ECSS-E-ST-70-11C
31 July 2008

Space engineering

Space segment operability

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

Foreword

This Standard is one of the series of ECSS Standards intended to be applied together for the management, engineering and product assurance in space projects and applications. 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-70-11 Working Group, reviewed by the ECSS Executive Secretariat and approved by the ECSS Technical Authority.

Disclaimer

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

Change log

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

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

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

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

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

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

2
Normative references

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

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-ST-50-04	Space engineering – Space data links – Telecommand protocols, synchronization and channel coding
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 commandable vital function

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

3.2.2.2 high priority command

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

3.2.2.3 high priority telemetry

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

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

3.2.2.4 locally-critical function

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

3.2.2.5 mission-critical function

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

3.2.2.6 permanent degradation of space segment function

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

3.2.2.7 permanent mission degradation

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

3.2.2.8 temporary degradation of space segment function

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

3.2.2.9 temporary mission degradation

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

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

3.2.2.10 vital function

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

3.2.2.11 vital telecommand

telecommand that activates a commandable vital function

3.2.3 Other terms

3.2.3.1 application process

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

3.2.3.2 authorization

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

3.2.3.3 chain

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

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

3.2.3.4 confidentiality

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

3.2.3.5 control function

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

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

3.2.3.6 data integrity

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

3.2.3.7 data origin authentication

corroboration that the source of the data received is as claimed

3.2.3.8 datation

attachment of time information to telemetry data

NOTE This includes payload measurement data.

3.2.3.9 device telecommand

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

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

3.2.3.10 housekeeping telemetry

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

3.2.3.11 loss of mission

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

3.2.3.12 memory

on-board data storage area

NOTE 1 This includes main memory and storage memory.

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

3.2.3.13 mode

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

3.2.3.14 mode transition

transition between two operational modes

3.2.3.15 on-board autonomy

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

3.2.3.16 on-board monitoring

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

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

3.2.3.17 on-board operations procedure

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

3.2.3.18 on-board operations schedule

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

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

3.2.3.19 operability

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

3.2.3.20 operations

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

3.2.3.21 parameter

lowest level of elementary data item on-board

3.2.3.22 parameter validity

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

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

3.2.3.23 peer-entity authentication

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

3.2.3.24 safe state

safe condition for a system, subsystem or payload

3.2.3.25 space segment status

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

3.2.3.26 survival mode

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

3.2.3.27 telecommand function

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

3.3 Abbreviated terms

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

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

3.4 Conventions

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

NOTE For example, <TC_VERIF_DELAY>

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

4
General requirements

4.1 Introduction

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

4.2 Observability

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

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

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

4.3 Commandability

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

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

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

4.4 Compatibility

a. The space segment shall conform to all on-board design standards specified for the mission in order to ensure compatibility with the specified ground systems.

b. The space segment design shall be such that its operation is not constrained by, nor adversely constrains, the availability or capacity of the space-Earth communications links.

4.5 Safety and fault tolerance

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

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

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

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

c. No single unintentional ground command or failure in one space segment element shall cause a failure in another space segment element.

d. The design of the space segment failure detection, isolation and recovery (FDIR) function shall be such that all anticipated on-board failures can be overcome either by autonomous on-board action or by clear, unambiguous and timely notification of the problem to the ground segment.

e. The FDIR design shall ensure that the space segment is safe without ground segment intervention for the specified duration in the presence of a single failure.

f. No reconfiguration of the spacecraft shall lead to a configuration where new single point failures are introduced.

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

4.6 Flexibility

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

h. The capability shall be provided 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 For example, power, cooling fluid, fuel.

NOTE 2 The accuracy is specified to be compatible with the mission requirements.

4.7 Testability

a. Each application process shall provide the capability to perform a set of end-to-end test functions 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 should be provided to operate redundant on-board equipment in an "off-line" manner (i.e. in parallel with, but without any disturbance to, the prime equipment).

NOTE 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.

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. Some of these functions correspond to services defined within ECSS-E-ST-70-41 (the packet utilization standard), which are, by definition, all optional. The services are:

- statistical data reporting;
- memory management;
- function management;
- on-board operations scheduling;
- on-board monitoring;
- large data transfer;
- telemetry generation and forwarding;
- on-board storage and retrieval;
- on-board traffic management;
- on-board operations procedures;
- event-to-action coupling.

5.2 Mission-level

5.2.1 Security

a. The space segment shall be designed such that the following can be ensured:

1. the integrity of each data stream produced;
2. the confidentiality of each data stream produced;
3. the authentication of each telecommand received;
4. the authorization of each telecommand received.

b. The space segment shall be designed such that 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 can be ensured.

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 be designed such that the recovery of access to both the telemetry and telecommand transmission functions can be ensured after all specified space and ground segment configuration changes.

5.2.2 Control functions

a. The design of the overall mission operations system (i.e. constituting both the ground and space segments) shall ensure that control functions that have response times shorter than <GRND_RESP_TIME> are implemented on-board.

b. Under all circumstances, the elapsed time for an application process to build and release telemetry source packets shall be such that the overall delay between the generation of a packet and its reception at the mission control centre is consistent with the response times <GRND_RESP_TIME> (there can be several such parameters for a given mission) that have been identified for ground control functions.

c. The frequency of generation of telemetry source packets shall be consistent with <GRND_RESP_TIME>.

d. The time differences between the release of packets containing data and packets containing ancillary information used for its ground processing shall be such that the effective operational information (i.e. after ground processing) is available within delays consistent with <GRND_RESP_TIME>.

5.2.3 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 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.

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 telemetry data and deferred telemetry data simultaneously.

e. Request-driven telemetry source packets (e.g. telecommand verification packets) shall be routed to the originating source of the telecommand.

NOTE 1 The source can be either the ground or an on-board application process. In the case of telecommands released from an on-board schedule, the source is the ground.

NOTE 2 On-board autonomous activities are reported to the ground segment using event report packets.

5.3 Telemetry

5.3.1 Telemetry design

a. Telemetry data shall be provided, as defined for all mission phases, for the ground segment to determine the status of the spacecraft subsystems and payloads and to monitor the execution of nominal and anticipated contingency 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 event reporting mechanisms and of the event 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. Essential space segment status data shall be derived from direct measurements.

NOTE This means that the essential status of the space segment is observable directly from the telemetry without the need for ground processing.

g. The design of telemetry shall be such that preconditions for the switching of on-board equipment and units are acquired independently, i.e. they are not dependent on the status of the equipment or unit to be switched.

NOTE 1 To comply with this requirement, power status and thermal data used prior to unit switch-on are managed at a higher level.

NOTE 2 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. Vital space segment health functions shall be monitored with redundant telemetry parameters (e.g. primary bus current and voltage, and propellant tank pressure).

l. 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 elements in hot redundancy, telemetry shall be provided to enable an independent and unambiguous evaluation of the status of each chain.

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

p. Where parameters are conditionally valid, the parameters determining their validity shall be telemetred with a frequency that is the same as, or higher than, the conditionally-valid parameter.

q. Sampling sequences and frequencies shall be specified for all related parameters that are correlated or combined for the purposes of space segment monitoring or performance evaluation to ensure that no information of operational significance is lost.

r. Where the interpretation of a parameter in a variable packet depends on the values of other on-board parameters, these parameters shall all be telemetred in the same packet.

NOTE When the interpretation of a parameter in a variable packet depends on the values of other onboard parameters, the first parameter is a deduced parameter, as defined in ECSS-E-ST-70-41.

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. The telemetry data at a given position in a telemetry packet shall either correspond to a given physical address on-board or to a given logical address, i.e. a mixture shall not be used.

NOTE Physical means that it corresponds to a physical unit on-board, whether or not that unit is being used as prime. Logical means that the telemetry corresponds to the prime unit, which can be either one of two different physical units.

v. If the same telemetry parameter appears more than once in the same housekeeping telemetry source packet, then the parameter shall be sampled regularly in time.

w. 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.

x. The capability shall be provided for the ground segment to define (and re-define) the packet contents for housekeeping telemetry source packets.

y. The capability shall be provided to request that housekeeping telemetry source packets are only sent to ground segment if there has been a change in value of specified contained parameters by more than a specified threshold.

z. Within a given virtual channel, 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.

aa. Within a given virtual channel, consecutive samples of the same telemetry parameter shall be transmitted to ground segment in chronological order, even if they appear in separate packets.

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

5.3.2 Diagnostic mode

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

b. All telemetry parameters shall be accessible in diagnostic mode.

c. The capability shall be provided to sample a given 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 5.8.9 for additional information).

5.4 Datation and synchronization

a. Timing information shall be provided in the telemetry such that on-board time and ground time can be correlated with an accuracy of <TIME_CORREL_ACCUR>.

NOTE For some missions, OBT/UTC time correlation is performed autonomously on-board (e.g. using GPS). Nevertheless, this requirement specifies the provision of means to check this correlation function on the ground.

b. On-board time shall be common to all spacecraft modes, including standby and survival modes.

NOTE For space segment modes see clause 5.6.1.

c. All timing information in the telemetry shall be synchronized with a single on-board reference clock.

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

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

f. For application processes using time synchronization, telemetry information shall be provided to enable the ground segment to verify synchronization.

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

h. 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.

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

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

k. The capability shall be provided to establish on the ground the time at which parameters of operational significance have actually been sampled on-board to an accuracy of <PARAM_ABS_SAMPL_TIME>.

l. 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.

m. 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.

n. If the requirements for timing accuracy are expected to vary during the course of a mission, the capability shall be provided to change the rate of generation of the time packet.

5.5 Telecommanding

5.5.1 Telecommand design

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

NOTE This implies the provision of a high priority command to re-establish command processing in the event of processor failure.

b. If a telecommand executes more than one control action, these actions shall be strictly operationally related, such that they constitute a single logical telecommand 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 packet shall contain one, and only one, telecommand 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 command functions contained in the load or schedule itself.

d. Where a given function is invoked by a sequence of two or more telecommands, the capability shall be provided to “pack” such telecommands within a single telecommand packet.

e. The capability shall be provided to aggregate telecommand packets within the same telecommand segment.

NOTE This does not apply to CPDU commands.

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

NOTE This precludes the use of flip/flop commands.

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

h. The execution of any telecommand shall not lead to permanent loss of the telecommand function.

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

j. 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 function, 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.

k. Command types shall correspond to the on-board function involved.

NOTE 1 The adjustment of the level or value of an on-board register or counter by the use of a register-load device command (not by a sequence of on/off commands).

NOTE 2 The command of an on/off device by an on/off device command (not by a sub-function of a register-load device command).

l. For redundant on-board units that can only be operated in cold standby (i.e. only one unit can be on at any given time), the equivalent telecommands on the prime and redundant equipment shall be:

1. identical, and
2. allocated the same APID.

m. For redundant on-board units that can be operated in parallel (i.e. both units can be operated simultaneously), the equivalent telecommands on the prime and redundant equipment shall be:

1. identical, and
2. allocated different APIDs.

n. The maximum execution duration of a telecommand shall be deterministic.

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.

5.5.2 Critical telecommands

a. The capability shall be provided to implement critical command functions using different categories of telecommand.

NOTE For example, the use of an on-board operations procedure or the on-board schedule to execute a critical telecommand function 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 and safety-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.

c. Register load telecommands that are mission-critical, safety-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 capability shall be provided to “interrupt” the transmission of a telecommand packet by the transmission of another telecommand packet of higher priority.

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

c. Telecommand routing shall ensure that an on-board “blockage” resulting from payload commanding has no impact on platform commanding.

NOTE For example, an extensive command sequence for the configuration of a payload, which has no impact on the essential commanding of platform subsystems in parallel.

d. Where the allocation of on-board routes can be modified (e.g. using a table-based mapping of APIDs to MAPs), the capability shall be provided to request a report of the on-board routing and status information.

e. 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 capability shall be provided to perform complete and unambiguous verification of well-defined stages of telecommand execution.

NOTE This applies to telecommands that are sent directly from the ground or are stored on-board for release at a later time.

b. The potential stages of telecommand execution that can be verified shall include acceptance, start of execution, progress of execution and completion of execution.

NOTE These stages of telecommand execution are defined in ECSS-E-ST-70-41, clause 4.4.3.

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

d. Verification of execution stages subsequent to acceptance:

1. need not be performed, and
2. may be different for individual telecommands.

e. Failure of telecommand execution at any of the identified stages shall either be explicitly reported or unambiguously observable in the housekeeping telemetry.

NOTE ECSS-E-ST-70-41 service 1 can be used for this purpose.

f. The telecommand packet shall indicate, in its packet data field header, the reports of successful execution to be generated.

g. The selection possibilities for the reports of successful execution shall range from “no telecommand verification packets” to “verification at each distinct step of acceptance and execution”.

h. 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.

i. 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.

j. Failure in the acceptance or the execution of commands originating on-board shall be notified to the ground segment by means of anomaly event reports.

k. Verification of completion of execution of a telecommand shall use telemetry sampled at the same level as the device or function for which the 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.

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

m. 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.

n. Register load commands shall be confirmed by unique telemetry parameters dedicated to each commanded register, echoing exactly the currently loaded value.

5.6 Configuration management

5.6.1 Modes

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

1. "nominal" modes ensuring the generation of mission products;
2. "standby" modes ensuring safe operation of all spacecraft subsystems and payloads;

3. "survival" 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. The telemetry shall provide unambiguous identification of the modes and mode transitions.

d. The capability shall be provided to perform payload mode-switching at a high-level, e.g. by sending a single mode-switching telecommand from the ground which initiates all the corresponding low-level commands to bring the payload into the desired 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.

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. 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. Telemetry indicating the cause of an on-board reconfiguration shall be available to the ground segment after the completion of the reconfiguration.

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. With the exception of high-priority commands, all potentially critical configuration change telecommands initiated by the ground segment shall be buffered on-board in such a way that all parameters defining the new configuration can be inspected by the ground segment, via telemetry, before executing the change on-board.

h. 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.

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

j. The capability shall be provided to configure the timing of the individual actions within on-board sequences by ground commands.

k. The effect of each individual action within an on-board sequence shall be visible in the telemetry.

l. 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.

m. 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 on-board autonomy management functions shall be capable of performing all operations to continue mission operations for an autonomy duration of <AUT_DUR_EXEC>.

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. The on-board autonomy management functions shall be capable of performing all operations to safeguard the space segment for an autonomy duration of <AUT_DUR_FAIL> in the presence of a single failure.

NOTE This includes the time used by the ground segment to perform failure diagnosis and full recovery.

e. The fault management functions implemented on-board shall be designed such that the reaction time for the ground segment is not less than <ANOM_RESP_TIME>.

f. The ground segment shall be capable of overriding any on-board autonomous function.

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, 5.8.11 and 5.8.12, 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 5.8.9.

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 the case of F2, see below) to recover the on-board functions affected by the failure such that mission operations can continue.

The following autonomy levels can be identified:

- autonomy to safeguard the space segment or its sub-functions;
- autonomy to continue mission operations.
- These autonomy levels are summarized in Table 5-3.

Table 5-3: Mission execution autonomy levels

Level	Description	Functions
F1	Establish safe space segment configuration following an on-board failure	Identify anomalies and report to ground segment Reconfigure on-board systems to isolate failed equipment or functions Place space segment in a safe state
F2	Re-establish nominal mission operations following an on-board failure	As F1, plus reconfigure to a nominal operational configuration Resume execution of nominal operations Resume generation of mission products

The corresponding requirements for fault management are addressed in clauses 5.7.5.2 to 5.7.5.7. The general FDIR requirements and the failure detection and isolation requirements are applicable to autonomy levels F1 and F2, while the failure recovery requirements given in clause 5.7.5.5 are only applicable to autonomy level F2.

5.7.5.2 General FDIR

a. The space segment shall provide FDIR functions that take into account:

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. The FDIR design should not be overly cautious, e.g. if a detected anomaly can be isolated to a specific payload or subsystem, it should not trigger a full payload switch-off or a switch to a spacecraft safe mode.

d. If an FDIR function that is implemented in software is not available, a fallback mechanism shall be provided using an independent mechanism.

NOTE The independent mechanism can be a watchdog running on a separate unit or a hardware-based mechanism.

e. The FDIR functions shall make use of the redundancy implemented on board.

f. Any abnormal operational situation of the spacecraft, its subsystems, equipment or units shall be notified to or detectable by the next higher operational control instance (FDIR level).

g. 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.

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

i. 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.

j. The FDIR functions implemented on-board should be intrinsically failsafe.

k. 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.

l. 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.

m. The FDIR functions shall not be based on processing of an input that is currently disabled.

n. The FDIR design shall be modular such that the ground segment can enable and disable parts of it in a graceful and consistent manner without having a detrimental effect on the overall system.

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. A separate telemetry indication should be generated if the exception condition disappears.

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. If a failure detection function uses multiple inputs which are combined (e.g. OR/AND), then these inputs shall be independently derived, i.e. the inputs shall not come from the same source (e.g. unit), in case that source is faulty.

h. 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.

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

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. A failure in the performance of an autonomous recovery action shall be followed by an action to ensure the safety of the spacecraft, subsystem or payload.

NOTE In some cases, pre-defined retries are implemented in the system (e.g. for protocol handling).

d. Where FDIR functions trigger an autonomous recovery to redundant units, the capability shall be provided to independently specify by telecommand the units to be monitored (for failure detection) and the combination of units to be selected for the recovery activities (from the available combinations).

5.7.5.6 Fault management level F1

a. The safety of the space segment and its sub-functions shall be ensured for a predefined period <AUT_DUR_FAIL> in the presence of a single on-board failure and in the absence of ground segment intervention.

b. After detection of an on-board failure that threatens space segment safety, the Level F1 fault management functions shall trigger reconfiguration activities leading to an on-board safe state.

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

d. The spacecraft shall not enter survival mode if no hazard exists that affects spacecraft or payload health or mission objectives.

NOTE In particular, this implies a robustness of the implementation of the hierarchical FDIR to cope with minor errors (e.g. operational errors resulting from a single telecommand issued in the wrong context) without causing entry into survival mode.

e. Recovery from survival mode shall be undertaken under ground control.

5.7.5.7 Fault management level F2

a. The failed function shall be restored within a mission-specified interval of time.

b. The on-board fault management function shall autonomously establish a fully operational configuration such that mission operations can continue, including the generation of the mission products.

5.8 Requirements specific to the telemetry and telecommand packet utilization standard

5.8.1 Application process and service design

a. The capability shall be provided for the ground segment to exercise control over an application process.

NOTE As a minimum this includes "reset".

b. The application process identifier (APID) shall uniquely identify the on-board address indicating the source (telemetry source packets) or destination (telecommand packets) of packets.

c. Different platform subsystems and payloads should be assigned different sets of APIDs.

d. The assignment of APIDs shall remain unchanged during the mission.

e. If the on-board design includes functions providing services and capabilities for which there is a standard service defined in ECSS-E-ST-70-41 clause 5.5, these services and capabilities should conform to ECSS-E-ST-70-41, clauses 6 to 21.

f. The structure of all variable telemetry and telecommand packets shall conform to ECSS-E-ST-70-41, clauses 5.3 and 5.4.

g. Each telecommand packet shall be characterized by its destination service type and by a service subtype indicating the type of function or activity requested to be executed by the service.

h. All telemetry packets containing a data field header shall include type and subtype fields which appear in the same location.

i. The structure of a telemetry packet containing a data field header shall be derivable from the combination of its APID, type and subtype and up to two auxiliary packet identification fields.

NOTE For example, the structure ID (SID) in ECSS-E-ST-70-41 housekeeping packets.

j. All telemetry packets of the same type and subtype shall contain the auxiliary identification fields at the same location and with the same width.

k. The combination of APID, packet type, subtype and auxiliary identification fields shall be uniquely assigned across the complete spacecraft (i.e. across all application processes generating telemetry).

l. Variable packet structures shall only be used for event-driven or request-driven telemetry packets.

NOTE This does not apply to payload measurement data.

m. The "Parameter#" used on-board to identify telemetry parameters shall be uniquely assigned across the complete spacecraft.

NOTE For the "Parameter#" used on-board to identify telemetry parameters, see ECSS-E-ST-70-41 for additional information.

n. The choice structure corresponding to a given value of a choice parameter shall be unique for the complete spacecraft.

NOTE For the choice structure corresponding to a given value of a choice parameter (see ECSS-E-ST-70-41 for additional information).

5.8.2 Statistical data reporting

a. The capability shall be provided to report statistics relating to a specified set of parameters over an interval of time.

b. The capability shall be provided to report maximum, minimum and mean values and the standard deviation.

c. The capability shall be provided to add and delete parameters from the set being evaluated.

d. The capability shall be provided to clear the set of parameters being evaluated.

e. The capability shall be provided to reset the evaluation of parameter statistics.

f. The capability shall be provided to request a report of the current set of parameters being evaluated.

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 to load a contiguous memory area (e.g. by specifying the start address and the data to be loaded).

c. The capability shall be provided to perform scatter loads with a single telecommand message (e.g. by specifying sets of start address and data to be loaded).

d. As part of the on-board acceptance of a memory load, the destination application process shall be able to detect data corruptions.

e. The on-board end-to-end verification of a memory load shall consist of confirming that the data has been correctly loaded into its destination memory (by reading it back from the memory and comparing it with the load data).

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

g. The capability shall be provided to request a memory dump from a contiguous memory area (e.g. by specifying the start address and the length of the dump).

h. A single memory dump telemetry packet shall only contain data from memory areas containing contiguous on-board memory addresses.

NOTE If a dump is requested across one or more discontinuities in memory address (e.g. due to memory pages), this implies that the memory dump uses different telemetry packets that are aligned with the address discontinuities.

i. The capability shall be provided to request scatter dumps (e.g. by specifying sets of start addresses and length of the dump).

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

k. The on-board system shall not impose artificial constraints on the uplink speed of memory load command or memory dump command.

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

m. The capability shall be provided to request a memory check of a contiguous memory area (e.g. by specifying the start address and the length of the area to be checked).

n. The capability shall be provided to request a memory check of several areas with a single telecommand message (e.g. by specifying sets of start addresses and lengths of areas to be checked).

o. In response to a request to check memory, the on-board action shall be to perform a checksumming over the requested address ranges and report the result to the ground segment.

p. 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.

q. Memory loads should be permanently available on-board to avoid time-consuming memory re-loads from the ground following memory switch on.

NOTE For example, using EEPROM.

5.8.4 Function management

a. The specialized ground-controllable tasks of an application process should be implemented using the "Function management service" specified in ECSS-E-ST-70-41.

b. The capability shall be provided for the ground segment to invoke a function and to pass instantiation parameters to it, by means of a single telecommand.

5.8.5 On-board operations scheduling

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

NOTE This restricts the maximum usable packet length of a telecommand, since it is a command embedded within an "insert-into-schedule" telecommand.

b. The capability shall be provided to edit the on-board operations schedule (insert, append and delete telecommands).

NOTE Although it can be assumed that most telecommands are appended (i.e. uploaded in execution time order), no constraint is imposed on the order in which telecommands are uploaded.

c. The capability shall be provided to perform the editing operations without stopping the schedule.

d. The capability shall be provided to start and stop the on-board operations schedule.

e. The on-board operations schedule shall consist of sub-schedules that can be individually controlled (started and stopped).

f. The capability shall be provided to time-shift (i.e. advance or retard) a selected set of telecommands that have already been loaded in the on-board operations schedule.

NOTE This function is used to support the re-scheduling of operations and to avoid having to delete and re-load the affected telecommands.

g. The capability shall be provided for a telecommand released from the on-board operations schedule to set an interlock on (i.e. condition the release of) subsequent telecommands within the same sub-schedule.

h. The capability shall be provided to request a report of the contents of the on-board operations schedule.

i. The capability shall be provided to perform all editing operations on the schedule even when it is in a stopped state.

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

k. 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.

l. 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.

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

n. A telecommand loaded into the on-board operations schedule with an on-board release time earlier that the current on-board time (OBT) shall be rejected.

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

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

q. Management of the memory area used for the on-board operations schedule shall be performed autonomously on-board and shall not restrict schedule operation or schedule editing operations.

r. The execution of each telecommand released from the on-board operations schedule shall result in the generation of either a “successful completion of execution” or an “execution failure” verification report.

5.8.6 On-board monitoring

a. The capability shall be provided to monitor on-board a set of on-board parameters defined by ground segment.

NOTE All telemetry parameters are normally available to the on-board monitoring function.

b. The on-board monitoring capabilities shall include limit-checking, expected-value-checking and delta-checking.

c. The capability shall be provided to specify more than one mode-dependent monitoring check for a given parameter.

NOTE "Mode dependent" means that the check is only applied if the corresponding mode is TRUE. In the event that more than one mode is contemporaneously TRUE, all corresponding checks are applied.

d. The capability shall be provided to enable and disable either the complete on-board monitoring function or selected parameters in the "monitoring list".

e. The capability shall be provided to add parameters and their monitoring information to the on-board monitoring list.

f. The capability shall be provided to modify the monitoring characteristics of a parameter, including limit sets, expected value checks, delta checks and filtering characteristics.

g. The capability shall be provided to modify parameter monitoring information without having to first delete the parameter and then add it again to the monitoring list.

h. The capability shall be provided to clear the complete on-board monitoring list or to delete selected parameters from it.

i. If the on-board monitoring list contains checks that are used by on-board FDIR functions, then the clear command shall be implemented as a mission-critical command.

j. All changes of monitoring status shall be reported to the ground segment by means of a "check transition" telemetry packet.

NOTE For example, a check transition telemetry packet produced when a parameter goes out-of-limits and when it subsequently returns back into limits.

k. The capability shall be provided for a change of monitoring status to give rise to an event report.

NOTE 1 This capability is used when an on-board action is defined for execution when this check transition occurs (see clause 5.8.12).

NOTE 2 This capability is not provided as a standard on-board monitoring service capability by ECSS-E-ST-70-41.

l. The capability shall be provided to request a report of the contents of the monitoring list including the parameter monitoring characteristics.

m. The capability shall be provided to request a report of the full set of parameters that are currently in violation of any of their monitoring checks.

n. The capability shall be provided to perform all editing operations on the on-board monitoring function even when it is in a disabled state.

5.8.7 Large data transfer

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. When transferring a set of data that exceeds the maximum packet size specified for the mission (e.g. memory loading or dumping), the capability shall be provided to transfer this data in more than one packet (part packet).

d. The capability shall be provided to send part packets with or without intermediate acknowledgement of receipt.

e. In the event that the transfer of a part packet to its destination is not successful, the capability shall be provided to transfer succeeding part packets.

NOTE The procedure used for the large data transfer protocol is defined in Clause 16 of ECSS-E-ST-70-41.

5.8.8 Telemetry generation and forwarding

a. The capability shall be provided to selectively enable and disable the forwarding of telemetry source packets to the ground segment.

b. The capability shall be provided to enable and disable telemetry source packet generation at the level of the originating service.

c. The capability shall be provided to request a report of which telemetry source packets generated by an application process are currently disabled for forwarding to the ground segment.

5.8.9 On-board storage and retrieval

a. For missions with intermittent ground coverage, the on-board storage capability shall be able to store all packets generated on-board for space segment monitoring and control purposes, for a duration at least equal to the longest non-coverage period.

b. For missions with continuous ground coverage, loss of one-shot packets (i.e. event-driven or request-driven packets) shall be remedied by the short-term on-board storage of the last <PKTS_NUM_STORED> packets.

NOTE This includes telecommand verification packets (they are effectively request-driven).

c. An on-board store shall be provided containing an "anomaly log" of all event or request-driven packets reporting on-board anomalies.

NOTE For example, autonomous switch-downs and command failure reports.

d. The content of the anomaly log specified in requirement 5.8.9c shall be persistent even after a reconfiguration or a cold restart of the application process managing the store.

e. On-board storage shall be such that the ground segment can retrieve the stored packets within specified delays <PKT_RETR_DELAY>.

NOTE 1 For example, packets of high operational significance, such as error or anomaly packets, processed on the ground with shorter delays than routine status reporting packets.

NOTE 2 There can be several such parameters for a given mission corresponding to data of different operational significance.

f. 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.

g. For each independent on-board store, the capability shall be provided for the ground segment to enable and disable the storage function.

h. For each independent on-board store, the capability shall be provided to specify the packets to be stored by adding or removing packets from a list maintained on-board.

i. The capability shall be provided to select a given telemetry packet to be stored in more than one on-board store.

j. On-board stores shall be either circular, where the oldest data is automatically overwritten when the store is full, or linear, where storage terminates when the on-board store is full.

k. The capability shall be provided for the ground segment to clear the contents of a linear on-board store.

l. The capability shall be provided to configure a linear packet store such that packets can be overwritten once they have been dumped and their reception has been acknowledged by the ground segment.

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

n. The capability shall be provided for the ground segment to request the retrieval of all packets from an on-board store or to specify a time window or a packet range for the retrieval.

o. The capability shall be provided to request the retrieval of telemetry packets that have previously been retrieved (provided they have not yet been overwritten).

p. The capability shall be provided to suspend and resume the retrieval of stored telemetry packets.

q. When resuming a retrieval, it shall continue from the point where it was suspended.

r. Housekeeping information shall be provided on the state of the on-board storage and retrieval function for each on-board store.

NOTE For example, fill level, pointer addresses.

5.8.10 On-board traffic management

a. The on-board packet distribution system shall generate a report whenever a problem arises with the on-board traffic.

NOTE For example, a bottleneck in the distribution of telecommand packets or of telemetry source packets on the packet bus.

b. Control capabilities shall be provided such that the ground segment can resolve all pre-identified on-board problems relating to telecommand packet re-assembly, telemetry data handling or on-board traffic.

c. Packet bus management and resource parameters, such as average and peak bus loading and numbers of packet retransmissions, shall be routinely reported to the ground segment.

5.8.11 On-board operations procedures

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

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

c. The control operations shall include load, delete, start, stop, suspend, resume and transfer parameters.

d. The ground segment shall be able to request a report of the currently active on-board operations procedures.

e. The ground segment shall be able to request a report of the currently loaded on-board operations procedures.

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

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

h. 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.

5.8.12 Event-to-action coupling

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.

c. The ground segment shall be able to add and delete event-to-action definitions to and from an on-board list and to request a report of the list.

d. The capability shall be provided to enable and disable individual actions without having to delete the event-to-action definition.

e. The triggering of an on-board action shall itself give rise to an event report.

5.9 Equipment- and subsystem-specific

5.9.1 On-board processors and software

a. The design (selection) of on-board processors shall ensure that the available memory and performance accommodates, with a margin of <RESOURCE_MARGIN>:

1. the requirements of the baseline (i.e. as launched) processes, and
2. a realistic allocation for processes and data to be developed and loaded after launch.

b. If 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 either that:

- the operational context need not be reloaded from the ground segment, or
- the new processor can be loaded with a safe default context before the switchover.

c. A processor switchover should not invalidate telecommands not yet released from any ground schedule.

NOTE This implies that telecommands defined for the prime unit are also valid for the redundant unit, except for any command routing data which the ground system can automatically change when addressing the redundant processor.

d. 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.

e. 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.

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

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

h. The capability shall be provided for the ground segment to patch the nominal software directly.

i. The contents of a RAM of a unit or instrument that is suspended or switched off as a result of an FDIR action shall be preserved so that the ground segment can dump the content for the purposes of failure investigation.

j. Enabling of on-board software should use only a single telecommand.

NOTE This does not preclude dual-step commanding because only the final command enables the software.

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

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

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

m. Whenever a processor is running synchronously scheduled tasks, it shall check at the end of each software cycle that all tasks scheduled for that cycle have been duly completed.

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

o. A processor overload condition should not automatically lead to the processor being halted.

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

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

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

s. Whenever a memory corruption is detected by an error detection and correction mechanism, an event report shall be generated.

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

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

v. 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.

5.9.2 Power supply and consumption

a. The power telemetry parameters assigned shall be such that the power available and power demand 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 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 that have primary power consumption greater than <POW_CONS_THRESH>, a thermistor on a hot point or a primary current sensor shall be provided and made available in telemetry.

d. The power for telemetry conditioning of equipment shall be hierarchically structured to avoid the generation of invalid telemetry (which could in turn trigger unnecessary recovery actions).

e. The power for telemetry conditioning of equipment shall not be supplied from other unrelated units that are not permanently powered.

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

g. The capability shall be provided to redefine the list of non-essential loads to be shed in the event of a power anomaly (e.g. battery undervoltage).

h. The capability shall be provided to change the state of a critical relay without powering it on.

5.9.3 Telemetry, tracking and command (TT&C)

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

b. Except following the occurrence of post-launch failures, the ground segment shall not be enabled to achieve by command a state where less than two receivers are active.

c. The combined coverage of all on-board TT&C antennas shall be such that telemetry and telecommand contact can be provided under specified attitude and orbit conditions.

NOTE This does not imply ensuring full ground segment coverage during all mission phases, but rather that the spacecraft can be accessed when specified.

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.

5.9.4 Attitude and orbit control

a. Telemetry generated by sensor elements shall be assigned to dedicated telemetry channels (i.e. parameters) in order to be able to monitor all sensors (whether used or not) for diagnostic purposes.

b. The operating ranges of on-board sensors shall accommodate all operational scenarios with adequate margins.

c. The telemetry of stimulated detectors shall be designed to handle all flight-phase conditions either in normal mode telemetry or by mode-switching to extended range.

d. Housekeeping telemetry shall be continuously available to enable verification of the operation of on-board attitude control functions and the results of any on-board attitude determination.

e. Telemetry monitoring of thruster actuation shall be provided to enable thruster on-time surveillance and fuel consumption determination.

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

g. Means shall be provided for determining from telemetry the remaining fuel in each independent propellant system.

h. The accuracy for determination of the amount of remaining fuel at any given point in the mission shall be related to the amount of fuel remaining, as agreed with the customer.

NOTE 1 This accuracy depends on the particular mission planning requirements.

NOTE 2 An accuracy of 5 % is normally acceptable at the start of the mission; however, when there is only 10% of the fuel remaining, the acceptable accuracy is normally about 10% to 20%.

5.9.5 Mechanisms

a. One-shot drivable mechanisms shall be provided with both hard and soft end-stops, independently telemetred.

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 position of all mechanisms shall be known for all anticipated operations.

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

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.

5.9.7 Payload

a. The design of the payload shall include taking protective action against potential damage caused by the external environment.

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

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

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 housekeeping 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.

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_DATA>

interval of time for which the space segment can store mission data on-board

<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.

<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

<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

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	
4.4a	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).
4.4b	X			X	
4.5a		X			
4.5b		X	X		
4.5c		X	X		
4.5d		X	X		
4.5e		X	X		
4.5f		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.
4.6d			X	X	
4.6e			X		Loss of capability to control the space segment in case of failures of automatisms.

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
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.
4.6g			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.
4.6h				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			
5.2.1c	X	X			
5.2.2a	X			X	High availability requirement on the ground segment which leads to the implementation of special ground functionality.
5.2.2b	X			X	
5.2.2c				X	

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
5.2.2d				X	Delays leading to inefficiencies in executing operations.
5.2.3a	X			X	More complex ground processing. Inefficient use of downlink bandwidth.
5.2.3b	X			X	
5.2.3c	X			X	
5.2.3d				X	Impact on the mission return if data recovery is part of the nominal operations to avoid data losses.
5.2.3e	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.
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	

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
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				
5.3.1u	X				
5.3.1v	X				
5.3.1w	X				
5.3.1x				X	
5.3.1y				X	Loss of flexibility to reduce the update and downlink rate of parameters (less frequent parameter updates or fewer packets).
5.3.1z	X			X	
5.3.1aa	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.
5.4b	X			X	Implementation of special ground processing.

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
5.4c				X	
5.4d				X	
5.4e				X	
5.4f				X	
5.4g	X			X	Implementation of special ground processing.
5.4h	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.
5.4i	X			X	Implementation of special ground processing.
5.4j			X	X	Ambiguity of telemetry.
5.4k			X	X	Potential inability to achieve the mission objectives if the specified timing accuracy is not provided.
5.4l			X		
5.4m	X			X	
5.4n				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	
5.5.1d				X	
5.5.1e				X	
5.5.1f	X		X	X	Higher complexity of the configuration control of commands. Risk of sending commands in the wrong context.

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
5.5.1g	X			X	
5.5.1h		X	X		
5.5.1i			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.
5.5.1j			X	X	Potential impact on the control of the space segment in specific failure situations.
5.5.1k	X			X	
5.5.1l	X			X	Increase in the size of the operational database and higher complexity of the configuration control task.
5.5.1m	X			X	
5.5.1n	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		
5.5.3a				X	Cumbersome uploading of memory load commands and the imposition of severe restrictions on the operations.
5.5.3b	X			X	
5.5.3c			X	X	
5.5.3d				X	
5.5.3e	X			X	
5.5.4a			X	X	
5.5.4b			X	X	

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
5.5.4c				X	
5.5.4d				X	
5.5.4e	X			X	
5.5.4f	X			X	
5.5.4g	X			X	
5.5.4h				X	Impact on the definition of efficient control procedures and command sequences.
5.5.4i			X	X	
5.5.4j	X			X	
5.5.4k				X	
5.5.4l			X	X	
5.5.4m			X	X	
5.5.4n	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.
5.6.2c				X	
5.6.2d				X	

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
5.6.2e			X	X	Impact on the detection of possible on-board failures.
5.6.2f				X	
5.6.2g			X	X	
5.6.2h		X	X		
5.6.2i	X	X	X		Potential entry of the space segment into a hazardous status if ground contact cannot be guaranteed.
5.6.2j			X		
5.6.2k				X	
5.6.2l			X		
5.6.2m		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	
5.7.5.2a	X		X	X	
5.7.5.2b			X		
5.7.5.2c			X		
5.7.5.2d		X	X		Impact on the safety of the space segment in the event of on-board processor failures.
5.7.5.2e			X		

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
5.7.5.2f			X		
5.7.5.2g			X		
5.7.5.2h			X	X	
5.7.5.2i			X	X	Impact on the identification of a non-nominal on-board behaviour.
5.7.5.2j		X	X		Potential entry of the space segment into dangerous configurations.
5.7.5.2k			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.
5.7.5.2l			X	X	ility of the ground to correct the on-board configuration in the event of performance degradation or on-board failures.
5.7.5.2m		X	X		
5.7.5.2n			X	X	
5.7.5.3a			X	X	
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.
5.7.5.3g		X	X		
5.7.5.3h				X	Reduced probability of safety mechanisms working.

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
5.7.5.3i			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		
5.7.5.5d		X	X		Potential failure of recovery if faulty equipment is used.
5.7.5.6a	X	X	X		
5.7.5.6b		X	X		
5.7.5.6c		X	X		
5.7.5.6d			X	X	Potential inappropriate entry of the space segment into survival states, which impacts the mission return.
5.7.5.6e			X	X	
5.7.5.7a			X	X	
5.7.5.7b				X	
5.8.1a			X	X	Loss of control of on-board processes in case of failures.
5.8.1b	X			X	
5.8.1c				X	
5.8.1d				X	Potential high complexity of the configuration control task on ground.

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
5.8.1e	X				Implementation of special ground processing functions and inability to reuse the standard infrastructure.
5.8.1f	X				
5.8.1g	X				
5.8.1h	X				
5.8.1i	X				
5.8.1j	X				
5.8.1k	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.
5.8.1l	X				
5.8.1m	X				Potential high complexity of the configuration control task on ground.
5.8.1n	X				
5.8.2a				X	Impact on long periods without ground coverage and on downlink efficiency.
5.8.2b				X	
5.8.2c				X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
5.8.2d				X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
5.8.2e				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
5.8.2f				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.
5.8.3b	X			X	
5.8.3c	X			X	
5.8.3d			X		
5.8.3e	X			X	
5.8.3f				X	
5.8.3g	X			X	
5.8.3h	X			X	High complexity of the processing of dump data.
5.8.3i	X			X	
5.8.3j	X			X	
5.8.3k	X			X	
5.8.3l				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.
5.8.3m	X			X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
5.8.3n	X			X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
5.8.3o	X			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
5.8.3p			X		
5.8.3q	X			X	
5.8.4a	X			X	Implementation of special ground processing functions, if this functionality is provided and ECSS-E-ST-70-41 is not followed.
5.8.4b	X			X	
5.8.5a				X	
5.8.5b				X	Significant impact on the execution of the operations.
5.8.5c				X	
5.8.5d				X	
5.8.5e				X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
5.8.5f				X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
5.8.5g			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.
5.8.5h				X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
5.8.5i				X	
5.8.5j				X	Endangering of the safety of the space segment if the space segment autonomy is not ensured.
5.8.5k				X	Potential inefficient use of the on-board operations schedule.
5.8.5l				X	Potential sending of commands in the wrong context.

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
5.8.5m			X	X	Potential sending of commands in the wrong context.
5.8.5n			X	X	
5.8.5o				X	
5.8.5p			X	X	Potential entry of the space segment into a dangerous state.
5.8.5q	X			X	
5.8.5r				X	
5.8.6a			X	X	Reduction of the on-board autonomy and potential inability to detect anomalies in time.
5.8.6b			X	X	
5.8.6c			X	X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
5.8.6d			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.
5.8.6e			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.
5.8.6f			X	X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
5.8.6g				X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
5.8.6h				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
5.8.6i		X		X	
5.8.6j	X			X	
5.8.6k				X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
5.8.6l	X			X	Implementation of a complex ground model. This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
5.8.6m				X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
5.8.6n				X	
5.8.7a	X			X	
5.8.7b	X			X	
5.8.7c	X			X	
5.8.7d				X	
5.8.7e				X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
5.8.8a				X	Inability to use the available telemetry bandwidth in an efficient manner and potential overflow in case of a failed application.
5.8.8b				X	Potential overflow in case of a failed application.
5.8.8c				X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
5.8.9a				X	Impact on the on-board autonomy and the completeness of the data. The functionality to be provided depends on the mission characteristics.

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
5.8.9b				X	
5.8.9c				X	
5.8.9d				X	
5.8.9e				X	
5.8.9f				X	
5.8.9g				X	
5.8.9h				X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
5.8.9i				X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
5.8.9j				X	
5.8.9k				X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
5.8.9l				X	
5.8.9m				X	
5.8.9n				X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
5.8.9o				X	This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
5.8.9p				X	
5.8.9q				X	
5.8.9r				X	
5.8.10a			X	X	Reduced probability of detecting on-board malfunctions.

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
5.8.10b			X	X	
5.8.10c				X	
5.8.11a			X	X	Potential non-compliance of the achieved on-board autonomy with the mission goals.
5.8.11b				X	
5.8.11c				X	
5.8.11d	X			X	Implementation of complex ground models. This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
5.8.11e	X			X	Implementation of complex ground models. This requirement corresponds to an optional capability of the corresponding ECSS-E-ST-70-41 service.
5.8.11f				X	
5.8.11g				X	
5.8.11h		X		X	
5.8.12a		X	X	X	Potential non-compliance of the achieved on-board autonomy with the mission goals.
5.8.12b		X	X	X	Potential non-compliance of the achieved on-board autonomy with the mission goals.
5.8.12c	X			X	
5.8.12d				X	
5.8.12e				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.
5.9.1a				X	Loss of flexibility to handle changes of the performance and functions of the space segment.
5.9.1b			X	X	

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
5.9.1c			X	X	Potential sending of commands in the wrong context.
5.9.1d	X			X	
5.9.1e			X	X	
5.9.1f			X	X	Potential inefficient use of the on-board processors.
5.9.1g			X	X	
5.9.1h			X	X	
5.9.1i		X	X	X	
5.9.1j				X	
5.9.1k	X			X	
5.9.1l			X	X	
5.9.1m			X	X	
5.9.1n			X	X	
5.9.1o		X	X	X	
5.9.1p			X	X	
5.9.1q			X	X	
5.9.1r			X	X	
5.9.1s			X	X	
5.9.1t			X	X	
5.9.1u			X	X	
5.9.1v				X	
5.9.2a			X	X	
5.9.2b			X	X	

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
5.9.2c			X	X	
5.9.2d			X		
5.9.2e			X		
5.9.2f		X	X		
5.9.2g			X		
5.9.2h			X	X	
5.9.3a			X		
5.9.3b		X	X		
5.9.3c			X	X	
5.9.3d			X	X	
5.9.4a	X		X	X	
5.9.4b		X	X		
5.9.4c			X	X	
5.9.4d			X	X	
5.9.4e			X	X	
5.9.4f	X		X	X	
5.9.4g			X	X	
5.9.4h			X	X	
5.9.5a			X	X	
5.9.5b			X	X	
5.9.5c			X	X	
5.9.5d			X	X	

Requirement	Ground segment function	Space segment safety	Space segment and mission degradation	Ops impact	Tailoring out implications
5.9.5e	X			X	
5.9.6a			X	X	
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