ESA PSS-01-40 Issue 2
September 1988

System safety requirements for ESA space systems

Prepared by:
Product Assurance & Safety Department
European Space Research and Technology Centre
Noordwijk, The Netherlands

Approved by:
The Inspector General, ESA

european space agency / agence spatiale européenne
8-10, rue Mario-Nikis, 75738 PARIS 15, France

Published by ESA Publications Division,
ESTEC, Noordwijk, The Netherlands.

Printed in the Netherlands.

ESA Price code: E1
ISSN 0379 - 4059

Copyright © 1988 by European Space Agency

ABSTRACT

This specification defines the system safety requirements which implement the ESA safety policy and which are applicable to ESA space systems and associated equipment. The specification is divided into two sections. Section I defines safety programme requirements, while Section II defines technical system safety requirements.

DOCUMENT CHANGE RECORD			
Issue	**Rev.**	**Change**	**Pages affected**
2	0	Document completely revised.	All

TABLE OF CONTENTS

TABLE OF CONTENTS
(continued)

TABLE OF CONTENTS
(continued)

PAGE INTENTIONALLY LEFT BLANK

INTRODUCTION

PAGE INTENTIONALLY LEFT BLANK

CHAPTER 1: INTRODUCTION

1.1 SCOPE

This specification defines the system safety requirements which implement the ESA Safety Policy and which are applicable to ESA space systems and associated equipment. The specification is divided into two sections. Section I defines safety programme requirements, while Section 2 defines technical system safety requirements.

1.2 ESA SAFETY POLICY

The ESA safety policy is defined in ESA PSS-01-0 (Product assurance and safety policy and basic requirements for ESA space systems), which is fully applicable.

The safety policy is supported by technical safety requirements which are defined in Section II of this specification. The primary technical requirements are:

— the implementation of failure tolerance where hazards can propagate to catastrophic or critical consequences;

— the provision of crew escape and rescue capabilities for all phases of manned spaceflight missions; and

— the incorporation of a hazard detection, annunciation, and safing function in manned spaceflight systems.

The Safety policy is applied by implementing a deterministic safety programme, supported by progressive risk assessment as defined in Section I of this specification, which may be summarised as follows:

— The hazardous characteristics (hazards and hazardous conditions) associated with system design and its mission phases, including the total system environment, are identified and progressively evaluated by performing an iterative process of systematic qualitative hazard analysis.

— The potential hazardous consequences associated with the identified system hazardous characteristics are reduced by the application of a reduction precedence whereby:

- hazardous characteristics are eliminated from the system (to the extent that this is consistent with project objectives);

- hazards associated with the remaining system hazardous characteristics are minimised in order to reduce the severity of the consequences of any associated hazardous event; and

- hazard controls (see Section II of this specification) are applied to the remaining system hazardous characteristics in order to reduce hazardous event occurrence rates and/or to mitigate the consequences of hazardous events should these occur.

— The residual hazards and risks remaining after the application of the elimination, minimisation and control process, are progressively assessed, and subjected to risk analysis, in order to:

- support design trades;

- identify and rank risk contributors;

- support risk apportionment and the establishment of safety targets;

- assess risk reduction progress;

- support the safety and project decision-making process (e.g waiver approval, residual hazard and risk acceptance).

— The adequacy of the hazard control measures which are applied, are formally verified in order to support hazard and risk acceptance.

— Hazards which cannot be eliminated or minimised and resolved in accordance with project requirements are high-lighted and presented to management for resolution.

Figure 1 provides an outline of the safety-programme life cycle for the implementation of this policy.

1.3 APPLICABILITY

This specification is applicable to ESA contracts where, during any project phase, there exists the potential for hazards to personnel or the general public, spaceflight systems, ground support equipment, facilities, public or private property, or the environment, as the result of ESA project activities involving ESA flight hardware, software, GSE, or ground facilities.

The specific applicability of the safety programme and technical requirements defined in this specification and its supporting specifications will be tailored by ESA in accordance with the project's safety criticality, and specific application. It is the contractor's responsibility to ensure that, in any subcontracts placed, the relevant requirements from this specification are applied.

The specific applicable requirements of Section I will be defined in the ESA Project Product Assurance and Safety Requirements. The specific applicable requirements of Section II will be defined in the ESA Project Technical Specification.

PAGE INTENTIONALLY LEFT BLANK

2.0 APPLICABLE DOCUMENTS

The following documents are applicable to the extent specified herein:

Section I

(a) PSS-01-11 Configuration management and control for ESA space systems.

(b) PSS-01-20 Quality assurance of ESA space systems.

(c) PSS-01-21 Software quality assurance for ESA space systems.

(d) PSS-01-30 Reliability assurance for ESA space systems.

(e) PSS-01-50 Maintainability and availability assurance of ESA space systems.

(f) PSS-01-60 Components selection, procurement and control for ESA space systems.

(g) PSS-01-70 Material and process selection and quality control for ESA space systems.

(h) PSS-01-400 Safety data package requirements.

(i) PSS-01-402 ESA design safety requirements.

(j) PSS-01-403 Hazard analysis requirements and methods.

(k) PSS-01-404 Risk assessment requirements and methods.

(l) PSS-06-20 ESA guidelines for project reviews.

Section II

(a) PSS-01-0 Product assurance and safety policy and basic requirements for ESA space systems.

(b) PSS-01-401 ESA fracture control requirements.

(c) PSS-01-402 ESA design safety requirements.

(d) NHB 1700.7 Safety policy and requirements for payloads using the STS.

(e) KHB 1700.7 STS payload ground safety handbook.

(f) SLP/2104 Spacelab payloads accommodation handbook.

SECTION I

SAFETY PROGRAMME REQUIREMENTS

PAGE INTENTIONALLY LEFT BLANK

CHAPTER I – 1: GENERAL

The contractor shall establish and implement a formally controlled and documented safety programme that complies with the safety requirements specified herein, with the Project objectives as defined in the Statement of Work and with the ESA Project product assurance and safety requirements.

The scope and content of the Project Safety Programme shall be tailored in accordance with the type of project, project safety criticality, complexity, and phase of development as defined in the Statement of Work and in the ESA Product Assurance and Safety Requirements. Nothing in this document shall be construed as a requirement for duplication of effort.

The contractor shall apply the launcher authority's safety requirements and regulations as defined in this specification, in its supporting specifications (if any) and in the Project requirements.

Compliance with the safety requirements defined herein shall in no way relieve contractors from the requirement to comply with their own country's national safety regulations. National safety regulations in countries other than those of the contractors, where project hardware or software is used or operated, shall be applied.

PAGE INTENTIONALLY LEFT BLANK

CHAPTER I – 2: SAFETY ASSURANCE ORGANISATION AND MANAGEMENT

The contractor shall have personnel who are responsible for system safety assurance who shall be part of the project team. These safety personnel shall be functionally responsible to a home department that has a reporting line to company management that is independent of the design, manufacturing, assembly, integration, and testing or operations departments. Within projects, the contractor's assigned safety personnel shall have a similarly independent reporting line to the Project Manager, in addition to that through their home department.

PAGE INTENTIONALLY LEFT BLANK

CHAPTER I – 3: SAFETY ASSURANCE PERSONNEL ACCESS AND AUTHORITY

Irrespective of company organisation, safety personnel shall have the right of access to all data relevant to safety and shall be at liberty to report freely and without organisational constraint on any aspect of safety. The organisation shall not permit any report which addresses matters related to safety to be issued without the signed approval of safety assurance personnel. No hazardous operation or system mission shall be permitted to proceed without prior safety assurance review and the written permission of the responsible safety assurance personnel.

PAGE INTENTIONALLY LEFT BLANK

CHAPTER I – 4: SYSTEM SAFETY PROGRAMME PLAN

I – 4.1 PREPARATION AND APPROVAL

The contractor shall prepare a System Safety Programme Plan in response to, and in compliance with, the Project contractural requirements and the applicable safety requirements defined herein. The Plan may either be included as part of an overall Project Product Assurance Plan, or as a separate subplan. The Plan shall be subject to approval by the ESA Project Organisation.

I – 4.2 APPLICABILITY AND ISSUE

Safety planning shall be provided for all phases of the project. The Plan shall initially be issued as required by the Statement of Work and shall cover the safety activities for the Project Phase(s) as defined in the Contract.

I – 4.3 SCOPE AND CONTENTS

The scope of the Plan shall encompass the activities which are necessary in order to comply with the requirements of this specification, its applicable supporting specifications, and the Statement of Work.

The Plan shall define the safety programme that is to be implemented and shall show how the contractor is to accomplish the tasks and verify their satisfactory completion. Each project safety activity shall be identified and defined, the method of implementation summarised, and the implementation schedule specified against project milestones. The safety programme implementation flow shall comply with the safety-programme life cycle shown in Figure 1.

The Plan shall include a description of the project safety organisation, its responsibilities, and its working relationship with the reliability, maintainability, parts, materials and processes, quality assurance, and configuration-management disciplines of product assurance, and with the system engineering and design and other project functions and company departments.

The Plan shall show how the safety programme is implemented as an integral part of the product assurance and safety function. Organisational responsibility for overlapping and interfacing functions, such as: reliability, maintainability, quality assurance, parts, materials and processes, and

configuration management and control, shall be clearly defined (see Figure 2).

The Plan shall describe how safety-related activities will be defined for, and controlled at, subcontractors' and suppliers' premises. Only those requirements that are relevant to the subcontractors' and suppliers' activities and responsibilities shall be made applicable.

The Plan shall also make provisions for conformance to safety requirements and regulations that are applicable to any other facilities and services to be utilised during the course of the project, as defined in the Statement of Work.

CHAPTER I – 5: SAFETY PROGRAMME TASKS

Safety-programme tasks to be performed during the various project phases are defined in Annex I. The specific applicability and scope of the safety-programme tasks to be performed will be defined in the ESA Project Product Assurance and Safety Requirements and the Statement of Work.

PAGE INTENTIONALLY LEFT BLANK

I – 6: PROJECT TECHNICAL SAFETY SPECIFICATION

The contractor shall prepare and issue a Project System Safety Technical Requirements Specification, which defines the design and operational safety requirements applicable to the Project. The specification shall include system-level design and operational safety requirements and appropriate functional, subsystem, equipment, and ground-support-equipment detailed safety requirements. The specification shall be subject to approval by the ESA Project organisation.

The appropriate requirements from ESA Project specification(s), Section II of this specification and PSS-01-402 (ESA design safety requirements), and from experience gained on similar projects, shall be included in the Project safety specification, either by specific reference, or by incorporation into the project specification. Additional safety requirements, identified as the result of hazard analysis and risk assessment during the course of the project, shall also be incorporated into the specification.

The Project System Safety Technical Requirements Specification shall be made applicable by reference in the Project System Requirements Specification, and in other lower-level specifications, as appropriate. Alternatively, technical safety requirements which are specifically applicable to lower-level elements, subsystems or equipment may be specified directly in the relevant specifications. The System Safety Technical Requirements shall be under formal verification control.

The Project Safety Specification shall be issued and updated as defined in Chapter I – 5, in order to ensure that the relevant safety requirements are available for application at the appropriate times during the project.

PAGE INTENTIONALLY LEFT BLANK

CHAPTER I – 7: SAFETY ASSURANCE

I – 7.1 SAFETY ANALYSIS

The contractor shall perform safety analyses in a systematic manner and update these as necessary throughout the safety programme in order to ensure that safety is designed into the system, that safety requirements are met and that hazards are identified, eliminated, minimised and resolved in a manner acceptable to ESA.

I – 7.1.1 Hazard analysis

The contractor shall perform hazard analyses in order to:

— identify design and operational hazards;

— evaluate the applicable hazards, hazardous conditions, and related hazardous events and their causes;

— categorise hazardous event consequences;

— support design trades;

— support hazard-reduction implementation;

— identify residual hazards;

— determine applicable safety requirements and hazard controls;

— demonstrate that the identified requirements and controls have been applied and their adequacy verified.

Hazard analysis shall be performed in a systematic and iterative manner, beginning in the concept phase and continuing through the operational phase.

Hazards that are associated with: hardware design, material or parts characteristics; software characteristics or functions; normal, back-up, emergency, assembly, or maintenance operations; procedural deficiencies; personnel errors; time limitations; and operational environments; shall be identified and evaluated.

The results of failure-mode, criticality and effect analyses, performed in accordance with the requirements of ESA PSS-01-30, shall be used as an input to the hazard analysis, as appropriate.

I – 7.1.1.1 Hazard consequence severity categories

The consequences of identified hazardous events shall be categorised as follows:

I CATASTROPHIC

— loss of life, life-threatening or permanently disabling injury or occupational illness;

II CRITICAL

— temporarily disabling, but not life-threatening injury, or temporary occupational illness;

— loss of, or major damage to, flight systems, major flight-system elements, or ground facilities;

— loss of, or major damage to, public or private property; or

— long-term detrimental environmental effects.

III MARGINAL

— minor non-disabling injury or occupational illness;

— minor damage to other hardware;

— minor damage to public or private property; or

— temporary detrimental environmental effects.

IV NEGLIGIBLE

Will not result in any of the above.

NOTE: For ESA projects launched by other agencies or launch authorities, the hazard categories defined by those agencies or launch authorities shall apply during the applicable operational phases.

I – 7.1.1.2 Hazard reduction

The following hazard reduction precedence shall be applied to the identified applicable hazards and hazardous conditions:

(a) **Hazard elimination**

From the commencement of the conceptual phase, hazards and hazardous conditions shall, as far as is consistent with the project and mission objectives, be eliminated from the design and operational concepts by the selection of the least hazardous design options and operational scenarios.

(b) **Design for minimum hazard**

Hazards, and hazardous conditions that cannot be eliminated, shall be minimised through the selection of design concepts and characteristics that minimise the severity of potential hazardous events and their hazardous consequences, and limit the exposure of personnel to hazardous consequences.

(c) **Hazard control**

The remaining hazards (residual hazards) shall be resolved by the application of the following hazard-control precedence:

(i) Selection and implementation of appropriate design features that minimise the probability of hazardous event occurrence and their propagation to hazardous effects, including application of failure tolerance, safety factors, materials and parts selection and control, safety devices, isolation of hazards, hazard containment, and damage control.

(ii) When corrective action is required in order to prevent the propagation of hazardous effects, warning devices shall be incorporated to provide timely detection and unambiguous visual and audible warning of the developing potentially hazardous events. The design shall provide the capability for the implementation of safing functions and/or contingency operations.

(iii) When it is not possible satisfactorily to minimise or control a residual hazard by design or by safety or warning devices, special procedures shall be developed to counter the associated

hazardous events and their consequences. Special procedures may include emergency and contingency procedures, procedural constraints, or the application of a controlled maintenance programme. Special Procedures shall be qualified by testing, and appropriate training shall be provided for personnel.

Special procedures are the least effective of the hazard-control measures available. Emphasis shall therefore be laid on hazard control by the application of the alternative hazard-control measures in the defined order of precedence.

I – 7.1.1.3 Preliminary hazard analysis (PHA)

Preliminary hazard analysis shall be started in the conceptual phase and shall continue through the project-definition phase at a level of detail commensurate with the evolution of the design concepts, and in accordance with ESA PSS-01-403 (Hazard analysis requirements and methods).

The preliminary hazard analysis shall identify the applicable hazards and hazardous conditions associated with the design concepts under study, the hazardous events that can result, and their causes and consequences. The analysis results shall be used to support: hazard reduction; the identification of hazard-control/safety requirements; the identification of safety critical functions and items; concept evolution; and design trades. The analysis shall also provide input data to the risk assessments performed in support of project and safety reviews during the conceptual and project-definition phases.

The results of the preliminary hazard analysis shall also be used as an input to the detailed system hazard analyses performed during the development and hardware phase of the project.

The analysis data and results shall be included in an analysis report, which shall be prepared in accordance with ESA PSS-01-400 (Safety data package requirements) and issued to support project and safety reviews. The report shall be subject to ESA review and acceptance.

I – 7.1.1.4 Preliminary operating hazard analysis (POHA)

Preliminary operating hazard analysis shall be started in the conceptual phase and shall continue through the project-definition phase, to a level of detail commensurate with the evolution, status and definition of the design concepts, and the mission operational scenarios, in accordance with ESA PSS-01-403 (Hazard analysis requirements and methods).

The preliminary operating hazard analysis shall identify the hazards and hazardous conditions associated with the different phases of the

operational scenarios under study (including both ground and flight operations), the hazardous events that can result, and their causes and consequences. The analysis shall also provide first estimates of the scope and depth of crew training necessary for the performance of hazardous operations, in order to avoid over or under training. Analysis results shall be used to support: hazard reduction; the identification of safety critical functions; the identification of hazard-control/safety requirements; concept evolution; and operational concept trades. The analysis shall also provide input data to the risk assessments performed in support of project and safety reviews during the conceptual and project-definition phases.

The results of the preliminary operating hazard analysis shall also be used as an input to the detailed system operating hazard analyses that are performed during the development and hardware phases of the project.

The analysis data and results shall be included in an analysis report, or combined with the preliminary hazard analysis report, which shall be prepared in accordance with ESA PSS-01-400 (Safety data package requirements) and issued to support project and safety reviews. The report shall be subject to ESA review and acceptance.

I – 7.1.1.5 System design hazard analyses

Detailed 'system' hazard analyses shall be performed on the design during the development and flight-hardware phase of the project, in accordance with ESA PSS-01-403 (Hazard analysis requirements and methods).

For the analyses, use shall be made of the results of the PHA and POHA as initial inputs together with the results of failure-mode effect and criticality analyses performed as part of the reliability programme. The 'system' hazard analyses shall be refined and updated in an iterative manner as the design process proceeds, to ensure that new hazards, hazardous conditions, hazardous events and their causes are identified, and that the relevant detailed design and operational requirements, hazard controls and verification activities are defined and implemented.

The detailed 'system' hazard analyses shall also be used to: provide input data to the risk assessments performed during the development and flight-hardware phase of the project; and identify subsystem and equipment design safety requirements.

The analyses shall be performed to a level of detail commensurate with the available design information, and shall include consideration of safety critical functions and end-to-end functional paths including system, element, module and subsystem interfaces, as appropriate. Lower-level detailed hazard analyses may be used to support the system hazard analysis, as necessary.

System hazard analysis documentation shall provide traceability to the design standard analysed. The analysis data and results shall be

included in an analysis report, which shall be prepared in accordance with ESA PSS-01-400 (Safety data package requirements) and issued to support project and safety reviews. The analysis report shall provide for hazard control status reporting and tracking. The report shall be subject to ESA review and approval.

I – 7.1.1.6 Operating hazard analysis

System, element and module operating hazard analyses shall be performed during the development and flight-hardware and operational phases of the project in accordance with ESA PSS-01-403 (Hazard analysis requirements and methods).

For these analyses, use shall be made of the results of the POHA as an initial input, together with the results of the detailed system and lower-level hazard-analysis activities, as these become available. The analyses shall be refined and updated in an iterative manner as operations and procedures are defined in more detail, or are modified, in order to ensure that new operational hazards, safety critical functions, hazardous conditions and hazardous causes are identified, and that the relevant design and operational requirements, hazard controls, procedural constraints and verification actions are defined and implemented. The analysis shall be performed to a level of detail commensurate with the available design and operational information, shall address nominal and contingency ground and flight operations and procedures. The analysis shall identify potentially hazardous operations and shall address sensitivity to human error. The estimates from the POHA of the scope and depth of crew training required shall be updated.

The operating hazard analyses shall be used to provide input data to the risk assessments performed during the development and flight-hardware phase of the project.

The analysis documentation shall provide traceability to the design standard and operational baseline analysed. The analysis data and results shall be included in an analysis report, which shall be prepared in accordance with ESA PSS-01-400 (Safety data package requirements) and issued to support project and safety reviews. The analysis report shall also provide for hazard control status reporting and tracking. The report shall be subject to ESA review and approval.

I – 7.1.2 Warning-time analysis

Warning-time analysis shall be performed during the development and flight-hardware phase when, during hazard analysis, time critical situations are identified, or the application of the hazard-control precedence sequence results in the use of warning devices and/or contingency procedures.

The analysis shall determine:

— the time during which the event must be detected and the response action taken;
— the detection capability of the proposed design with respect to detection sensitivity and detection times;
— the resultant time available for response;
— the adequacy of the proposed design and/or contingency procedures, including emergency evacuation, rescue, system reconfiguration, redundancy switching, and maintenance.

The detection times to be determined shall be:

— from the occurrence of the fault condition to the time when a hazardous condition develops;
— the time from the occurrence of the fault condition to the time of detection and/or annunciation; and
— the time taken for corrective action to be implemented.

The results of the analysis shall be documented in a Warning Time Analysis Report, which shall be issued to support project and safety reviews. The report shall be subject to ESA review and acceptance.

I – 7.1.3 Caution and warning analysis

Caution and warning analysis shall be performed during the development and flight-hardware phase of manned spaceflight programmes.

The analysis shall identify: emergency, warning and caution parameters; safing functions; limit sensing requirements; and the applicability of the individual 'caution and warning' functions to the various mission phases.

For caution and warning analyses, use shall be made of the results of the warning-time and hazard analyses, as appropriate. The analysis shall be documented in a Caution and Warning Analysis Report, which shall be issued in support of project and safety reviews. The report shall be subject to ESA review and acceptance.

I – 7.2 HAZARD TRACKING AND ACCEPTANCE

The contractor shall establish a system for tracking the status of all identified hazards. The system shall be applied for all catastrophic, critical and marginal hazard consequences. The status of each hazard shall, as a minimum, be indicated as:

— being evaluated;

— eliminated;

— confirmed residual hazard;

— hazard controls defined and agreed within the contractor's project organisation;

— hazard control verification methods defined and agreed within the contractor's project organisation;

— hazard control verification completed and submitted to ESA for acceptance;

— unresolved residual hazard.

Hazard status shall be reported at safety progress meetings and documented for ESA review for formal safety reviews.

When a hazard has been eliminated by design, the contractor shall submit documentary evidence which verifies accomplishment.

A hazard shall be considered for acceptance only if the hazard has been minimised and/or resolved in an acceptable manner in accordance with the hazard reduction precedence, and implementation has been verified by way of the successful completion of: drawing review; inspection; the required test programmes; analytical studies; design review; procedure preparation; and/or training programmes, as appropriate.

All catastrophic, critical and marginal hazards that cannot be eliminated by application of the hazard reduction precedence shall be designated as 'residual hazards'.

Catastrophic and critical residual hazards shall be submitted for review and formal disposition by ESA, and as appropriate by the launch authority. Marginal residual hazards may be accepted by the contractor. Marginal residual Hazards will be subject to audit by ESA for correct categorisation and adequacy of control.

I – 7.3 UNRESOLVED RESIDUAL HAZARDS

Catastrophic and critical residual hazards that cannot be minimised and/or resolved in accordance with the hazard reduction precedence sequence shall be identified for special safety and management attention. These unresolved residual hazards shall be listed and the list provided to ESA. The information required for each unresolved residual hazard is defined in Annex II to this specification.

Unresolved residual hazards that through subsequent actions are eliminated or minimised and/or controlled in accordance with the requirements of this specification shall be deleted from the list on the approval of ESA.

The Unresolved Residual Hazard List shall be issued for each safety review and major project review. Additions to, or proposed deletions from, the list shall initially be reported in the Product Assurance Progress Report.

I – 7.4 IDENTIFICATION AND CONTROL OF SAFETY-CRITICAL FUNCTIONS AND SAFETY-CRITICAL ITEMS

System functions that, if lost or degraded, or that, through incorrect or inadvertent operation, would result in a catastrophic hazard consequence shall be identified as safety critical. Hardware, software and firmware that perform a safety-critical function shall be identified as safety-critical items. Flight or ground-control procedures which control safety-critical functions shall be identified as safety critical.

The contractor shall prepare a Safety-critical Items List which is subject to ESA approval. The Safety-critical Items List shall identify the safety-critical functions and the associated safety-critical procedures and items, and shall include each item's safety-critical performance characteristics. Safety-critical items shall be ranked for criticality with the aid of criteria defined by the contractor and approved by ESA.

Safety-critical functions, procedures and items shall be controlled by an integrated Critical Items Control Programme, which shall be established and run by the contractor. The programme shall be subject to ESA approval.

The Critical Items Control Programme shall ensure that:

— all design, manufacturing and testing documentation that is related to safety-critical functions, items and procedures is identified and marked, and that document traceability is maintained by document number and issue;

— safety-critical functions are subject to sneak-circuit analysis;

— Safety is represented on Material Review Boards (MRB), Failure Review Boards (FRB), Configuration Control Boards (CCB) and Test Review Boards (TRB) that are concerned with safety-critical functions, procedures and items;

— the qualification status of all safety-critical functions, procedures and items is tracked;

— safety-critical functions, procedures and items are qualified in accordance with the requirements of Paragraph I – 7.5;

— assembly, maintenance, servicing, testing and operation of safety-critical items is monitored for problems affecting the critical characteristics of the items which may arise during the operational phase.

The Safety Critical Items List and Control Programme shall be co-ordinated and integrated with the Project Critical Items List and Control Programme. The Safety Critical Items Control Programme shall be implemented during the design and flight-hardware and operational phases of the project. The Safety Critical Items List shall be issued to support design and safety reviews.

I – 7.5 SAFETY VALIDATION AND QUALIFICATION TESTING

The contractor shall include testing of hardware, software, firmware and procedures that perform safety-critical functions, in order to verify the required margin of safety in the design and in the operational modes and procedures. The tests shall include the demonstration of nominal, contingency and emergency procedures.

Safety-critical functions shall be validated by end-to-end testing that includes application of the operating procedures, the 'man-in-the-loop', and the verification of the effectiveness of applicable fault-tolerance requirements.

The safety-critical characteristics of all safety-critical items shall be fully qualified by test.

Qualification testing of safety-critical items shall include the determination of performance margins, considering worst-case combinations of induced and natural environments and operating conditions. Qualification 'by similarity' shall be applied only after ESA approval on a case-by-case basis.

Induced failure tests shall be considered for evaluating failure effects and for demonstrating failure tolerance compliance in safety-critical functions and items. Validation of unique safety-required design or

operational characteristics shall form part of the development, qualification and/or acceptance testing programme, as appropriate. Where full-scale testing is not possible owing to cost or technical constraints, separate equivalent safety-validation testing may be performed with the aid of technically representative hardware or models on ESA approval.

I – 7.6 NONCONFORMANCES AND WAIVERS

The contractor shall identify all nonconformances and waivers that affect: the applicable project safety requirements or safety-critical functions and items. These nonconformances and waivers shall be reviewed by the project safety organisation to ensure that: possible impacts on safety are fully analysed; no unacceptable hazardous conditions can arise; and adequate justification for any nonconformance that is considered to be acceptable by the contractor is provided. Safety shall be represented on the relevant CCB's, MRB's, FRB's, and TRB's to support this activity.

The accumulated nonconformances and waivers that affect safety shall be assessed to ensure that the effects of individual nonconformances do not invalidate the rationale used for the acceptance of other nonconformances.

The contractor shall maintain a tracking list of all safety-related nonconformances and waivers reviewed.

Nonconformances and waivers that affect project safety requirements or safety-critical functions and items, which the contractor considers to be acceptable, shall be the subject of review and disposition by ESA Safety, and shall be processed in accordance with project procedures.

I – 7.7 PROGRESSIVE RISK ASSESSMENT

Risk assessment shall be performed in progressive steps during the implementation of the safety programme, in accordance with ESA PSS-01-404 (Risk assessment requirements and methods). Risk Assessment shall be used to:

— support design trades (risk comparison);

— rank risk contributors;

— identify major risk contributors;

— perform sensitivity analysis;

— support risk apportionment;

— support the decision-making process (e.g. for waivers, unresolved residual hazards, etc.);

— monitor the effectivity of the hazard-control and risk-reducing process;

— evaluate performance trends and anomalies.

The results of quantitative analysis shall not be used as the sole basis for acceptance/rejection of residual hazards or system risk.

System risk assessment shall be performed in support of project and safety reviews (see Figure 1). The assessment shall include evaluation of the effects of hazard-control activities and the accumulated effects of residual hazards, safety nonconformances and waivers, in order to determine the overall project safety risk. The assessment shall ensure that overall project safety is not eroded by: design or operational changes; interactions; anomalies; trends; the inability to comply with safety requirements; the inability to implement hazard-control requirements or actions as defined; or the unacceptable accumulation/concentration of risk contributors in individual system functions or operational phases.

Data sources used for risk assessment shall be identified and classified as subjective/objective. Such data sources are:

— expert judgement (subjective);

— derived data, e.g. by similarity (partially subjective/partially objective);

— data from previous experience, e.g. generic parts data (objective);

— directly relevant test data (objective).

Confidence in data shall be determined by considering:

— the number and classification (gradation of optimism/pessimism) of independent experts used;

— the number of trials by test;

— the size of the experience data set relating to normal operation.

An acceptable minimum level of data confidence shall be defined and applied to determine which data are acceptable for use in analysis.

All acceptable relevant data (i.e subjective to objective) shall be used in risk assessment. The confidence level of the subjective and/or objective data is a separate risk parameter that shall be considered

in addition to the consequence severity and occurrence rate of the undesired hazardous event. Degrees of subjectivity and objectivity shall be displayed together with the levels of data confidence in the analysis results.

The results of the risk assessment shall be included in a Risk Assessment Report which shall also give the contractor's opinion on the acceptability or otherwise of the assessed risk, and identify any sources of potential concern (including major risk contributors and unresolved residual hazards) together with the contractor's recommendations for their resolution. The report shall be issued to support Project Design, Qualification, Acceptance, Flight Readiness, and Launch Commitment Safety Reviews, as required by the contract. The report shall be subject to ESA approval.

I – 7.8 CONTROL OF HAZARDOUS OPERATIONS

I – 7.8.1 Readiness reviews and monitoring

The Contractor shall institute procedures to perform safety readiness reviews and inspections prior to the performance of any operation or test which:

— is potentially hazardous to personnel or hardware;

— has high risks in terms of programme importance; or

— involves particularly valuable or critical test hardware, facilities or effort.

Readiness reviews and inspections shall include safety assessments of facilities, equipment, test articles, operating test and contingency procedures, access controls, and personnel capabilities. These reviews and inspections shall be included in the contractor's mandatory and key inspection programme.

Hazardous operations shall be monitored for compliance with safety requirements and procedures, and for the possible development of hazardous conditions. Where necessary, contingency and emergency procedures shall be established and verified.

I – 7.8.2 Safety training and certification

The Contractor shall establish training programmes, provide training and, where applicable, certification for personnel who are involved in project hazardous operations and activities, or activities that are critical to the safety of personnel and/or the flight hardware.

Applicable ESA, national, industrial and other agency (e.g. CNES, NASA) safety requirements and procedures shall form a basis for this training.

Where safety training is required for the flight operations crew, or for mission control personnel, this shall be identified to ESA, together with a definition of the type of training required, and its scope.

I – 7.9 ACCIDENT/INCIDENT REPORTING AND INVESTIGATION

I – 7.9.1 Reporting requirements

The contractor shall report to ESA all accidents that occur during project activities under the control of the contractor or his sub-contractors. The contractor shall also report incidents that could have resulted in personnel loss of life or serious injury.

When an accident or reportable incident occurs, the contractor shall, within 24 hours, notify ESA by telex of the following:

(a) brief description of accident/incident;

(b) tentative cause;

(c) personnel involved/injured;

(d) estimated damage to project hardware;

(e) estimated damage to property;

(f) estimated consequences to the project;

(g) proposed corrective actions.

The Contractor shall follow up the telex report with an Accident/Incident Report containing the following information:

(a) report number;

(b) distribution and number of copies;

(c) originating contractor;

(d) date of accident/incident;

(e) location of accident/incident;

(f) identification of personnel/project hardware involved;

(g) description of the accident/incident together with identification of possible causes;

(h) estimate of schedule and cost impact;

(i) recovery proposal.

The reporting format shall be standardised across the project.

I – 7.9.2 Investigation, analysis and closure

The contractor's safety organisation shall be responsible for the investigation of any reportable accident/incident. The safety organisation shall co-ordinate the investigation in co-operation with other functional departments, and subcontractors as necessary. All accident/incident investigation results shall be evaluated for necessary feedback into design, procedures, personnel training, or facility equipment.

The contractor shall prepare an accident/incident analysis report. The report shall be based on the accident/incident report issued, but shall provide more technical detail of the identified cause(s), recovery actions taken, and the recurrence control implemented, or to be implemented. The accident/incident shall remain open until closure is approved by ESA.

I – 7.10 SAFETY REVIEWS AND MEETINGS

The contractor shall hold regular safety progress meetings with ESA and his subcontractors. The contractor shall plan and support reviews by ESA (and, as necessary, the launcher authority) of the project safety status, as required by this specification and the contract. Safety reviews shall be performed at all levels necessary to ensure satisfactory implementation of safety-programme and technical-safety requirements. ESA shall chair all safety reviews. As a minimum, ESA will perform safety reviews in conjunction with the following milestones, with the objectives specified:

(a) **System Requirements Review/Concept Review (see ESA PSS-06-20)**
System-level applicable hazards, hazardous conditions and events, together with safety-critical aspects of the concept selected, shall be identified. Project system-level safety requirements shall be defined. A Safety Data Package and preliminary Safety Risk Assessment Report shall be prepared and made available for ESA review and approval.

(b) **System Baseline Review/Design Definition Review (see ESA PSS-06-20)**

Safety Requirements shall be specified down to subsystem level in sufficient detail for the preliminary design to commence. Verification methods for hazard controls and safety requirements down to subsystem level shall be defined and included in the project verification programme. The following documents shall be available for ESA review and approval:
the Project Technical Safety Requirements Specification;
the Safety Plan for the Development and Flight Hardware Phase;
a Project Safety Data Package; and
a Safety Risk Assessment Report.

(c) **Preliminary Design/Subsystem Baseline Review (see ESA PSS-06-20)**

Hazard controls and safety requirements shall be sufficiently defined for detailed design to commence. The design as presented shall comply with the safety requirements to the level of detail required by the review. Verification methods for all hazard controls and safety requirements shall be defined, and the required activities included in the project verification programme. Safety-critical items shall be identified and listed. Noncompliances with safety requirements shall be identified. A Safety Data Package and a Safety Risk Assessment Report shall be prepared and made available for ESA review and approval.

(d) **Development Test Review/Critical Design Review (see ESA PSS-06-20)**

All safety requirements shall be incorporated into the design, or adequate justification for noncompliance processed. Development testing of safety-critical items and functions shall be completed and the test reports issued. A Safety Data Package and a Safety Risk Assessment Report shall be prepared and made available for review.

(e) **Qualification Reviews (see ESA PSS-06-20)**

All qualification activities related to safety-critical and fracture-critical items and safety-critical functions, as appropriate to the level of the review, shall be completed and the applicable reports approved, as required by the contract.

(f) **Flight Readiness Review/Flight Acceptance Review (see ESA PSS-06-20)**

Compliance verification for all defined hazard-control measures shall be completed and accepted. Verification of compliance with safety

requirements shall be completed. All safety-critical items and functions shall be qualified, and all safety-related nonconformances, failures, waivers, and accident/incident reports shall be formally accepted and closed, or documented on an open items list with any constraints identified. A Safety Data Package and a Safety Risk Assessment Report shall be presented for review and formal acceptance by ESA.

(g) **Launch Readiness Review**
(see ESA PSS-06-20)
All open work related to safety-critical items and functions shall be completed, or scheduled as part of normal pre-launch activities. All safety-related nonconformances, failures, waivers, and accident/incident reports shall be formally accepted and closed. All safety-related flight anomalies on previously flown designs or reflown hardware shall be resolved and closed. A current project Safety Risk Assessment Report shall be presented for review and formal acceptance by ESA, and the launch authority where appropriate.

(h) **Launch Commitment**
(Normally during the launch countdown)
A delta Safety Risk Assessment Report shall be presented, which documents the current risk situation, including any potential effects of countdown anomalies, weather, and hardware or personnel conditions. The report shall be subject to review and formal acceptance by ESA, and the launch authority where appropriate.

Safety Review Data Packages shall be prepared in accordance with ESA PSS-01-400 (Safety data package requirements) and the requirements of this paragraph.

I-7.11 DOCUMENTATION AND CHANGE REVIEW

The contractor shall review project documentation, including: specifications; drawings; analyses; procedures and reports; nonconformance reports; failure reports; waivers; and documentation changes; in order to verify, or assess impact on:

— the implementation of safety requirements and hazard controls;

— incorporation of hazard controls into the design, or the verification programme;

— completion of verification activities;

— the design and operational safety of the system;

— the validity of safety and risk analyses performed and documented.

Records shall be maintained of the documents reviewed. Safety documentation shall be updated where necessary to maintain currency.

Safety shall be represented at CCB's, MRB's, FRB's, TRB's, and at qualification and acceptance reviews where safety requirements and safety-critical functions and/or items are involved.

I – 7.12 SAFETY AUDITS

The Contractor shall perform safety audits of his own and subcontractor project activities to verify compliance with project safety policy and requirements, and to identify safety problem areas and errors which are not covered by specific safety requirements. ESA shall be informed of the audit schedule. Right of access shall be provided for participation by ESA in these audits, and for ESA safety audits of the contractor and his project-related activities.

CHAPTER I – 8: SAFETY DATA FILE

As part of the project documentation, the contractor shall maintain a safety documentation file. The file shall be kept current and shall include as a minimum:

— hazards analysis input data (e.g. design and operational data either by document reference and issue, or the document copy);

— hazard analyses and reports (PHA's, POHA's, SHA's, OHA's etc., as appropriate);

— supporting analyses (e.g. fault or event tree analyses, FMECA's, hazard checklists, software analyses, procedure analyses, contingency analyses, safety studies etc., which are performed in support of hazard identification and evaluation);

— design safety requirements file;

— hazard control documentation (analyses, qualification test procedures, drawings etc., either by document reference and issue, or the document copy);

— safety analyses (warning time analysis, caution and warning analysis etc.);

— safety review data packages (as appropriate to the project);

— risk assessment data;

— risk assessment reports;

— action tracking;

— minutes of meetings;

— safety review and safety audit results;

— safety-related nonconformances (including waivers) and failure documentation;

— document review tracking data;

— accident and incident data;

— safety requirements compliance data;

— safety problem data;

— safety lessons learned file.

ESA shall be given access to the data contained in the Safety Data File on request during audits, safety reviews and meetings held at the contractor's premises.

PAGE INTENTIONALLY LEFT BLANK

SECTION II

SYSTEM LEVEL TECHNICAL REQUIREMENTS

PAGE INTENTIONALLY LEFT BLANK

CHAPTER II – 1: GENERAL SYSTEM DESIGN REQUIREMENTS

The safety of human life shall be the overriding consideration during the design and operation ESA space systems and associated equipment, including facilities and ground support equipment.

II – 1.1 FAILURE-TOLERANT DESIGN

The acceptability of the following failure tolerance requirements is predicated on assurance that the system is designed, qualified, manufactured, and operated in accordance with the ESA product assurance requirements as defined in ESA PSS-01-0 (Product assurance and safety policy and basic requirements for ESA space systems) and its supporting specifications.

II – 1.1.1 Failure-tolerant design shall be applied whenever the potential for catastrophic or critical hazardous consequences exists as the result of the design or operation of ESA space systems and their associated equipment. The following requirements are applicable:

(a) NO SINGLE FAILURE SHALL HAVE A CATASTROPHIC OR CRITICAL HAZARDOUS CONSEQUENCE.

(b) NO SINGLE OPERATOR ERROR SHALL HAVE A CATASTROPHIC OR CRITICAL HAZARDOUS CONSEQUENCE.

(c) NO COMBINATION OF A SINGLE FAILURE AND A HUMAN OPERATIONAL ERROR SHALL HAVE A CATASTROPHIC HAZARDOUS CONSEQUENCE.

II – 1.1.2 The defined failure tolerance requirements apply during planned and contingency operations (including maintenance).

II – 1.1.3 Escape and rescue and extravehicular activity (EVA) shall not be applied as a means of complying with these basic failure tolerance requirements.

II – 1.1.4 Multiple failures that result from common-cause or common-mode failure mechanisms shall be considered as single failures for the purpose of determining fault tolerance.

II – 1.1.5 Failures shall be considered to originate within hardware, software, firmware or procedures as the result of design error or random failure, or to be caused by natural or induced environmental effects.

II – 1.1.6 Functions that are provided by carrier space systems in support of payloads shall be designed in accordance with the failure tolerance requirements applicable to the hazard severity of the failure effect of the service function, including the payload portion of that function. The failure tolerance shall be incorporated in the function on the carrier side of the functional interface with the payload.

II – 1.1.7 The failure tolerance requirements of Paragraph II – 1.1.1 do not apply to: primary structures; load-bearing structures; load-bearing structural fasteners; load-bearing paths within mechanisms; or pressure vessels. When structural failure can have catastrophic or critical hazardous consequences, these shall be designed in accordance with fracture-control principles as set out in ESA PSS-01-401 (ESA fracture-control requirements).

II – 1.2 SAFETY-CRITICAL FUNCTIONS AND ITEMS

II – 1.2.1 Safety-critical functions shall comply with the failure tolerance requirements of Paragraph II – 1.1, which are applicable to catastrophic hazardous consequences.

II – 1.2.2 The required failure tolerance for redundant software involved in safety-critical functions shall be implemented with the aid of alternate methods and algorithms (e.g. N-version programming), unless the software is capable of modification and validation within the time from the occurrence of the software failure to the hazardous consequence. Alternatively, independent hardware back-up to the software function may be provided.

II – 1.2.3 EEE parts used in safety-critical items in flight hardware shall meet testing level B in accordance with the requirements of ESA PSS-01-60 (Components selection, procurement and control for ESA space systems).

II – 1.3 FAILURE PROPAGATION

II – 1.3.1 Hardware or software failures shall not cause additional failures with hazardous effects, or propagate to cause the hazardous operation of interfacing hardware.

II – 1.3.2 Safety-critical functional paths (both hardware and software) shall be separated from non-safety-critical functional paths, in order to prevent failures within non-safety critical functions from propagating to safety-critical functions.

II – 1.3.3 Alternate or redundant safety-critical functional paths shall be separated or protected in such a way that any event that causes the loss of one functional path will not result in the loss of alternate back-up, or redundant functional paths.

II – 1.4 OPERATIONAL SAFETY

II – 1.4.1 Parametric operating ranges and performance limits for safe operation shall be established for the design and shall be specified.

II – 1.4.2 The design shall not require continuous active control by personnel to ensure that the established operating ranges and performance limits are not exceeded.

II – 1.4.3 Before operation, rules and contingency procedures shall be established for hazardous 'limit' conditions which may occur during ground and in-flight operations.

II – 1.4.4 The system design shall provide protection to avoid the erroneous acceptance of commands that may affect personnel safety or cause hardware or software damage. The failure tolerance requirements of Paragraph II – 1.1 are applicable.

II – 1.4.5 Labelling, colour codes, switch conventions, and the procedures and communications language shall be standardised.

II – 1.5 HUMAN ERROR

II – 1.5.1 Man/machine interfaces shall be designed, and the personnel tasks scoped, to minimise the potential for hazardous events resulting from human error.

II – 1.5.2 The human error failure tolerance requirements of Paragraph II – 1.1 apply to man/machine interfaces.

II – 1.6 DEBRIS, FALLOUT AND IMPACT REQUIREMENTS

II – 1.6.1 The failure tolerance requirements of Paragraph II – 1.1 apply to the prevention of debris, fallout and impact.

II – 1.6.2 Means shall be provided to prevent the hazardous descent of debris as the result of a launch vehicle launch abort, or the uncontrolled de-orbiting or orbital decay of spacecraft, or space system elements that are likely to survive re-entry.

II – 1.6.3 Normal or abort operations shall not result in such contamination of the atmosphere as to endanger human health, crops, natural resources or the environment.

II – 1.6.4 The creation of space debris in orbits that repeatedly intersect orbital paths used by space systems shall be avoided.

II – 1.6.5 Means shall be provided to prevent re-contact or impact of separated or jettisoned hardware due to cold thrusting, tumbling, attitude changes or inadvertent thruster operation.

II – 1.7 DETAILED TECHNICAL SAFETY REQUIREMENTS

The requirements of ESA PSS-01-402 (ESA design safety requirements) are applicable.

CHAPTER II – 2: MANNED SYSTEM SAFETY REQUIREMENTS

These requirements are applicable to ESA projects that concern, or are associated with, the development, manufacture, procurement or operation of: man-carrying space transportation systems, manned orbital systems or spacecraft, or orbital systems intended to operate or interface with either of the foregoing. These requirements are to be applied in addition to those defined in Paragraph II – 1.

II – 2.1 ESCAPE AND RESCUE

Crew escape and rescue capabilities shall be provided for all mission phases, including on-pad operations. Application of this requirement shall be in addition to that of the failure tolerance requirements of Paragraph II – 1.2. Functions that support crew escape and rescue shall be categorised as safety critical, and shall comply with the failure tolerance requirements of Paragraphs II – 1.1 and II – 1.2 for inadvertent operation. The reliability for successful operation of escape and rescue functions shall be defined and engineered into the design.

II – 2.2 CONTINGENCIES

Failures that result in failure tolerance degradation below that required by Paragraph II – 1.1.1 shall be cause for contingency action, which may include: system reconfiguration; function shut-down and unscheduled maintenance; operation or mission termination/abort or crew emergency escape, as appropriate.

II – 2.3 SAFE HAVEN

II – 2.3.1 The design shall provide safe-haven capabilities for the crew in case of uncontrollable emergency conditions which may arise during manned operations in orbit. These safe-haven capabilities shall sustain crew life until escape or rescue can be accomplished, or the situation is rectified.

II – 2.3.2 The design shall provide for rapid crew transfer to the designated safe haven when an immediately uncontrollable hazardous condition occurs.

II – 2.3.3 The design shall provide for the isolation of habitable volumes to protect the safe haven from the propagation of immediately uncontrollable and life-threatening situations.

II – 2.7.2 Means shall be provided for the maintenance of habitable conditions for the crew, and for the removal and disposal of crew metabolic waste products.

CHAPTER II – 3: LAUNCHER SYSTEMS

II – 3.1 LAUNCHER SAFETY REQUIREMENTS FOR UNMANNED MISSIONS

These requirements are to be applied in addition to those of Paragraph II – 1.

II – 3.1.1 Design safety requirements for unmanned missions

II – 3.1.1.1 Launch vehicle and spent stages shall be equipped with tracking aids to permit monitoring of trajectories and prediction of impact points.

II – 3.1.1.2 In the case of a deviation from the planned trajectory during ascent, launch vehicle stages shall be equipped with a remotely commandable engine shut-off and/or stage destruction capability, as appropriate, in order to prevent the descent of stages and/or stage debris outside predefined safety limits.

II – 3.1.1.3 Orbiting spent stages shall have the capability of being safely de-orbited.

II – 3.1.1.4 Launch vehicles shall be designed to be insensitive to lightning strike when on the launch pad and during atmospheric flight.

II – 3.1.2 Operational safety requirements for unmanned missions

II – 3.1.2.1 Hazards to the public, to public and private property and to the environment resulting from the operation or malfunction of launcher systems shall be precluded by constraints applied to nominal and abort trajectories, staging, and the descent of spent stages.

II – 3.1.2.2 In the case of a deviation from the planned launch trajectory during ascent, launch vehicle stages shall be remotely destroyed and/or have their propulsion engines shut off, as appropriate, to prevent stages and/or debris from falling outside predefined safety limits.

II – 3.1.2.3 The launch vehicle and spent stage trajectories shall be continuously monitored to determine vehicle, stage or debris impact points.

II – 3.1.2.4 Spent or aborted vehicle stages shall be recovered, or safely destroyed during descent prior to impact.

II – 3.1.2.5 Residual propellants contained in spent or aborted stages shall be safely dispersed.

PAGE INTENTIONALLY LEFT BLANK

CHAPTER II – 4: PAYLOAD SAFETY REQUIREMENTS

II – 4.1 PAYLOADS TO BE FLOWN ON MANNED ESA PAYLOAD CARRIERS

II – 4.1.1 Payloads shall be so designed that loss or degradation of resources supplied to the payload by the carrier shall not result in catastrophic or critical hazards.

II – 4.1.2 Payload structural interfaces with the carrier shall be designed in accordance with the fracture-control principles defined in ESA PSS-01-401 (ESA fracture-control requirements).

II – 4.1.3 Safety-critical payload functions the hazards of which are not controlled by the failure-tolerance provided in the carrier-to-payload services (see Para. II – 1.1.6) shall meet the applicable requirements of Paragraphs II – 1.1 (excluding Para. II – 1.1.6) and II – 1.2.

II – 4.1.4 Payloads shall be designed to comply with the requirements of Paragraphs II – 1.0, II – 1.3, II – 1.4, II – 1.5 and II – 1.6.

II – 4.1.5 Payloads shall be designed in accordance with the applicable requirements of ESA PSS-01-402 (ESA design safety requirements).

II – 4.2 PAYLOADS TO BE FLOWN ON THE NASA STS

II – 4.2.1 The technical requirements of NASA documents NHB 1700.7 (Safety policy and requirements for payloads using the Space Transportation System) and KHB 1700.7 (Space Transportation System payload ground safety handbook) are applicable to payloads and payload ground support equipment of the NASA STS.

II – 4.2.2 When fracture control is required by NHB 1700.7 to be implemented for payload design, ESA PSS-01-401 (ESA fracture-control requirements) shall be applicable.

II – 4.3 SPACELAB PAYLOADS

The requirements of Paragraph II – 4.2 and the safety-related requirements of SLP/2104 (Spacelab payloads accommodation handbook) are applicable.

PAGE INTENTIONALLY LEFT BLANK

CHAPTER II – 5: GROUND EQUIPMENT AND FACILITIES

II – 5.1 GROUND SUPPORT EQUIPMENT

II – 5.1.1 Ground support equipment when operated alone or in conjunction with flight hardware shall, as a minimum, meet the applicable failure tolerance requirements of Paragraph II – 1.1.

II – 5.1.2 Ground support equipment shall include design features to prevent hazardous events occurring as a result of facility failure or malfunction.

II – 5.1.3 Ground support equipment used during checkout and pre-launch operations of manned systems shall be equipped to interface with the flight-system emergency, warning and caution function and shall be capable of displaying and announcing the relevant signals, and of initiating appropriate safing commands.

II – 5.2 LAUNCH- AND MISSION-CONTROL FACILITIES FOR MANNED MISSIONS

II – 5.2.1 Launch-and mission-control functions that support manned-system safety-critical functions shall be categorised as safety critical and shall meet the applicable requirements of Paragraph II – 1.2.

II – 5.2.2 Launch- and mission-control safety-critical functions that have a high-availability requirement in order to protect crew safety shall be supported by sufficient redundancy to ensure that the availability requirement is met.

II – 5.2.3 A back-up launch-control centre shall be available and on standby during the launch and ascent phase until the point of control transfer to mission control.

II – 5.2.4 Safety-critical mission-control functions shall be backed up by redundant functions in separate facilities.

II – 5.2.5 Transfer of control of manned space-transportation systems from the launch-control centre to the mission-control centre shall be accomplished at a 'relatively stable' point in the mission.

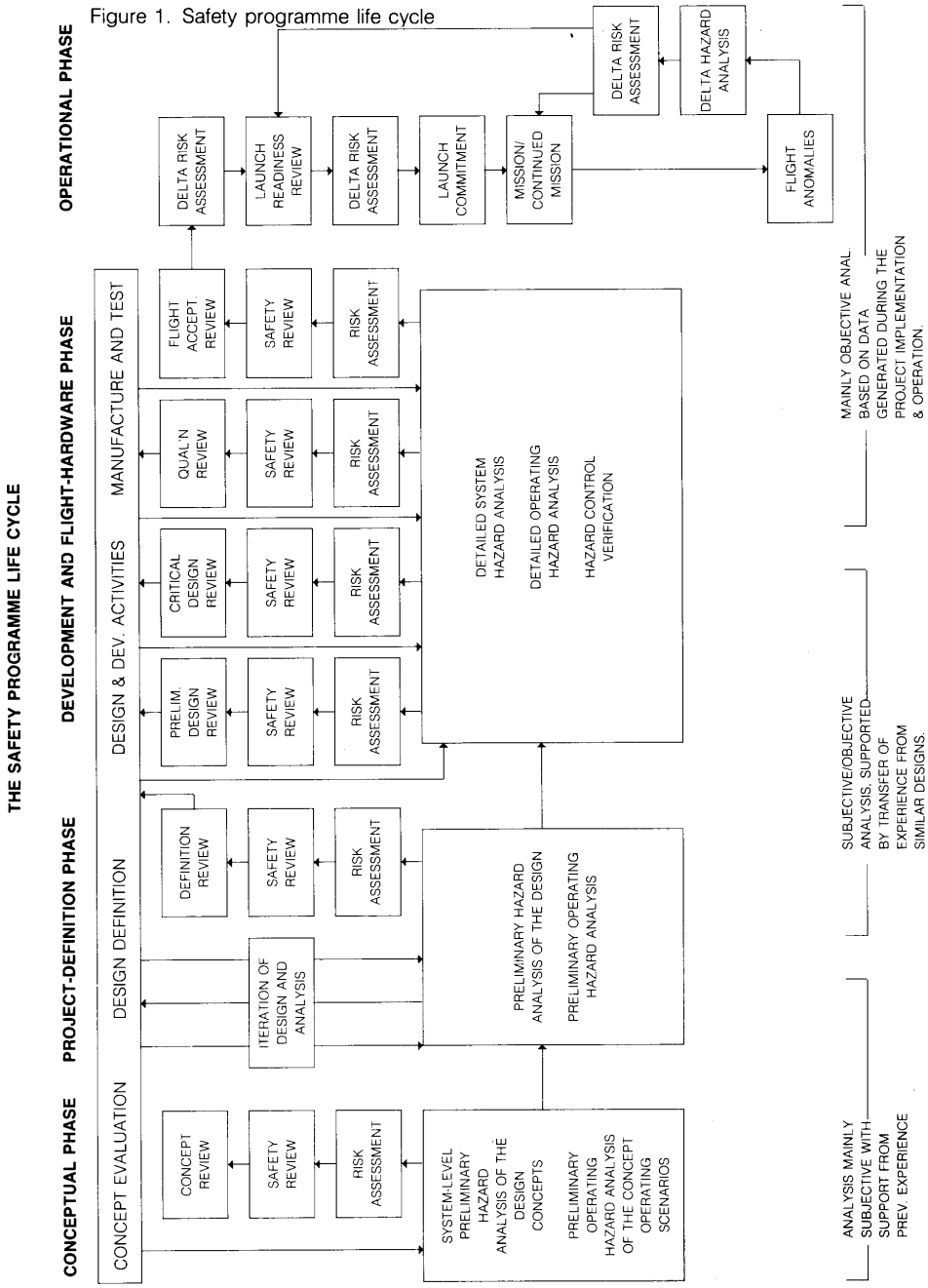
II – 5.2.6 Payload operations shall be controlled from a control centre that is separate from the mission-control centre.

II – 5.2.7 Commands and data that can have catastrophic or critical hazardous consequences shall be authorised and verified by the mission-control centre.

II – 5.2.8 Mission-control equipment shall be designed to accepted ergonomic principles, including consideration of operator stress-reduction factors, and lessons learned from operator experience.

II – 5.2.9 Mission control shall be supported by a mission-operations technical-support (MOTS) centre that provides real-time mission technical support such as: anomaly investigation, data evaluation, data searches, development of contingency-support and procedures etc.

Figure 1. Safety programme life cycle



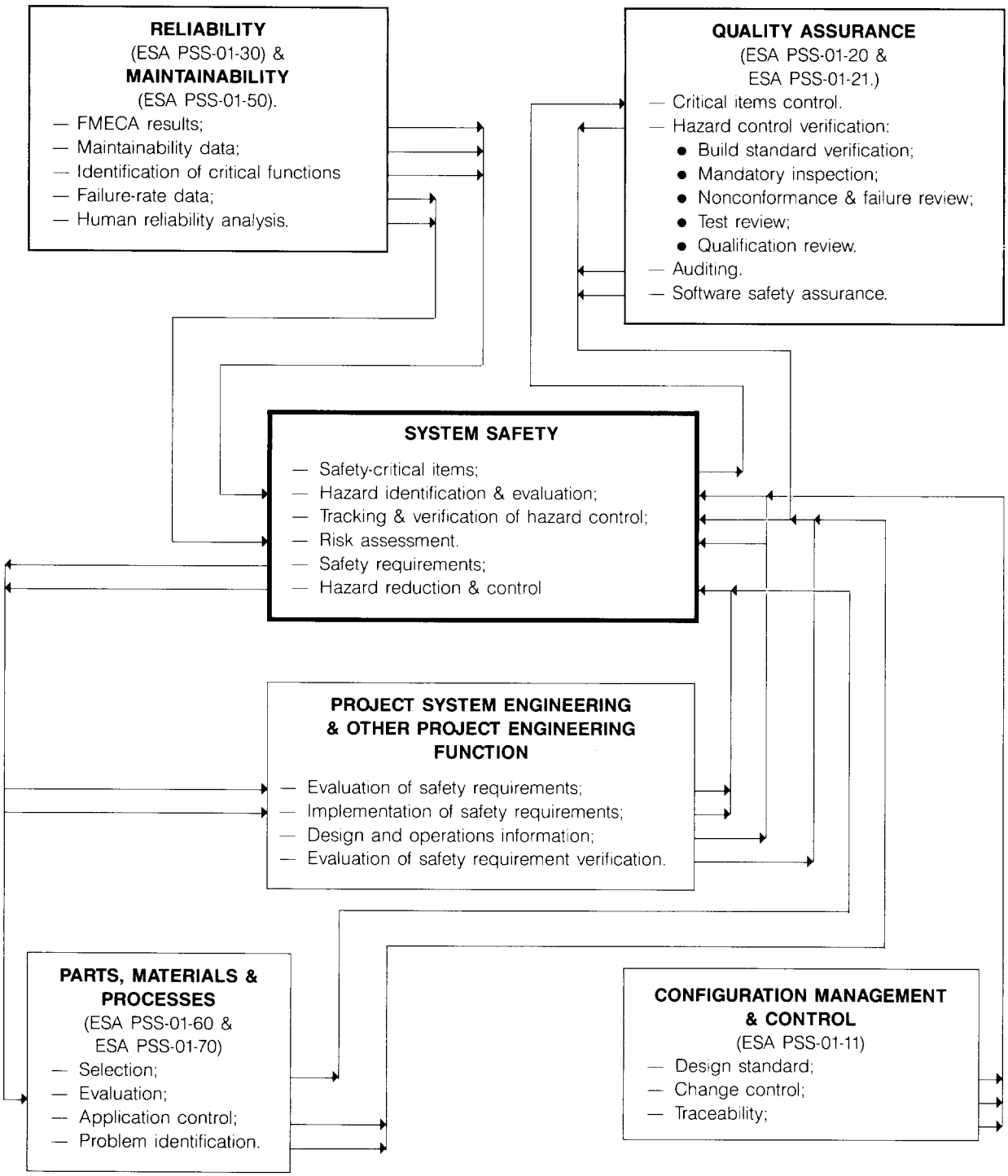


Figure 2. Implementation of product assurance integrated system safety

ANNEX 1
SAFETY PROGRAMME TASKS

1. CONCEPTUAL PHASE

(a) Commence preliminary hazard analyses of the design and operations concepts in order to identify applicable system-level hazards, hazardous conditions and potential hazardous events and consequences.

(b) Support concept trades by identifying safety-critical aspects of the concept options.

(c) Apply hazard elimination and minimisation and make safety recommendations.

(d) Perform comparative risk assessments of the concept options.

(e) Perform a system risk assessment.

(f) Identify system-level safety requirements.

(g) Plan safety activities for the project-definition phase.

(h) Support the concept review.

2. PROJECT DEFINITION PHASE

(a) Update preliminary hazard analysis (PHA) and preliminary operating hazard analysis (POHA) in support of design and mission concept definition activities, in order to optimise design and operational safety by the application of the risk-reduction precedence, and to identify initial project safety requirements.

(b) Identify safety-critical functions and applicable failure tolerance requirements.

(c) Identify, assess and make recommendations concerning candidate unresolved residual hazards.

(d) Update the system risk assessment.

(e) Prepare and issue the project safety requirements specification.

(f) Ensure that project requirement documentation and activities comply with project safety requirements.

(g) Support a concept-definition/safety-requirements review.

(h) Plan verification of safety-requirements implementation.

(i) Prepare the Safety Plan for the development and flight-hardware phase.

3. DEVELOPMENT AND FLIGHT-HARDWARE PHASE

(a) Perform system hazard analysis (SHA).

(b) Perform operating hazard analysis (OHA) of ground and flight operations.

(c) Update identification of safety-critical functions and failure-tolerance requirements and identify safety-critical items.

(d) Implement control programme for safety-critical items.

(e) Update the project technical-safety requirements to the extent necessary to incorporate the results of hazard analyses.

(f) Ensure that identified hazard-control verification activities (reviews, inspections, analyses, tests etc.) are covered by the project implementation and verification programme.

(g) Perform safety analyses as necessary to support hazard-control definition and verification.

(h) Perform progressive risk assessment in support of design optimisation and project reviews.

(i) Verify implementation of safety requirements.

(j) Verify and document implementation of hazard control.

(k) Perform project internal safety reviews and internal audits.

(l) Identify and monitor assembly, integration, testing and handling operations that are potentially hazardous to personnel and/or hardware.

(m) Review and approve hazardous and safety-critical operational procedures.

(n) Perform accident/incident reporting and investigation.

(o) Support customer safety reviews at major programme milestones.

(p) Prepare a project safety 'lessons learned' report.

(q) Prepare safety plan for operational phase.

4. OPERATIONAL PHASE

(a) Issue the safety plan for the operational phase.

(b) Review operational procedures.

(c) Approve safety-critical operational procedures.

(d) Identify and monitor hazardous operations.

(e) Support flight-readiness and launch-commitment reviews.

(f) Support ground and flight operations.

(g) Control safety-critical items.

(h) Monitor and assess evolution of the system configuration and operations resulting from design fixes and updates.

(i) Update hazard analyses and implement additional hazard controls as necessary.

(j) Investigate safety-related flight anomalies and trends.

(k) Perform continued progressive risk assessment.

PAGE INTENTIONALLY LEFT BLANK

ANNEX 2
DATA REQUIREMENTS FOR UNRESOLVED RESIDUAL HAZARDS

The following data shall be provided as a minimum:

— The title of the unresolved residual hazard.

— A unique reference number.

— The applicable hazardous consequence.

— The severity category of the hazardous consequence.

— A brief description of the potential hazardous event.

— Identification of the applicable operational or mission phases(s).

— Identification of what the hazardous event could affect (personnel, the system itself or other systems).

— Identification of the causes of the hazardous event.

— Reference to the identifying hazard-analysis entry or harzard-consequence report, as appropriate.

— The safety requirement(s) affected.

— The RFD/RFW number (if applicable).

— The resolution actions planned, under way or completed, as appropriate.

— The probability of occurrence or estimated occurrence rate prior to and after application of the planned resolution actions.

— The rationale for acceptance if no further action is proposed.

— Related warning times and caution and warning parameters and limits (where applicable).

— The status (i.e. initial identification; resolution action agreed; resolution action completed and submitted for deletion from the list, or for formal acceptance; and accepted by ESA), with space provided for signatures, and date.

PAGE INTENTIONALLY LEFT BLANK

ANNEX 3
SAFETY PROGRAMME
DELIVERABLE DOCUMENTS LIST

Document:	Section I Para. No:
Safety-programme plan	4.0
Project technical safety specification	6.0
Preliminary hazard-analysis report	7.1.1.3
Preliminary operating hazard-analysis report	7.1.1.4
System hazard-analysis report	7.1.1.5
Operating hazard-analysis report	7.1.1.6
Warning-time analysis report	7.1.2
Caution-and-warning analysis report	7.1.3
Hazard-status report	7.2 (see also 7.1.1.5 and 7.1.1.6)
Unresolved-residual-hazard list	7.3
List of safety-critical items	7.4
Safety-critical items: control plan (may be included in the integrated Project critical-item control plan)	7.4
Risk-assessment report	7.7
Accident/incident reporting: — Telex — Report — Analysis report	7.9
Safety-review data package	7.10

PAGE INTENTIONALLY LEFT BLANK

ANNEX 4
DEFINITIONS

ACCIDENT:

An unexpected event that, as a result of work on or with project hardware or software, results in human death or injury, or which causes loss of or damage to:
— project hardware, software or facilities that could affect the space-worthiness of the project flight hardware,
— public or private property,
or which has detrimental effects on the environment.

CARRIER:

The portion of a system that supports and provides services such as transportation, stabilisation, and supply of resources, to one or more payloads.

CAUSE:

When used in the context of hazard analysis, the action by which a hazardous event is initiated. The cause may be the result of system failure, human error, induced or natural environment, system configuration or operational mode(s).

COMMON CAUSE FAILURE:

The failure of more than one item (components, equipment etc.) as the result of an external influence (e.g. temperature, vibration etc.).

COMMON MODE FAILURE:

The failure of more than one identical item (components, equipment etc.) as the result of a failure-initiating condition that is a common characteristic of the items (e.g. a manufacturing error).

ESCAPE:

In the context of 'crew escape and rescue', to get safely away (from the consequences of a hazardous event) to a place of temporary or permanent safety without external assistance.

FUNCTION:

The mode of action by which the system fulfils one or more defined performance characteristics.

HAZARD:

A source of potential threat to safety (danger).

HAZARD ANALYSIS:

A systematic qualitative analysis of system design or operational characteristics that identifies and assesses:
— applicable hazards and potentially hazardous conditions,
— the associated possible hazardous events, and
— the severity of the consequences of those events.
Hazard analysis does not address hazardous-event occurrence rates.

HAZARD CONSEQUENCE:

The effect of one or more hazardous events.

HAZARDOUS CONDITION:

A system configuration or operational state with which are associated one or more hazards that may propagate to bring about a hazardous event.

HAZARDOUS EVENT:

An occurrence, with possible hazardous consequences, arising as the result of a hazardous condition.

HUMAN OPERATOR ERROR:

The failure of an operator to perform as required or trained (e.g. failure to follow a procedure or to respond correctly to an indication).

INCIDENT:

An unexpected event that could have resulted in an accident, but did not.

OPERATING HAZARD ANALYSIS:

A systematic analysis of the 'system' operations and operating procedures that is performed in the detailed design and operational stages of a project. The analysis is repeated as the design and operational detail evolves, paying particular attention to system operational modes and man-machine interfaces.

PAYLOAD:

The part of the system that is carried in order to achieve a productive purpose, and is unrelated to the functions of the carrier system.

PERMANENTLY DISABLING INJURY:

An injury that results in a permanent reduction in the quality of life of the person injured.

PRELIMINARY HAZARD ANALYSIS:

A broad initial study of the early design, in order to identify:
— apparent hazards,
— possible hazardous events and their consequences;
— feasibility of hazard elimination, minimisation and methods of control.
Preliminary hazard analysis is not a discrete technique, but the early application of selected techniques.

PRELIMINARY OPERATING HAZARD ANALYSIS:

A broad initial study of the early operational concept(s) and scenarios with the same objectives as **preliminary hazard analysis**.

PRESSURE VESSEL:

A container that stores pressurised fluids and:
(a) contains stored energy of 19 310 joules or greater, based on the adiabatic expansion of a perfect gas, or
(b) contains a gas or liquid that may result in a hazardous event if released, or
(c) will experience a design limit pressure greater than 0.69 MPa.

PROGRESSIVE RISK ASSESSMENT:

Risk assessment performed at various stages of the evolution of a project using a mixture of subjective and objective data. Initial assessment uses mainly subjective data (where objective data is not available), while subsequent assessment utilises higher proportions of relevant objective data as this becomes available (e.g. from testing).

RESCUE:

In the context of 'crew escape and rescue', to assist away (from the consequences of a hazardous event) to safety.

RESIDUAL HAZARD:

A hazard or hazardous condition with potentially catastrophic, critical, or marginal consequences that has not been eliminated from the system.

RISK:

A measure of the magnitude of the threat to safety.

SAFETY ANALYSIS:

Any analysis performed to assess or verify the safety of the design or operation of a system. Safety analyses include:
hazard analysis;
risk analysis;
warning-time analysis;
caution-and-warning analysis;
fault-tree analysis;
event-tree analysis;
common-cause analysis;
etc.

SAFETY-CRITICAL CHARACTERISTIC:

The vital performance characteristic(s) of a **safety-critical item** the failure of which could cause a hazardous event with catastrophic consequences, irrespective of the redundancy designed into the safety-critical functional path.

SAFETY-CRITICAL FUNCTION:

A function that, if lost or degraded, or that, through inadvertent operation, could cause a hazardous event with catastrophic consequences.

SAFETY-CRITICAL ITEM:

Hardware, software, firmware, man/machine interface, or procedure that forms an operating part of the safety-critical functional path through the system.

SEVERITY:

A measure of the possible consequence of the propagation of a hazardous condition to a hazardous event.

SYSTEM:

A related set of operational elements, subsystems, equipment, components, firmware, software, operating procedures and personnel that function in an interactive manner to achieve a defined purpose.

SYSTEM HAZARD ANALYSIS:

A systematic analysis of a 'system' that is carried out in the detailed design stages of a project and is repeated as the design evolves, paying particular attention to internal and external interfaces, failures and operational modes that can result in hazardous events. System hazard analysis is not a discrete technique, but the structured application of selected systematic analysis techniques.

VALIDATION TESTING:

Testing performed to confirm specified functional capabilities within the specified operating limits.