DRAFT INTERNATIONAL STANDARD ISO/DIS 14950

ISO/TC **20**/SC **14**

Secretariat: **ANSI**

Voting begins on
2002-01-03

Voting terminates on
2002-06-03

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION

Space systems — Unmanned spacecraft operability

Systèmes spatiaux — Opérabilité des engins spatiaux non habités

ICS 49.140

Contents

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

International Standard ISO 14950 was prepared by Technical Committee ISO/TC 20, *Aircraft and space vehicles*, Subcommittee SC 14, S*pace systems and operations*.

Introduction

The **operation** of a spacecraft is an activity performed from a mission control centre in order to:

a) ensure provision of mission and science products/services;

b) carry out routine housekeeping operations;

c) recover from on-board contingencies;

d) manage on-board resources in order to maximise the provision of products/services and the mission lifetime.

The **operability** of a spacecraft is the capability of the space segment to be operated by a ground segment comprising hardware, software, personnel, and procedures, during the complete mission lifetime of the spacecraft, by using a minimum of resources, while maximising the quality, quantity, and availability (or timeliness of delivery) of mission products, without compromising spacecraft safety. The key factors that determine the operability of a spacecraft are:

e) the ability to control the spacecraft in any nominal or non-nominal scenario in order to maintain the mission availability;

f) the capability to manage on-board resources and to maximise the mission lifetime;

g) the extent to which its operations are routine and non-hazardous, thus minimising ground segment resources for all operations including fault avoidance and correction;

h) the flexibility of the design for spacecraft reconfiguration, including software, in orbit;

i) the reliability of operations and robustness against human error;

j) the simplicity of the space and ground segment required to fulfil the mission requirements and respect the mission constraints.

k) the autonomous capability of the space systems

l) the complexity and interdependance of the flight system

Spacecraft operability can be quantified by the following measures:

the capability to detect abnormal trends or status and the speed of reconfiguration back to an operational mission to minimise duration of outage;

the number of staff required to operate the spacecraft during the operational phase and to maintain the ground segment;

the qualification level of staff required to perform operations;

the quantity and complexity of mission-specific knowledge required to perform operations.

Spacecraft operability is an input to total life cycle cost. Increased operability will, in general, decrease operations and maintenance costs but increase development costs. Thus, specific operability goals should be determined by careful balancing of costs, risks, and schedules for both procurement and operations/maintenance.

The key objectives of this International Standard are:

to ensure that a spacecraft operates in a safe and cost-effective manner and may be operated with an optimised workload;

to facilitate and/or enhance the tasks of preparation for, execution and evaluation of, spacecraft check-out and mission operations activities;

to facilitate the tasks of spacecraft prime contractors when preparing a proposal in answer to an international request for proposal (RFP).

This International Standard is written in such a way that technological advances will not invalidate the standard. Thus, this standard is not project or machine specific.

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

Conventions

Requirements are identified by an acronym, which indicates the nature/grouping of the requirement, followed by a serial number, and appear in bold type (e.g., **OBSERV-0010)**. The serial number comprises four digits starting at 0010 and is incremented by 10 to facilitate configuration control for later versions of the document. Where a major requirement is broken down into subsidiary requirements, the serial number is extended to reflect this structure (e.g., **TEST-1010.1** would represent the first sub-requirement of requirement 1 relating to Testability). General operability requirements are numbered in the range 0010 to 0999, while detailed operability requirements are numbered in the range 1010 to 1999.

Some of the detailed operability requirements in clause 6 are only relevant for a given level of on-board autonomy. In such cases, the corresponding autonomy level (as defined in clause 4), is indicated as a super-script following the requirement ID. For example, **FAULT-1100^{C3}**.

Some requirements introduce quantities for which values cannot be defined across the board but will need to be defined on a mission-by-mission basis (e.g., time intervals, response times, etc.). These are termed mission constants and are identified within this International Standard in «<>» (for example, <TC_VERIF_DELAY>) and, where appropriate, typical values may be indicated. These mission constants are also summarised, for information only, in Annex A.

Guidelines for applicability

This International Standard specifies a set of general operability requirements and a set of detailed operability requirements. Many of the detailed operability requirements apply to specific on-board functions. The general operability requirements are intended to be applicable to spacecraft missions of all classes (i.e., science, telecommunications, meteorology, Earth observation, geostationary, low-Earth orbiting and interplanetary).

The steps for designing a new mission are normally:

m) the mission constraints are identified (e. g., design constraints, cost constraints);

n) the mission operations concept is developed, including the level of on-board autonomy for routine and contingency operations;

o) the spacecraft is designed, based on m) and n) above.

The applicability of the detailed requirements in this International Standard should be determined during step m). As indicated above, some of the detailed requirements are only applicable to a given level of autonomy.

During step o), the mission operations concept and the applicability of the detailed requirements may be iterated.

Space systems — Unmanned spacecraft operability

1 Scope

This International Standard defines the essential properties pertaining to the operation of unmanned spacecraft and defines requirements and guidelines for spacecraft on-board functions in order to enable the spacecraft to be operated in any nominal or predefined contingency situation.

2 Terms and definitions

For the purposes of this International Standard, the following terms and definitions apply:

2.1 Categories of operability

2.1.1
commandability
the ability of the ground to safely control and configure all the equipment and software on-board the spacecraft as required for the execution of the nominal mission, for failure identification and recovery, for performance assessment and for system maintenance subsequent to performance change and system degradation

2.1.2
compatibility
the extent to which the design of the space segment conforms with the existing ground segment infrastructure (if any) and with existing operational practices

2.1.3
efficiency
the optimum distribution of tasks between the ground and space segments taking into account cost, complexity, technology and reliability

2.1.4
flexibility
the capacity to configure and make optimum use of:

> existing on-board functions,

> space-earth communications links,

> any redundancy built into the design in order to meet reliability targets,

as well as the capacity to optimise missions products according to the mission events

2.1.5
observability
the ability to acquire operationally significant information for physical and logical parameters on-board the spacecraft.

NOTE 1   This information is delivered to the ground through the telemetry channel and/or made available to on-board processors.

NOTE 2   The definition of observable parameters is a key requirement for operating spacecraft, monitoring the behaviour of all on-board systems, performing diagnosis of anomalies, and collecting sufficient information for feedback into ground-based models.

2.1.6
safety
the extent of on-board protection against failure and the provision of fail-safe modes of operation

2.1.7
security
the extent of on-board protection against unauthorised access to on-board telecommand functions, jamming of the telecommand channel, or corruption of the telecommand data, unauthorised access to telemetry data, or the corruption of these data

2.1.8
testability
the capability and ease with which the functions of the spacecraft and its interfaces and compatibility with ground systems can be verified and validated

NOTE   In particular, this relates to functions that do not form part of the current operational chains (i.e., redundant functions).

2.2   Other terms

2.2.1
application process
an on-board element capable of generating telemetry source data and receiving telecommand data.

NOTE   An application process may be implemented in software, firmware, or hardware. There are no restrictions on the mapping between application processes and the usual functional subdivision of a spacecraft into subsystems and payloads. In a relatively simple spacecraft, there may be a centralised application process that provides a number of "dumb" platform subsystems and payloads with collection of housekeeping data, the distribution of device commands, on-board scheduling, on-board monitoring, etc. In a more complex spacecraft, each subsystem and payload might be served by its own independent application process. A given processor may host one or several application processes. However, it is also possible that a given application process could be distributed across two or more processors.

2.2.2
autonomy
the extent to which a spacecraft can handle nominal and/or contingency operations without ground intervention

2.2.3
chain
a set of hardware and/or software units that operate together to achieve a given function

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.

2.2.4
control loop
the mechanisms to maintain a parameter or a set of parameters within prescribed limits

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

2.2.5
device telecommand
a telecommand that is routed to and executed by on-board hardware

EXAMPLE   a relay switching telecommand, a telecommand to load an on-board register

2.2.6
ground segment
all ground facilities and personnel involved in the preparation and/or execution of mission operations

2.2.7
high level telemetry
telemetry derived from the low level telemetry by an on-board application process

2.2.8
low level telemetry
the lowest level of readable on-board information

EXAMPLE   register readout, relay status

2.2.9
memory
any on-board memory area, whether main memory or storage memory, such as disk, tape, or bubble-memory

2.2.10
mission management
on-board functionality that allows a mission to undertake routine operations highly autonomously with the minimum of ground intervention

2.2.11
mission manager
an on-board function that supervises (or performs) the system-level mission management activities

NOTE 1   Future autonomy concepts foresee a distributed on-board "control authority" that is able to manage functions at both system-level and subsystem-level.

NOTE 2   Within this concept, the mission manager supervises the execution of high-level instructions from the ground expressed as mission goals.

NOTE 3   The mission manager performs all the system-level functions, while subsystem (and payload) managers perform the subsystem-level functions.

2.2.12
no ground contact
the period of time during a mission when ground contact is not possible due to the unavailability of the telecommand/telemetry links

The reasons for this unavailability may include:

a)   predictable events such as:

    1)   non-permanent visibility due to spacecraft orbit characteristics combined with radio frequency coverage of telemetry and telecommand links;

    2)   time-shared access to the spacecraft.

b)   unpredictable events such as:

    1)   spacecraft attitude depointing;

    2)   on-board failure of the telemetry and telecommand links;

    3)   ground station failure/unavailability;

    4)   link budget degradation.

2.2.13
on-board fault management
on-board functionality that allows the detection and management of on-board failures without ground intervention

NOTE 1   The primary objective of on-board fault management is to ensure the survival of the spacecraft

NOTE 2   Where possible without hazard to the spacecraft, and within the mission constraints, on-board fault management shall maintain payload operations

NOTE 3   In addition, on-board fault management should assist in rapid diagnosis and subsequent reconfiguration back to an optimal operational status.

2.2.14
on-board monitoring
a set of processing functions that is applied to a set of on-board parameters

NOTE 1   These functions may include limit/status/delta checking, the evaluation of statistics, including minimum and maximum values over a time interval, etc,

NOTE 2   Detected events or evaluation results are telemetred to ground

NOTE 3   The scope of the function may be even wider, e.g., to include the triggering of on-board actions in response to detected events.

2.2.15
on-board operations scheduling
a capability for controlling and executing commands that were loaded in advance from the ground

NOTE   In its simplest form, the on-board operations schedule stores time-tagged commands loaded from the ground and releases them to the destination application process when their on-board time is reached, but with no feedback being generated by the destination application process.

2.2.16
on-board operations procedure
a simple operations procedure that can be controlled from ground (loaded, edited, started, stopped, etc.) or can be invoked by the occurrence of a predefined on-board event

NOTE   In its simplest implementation, an operations procedure may consist of a sequence of low-level commands, historically referred to as a macrocommand.

2.2.17
parameter
the lowest level of elementary data item on-board and which, therefore, has a unique interpretation

2.2.18
parameter validity
the conditions that determine whether the interpretation of a given telemetry parameter is meaningful

EXAMPLE   The angular output of a gyro may only have a valid engineering meaning if the power to the gyro is "on", while at other times, the output may be random, or at best should not be relied upon.

NOTE   Such a parameter is deemed conditionally valid, with its validity determined from the power status.

2.2.19
protection system
an on-board function (implemented either in hardware or software) that is provided to monitor sensor or logic readings and, based on their output, either direct or processed, to:

prevent the propagation of the failure at equipment or system level; or

reconfigure the spacecraft system or subsystem into a "safe" configuration

NOTE   Subsequent analysis and recovery action will normally be performed by the ground.

2.2.20
space segment
those elements of the overall mission system that are operated in outer space

2.2.21
spacecraft
all subsystems (sometimes called the platform, the service module or the bus) plus any experiment or payload elements (sometimes called the payload module)

2.2.22
spacecraft status
all the information necessary to assess the operational status of the spacecraft at a given time

EXAMPLE   all the information needed to determine all the criteria driving operational decisions

2.2.23
subsystem
any combination of units within the spacecraft platform that fulfils a well-defined and usually self-contained set of on-board functions

2.2.24
telecommand criticality
the importance of a telecommand in terms of the nature and significance of its on-board effect

The following telecommand criticality levels are identified:

2.2.24.1
Level A
telecommands that are not expected to be used for nominal or foreseeable contingency operations, that are included for unforeseen contingency operations, and that could cause irreversible damage if executed at the wrong time or in the wrong configuration

NOTE   This level is called forbidden telecommands.

2.2.24.2
Level B
telecommands that, if executed at the wrong time or in the wrong configuration, could cause irreversible loss or damage for the mission (i. e., endanger the achievement of the primary mission objectives)

NOTE   This level is called critical telecommands.

2.2.24.3
Level C
telecommands that are not critical telecommands but are essential to the success of the mission and, if sent at the wrong time, could cause momentary loss of the mission

NOTE   This level is called vital telecommands.

2.2.24.4
Level D
all the remaining commands.

2.2.25
telecommand function
an operationally self-contained control action that may comprise or invoke one or more lower level control actions

3 Symbols and acronyms

AMF	apogee motor firing
AOCS	attitude and orbit control subsystem
CPU	central processor unit
I/O	input/output
ID	Identifier
LSW	least significant word
MSW	most significant word
EEPROM	electrically erasable programmable read-only memory
RAM	random access memory
RF	radio frequency
RFP	request for proposal
TT&C	telemetry, tracking and command

4 Autonomy levels

Tables 1 and 2 identify a number of autonomy levels for routine and contingency operations, in terms of the corresponding on-board autonomous capabilities. These autonomy levels are referenced in the requirements in later clauses of this International Standard.

Table 1 — Autonomy Levels for Routine Operations

Level R1	Real-time commanding is required for all on-board reconfigurations
Level R2	Autonomous execution of all predictable and time-dependent operations, for a limited period, on the basis of pre-programmed commands from ground
Level R3	Capability to store mission products on-board without loss
Level R4	Event-driven on-board control capabilities (e.g., power management and autonomous navigation)
Level R5	On-board operations planning and mission product optimisation to maximise mission product return

Table 2 — Autonomy Levels for Contingency Operations

Level C1	Survival mode switching in the event of failures that may be critical for survival (e.g., a power supply short circuit or loss of attitude). No automatic attempt to continue mission product generation.
Level C2	Redundancy switching for vital functions with the objective of continuing mission product generation (problem analysis and reconfiguration back to prime chain performed under ground control)
Level C3	Fully autonomous fault management

It should be noted that different autonomy levels may be implemented for routine and contingency operations (i.e., the implementation of Level n for routine operations does not necessarily imply the implementation of the same Level n for contingency operations).

The mission operations concept will dictate the choice of autonomy levels and the design of autonomous functions for a given mission. This decision and design process should consider complexity implications on the space and ground segments and should be optimised at the overall mission operations system level with respect to mission return, risk, and cost. Typical factors to be taken into account will include:

   mission product availability requirements;

   propagation delay (where applicable);

   ground station coverage;

   potential communications outages due to orbital events (e.g., solar conjunctions periods);

   ground segment availability (considering potential failures and scheduled maintenance operations).

In general, the spacecraft will not be required to maintain its autonomy indefinitely, but rather for a defined minimum interval of time, <AUT_DUR>, which may have a different value for routine and contingency operations. In determining the value of this parameter (these parameters) for a given mission, due consideration must be given to such factors as:

   the maximum period of «no ground contact» during different mission phases, for spacecraft with intermittent ground coverage;

   the maximum period of ground segment outages, either predictable (e.g., scheduled maintenance operations) or non-predictable (e.g., recovery from failures);

   the reaction time for the ground to respond to on-board anomalies (anomaly-dependent).

5   General requirements

5.1. Observability

OBSERV-0010   The space segment shall provide visibility of its internal status and configuration to the Mission Control System in sufficient detail and within time delays consistent with all routine and foreseeable contingency operations.

5.2. Commandability

CMD-0010   Sufficient control functions (telecommands) shall be provided at each level of the design hierarchy to enable the mission objectives can be achieved under all foreseeable circumstances (including the use of redundant equipment where required to meet the overall system reliability requirements).

5.3. Compatibility

COMPAT-0010   To foster compatibility with standard ground segment designs, he space segment shall conform to all established and agreed on-board design standards as listed in the space segment contract documents.

COMPAT-0013 Where existing ground systems are to be used to operate the spacecraft, the space segment shall conform to the applicable design standards as listed in the space segment contract documents.

COMPAT-0016 The space segment should utilise, as far as possible, tried and tested operational practices.

COMPAT-0020 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.

5.4. Security

SECUR-0010 The space segment shall be adequately protected against intentional or unintentional access by unauthorised parties.

5.5. Safety

SAFETY-0010 The space segment shall be tolerant to all foreseeable unintentional operator errors. In particular no single command shall lead to the loss of the space segment.

SAFETY-0020 The space segment shall be tolerant to any period of outage of ground segment equipment that is compatible with the agreed ground segment availability requirements.

SAFETY-0030 No single operational error or failure in one spacecraft element shall result in a failure that is propagated into another spacecraft element or functional area. Exceptions to this requirement shall be identified, part of contractual requirements and, where possible, operational contingency procedures shall be defined to mitigate the results of such failures.

SAFETY-0040 The design of the space segment shall be such that all foreseeable catastrophes due to an on-board failure may be averted either by autonomous on-board action or by clear, unambiguous and timely notification of the problem to the ground. In the latter case, a well-defined recovery procedure shall exist.

SAFETY-0050 It shall be ensured that any reconfiguration of the spacecraft (required for offline testing or any other purpose) shall be such that no single failure either in a control function or in any other element leads to a hazardous on-board situation.

5.6. Flexibility

FLEX-0010 The on-board systems shall be configurable in ways that optimise and enhance the controllability of the space segment.

FLEX-0020 The on-board systems shall be configurable to operate with any combination of prime and redundant equipment with the same operability characteristics.

FLEX-0030 The on-board systems shall be configurable such that permanent work-around solutions can be introduced in the event of non-recoverable failure.

FLEX-0040 Where possible, critical on-board storage/buffer should be resizable to cater to unforeseen mission events.

FLEX-0050 Any selection and operation of redundant equipment shall be reversible without loss of functionality. If specific constraints or monitoring rules exist, they shall be clearly identified.

FLEX-0060 The on-board functions shall have defined inputs and outputs accessible from the ground for workarounds in case of contingency operations.

FLEX-0060.1 Where appropriate, it shall be possible to replace on-board functions by ground functions.

FLEX-0070   The allocation of budgets for on-board resources during the design phase shall consider spare capacities of <RESOURCE_MARGIN> for each subsystem and each payload in order to ensure flexibility during the mission.

FLEX-0080   At any point in the mission, it shall be possible to determine the remaining mission lifetime with an accuracy compatible with the mission requirements.

5.7. Efficiency

EFFIC-0010   Allocation of functionality between the space and ground segment shall be performed to balance the following considerations :

a)   System operation/maintenance costs and risks can usually be reduced by performing most functions on-board.

b)   Development costs and risks for the combined space and ground segments can usually be reduced by performing most functions on the ground. (See CLOOP-0010 for exceptions.)

c)   Repetitive operations can sometimes be performed more efficiently on-board due to issues such as transmission delays, visibility times, amount of information/telemetry available, command rates, and reuse of other on-board functions.

d)   The ground segment is inherently more flexible than the space segment due to accessibility and less stringent resource limitations (mass, power, etc.).

5.8   Testability

TEST-0010   Each application process shall provide the capability to perform a set of end-to-end test functions that can be tests exercised under ground control to verify end-to-end performance. Provision of an end-to-end test function should be considered.

TEST-0020   An "are you alive" function shall be provided for testing the end-to-end connection between the ground and an application process.

TEST-0030   It shall be possible to check redundant on-board functions in an "off-line" manner (i.e., in parallel with, but without any disturbance to the prime function).

TEST-0040   Adequate observability and commandability shall be provided to assess the proper functioning at the redundant cross-strapped level.

TEST-0050   It shall be possible to check a redundant unit prior to switchover.

TEST-0060   It shall be possible to load and check redundant memory prior to switchover.

TEST-0070   It shall be possible to verify, by independent means, that all critical on-board measurements reliably reflect the values of the parameters they represent under all predictable levels of noise sources (whether radiative, capacitive, inductive, or impulsive). Critical measurements are those parameters specifically identified in the space segment contractual requirement as absolutely necessary to meet mission objectives.

6   Detailed requirements

6.1 Spacecraft observability requirements

6.1.1   Telemetry design

TMDES-1010   Standard telemetry reporting mechanisms shall be provided that allow access to all the data required to determine the status of the spacecraft and to monitor the execution of all nominal operations and foreseen contingency operations for the spacecraft platform subsystems and the payload. As a goal, this shall include:

a)   the status of all relays and switches;

b)   the power status of all units connected to the spacecraft bus;

c)   the status of all on-board equipment and software;

d)   all sensor readings;

e)   contents of all registers;

f)   indication of all on-board events of operational significance;

g)   indication of all actions taken by on-board autonomous functions;

h)   parameters used by monitoring or reconfiguration logic;

i)   status of all autonomous functions (enable/inhibit);

j)   status of all security mechanisms (triggered/not triggered);

k)   condition/status of deployable mechanisms and covers;

l)   separation status of deployed vehicle and boosters.

This data shall be telemetred to the ground in a complete, unambiguous, and timely manner.

Where these goals cannot be met, other observables shall be identified to determine the status of the listed parameters.

TMDES-1020   For a given mission, there shall be a sub-set of data that is sufficient to characterise the current state of the spacecraft and indicate if an anomalous condition has occurred that requires intervention from the ground.

TMDES-1020.1   An appropriate reserved bandwidth shall be provided for this data (even though it may not always be used).

TMDES-1030   Parameters that indicate vital spacecraft health functions shall be provided with redundant telemetry (e.g., primary bus current, voltage, propellant tank pressure, etc,).

TMDES-1040   Telemetry information shall be provided from direct measurements rather than secondary effects. In particular, the complete status of the spacecraft shall be derivable from the telemetry and other observables without the need for reference to the telecommand history or any record of on-board autonomous actions.

TMDES-1050   In some cases, parameters may change value for very short time periods. If it is necessary, for operational reasons, to detect such occurrences (e.g., as an indication of an on-board failure)

and no adequate telemetry sampling of the parameter can be provided, the event shall be stored and the stored value shall be telemetred.

TMDES-1060   For equipment in hot redundancy, telemetry shall be implemented to allow an independent and unambiguous status evaluation of each chain. For elements in redundancy, the loss or failure of one channel shall not prevent access to the telemetry of the other channel.

TMDES-1070   For parameters that are conditionally valid, their validity shall be determinable unambiguously from the telemetry.

TMDES-1080   Processors/memory auto-test results and diagnoses shall be available through telemetry.

TMDES-1090   The value of analogue parameters shall be derivable from telemetry such that the resolution and range is appropriate for monitoring purposes in all nominal and foreseen contingency situations.

TMDES-1100   Suitable sampling sequences and frequencies shall be provided for all related parameters that require direct correlation or combination for the purposes of performance evaluation.

TMDES-1110   All reconfigurations shall end with an unambiguously known and observable state of all involved units and software.

TMDES-1120   Telemetry shall be provided to isolate any identified failure at least down to function/equipment level.

6.1.2   Telemetry timing information

TIMING-1010   For different operational purposes (e.g., detailed performance evaluation, data or event correlation at the time of on-board anomalies, etc.) it shall be possible via analysis to establish the original on-board sampling time of the telemetry parameters.

TIMING-1010.1   For anomaly troubleshooting, it shall be possible to establish this information retroactively in time.

TIMING-1010.2   It shall be possible to determine the absolute (on-board) sampling time of parameters to an accuracy of <PARAM_ABS_SAMPL_TIME> (may be parameter-specific).

TIMING-1010.3   It shall be possible to determine the relative sampling time of any two parameters to an accuracy of <PARAM_REL_SAMPL_TIME>.

TIMING-1020   Timing information shall be provided in the telemetry that allows the correlation of on-board time with ground time with an accuracy of <TIME_CORREL_ACCUR>.

TIMING-1030   All timing information in the telemetry shall be synchronised with a single on-board Master Clock or synchronization signal.

6.1.3   Diagnostic mode

DIAG-1010   Under all foreseen operational conditions, sufficient telemetry bandwidth shall be available to allow the ground to select (by telecommand) a set of telemetry data to be sampled at a high rate for investigation purposes. The essential characteristics of this capability are the following:

DIAG-1010.1   Access shall be available to all on-board parameters.

DIAG-1010.2   It shall be possible to sample a given telemetry parameter at any sampling rate down to a minimum sampling interval <MIN_SAMPLE_INT>.

6.2 Spacecraft commandability requirements

6.2.1 Telecommand design

TCDES-1010   No telecommand shall contribute to permanent loss of the telecommand function.

TCDES-1020   All telecommands shall always have the same action definition during the mission.

TCDES-1030   Repetition of the same telecommand shall be possible without any detrimental effect on the spacecraft unless the command is forbidden (Level A) or critical (Level B).

TCDES-1040   For frequent or elementary operations, it is recommended that on-board functions be defined to limit the ground action to a small number of high level/goal oriented commands (this number will be function-specific).

TCDES-1050   If a device telecommand executes more than one control action, these actions must be strictly operationally related, so they constitute a single logical telecommand function

EXAMPLE   A device telecommand shall not put a battery in trickle charge and at the same time switch on a heater, unless these operations are always strictly related.

TCDES-1060   Where more than one device telecommand is required to invoke a given function, it shall be possible to «pack» such device telecommands within a single telecommand protocol unit. A telecommand protocol unit being a set of commands with minimal spacing and designed to provide efficiency in transmitting multipart telecommands.

TCDES-1070   The ground shall have the capability to command all equipment/functions of the spacecraft required to operate the spacecraft under all nominal and foreseen contingency conditions. This shall include:

a)   the configuration of all relays or on-board logic;

b)   the loading/updating of all operational parameters and registers;

c)   the loading/updating of all monitoring and reconfiguration criteria;

d)   the loading/dumping of re-programmable memory areas.

TCDES-1080   It shall be possible to command all on-board devices individually from the ground (i.e., if a device is normally commanded using a higher-level telecommand function, it shall nevertheless be possible for the ground to issue a device telecommand destined solely for that device).

TCDES-1100   The operation of reconfiguring on-board units or switching between on-board functions shall not affect the status, configuration, or continued proper operation of any other unit or function.

TCDES-1110   Where necessary to meet critical mission requirement, it shall be possible to pre-configure units in the «off» state to come on in any desired configuration

EXAMPLE   the bolometer inhibition status of an infrared attitude sensor.

TCDES-1120   There shall be no requirement for the ground to send telecommands, as the result of anomalies detected from the telemetry, with a response time of less than <ANOM_RESP_TIME>, (typically 1 minute).

TCDES-1130   The level or value of an on-board register or counter shall only be adjusted (from the ground) by the use of a register load device command (i.e., On/Off pulses shall not be used).

TCDES-1140 For in-orbit operation, the conditions under which a configuration-dependent telecommand may be sent (or may not be sent) shall be determinable unambiguously from the telemetry indicating the status of the spacecraft.

6.2.2 Critical telecommands

The definition of telecommand criticality levels is given in subclause 2.2.

CRITTC-1010 Telecommands of criticality level A or level B shall require at least two separate command actions for execution, i.e., an arm/safe or enable/disable command followed by an execute command.

EXAMPLE commands for pyrotechnic devices

CRITTC-1020 Redundant telecommands shall be provided for all telecommands of criticality levels A and B by means of a maximum diversity on-board routing (i.e., using on-board routes that share no common nodes or paths).

CRITTC-1030 A register load telecommand of criticality level A, B or C shall have a separate execute command to permit verification of the loaded data.

CRITTC-1040 For commands of criticality level A or level B, on-board protection shall be implemented to ensure that commands are only accepted if the on-board context is correct.

CRITTC-1050 Forbidden telecommands (criticality level A), shall either be omitted from the spacecraft databases or shall be clearly identified to allow proper ground system processing.

6.2.3 Control of autonomous functions

CONTR-1010 The spacecraft shall provide the capability to enable/inhibit/command any of its on-board autonomous functions.

CONTR-1020 The ground shall have the capability to override any on-board automatic functions.

CONTR-1030 For all on-board automatic functions resulting from a logical combination of several elementary monitoring criteria, inhibition and authorisation shall be possible independently and individually for each criterion.

6.2.4 Telecommand transmission and distribution

TCTRANS-1010 The on-board reception, processing, and distribution of telecommands shall ensure that no restrictions arise when the ground transmits telecommands of any type at the highest possible rate (i.e., making full use of the available uplink bandwidth), unless the ground system has specific features to allow adaptable command spacing.

TCTRANS-1020 In order to circumvent potential lock-out problems affecting telecommand routing and delivery, it shall be possible to route a limited number of selected device telecommands directly to the end-item device (i.e., without the need for any intervening software or on-board bus).

6.2.5 Telecommand verification

TCVERIF-1010 Verification telemetry shall be provided for all telecommands that have been properly executed, whether these are sent directly from the ground, are stored on-board for release at a later time, or are generated autonomously on-board.

TCVERIF-1020 Verification telemetry shall be provided with a delay of less than <TC_VERIF_DELAY> with respect to the time of completion of the telecommand execution (typically less than one minute).

TCVERIF-1030   A telecommand shall be verified by telemetry measured directly for the device or function for which the telecommand is executed (e.g., a device telecommand shall be verified by a hardware measurement that is directly telemetred without intermediate processing).

TCVERIF-1040   If a telecommand results directly in one or more changes in the spacecraft configuration, these changes shall be reflected in the telemetry indicating the spacecraft status.

TCVERIF-1050   Multidata commands (e.g., register load commands) controlling subsystem equipment configurations shall be acknowledged by telemetring all data (e.g., the corresponding register contents).

TCVERIF-1060   The ground shall be notified of any telecommand not executed, not received properly, or not executed properly.

6.3   Memory management

MMGMT-1010   Integrity of the memory area during the load/dump/check process shall be ensured by on-board application processes or by procedural inhibits/constraints. Memory integrity typically requires that no other application process shall have read/write access to this memory area during the load/check process. It is recommended that on-board processes ensure the integrity of memory since this provides a significantly more robust data load operation. Procedural inhibits/constraints should be minimised.

MMGMT-1020   It shall be possible for the ground to load/dump/check any changeable on-board memory area example : Random Access Memory (RAM), Electrically Erasable Programmable Read Only Memory (EEPROM), etc.,

MMGMT-1030   It shall be possible either to load, with a single telecommand message, a contiguous memory area (e.g., indicating the start address and the length of the load) or to perform scatter loads (e.g., specifying pairs of memory addresses and data to be loaded).

MMGMT-1040   It shall be possible either to request a memory dump, with a single telecommand sequence, from a contiguous memory area (e.g., indicating the start address and the length of the dump) or to perform scatter dumps (e.g., specifying pairs of memory addresses and length to be dumped).

MMGMT-1050   It shall be possible either to request a memory check, with a single telecommand, from a contiguous memory area (e.g., specifying the start address and the length of the area to be checked) or to perform checks on several areas (e.g., specifying pairs of memory addresses and length to be checked).

MMGMT-1060   Address data loading shall always be performed in the same order: Most Significant Word (MSW) loaded before Least Significant Word (LSW).

6.4   On-board processing functions

6.4.1   Control loops

CLOOP-1010   The design of the overall Mission Operations System (i.e., constituting both the ground and space segments) shall ensure that control loops that have short response times are implemented on-board.

CLOOP-1020   There may be ground control loops with identified response times <GRND_RESP_TIME> (there may be several such parameters for a given mission). Spacecraft status telemetry shall, therefore, comply with the following requirements for generation and transmission:

CLOOP-1020.1   Under all circumstances, the elapsed time for an application process to build and release telemetry source data shall be such that the overall delay between the generation of telemetry

source data and its reception at the Mission Control Centre is compatible with any response times that have been identified for ground control loops.

CLOOP-1020.2 Parameters within the telemetry that are generated periodically shall be sampled at a frequency that ensures no information of operational significance is lost for all nominal and foreseen contingency operations.

CLOOP-1020.3 The frequency of generation shall be compatible with the response times that have been identified for any control loops implemented on the ground.

6.4.2 On-board monitoring

OBMON-1010 It shall be possible to apply a suite of on-board monitoring functions to a set of on-board parameters. These functions shall include limit/status/delta checking and the evaluation of statistics, including minimum and maximum values over a time interval, etc.

OBMON-1020 Detected events (such as out-of-limits) or evaluation results from the on-board monitoring function shall be telemetred to ground.

OBMON-1030 It shall be possible to enable and disable the monitoring of any on-board parameter.

OBMON-1040 It shall be possible to reconfigure, in a flexible manner:

a) the selection of parameters to be monitored;

b) the monitoring criteria/required evaluation results for the selected parameters.

OBMON-1050 When on-board monitoring of a specific parameter is mode-dependent, then this shall be defined and automatically selected on-board.

6.4.3 On-board operations scheduling

OBSCH-1010[R2] It shall be possible to release any telecommand from the on-board operations schedule.

OBSCH-1020[R2] The status of the on-board operations schedule shall be periodically telemetred to the ground.

OBSCH-1030[R2] It shall be possible to start/stop the on-board operations schedule.

OBSCH-1040[R2] It shall be possible to load/add/delete any part of, or any command in, the on-board operations schedule.

OBSCH-1050[R2] The ground shall have access to the content of the on-board operations schedule through dump requests.

OBSCH-1060[R2] Time-tag dating and on-board command capacity shall cover at least the needs of the autonomy period.

OBSCH-1070[R2] The elapsed time for the on-board transfer of commands from the on-board operations schedule to the destination application process shall be predictable to an accuracy compatible with the required command execution time accuracy.

OBSCH-1080[R2] The protocol for the on-board transfer of commands to their destination application process shall ensure that any transfer error is reported to the on-board operations schedule.

OBSCH-1090[R2] The on-board operations schedule shall detect any situation that forbids the on-board transfer of a command to its destination application process.

6.4.4   On-board operations procedures

OBPROC-1010^{R2}   It shall be possible to control an on-board operations procedure from ground. Control operations shall include load, edit, start, stop, suspend, resume, etc.

OBPROC-1020^{R4}   It shall be possible to invoke an on-board operations procedure by the occurrence of a pre-defined on-board event.

OBPROC-1030^{R2}   It shall be possible to access the content of an operations procedure from ground.

6.4.5   On-board storage and retrieval

STORE-1010^{R3}   Housekeeping information shall be provided on the state of the on-board storage and retrieval function.

STORE-1020^{R3}   It shall be possible for the ground (and only the ground) to clear the contents of an on-board store.

STORE-1020.1^{R3}   It shall be possible to configure the on-board store to either overwrite old data or abort storage when it is out of memory.

STORE-1030   The capability shall be provided to store in a table a set of data representative of the health of the spacecraft. This table shall be frozen in case of failure detection or reconfiguration order.

STORE-1040   For missions with intermittent ground coverage, the on-board storage capability shall be sufficient to store all data generated on-board that may be required for spacecraft monitoring and control purposes, for a duration at least equal to the longest non-coverage period plus a mission-dependent margin <DATA_STORAGE_TIME>, typically one orbit for low-Earth orbiting spacecraft.

STORE-1050^{R3}   On-board storage shall be such that the ground can retrieve the stored data within specified delays <DATA_RETR_DELAY>. There may be several such parameters for a given mission, corresponding to data of different operational significance.

EXAMPLE   Data of high operational significance, such as anomaly telemetry, is normally needed on the ground with shorter delays than routine status telemetry.

6.4.6   Mission management

MIMGT-1010^{R2}   The design of the on-board mission management function and the associated autonomy duration <AUT_DUR> shall take into account mission-specific factors such as:

a) mission product availability requirements,

b) space segment and ground segment complexity,

c) ground station coverage,

d) communications outages due to orbital events,

EXAMPLE   solar conjunctions periods

e) ground segment non-availability

MIMGT-1020^{R2}   The mission management function shall be capable of performing all necessary actions to maintain mission operations during the autonomy duration <AUT_DUR> without any actions from the ground, except in case of failures.

MIMGT-1030^{R2} The mission management function shall be hierarchically structured and accommodated as a distributed system in the various processors available on-board. The guiding principle for the distribution of functions is that control shall be exercised at the lowest possible level.

MIMGT-1040^{R2} The management of subsystem and payload internal commanding, including all necessary relative time control, shall reside in the corresponding subsystem and payload application processes. This may be in the form of:

   software control processes, using look-up tables if necessary;

   on-board operations procedures.

MIMGT-1050^{R2} For the attitude and orbit acquisition phase, it shall be possible to initiate or reconfigure the sequence of operations used in this phase:

a)   in an autonomous way, with a possibility of handover from the ground,

b)   directly and manually from the ground, if necessary.

MIMGT-1050.1^{R2} An automatic sequence shall be initiated on-board upon detection of launcher separation to obtain a safe configuration without ground intervention.

MIMGT-1050.2^{R2} It shall be possible to tune on-board delays to follow critical operations from selected ground stations

EXAMPLE   some pyrotechnic sequences, appendage deployments, first manoeuvres

6.4.7 On-board fault management

The primary purpose of on-board monitoring is to reduce the necessity for continuously transmitting all the low-level housekeeping data to the ground or for the ground to be continuously available to monitor this data

FAULT-1010 The design of the on-board fault management function and the associated autonomy duration <AUT_DUR> shall take into account mission-specific factors such as:

a)   mission product availability requirements,

b)   space segment and ground segment complexity,

c)   fault tolerance,

d)   ground station coverage,

e)   communications outages due to orbital events

EXAMPLE   solar conjunctions periods,

f)   ground segment non-availability.

FAULT-1020 The on-board fault management function shall be capable of performing all necessary actions to react to on-board faults during the autonomy duration <AUT_DUR> without any actions from the ground.

FAULT-1030^{C3} The management of anomalies and failures within a subsystem or payload shall be accommodated within their own application processes. This implies that within each of these application processes, functions must be provided to detect all internal failures that either endanger the subsystem or payload in question or would lead to severe degradation of mission products. These functions shall also be able to execute internal failure correction actions.

FAULT-1040 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, although a separate telemetry indication should be generated if the exception condition disappears.

FAULT-1050 The fault detection functions shall run independently from the functions being monitored and should wherever possible be based on independent inputs.

FAULT-1060[C3] It shall be possible to detect faults in systems that are off line (i.e., not involved in any primary function) as well as on line.

FAULT-1070[C1] The baseline philosophy for failure isolation at subsystem or payload level shall be to attempt to immediately disable the function affected (i.e., to ensure survival).

FAULT-1080[C2] The baseline philosophy for failure correction shall be to immediately restore the failed function by appropriate internal redundancy switching (i.e., to provide continuity of product generation). A short "hiccup" may be expected with this approach but not an outage.

FAULT-1090[C3] Following failure isolation and (where relevant) correction, the subsystem or payload application process shall issue an event message to the mission manager, which shall then initiate any further system level actions, as necessary. The event message shall clearly identify the event, its time of occurrence, the parameters in anomaly, their values, any recovery action taken autonomously, and any other information that would be required for later analysis and understanding of the anomaly on the ground.

FAULT-1100[C3] The mission manager shall be able to detect system-level anomalies that cannot be recognised by subsystems or payloads.

FAULT-1110[C3] The mission manager shall handle the management of both system-level anomalies and system-level reactions to subsystem or payload internal anomalies. This implies that the mission manager shall be able to determine whether an internal failure within a subsystem or payload necessitates reconfiguration of other subsystems. If so, it shall determine which reconfiguration steps or procedures shall be applied and issue the corresponding commands to the subsystems or payloads.

FAULT-1120[C3] The baseline philosophy for fault management at system level shall be to ensure survival and to re-optimise product generation. Should such system level reconfigurations raise conflicts with the operations plan in the on-board operations schedule, then the execution of the on-board operations schedule shall be inhibited and the entire spacecraft shall be switched to a well-defined survival mode.

FAULT-1130[C3] The mission manager shall be able to perform regular "are you alive" checks of subsystem and payload application processes.

FAULT-1140[C3] The mission manager shall have a "watch-dog" process for its own health check. Detection of an anomaly shall result in immediate changeover to a redundant processor.

FAULT-1150 Each protection system shall be intrinsically failsafe.

FAULT-1160 It shall be possible to enable and to disable any on-board protection system (or safety mode logic) by telecommand.

FAULT-1170 Where applicable, parameters of protection system detection criteria (e.g., thresholds, number of failure repetition, etc.) shall be modifiable by telecommand.

FAULT-1180 Where the protection system mode has several inputs that are logically "OR-ed" to detect failure (e.g., sensor readings, unit status, etc.), it shall be possible to enable and disable each independent input by telecommand.

FAULT-1190   Where a protection system selects redundant units for automatic reconfiguration, it shall be possible to specify by telecommand which units are to be monitored (for failure) and which combination of units is to be selected for the reconfiguration (from the allowable combinations).

FAULT-1200[C1]   The spacecraft shall enter survival mode if any hazard exists that affects life, payload capability, or mission objectives.

FAULT-1210[C1]   The spacecraft shall not enter survival mode if no such operational hazard exists. In particular, the system-level protection logic shall allow for the possibility of non-hazardous operational errors without causing entry into survival mode, but instead shall generate appropriate warning-level telemetry.

FAULT-1220[C1]   Survival mode shall ensure the safety of the spacecraft, and a minimum survival duration shall be defined for each mission <MIN_SURV_DUR>.

FAULT-1230[C1]   Recovery from survival mode shall always be undertaken under ground control.

6.5   Equipment/subsystem-specific requirements

6.5.1   On-board processors and software

PRSO-1010   The design (selection) of on-board processors shall ensure that the available memory and performance accommodates, with an adequate margin of <RESOURCE_MARGIN>:

a)   the requirements of the reference process (i. e., at launch);

b)   a realistic allocation of the process that may be developed and loaded after launch.

PRSO-1020   If an on-board processor is switched from a prime to a redundant unit (or vice versa), the switchover shall be seamless. This implies that it shall either not be necessary to re-load the operational context from ground (autonomy level R5/C3) or it shall be possible to load the new processor before the switchover.

PRSO-1020.1 [R5/C3]The switchover shall not invalidate on-board commands or operation schedules that are already defined for future operations (this implies that the commands defined for the prime unit shall also be valid when loaded in the redundant unit).

PRSO-1020.2   The switchover shall not invalidate any commands in a ground schedule that are already defined for future operations (this implies that the commands defined for the prime unit shall also be valid for the redundant unit, except for the command routing bits which the ground system can automatically change when addressing the redundant processor).

PRSO-1030   A redundant processor shall provide the capability to be turned on and operated out of the control loop, for the purpose of evaluating its performance prior to switching to it as the prime controller.

PRSO-1040   All on-board software shall be structured in a modular manner to facilitate testing to ensure reliable operation and to simplify the isolation of, and recovery from, software faults.

PRSO-1050   On-board software shall allow extensive and flexible reprogramming capabilities through the use of adequate commanding tools and memory margins.

PRSO-1060   It shall be possible to check on-board software modifications before enabling them.

PRSO-1070   The resources utilised by on-board software shall be telemetred (e.g., memory usage, Central Processor Unit (CPU) usage, Input/Output (I/O) usage).

PRSO-1080   It shall be possible to exercise control over an application process.

PRSO-1090   Whenever a condition that forces a processor reset is detected by software, this shall be reported in the telemetry prior to enforcement of the reset.

PRSO-1100   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 were duly completed. Should this not be the case, a processor overload condition shall be reported in the telemetry.

PRSO-1110   Whenever an unexpected arithmetic overflow condition is detected, this shall be reported in the telemetry.

PRSO-1120   Whenever an illegal program instruction is encountered during execution of a program code, this shall be reported in the telemetry.

PRSO-1130   Should a data bus error be detected by software, this shall be reported in the telemetry.

PRSO-1140   Whenever a memory corruption is detected by an error detection and correction mechanism, this shall be reported in the telemetry.

PRSO-1150   Whenever a checksum error is detected, this shall be reported in the telemetry.

PRSO-1160   Whenever feasible, a processor shall perform internal consistency checks by comparing its actual status and configuration against a set of allowable status and configuration tables. Whenever an internal inconsistency is detected by this mechanism, this shall be reported in the telemetry.

6.5.2   Power supply and consumption

POWER-1010   The power for telemetry conditioning of equipment shall be hierarchically structured and, in particular, shall not be supplied from other unrelated units that are not permanently powered.

POWER-1020   There shall be sufficient telemetry parameters assigned that the power available and power demand can be directly established from the telemetry alone. (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.)

POWER-1030   Adequate means and telemetry shall be provided for the ground to determine the state of charge of each battery throughout all mission phases, to an accuracy of better than 10 percent.

POWER-1040   Monitoring of power-dissipating equipment (e.g., converters) shall be performed through the parameters listed by priority order: primary current, temperature and secondary voltage.

POWER-1050   For all units that have a primary consumption greater than <POW_CONS_THRESH>, to be defined on a mission basis, a thermistor on a hot point or a primary current sensor shall be provided and made available through telemetry.

6.5.3   Telemetry, tracking and command (TT&C)

TT&C-1010   Independent access must be maintained using either payload or platform radio frequency (RF) receiver links, to obviate the need to rely on the ground to reinstate the mission support. This implies that the appropriate receivers shall be continuously active.

TT&C-1020   Redundant receivers shall be provided, which shall be cross-strapped to redundant decoders.

TT&C-1030   For Earth-orbiting spacecraft, the characteristics of the combined TT&C coverage shall be such that telemetry and telecommand contact can be provided under all foreseeable attitude and orbit conditions.

TT&C-1040   Where switching between antennas is required, it shall be ensured that there is sufficient overlap between antenna patterns so there is at least 1 minute to effect antenna-switching under all foreseeable orbit and attitude conditions.

6.5.4 Attitude and orbit control

AOCS-1010   Telemetry generated by sensor elements shall be assigned to dedicated telemetry channels in order to allow the monitoring of all sensors (whether used or not) for diagnostic purposes.

AOCS-1020   Angular detectors shall be designed so their output is unambiguous. In particular, if analogue components (such as bolometers) are incorporated, non-volatile memory provisions shall be included, at least at the level of an order of magnitude step.

AOCS-1030   Stimulated elements shall be protected from foreseeable sources of spurious signals using level, event duration, or phase discrimination as appropriate. Marginal conditions shall be suitably protected to avoid the generation of false data, especially if the data are used to authorise, veto, or condition an on-board process.

AOCS-1040   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.

AOCS-1050   Adequate telemetry monitoring of thruster actuation shall be provided to enable thruster on-time surveillance and fuel consumption determination.

AOCS-1060   Means shall be provided for determining from telemetry the remaining fuel in each independent propellant system.

AOCS-1070   The achievable accuracy for determination of the amount of remaining fuel at any given point in the mission, while being dependent on the particular mission planning requirements, shall be appropriately related to the amount of fuel remaining. (For example, an accuracy of 5 percent is normally acceptable at the start of the mission; however, when there is only 10 percent of the fuel remaining, this must be determinable to an accuracy of, typically, 10 percent to 20 percent.)

6.5.5 Mechanisms

MECH-1010   Drivable mechanisms shall be provided with both hard and soft end-stops, which shall be independently telemetred.

MECH-1020   Mechanisms (except the "single shot" type) shall be designed so they cannot be driven into a non-recoverable condition.

6.5.6 Thermal control

THERM-1010   The performance of the thermal control subsystem shall be validated prior to launch so there is an accurate prediction of the in-flight performance.

THERM-1020   The target accuracy for thermal predictions shall be typically plus or minus 3 °C for all those elements with quasi-ambient temperatures.

NOTE   This excludes, thruster assemblies and parts of the spacecraft significantly affected by Apogee Motor Firing (AMF) soakback.

THERM-1030   Means shall be provided for determining from telemetry the remaining cooling fluid (where applicable).

THERM-1040   The achievable accuracy for determination of remaining cooling fluid at any given point in the mission, while being dependent on the particular mission planning requirements, shall be appropriately related to the amount of cooling fluid remaining. (For example, an accuracy of 5 percent is normally acceptable at the start of the mission, however when there is only 10 percent of the cooling fluid remaining, this must be determinable to an accuracy of, typically, 10 percent to 20 percent.)

Annex A
(informative)

Mission constants

The mission constants identified within the body of this International Standard are summarised in this Annex, for informative purposes.

<ANOM_RESP_TIME>

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

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

<AUT_DUR>

the period of time for which the spacecraft can operate autonomously.

A different autonomy duration may apply for routine and contingency operations.

<DATA_RETR_DELAY>

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

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

<DATA_STORAGE_TIME>

the time for which telemetry data shall be stored on-board for later dumping to ground, over and above the longest time interval without ground coverage

This is applicable for missions with discontinuous ground coverage.

<GRND_RESP_TIME>

the response time for control loops involving the ground

There may be several such parameters for a given mission.

<MIN_SAMPLE_INT>

the minimum time interval down to which it is possible to sample an on-board parameter for telemetring to ground for investigation purposes

<MIN_SURV_DUR>

the minimum time duration for which the survival of the spacecraft shall be ensured (without ground intervention), having entered survival mode following the occurrence of an on-board failure

<PARAM_ABS_SAMPL_TIME>

the accuracy with which it shall be possible to determine the absolute (on-board) sampling time of a telemetry parameter

<PARAM_REL_SAMPL_TIME>

the accuracy with which it shall be possible to determine the relative sampling time of any two telemetry parameters

<POW_CONS_THRESH>

the threshold of electrical power consumption beyond which specific requirements are imposed for the provision of telemetry data.

<RESOURCE_MARGIN>

the margin of resources for on-board subsystems and payloads that is available during the mission

EXAMPLE   power, on-board memory, CPU load, bus traffic, registers

<TC_VERIF_DELAY>

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

<TIME_CORREL_ACCUR>

the accuracy with which on-board time shall be correlated with ground time