ECSS-E-ST-70-11C Rev.1 DIR1
5 July 2024

Space engineering

Space segment operability

This Draft is distributed to the ECSS community for Public Review.
NOTE: The Tailoring guideline in Table B-1 will only be updated after the Public Review.
Duration: The 8-weeks duration of the review was extended to account for the summer vacation period.

Start of Public Review: 8 July 2024
End of Public Review: 20 September 2024

DISCLAIMER (for drafts)
This document is an ECSS Draft Standard. It is subject to change without any notice and may not be referred to as an ECSS Standard until published as such.

ECSS Secretariat
ESA-ESTEC
Requirements & Standards Section
Noordwijk, The Netherlands

Foreword

ECSS is a cooperative effort of the European Space Agency, national space agencies and European industry associations for the purpose of developing and maintaining common standards. Requirements in this Standard are defined in terms of what shall be accomplished, rather than in terms of how to organize and perform the necessary work. This allows existing organizational structures and methods to be applied where they are effective, and for the structures and methods to evolve as necessary without rewriting the standards.

This Standard has been prepared by the ECSS-E-ST-70-11C Rev.1 Working Group, reviewed by the ECSS Executive Secretariat and approved by the ECSS Technical Authority.

Disclaimer

ECSS does not provide any warranty whatsoever, whether expressed, implied, or statutory, including, but not limited to, any warranty of merchantability or fitness for a particular purpose or any warranty that the contents of the item are error-free. In no respect shall ECSS incur any liability for any damages, including, but not limited to, direct, indirect, special, or consequential damages arising out of, resulting from, or in any way connected to the use of this Standard, whether or not based upon warranty, business agreement, tort, or otherwise; whether or not injury was sustained by persons or property or otherwise; and whether or not loss was sustained from, or arose out of, the results of, the item, or any services that may be provided by ECSS.

Published by: ESA Requirements and Standards Section
ESTEC, P.O. Box 299,
2200 AG Noordwijk
The Netherlands

Change log

	Change log for Draft development
Previous steps	
DFRECSS-E-ST-70-11C Rev.1 DFR1 2 July 2024	DFR released by E-70 TAAR on 4 July 2024
Current step	
ECSS-E-ST-70-11C Rev.1 DIR1 5 July 2024	Public Review 8 July – 20 September 2024 Duration of the Public Review
Next Steps	
DIR + impl. DRRs	Draft with implemented DRRs
DIR + impl. DRRs	DRR Feedback
DIA	TA Vote for publication
DIA	Preparation of document for publication (including DOORS transfer for Standards)
	Publication
	Change log for published Standard (to be updated by ES before publication)
ECSS-E-70-11A 5 August 2005	First issue
ECSS-E-70-11B	Never issued
ECSS-E-ST-70-11C 31 July 2008	Second issue Editorial changes to conform to the ECSS template, including renumbering of the requirements
ECSS-E-ST-70-11C Rev.1 DIR1 5 July 2024	Second issue, Revision 1 Changes with respect to ECSS-E-ST-70-11C (31 July 2008) are the following and identified in the document with revision tracking. **Main changes are:** • Xxxxxx • Yyyyyyy

Table of contents

Tables

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 specification 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.

This standard covers the operability requirements that typically apply to missions. Each mission needs to tailor this standard in accordance with their operational need. Based on the operational function required, tailoring implies a selection of the applicable standardised requirements and adding any mission specific requirements.

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.

ECSS-S-ST-00-01	ECSS system – Glossary of terms
ECSS-E-ST-50-03	Space engineering – Space data links – Telemetry transfer frame protocol
ECSS-E-AS-50-24	Adoption Notice of CCSDS 231.0-B, TC Synchronization and Channel Coding
ECSS-E-AS-50-25	Adoption Notice of CCSDS 232.0-B, TC Space Data Link Protocol
ECSS-E-AS-50-26	Adoption Notice of CCSDS 232.1-B, Communications Operation Procedure-1
ECSS-E-ST-70-41	Space engineering – Telemetry and telecommand packet utilization

3 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 essential telecommands

telecommands that are distributed 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 telecommand

telecommand that activates a vital function

3.2.3 Other terms

3.2.3.1 application process

process that is in charge of executing functions on-board, either autonomously or remotely initiated

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 autonomous function

function implemented in on-board autonomy

3.2.3.4 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.

3.2.3.5 confidentiality

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

3.2.3.6 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.

3.2.3.7 data integrity

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

3.2.3.8 data origin authentication

corroboration that the source of the data received is as claimed

3.2.3.9 datation

attachment of time information to telemetry data

NOTE This includes payload measurement data.

3.2.3.10 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.

3.2.3.11 telemetry

Engineering or payload or science data generated on-board

3.2.3.12 engineering telemetry

data generated on-board for the purposes of monitoring the functioning and the health of the space segment

3.2.3.13 housekeeping telemetry

cyclic engineering telemetry sent to ground

3.2.3.14 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)

3.2.3.15 on-board memory

logical memory space

NOTE The on-board memories can potentially be managed by different on-board processors. The mapping between the on-board memories and the physical memories is out of the scope of this Standard.

3.2.3.16 on-board data storage

on-board memory used to maintain data generated by application processes on-board

3.2.3.17 mode

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

3.2.3.18 mode transition

transition between two operational modes

3.2.3.19 on-board autonomy

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

3.2.3.20 on-board function

lowest level of aggregation of spacecraft capability which can be operated independently

3.2.3.21 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.

3.2.3.22 on-board operations procedure

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

3.2.3.23 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.

3.2.3.24 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

3.2.3.25 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

3.2.3.26 parameter

data item or data structure on-board that is considered elementary for operations

3.2.3.27 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.

3.2.3.28 peer-entity authentication

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

3.2.3.29 report

self-contained item made of telemetry data aggregated together in order to simplify and optimise their distribution, storage, transmission and processing

3.2.3.30 safe mode

S/C operating mode guaranteeing the spacecraft safety, that can be autonomously sustained for a specified period of time and in which permanent communications with ground are available to the operators to perform the recovery procedures

NOTE A specified period of time is a period of time significantly longer than the ground reaction time.

3.2.3.31 safe state

safe condition for a system, subsystem or payload

3.2.3.32 space segment status

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

3.2.3.33 survival mode

S/C operating mode guaranteeing the spacecraft safety without permanent communications with ground, that can be autonomously sustained for a specified period of time in case the safe mode conditions cannot be reached.

NOTE 1 Survival mode might imply unavailability of specific functionality (e.g. 3-axes attitude stabilisation), severe constraints in the communication links with ground (e.g. intermittent TM/TC access, no TM link), thus implying extremely complex recovery procedures.

NOTE 2 A specified period of time is a period of time significantly longer than the ground reaction time

3.2.3.34 telecommand

self-contained data item issued by ground containing one or more commands to execute on-board.

NOTE Telecommands and commands are called requests and instructions in the PUS.

3.2.3.35

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).

NOTE This standard does not address specific requirements on relay communications (multi-spacecraft communications)."

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 monitoring and control functions 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 operations shall not be constrained by, nor adversely constrain, the availability or capacity of the space-Earth communications links.

NOTE This means the operation of the communications link is decoupled from other platform/instrument operations.

b. The space-ground communication links shall provide the capacity and availability to support all nominal and anticipated contingency operations.

4.5 Safety and fault tolerance

a. No telecommand executed at the wrong time or in the wrong configuration shall lead to the loss of the mission.

NOTE For a mission-critical on-board function, this can be ensured by the provision of two independent telecommands, 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.

c. No single unintentional telecommand addressed to one on-board function shall cause a failure in another on-board function.

d. 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. No autonomous on-board reconfiguration shall lead to an unprotected state.

NOTE 1 An unprotected state is where the FDIR is disabled.

NOTE 2 An ultimate fallback mode after multiple reconfiguation is considered an exception.

f. The spacecraft shall provide the capability to update any operational context data in an operationally safe and consistent way.

NOTE This means that during updates of operational context data there will be no intermediate state that invalidates the functionality of any on-board autonomy.

g. The process of updating the operational context data shall be independent of the current on-board configuration.

NOTE This means that the user is able to perform partial updates in the context data.

4.6 Flexibility

a. All supported 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. The spacecraft shall provide the capability to overwrite the current live selection of prime and redundant equipment, and to reversibly switch over usage between prime and redundant units.

NOTE This implies that the space segment supports switching between prime and redundant equipment in both directions. This is typically used to test redundant units in flight, or to return to operations a unit previously declared failed by an on-board surveillance.

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. All parameters used for autonomous operations shall be able to be updated by telecommand and available in engineering telemetry, without requiring ground use of on-board software patch and dump commands.

NOTE Example parameters include thresholds for limit checking or thresholds and biases for attitude control.

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

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

g. The spacecraft shall provide the cabability to determine, at any point in the mission and with the specified accuracy, the remaining on-board resources that impact on mission lifetime.

NOTE 1 This includes: remaining propellant, maximum solar array power generation, maximum battery capacity, remaining coolant for instruments (if applicable).

NOTE 2 The capability to determine the remaining on-board resources can be achieved using on-board engineering telemetry and associated ground processing algorithms.

h. The on-board resource usage associated to given configurations of the spacecraft and its payloads, subsystems and units shall be deterministic.

NOTE Examples include power consumption and data generation rate.

4.7 Testability

a. The spacecraft shall provide the capability to perform end-to-end tests of any on-board application process, which can be exercised under ground control.

NOTE For example, an “are you alive” function which generates a response for testing the end-to-end connection between the ground and an application process.

b. For test purposes, the capability shall be provided to operate redundant on-board equipment in an “off-line” manner.

NOTE 1 Off-line means in parallel with, but without any disturbance to, the prime equipment.

NOTE 2 This capability can be unfeasible if the redundant unit has an unacceptable disturbing influence such as in the case of a momentum wheel.

c. The capability should be provided to confirm the health of a currently unused unit prior to operational utilization.

NOTE This applies in particular to units that are vital for the health and control of the space segment. The selection of units is to be made on a case-by-case basis, taking into account the impact on the space segment design (e.g. the telemetry definition).

d. The capability shall be provided to load and check redundant memory prior to operational utilization.

e. Entering a test mode shall not require or imply disabling of fault management functions.

f. No fault management function shall trigger on offline data generated by a unit operating in "off-line" mode.

NOTE Offline data is data not used by the on-board control or FDIR monitoring loops.

4.8 Deactivation

a. On-board resources shall be provided for configuring the spacecraft into a safe state at the end of its life.

NOTE 1 This can include de-orbiting (essential for LEO spacecraft) or bringing the spacecraft to a graveyard orbit (GEO spacecraft).

NOTE 2 Safe state means safe for the space environment.

b. The capability shall be provided to completely deactivate the spacecraft at the end of its life.

NOTE This can include the removal of all internal energy sources, e.g. power and fuel.

5 Detailed requirements

5.1 Introduction

Requirements in this clause are grouped according to function, in contrast to Clause 4 where they are grouped according to operability class. It follows therefore that the requirements are only applicable if the corresponding function is actually implemented on-board.

5.2 Mission-level

5.2.1 Security

a. The space segment shall provide a level of security commensurate with the mission needs.

NOTE 1 Security can include such measures as the:

- confidentiality of each data stream produced;
- authentication of each telecommand received;
- authorization of each telecommand received.

NOTE 2 It is recommended to implement the CCSDS Space Data-Link Layer Security Protocol Standard [CCSDS 355.0-B] (Baseline Mode for Telecommand Authentication – Annex E) and CCSDS SDLS Extended Procedures Standard [CCSDS 355.1-B] (Baseline Implementation Mode – Annex D). Refer also to the CCSDS SDLS Protocol Summary of Concept and Rationale [CCSDS 350.5-G], which presents the concept and rationale of the CCSDS.

b. The space segment shall ensure continued access to both the telemetry and telecommand transmission functions in the presence of specified external influences outside the control of the mission control team.

NOTE The external influences to be accommodated are identified during the spacecraft design phase, i.e. at mission analysis level. They generally include RFI and adverse weather conditions. However, other influences, such as meteorite impacts or malicious dazzling of the uplink, clearly cannot be accommodated.

c. The space segment shall ensure the recovery of access to both the telemetry and telecommand transmission functions after all specified space and ground segment configuration changes.

5.2.2 Uplink and downlink

a. Different downlink bandwidths shall be allocated to different classes of data using physical channels and virtual channels.

b. The assignment of virtual channels to different data classes shall not be changed during the mission.

NOTE 1 Data classes means distinct data streams, such as real-time housekeeping telemetry, science data or playback data rather than different packet types within the same stream.

NOTE 2 Assignation of virtual channels to data types (i.e. real-time TM, playback, HPTM, CEL) is agreed with the Operator.

c. The allocation of bandwidth to different virtual channels shall be modifiable during the mission.

d. The capability shall be provided to transmit real-time and deferred telemetry data simultaneously.

5.3 Telemetry

5.3.1 Telemetry data

a. Throughout all mission phases, engineering telemetry data shall be provided for the ground segment to determine the status, health and performance of the spacecraft subsystems and payloads and to monitor the execution of nominal and anticipated contingency operations, independently of telecommand history on-board actions or previous telemetry.

NOTE This requirement covers the information to be telemetered for the purpose of both ground testing and in-flight operations.

b. The data specified in requirement 5.3.1a shall include sensor readings, register readouts, equipment status (including power status), function status, reports of on-board events and actions taken by autonomous functions, and processor and memory auto-test results.

c. The data specified in requirement 5.3.1a shall be telemetred to the ground segment in a complete, unambiguous, and timely manner.

d. Event-based reporting shall be achieved by means of dedicated event report packets (progress or anomaly reports) which are generated on-board, e.g. by a failure detection and recovery function.

e. The design of telemetry reporting mechanisms and of the telemetry report packets themselves shall be such that the utilization of the downlink bandwidth does not adversely affect the availability of other operational information to the ground segment.

f. Status information in engineering telemetry shall be provided from direct measurements from operating units rather than requiring derivation from secondary effects.

NOTE This is particularly essential for the status of all on-board switches.

g. The information required to determine the preconditions for the switching of on-board equipment and units are acquired independently.

NOTE 1 This means precondition information is not dependent on the status of the equipment or unit to be switched.

NOTE 2 To comply with this requirement, power status and thermal data used prior to unit switch-on are managed at a higher level.

NOTE 3 This provides the capability of monitoring and assessing the status of a unit even when it is switched off.

h. The values of telemetred parameters shall be self-contained.

NOTE This precludes, for instance, the telemetring of delta-changes or status changes.

i. If operationally-significant parameters monitored on-board (e.g. pyro currents) can change value at a frequency in excess of the telemetry sampling frequency, the event shall be memorized and the memorized value telemetred.

j. The resolution and range of analogue telemetry parameters shall be such that monitoring can be performed in all nominal and anticipated contingency situations.

k. The state of all mission critical functions shall be observable by at least 2 independently obtained measurements.

l. Engineering telemetry shall be provided to enable detection and diagnosis of any failure identified during the failure analysis phase (e.g. as defined in the FMECA) at least down to function or equipment level.

m. Where telemetry measurements are processed on-board, the capability shall be provided to downlink the raw data to the ground segment, on request.

NOTE For example, AOCS sensor data.

n. For units that can be operated in parallel within a given subsystem independent and unambiguous engineering telemetry shall be provided to enable the evaluation of the status of each unit.

NOTE 1 For example, this refers to hot redundant units or subsystems where prime and redundant units can be activated/operated in parallel.

NOTE 2 This refers not only to periodic housekeeping telemetry, but also to other telemetry" packets, such as events, to allow to distinguish among the two units.

o. For elements in redundancy, the loss or failure of one chain shall not prevent access to the telemetry of the other chain.

p. Any packet carrying measurement and performance information for a unit shall also contain the information necessary to calibrate and to determine the validity of the contained data.

q. Housekeeping telemetry parameters shall be sampled at a frequency ensuring that no information of operational significance, for all nominal and contingency operations, is lost.

r. All onboard parameters contributing to the interpretation of a parameter shall appear together with the parameter in the same packet.

NOTE As an example, this is applicable for synthetic parameters which are calculated using other parameters, conditionally valid parameters, or deduced parameters). This is to avoid problems that occur due to the absence of contributing packets, or due to inconsistencies caused by time differences between the contributing packets.

s. A telemetry parameter shall always have the same structure and interpretation, even if it appears in different telemetry source packets.

t. The location of a parameter within a non-variable telemetry source packet shall be fixed and derivable from an implicit knowledge of the packet structure.

u. If a parameter is super-commutated in a telemetry source packet, then the parameter shall be sampled regularly in time.

NOTE A super-commutated parameter is one that appears more than once in a packet.

v. The design of housekeeping telemetry source packets shall not use sub-commutation.

NOTE A sub-commutated parameter is one that does not appear (at a given location) in each a packet, but only in every n-th packet.

w. Within a given virtual channel, engineering telemetry packets originating from the same APID shall always be delivered to the ground segment in the same sequence as they are generated on-board.

NOTE This does not apply across separate retrievals from on-board storage, where the original chronological order is not always retained.

x. The data needed to determine the status, health and performance of the spacecraft subsystems and payloads and to monitor the execution of nominal and anticipated contingency operations, shall be reported to ground exclusively as part of engineering telemetry packets.

NOTE Engineering telemetry is processed by the ground control system. However, most science telemetry is not processed by the ground control system.

y. High priority engineering telemetry enabling a reliable determination of the current status of the vital on-board computer equipment, critical Latching Current Limiters and Telemetry Tracking and Command status under all circumstances shall always be available for real-time downlink whenever at least one transmitter is active.

NOTE 1 This requirement includes the cases where the on-board application software is not running.

NOTE 2 This function is typically hardware-generated to ensure certain independence from the on-board software.

z. The value of an engineering telemetry parameter shall be transmitted in contiguous bits within one packet.

aa. All telemetry packets generated, with the exception of idle packets, time packets and high priority telemetry packets, shall be available for storage on-board until deleted by ground or overwritten as part of cyclic files, regardless of the virtual channel used for transmission.

NOTE Idle packets, time packets and high priority telemetry packets, are not be stored on-board, but are only available in the real-time downlink.

bb. All on-board Application Processes shall initiate the delivery of the telemetry which they generate in chronological order, based on generation time.

cc. The engineering telemetry configuration including generation, storage and downlink shall not require dynamic management by ground during nominal operations.

NOTE This implies sufficient margin on the satellite design to allow generation of all telemetry required to perform all nominal operations including routine maintenance activities.

dd. Idle frames shall be downlinked in a dedicated virtual channel.

NOTE 1 Idle frames are used exclusively to occupy unused downlink bandwidth.

NOTE 2 Idle packets are exclusively used to complete a frame already containing a meaningful packet which, otherwise would not be down-linked in an acceptable time (e.g. last packet of a dump in a dedicated virtual channel, infrequent packet production by the on-board software, etc.).

ee. Telemetry data shall take priority over idle frames and idle packets when occupying the full downlink bandwidth.

NOTE In particular, idle frames and idle packets are not to be interleaved with other packets, as long as there is data to be downlinked (e.g. during packet store dumps).

ff. The spacecraft shall provide ground the means to verify completeness of the downlinked telemetry data independently of the route used to transmit them.

gg. Telemetry storage configuration and data shall be preserved in case of safe mode and in case of a reconfiguration of the unit implementing the on-board storage and retrieval subservices.

NOTE 1 A full loss of power scenario can be considered an exception.

NOTE 2 This is applicable regardless of the storage method and medium, i.e. for data stored in packet stores and/or files.

hh. After safe mode or unit reconfiguration, the preserved telemetry storage configuration and data shall be accessible using the standard means of the on-board storage and retrieval subservices.

ii. All on-board storage shall remain functional and accessible during and after the safe mode or unit reconfiguration without need of ground intervention.

NOTE 1 A full loss of power scenario can be considered an exception.

NOTE 2 Independent of the storage method and medium, i.e. for data stored in packet stores and/or files.

5.3.2 Diagnostic mode

a. For anomaly investigation purposes, the capability shall be provided for the ground segment to select a set of housekeeping telemetry parameters to be sampled at a high rate.

b. For diagnostic purposes the spacecraft shall provide the capability to generate housekeeping telemetry packets reporting any on-board parameter at the same frequency as their sampling rate.

c. The capability shall be provided to sample a given housekeeping telemetry parameter at a configurable sampling rate down to a minimum sampling interval of <DIAG_MIN_INTERV>.

d. The capability shall be provided to record diagnostic mode data on-board for later retrieval by the ground segment.

NOTE For example, by using the ECSS-E-ST-70-41 on-board storage and retrieval service (see clause 5.8.8 for additional information).

5.3.3 Data compression

a. For missions that implement data compression on-board, the compression performance and uncertainty shall be documented.

NOTE Data compression is typically applied to payload data on-board before downlink to ground. The documented performance and uncertainty allows ground to predict the downlinked data volume.

5.4 Datation and synchronization

a. The space segment shall provide timing information such that the correlation on ground of the on-board time with UTC can be maintained with an accuracy better than <TIME_CORREL_ACCUR> over a period of <TIME_CORREL_PERIOD>.

NOTE The operations concept and routine ground station pass profile is relevant to this requirement.

b. The spacecraft shall provide the capability for ground to set the on-board time by telecommand.

c. On-board time shall be monotonically increasing across all spacecraft modes, including standby and survival modes.

NOTE Exceptions to this requirement may be agreed in case of need (e.g. In the case of a ground commanded OBT maintenance TC)..

d. All on-board functionality requiring timing information shall be synchronized with a single Central Time Reference.

NOTE 1 This applies to redundant units activated in parallel to the operated ones (e.g. redundant Star Tracker for checkout, processor in Service Mode).

NOTE 2 In addition to timing provided in telemetry, time can be used in functions like time-tagging of telecommands and running of application software.

e. When an application process using time synchronization has just been initialized, engineering telemetry shall be provided to notify the ground segment that time synchronization has not yet occurred.

f. After initialization of an application process using time synchronization, engineering telemetry shall be provided to notify the ground segment when time synchronization has been achieved.

g. For application processes using time synchronization, engineering telemetry information shall be provided to enable the ground segment to verify the state of the time synchronization.

h. No on-board clock shall wrap-around during the mission lifetime.

i. All telemetry source packets should have an on-board generation time in their packet header.

NOTE Generation time is the time when the packet is created.

j. The on-board time, as telemetered to the ground segment, shall not wrap-around during the mission lifetime.

k. No on-board counter telemetered to ground segment shall wrap around within the agreed ground segment non-availability period.

l. It shall be possible to establish the original on-board sampling time of any spacecraft status telemetry parameter appearing in the telemetry source packets.

m. The capability shall be provided to determine the relative sampling time of any two parameters to an accuracy of <PARAM_REL_SAMPL_TIME>.

NOTE This also applies if the parameters appear in different packets, whether housekeeping or scientific in nature.

n. The on-board sampling time of a telemetry parameter in a non-variable content telemetry packet shall be derivable from the packet generation time by adding or subtracting an implicitly known time offset.

o. The total contribution of the on-board time system to the correlation of the on-board time with UTC shall not exceed <ONBOARD STABILITY> ms/day.

NOTE <ONBOARD STABILITY> is mission specific. It includes the uncertainties on the stability of the on-board clock.

p. The spacecraft shall provide the capability to synchronise the clock maintained by any unit with the on-board Central Time Reference.

q. If several time sources are present on-board, provided housekeeping telemetry shall allow ground to derive a precise correlation between the different time sources used on board.

NOTE Examples of onboard time references include GNSS time, OBC OBT, instrument OBT, etc.).

r. When a GNSS receiver is used to generate the on-board time reference, an on-board GNSS/OBT correlation mechanism shall be implemented, with periodic Housekeeping telemetry packets reporting the correlation to allow ground to perform a precise time correlation.

NOTE This requirement is specific for Missions with GNSS receiver (typically Earth Observation).

s. When a GNSS receiver proving time is used to generate on-board time reference, ground will be provided the capability to enable/disable the time synchronisation between the GNSS and the OBT via telecommand, even if the GNSS is not being used in the AOCS loop.

NOTE This requirement is specific for Missions with GNSS receiver (typically Earth Observation).

t. The system, including the AOCS controllers, shall perform nominally in the presence of backward and forward synchronisation/re-synchronisation of the OBT with the GNSS Time, whether commanded by ground or automatic, even when the GNSS is being used in the AOCS control loop.

NOTE This requirement is specific for Missions with GNSS receiver (typically Earth Observation).

u. When a GNSS receiver is used to generate on-board time reference and the synchronization with the GNSS is enabled, the OBT shall be able to synchronize to the GNSS time periodically at a rate compatible with the timing accuracy requirements of the mission.

NOTE This requirement is specific for Missions with GNSS receiver (typically Earth Observation).

v. The on-board system shall monitor and provide engineering telemetry to ground of the proper synchronisation of any on-board application time reference to the Central Time Reference.

w. Any on-board delays contributing to the correlation of the on-board time with UTC shall be documented.

x. When a GNSS receiver providing time is used to generate on-board time reference, leap seconds shall be reported and handled autonomously.

NOTE This means ground does not need to update on-board the offset between UTC and TAI.

5.5 Telecommanding

5.5.1 Telecommand function

a. Telecommands shall be available to command all on-board equipment and functions under all nominal and anticipated contingency conditions.

NOTE This implies the provision of "essential telecommands" (eTC, also known as high priority telecommands) to re-establish command processing in the event of processor failure.

b. If a telecommand executes more than one action, these actions shall be strictly operationally related, such that they constitute a single logical on-board function.

NOTE To comply with this requirement, a device telecommand cannot put a battery in trickle charge and at the same time switch on a heater, unless these operations are always strictly related.

c. A telecommand shall contain one, and only one, on-board function.

NOTE A telecommand that loads or starts an on-board schedule only executes a single function (load or start) irrespective of the number of telecommands contained in the load or schedule itself.

d. A telecommand shall have the same action definition for the complete mission duration.

NOTE This precludes the use of flip/flop commands.

e. The conditions under which a configuration-dependent telecommand can be sent (or cannot be sent) shall be determinable unambiguously from the housekeeping telemetry.

f. The execution of any telecommand shall not lead to permanent loss of telecommandinging capability.

NOTE This refers to the functional ability of the spacecraft to receive and process telecommands from ground.

g. Repetition of the same telecommand shall not result in any permanent degradation or loss of on-board functionality.

h. The capability shall be provided to command all on-board devices individually from the ground.

NOTE 1 If a device is normally commanded using a higher-level telecommand, this requirement specifies the capability for the ground segment to issue a device telecommand to be routed directly to that device.

NOTE 2 This does not imply the use of high-priority commands, but can be achieved using bus-level commands.

i. Redundancy switching at unit level shall not require changes in operational procedures / telecommands directed to the operational unit.

NOTE This allows previously loaded commands (e.g. mission timeline, OBCPs) to address the current operational unit. This implies a different method than that used for direct physical unit control.

j. The maximum execution duration of a telecommand shall remain unchanged for the entire duration of the mission.

NOTE This implies knowledge by the ground segment that a command has been successfully executed so that the next command can be initiated. This does not exclude the possibility that subsequent automated processes with a specified goal (bounded duration) are triggered by a telecommand, so long as the process can be monitored as specified in clause 5.3.1.

k. The value of telecommand parameter shall be transmitted in contiguous bits within one packet.

l. Changes to on-board parameters and configuration tables shall be implemented via a dedicated telecommand and not via a multi-purpose memory load telecommand.

NOTE This can include individually instantiated telecommands and reports using generic parameter access/report service.

m. Readouts of loaded on-board parameters and configuration tables shall be requested via a dedicated telecommand and not via a multi-purpose memory dump telecommand.

NOTE This can include individually instantiated commands and reports using generic parameter access/report service.

n. The on-board Telecommand Function shall be able to distribute commands at a minimum rate of <TC_DISTR_RATE> independently from the source and size of the telecommands.

NOTE 1 This is the minimum rate and is mission specific.

NOTE 2 The final distribution rate includes parallel commanding sources considered as part of a traffic scenario definition.

o. Each on-board Application Process shall support the execution of at least <TC_EXEC_RATE> commands per second.

NOTE 1 This is the minimum rate applicable to all application processes and is mission-specific and accounts for parallel commanding by independent sources (e.g. ground, Mission Timeline, OBCP, fault management autonomy).

NOTE 2 This is expected to be consistent with the outcome of a traffic scenario definition to be performed during the implementation phase, noting however that some application processes can accept higher rates as part of this analysis.

p. It shall be possible to issue essential telecommands directly from the on-board telecommand decoder, without the involvement of on-board software.

NOTE Critical functions accessed via essential telecommands can include for example:

- PM ON/OFF
- PM Reset
- Watchdog enable/disable
- Reconfiguration Module enable/disable
- Transmitter ON/OFF

q. The spacecraft shall provide the capability to support all essential telecommands by means of redundant and independent hardware implementation.

NOTE For example, this implies at least two telecommand decoders with independent hardware are provided in order to fulfil single point failure requirements.

r. The essential telecommands performing the same action shall be identical regardless of the commanding route.

s. The accuracy, precision and encoding of commandable on-board parameters shall be commensurate with the mission objectives.

NOTE This is to avoid that rounding errors impact operations.

t. For missions using the COP-1 protocol and associated AD service, the service shall be configured for the applicable in-orbit conditions avoiding to artificially limit the uplink rate.

NOTE 1 For the COP-1 protocol refer to ECSS-E-AS-50-26and CCSDS 232.1-B.

NOTE 2 This means that the AD service sliding windows are optimised for the in-orbit conditions.

u. The spacecraft shall be able to perform several operations in parallel without restricting ground commanding.

NOTE This implies for example that schedules executed on-board do not constraint the operations, e.g. rejecting a command sent to manage the on-board scheduler when that scheduler is releasing time tagged commands.

5.5.2 Critical telecommands

a. The capability shall be provided to implement critical telecommands via use of different categories.

NOTE For example, the use of an on-board operations procedure or the on-board schedule to execute a critical telecommand that is normally executed from the ground using a CPDU telecommand; the use of low-level commands to replace a nominal high-level function.

b. At least two separate command actions shall be used for the execution of mission-critical functions.

NOTE 1 This means an arm/safe or enable/disable command followed by an execute command.

NOTE 2 See clause 3.2.2 for the definition of telecommand criticality categories.

NOTE 3 An example where this requirement is applicable, is for commands for pyrotechnic devices.

NOTE 4 In the case of mission critical register load telecommands can have a separate execute command so that the loaded data can be verified prior to execution.

c. Register load telecommands that are mission-critical or vital in nature shall have a separate execute command so that the loaded data can be verified prior to execution.

d. Redundant telecommands shall be provided for all mission-critical and vital telecommands by means of a maximum diversity on-board routing, i.e. using on-board routes that share no common nodes or paths.

NOTE This can be achieved by using redundant equipment.

5.5.3 Telecommand transmission and distribution

a. The on-board processing and distribution of telecommands shall ensure that no restrictions arise when the ground segment transmits telecommands of any type at the highest possible rate (i.e. making full use of the available uplink bandwidth).

NOTE 1 This includes the case where all commands are of the same type and to the same application process, e.g. a memory load.

NOTE 2 Sufficient resources are made available on-board to queue the telecommands that cannot be immediately processed, e.g. telecommands with long execution times such as copy.

b. The routing to, and execution of telecommands by, an application process shall not interfere with the routing and execution of other telecommands to other application processes.

NOTE For example, an extensive sequence of telecommands for the configuration of a payload, has no impact on the commanding of platform subsystems.

c. In order to be able to unambiguously identify the source of a telecommand (e.g. the ground or a given on-board application process), the source shall be explicitly indicated within the telecommand packet itself.

NOTE The source of telecommands released from an on-board schedule is the ground segment.

5.5.4 Telecommand verification

a. The spacecraft shall provide the capability to allow complete and unambiguous verification on-ground of on-board acceptance and execution of any telecommands sent from any source.

NOTE 1 This is expected to be achieved by an appropriate combination of dedicated telecommand verification reports and housekeeping telemetry.

NOTE 2 This includes the operation of e.g. non-packetised units on the bus and essential Telecommands processed directly by the hardware without software intervention.

NOTE 3 This includes positive (success) as well as negative (failure) verification.

b. Except for telecommands that are executed purely by hardware (e.g. CPDU commands), verification of the acceptance stage shall be provided for all telecommands.

c. The spacecraft shall provide the capability to disable the generation of verification reports of the successful acceptance and execution of any telecommand issued by ground.

NOTE This applies only to telecommand verification implemented by verification reports.

d. Verification telemetry shall be provided with a delay of less than <TC_VERIF_DELAY> with respect to the time of completion of the corresponding telecommand execution stage.

e. If a telecommand is invalid, it shall fail verification at the acceptance stage and shall not be distributed further.

NOTE For example, the length or CRC are wrong or the APID is invalid.

f. Failure in the acceptance or the execution of commands autonomousliy generated by an on-board application process shall be notified to the ground segment by means of anomaly event reports.

g. Verification of execution of any telecommand shall be possible using housekeeping data which are generated in all circumstances under which that telecommand is executed.

NOTE Examples are:

- A device telecommand verified by a hardware measurement that is directly telemetred without intermediate processing.
- A bi-level command verified by a status parameter.

h. If a telecommand results directly in one or more changes to the space segment configuration, these changes shall be reported in the housekeeping telemetry.

i. The effect of a telecommand shall be observable on the ground using telemetry data available under all circumstances under which the telecommand can be successfully executed.

NOTE To comply with this requirement, the effect of a telecommand affecting the status of on-board units involved in the generation or routing of telemetry is available in the “high priority” telemetry.

j. The execution of register load commands shall be confirmed by unique telemetry parameters dedicated to each commanded register, echoing exactly the currently loaded value.

k. Failure in the acceptance or the execution of commands issued by the ground shall always be notified to the ground.

l. A telecommand, whose effect was already achieved before its execution, shall be positively acknowledged.

5.6 Configuration management

5.6.1 Modes

a. For spacecraft management purposes, the spacecraft shall be able to support at least the following modes:

1. Pre-Launch Modes for configuration of the spacecraft for launch and ground testing;
2. Operational Modes ensuring the generation of mission products;
3. Safe Modes ensuring safety of all spacecraft subsystems and payloads.

b. The operational modes of the space segment and its payload, subsystems and units shall be clearly identified in terms of both hardware and software configurations.

c. Periodic housekeeping telemetry shall provide unambiguous identification of the subsystem modes.

d. It shall be possible to command any subsystem, unit or instrument into each of their pre-defined modes by means of a single telecommand function which initiates all the corresponding low-level actions necessary to establish the commanded mode.

NOTE For example, the on-board software could perform the following actions: configuration of the necessary hardware (e.g. sensors, actuators), activation of a default periodic telemetry configuration, and automatic processes required to achieve the objective of the mode.

e. The capability shall be provided to perform all routine maintenance activities for spacecraft units by using nominal modes and mode transitions without impact on the performance of the modes and mode transitions.

f. Mode transitions shall be reported using event telemetry packets.

g. All modes shall be defined such that, for any logical unit used in this mode, any serviceable combination of physical units is possible.

NOTE 1 Logical unit refers to the role of the unit in the redundancy scheme (i.e. nominal or redundant).

NOTE 2 Serviceable means that is not necessary to consider configurations that do not make sense (e.g. operating only on one wheel).

h. Execution of forbidden mode transitions shall be prevented on-board.

NOTE Forbidden mode transitions are mode transitions for which the spacecraft is not designed for, and protects against, or when the mode transition preconditions are not met.

i. The spacecraft shall provide the capability for ground to be able to force the execution of any forbidden mode transition.

NOTE 1 Such forcing of forbidden mode transitions by ground would be performed only in exceptional circumstances (e.g. end-of-life passivation).

NOTE 2 Execution of this forcing of forbidden mode transition voids requirements on spacecraft/equipment safety.

j. Whenever the spacecraft generates telemetry, the capability to continuously store it on-board shall be provided, independently of the mode of operation, including Safe Mode.

NOTE In Safe Mode it is sufficient to store engineering telemetry.

k. The spacecraft shall make available for use by on-board autonomy the operational mode of its subsystems and units.

l. The spacecraft shall not require any monitoring or commanding from ground during the Launch Phase, up to and including separation from the launcher.

m. The spacecraft shall generate and store engineering telemetry data, for the entire duration of the ascent and initial post-separation phase, until ground asserts control.

n. The spacecraft transmitters shall be autonomously activated as soon as the launcher and system constraints permit.

o. During the Commissioning Phase the spacecraft shall be able to be operated as foreseen in all operational scenarios.

NOTE This includes utilizing all spacecraft subsystems, early validation of specific mission modes, tracking for orbit determination, early trajectory maintenance and correction maneuvers, all operational communication links, health checks, etc.

p. The spacecraft shall support checkouts of payload instruments and relevant platform sensors, actuators, and mechanisms during non-operational science Phases.

5.6.2 On-board configuration handling

a. All on-board reconfigurations shall end with an unambiguously known and observable state of all involved elements (hardware and software).

b. The maximum duration of an on-board reconfiguration shall be deterministic.

c. Engineering telemetry shall be available for the ground segment to monitor all stages of an on-board reconfiguration.

d. The reconfiguration of on-board units or the switching between on-board functions shall not affect the status, the configuration, or the proper operation of any other unrelated unit or function.

e. Engineering telemetry indicating the cause of a single or multiple consecutive on-board reconfiguration shall be available to the Ground at the end of the last reconfiguration process.

f. The capability shall be provided to pre-configure selected units into consistent configurations prior to their selection as operational.

NOTE For example, the bolometer inhibition status of an infrared attitude sensor.

g. The capability shall be provided to trigger any on-board reconfiguration activities that put the space segment into a predefined safe state:

1. autonomously, and
2. by ground commanding.

h. After separation from the launcher, the space segment shall enter a state in which it can survive for a predefined period without ground segment support.

NOTE 1 For example, an automatic sequence triggered on detection of the separation.

NOTE 2 The duration of the period without ground support in critical mission phases <GRD_RSP_TIME_CRIT> is defined as part of mission design.

i. The space segment shall provide mechanisms to avoid or recover from any conflict that can arise from the execution of on-board autonomous actions and ground scheduled commands.

NOTE For example, the parallel execution of routine procedures and event-driven procedures.

j. At power up, restart and upon recovery from any power loss, the space segment electrical configuration (including all subsystems, units and instruments) shall be set into a known deterministic and reproducible state.

5.7 On-board autonomy

5.7.1 Introduction

On-board autonomy management addresses all aspects of on-board autonomous functions that provide the space segment with the capability to continue mission operations and to survive critical situations without relying on ground segment intervention.

The implementation of on-board autonomy depends on the specific mission requirements and constraints, and can therefore vary between a very low level of autonomy involving a high level of control from ground to a high level of autonomy, whereby most of the functions are performed on-board.

5.7.2 General autonomy

a. The space segment shall provide on-board autonomy management functions taking into account specific mission constraints and characteristics such as:

1. acceptable mission outage;

2. expected ground station coverage;

3. maximum unexpected ground segment non-availability period.

b. The spacecraft shall be able to autonomously continue nominal operations without the need for ground contact for a period of at least <NOM_OPS_PER> days, including failures covered by fail-operational autonomy.

NOTE 1 This period is independent of the maximum storage capacity for science data.

NOTE 2 For deep-space missions <NOM_OPS_PER> is 10 days plus maximum conjunction duration, if any. <NOM_OPS_PER> days is mission-specific.

c. The on-board autonomy management functions shall be capable of performing all operations to store mission products for an autonomy duration of <AUT_DUR_DATA>.

d. In case of an autonomously non-recoverable system failure on one or more uncorrelated on-board functions, the spacecraft shall be able to survive in Safe Mode without the need for ground contact for a period of at least <SAFE_TIME> days.

NOTE This means that FDIR is still active in Safe Mode. <SAFE_TIME> is mission specific. In particular, for deep-space missions <SAFE_TIME> days is recommended to be at least the maximum duration of solar conjunctions + 10 days.

e. During non-critical mission phases there shall be no requirement for the Ground to react in nominal or contingency cases in less than <GRD_RSP_TIME_NOM> hours.

NOTE The value for <GRD_RSP_TIME_NOM> is defined as part of the mission design.

f. It shall be possible for the Ground to enable and disable each individual autonomous function, whether routine or fault management.

g. During critical mission phases there shall be no requirement for the Ground to react in nominal or contingency cases in less than <GRD_RSP_TIME_CRIT> hours.

NOTE The value for <GRD_RSP_TIME_CRIT> is defined as part of the mission design.

h. The on-board autonomy shall be able to access any engineering telemetry.

NOTE 1 This explicitly means the central on-board autonomy function is able to access and process the content of the housekeeping reports generated by any on-board packetised unit.

NOTE 2 This includes in particular non-periodic event reports which can be used to trigger recovery actions at system or sub-system level, as a result of an anomaly occurred (and detected) in another subsystem and / or packetised unit.

NOTE 3 This includes housekeeping telemetry generated by the spacecraft subsystems and non-packetised data acquired by the data handling subsystem.

i. The spacecraft shall provide to the ground the capability to access and report any parameters used by any on-board autonomy function.

NOTE 1 This implies ground access to input and output parameter values used by the autonomy functions.

NOTE 2 Examples of such parameters include: thresholds and filters for limit checking, thresholds and biases for attitude control, fault management enable / disable statuses, input / output of orbit and attitude control functions, on-board control procedures internal variables, input output for OBCPs.

j. Any on-board autonomy process shall operate using only valid parameter acquisitions.

NOTE Invalid parameter acquisitions are data which are no longer relevant to the present spacecraft state. e.g. outdated acquisitions from switched off equipment that have not been refreshed.

k. For autonomous functions used both in nominal and safe/survival spacecraft modes, ground shall have the capability to enable/disable the function independently for nominal and safe/survival modes.

NOTE This includes FDIR functions.

l. For parameter-based surveillance, FDIR shall not trigger on a single sample of a parameter value.

NOTE Redundant readings or consecutive samples can be used.

m. FDIR surveillance limits shall be set to avoid false triggerings, while not compromising mission safety.

NOTE This means that the operating range of FDIR monitored on-board parameters is expected to have sufficient margin w.r.t. to the corresponding FDIR surveillance limits to avoid false triggering.

5.7.3 Autonomy for execution of nominal mission operations

For the execution of nominal mission operations, the following autonomy levels can be identified:

- execution mainly under real-time ground control;
- execution of pre-planned mission operations on-board;
- execution of adaptive mission operations on-board;
- execution of goal-oriented mission operations on-board.

These autonomy levels are summarized in Table 5-1.

Table 5-1: Mission execution autonomy levels

Level	Description	Functions
E1	Mission execution under ground control; limited on-board capability for safety issues	Real-time control from ground for nominal operations Execution of time-tagged commands for safety issues
E2	Execution of pre-planned, ground-defined, mission operations on-board	Capability to store time-based commands in an on-board scheduler
E3	Execution of adaptive mission operations on-board	Event-based autonomous operations Execution of on-board operations control procedures
E4	Execution of goal-oriented mission operations on-board	Goal-oriented mission re-planning

The corresponding requirements for on-board operations scheduling, on-board operations procedures and event-action coupling are addressed in clauses 5.8.5, 5.8.9 and 5.8.10, respectively.

5.7.4 Autonomy for mission data management

For mission data management, the following autonomy levels can be identified:

- essential mission data used for operational purposes can be stored on-board;
- all mission data can be stored on-board (science data and housekeeping data).

These autonomy levels are summarized in Table 5-2.

Table 5-2: Mission execution autonomy levels

Level	Description	Functions
D1	Storage on-board of essential mission data following a ground outage or a failure situation	Storage and retrieval of event reports Storage management
D2	Storage on-board of all mission data, i.e. the space segment is independent from the availability of the ground segment	As D1 plus storage and retrieval of all mission data

The corresponding requirements for on-board storage and retrieval are addressed in clause 5.8.8.

5.7.5 On-board fault management

5.7.5.1 Overview

The overall on-board fault management concept is based on the failure detection, isolation and recovery (FDIR) paradigm. This means that functions are implemented:

- to detect on-board failures and to report them to the relevant on-board units or subsystems and to the ground segment;
- to isolate the failure, i.e. to avoid the propagation of the failure and the deterioration of equipment;
- in some cases, to recover the on-board functions affected by the failure such that mission operations can continue.

5.7.5.2 General FDIR

a. The space segment shall provide FDIR functions that take into account the applicable operability requirements and constraints such as:

1. the autonomy requirements addressed in clause 5.7.2a,
2. system, subsystem, equipment and unit safeguarding needs, and
3. ground segment intervention conditions.

NOTE FDIR functions are those functions that implement the failure detection, isolation and recovery actions. The FDIR functionality is established at various levels within the space segment, e.g. at hardware and software levels. The implementation of the FDIR functions is based on specific system needs, e.g. specific time constants.

b. FDIR functions shall be implemented in a hierarchical manner in order to detect, isolate and recover failures at the lowest possible implementation level.

NOTE 1 For example, FDIR handling on an on-board data bus implying retries and subsequent error mechanisms in case these retries are unsuccessful.

NOTE 2 This requirement can imply a staggered recovery scheme based on retry functions (see also clause 5.7.5.4).

c. Failures that cannot be handled at a given level shall be handed over to the next higher operational instance, the highest instance being the ground segment.

d. Failure detection, isolation and recovery activities performed on-board shall be reported in an unambiguous manner to the ground segment.

e. The reporting of FDIR activities shall contain all information for failure analysis (e.g. time of occurrence, parameter out-of-limit, switching performed).

NOTE A time delay for this reporting can be accepted if, for example, the reporting uses an operational on-board processor.

f. <<deleted>>

g. Except for passive hardware functions that cannot be overridden (such as fuses), the capability shall be provided to enable and to disable any on-board FDIR function by telecommand.

NOTE For example, the inhibition of a latch-up detector or the bypassing of an auto-test function.

h. Where FDIR functions are based on several inputs (e.g. sensor readings, and unit status), which are independently tested to determine a failure condition, the capability shall be provided to enable and disable each such input by telecommand.

i. The ground segment shall be able to enable and disable each detection and recovery function in a consistent manner without having a detrimental effect on the overall system.

j. A single detected failure shall result in the triggering of a single surveillance.

NOTE This implies that functional overlap of surveillances is avoided and conditional monitoring applies.

k. The spacecraft shall provide the capability to generate and route to ground all engineering telemetry reports considered relevant for the ground analysis of a failure detected by on-board FDIR.

NOTE The requirement is addressing the generation and routing to ground of telemetry within the available bandwidth.

l. The spacecraft shall manage the available or failed status of each unit and report these statuses in telemetry.

m. The ground shall be able to update the available or failed status of each unit by telecommand.

n. In nominal spacecraft modes, an autonomous function disabled by ground shall remain disabled until re-enabled by ground.

NOTE In particular, the function is not be autonomously re-enabled upon routine mode transitions.

o. The on-board fault management shall avoid continuous toggling of the configuration of a unit between prime and the redundant element.

NOTE This is to avoid an endless loop condition.

p. Local reconfiguration to a unit or to a subsystem, which is suspected to be failed, shall not be performed autonomously.

NOTE This is to prevent infinite reconfiguration loops at low FDIR levels. In case of FDIR escalation, system-level triggers (e.g. reboot) can result in configurations using previously suspected units.

q. The spacecraft shall provide the capability to protect against unintended modification by Ground of FDIR monitored parameters and recovery actions.

NOTE This can be implemented by a two-step process involving disabling a protection before allowing the modification.

r. The spacecraft shall provide the capability to report to ground the definition of all on-board monitorings.

NOTE The generated reports include the identifier of the on-board monitorings and their complete definition (parameter being monitored, thresholds applied, filters applied and enable/disable status).

s. The statuses of all FDIR monitorings and recovery actions shall be available in cyclic housekeeping telemetry reports.

5.7.5.3 Failure detection

a. The space segment shall provide the means to detect and report any on-board anomaly condition.

NOTE This includes both hardware and software anomalies.

b. The capability shall be provided to monitor and to define out-of-limit conditions for essential on-board parameters (see clause 5.8.6).

c. Failure detection algorithms shall not repeat the generation of the same exception telemetry if the same failure is detected at each successive failure detection cycle.

d. All actions of operational significance taken by the on-board autonomy shall be reported to ground as part of the housekeeping telemetry.

NOTE 1 Any on-board anomaly condition is reported by means of events reports and can also be included in cyclic telemetry.

NOTE 2 Actions of operational significance are those that induce changes in the on-board configuration and / or require ground intervention.

e. Anomaly reports shall contain a unique identification of the anomaly, its time of occurrence, and a record of the input data to the anomaly detection function.

NOTE The record of the input data can range from a snapshot to a historical record.

f. The failure detection functions shall be independent from the nominal monitoring and control functions.

NOTE For example, an AOCS FDIR function using different sensors from those used by the nominal AOCS control function.

g. The capability shall be provided to detect failures in systems that are off line (i.e. not involved in any primary function) when this does not conflict with operational configurations or operational constraints.

h. Except for hardwired failure detection mechanisms, parameters of failure detection criteria (such as thresholds and number of failure repetitions) shall be modifiable by telecommand.

i. All units capable of performing self-checks shall report any detected failures.

j. The spacecraft shall provide the means to detect and report any failure that compromises operational integrity.

NOTE Examples include late scheduled command execution and failure of on-board TC file execution.

5.7.5.4 Failure isolation

a. The space segment shall provide functions to isolate the failed unit or subsystem, to avoid failure propagation and deterioration of the impacted equipment.

b. For failures whose resolution implies safeguarding of system functions, the offending unit, subsystem or function shall be disabled or switched off.

NOTE For example, avoidance of power drain by a failed unit to a level where the ability to provide power to the rest of the spacecraft (a vital system function) is endangered.

c. For failures whose resolution does not imply the safeguarding of system functions, hierarchical isolation steps shall be applied (e.g. protocol-level retries or on-board operations procedures) before removal of the failed unit from the operational configuration.

NOTE The hierarchical isolation steps can include:

- command retries and telemetry readback;
- appropriate equipment switching, i.e. the selection of redundant equipment by

telecommand or by on-board operations procedures, including functional verification;

- application of delay times before switching off the failed equipment.

5.7.5.5 Failure recovery

a. If an on-board failure detection function identifies an anomalous situation, it shall trigger autonomous recovery actions consistent with the specific mission needs without ground segment intervention.

b. Any potential conflict between failure recovery activities and nominally ongoing on-board commanding activities shall be identified and managed.

NOTE This can imply suspending the on-board operations schedule and currently active on-board operations procedures.

c. The safety of the spacecraft, subsystem or payload shall be guaranteed even in case of a failure in the performance of any autonomous recovery action

d. The end configuration of the spacecraft as set up by the FDIR function in response to the triggering of a failure monitor shall be deterministic.

5.7.5.6 Fault management

a. When enabled, Safe Mode shall guarantee the achievement of a stable safe condition from any possible initial condition.

NOTE Safe Mode has an autonomy time without ground contact of at least <SURV_TIME>.

b. The spacecraft shall enter a safe state if any hazard exists that affects spacecraft or payload health or mission objectives.

c. The spacecraft shall only enter safe or survival mode if a vital or spacecraft-level critical function is affected.

NOTE In particular, this implies a robustness of the implementation of the hierarchical FDIR to cope with minor errors without causing entry into safe or survival mode.

d. Recovery from safe mode shall be undertaken under ground control.

e. When triggered by ground, the spacecraft shall autonomously transition from safe mode back to a nominal mode.

NOTE Such a transition is triggered after isolation of any failed or suspected failed unit.

f. The Safe Mode final condition shall be defined such that up- and downlink communication with the Ground is permanently guaranteed.

g. In case of conditions preventing the spacecraft to reach a stable Safe Mode the spacecraft shall enter Survival Mode.

NOTE Examples of conditions preventing transition to Safe Mode are: solar flare preventing nominal star tracker operations, corruption of ephemeris kept on-board, multiple failures.

h. The spacecraft shall support automatic transition from Survival to Safe Mode.

i. Ground shall be provided with the capability to enable / disable the automatic transition from Survival to Safe Mode, for immediate effect as well as for the next spacecraft reconfiguration.

j. If the automatic transition between Survival and Safe Mode is enabled, the spacecraft shall keep attempting to perform this transition.

k. The number of different Safe/Survival Mode configurations shall be minimised by spacecraft design.

l. The entry into Safe/Survival Mode shall include all payload re-configuration activities necessary to put the payload in a safe and recoverable mode.

NOTE Payload reconfiguration activities include, for example, park/stow of instruments needed to react to changes of attitude, activation of thrusters.

m. In case of entry into Safe/Survival Mode the spacecraft shall transmit to Ground the necessary set of engineering telemetry packets to allow unambiguous and rapid identification of the Safe/Survival Mode condition by ground.

n. After transition into Safe or Survival Mode, the reason for the transition shall be accessible in telemetry sent to ground in real time as well as stored on-board for later retrieval by ground.

NOTE The history of the event-driven reports produced before and after the detection of the failure condition are used to reconstruct the cause of the entry.

o. It shall be possible to enable and disable autonomous entry into Safe and Survival mode, with enabled being the default status.

NOTE Disabling the safe/survival mode entry is a critical last-resort activity to be assessed in exceptional circumstances by Ground.

p. To protect against unintentional disabling of Safe/Survival autonomous entry a protection mechanism shall be implemented on-board.

NOTE This can be achieved by the use of two telecommands (e.g. unlock then disable).

q. The enable/disable status of safe/survival mode autonomous entry shall always be available in cyclic telemetry.

r. No nominal operation shall require inhibition of the safe/survival Mode nor a forced entry into safe/survival Mode.

NOTE This applies also to critical operations in the nominal timeline

s. The transition to a safe/survival mode once started shall not be interruptible.

NOTE High priority hardware commanding is considered an exception.

t. The successful transition, execution and stabilisation of safe/survival mode shall not rely on residual values coming from previous spacecraft modes.

NOTE 1 Residual values are those that are left over unrefreshed from the previous modes.

NOTE 2 The use of some saved context data is allowed such as spacecraft unit configuration status or Earth ephemeris data to allow high gain antenna pointing to Earth at large distances.

u. The spacecraft shall provide the capability for Ground to recover from Safe Mode and re-enter a nominal operations mode within <SM_RECOVERY_TIME>, using the lowest telemetry and telecommand bit rate available in Safe Mode.

NOTE 1 The downlink bit rate is sized to return basic spacecraft real-time telemetry (sufficient to assess current spacecraft status) and enough stored telemetry to support trouble-shooting and recovery operations.

NOTE 2 <SM_RECOVERY_TIME> is the time needed by ground to configure the spacecraft (e.g. isolation of suspected subsystems, configuration of FDIR tables) and to return to nominal operations assuming ground station contact is available during this time.

v. The operational context, including spacecraft settings and configurations for nominal and safe/survival mode shall be stored in non-volatile memories.

NOTE The extent of the information belonging in the context is mission-specific.

w. The spacecraft shall provide the capability to return the contents of the on-board critical event log within <CEL_DUMP_TIME> time during safe/survival mode.

NOTE <CEL_DUMP_TIME> time is mission specific. This contributes to the margin to be provided on the downlink bandwidth with respect to real-time housekeeping generation rate.

x. In safe mode, ground shall be provided with permanent uplink and downlink capability.

y. The downlink signal to ground shall be initiated latest <DL_START_TIME> after a transition to safe/survival Mode.

5.8 The ECSS-E-ST-70-41 Telemetry and telecommand packet utilization standard

5.8.1 Introduction

In order to ensure that the space assets can be adequately operated as specified within this standard, this standard assumes and requires that the monitoring and control services are supported on-board as specified in the ECSS-E-ST-70-41 Telemetry and Telecommand Packet Utilization standard, i.e. the PUS.

The PUS provides a logical view for monitoring and controlling any spacecraft, based on the concepts of services that are deployed, on-board.

The PUS standardizes a number of service types with associated subservice types and message types (request types and report types) and provides rules for defining additional, mission specific service types, subservice types and message types.

The deployment of the PUS standard on-board consists in identifying what application processes are required and taking into account the physical architecture of the spacecraft, its subsystems and payloads:

- to identify the PUS services to be hosted on-board, to implement the spacecraft functionality, and
- per application process, to identify the required subservices and related functionality to be hosted by that application process.

This clause 5.8 provides relevant requirements that complement the specification of the various PUS services.

5.8.2 General service design

a. The monitoring and control of each subsystem, on-board, shall be provided by one or more application process(es) dedicated to that subsystem.

NOTE This applies to both, the platform related and payload related subsystems.

b. The assignment of application process identifiers shall remain unchanged during the mission.

c. The combination of telemetry and telecommand packet identification fields shall be such to uniquely identify the packet structure and content across the complete spacecraft.

NOTE The packet identification fields include for each telemetry and telecommand packet the Application Process Identifier, the Type and the Subtype. Additional packet identification fields are type and subtype specific.

d. In case a given service is provided by multiple application processes on-board, the structure of telemetry and telecommand packets associated to it shall be identical.

NOTE The exact position and length of the packet identification fields is however allowed to differ between application processes in case of need.

e. The structure of housekeeping telemetry reports shall be such that each instance of a given packet contains the same set of telemetry parameters in the same position and with a sample time which is associated to a fixed offset compared to the packet generation time.

NOTE This implies that variable arrays of parameters and deduced presence of parameters and arrays cannot be used.

f. The parameter identifier used on-board to identify telemetry parameters shall be uniquely assigned across the complete spacecraft.

5.8.3 Memory management

a. The capability shall be provided for the ground segment to load any changeable memory area.

b. The capability shall be provided for the ground segment to dump any memory area, on request.

c. The on-board system shall not impose additional constraints on the size of memory areas that can be loaded and dumped based on a single command.

NOTE For example, additional constraints could include not being able to dump a complete memory area with a single command.

d. The capability shall be provided for the ground segment to request a check of any on-board memory.

e. Integrity of the memory area during load, dump or check operations shall be ensured by the on-board application process.

NOTE Memory integrity is normally ensured by preventing other application processes from writing to this memory area during the load or check process.

f. The capability shall be provided to persistently store updated memory content on-board, such that time-consuming memory re-loads from the ground following memory switch on are avoided.

NOTE For example, using EEPROM.

g. When the onboard system implements files, the spacecraft shall provide the capability to load all or part of any onboard memory image as a file.

h. When the onboard system implements files, the spacecraft shall provide the capability to dump all or part of any onboard memory image as a file.

5.8.4 Tine management

a. The relationship between time packet reception and the corresponding telemetery transfer frame which triggered its generation shall be unambiguously derivable on ground.

5.8.5 On-board operations scheduling

a. The capability shall be provided for the ground segment to load any telecommand into on-board operations schedule.

b. The capability shall be provided to perform any action affection on-board schedules content without disabling the schedule execution function.

c. The capability shall be provided to perform any action affecting on-board schedules content even when the schedule execution is in a disabled state.

d. The capacity of the on-board operations schedule shall cover at least the needs of the autonomy period.

e. The elapsed time for the on-board transfer of telecommands from the on-board operations schedule to the destination application process shall be predictable to an accuracy compatible with the telecommand execution time accuracy specified for the mission.

f. The protocol for the on-board transfer of telecommands to their destination application process shall ensure that any transfer error is reported to ground and to the on-board operations schedule service.

g. The on-board operations schedule service shall detect any situation that prevents the on-board transfer of a telecommand to its destination application process.

h. A telecommand loaded into an on-board operations schedule with an on-board release tag equal to that of a telecommand already loaded shall not be rejected but released immediately after that other telecommand.

i. Any telecommands in an on-board schedule that have “elapsed” because the schedule, sub-schedule or application process to which they relate has been disabled and subsequently enabled, shall not be released.

5.8.6 On-board parameter and functional monitoring

a. The capability shall be provided to monitor any on-board parameter and function upon ground request.

NOTE This includes all on-board engineering telemetry parameters including those that are generated by application processes that do not support the on-board monitoring function.

b. The capability shall be provided to perform any action affecting on-board monitoring definitions without disabling the on-board monitoring function.

c. The capability shall be provided to perform any action affecting on-board monitoring definitions even when the on-board monitoring function is in a disabled state.

5.8.7 Large packet transfer

5.8.7.1 Overview

This service provides a standardised ability to exchange with ground packets that exceed the maximum size specified for the uplink or downlink.

5.8.7.2 Large packet transfer requirements

a. Taking into account factors such as uplink bandwidth, ground contact periods and time to recover from telecommand failure, a given mission shall be capable of defining a maximum telecommand packet length which is less than the maximum specified by ECSS-E-ST-50-04.

b. Taking into account factors such as downlink bandwidth and ground contact periods, a given mission shall be capable of defining a maximum telemetry source packet length which is less than the maximum specified by ECSS-E-ST-50-03.

c. The capability shall be provided to downlink and uplink large packets.

NOTE 1 A large packet is a packet that exceed the maximum packet size defined for the mission, refer to requirement a for uplinked packets, requirement b for downlinked packets.

NOTE 2 Downlinking or uplinking large packets can be implemented by splitting the large packets into a number of packets in compliance with the maximum size used for uplinking and downlinking.

5.8.8 On-board storage and retrieval

a. The on-board storage function shall be able to store any packetised data generated on-board.

NOTE Packetised data includes any data transferred on-board within the data handling system (including platform and payload). The storage function stores the packetised data on-board in packet stores and / or file(s).

b. The on-board storage capacity shall be sized such that all engineering telemetry generated on-board can be stored for a duration at least equal to the specified autonomy period.

c. The on-board storage function shall provide the capability to store the same packet in more than one store.

d. Packetised data stored on-board shall be persistent and fully retrievable by ground via the standard services even after a reconfiguration or a cold restart of the application process managing the on-board storage.

NOTE Anomalies directly affecting the storage function itself, such as memory failures, are excluded.

e. The capability shall be provided to assign priorities to parallel retrievals from different stores.

NOTE These priorities can be assigned to maximize the utilization of the downlink bandwidth.

f. The storage of packetised data shall not be interrupted if the ground segment requests a retrieval from, or reset of, the on-board storage.

g. If multiple storage and retrieval devices are implemented on-board, the management of these devices shall be independent.

NOTE For example, in the case of separate mass memory units for engineering and science data.

5.8.9 On-board operations procedures

a. The capability shall be provided to execute a set of operations procedures which can be loaded and controlled by ground.

b. The capability shall be provided to execute more than one operations procedure at the same time.

c. On-board operations procedures shall be capable to send any command available for transmission from the ground.

d. On-board operations procedures shall have access to any engineering telemetry parameter available to the ground.

e. The capability shall be provided to prioritize the execution of on-board operations procedures.

NOTE 1 For example, to give priority to fault management procedures.

NOTE 2 Priority applies in the event of conflicts.

5.8.10 Event action

a. The capability shall be provided to trigger an on-board action as a result of the detection of an on-board event.

NOTE An action in this context is a telecommand, which can itself initiate other on-board actions (e.g. a telecommand which starts an on-board operations procedure).

b. On-board actions shall include any command available for transmission from the ground segment.

5.8.11 File based operations

a. The spacecraft shall support files as native data units to manage interactions with ground.

NOTE This includes support of:

- Files storage and management in file systems.
- Files transfer from/to ground and control of associated transactions.
- Files content access by the on-board applications.
- Automatic management of telemetry data to be downlinked in files via an onboard file manager.
- Automatic creation and closure of files from a onboard data source.
- Files containing a sequence of telecommands which are released onboard upon activation.

b. The spacecraft shall expose to the ground the same interface to the on-board file system(s), for the purpose of file transactions.

NOTE This can be achieved for example, by a single instance hosted by one centralised application process or by multiple instances hosted by different application processes covering each file system.

5.9 Equipment- and subsystem-specific

5.9.1 On-board processors and software

a. Whenever an on-board processor is switched from a prime to a redundant unit (or vice versa), the switchover shall be such that operations can continue safely.

NOTE This implies the maintenance of an operational context in non-volatile memory on-board.

b. The capability shall be provided to save the operational context in non-volatile memory so that it can be restored if a processor is reset or temporarily switched off.

c. Redundant processors should provide the capability to be turned on and operated outside of any control function, for the purpose of evaluating their performance prior to switching to become prime.

d. The resources utilized by on-board software shall be telemetered (e.g. memory usage, central processor unit (CPU) usage and I/O usage).

e. The capability shall be provided to check that on-board software has been correctly uploaded before enabling it.

f. <<deleted>>

g. <<deleted>>

h. The spacecraft shall provide the capability to select the version of any on-board software to be loaded upon software reset using a single telecommand.

i. Any communication between the ground and an on-board software function shall be effected by means of telecommand and telemetry specifically designed for the purpose.

NOTE The objective is to ensure that memory dump and memory load commands (for example) are not used for this purpose. They are not adequate for changes of this operational significance.

j. Whenever a condition that forces a processor reset is detected by software, an event report shall be generated prior to enforcement of the reset.

k. The spacecraft shall provide the capability to report to ground in case any of the synchronously scheduled tasks fail to be completed by the end of the allocated software cycle.

l. Whenever a processor overload condition is detected, an event report shall be generated.

m. Whenever an unexpected arithmetic overflow condition is detected, an event report shall be generated.

n. Whenever an illegal program instruction is encountered during execution of a program code, an event report shall be generated.

o. Whenever a data bus error is detected, an event report shall be generated.

p. The spacecraft shall report to the ground each occurrence of a non-correctable memory corruption event that is detected onboard

q. Whenever a checksum error is detected, an event report shall be generated.

r. Whenever an internal inconsistency is detected, an event report shall be generated.

s. The event reports that are generated in the case of a failure shall indicate the type of failure, its location and any additional information needed for failure diagnosis.

t. The spacecraft shall be robust against complete loss of the operational context.

NOTE This implies the existence of a safe mode level that does not rely on the operational context.

u. The memories available to nominal and redundant processor modules shall be sized to allow storage of at least two complete software images per processor module.

NOTE This ensures, for example, that at least two software images are always available in the case of a single failure.

v. Context required for successful booting of any on-board software image shall be modifiable in non-volatile memory independently of the software image.

NOTE Such context can include default OBCPs if used, or operational context data structures.

w. The process of loading a software image from non-volatile memory to RAM upon boot shall be robust to data corruptions.

x. For each on-board processor, the spacecraft shall provide the capability for ground to select the prime and redundant software images, located in non-volatile memory, to use at the next processor reset / reconfiguration.

NOTE This does not preclude the use of more than one redundant image.

y. The spacecraft shall provide the capability for ground to load software patches directly into RAM without updating the relevant software image in non-volatile memory.

NOTE Upon re-loading the software from the non-volatile memory of the relevant unit the RAM patches are lost.

z. The spacecraft shall provide the capability to report to ground the software version of any software executing on an on-board processor module.

aa. Each on-board application software shall save, in non-volatile memory, and report to ground, data to support failure investigation in case of processor reset, reboot or reconfiguration.

NOTE Such reports are typically referred to as death reports.

bb. Each on-board application software shall save, in non-volatile memory, and report to ground, data relating to the self-test executed by the boot software.

NOTE Such reports are typically referred to as boot reports.

cc. The spacecraft shall provide protections against corruption of the operational context.

dd. Software images on-board shall be stored in non-volatile memory.

ee. The spacecraft shall provide the capability to access (i.e. patch/dump/check) all non-volatile memories containing software images, independently of which processor is in-use.

NOTE A redundant processor can be activated in maintenance mode to achieve this.

ff. For each on-board memory, the spacecraft shall provide the cumulative number of corrected errors of any kind and the last corrected error location in cyclic telemetry.

NOTE Corrected error examples include Single Event Upsets, stuck bits.

gg. The spacecraft shall provide the capability for ground to define a set of patches to on-board software images stored in non-volatile memory that are used in conjunction with the full image as part of the boot process.

5.9.2 Power supply and consumption

a. The power telemetry parameters available to Ground shall be such that the total power generated and power consumed can be directly established from the telemetry alone.

NOTE This becomes critical in eclipse seasons, for instance, when the solar array degrades to a level approaching the sunlit demand plus recharge demand, or when the in-eclipse loads closely match the battery capabilities.

b. Means and engineering telemetry shall be provided such that the ground segment can determine the state of charge of each battery throughout all mission phases, to an accuracy of better than <BATT_CHARGE_ACC>.

c. For all units consuming power, a primary current sensor shall be provided and made available in telemetry.

d. The power status of each equipment shall be available in engineering telemetry under all circumstances

NOTE This is to avoid the case whereby e.g. the power status of units would be lost in case another unrelated unit or the unit itself is switched off.

e. Vital power control functions shall have a switch-over function to the redundant path, but never a switch-off function.

f. If a power-shed function is implemented on-board, the capability shall be provided to modify the list of non-essential loads to be switched off in the event of a power anomaly.

NOTE This can be caused, for example, by battery undervoltage.

5.9.3 Telemetry, tracking and command (TT&C)

a. Redundant receivers, cross-strapped to redundant decoders, shall be provided.

b. At all times in the mission, at least two platform receivers, connected to different antennas, shall be active.

c. In all modes and all mission phases, the spacecraft shall be commandable at any time

NOTE This is to ensure commanding capability throughout the mission in nominal and contingency situations, covering any spacecraft attitude. This is typically achieved by the use of multiple omnidirectional antennas.

d. Where the on-board design implies switching between antennas (e.g. for inertial-pointing spacecraft or during attitude manoeuvres), it shall be ensured that the overlap between antenna patterns is such that there is at least <ANT_SWITCH_TIME> to effect antenna-switching under all expected orbit and attitude conditions.

e. The spacecraft shall process without errors telecommands that contain repetitive bit patterns or without bit transitions.

NOTE Command randomisation as specified in ECSS-E-ST-50-04 can be used to satisfy this requirement.

f. The spacecraft shall trigger an on-board contingency recovery if no telecommand has been received in a defined period <NO_TC_TIMEOUT>, which is configurable by Ground.

NOTE This can, for example, imply reconfiguring the TT&C or a full system level recovery. In addition, for missions with TC authentication this can imply the need to clear the authentication in the defined period.

g. In compliance with the nominal mission operations concept, the spacecraft shall provide the capability to downlink during every pass all engineering telemetry stored on-board the spacecraft since the end of the previous pass, up until the end of the current pass.

NOTE The ground station pass duration and frequency is defined in the mission operations concept during the development phase and is an input to the achievement of this requirement.

h. The maximum TC uplink rate as specified in Space-to-Ground ICD shall be possible for all nominal phases of the mission.

i. For each radio frequency band supported on-board, the spacecraft shall provide the capability for ground to set the downlink bit rate independently.

j. For each radio frequency band supported on-board, the spacecraft shall provide the capability for ground to configure the modulation scheme independently.

k. The spacecraft shall provide the capability for ground to configure each transponder to operate either in non-coherent mode or in coherent mode.

NOTE Coherent mode is dependent upon the lock status of the receiver.

l. The spacecraft shall provide the capability for ground to switch between antennas, without the need to switch off the active transmitter.

NOTE Need for antenna switching is mission specific.

m. The spacecraft shall support the following modes for the data uplink and downlink:

1. Carrier only;

2. Telemetry/Telecommand;

3. Ranging;

4. Simultaneous Telemetry/Telecommand and Ranging.

n. The spacecraft shall support continuous active transmitter operations during all ground station pass durations in the nominal mission operations concept.

NOTE 1 The maximum pass duration is supported without being impacted, for example by power and thermal constraints.

NOTE 2 The minimum pass duration is relevant to the transmitter switch on duration.

o. For the purpose of calculating telemetry data return budgets, the effective data downlink duration of each ground station pass shall be assumed to be <DATA_RETURN_DELTA> less then the visibility period.

NOTE Data Return budgets and analyses demonstrate the capability of the mission to return the data required to fulfil its objectives.

p. The spacecraft shall avoid the loss of telemetry upon changing telemetry bit rate.

NOTE This can be achieved by sending a synchronisation stream (i.e. idle frames) of sufficient duration to allow receivers at the ground station to re-synchronise.

q. The spacecraft shall provide the capability, in all supported nominal and contingency scenarios, to determine the orbit within the precision required by the mission.

NOTE NOTE: This is typically achieved using TT&C Doppler and ranging radiometric data.

r. The spacecraft design shall not place a constraint on the achievable daily duration for ground communication.

5.9.4 Attitude and orbit control

a. The spacecraft shall provide all necessary engineering telemetry to allow Ground to determine the spacecraft attitude independently of the on-board estimation process

b. Engineering telemetry monitoring of thruster actuation shall be provided to enable thruster on-time surveillance and fuel consumption determination.

c. In normal conditions the avionics of 3-axis controlled spacecraft should maintain the knowledge of the current 3-axis attitude.

d. Means shall be provided for determining from engineering telemetry the remaining fuel in each independent propellant system to an accuracy of <PROP_ACCURACY>.

NOTE NOTE: The accuracy may depend on the level of the remaining fuel.

e. The spacecraft shall autonomously be able to safeguard sensitive equipment upon unplanned thruster firing.

NOTE 1 Examples include a Safe Mode transition or an autonomous wheel off-loading.

NOTE 2 Equipment sensitive to unplanned thruster firing is mission-specific.

f. The ground shall be able to command AOCS fallback entry from any AOCS mode, including the fallback mode itself.

NOTE An example of an AOCS fallback mode can be a sun acquisition mode.

g. The spacecraft shall provide the capability for ground to override and re-enable the value of any AOCS biases and drifts which may be calculated onboard autonomously.

NOTE 1 For example, the drift of an on-board gyro stellar estimator.

NOTE 2 The values uploaded by ground are persistent until the autonomous on-board function is re-enabled by ground.

h. The spacecraft shall provide the capability for ground to command, via dedicated telecommands, any individual actuator.

NOTE This can involve Ground activating an actuator not used by the on-board control loop.

i. The spacecraft shall provide all necessary engineering telemetry to allow the Ground to verify the correct performance of the on-board attitude and orbit control algorithms.

j. The maximum orbit degradation induced by thruster based attitude control and wheel momentum off-loading shall be commensurate with the mission operations concept.

k. The spacecraft shall be capable of maintaining the communication link with the ground during any nominal attitude and orbit control operations.

NOTE This applies, for example, to wheel momentum off-loading.

l. The spacecraft shall provide the capability to autonomously maintain attitude control over a period of <MAX_SENSOR_OUTAGE_PERIOD> in the presence of any transient attitude sensor loss induced by environmental effects.

NOTE This includes, for example, Star Tracker loss of tracking due to radiation blinding from a solar flare.

m. The spacecraft shall autonomously maintain communication with ground in case of attitude sensor outage duration exceeding <MAX_SENSOR_OUTAGE_PERIOD>.

NOTE In this case, it is acceptable to rely on degraded communication.

n. The spacecraft shall be capable of performing all manoeuvres without the need for real-time interaction with the ground.

o. The spacecraft shall provide the capability to perform a direct mode transition from safe mode to an orbit control mode upon request from ground.

NOTE 1 The objective is to minimise the time, and ground interactions, required to perform a time-critical orbital manoeuvre (e.g. in LEOP or close to a Gravity Assist Manoeuvre).

NOTE 2 The target orbit control mode may be a simplified version of the nominal orbit control mode.

p. Commanding interactions from ground to maintain the routine operation of the AOCS shall be minimised as goal and commensurate with the autonomy concept.

NOTE Typically AOCS context data is uploaded by ground on a periodic basis. This context data is the set of time-varying data required for the system to perform its function (e.g. ephemeris, guidance, SA profiles, antenna profiles, etc).

q. A generic attitude guidance function shall be provided allowing ground to program the required spacecraft guidance for any three-axis stabilised mode.

r. A single generic thruster modulator function shall be provided capable of implementing forces and torques for any thruster control mode.

s. Reaction wheel offloading shall be autonomously calculated and executed onboard, and implemented to minimise mission interruption.

t. The spacecraft shall provide the capability to enable and disable autonomous thruster-based reaction wheel offloading via ground command.

u. The ground shall be able to program the thruster modulator function such that any meaningful thruster configuration can be used.

v. The ground shall be able to command thruster-based reaction wheel offloading directly.

NOTE Ground initiated reaction wheel offloading can be implemented to avoid autonomously executed offloading events occurring within protected periods, such as specific observations.

5.9.5 Mechanisms

a. Full deployment status of one-shot drivable mechanisms shall be telemetered.

NOTE Deployment statuses are considered mission critical functions and are subject to 5.3.1k.

b. The status of mechanisms that are locked during launch shall be available during the pre-launch phase.

c. The capability shall be provided to monitor the various stages of a deployment process.

NOTE For example, all motorized deployments monitored by potentiometers.

d. The spacecraft shall report the current position of all mechanisms in engineering telemetry.

NOTE 1 Mechamism telemetry is provided when the relevant unit is on.

NOTE 2 This includes the final pre-flight positions of all mechanisms.

e. The positions of all mechanisms shall be commanded and monitored absolutely, i.e. not commanded incrementally or monitored by relative or cyclic readings.

f. Mechanisms, except the "single shot" type, shall be designed so that they cannot be driven into a non-recoverable condition.

5.9.6 Thermal control

a. The capability shall be provided for the ground segment to enable and disable each individual thermal control loop.

b. With the exception of loops that are driven by thermostats, the capability shall be provided to adjust the temperature control thresholds of each thermal control loop by ground command.

c. Thermistors shall be provided to allow ground to monitor temperature changes across the spacecraft platform, payload and structure without significant gaps.

NOTE This allows ground to understand in detail the thermal balance across the spacecraft (e.g. location of possible sublimation products etc).

d. Thermistors shall be provided to allow ground to monitor temperature changes across the spacecraft platform, payload and structure in sufficient resolution to monitor expected routine temperature variations.

5.9.7 Payload

a. The design of the payload shall include taking protective action against potential damage caused by the external environment, even when the instrument is not operated.

NOTE 1 For example, switch-off of the high voltages if the background radiation level is detected to be too high.

NOTE 2 The protective action can involve functions from the spacecraft system, for example the spacecraft platform commands a shutter closure to protect against sun illumination in an attitude anomaly.

b. Payloads shall provide the capability to enter a safe state upon receipt of a specific telecommand.

c. There shall be no requirement for the ground segment to perform extensive payload operations for an interval <PAYLOAD_INT> after separation from the launcher.

NOTE Simple instrument switch-on, or heater activation is not excluded.

d. If data compression techniques are implemented, they shall not impose special requirements on the design of the ground segment, such as redundant links or larger antennae.

e. The interpretation of compressed data shall not depend on the telemetry history.

f. All information to assess the health and safety of a payload instrument shall be available in the engineering telemetry, i.e. this information shall be available without accessing science telemetry.

g. Any operationally-significant information on the configuration and timing of payload operations should be downlinked in the telemetry.

5.9.8 On-board storage and file system

a. Any file system maintenance shall be performed autonomously on-board.

NOTE For example, operations like defragmentation.

b. All services exposed by the on-board file system(s) related to file management shall be accessible by ground.

NOTE This does not necessarily imply that ground is able to directly modify the content of individual files but ground will be able to control the routing of data into files.

c. The spacecraft shall provide the capability for ground to manage the status and content of any on-board file system.

NOTE Management of the status and content of the file system implies the setting of file attributes, such as lock status, repository path, size and name.

d. Each file system shall support directories.

e. The spacecraft shall support the capability to exchange files between ground and space segment.

NOTE This can be achieved via CFDP protocol, for example.

f. The spacecraft shall provide the capability for ground to verify the completeness and correctness of each file transfer transaction.

g. The file transfer protocol shall provide the capability to ensure completeness of file transfers with minimal bandwidth utilisation overhead as determined on the basis of mission specific characteristics.

h. The spacecraft shall provide the capability for ground to control the downlink of files.

NOTE For example, start, stop, suspend, resume file downlink.

i. The spacecraft shall provide the capability for ground to control the transfer of files at the level of:

1. each individual transaction;

2. all uplink transactions;

3. all downlink transactions;

4. all uplink and downlink transactions.

j. The spacecraft shall provide the capability to manage large file sizes.

NOTE 1 This applies to file transfer (uplink and downlink) and the characteristics of the on-board file system(s).

NOTE 2 The maximum file size is typically maximised to enable an efficient operational interface. The maximum file size is tuned with the mission characteristics.

k. The spacecraft shall provide the capability to manage several file transfer transactions in parallel in each direction.

NOTE This applies to both uplink and downlink transactions independently.

l. The on-board file systems and their content shall be persistent and fully functional even after a reconfiguration or a cold restart of the application process managing the file systems.

NOTE Anomalies directly affecting the storage function itself, such as memory failures, are excluded.

m. The spacecraft shall provide the capability for ground to change the data storage configuration.

NOTE This for example means configuration of different memory area used on-board.

n. The spacecraft shall provide the capability for ground to perform a self test of all memory areas used for data storage.

o. The creation of files within the file system shall not result in the activation of data storage hardware.

NOTE This is to avoid having unused memory areas power up autonomously, such that this would affect the resource usage without ground control.

p. Any on-board detection of a new failed or corrupted memory block shall be reported in event telemetry.

NOTE A memory block here indicates the smallest memory area that can be allocated to a file.

q. The spacecraft shall provide the capability for ground to request the list of all failed memory blocks.

NOTE A 'memory block' is meant as the smallest memory area assigned for file data storage.

5.10 File based operations (General)

a. For each file system on-board, all file system related services supported by that file system shall be accessible by some on-board applications.

NOTE On-board applications involved in file based operations need access to the on-board file system(s). For example payloads may write data into files.

b. The spacecraft shall provide to ground full visibility of the status and contents of the on-board file systems.

c. The on-board file system(s) and their content shall be persistent and fully functional even after a reconfiguration or a cold restart of the application process managing the file systems.

NOTE Anomalies directly affecting the storage function itself, such as memory failures, are excluded.

Annex A (informative) Mission constants

The mission constants identified within the body of this Standard are summarized and defined below.

<ANOM_RESP_TIME>

minimum response time for the ground segment to react to anomalies detected from the telemetry with the generation of a telecommand

NOTE This is applicable for short, well-defined intervals during critical mission phases and for pre-agreed contingencies and anomaly conditions.

<ANT_SWITCH_TIME>

minimum time interval that is available for switching between on-board antennas

<AUT_DUR_EXEC>

interval of time for which the space segment can execute nominal mission operations autonomously

<AUT_DUR_FAIL>

interval of time for which the space segment safety is ensured (without ground segment intervention) in the event of a single failure

<BATT_CHARGE_ACC>

accuracy to which the charge status of an on-board battery can be determined

<DIAG_MIN_INTERV>

minimum sampling interval for sampling an on-board parameter in diagnostic mode

<GRND_RESP_TIME>

response time for control functions involving the ground segment

NOTE There can be several such parameters for a given mission.

<NO_TC_TIMEOUT>

time without receiving a telecommand by Ground before which the spacecraft shall trigger a pre-defined on-board contingency recovery. NOTE The variable is configurable by Ground

<PARAM_ABS_SAMPL_TIME>

accuracy of determination of the absolute (on-board) sampling time of a telemetry parameter

<PARAM_REL_SAMPL_TIME>

accuracy of determination of the relative sampling time of any two telemetry parameters

<PAYLOAD_INT>

interval of time following separation from the launcher during which there is no requirement for the ground segment to perform extensive payload operations

<PKT_RETR_DELAY>

maximum time delay for the ground segment to retrieve data generated at an earlier time and stored on-board

NOTE There can be several such mission parameters relating to data of different operational priority.

<PKTS_NUM_STORED>

number of packets stored in short-term storage on-board

NOTE This is applicable for missions with continuous ground coverage.

<POW_CONS_THRESH>

threshold of electrical power consumption beyond which specific requirements exist for the provision of telemetry data

<RESOURCE_MARGIN>

minimum resource margin for on-board subsystems and payloads that is available at all times during the mission

NOTE For example, power, on-board memory, CPU load, bus traffic and registers

<SAFE_TIME>

interval of time for which the space segment safety is ensured

<TC_VERIF_DELAY>

maximum delay between the execution of a telecommand and its verification within the telemetry

<TIME_CORREL_ACCUR>

correlation accuracy between on-board time and ground time

Annex B (informative) Tailoring guide

For tailoring purposes, the following major areas of potential impact are identified:

- **Ground segment functions**

  If a requirement is tailored out, this can give rise to a requirement (tailored in) for special ground segment functions instead. For example, a requirement for an additional ground station in order to increase the coverage or a requirement for complex ground functions to process the telemetry or telecommand data.

- **Space segment safety**

  If a requirement is tailored out, the safety of the space segment can be endangered. This relates either to unauthorized access to the spacecraft, or to loss of control of the spacecraft.

- **Space segment and mission degradation**

  If a requirement is tailored out, this can have consequences in terms of:

  — Temporary or permanent degradation of a space segment function.

  NOTE As long as redundancy is provided, the mission objectives can still be achievable.

  — Temporary or permanent degradation of the mission.

- **Operations impact**

  If a requirement is tailored out, the efficient control of the satellite can be impacted, with a subsequent effect on the mission performance.

Table B-1 shows the impact of each requirement in each of these areas and also provides additional comments concerning the potential implications if the requirement is tailored out.

Table B-1: Tailoring guide

NOTE Dear Reviewer, be informed that this Tailoring guideline will be updated after the Public Review.

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
4.2a		X	X	X	
4.3a			X	X	
1.1.1.1.1a	X				High complexity ground segment functions to process the data, if the space segment is not designed in conformance with to Standards (e.g. telemetry and telecommand packet definitions).
4.4a	X			X	
4.5a		X			
4.5b		X	X		
4.5c		X	X		
4.5d		X	X		
1.1.1.1.1a		X	X		
4.5e		X	X		
4.6a				X	Definition by the control centre of special procedures and limit checks for each combination of equipment.
4.6b				X	
4.6c				X	Loss of capability to check redundant equipment before their utilisation by the control centre.

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
4.6d			X	X	
4.6e			X		Loss of capability to control the space segment in case of failures of automatisms.
4.6f			X		Loss of flexibility to handle changes to ensure that the mission goals can be achieved. The flexibility to be provided is highly dependent on the mission duration and complexity. The longer the mission the more likely are changes.
1.1.1.1.1a			X		Loss of flexibility to handle changes to ensure that the mission goals can be achieved. The flexibility to be provided is highly dependent on the mission duration and complexity. The longer the mission the more likely are changes.
4.6g				X	
4.7a				X	
4.7b				X	Loss of control of the space segment if the redundant equipment is not working as expected. If this function is not implemented as far as possible (i.e. ensuring that on-board design constraints, e.g. power constraints, are not violated), an increase in the risk of losing control can be expected.
4.7c			X		Potential severe impact on the mission in case of a failure.
4.7d			X		
4.8a				X	
4.8b				X	
5.2.1a		X			
5.2.1b	X	X			

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
5.2.1c	X	X			
1.1.1	X			X	High availability requirement on the ground segment which leads to the implementation of special ground functionality.
1.1.1	X			X	
1.1.1				X	
1.1.1				X	Delays leading to inefficiencies in executing operations.
5.2.2a	X			X	More complex ground processing. Inefficient use of downlink bandwidth.
5.2.2b	X			X	
5.2.2c	X			X	
5.2.2d				X	Impact on the mission return if data recovery is part of the nominal operations to avoid data losses.
1.1	X			X	
5.3.1a			X	X	
5.3.1b				X	
5.3.1c				X	
5.3.1d				X	Potential for the ground segment to miss essential on-board events.
5.3.1e	X				
5.3.1f				X	
5.3.1g			X		Wrong decision by the ground segment if invalid or out-of-date telemetry data are used.

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
5.3.1h				X	
5.3.1i			X		
5.3.1j			X	X	
5.3.1k			X		
5.3.1l			X	X	
5.3.1m				X	Potential for the ground segment to be misled by incorrect processing of the telemetry. This concerns in particular AOCS sensor data.
5.3.1n			X	X	
5.3.1o			X	X	
5.3.1p	X			X	Wrong decision by the ground segment if invalid telemetry data are used.
5.3.1q	X			X	
5.3.1r	X			X	
5.3.1s	X				
5.3.1t	X				
1.1.1.1.1a	X				
5.3.1u	X				
5.3.1v	X				
1.1.1.1.1a				X	

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
1.1.1.1.1a				X	Loss of flexibility to reduce the update and downlink rate of parameters (less frequent parameter updates or fewer packets).
5.3.1w	X			X	
1.1.1.1.1a	X			X	
5.3.2a				X	Limitation of the detailed analysis of specific anomaly cases.
5.3.2b				X	Limitation of the detailed analysis of specific anomaly cases.
5.3.2c				X	
5.3.2d				X	Loss of flexibility of data analysis. This requirement is only applicable if an on-board storage function is provided.
5.4a			X	X	Potential inability to achieve the mission objectives if the specified timing accuracy is not provided.
5.4c	X			X	Implementation of special ground processing.
5.4d				X	
5.4e				X	
5.4f				X	
5.4g				X	
5.4h	X			X	Implementation of special ground processing.
5.4i	X				Inability to apply the standard ground segment processing software. This requirement is essential for housekeeping telemetry but can be relaxed for payload data if the relevant time information appears elsewhere within the packet.

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
5.4j	X			X	Implementation of special ground processing.
5.4k			X	X	Ambiguity of telemetry.
5.4l			X	X	Potential inability to achieve the mission objectives if the specified timing accuracy is not provided.
5.4m			X		
5.4n	X			X	
1.1.1.1.1a				X	
5.5.1a		X	X		
5.5.1b	X			X	Higher complexity of the configuration control of commands. Risk of sending commands in the wrong context.
5.5.1c	X			X	
1.1.1.1.1a				X	
1.1.1.1.1a				X	
5.5.1d	X		X	X	Higher complexity of the configuration control of commands. Risk of sending commands in the wrong context.
5.5.1e	X			X	
5.5.1f		X	X		
5.5.1g			X	X	Inability of the ground to send commands in a safe manner when the on-board situation is unclear, e.g. in the event that telemetry data is not available.
5.5.1h			X	X	Potential impact on the control of the space segment in specific failure situations.

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
1.1.1.1.1a	X			X	
5.5.1i	X			X	Increase in the size of the operational database and higher complexity of the configuration control task.
1.1.1.1.1a	X			X	
5.5.1j	X			X	
5.5.2a			X	X	Potential impact on the access to the space segment in the event of processor failures.
5.5.2b		X	X		
5.5.2c		X	X		
5.5.2d		X	X		
1.1.1.1.1a				X	Cumbersome uploading of memory load commands and the imposition of severe restrictions on the operations.
5.5.3a	X			X	
5.5.3b			X	X	
1.1.1.1.1a				X	
5.5.3c	X			X	
5.5.4a			X	X	
1.1.1.1.1a			X	X	
5.5.4b				X	
1.1.1.1.1a				X	

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
1.1.1.1.1a	X			X	
5.5.4c	X			X	
1.1.1.1.1a	X			X	
5.5.4d				X	Impact on the definition of efficient control procedures and command sequences.
5.5.4e			X	X	
5.5.4f	X			X	
5.5.4g				X	
5.5.4h			X	X	
5.5.4i			X	X	
5.5.4j	X			X	Implementation of special ground processing functions.
5.6.1a			X	X	Loss of flexibility to control the configuration of the space segment.
5.6.1b				X	
5.6.1c				X	
5.6.1d				X	
5.6.1e				X	
5.6.2a				X	
5.6.2b				X	Loss of the capability to identify whether an on-board reconfiguration is executed nominally and to intervene early enough in the event of malfunctions.

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
5.6.2c				X	
5.6.2d				X	
5.6.2e			X	X	Impact on the detection of possible on-board failures.
5.6.2f				X	
1.1.1.1.1a			X	X	
5.6.2g		X	X		
5.6.2h	X	X	X		Potential entry of the space segment into a hazardous status if ground contact cannot be guaranteed.
1.1.1.1.1a			X		
1.1.1.1.1a				X	
5.6.2i			X		
5.6.2j		X	X		Potential entry of the space segment into a non recoverable state.
5.7.2a	X		X	X	Exacting requirements on the ground segment availability, i.e. substantial redundancy requirements.
5.7.2b			X	X	
5.7.2c			X	X	
5.7.2d		X	X	X	
5.7.2e	X			X	Special set-up on ground, which can also include extra manpower.
5.7.2f		X		X	

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
5.7.5.2a	X		X	X	
5.7.5.2b			X		
1.1.1.1.1a			X		
1.1.1.1.1a		X	X		Impact on the safety of the space segment in the event of on-board processor failures.
1.1.1.1.1a			X		
1.1.1.1.1a			X		
5.7.5.2c			X		
5.7.5.2d			X	X	
5.7.5.2e			X	X	Impact on the identification of a non-nominal on-board behaviour.
5.7.5.2f		X	X		Potential entry of the space segment into dangerous configurations.
5.7.5.2g			X	X	Potential loss of the mission or at least potential significant impact on the performance (e.g. non-availability of a function) if an on-board mechanism fails.
5.7.5.2h			X	X	ility of the ground to correct the on-board configuration in the event of performance degradation or on-board failures.
1.1.1.1.1a		X	X		
5.7.5.2i			X	X	
5.7.5.3a			X	X	

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
5.7.5.3b			X	X	Out-of-limit conditions can only be detected during ground coverage. This requirement is applicable if the space segment provides an on-board monitoring function.
5.7.5.3c	X		X	X	Potential for the ground to be misled by the telemetry information and to overlook essential information.
5.7.5.3d			X	X	
5.7.5.3e				X	
5.7.5.3f		X	X		Potential impact on the recovery from an anomaly condition of the failure that caused the entry into that anomaly condition.
1.1.1.1.1a		X	X		
5.7.5.3g				X	Reduced probability of safety mechanisms working.
5.7.5.3h			X	X	Inability of the ground to correct the on-board configuration in the event of performance degradation or on-board failures.
5.7.5.4a		X	X		
5.7.5.4b			X		
5.7.5.4c			X		
5.7.5.5a	X	X	X		
5.7.5.5b	X		X	X	
5.7.5.5c		X	X		
1.1.1.1.1a		X	X		Potential failure of recovery if faulty equipment is used.

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
1.1.1.1.1a	X	X	X		
5.7.5.6a		X	X		
5.7.5.6b		X	X		
5.7.5.6c			X	X	Potential inappropriate entry of the space segment into survival states, which impacts the mission return.
5.7.5.6d			X	X	
1.1			X	X	
1.1				X	
1.1.1.1.1a			X	X	Loss of control of on-board processes in case of failures.
1.1.1.1.1a	X			X	
1.1.1.1.1a				X	
1.1.1.1.1a				X	Potential high complexity of the configuration control task on ground.
1.1.1.1.1a	X				Implementation of special ground processing functions and inability to reuse the standard infrastructure.
1.1.1.1.1a	X				
1.1.1.1.1a	X				
1.1.1.1.1a	X				
1.1.1.1.1a	X				
1.1.1.1.1a	X				

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
1.1.1.1.1a	X				Implementation of special ground processing functions and inability to reuse the standard infrastructure. This requirement can be relaxed for payload data, for which special processing is envisaged.
1.1.1.1.1a	X				
1.1.1.1.1a	X				Potential high complexity of the configuration control task on ground.
1.1.1.1.1a	X				
1.1.1				X	Impact on long periods without ground coverage and on downlink efficiency.
1.1.1				X	
1.1.1				X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
1.1.1				X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
1.1.1				X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
1.1.1				X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
5.8.3a				X	Loss of flexibility to react to changes of the on-board performance and functions.
1.1.1.1.1a	X			X	
1.1.1.1.1a	X			X	
1.1.1.1.1a			X		

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
1.1.1.1.1a	X			X	
5.8.3b				X	
1.1.1.1.1a	X			X	
1.1.1.1.1a	X			X	High complexity of the processing of dump data.
1.1.1.1.1a	X			X	
5.8.3c	X			X	
1.1.1.1.1a	X			X	
5.8.3d				X	Risk of inconsistent on-board memory if there are no automatic on-board functions to check the consistency of the memory. This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
1.1.1.1.1a	X			X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
1.1.1.1.1a	X			X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
1.1.1.1.1a	X			X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
5.8.3e			X		
5.8.3f	X			X	
1.1.1.1.1a	X			X	Implementation of special ground processing functions, if this functionality is provided and ECSS-E-ST-70-41 is not followed.

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
1.1.1.1.1a	X			X	
5.8.5a				X	
1.1.1.1.1a				X	Significant impact on the execution of the operations.
5.8.5b				X	
1.1.1.1.1a				X	
1.1.1.1.1a				X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
1.1.1.1.1a				X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
1.1.1.1.1a			X	X	Risk of releasing commands in the wrong context, which can lead to hazardous situations. This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
1.1.1.1.1a				X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
5.8.5c				X	
5.8.5d				X	Endangering of the safety of the space segment if the space segment autonomy is not ensured.
5.8.5e				X	Potential inefficient use of the on-board operations schedule.
5.8.5f				X	Potential sending of commands in the wrong context.
5.8.5g			X	X	Potential sending of commands in the wrong context.
1.1.1.1.1a			X	X	

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
5.8.5h				X	
5.8.5i			X	X	Potential entry of the space segment into a dangerous state.
1.1.1	X			X	
1.1.1				X	
5.8.6a			X	X	Reduction of the on-board autonomy and potential inability to detect anomalies in time.
1.1.1.1.1a			X	X	
1.1.1.1.1a			X	X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
1.1.1.1.1a			X	X	Risk of false anomaly notifications in the event of an on-board failure, which can lead to wrong operational decisions. This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
1.1.1.1.1a			X	X	Loss of flexibility to handle changes of the performance and functions of the space segment e.g. in the event of failures. This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
5.8.6b			X	X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
1.1.1.1.1a				X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
1.1.1.1.1a				X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
1.1.1.1.1a		X		X	
1.1.1.1.1a	X			X	
1.1.1.1.1a				X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
1.1.1.1.1a	X			X	Implementation of a complex ground model. This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
1.1.1.1.1a				X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
1.1.1.1.1a				X	
5.8.7.1	X			X	
5.8.7.2b	X			X	
5.8.7.2c	X			X	
1.1.1				X	
1.1.1				X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
1.1.1				X	Inability to use the available telemetry bandwidth in an efficient manner and potential overflow in case of a failed application.
1.1.1				X	Potential overflow in case of a failed application.
1.1.1				X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
5.8.8a				X	Impact on the on-board autonomy and the completeness of the data. The functionality to be provided depends on the mission characteristics.
1.1.1.1.1a				X	
1.1.1.1.1a				X	
5.8.8d				X	
1.1.1.1.1a				X	
5.8.8e				X	
1.1.1.1.1a				X	
1.1.1.1.1a				X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
1.1.1.1.1a				X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
1.1.1.1.1a				X	
1.1.1.1.1a				X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
1.1.1.1.1a				X	
5.8.8f				X	
1.1.1.1.1a				X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
1.1.1.1.1a				X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
1.1.1.1.1a				X	
1.1.1.1.1a				X	
1.1.1.1.1a				X	
1.1.1			X	X	Reduced probability of detecting on-board malfunctions.
1.1.1			X	X	
1.1.1				X	
5.8.9a			X	X	Potential non-compliance of the achieved on-board autonomy with the mission goals.
5.8.9b				X	
1.1.1.1.1a				X	
1.1.1.1.1a	X			X	Implementation of complex ground models. This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
1.1.1.1.1a	X			X	Implementation of complex ground models. This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
5.8.9c				X	
5.8.9d				X	
5.8.9e		X		X	
5.8.10a		X	X	X	Potential non-compliance of the achieved on-board autonomy with the mission goals.

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
5.8.10b		X	X	X	Potential non-compliance of the achieved on-board autonomy with the mission goals.
1.1.1	X			X	
1.1.1				X	
1.1.1				X	Reduced probability of detecting the execution of an on-board action with the risk that the ground interferes erroneously with an on-board process.
1.1.1.1.1a				X	Loss of flexibility to handle changes of the performance and functions of the space segment.
5.9.1a			X	X	
1.1.1.1.1a			X	X	Potential sending of commands in the wrong context.
5.9.1b	X			X	
5.9.1c			X	X	
5.9.1d			X	X	Potential inefficient use of the on-board processors.
5.9.1e			X	X	
5.9.1f			X	X	
5.9.1g		X	X	X	
5.9.1h				X	
5.9.1i	X			X	
5.9.1j			X	X	
5.9.1k			X	X	

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
5.9.1l			X	X	
1.1.1.1.1a		X	X	X	
5.9.1m			X	X	
5.9.1n			X	X	
5.9.1o			X	X	
5.9.1p			X	X	
5.9.1q			X	X	
5.9.1r			X	X	
5.9.1s				X	
5.9.2a			X	X	
5.9.2b			X	X	
5.9.2c			X	X	
1.1.1.1.1a			X		
5.9.2d			X		
5.9.2e		X	X		
5.9.2f			X		
NOTE			X	X	
5.9.3a			X		

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
5.9.3b		X	X		
5.9.3c			X	X	
5.9.3d			X	X	
1.1.1.1.1a	X		X	X	
1.1.1.1.1a		X	X		
1.1.1.1.1a			X	X	
5.9.4a			X	X	
5.9.4b			X	X	
5.9.4c	X		X	X	
5.9.4d			X	X	
1.1.1.1.1a			X	X	
5.9.5a			X	X	
5.9.5b			X	X	
5.9.5c			X	X	
5.9.5d			X	X	
5.9.5e	X			X	
5.9.6a			X	X	

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
5.9.6b			X	X	
5.9.7a		X	X		This requirement depends on the mission characteristics.
5.9.7b		X	X	X	
5.9.7c	X			X	Implementation of special functions on ground.
5.9.7d	X			X	Implementation of special functions on ground.
5.9.7e	X			X	Implementation of special functions on ground. High availability of the ground segment.
5.9.7f	X			X	Implementation of special functions on ground.
5.9.7g			X	X	

Bibliography

ECSS-S-ST-00	ECSS system — Description and implementation and general requirements
CCSDS 350.5-G	Space Data Link Security Protocol-Summary of Concept and Rationale
CCSDS 232.1-B	Communications Operation Procedure-1
CCSDS 355.0-B	Space Data Link Security Protocol
CCSDS 355.1-B	Space Data Link Security Protocol - Extended Procedures