD&QA risk management by implementing it in stages. Organizations can evaluate their existing SD&QA programme against the criteria in this document to identify the activities that need to be added, deleted, or modified to achieve the desired technical risk management effort. The phrase “desired technical risk management effort” means the activities and resources used to identify, assess, and eliminate or mitigate technical risks and commensurate with the product’s unit-value/criticality and systems engineering life cycle data content/maturity.

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 10794, *Space systems — Programme management, materials, mechanical parts and processes*

ISO 10795, *Space systems — Programme management and quality — Vocabulary*

ISO 14300-2, *Space systems — Programme management — Part 2: Product assurance*

ISO 14620-1, *Space systems — Safety requirements — Part 1: System safety*

ISO 17666, *Space systems — Risk management*

ISO 23460, *Space systems — Programme management — Dependability requirements*

ISO 27025, *Space systems — Programme management — Quality assurance requirements*

ISO 9000, *Quality management systems — Fundamentals and vocabulary*

NOTE A number of process level documents that are available to aid contractors achieve their safety, dependability, and quality assurance requirements are provided in the [Annex D](#).

3 Terms, definitions and abbreviated terms

For the purposes of this document, the terms and definitions given in ISO 10794, ISO 10795, ISO 14300-2, ISO 14620-1, ISO 17666, ISO 23460, ISO 27025, and ISO 9000 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 <https://www.iso.org/obp>