ECSS-Q-30-09A
7 December 2005

Space product assurance

Availability analysis

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

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

ISSN: 1028-396X

Price: € 10

Printed in: 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.

The formulation of this Standard takes into account the existing ISO 9000 family of documents.

This Standard has been prepared by the ECSS-Q-30-09 Working Group, reviewed by the ECSS Product Assurance Panel and approved by the ECSS Steering Board.

(This page is intentionally left blank)

Contents

Figures

Tables

1

Scope

This Standard is part of a series of ECSS Standards belonging to ECSS-Q-30, Space product assurance – Dependability. The present standard defines the requirements on availability activities and provides where necessary guidelines to support, plan and implement the activities.

It defines the requirement typology that is followed, with regard to the availability of space systems or subsystems in order to meet the mission performance and needs according to the dependability and safety principles and objectives.

This Standard also describes the process that is followed and the most significant methodologies for the availability analysis to cover such aspects as

- evaluation of the space element or system availability figure,
- allocation of the requirement at lower level, and
- outputs to be provided.

This Standard applies to all elements of a space project (flight and ground segments), where Availability analyses are part of the dependability programme, providing inputs for the system concept definition and design development.

The on-ground activities and the operational phases are considered, for availability purposes, in order to

- acquire additional information essential for a better system model finalization and evaluation, and
- monitor the system behaviour to optimize its operational performance and improve the availability model for future applications.

When viewed in a specific project context, the requirements defined in this Standard should be tailored to match the genuine requirements of the particular profile and circumstances of a project.

NOTE Tailoring is a process by which individual requirements or specifications, standards and related documents are evaluated and made applicable to a specific project. This process can result in deletion, addition or modification of requirements.

(This page is intentionally left blank)

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-P-001B ECSS — Glossary of terms

(This page is intentionally left blank)

3

Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ECSS-P-001 and the following apply.

3.1.1
active redundancy
every entity is operating and the system can continue to operate without downtime or defects despite the loss of one or more entities

3.1.2
achieved availability
probability that a system, subsystem or equipment, when used under stated conditions in an ideal support environment operates satisfactorily at a given time

NOTE The downtime is associated only to the active preventive and corrective maintenance.

3.1.3
corrective maintenance
maintenance performed to restore system hardware integrity following anomalies or equipment problems encountered during system operations

3.1.4
flight segment
product or a set of products intended to be operated in space

3.1.5
ground segment
all ground infrastructure elements that are used to support the preparation activities leading up to mission operations, the conduct of mission operations and all post-operational activities

3.1.6
hot redundancy
redundancy entity is “ON”, but not necessarily in the right configuration to accomplish the function

3.1.7
instantaneous availability
<intrinsic or inherent>
probability that an item is in a state to perform a required function under given conditions at a given instant in time, assuming that the required external resources are provided

NOTE Preventive maintenance is generally not taken into account for intrinsic availability.

3.1.8
instantaneous availability
<operational>
probability that an item is in a state to perform a required function under given conditions at a given instant of time, taking into account the maintenance strategy (spares policy and related in logistic delays and constraints)

3.1.9
lead time (supplier delay)
mean time for supplier to provide spares (including shipping time)

3.1.10
logistic delay
mean time for human and material maintenance means to be available (call-out time)

3.1.11
mean availability
<intrinsic or inherent>
percentage of time that a system, subsystem or equipment, used under stated conditions, without any scheduled or preventive action and with ideal logistical support, operates satisfactorily for a defined time period

3.1.12
mean availability
<operational>
percentage of defined time period in which a system, subsystem or equipment, operates satisfactorily used under stated conditions in an actual support environment

NOTE The down time is relevant to the corrective maintenance, preventive maintenance, logistic and administrative delays.

3.1.13
mean down time
mean time between service interruption and service resumption

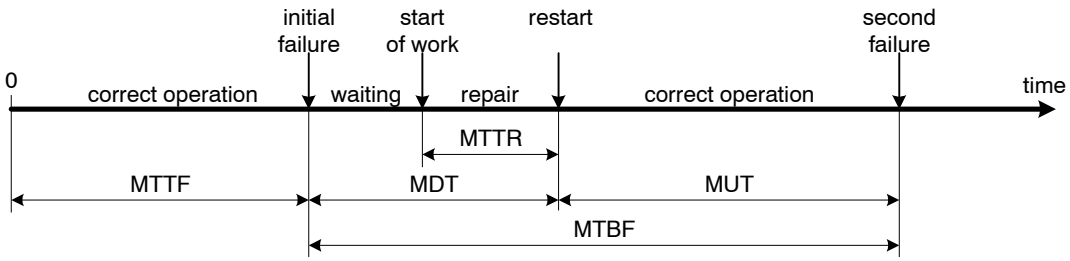

Figure 1: Relations between the various values that characterize the reliability, maintainability and availability of equipment

3.1.14
mean time between failures
mean time between two consecutive failures

3.1.15
mean time between outages
mean time of operation of an entity between two consecutive non-operational phases caused by corrective or preventive maintenance activities

3.1.16
mean time to failure
mean time of working of an entity before its first failure

NOTE Also known as "mean time to first failure" (MTTFF).

3.1.17
mean time to outage
mean time of working of an entity before its first outage

3.1.18
mean time to repair
mean duration to repair equipment with human and material maintenance means being available

3.1.19
mean up time
mean time of working of an entity after corrective maintenance (covering repair and replacement)

3.1.20
outage
state of an item of being unable to perform its required function

[IEC Multilingual Dictionary:2001 edition]

NOTE 1 Causes of outages can be failures, upsets or planned and unplanned events.

NOTE 2 The failures can be due to cataleptic intrinsic events or external events.

3.1.21
passive redundancy
redundancy not activated before necessary

NOTE Also knows as "standby redundancy" or "cold redundancy".

3.1.22
preventive maintenance
scheduled or on-condition maintenance actions performed on equipment to reduce its probability of failure or degradation

NOTE Preventive maintenance is performed to keep the system at designed reliability and safety levels before failure occurrence.

3.1.23
steady-state availability (asymptotic availability)
limit, if any, on the instantaneous availability as time approaches infinite

3.2 Abbreviated terms

The following abbreviated terms are defined and used within this document:

Abbreviations	Meaning
FMECA	failure modes, effects and criticality analysis
GPS	global positioning system
LD	logistic delay
MDT	mean down time
MTBF	mean time between failures
MTBO	mean time between outages
MTTF	mean time to failure
MTTFF	mean time to first failure
MTTO	mean time to outage
MTTR	mean time to repair
MUT	mean up time
NRB	nonconformance review board
PDF	probability density function
RAM	reliability availability and maintainability
SOW	statement of work
TWT	travelling wave tube
w.r.t.	with respect to

4

Objectives of availability analysis

The availability analysis is developed in order to

- verify the conformance of the selected system design with the applicable availability requirements, and
- provide inputs to estimate the life cycle cost of the system.

The above design activity leads to the optimization of the system concept definition with respect to design baseline, operations and logistics provisions.

The availability analysis identifies the unavailability contributors in order to quantify their impact in supporting

- the decision making process, and
- risk evaluation, reduction and control (see ECSS-M-00-03).

The availability activity is fully integrated into the development programme to ensure the correct support to the other disciplines (e.g. engineering, operations and logistics).

(This page is intentionally left blank)

5

Specifying availability and the use of metrics

5.1 General

5.1.1 Introduction

The mission success criteria, from a probabilistic point of view, can be established in different ways. As a consequence, the selection of the most adequate dependability requirement depends on all of the operational constraints and mission objectives.

5.1.2 Availability requirements

a. Availability requirements shall respect the mandatory characteristics defined by the system engineering process (e.g. traceable, identified, unique, or unambiguous).

b. For each availability requirement, a verification method shall exist.

c. Each availability requirement shall be a quantitative requirement.

d. The process leading to the definition of the availability requirement shall be user oriented (availability of mission service) and not design focused

e. The process leading to the definition of the availability requirement shall include the following aspects necessary to characterize the project under development:

   1. functional and performances objectives (e.g. What is the “threshold” between nominal behaviour and failure mode? What are the contributors to mission success under system visibility and responsibility?).
   2. “environmental” conditions (e.g. for which environment, interfaces, provisions,… shall the above objectives be met?).
   3. operational time frame (e.g. for which period, at what date).
   4. unavailability contributors (e.g. detection, logistics, and administrative delays), to be taken into account in the analysis on the basis of the contractor’s visibility and responsibility for the logistic scenario or support.

f. Availability requirements shall be specified according to one or several of the following classes of availability specifications detailed in 5.2.

5.2 Different ways of specifying availability

5.2.1 Probability figure convention

For each type of availability requirement, specified figures shall be defined as "mean" or "best estimate" probability figures (point estimation). Unit failure rates are generally computed in this way (or sometimes at 60 % confidence level).

5.2.2 Availability during mission lifetime for a specified service

5.2.2.1 General

a. Availability during mission lifetime for a specified service is currently used for missions where a "steady-state" nominal service is planned, and for which a percentage of the mission time can be specified as an availability performance measure.

b. The availability during mission lifetime applies to maintainable, on-ground or in-orbit (e.g. Space Station), and non-maintainable systems (e.g. satellites).

c. Generic potential contributors for outage periods can be, for instance, maintenance activities (preventive as far nominal service is impacted, corrective), periodic manoeuvres, reconfiguration delays for redundant payload, recoveries from safe mode, upsets, eclipses.

d. In some applications, the mission lifetime can be subdivided into several periods for which the availability requirement shall be met.

EXAMPLE "The system shall be operational during 11 months per year during the mission lifetime".

5.2.2.2 Requirements

a. If the operative scenario duration is longer than the system or equipment mean down time (more than 5 MDT), the instantaneous or mean availability can reach an asymptotic (or steady state) behaviour. Then the requirement shall be formulated in terms of steady-state availability, assuring a simplifying (and generally conservative) approach.

b. The availability during mission lifetime shall be computed as the ratio of time during which service is fulfilled over the total mission lifetime.

c. For non-maintainable systems, the availability during mission lifetime requirements shall be established considering that the mission is still operational at end of life (for example, no single point failure is considered as an unavailability contributor).

d. The availability during mission lifetime can take into account radiation's effects: such as upset for logic parts, SET for opto and linear parts, and latch up.

e. Functional effects on equipment or subsystems due to radiation single events shall be evaluated to give quantified inputs to availability analyses.

NOTE ECSS-Q-60 branch standard gives methodology to evaluate behaviour of electronic parts within their functional conditions.

5.2.3 Availability at a specific time (or time interval) for a specified service

5.2.3.1 General

Availability at a specific time applies mainly for systems where specific critical operations are scheduled in the mission timeline. Typical applications are a launcher control bench availability at a specific time or a scientific satellite with a planned comet rendezvous mission.

5.2.3.2 Requirements

a. The availability at a specific time requirement shall address the probability that this "quasi-instantaneous" operation is successfully handled.

b. For non-maintainable systems, the availability at a specific time requirement shall specify by a single requirement both the availability and reliability characteristic.

c. Availability at a specific time shall be computed considering the mission loss probability.

5.2.4 Percentage or number of successfully delivered products

5.2.4.1 General

For some applications, the user-oriented approach can characterize the system in a "black-box" manner and specifying availability according to the number off, for instance, delivered products, services, or mission data with respect to user demands or nominal scenario.

5.2.4.2 Requirements

If the availability is specified by a percentage or number of successfully delivered products, the availability requirement shall be expressed as:

a. ratio of successfully delivered products (for instance w.r.t. the applicable criteria for performance, delay, and coverage) over number of requested products;

b. cumulated service hours during the mission;

EXAMPLE Expected number of TWTs × hours operation from a 12 out of 16 redundant channels configuration over 10 years.

c. acquired database volume or percentage.

EXAMPLE Geographical coverage for an Earth observation mission.

5.2.5 Outage probability distribution

a. In particular cases, it can be relevant to specify the availability with an outage distribution and duration. If a maximum duration is specified, a probability of exceeding this duration shall be associated.

NOTE This can apply at subsystem level when a short service interruption is masked or filtered by the upper level function.

EXAMPLE Typically a GPS receiver temporary outage is tolerated by a navigation model. For this type of application, numerous short outages would be preferable to a few long ones.

b. If several classes of outage are identified, an availability specified through an outage probability distribution shall be allocated for each class (associated duration and probabilities).

5.3 Metrics commonly used

a. The availability requirements shall be quantified using one or several of the following metrics:

1. inherent instantaneous availability;
2. operational instantaneous availability;
3. inherent mean availability;
4. operational mean availability;
5. inherent steady-state availability;
6. operational steady-state;
7. outage duration and occurrence;
8. MUT and MDT (or mean time to restore);
9. MTBF or MTBO, and MTTR;
10. MTTF or MTTO;
11. amount of successfully delivered products.

5.4 Metrics mapping

5.4.1 General

Following the definition of the system level availability requirements according to subclause 5.2, the availability metrics and supporting metrics shall be selected according to Table 1.

Table 1: Availability and supporting metrics applicable at system and subsystem level

		Metric										
		Inherent instantaneous availability	Operational instantaneous availability	Inherent mean availability	Operational mean availability	Inherent steady-state availability	Operational steady-state	Outage duration and occurrence	MUT and MDT (or mean time to restore)	MTBF/MTBO and MTTR	MTTF/MTTO	Amount of successfully delivered product
System/ Subsystem level	Availability during mission lifetime			●	●	●	●					
	Availability at a specific time interval	●	●	●	●							
	Outage probability distribution							●	●			
	Percentage of successfully delivered products											●
Equipment level	Availability during mission lifetime									●	●	
	Availability at a specific time interval									●	●	
	Outage probability distribution							●				
	Percentage of successfully delivered products	Not applicable at equipment level										

5.4.2 Metrics mapping at system or subsystem level

a. The metrics selection performed at system level depends on all of the mission characteristics. In particular, the choice between an instantaneous availability, mean availability or steady state availability shall be based on the mission time schedule.

b. The choice between Inherent and Operational availability shall be based on the possibility to access information from the logistic support analysis necessary to assess the Operational availability.

NOTE If logistic and administrative delays necessary to assess the Operational availability cannot be obtained, the Achieved availability may be used as the metric to take preventive maintenance into account in the assessment.

c. The choice between MUT with MDT and outage distribution shall be based on the number or duration of mission specific events, or only on the mean values for up time and down time.

5.4.3 Metrics mapping at equipment level

The choice between MTBF with MTTR and outage distribution shall be based on the number or duration of mission specific events, or only on the mean values for up time and down time.

NOTE For availability considerations, the equipment level refers to the lowest level of replaceable unit (LRU level).

6

Availability assessment process

6.1 Overview of the assessment process

The availability assessment process is represented as shown in Figure 2 . The process steps identified in the different sections of the figure are addressed in detail in clauses 6.2 through 6.5 and in Annex A for the assessment availability methods.

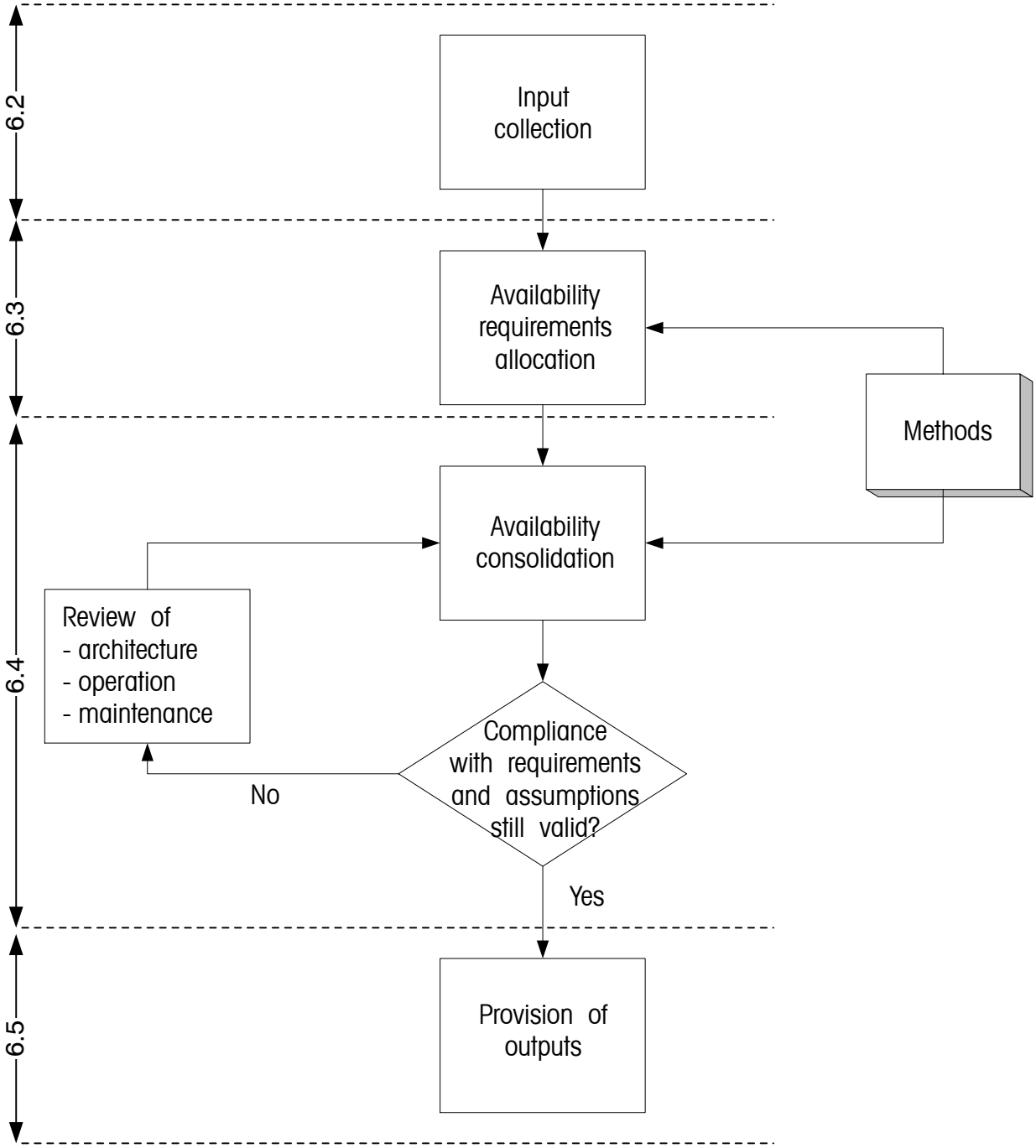

Figure 2: Availability assessment process

6.2 Mandatory inputs for availability assessment

6.2.1 General

The mandatory availability inputs come from various origins:

- Functional analysis
- Design reports (e.g. analysis, configuration, and ICD)
- FMECA (see ECSS-Q-30-02)
- Logistics analysis
- Operations analysis
- Contingency analysis

6.2.2 Requirements

a. The input collection shall include at least the following:
   1. A preliminary functional architecture (e.g. mission lifetime) followed by the preliminary physical layout as soon as it is available.
   2. Items or equipment failure and repair rates
   3. Operative scenario
   4. Maintenance policy including
      (a) spares strategy at each maintenance level,
      (b) logistic delays,
      (c) supplier delays, and
      (d) preventive maintenance strategy (e.g. schedule, and duration).

b. Items or equipment failure and repair rates shall be provided identifying adequately the item or equipment typology (i.e. time sensitive, cycle sensitive and one shot). For the time sensitive items or equipment, the failure rate in active and stand-by (or passive or dormant) mode shall be evaluated. When the constant failure rate model is not applicable, the applicable PDF for the time to failure shall be defined.

c. For each item or equipment, the expected operative status in each mission phase shall be considered, and the monitoring strategy shall be taken into account.

d. For each piece of data or information, a reference to the relevant source shall be provided.

6.3 Availability allocation

a. The availability allocation shall be based on the
   1. subsystem failure's effect on the mission derived from the system analysis,
   2. previous experience from similar programmes,
   3. subsystem complexity or cost,
   4. subsystem technology maturity, and
   5. already designed and developed subsystem.

   NOTE The criteria order of priority is application dependent.

b. The availability requirement allocation process shall be addressed early in the design phases (according to clause 7) to evaluate realistically the criticality of each system section and therefore the most appropriate baseline.

6.4 Iterative availability assessment

a. A preliminary availability evaluation based on previous experience or judgement expertise shall be performed in order to assess a risk of not meeting the requirements.

NOTE Such a preliminary availability evaluation is performed during the allocation process if a realistic allocation cannot be achieved.

b. The assessment process shall be conducted as follows:

1. identification of the most appropriate method for availability assessment (see Annex A);
2. collection and verification of data coming from the lower level analyses;
3. system availability assessment (including compliance verification) and identification of the project criticalities;
4. architecture, operations or logistics modifications or more accurate analysis (e.g. refinement of the working hypothesis on the stand-by failure rates, more realistic modelling of the functional redundancies) to reach the availability objective. This can imply the subsystem or equipment level contribution;
5. decision making process to eliminate (or reduce the impact of) the criticalities;
6. assessment process reiteration in each project phase according to the system design evolution.

c. An appropriate method, Analytic, Markovian or Monte-Carlo simulation, recognized as suitable for the assessment shall be used. The choice shall be explained and justified.

d. Sources of numerical data shall be provided (e.g. internal database from supplier data, field return experience, or calculation from standard handbooks, such as MIL HDBK 217 or UTEC 80810).

e. Each equipment item's availability shall be estimated, taking into account random and deterministic events. The dynamic behaviour models can be typically sketched as shown in Figure 3. More complex flow charts can be developed depending on the system architecture and renewal process characteristics.

f. The results of availability analyses shall be reiterated in a timely manner through the design, integration processes and operation engineering to reflect the actual system baseline.

g. For flight equipment, the availability analysis shall take into account radiation effects: for instance, upset for logic parts such as SET for opto and linear parts, and latch up.

h. Functional effects on flight equipment due to radiation single events shall be evaluated to provide quantified inputs for availability analysis."

NOTE ECSS-Q-60 branch standard gives methodology to evaluate behaviour of electronic parts within their functional conditions.

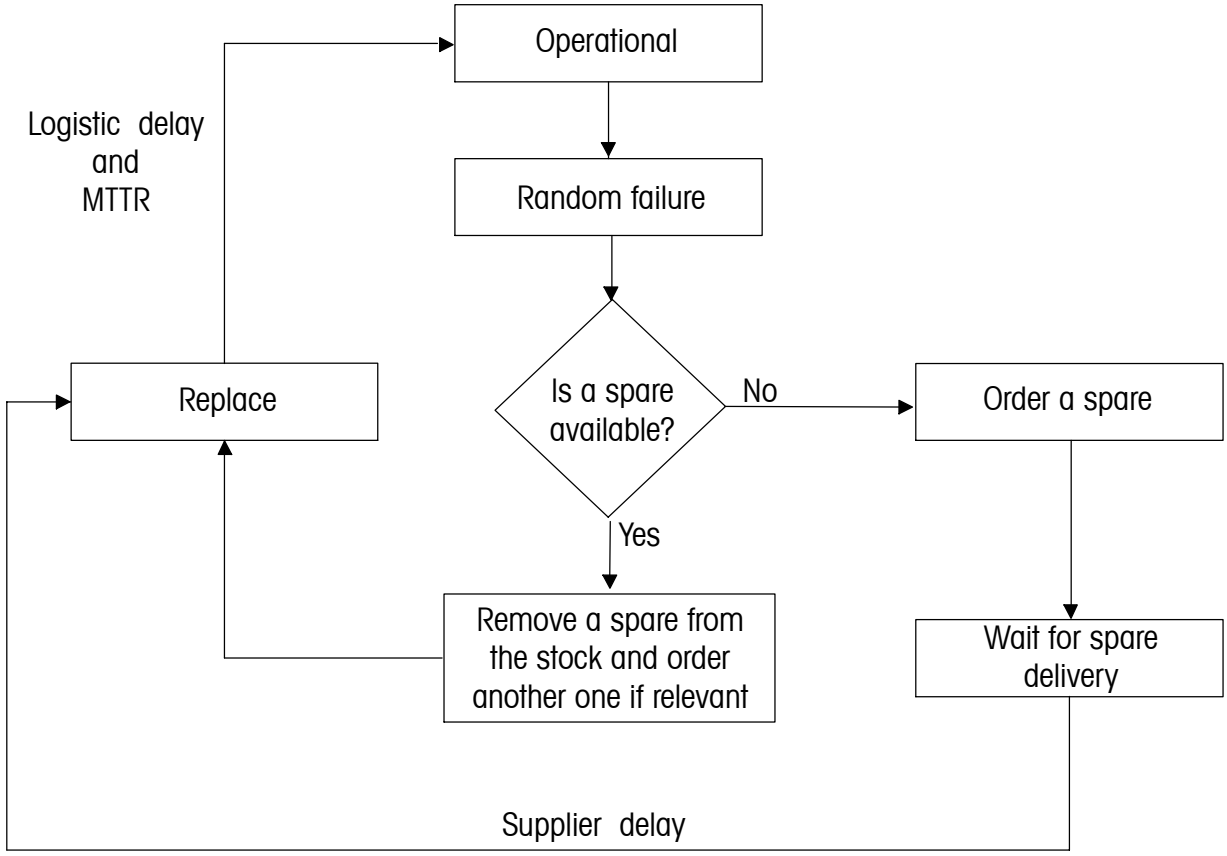

Figure 3: Example of a dynamic behaviour model

6.5 Availability report content

a. The availability analysis performed in each project phase shall contribute to the preparation of
   1. specifications,
   2. trade-off reports, and
   3. availability assessment reports.

b. Concerning the specifications, the requirements defined at lower level as a result of the allocation process shall be reported in a dedicated section.

c. The specifications section shall also include all the additional information (e.g. logistics constraints, operations provisions, and reference mission scenario) useful for the correct implementation of the requirements.

d. The availability evaluations and considerations shall be clearly described with the relevant data and assumptions.

e. The availability assessment report shall provide all the information needed to understand correctly the evaluations performed and to allow appropriate integration of the results obtained with the higher level analysis.

f. The availability assessment report shall cover the following aspects:
   1. self-standing description of the system or equipment baseline, logistics support and operations;
   2. the content, derived from the relevant reports, is useful to acquire all the elements taken into account in the availability model;
   3. availability requirements description and interpretation (this allows the verification of the correct requirement implementation);

4. availability model description (including details of the selected mathematical approach and relevant assumptions or hypotheses);
5. inputs (e.g. reliability data, logistic times, and working hypotheses);
6. results obtained;
7. conclusions and recommendations.

g. The availability assessment reports shall be delivered at project review as per contract SOW.

7

Implementation of availability analysis

7.1 General

Availability is regularly integrated into the design process. The availability characteristics can be traded with other system attributes such as cost and performance during the optimization of the design.

Availability teams are regularly integrated into the development teams during the design process. Availability analysis should be performed in close interaction with the following functions:

- integrated logistics support;
- operations;
- engineering.

7.2 Availability activities and programme phases [1)]

7.2.1 Feasibility phase (Phase A)

During Phase A, the availability analysis shall cover the following aspects:

a. identification of the methodology for the most realistic evaluation of the availability figures;

NOTE The methodology can be improved or even changed in the following phases.

b. support to the preliminary design definition in terms of trade-off studies, rough availability estimations, identification of critical areas;

c. evaluation of the availability performance of the selected reference system or equipment baseline;

d. allocation (where necessary) of the applicable requirements at lower level;

e. planning of the availability tasks for the design definition phase (Phase B or Phase C).

7.2.2 Preliminary definition phase (Phase B)

During Phase B, the availability analysis shall cover the following aspects:

a. finalization of the availability methodology;

1) For programme phases see ECSS-M-30.

b. review of the lower level analyses;
c. support to local trade-off studies and design definition;
d. contribution to maintenance strategy definition;
e. definition of input data for the availability model (e.g. manufacturer data, lower level outputs, data sources, and logistics information);
f. evaluation of the availability performance of the selected reference system or equipment baseline;
g. revision of the allocation process (where necessary);
h. support to preparation of availability specifications;
i. identification of the critical areas and support to the decision making process;
j. planning of the availability tasks for the detailed design definition phase and development and preparation of the relevant section in the PA plan.

7.2.3 Detailed definition and production phases (Phase C/D)

During Phase C/D, the availability analysis shall cover the following aspects:

a. review of the lower level analyses;
b. consolidation of the input data (input data consistency check);
c. support to the design, logistics and operations activities;
d. contribution to design reviews;
e. evaluation of the availability performance of the system or equipment baseline;
f. identification of the critical parameters or points to be monitored or controlled;
g. support to quality assurance activity during manufacture, integration and test, nonconformance review board (NRB) and failure review board;
h. support flight readiness reviews.

7.2.4 Utilization phase (Phase E)

During Phase E, the availability analysis shall cover the following aspects:

a. support to ground and flight operations;
b. evaluation of the design and operational changes and their impacts on availability;
c. collection of availability data during operation to assess the operational availability and issue of the operational availability report (when required).

Annex A (informative)

Suitable methods for availability assessment

A.1 General

This annex provides a short description of the main methods available to assess availability performance.

The application of probability theory to the availability problems has led to the development of different methodologies that allow all practical situations to be managed with the accuracy required / specified by the customer. The selection of a particular mathematical approach depends on several considerations, such as:

a. a probability density function associated with the parameters involved;

b. complexity of the system design and associated operations and logistics support;

c. time constraints for project development;

d. preventive maintenance planned during the system's operating life;

e. spares policy.

The present annex aims to list the main methods; for more details, refer to the technical literature on reliability and availability engineering.

A.2 Analytical method

The calculations use the following mathematical modelling:

$$\text{Steady state availability} = \frac{MUT}{MUT + MDT}$$

This generic formula can be adapted to the application (e.g. for operational or intrinsic for system as well as equipment level).

For components or functions that are physically independent, the resulting availability is evaluated using the basic formulae shown in Figure 4, depending on the redundancy scheme.

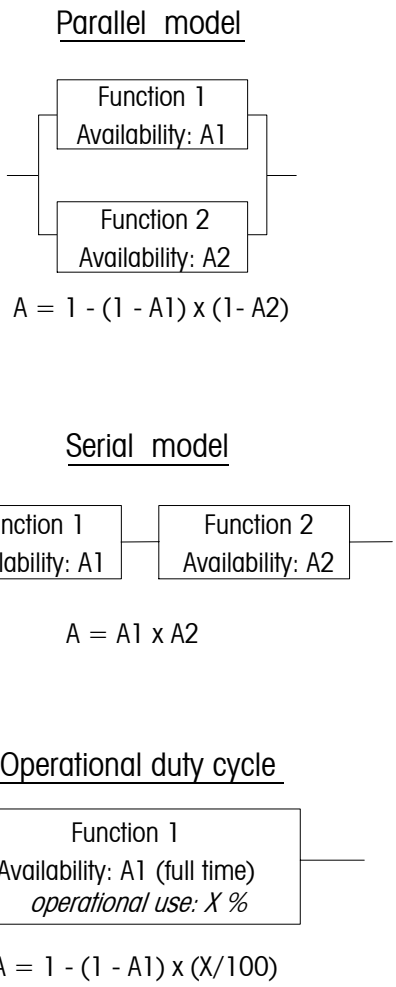

Figure 4: Basic availability formulae

A.3 Markov process

This approach, shown in Figure 5, is based on the exponential law for the time to failure and the time to repair. Markov process theory is important because

a. it provides a good representation of system behaviour for communication with the engineering teams, and

b. it allows the estimation of good approximations for the asymptotic (or steady-state) availability of some space applications, and has, for example, been efficiently applied to space ground segments.

However, the system complexity can generate a high number of expected states that impact on the calculation aspects (time and accuracy). Realistic representation of logistic times (generally associated with normal or log normal distributions) is also not possible. Markov Graph is for a simple parallel model, states 1 and 2 representing a functional system with or without redundancy being available for each state.

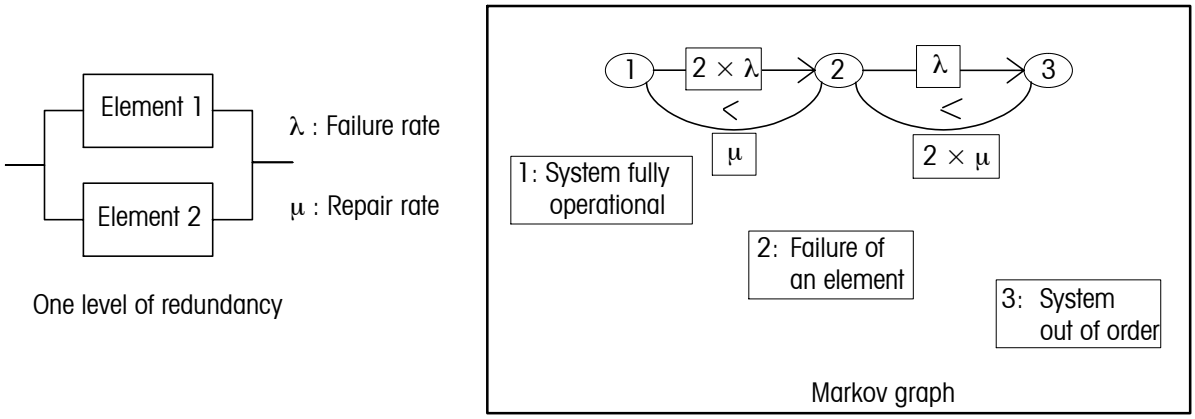

Figure 5: Example of Markov graph

A.4 Monte-Carlo simulation

This numerical technique allows the evaluation of availability taking into account in a realistic way all aspects associated with the design, logistics and operations.

In a lot of applications, Petri nets are used to model the system operating scenario, shown in Figure 6. The main advantages of Monte-Carlo simulation are the ability to handle complex system scenarios with deterministic or probabilistic delays, and one shot reliability. However, this method can involve

a. heavy effort for system modelling (not recommended for short-term programmes), and

b. long calculation times (not acceptable during the trade-off or feasibility study).

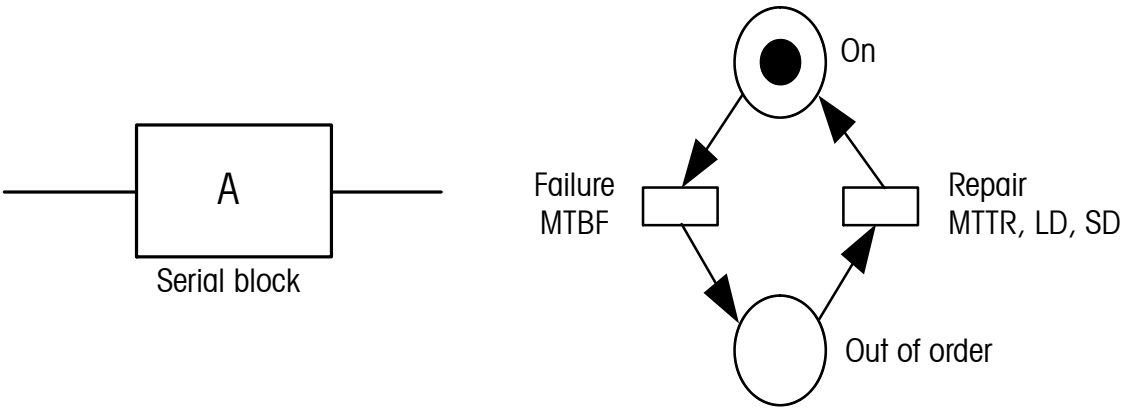

Figure 6: Example of Petri net modelling

(This page is intentionally left blank)

Annex B (informative)

Typical work package description for availability activities

The system or subsystem level RAM group can advantageously develop the following activities accordingly to the contract SOW:

a. Review of the availability requirements and verification of their acceptability by preliminary evaluations based on previous experiences or approximate models. This step is important to avoid the implementation of unachievable requirements considering, among others, the allowed logistics support, operations provisions, and power and mass budget.

b. Identification of the most appropriate availability model taking into account the mission scenario, project complexity, and time and cost constraints. If the selected methodology is extended to a lower level, dedicated procedures shall be used.

c. Preparation of lower level specification to translate the system availability requirements.

d. Definition of the system availability model.

e. Review of the lower level availability reports.

f. Verification and consolidation of the inputs coming from the other design areas (e.g. engineering, logistics, and operations).

g. Evaluation of the system availability.

h. Trade-off analysis.

i. Support to project management to finalize the system operational cost.

j. Availability activities progress reporting.

k. Support to design reviews.

l. Preparation of audits to verify the subcontractors knowledge and organization relevant to the availability discipline.

m. Support to logistics and operations department for specific probabilistic or qualitative assessments useful in the finalization of the availability model.

n. Support during the system exploitation phase for

   1. data collection,
   2. decision making process, and
   3. optimization of system operation.

(This page is intentionally left blank)

Bibliography

List of references not referenced in the normative part of the standard and provided for information purposes.

ECSS-Q-30	Space product assurance – Dependability
ECSS-Q-30-02	Space product assurance – Failure modes, effects and criticality analysis (FMECA)
ECSS-Q-40	Space product assurance – Safety
ECSS-Q-40-12	Space product assurance – Fault tree analysis – Adoption notice ECSS/IEC 61025
ECSS-M-00-03	Space project management – Risk management
ECSS-M-30	Space project management – Project phasing and planning

(This page is intentionally left blank)

ECSS Change Request / Document Improvement Proposal

A Change Request / Document Improvement Proposal for an ECSS Standard may be submitted to the ECSS Secretariat at any time after the standard's publication using the form presented below.

This form can be downloaded in MS Word format from the ECSS Website (www.ecss.nl, in the menus: Standards - ECSS forms).

ECSS Change Request / Document Improvement Proposal

1. Originator's name: Organization: e-mail:				2. ECSS Document number: 3. Date:	
4. Number.	5. Location of deficiency clause (e.g. 3.1)	page (e.g. 14)	6. Changes	7. Justification	8. Disposition

Filling instructions:

1. **Originator's name -** Insert the originator's name and address
2. **ECSS document number -** Insert the complete ECSS reference number (e.g. ECSS-M-00B)
3. **Date -** Insert current date
4. **Number -** Insert originator's numbering of CR/DIP (*optional*)
5. **Location -** Insert clause, table or figure number and page number where deficiency has been identified
6. **Changes -** Identify any improvement proposed, giving as much detail as possible
7. **Justification -** Describe the purpose, reasons and benefits of the proposed change
8. **Disposition -** not to be filled in (*entered by relevant ECSS Panel*)

Once completed, please send the CR/DIP by e-mail to: ecss-secretariat@esa.int

(This page is intentionally left blank)