

DIN EN 16603-70-11

ICS 49.140

Einsprüche bis 2014-10-08

Entwurf**Raumfahrttechnik –
Raumsegment-Bedienbarkeit;
Englische Fassung FprEN 16603-70-11:2014**

Space engineering –
Space segment operability;
English version FprEN 16603-70-11:2014

Ingénierie spatiale –
Opérabilité du segment spatial;
Version anglaise FprEN 16603-70-11:2014

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2014-08-08 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nl@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den Normenausschuss Luft- und Raumfahrt (NL) im DIN, 10772 Berlin (Hausanschrift: Burggrafenstr. 6, 10787 Berlin).

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 83 Seiten

Normenausschuss Luft- und Raumfahrt (NL) im DIN

Nationales Vorwort

Dieses Dokument (FprEN 16603-70-11:2014) wurde vom Technischen Komitee CEN/CLC/TC 5 „Raumfahrt“ erarbeitet, dessen Sekretariat vom DIN (Deutschland) gehalten wird.

Dieses Dokument ist derzeit zum einstufigen Annahmeverfahren vorgelegt.

Dieses Dokument wurde speziell zur Behandlung von Raumfahrtsystemen erarbeitet und hat daher Vorrang vor jeglicher Europäischer Norm, da es denselben Anwendungsbereich hat, jedoch über einen größeren Geltungsbereich (z. B. Luft- und Raumfahrt) verfügt.

Das zuständige deutsche Normungsgremium ist der Arbeitsausschuss NA 131-10-01 AA „Interoperabilität von Informations-, Kommunikations- und Navigationssystemen“ im DIN-Normenausschuss Luft- und Raumfahrt (NL).

Nationaler Anhang NA (informativ)

3 Begriffe und Abkürzungen

3.1 Begriffe aus anderen Normen

Für die Anwendung dieser Norm gelten die Begriffe nach ECSS-S-ST-00-01.

3.2 Für diese Norm spezifische Begriffe

3.2.1 Kategorien der Bedienbarkeit

3.2.1.1

Steuerbarkeit

Bereitstellung angemessener Steuerfunktionen mit dem Ziel der Konfiguration der bordseitigen Systeme für die Ausführung der Nenn-Missionsoperationen und der Fehlererkennungs-, -identifizierungs-, -isolierungs- und -diagnose- sowie Wiederherstellungs- und Instandhaltungsoperationen

3.2.1.2

Kompatibilität

Fähigkeit zweier oder mehrerer Systeme oder Komponenten zur Ausführung ihrer festgelegten Funktionen ohne Interferenz

3.2.1.3

Deaktivierung

Fähigkeit zur Durchführung geplanter Operationen mit dem Ziel der Beendigung der Mission am Ende ihrer Nutzlebensdauer

ANMERKUNG zum Begriff: Beendigung kann die Deaktivierung des Raumfahrzeugs, dessen Zurückholen aus der Umlaufbahn oder beides bedeuten.

3.2.1.4

Flexibilität

Fähigkeit zur Konfiguration und optimalen Nutzung bestehender bordseitiger Funktionen, der Kapazität der Weltraum-Erde-Kommunikationsverbindungen sowie jeglicher in das Design integrierter Redundanzen mit dem Ziel der Erfüllung der Ziele im Zusammenhang mit der Funktionsfähigkeit

3.2.1.5

Überprüfbarkeit

Verfügbarkeit von Informationen zu Status, Konfiguration und Leistung des Raumsegments für das Bodensegment und die bordseitigen Funktionen

3.2.1.6

Testbarkeit

Prüfbarkeit

Fähigkeit zur Prüfung der bordseitigen Funktionen des Raumsegments, einschließlich der im „Offline-Zustand“ befindlichen

Anmerkung zum Begriff: „Offline-Zustand“ bezieht sich auf Funktionen, die nicht Teil der aktuellen betrieblichen Konfiguration sind.

3.2.2 Begriffe im Zusammenhang mit kritischen Funktionen

3.2.2.1

steuerbare wichtige Funktion

wichtige Funktion, die ohne Eingriff der bordseitigen Software durch Befehle hoher Priorität steuerbar ist

3.2.2.2

Befehl hoher Priorität

Impulsbefehl, der mithilfe einer bordseitigen Befehls-Impulsverteilereinheit (CPDU) direkt der Hardware zugeführt wird

3.2.2.3

Telemetrie hoher Priorität

Telemetrie, die eine zuverlässige Bestimmung des aktuellen Status der wichtigen bordseitigen Geräte ermöglicht und unter allen Bedingungen verfügbar ist

Anmerkung zum Begriff: Die Telemetrie hoher Priorität kann mithilfe eines Mechanismus verwaltet werden, der von dem für die genormte betriebliche Telemetrie eingesetzten unabhängig ist, üblicherweise ohne Beteiligung von Mikroprozessoren.

3.2.2.4

Funktion lokaler Kritikalität

Funktion, die im Falle ihrer Ausführung im falschen Kontext (z. B. zur falschen Zeit) eine vorübergehende oder dauerhafte Qualitätsabnahme der zugehörigen lokalen Funktionen verursachen kann, jedoch nicht die Funktionalität auf höherer Ebene beeinträchtigt

3.2.2.5

missionskritische Funktion

Funktion, die im Falle ihrer Ausführung im falschen Kontext (z. B. zur falschen Zeit) oder auf die falsche Weise eine dauerhafte Qualitätsabnahme der Mission verursachen kann

3.2.2.6

dauerhafte Qualitätsabnahme der Raumsegmentfunktion

Situation, in der eine gegebene bordseitige Funktion für die gesamte übrige Lebensdauer der Mission weder auf der Nennkette noch auf einer beliebigen redundanten Kette erreicht werden kann

3.2.2.7

dauerhafte Qualitätsabnahme der Mission

Situation, in der Raumsegmentfunktionen oder -leistungen, die die Erzeugung von Missionsprodukten oder primären Missionszielen beeinflussen, für die gesamte übrige Lebensdauer der Mission weder auf der Nennkette noch auf einer beliebigen redundanten Kette erreicht werden können

3.2.2.8

vorübergehende Qualitätsabnahme der Raumsegmentfunktion

Situation, in der eine gegebene bordseitige Funktion für eine begrenzte Zeitdauer weder auf der Nennkette noch auf einer beliebigen redundanten Kette erreicht werden kann

3.2.2.9

vorübergehende Qualitätsabnahme der Mission

Situation, in der Raumsegmentfunktionen oder -leistungen, die die Erzeugung von Missionsprodukten oder primären Missionszielen beeinflussen, für eine begrenzte Zeitdauer weder auf der Nennkette noch auf einer beliebigen redundanten Kette erreicht werden können

Anmerkung zum Begriff: Beispielsweise ein nicht verfügbarer Zustand einer Mission nach dem Übergang in den Überlebensmodus.

3.2.2.10

wichtige Funktion

Funktion, die von wesentlicher Bedeutung für den Erfolg der Mission ist und eine dauerhafte Qualitätsabnahme der Mission verursachen kann, sofern sie zum falschen Zeitpunkt, auf falsche Weise oder im falschen Kontext ausgeführt wird

3.2.2.11

wichtiger Fernsteuerbefehl

Fernsteuerbefehl, der eine steuerbare wichtige Funktion aktiviert

3.2.3 Weitere Begriffe

3.2.3.1

Anwendungsprozess

bordseitige Instanz, die in der Lage ist, telemetriebezogene Quelldaten zu erzeugen und fernsteuerbezogene Daten zu empfangen

3.2.3.2

Authorisierung

Recht einer authentifizierten Instanz, eine Funktion auszuführen oder Zugang zu einer Dateneinheit oder einem Datenfluss zu erhalten

3.2.3.3

Kette

Satz von Hard- oder Softwareeinheiten, die zusammenarbeiten, um eine gegebene Funktion auszuführen

Anmerkung zum Begriff: Beispielsweise bilden der Prozessor eines Lage- und Bahnregelungssystems (AOCS) und die zugehörige Software sowie ein Satz von AOCS-Sensoren und -Auslösern gemeinsam eine AOCS-Kette.

3.2.3.4

Vertraulichkeit

Eigenschaft, die darin besteht, dass Informationen unbefugten Einzelpersonen, Instanzen oder Prozessen nicht zur Verfügung gestellt oder bekannt gegeben werden

3.2.3.5

Steuerfunktion

Mechanismus, der dazu dient, einen Parameter oder Satz von Parametern innerhalb festgelegter Grenzen zu halten

Anmerkung zum Begriff: Eine Steuerfunktion besteht üblicherweise aus einem Satz von Messungen und Reaktionen (Befehlen), die entsprechend einer Funktion, eines Algorithmus oder eines Satzes von Regeln miteinander im Zusammenhang stehen.

3.2.3.6

Datenintegrität

Eigenschaft, die darin besteht, dass die Daten nicht auf unbefugte Weise verändert oder zerstört wurden

3.2.3.7

Authentifizierung der Datenherkunft

Bestätigung, dass die Quelle der empfangenen Daten dem Anspruch entspricht

3.2.3.8

Datierung

Zuordnung von zeitbezogenen Informationen zu Telemetriedaten

Anmerkung zum Begriff: Dies umfasst die Messdaten zur Nutzlast.

3.2.3.9**gerätebezogener Fernsteuerbefehl**

Fernsteuerbefehl, der der bordseitigen Hardware zugeführt und durch diese ausgeführt wird

Anmerkung zum Begriff: Beispielsweise ein Fernsteuerbefehl zum Schalten eines Relais oder ein Fernsteuerbefehl zum Laden eines bordseitigen Registers.

3.2.3.10**betriebliche Telemetrie**

Telemetrie, die der Überwachung des ordnungsgemäßen Zustands und der ordnungsgemäßen Funktion des Raumsegments dient

3.2.3.11**Missionsverlust**

Zustand, in dem das Bodensegment das Raumsegment nicht länger kontrollieren kann (z. B. aufgrund des Kontaktverlusts) oder in dem das Raumsegment nicht länger die Ziele der Mission erfüllen kann (z. B. aufgrund von Anomalien)

3.2.3.12**Speicher**

Datenspeicherbereich an Bord

Anmerkung 1 zum Begriff: Dies umfasst den Hauptspeicher und weitere Speicher.

Anmerkung 2 zum Begriff: Beispiele für Speicher sind Disketten, Bänder und Magnetblasenspeicher.

3.2.3.13**Betriebsart**

Betriebszustand eines Raumfahrzeugs, eines Subsystems oder einer Nutzlast, in dem bestimmte Funktionen ausgeführt werden können

3.2.3.14**Modenübergang**

Übergang zwischen zwei Betriebsarten

3.2.3.15**bordseitige Autonomie**

Fähigkeit des Raumsegments, für eine gegebene Zeitdauer Nenn- oder Störfalloperationen ohne Eingriff des Bodensegments zu handhaben

3.2.3.16**bordseitige Überwachung**

an Bord erfolgende Anwendung der Prüffunktionen auf einen Satz bordseitiger Parameter unter Einhaltung vordefinierter Kriterien

Anmerkung zum Begriff: Die Überwachungsfunktionen umfassen die Prüfung von Grenzwerten und erwarteten Werten sowie Deltaprüfungen.

3.2.3.17**bordseitige Betriebsprozedur**

Überwachungs- und Kontrollprozedur, die an Bord gespeichert und deren Aktivierung durch das Bodensegment gesteuert wird

3.2.3.18**Zeitplan der bordseitigen Operationen**

bordseitige Einrichtung für die Speicherung und Freigabe von Fernsteuerbefehlen, die zuvor vom Boden aus geladen wurden

Anmerkung zum Begriff: In seiner einfachsten Form speichert der Zeitplan der bordseitigen Operationen zeitlich gekennzeichnete Fernsteuerbefehle, die vom Boden aus geladen wurden, und gibt sie an den Bestimmungs-Anwendungsprozess frei, sobald ihre Bordzeit erreicht wurde.

3.2.3.19

Bedienbarkeit

Fähigkeit des Raumsegments, über die gesamte Lebensdauer der Mission durch das Bodensegment betrieben zu werden und gleichzeitig die Nutzung der Ressourcen zu optimieren sowie die Qualität, Quantität und Verfügbarkeit (oder Rechtzeitigkeit der Lieferung) der Missionsprodukte ohne Einschränkung der Sicherheit des Raumsegments zu maximieren

3.2.3.20

Operationen

Tätigkeiten, die durch das Boden- und das Raumsegment vorgenommen werden, um die rechtzeitige Bereitstellung der Missionsprodukte oder -dienstleistungen sicherzustellen, die Wiederherstellung nach Störungen an Bord zu ermöglichen, routinemäßige Instandhaltungstätigkeiten durchzuführen und die bordseitigen Ressourcen zu verwalten, um die Bereitstellung der Missionsprodukte oder -dienstleistungen sowie die Lebensdauer der Mission zu maximieren

3.2.3.21

Parameter

unterste Ebene der elementaren Dateneinheiten an Bord

3.2.3.22

Gültigkeit der Parameter

Bedingung, die definiert, ob die Auslegung eines Telemetrieparameters zuverlässig und sinnvoll ist

Anmerkung zum Begriff: Die Ausgabe der Winkelwerte eines Gyroskops weist nur dann eine gültige technische Bedeutung auf, wenn die Energieversorgung des Gyroskops „eingeschaltet“ ist; ansonsten handelt es sich um eine zufällige Ausgabe. Ein derartiger Parameter wird als bedingt gültig angesehen, wobei die Gültigkeit entsprechend dem Energiezustand bestimmt wird.

3.2.3.23

Partnerinstanz-Authentifizierung

Authentifizierung gleichrangiger Instanzen

Bestätigung, dass die Partnerinstanz in einer Assoziation dem Anspruch entspricht

3.2.3.24

sicherer Zustand

sichere Bedingung eines Systems, eines Subsystems oder einer Nutzlast

3.2.3.25

Raumsegment-Status

Informationen, mithilfe derer der betriebliche Zustand des Raumsegments beurteilt wird und die Kriterien bestimmt werden, auf deren Grundlage die betrieblichen Entscheidungen getroffen werden

3.2.3.26

Überlebensmodus

Survivalzustand

Konfiguration eines Raumfahrzeugs, in der es für eine festgelegte Zeitdauer ohne Eingriff des Bodensegments im sicheren Zustand verbleiben kann

3.2.3.27

Fernsteuerfunktion

durch einen Fernsteuerbefehl ausgelöste betrieblich eigenständige Steuertätigkeit, die eine oder mehrere Steuertätigkeit(en) auf niedrigerer Ebene umfassen oder aufrufen kann

3.3 Abkürzungen

Für die Anwendung dieser Norm gelten die Abkürzungen in ECSS-S-ST-00-01 und die folgenden Abkürzungen:

Abkürzung	Bedeutung
AOCS	Lage- und Bahnregelungssystem (en: attitude and orbit control subsystem)
APID	Anwendungsprozess-Kennung (en: application process identifier)
CPDU	Befehls-Impulsverteilereinheit (en: command pulse distribution unit)
CPU	Hauptprozessor (en: central processor unit)
CRC	zyklische Redundanzprüfung (en: cyclic redundancy check)
EEPROM	elektrisch löschbarer programmierbarer Nur-Lese-Speicher (en: electrically erasable programmable read-only memory)
FDIR	Ausfallerkennung, Isolierung und Wiederherstellung (en: failure detection, isolation and recovery)
GPS	weltweites Ortungssystem, globales Navigationssatellitensystem (en: global positioning system)
I/O	Eingabe/Ausgabe; Eingang/Ausgang (en: input/output)
ID	Kennung (en: identifier)
MAP	Mehrfachzugangspunkt (en: multiplexed access point)
OBT	Bordzeit (en: on-board time)
RAM	Speicher mit wahlfreiem/direktem Zugriff (en: random access memory)
RF	Funkfrequenz (en: radio frequency)
RFI	Funkstörung (en: radio frequency interference)
RFP	Angebotsanfrage (en: request for proposal)
TT&C	Telemetrie, Nachführung und Befehl (en: telemetry, tracking and command)
UTC	koordinierte Weltzeit, koordinierte Universalzeit (en: universal time coordinated)

3.4 Konventionen

Einige Anforderungen stehen mit Größen im Zusammenhang, deren Werte nicht pauschal, sondern nur missionsweise definiert werden können (z. B. Zeitintervalle oder Reaktionszeiten). Sie werden als Missionskonstanten bezeichnet und in dieser Norm durch eckige Klammern dargestellt.

Anmerkung zum Begriff: Beispielsweise <TC_VERIF_DELAY>

In einigen Fällen sind Beispielwerte angegeben. Diese Missionskonstanten sind in Anhang A zusammengefasst.

May 2014

ICS 49.140

English version

Space engineering - Space segment operability

Ingénierie spatiale - Opérabilité du segment spatial

Raumfahrttechnik - Raumsegment-Bedienbarkeit

This draft European Standard is submitted to CEN members for unique acceptance procedure. It has been drawn up by the Technical Committee CEN/CLC/TC 5.

If this draft becomes a European Standard, CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

This draft European Standard was established by CEN and CENELEC in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.



CEN-CENELEC Management Centre:
Avenue Marnix 17, B-1000 Brussels

Table of contents

Foreword	5
Introduction.....	6
1 Scope.....	7
2 Normative references	8
3 Terms, definitions and abbreviated terms.....	9
3.1 Terms from other standards.....	9
3.2 Terms specific to the present standard	9
3.3 Abbreviated terms.....	14
3.4 Conventions.....	14
4 General requirements.....	15
4.1 Introduction.....	15
4.2 Observability	15
4.3 Commandability	15
4.4 Compatibility	16
4.5 Safety and fault tolerance	16
4.6 Flexibility.....	17
4.7 Testability	18
4.8 Deactivation.....	18
5 Detailed requirements	19
5.1 Introduction.....	19
5.2 Mission-level	19
5.2.1 Security.....	19
5.2.2 Control functions	20
5.2.3 Uplink and downlink	20
5.3 Telemetry	21
5.3.1 Telemetry design	21
5.3.2 Diagnostic mode	23
5.4 Datation and synchronization.....	24
5.5 Telecommanding	25

5.5.1	Telecommand design.....	25
5.5.2	Critical telecommands.....	27
5.5.3	Telecommand transmission and distribution.....	27
5.5.4	Telecommand verification	28
5.6	Configuration management.....	29
5.6.1	Modes	29
5.6.2	On-board configuration handling	30
5.7	On-board autonomy.....	31
5.7.1	Introduction	31
5.7.2	General autonomy.....	31
5.7.3	Autonomy for execution of nominal mission operations.....	32
5.7.4	Autonomy for mission data management	33
5.7.5	On-board fault management	33
5.8	Requirements specific to the telemetry and telecommand packet utilization standard	38
5.8.1	Application process and service design.....	38
5.8.2	Statistical data reporting.....	39
5.8.3	Memory management	40
5.8.4	Function management	41
5.8.5	On-board operations scheduling	41
5.8.6	On-board monitoring	42
5.8.7	Large data transfer.....	44
5.8.8	Telemetry generation and forwarding.....	44
5.8.9	On-board storage and retrieval	44
5.8.10	On-board traffic management	46
5.8.11	On-board operations procedures.....	46
5.8.12	Event-to-action coupling.....	47
5.9	Equipment- and subsystem-specific	47
5.9.1	On-board processors and software	47
5.9.2	Power supply and consumption.....	49
5.9.3	Telemetry, tracking and command (TT&C).....	49
5.9.4	Attitude and orbit control	50
5.9.5	Mechanisms.....	50
5.9.6	Thermal control	51
5.9.7	Payload.....	51
Annex A (informative) Mission constants		52
Annex B (informative) Tailoring guide		54

Bibliography	75
---------------------------	-----------

Tables

Table 5-1: Mission execution autonomy levels	32
Table 5-2: Mission execution autonomy levels	33
Table 5-3: Mission execution autonomy levels	34
 Table B-1 : Tailoring guide	 55

Foreword

This document (FprEN 16603-70-11:2014) has been prepared by Technical Committee CEN/CLC/TC 5 "Space", the secretariat of which is held by DIN (Germany).

This document (FprEN 16603-70-11:2014) originates from ECSS-E-ST-70-11C.

This document is currently submitted to the Unique Acceptance Procedure.

This document has been developed to cover specifically space systems and will therefore have precedence over any EN covering the same scope but with a wider domain of applicability (e.g. : aerospace).

Introduction

The operability of the space segment has an impact on total life cycle cost inasmuch as increased operability can increase development costs, but certainly decreases operations and maintenance costs. Therefore, the adoption of specific operability goals for a given mission is decided by careful balancing of costs, risks, and schedules for both the development and the operations and maintenance phases.

The objective of this standard is to define operability requirements that:

- ensure that the space segment can be operated in a safe and cost-effective manner;
- facilitate the tasks of preparation for, and execution and evaluation of, space segment check-out and mission operations activities;
- facilitate the tasks of space segment suppliers when preparing a proposal in response to a request for proposal (RFP).

1

Scope

This Standard contains provisions for the design of on-board functions for unmanned space segments in order to ensure that the space segment can be operated in-flight in any nominal or predefined contingency situation.

The requirements in this Standard are grouped in two clauses, containing general operability requirements and detailed operability requirements, respectively. The general operability requirements can be applied to all missions, whilst the detailed operability requirements are only applicable if the corresponding on-board function is implemented.

The operability of the space segment to meet mission-specific requirements is outside the scope of this standard.

To support the users of this Standard in tailoring the requirements to the needs of their particular mission, Annex B contains a table that indicates, for each requirement, the potential impact of its omission.

This standard may be tailored for the specific characteristics and constraints of a space project, in conformance with ECSS-S-ST-00.

2

Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this ECSS Standard. For dated references, subsequent amendments to, or revisions of any of these publications, do not apply. However, parties to agreements based on this ECSS Standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references the latest edition of the publication referred to applies.

EN reference	Reference in text	Title
EN 16601-00-01	ECSS-S-ST-00-01	ECSS system – Glossary of terms
EN 16603-50-03	ECSS-E-ST-50-03	Space engineering – Space data links – Telemetry transfer frame protocol
EN 16603-50-04	ECSS-E-ST-50-04	Space engineering – Space data links – Telecommand protocols, synchronization and channel coding
EN 16603-70-41	ECSS-E-ST-70-41	Space engineering – Telemetry and telecommand packet utilization

Terms, definitions and abbreviated terms

3.1 Terms from other standards

For the purpose of this Standard, the terms and definitions from ECSS-S-ST-00-01 apply.

3.2 Terms specific to the present standard

3.2.1 Categories of operability

3.2.1.1 commandability

provision of adequate control functions to configure the on-board systems for the execution of nominal mission operations, failure detection, identification, isolation, diagnosis and recovery, and maintenance operations

3.2.1.2 compatibility

ability of two or more systems or components to perform their specified functions without interference

3.2.1.3 deactivation

capability to undertake planned operations to terminate the mission at the end of its useful lifetime

NOTE Terminate can mean to deactivate the spacecraft, to de-orbit it, or both.

3.2.1.4 flexibility

capability to configure and make optimum use of existing on-board functions, the capacity of the space-Earth communications links, and any redundancy built into the design in order to meet the reliability targets

3.2.1.5 observability

availability to the ground segment and to on-board functions of information on the status, configuration and performance of the space segment

3.2.1.6 testability

capability to test the on-board functions of the space segment including those that are “off-line”

NOTE “Off-line” means functions that do not form part of the current operational configuration.

3.2.2 Terms pertaining to critical functions

3.2.2.1 commandable vital function

vital function that is commandable by high-priority commands without the involvement of on-board software

3.2.2.2 high priority command

pulse command that is routed directly to hardware by means of an on-board command pulse distribution unit (CPDU)

3.2.2.3 high priority telemetry

telemetry that enables a reliable determination of the current status of vital on-board equipment and which is available under all circumstances

NOTE High priority telemetry can be managed by a mechanism that is independent of the one used for standard housekeeping telemetry and normally without any microprocessor involvement.

3.2.2.4 locally-critical function

function that, when executed in the wrong context (e.g. at the wrong time), can cause temporary or permanent degradation of the associated local functions, but does not compromise higher level functionality

3.2.2.5 mission-critical function

function that, when executed in the wrong context (e.g. at the wrong time), or wrongly executed, can cause permanent mission degradation

3.2.2.6 permanent degradation of space segment function

situation where a given on-board function cannot be achieved either on the nominal or on any redundant chain for the remainder of the mission lifetime

3.2.2.7 permanent mission degradation

situation where space segment functions or performances affecting mission product generation or primary mission objectives cannot be achieved either on the nominal or on any redundant chain for the remainder of the mission lifetime

3.2.2.8 temporary degradation of space segment function

situation where a given on-board function cannot be achieved either on the nominal or on any redundant chain for a limited period of time

3.2.2.9 temporary mission degradation

situation where space segment functions or performance affecting mission product generation or primary mission objectives cannot be achieved either on the nominal or on any redundant chain for a limited period of time

NOTE For example, a mission outage following transition to survival mode.

3.2.2.10 vital function

function that is essential to mission success and that can cause permanent mission degradation if not executed when it should be, or wrongly executed, or executed in the wrong context

3.2.2.11 vital telecommand

telecommand that activates a commandable vital function

3.2.3 Other terms

3.2.3.1 application process

on-board entity capable of generating telemetry source data and receiving telecommand data

3.2.3.2 authorization

right of an authenticated entity to perform a function or access a data item or data stream

3.2.3.3 chain

set of hardware or software units that operate together to achieve a given function

NOTE For example, an attitude and orbit control subsystem (AOCS) processor and its software and a set of AOCS sensors and actuators together constitute an AOCS chain.

3.2.3.4 confidentiality

property that information is not made available or disclosed to unauthorized individuals, entities or processes

3.2.3.5 control function

mechanism to maintain a parameter or a set of parameters within specified limits

NOTE A control function normally consists of a set of measurements and responses (commands) related according to a function, algorithm, or set of rules.

3.2.3.6 data integrity

property that the data has not been altered or destroyed in an unauthorized manner

3.2.3.7 data origin authentication

corroboration that the source of the data received is as claimed

3.2.3.8 datation

attachment of time information to telemetry data

NOTE This includes payload measurement data.

3.2.3.9 device telecommand

telecommand that is routed to and executed by on-board hardware

NOTE For example, a relay switching telecommand, a telecommand to load an on-board register.

3.2.3.10 housekeeping telemetry

telemetry provided for the purposes of monitoring the health and functioning of the space segment

3.2.3.11 loss of mission

state where the ground segment can no longer control the space segment (e.g. due to loss of contact), or where the space segment can no longer achieve the mission goals (e.g. due to anomalies)

3.2.3.12 memory

on-board data storage area

NOTE 1 This includes main memory and storage memory.

NOTE 2 Examples of memory are disk, tape, and bubble-memory.

3.2.3.13 mode

operational state of a spacecraft, subsystem or payload in which certain functions can be performed

3.2.3.14 mode transition

transition between two operational modes

3.2.3.15 on-board autonomy

capability of the space segment to manage nominal or contingency operations without ground segment intervention for a given period of time

3.2.3.16 on-board monitoring

on-board application of checking functions to a set of on-board parameters in conformance with predefined criteria

NOTE Monitoring functions include limit-checking, expected-value-checking and delta-checking.

3.2.3.17 on-board operations procedure

monitoring and control procedure that is stored on-board and whose activation is under ground segment control

3.2.3.18 on-board operations schedule

on-board facility for storing and releasing telecommands that were loaded in advance from the ground

NOTE In its simplest form, the on-board operations schedule stores time-tagged telecommands loaded from the ground and releases them to the destination application process when their on-board time is reached.

3.2.3.19 operability

capability of the space segment to be operated by the ground segment during the complete mission lifetime, whilst optimizing the use of resources and maximizing the quality, quantity, and availability (or timeliness of delivery) of mission products, without compromising space segment safety

3.2.3.20 operations

activities undertaken by the ground and space segments in order to ensure the timely provision of mission products or services, recover from on-board contingencies, carry out routine maintenance activities and manage on-board resources in order to maximize the provision of mission products or services and the mission lifetime

3.2.3.21 parameter

lowest level of elementary data item on-board

3.2.3.22 parameter validity

condition that defines whether the interpretation of a telemetry parameter is reliable and meaningful

NOTE The angular output of a gyro only has a valid engineering meaning if the power to the gyro is “on”, while at other times the output is random. Such a parameter is deemed conditionally valid, with its validity determined from the power status.

3.2.3.23 peer-entity authentication

corroboration that a peer entity in an association is the one claimed

3.2.3.24 safe state

safe condition for a system, subsystem or payload

3.2.3.25 space segment status

information from which the operational status of the space segment is assessed and the criteria driving operational decisions are determined

3.2.3.26 survival mode

configuration of a spacecraft in which it can remain safely without ground segment intervention for a specified period

3.2.3.27 telecommand function

operationally self-contained control action initiated by telecommand that can comprise or invoke one or more lower level control actions

3.3 Abbreviated terms

For the purpose of this Standard, the abbreviated terms from ECSS-S-ST-00-01 and the following apply:

Abbreviation	Meaning
AOCS	attitude and orbit control subsystem
APID	application process identifier
CPDU	command pulse distribution unit
CPU	central processor unit
CRC	cyclic redundancy check
EEPROM	electrically erasable programmable read-only memory
FDIR	failure detection, isolation and recovery
GPS	global positioning system
I/O	input/output
ID	identifier
MAP	multiplexed access point
OBT	on-board time
RAM	random access memory
RF	radio frequency
RFI	radio frequency interference
RFP	request for proposal
TT&C	telemetry, tracking and command
UTC	universal time coordinated

3.4 Conventions

Some requirements introduce quantities for which values cannot be defined across the board, but only on a mission-by-mission basis (e.g. time intervals or response times). These are termed mission constants and are identified within this Standard in angular brackets.

NOTE For example, <TC_VERIF_DELAY>

Example values are indicated in some cases. These mission constants are summarized in Annex A.

4

General requirements

4.1 Introduction

This clause contains general (high-level) requirements that pertain to the different categories of operability identified in clause 3.2.1. The requirements can be applied to missions of all classes (e.g. science, telecommunications or Earth observation) and orbit-type (e.g. geostationary, low-Earth orbiting or interplanetary).

4.2 Observability

- a. The space segment shall provide visibility of its internal status, configuration and performance to the ground segment in conformance with the level of detail and the time delays specified for all routine and specified contingency operations, including subsequent diagnostic activities.

NOTE 1 For detailed operability requirements reflecting these objectives, refer to clause 5.2.

NOTE 2 Specified contingency operations are derived during the failure analysis performed in the mission development process (e.g. the failure modes, effects and criticality analysis (FMECA)).

4.3 Commandability

- a. The control functions (telecommands) provided at each level of the system hierarchy shall be capable of achieving the mission objectives under all specified circumstances.

NOTE 1 This can include the use of redundant equipment to meet the overall system reliability requirements.

NOTE 2 Detailed operability requirements reflecting these objectives appear in clause 5.5.

4.4 Compatibility

- a. The space segment shall conform to all on-board design standards specified for the mission in order to ensure compatibility with the specified ground systems.
- b. The space segment design shall be such that its operation is not constrained by, nor adversely constrains, the availability or capacity of the space-Earth communications links.

4.5 Safety and fault tolerance

- a. No single command function executed at the wrong time or in the wrong configuration shall lead to the loss of the mission.

NOTE For a mission-critical command function, this can be ensured by the provision of two independent commands, both to be executed (e.g. ARM and FIRE).

- b. Except for explicitly agreed single point failures, the capability shall be provided to recover all on-board functions after a single failure within a specific function.

NOTE The impact of several non-correlated failures occurring at the same time has to be assessed at mission-level.

- c. No single unintentional ground command or failure in one space segment element shall cause a failure in another space segment element.
- d. The design of the space segment failure detection, isolation and recovery (FDIR) function shall be such that all anticipated on-board failures can be overcome either by autonomous on-board action or by clear, unambiguous and timely notification of the problem to the ground segment.
- e. The FDIR design shall ensure that the space segment is safe without ground segment intervention for the specified duration in the presence of a single failure.
- f. No reconfiguration of the spacecraft shall lead to a configuration where new single point failures are introduced.

NOTE With the exception of reconfigurations that are triggered on-board as the result of genuine failures.

4.6 Flexibility

- a. All authorized combinations of prime and redundant equipment shall exhibit the same operational characteristics.

NOTE 1 This requirement does not prevent a change of calibration data, but it precludes different operational procedures.

NOTE 2 This does not include any reduced redundancy that exists following a failure.

- b. The capability shall be provided for the ground segment to allocate which of the redundant units are included in the nominal chain and which in the redundant chain.

NOTE 1 This enables redundancy to be restored without reconfiguring the on-board hardware and also enables a failed unit to be removed from both the nominal and redundant chains while maintaining the rest of the redundancy of the chain.

NOTE 2 Software-selectable units, rather than hardware, are more suitable for use where the extent of cross-strapping provided is determined from the reliability analysis.

- c. Any selection of prime or redundant equipment shall be reversible.

NOTE This implies that the space segment design supports switching between prime and redundant equipment in both directions.

- d. For each on-board function, there shall be at least one alternative configuration that can achieve the same function using different on-board units.

- e. On-board functions shall have well-defined inputs and outputs that are accessible from the ground for workaround solutions in case of contingency operations.

NOTE Whilst inputs to on-board functions can be modified from the ground (e.g. threshold settings), this does not include the manipulation of on-board measurements.

- f. On-board storage and buffer areas should be resizable to cater for non-nominal mission events.

NOTE There can be operational restrictions on how this is achieved.

- g. The allocation of budgets for on-board resources shall provide the specified spare capacity for each subsystem and each payload.

NOTE 1 For example, mass memory, power, fuel.

NOTE 2 This spare capacity is provided in order to ensure flexibility during the mission.