INTERNATIONAL STANDARD

ISO 14950

First edition
2004-02-15

Space systems — Unmanned spacecraft operability

Systèmes spatiaux — Opérabilité des satellites non habités

Reference number
ISO 14950:2004(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

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 2.

The main task of technical committees is to prepare International Standards. 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.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

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

0 Introduction

0.1 Spacecraft operation

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

a) ensure availability of mission and science products/services or data;

b) carry out routine housekeeping operations;

c) recover from on-board contingencies;

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

0.2 Spacecraft operability

The *operability* is a feature of the spacecraft itself that enables a specified ground segment comprising hardware, software, personnel, and procedures, to operate the space segment during the complete mission lifetime of the spacecraft, by using a minimum of resources, while maximizing 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:

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

b) the capability to manage on-board resources and to maximize the mission lifetime;

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

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

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

f) the simplicity of the space and ground segment required to fulfil the mission requirements and respect the mission constraints;

g) the autonomous capability of the space systems;

h) the complexity and interdependence 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 minimize 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 optimized 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 International Standard. Thus, this International Standard is not project or machine specific.

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

0.3 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 superscript 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.

0.4 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:

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

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

c) the spacecraft is designed, based on a) and b) above.

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

During step c), 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 a specified ground segment to operate the spacecraft in any nominal or predefined contingency situation.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 14620-1:2002, *Space systems — Safety requirements — System safety*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1 General terms

3.1.1
commandability
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

3.1.2
compatibility
extent to which the design of the space segment conforms with the existing ground segment infrastructure (if any) and with existing operational practices

3.1.3
efficiency
optimum distribution of tasks between the ground and space segments taking into account cost, complexity, technology and reliability

3.1.4
flexibility
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 optimize mission products according to the mission events

3.1.5
observability
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.

3.1.6
operation
⟨spacecraft⟩ activity performed from a mission control centre

NOTE See the Introduction, 0.1, for further details defining spacecraft operation.

3.1.7
operability
⟨spacecraft⟩ feature of the spacecraft itself that enables a specified ground segment to operate the space segment during the complete mission lifetime of the spacecraft

NOTE See the Introduction, 0.2, for further details defining spacecraft operability.

3.1.8
safety
extent of on-board protection against failure and the provision of fail-safe modes of operation

3.1.9
security
extent of on-board protection against unauthorized access to on-board telecommand functions, jamming of the telecommand channel, or corruption of the telecommand data, unauthorized access to telemetry data, or the corruption of these data

3.1.10
testability
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).

3.2 Other terms

3.2.1
application process
on-board element capable of generating telemetry source data and receiving telecommand data

NOTE An application process can 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 can be a centralized 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 can host one or several application processes. However, it is also possible that a given application process could be distributed across two or more processors.

3.2.2
autonomy
extent to which a spacecraft can handle nominal and/or contingency operations without ground intervention

3.2.3
chain
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.

3.2.4
control loop
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.

3.2.5
device telecommand
telecommand that is routed to and executed by on-board hardware

EXAMPLE A relay switching telecommand or a telecommand to load an on-board register.

3.2.6
ground segment
all ground facilities and personnel involved in the preparation and/or execution of mission operations

3.2.7
high level telemetry
telemetry processed from the low level telemetry by an on-board application process

3.2.8
low level telemetry
elementary readable on-board information

EXAMPLE Register readout or relay status.

3.2.9
memory
any on-board memory area, whether main memory or storage memory, such as disk, tape, or bubble-memory

3.2.10
mission management
on-board functionality that allows a mission to undertake routine operations highly autonomously with the minimum of ground intervention

3.2.11
mission manager
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.

3.2.12
no ground contact
period of time during a mission when ground contact is not possible due to the unavailability of the telecommand/telemetry links

NOTE The reasons for this unavailability can 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.

3.2.13
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.

3.2.14
on-board monitoring
set of processing functions that is applied to a set of on-board parameters

NOTE 1 These functions can 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 can be even wider, e.g. to include the triggering of on-board actions in response to detected events.

3.2.15
on-board operations scheduling
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.

3.2.16
on-board operations procedure
simple operations procedure that can be controlled from the 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 can consist of a sequence of low-level commands, historically referred to as a macrocommand.

3.2.17
parameter
elementary data item on-board

NOTE A parameter has a unique interpretation.

3.2.18
parameter validity
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.

3.2.19
protection system
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.

3.2.20
space segment
those elements of the overall mission system that are operated in outer space

3.2.21
spacecraft
all subsystems (sometimes called the platform, the service module or the bus) plus any experiment or payload elements (sometimes called the payload module)

3.2.22
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.

3.2.23
subsystem
any combination of units within the spacecraft platform that fulfils a well-defined and usually self-contained set of on-board functions

3.2.24
survival mode
non-operational, temporary and safe-life mode of a spacecraft, defined to avoid its loss in case of contingency (catastrophic or critical failure, aggressive environment, etc.)

3.2.25
telecommand criticality
importance of a telecommand in terms of the nature and significance of its on-board effect

NOTE Telecommand criticality levels are categorized as Levels A to D as defined in 3.2.25.1 to 3.2.25.4.

3.2.25.1
Level A
forbidden telecommand
telecommand that is not expected to be used for nominal or foreseeable contingency operations, that is included for unforeseen contingency operations, and that could cause irreversible damage if executed at the wrong time or in the wrong configuration

3.2.25.2
Level B
critical telecommand
telecommand 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)

3.2.25.3
Level C
vital telecommand
telecommand that is not a critical telecommand but is essential to the success of the mission and, if sent at the wrong time, could cause momentary loss of the mission

3.2.25.4
Level D
all the remaining commands

3.2.26
telecommand function
operationally self-contained control action that can comprise or invoke one or more lower level control actions

4 Abbreviated terms

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