General

SYSTEM SAFETY STANDARD

Rev.C : August 20, 2018

Japan Aerospace Exploration Agency

This is an English translation of JMR-001C and does not constitute itself.
Whenever this document conflicts with the original document in Japanese, the original document takes precedence.

Disclaimer

The information contained herein is for general informational purposes only. JAXA makes no warranty, express or implied, including as to the accuracy, usefulness or timeliness of any information herein. JAXA will not be liable for any losses relating to the use of the information.

Published by
Japan Aerospace Exploration Agency
Safety and Mission Assurance Department
2-1-1 Sengen Tsukuba-shi,Ibaraki 305-8505, Japan

- Contents -

1. GENERAL

1.1 Purpose

This standard provides requirements for implementing a system safety program for the JAXA's development and contract projects (JAXA responsible divisions) in Japan Aerospace Exploration Agency (JAXA) and the contractors. The word "the contractors" herein also includes system integrator, consignee customer, and cooperate developer. The JAXA projects and the contractors should identify, eliminate, mitigate and control the hazards of the system to protect human life, properties, and environments from mishaps by the system safety program throughout the system life cycle; e.g. research, design, production, test, launch operation, support and disposal. The word "the system" herein also includes a system, subsystems and components.

1.2 Scope

1.2.1 Applicability

The JAXA responsible divisions and the contractors shall apply this standard to all JAXA's development and consignment system except when the necessary safety throughout the development is insured by the only observance of the law and safety regulations of JAXA. The JAXA responsible divisions and the contractor should establish the system safety program plan at the beginning of the project and, the all system safety efforts should be reviewed by the safety review panel based on this standard.

1.2.2 Responsibility

The JAXA responsible divisions and the contractors shall be responsible for both the observance of the safety law and regulations, and taking actions required to ensure the safety associated with project in accordance with the requirements of this standard.

1.2.3 Tailoring

(1) Tailoring of system safety management requirements

System safety management requirements can be applied by correcting them in accordance with the features and characteristics of the applicable systems. The JAXA responsible divisions shall discuss corrections and the reason for corrections in accordance with the levels of system safety review defined in operation plans, with safety department to which the JAXA responsible divisions belongs (Safety and Mission Assurance Department, in the case of a division without a safety department) and Safety and Mission Assurance Department (all referred to as "Safety Divisions"), shall incorporate the corrections in the system safety program plan, and shall need to receive approval in the safety review of JAXA.

(2) Tailoring of Safety Requirements

The safety requirements applied in the system safety program plan (safety design requirements, operational safety requirements, and space debris requirements) may be

applicable by correcting them in accordance with the features and characteristics of the applicable systems. The JAXA responsible division shall consult with the JAXA safety divisions about corrections and the reason for corrections, indicate how to make adjustments in the format of Table 1.2.3-1 or equivalent format, and attach the format to a system safety program plan to receive approval in the safety review of JAXA.

2. RELATED DOCUMENTS

2.1 Applicable Documents

The following documents shall be applied to the development paragraphs to the extent that they are referred to in this standard. The latest edition of the applicable documents shall be used. If applying that edition is difficult, the Safety and Mission Assurance Department shall be consulted.

(1) NPR8715.3 NASA Procedual Requirements NASA General Program Requirements Chapter 2, System Safety
(2) MIL-STD-882 Department of Defense Standard Practice for System Safety
(3) JMR-002 Launch Vehicle Payload Safety Standard
(4) JMR-003 Space Debris Mitigation Standard
(5) JERG-1-007 Launch Site and Flight Safety Engineering Standard
(6) JERG-1-006 Safety Engineering Standard for Development of Rocket Systems

3. DEFINITION OF TERMS

The terms used in this standard are defined in Appendix I.

4. SYSTEM SAFETY REQUIREMENTS

4.1 Basic Requirements

The JAXA responsible divisions and the contractors, as specified in a procurement specification or other relevant document, shall develop and implement a safety program to ensure system safety throughout the design, manufacture, test and operation phases of the system, etc.

This standard sets forth the following basic requirements for system safety:

(1) A system safety management organization that effectively implements the system safety program shall be established (4.2.3).
(2) Hazard of systems including subsystems and components shall be identified and managed throughout their entire life cycle to minimize risks, and it shall be verified that the risks are within the allowable levels at each phase of development (4.3.2).
(3) Safety requirements for hazard control shall be established, and the cause(s) of each hazard shall be identified to execute appropriate measures to control each cause (4.3.1).
(4) A safety design shall be verified by test or other appropriate means (4.3.3).
(5) It shall be ensured that operation procedures and other relevant documents incorporate appropriate safety procedures and that each task is conducted in strict accordance with these procedures (4.2.4).

(6) The results of system safety program activities shall be documented (4.4).

(7) Safety data shall be maintained and managed (4.4).

(8) An effective system safety program plan to implement system safety shall be prepared based on the above activities and their results (4.2.1). Also, milestones for the system safety program shall be established based on the milestones for the entire project; to define hazard analysis, safety reviews, establishing safety requirements and management standards/procedures, report timing, audit, submitting documents, and developing education/training plan, as required, which are key activities of the system safety program.

4.2 System Safety Program Management

4.2.1 System safety program plan

The JAXA responsible divisions and the contractors, as specified in the procurement specification, shall prepare a “system safety program plan” that satisfies the requirements of this standard. The system safety program plan shall be reviewed by the Safety Division, if it is drafted by the JAXA responsible divisions or by the JAXA responsible divisions if it is drafted by the contractors. The safety review of the system safety program plan drafted by the JAXA responsible divisions shall be conducted according to an applicable regulation of JAXA. System safety program plan shall be updated at all times.

(1) The organization of the system safety program plan shall comply with Table 4.2.1-1 and shall undergo a safety review.

(2) The system safety program plan prepared by the contractors may be based on NPG8715.3, MIL-STD-882 or equivalent standard, provided that it incorporates applicable requirements defined in this standard.

Table 1.2.3-1(1/2) Tailoring application about safety requirements Format (1)

<table>
<tr><td colspan="2">1. Title</td><td>Number
Year, Month, Date</td><td colspan="2">Responsible organization names of systems</td></tr>
<tr><td colspan="2" rowspan="2">2. (1) Applicable system names

(2) Subsystem names</td><td>Person in charge of implementation</td><td>Person in charge of system safety program*</td><td>Prepared by</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td colspan="5">3. Applicable document names, document numbers, and paragraph numbers of the safety requirements applicable to tailoring</td></tr>
<tr><td colspan="5">4. Tailoring descriptions and safety requirement descriptions of applicable documents, and comparison of measures
4.1 Comparison of safety requirements (comparison among cases with or without tailoring)

4.2 Comparison of safety measure (hazard control) descriptions based on safety requirements (comparison among cases with or without tailoring)

(If the space in this column is insufficient, provide additional descriptions on the next pages.)</td></tr>
<tr><td colspan="5">5. Reason why tailoring is required

(If the space in this column is insufficient, provide additional descriptions on the next pages.)</td></tr>
<tr><td colspan="5">6. Description of reasons why comparable safety is secured

(If the space in this column is insufficient, provide additional descriptions on the next pages.)</td></tr>
<tr><td colspan="2" rowspan="2">Decision: Approval Approval with comments Reconsideration (Selection)
Reasons and comments:</td><td>JAXA/Safety Div.</td><td colspan="2">JAXA responsible division</td></tr>
<tr><td></td><td>Person in charge division</td><td>Person in charge of system safety program*</td></tr>
<tr><td colspan="2"></td><td>Year, Month, Date</td><td>Year, Month, Date</td><td>Year, Month, Date</td></tr>
</table>

Note: This document makes up a part of the System safety program plan, and descriptions are reviewed in the safety review of the system safety program plan. Make adjustment and verification with JAXA and the Safety Div. in advance with regard to descriptions.

*: System safety program manager: System safety program manager

Table 1.2.3-1(2/2)　Tailoring application about safety requirements　Format (2)

1. Title (continued)	Number
2. (1) Applicable system names　(2) Subsystem names	

Table 4.2.1-1 System safety program plan Contents standard

Item	Remarks	Application Item
1. General 1.1 Purpose		
1.2 Scope	The contractors shall add the following paragraph to the plan. 1.3 Relationship with other contructual requrements 1.4 Responsibility of the contractors 1.5 Responsibilities of JAXA	
2. Applicable documents Indicating applicable documents and references		
3. General description 3.1 Organization and Structure (1) Clearly define the project manager, the system safety program manager, persons in charge, and related divisions. (2) Illustrate the system safety management organization including related divisions. (3) If contract development items are included, portions to be executed by the contractors will be distinguished from those to be executed by the JAXA responsible divisions	In the case of the plan prepared by JAXA, related divisions mean “the JAXA responsible division and the Safety Division” as defined in this standard. If a direct contract with a supplier is involved, system safety program management should cover the contract.	4.2.3
3.2 System safety review method		4.2.4
3.3 System safety activities in each phase of development (1) Specify hazard analysis, safety requirements, system safety reviews, and other activities for each phase of development. (2) Illustrate schedule for each of the above activities in the system safety program milestone.		Table 4.2.4-1 Figure 4.2.2-1
3.4 Hazard classification		4.3.2.1
3.5 Risk assessment		4.3.2.2
3.6 Hazard analysis		4.3.2.3
3.7 Safety Requirements (1) Applicable Documents (including application of chapter 5 of JMR-002, chapter 4 of JERG-1-007, chapter 5 of JMR-003, and JERG-1-006 if a system is applicable) (2) Non-applicable items related to the applicable documents, tailored items (*) subject to prior coordination, etc. (3) Additional requirements resulting from hazard analysis Applicable Japanese laws and regulations required for administrative procedures		4.2.2 and others
3.8 Safety verification		4.3.3
3.9 Education/Training		4.2.6
3.10 Audit		4.2.7
3.11 Reporting		4.2.8
3.12 Mishap investigation and reporting		4.2.9
4. Documentation and Safety Data		4.4

*: If tailoring paragraphs exist, indicate descriptions in the format of Table 1.2.3-1.

4.2.2 System safety program activities

The JAXA projects and the contractors shall conduct system safety program activities throughout the life cycle in an effective manner to ensure safety related to the systems and to minimize and keep risks within an allowable level throughout the design, manufacture, test, and operation phases.

Fig.4.2.2-1 shows the required system safety program activities for the development item's life cycle. The system safety program activities performed in each phase are described below.

The System safety program activities shall begin in the early stages of the phase of conceptual designs and plan decisions.

(1) Phase of conceptual designs and plan decisions (phase 0)

a. A system safety program plan throughout design, manufacturing, test, and operation phases shall be prepared.

b. Phase 0 hazard analysis shall be conducted in order to identify hazards as system including subsystems and components and to consider measures. On the basis of this consideration, safety requirements shall be specified in addition to chapter 5 of JMR-002, chapter 4 of JERG-1-007, chapter 5 of JMR-003, and JERG-1-006 (include tailored descriptions, if any). (Note: As "hazard identification" is performed throughout all phases, prepare the hazard identification table defined in 4.3.2.4 and Table 4.3.2.4-1 in the early phase of the design process and update it as the design matures.

c. Construct a safety requirement compliance matrix and check that the design, manufacture, test, and operation plans for the systems comply with the safety requirements. Table 4.2.2-1 shows the safety requirement compliance matrix form.

d. The results of the Phase 0 hazard analysis shall be documented and these results shall be incorporated into the conceptual study/definition design.

(2) Preliminary design phase (Phase I)

a. The results of the Phase 0 hazard analysis shall be reviewed in the early stage of this phase and detailed safety requirements shall be established as required.

b. The Phase Ⅰ hazard analysis shall be performed in order to identify system hazards and examine their influence and control measures. Then the detailed safety requirements shall be reviewed and the safety requirement compliance matrix shall be modified based on the results of this analysis.

c. The results of the Phase Ⅰ hazard analysis shall be documented and incorporated into the preliminary design.

d. The system safety program plan shall be maintained/ updated as required.

(3) Critical design phase (Phase II)

a. The Phase II hazard analysis shall be conducted to review Phase I hazard analysis result along with progress in design and perform detailed safety assessment. Also design compliance with the basic and detailed safety requirements shall be verified.

b. The results of the Phase II hazard analysis shall be documented and incorporated into the critical design.

c. Safety-related verification tests shall be conducted using hardware and/or software, as well

as operation concepts, the detailed safety requirements shall be reviewed, and the safety requirement compliance matrix shall be updated, as required.

d. The system safety program plan shall be maintain/revised as required.

e. Safety requirements compliance is confirmed in the design review. If specifications that are not compliant with safety requirements are found, the design shall be revised to ensure compliance. If compliance cannot be attained, a detailed review of safety requirements compliance shall be prepared to clearly state that existing risks are at an allowable level. The JAXA responsible division shall discuss details with the JAXA safety review organization, and contractors shall discuss with the divisions of the responsible safety divisions and shall need to receive approval in the safety review of JAXA.

(4) Manufacturing and verification phase (Phase III)

a. The results of the Phase II hazard analysis shall be reviewed as required.

b. Process specifications and other relevant documents relating to manufacturing, verification and launch site operations shall be prepared, and maintained/revised.

c. It shall be ensured that hazardous manufacturing, verification and launch site operation processes are performed according to the applicable documents.

d. Any newly identified hazard shall be investigated and analyzed, if any, in coordination with the reliability and quality program, and corrective actions shall be taken.

e. The Phase III hazard analysis shall be conducted to clarify the results of verification of hazard controls. The operation procedures shall be prepared based on the results of analysis and the compatibility between the operation procedures and the detailed safety requirements shall be confirmed. The operation procedures shall include the following:

(i) Requirements for safety equipment and devices, and maintenance procedures required detecting malfunctions

(ii) Warnings, cautions, special operation procedures, and emergency measures during the system operation and maintenance

(iii) Handling, storage, transportation and maintenance procedures

f. It shall be confirmed that all safety verifications have been completed. Safety verification results that can be verified only on site shall be described in the safety verification tracking log (Table 4.2.4-2 or equivalent format), be followed, and be closed before operation.

g. The System safety program plan shall be maintained/ revised as required.

(5) Operation phase

a. Phase III hazard analysis results shall be reviewed and operational procedures, and such like of launch sites shall be reviewed as required.

b. It shall be confirmed that all activities are conducted according to the system safety program plan and the operation procedures

c. If new hazards are identified, an investigation and study shall be made in cooperation with the reliability and quality program and the required corrective actions shall be taken.

d. In the case of a design change, safety requirements associated with the design change shall be incorporated.

4.2.3 System safety management organization

The System safety management organization shall be operated under the following conditions:

(1) The head of the JAXA responsible division and the contractors shall establish each system safety management organization responsible for planning and implementing its own system safety program by clearly defining the respective roles, responsibility, authority, tasks, and reporting structure. The system safety management organization can take independence into consideration and be set up in accordance with factors such as details and scales of systems.

(2) The head of the JAXA responsible division and the contractors shall appoint each system safety program manager who is responsible for system safety management throughout the design, manufacture, test, and operation of the systems. A system safety program manager of each system shall have sufficient knowledge and experience in system safety and its management.

(3) The system safety program manager has the following authority and responsibility:

a. Establish or prepare the system safety program plan in accordance with the authority of the system safety program manager.
b. Establish management procedures required for implementing the system safety program.
c. Conduct a review, from a safety perspective, of specifications, procedures and other documents.
d. Promote hazard analyses and safety reviews.
e. Resolve major safety issues through coordination with related divisions.
f. Make reports and recommendations relating to the implementation of the system safety program, directly to the project manager or other person responsible for development.
g. Stop and prevent the execution of a project activity or the establishment or revision of a document that deviates from safety requirements or procedures.
h. Stop and correct any safety critical operations that deviate from the established procedures.

Date of implementation (Western calendar) / Phase of development / System safety program activities		Conceptual design and plan decision (Phase 0)	Preliminary Design (Phase I)	Critical Design (Phase II)	Manufacture/verification (Phase III)	Operation	Remarks
Overall Milestones	JAXA responsible divisions and contractors	System requirement review(SRR) ▽ System definition review(SDR) ▽	Preliminary design review (PDR) ▽	Critical design review (CDR) ▽	Post-qualification review or pre-shipment review (PQR or PSR) ▽		
	JAXA Review	Project shift review ▽ System definition review ▽			Development completed Review ▽	Final confirmation Review ▽	
System safety program plan		Preparation ▽	Maintenance /Revision ▽	Maintenance /Revision ▽	Maintenance /Revision ▽	Maintenance /Revision ▽	
Safety review		Phase 0 Safety Review ▽	Phase I Safety Review ▽	Phase II Safety Review ▽	Phase III Safety Review ▽	Safety review after phase III ▽ (as required)	
Hazard analysis		Phase 0 Hazard Analysis	Follow-up Review				
			Phase I Hazard Analysis				
				Phase II Hazard Analysis	Follow-up Review (as required) Phase III hazard analysis	Follow-up Review	
Safety Requirements		Initial settings of safety requirements ▽ Safety requirement settings ▽	Reviewing detailed requirements as required ▽ ▽				
Operation Procedures, etc.					Preparation (Manufacture and verification procedure	ocedures,	

Figure 4.2.2-1 System safety program activities in life cycle

Table 4.2.2-1 Safety Requirements compliance matrix

(Document name of safety requirements, document number with revision sign)		Compliance	Noncompliance	N/A	Program	
Paragraph	Requirement Description				Results	Remarks

4.2.4 Safety review

Safety reviews are conducted, regarding the systems, to confirm safety requirements established according to each hazard identified and its compliance with requirements, and identify hazard and its cause, evaluate the control method, control verification method, and validity of verification results. For any residual risks, evaluate details of minimization and its acceptability.
JAXA shall perform safety reviews according to an applicable regulation of JAXA and the contractors shall perform safety reviews according to the following:

(1) The system safety program manager or a designated representative shall conduct safety review to determine that the system safety is implemented properly for the systems, thus achieving the safety objective.
(2) Safety reviews shall be conducted four times, namely the Phase 0 safety review, the PhaseI safety review, the Phase II safety review, and the Phase III safety review. Some or all of these reviews may be performed collectively if the system size or other rationale permits, and each safety review may be included in the milestone reviews, subject to JAXA approval.
(3) A safety review manual shall be established to perform safety reviews.
(4) All safety review material, the minutes, action item list, and support data shall be compiled as a safety data package, snd submitted to the project immediately after completion of each safety review. JAXA responsible divisions may participate in the safety review as an observer.
Table 4.2.4-1 shows a general outline of the safety reviews, including their implementation schedules, primary purposes, review documents, and major system safety program activities to be conducted in each development phase.

4.2.5 Detailed review on compliance with safety requirements

If an item that does not conform with the safety requirements compliance matrix (Table 4.2.2-1) prepared by the system safety program activities (4.2.2) is identified, the review details about the reason for non-compliance, alternative measures, and the basis for guaranteeing the safety requirements shall be indicated in the safety requirements compliance detailed review (use the format in Table 4.2.5-1), and after consultation with the JAXA safety division, a deviation or waiver approval shall need to be received in the safety review of JAXA. The review shall be incorporated in the hazard report also.

Table 4.2.4-1 Outline of system safety activities in safety review and each development phase.

Safety review	Review Timing	Primary Purpose of Safety Review	Review document (Note 2)	Major system safety activities in each development phase
Phase 0 Safety review (Note 1)	Conceptual Study/ Definition Design	Verification of hazard and hazard causes (Refer to Table 4.3.2.3-1 Hazard analysis table) Verification of Applicable Safety Requirements	Description documents about systems and subsystems, configurations and operations Review documents of hazard identification and measures about system Safety Requirements (including additional requirements by tailoring and hazard analysis, if any)	As phase 0 hazard analysis Identifying hazards, causes of hazards, and Discussion on measures (Refer to Table 4.3.2.3-1 Hazard analysis table) Initial settings of safety requirements and safety requirements settings
Phase I Safety review	At Preliminary Design Review (At PDR)	Verifying hazards and hazard causes Verifying hazard controls To confrim verification methods Confirming safety requirements described in detail as required	Description documents about systems and subsystems, configurations and operations With regard to systems and subsystems important for safety and operations, description document containing features of safety design, schematic for identifying independence such as inhibition and block diagram. Trade-off study implemented for summarizing hazard report and special study result documents Hazard report, supplementary documents and FTA Detailed safety requirements	Reviewing phase 0 hazard analysis results and setting detailed safety requirements as required. As phase I hazard analysis Hazard classification Identifying hazard causes Discussion on hazard controls Discussion on safety verification methods (general outline) Review on safety requirements is made detailed on the basis of the analysis results above
Phase II Safety review	At critical design review(CDR) (At CDR)	Verifying that hazard control is implemented in the design Confirming that a verification methods is established in detail	Description documents about systems and subsystems, configurations and operations Document describing safety critical systems/subsystems and their operation, including schematic and block diagrams with safety features, independent inhibits, and controls identified Hazard report, supplementary documents and FTA Detailed safety requirements Phase I Treating condition document of safety review action item	Phase I Review of hazard analysis results As Phase II hazard analysis Incorporating hazard controls in critical design To discuss the safety verification methods in detail. Safety verification test on hardware and software as required Operational proposal and review of detailed safety requirements To confirm that safety verification is incorporated in process specifications and test procedures.
Phase III Safety review	During JAXA's development completion review	To confirm that safety verification has been completed To confirm that all action items are closed	Description documents about systems and subsystems, configurations and operations Description document clarifying systems and subsystems important for safety and final configuration of operations Including safety features of systems of completed manufacturing, and schematic and block diagrams with safety features, independent inhibits, and controls identified Hazard report, supplementary documents and FTA Safety verification data such as analysis, inspection, test, and demonstration (Drawings, analysis document, test report, and manufacture records, etc.) Detailed review on compliance with safety requirements Safety verification tracking log (Note 3) Phase II Treating condition document of safety review action item	Compliance evaluation and verification of manufacturing and test results against hazard verification Verification that safety verification is incorporated in operational procedures and such like related to operations Confirmation of deviation/waiver handling

Note 1: As the Phase 0 safety review, an informal safety review conducted in a normal working group meeting form is acceptable; however, it shall need to undergo a safety review of JAXA.

Note 2: Details of reviewed documents shall be determined with reference to this table, by prior consultation with the JAXA responsible division at contractors, and by prior consultation with the safety division in the JAXA responsible division.

Documents to be reviewed shall be prepared and maintained on the basis of the latest configuration in the current phase.

Note 3: Open descriptions of safety verification for the Phase III hazard report shall be recorded in a Safety verification tracking log in format of Table 4.2.4-2 or equivalent format.

Table 4.2.4-2 Safety verification tracking log format

System names:_____ Preparation and revision date:_____

Log No.	Hazard report number	Safety Verification No.	Verification item and method of closure	Constraints on Launch site operation	Completion Scheduled date	Completion date	Verification confirmation results	Remarks (Procedure number /Title)
1								
2								
3								
4								

Table 4.2.5-1 Detailed review on compliance with safety requirementsFormat

<table>
<tr><td colspan="2">Paragraph name of study on compliance details</td><td colspan="2">Number</td><td>Date</td></tr>
<tr><td colspan="2" rowspan="2">System names</td><td colspan="3">Names of JAXA responsible divisions and contractors</td></tr>
<tr><td>Development manager</td><td>System safety program manager</td><td>Preparation</td></tr>
<tr><td>Action:
(Circle applicable one)</td><td>• Deviation (Compliance)
• Waiver</td><td colspan="3"></td></tr>
<tr><td colspan="5">Applicable Safety Requirements</td></tr>
<tr><td colspan="5">Description Non-Compliance</td></tr>
<tr><td colspan="5">Reason for Non-Compliance

(If the space in this column is insufficient, provide additional descriptions in the appendix, etc.)</td></tr>
<tr><td colspan="5">Measure against hazard applicable to safety requirements (Number of applicable hazard report:)

(If the space in this column is insufficient, provide additional descriptions in the appendix, etc.)</td></tr>
<tr><td colspan="2" rowspan="2">Decision</td><td>Project manager/person in charge of implementation,</td><td>System safety program manager</td><td></td></tr>
<tr><td colspan="3">JAXA/Safety Div.</td></tr>
</table>

Remarks: A contractor shall submit documents to the JAXA responsible division, and the JAXA responsible division shall submit documents to the safety division.
Attach supplemental documents and data.

4.2.6 Education/Training

For a task or operation conducted by an engineer, technician, operator, or other personnel, which may result in loss of human life/injury or damage to the systems, appropriate education/training shall be conducted prior to the start of the task or operation.

Such education/training shall be conducted according to the education/training plan and shall meet the following requirements:

(1) Clearly identify the equipment, operation and support tasks that require training.
(2) Clearly define the need for any qualification.
(3) The education/training plan shall cover the following areas:
    a. Hazard identification and classification, hazard causes, consequences, preventive measures, and controls
    b. Procedures, checklists, and contingency procedures
    c. Functions and operations of safety devices, protective devices, monitoring equipments, and warning devices
    d. Preventive measures for human errors
(4) An up-to-date records of education/training participant names and the result of education/training shall be maintained.

4.2.7 Audit

The actual progress of the system safety program shall be audited according to an audit plan.

The audit shall be conducted for suppliers who request application of the system safety program and shall meet the following requirements:

(1) Audits shall be conducted with the use of manuals or other documents.
(2) Audits shall be conducted by a team which includes persons who are familiar with the system safety program.
(3) Audits shall include document reviews, manufacturing and operation area safety assessments, and any other related safety items to validate the system safety program.
(4) Audits shall be conducted on a regular basis. Additionally, spot/unscheduled audits shall be conducted randomly to verify safety conditions.
(5) Audit reports, including findings and recommendations, shall be prepared and submitted to the system safety program manager.
    Then correction of the issue or non-conformance shall be confirmed and reported to the system safety program manager.
(6) Audit reports shall be maintained as system safety program documentation.

4.2.8 Reporting

When any circumstance change that affects system safety occurs, a report shall be prepared and submitted to the Safety Division (in the case of the JAXA responsible divisions) and to the JAXA responsible divisions (in the case of the contractors).

The report shall contain the following:

Problems

(1) Problems and corrective actions relating to the system safety issue.
(2) Explanation of decisions and corrective actions that affected the system safety program activity and their expected impacts on the system safety of the development item.
(3) The expected delay in the schedule of the system safety program and its impacts

4.2.9 Mishap investigation and reporting

Contactors and the JAXA responsible divisions must take the following actions:

(1) Contractors shall immediately report to the JAXA responsible division, about any injury or death of a personnel and damage to property, accidents having an unusual effect on environments inside and outside the JAXA site, and accidents that affect third parties.
A report about an accident shall be described in the latest format at the point of submission, and the report shall be submitted to JAXA within 5 operating days.
If a detailed report is required, the report shall be submitted within 30 days after the day of the accident.
If a potentially serious error, which may have caused such an accident as above, occurred then the conditions and causes of the error shall be investigated and verified. After considering preventive measures, the JAXA responsible division shall report it to the JAXA safety division or a contractor shall report it to the JAXA responsible division in the latest format.

(2) With regard to an accident whose safety is critical, which occurred before carrying items into the JAXA site, if a similar process exists in the JAXA site, causes and conditions of the accident shall be investigated and verified, and reported to JAXA.
If a potentially serious error, which may have caused such an accident as above occurred then the conditions and causes of the error shall be investigated and verified. After considering preventive measures, it shall be reported to the JAXA responsible division.

4.3 System Safety Engineering

4.3.1 Safety design principle

Safety design of systems shall be primarily based on fault tolerance design.
When the verification data to make an appropriate design on the basis of section 4.3.1.4 can be indicated, design for minimum risk may be used.
If neither of the above two design approaches can be used, a probabilistic risk assessment shall be used, provided that sufficient coordination with the Responsible Division is made. However, if this method is used, a contractor shall have adequate consultation with the JAXA responsible division, and the JAXA responsible division shall have adequate consultation with the safety management review organization.

4.3.1.1 Safety design precedence

Safety Design Precedence shall be as follows:

(2) Design to eliminate hazard.
(3) Design to minimize hazard.
(4) Design to control hazard (in a narrow sense).
(5) Use of safety devices.
(6) Use of protective devices.
(7) Use of warning devices (should be related to an emergency disposition).
(8) Application of hazard control method relying on special procedures and/or training.

(Note: In all items other than 4.3.1, this standard generally defines all items (3) through (7) above as hazard control.)

4.3.1.2 Fault tolerance design

The following fault tolerance design requirements shall be satisfied to control hazards, and reduce the likelihood of their occurrence to an allowable level in accordance with the hazard level.

(1) Double failures, a combination of one failure and one human error, and double human errors shall not cause a catastrophic failure.
(2) One failure or one human error shall not cause a severe accident.

4.3.1.3 Retarding functions leading to accident (Retarding hazardous function)

Functions that may lead to an accident shall satisfy the following requirements to prevent the functions from operating on an unwanted occasion due to a failure or a human error, and to reduce the likelihood of occurrence to within an allowable level.

(1) For functions that could potentially cause a catastrophic accident, at least three independent inhibiting measures shall be provided between the functions and energy source. It is desirable that the ground-return circuit of the function should be controlled with one of the above inhibiting actions.
Monitoring at least two of the three required inhibiting functions shall be made possible.
(2) For functions that could potentially cause a severe accident, at least two independent inhibiting measures shall be provided between the functions and energy source.

4.3.1.4 Design for minimum risk

Design for minimum risk can be applied if the verification data to make a design on the basis of a design standard specified by JAXA can be indicated. Design shall be managed by considering sufficient design margins, safety factors, and appropriate selection of material and EEE parts.
"Design for Minimum Risk" is usually applied to the following.

- Structures
- Pressure vessels
- Pressurized piping and joints
- Pyrotechnic devices
- Material compatibility
- Material flammability
- Some mechanisms

If structural destruction may cause a catastrophic or severe accident, a fracture control standard shall be specified for structures, pressure vessels, fasteners, and load-supporting materials.

4.3.1.5 Preventing failure propagation

The design shall not allow a primary failure or functionality loss (including those caused by human error) in equipment and functions to induce other failures or increase the likelihood of an accident.

4.3.1.6 Safety maintaining function

(1) The functions shall be fail-safe and foolproof.
(2) Multiple control functions against individual hazards shall be mutually independent.
(3) Safety shall be maintained against interruption of power supply for the period until a safety measure is taken.

4.3.1.7 Special procedures

If hazard control is insufficient by design, or by installation of a safety device, protection device or warning device, a system shall be designed to allow the likelihood of a hazard occurring to be reduced by operation.
In addition, hazard control shall be provided by education and training of personnels, specifying appropriate procedures, and providing the required maintenance.

4.3.2 Hazard analysis

Hazard analysis is a technique used to identify and assess, systematically and logically, all hazards relating to systems and its operation throughout the life cycle.
Hazard analysis shall be performed in consideration of worst case environmental conditions that are encountered during the life cycle of the systems. Lessons learned from past experience on similar projects shall be incorporated into hazard analysis.
The steps taken in hazard analysis are shown in Fig.4.3.2-1.

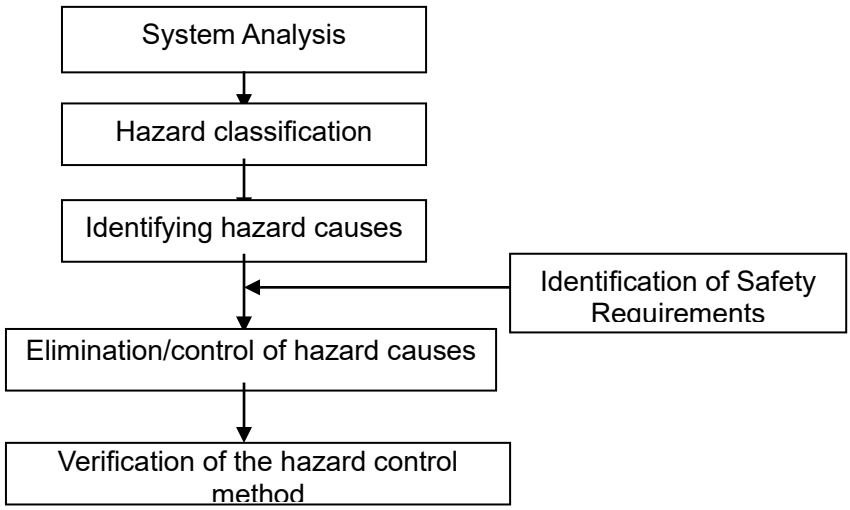


Figure 4.3.2-1 Analysis steps of Hazard analysis.

(1) System Analysis
In assessing the system's safety, it is important to understand the system, operation, mission, environmental conditions, interfaces with other systems, and other relevant factors.
(2) Hazard classification
Based on the "system analysis" conducted in (1) above, hazards shall be identified in terms of energy source, environment, operation and other factors, and their descriptions, occurrence phase, hazard severity, and likelihood of occurrence shall be clearly defined.
Hazard severity shall be defined pursuant to 4.3.2.1 (1) and the likelihood of occurrence pursuant to 4.3.2.1(2).
(3) Identifying hazard causes
For each hazard identified in (2) above, its cause(s) shall be determined in consideration of

hardware and software used, operation, human errors, interface, and environmental conditions.
In the process, the FTA (Fault Tree Analysis) method shall be used and the results shall be crosschecked with those obtained from the FMEA (Failure Modes and Effects Analysis).

(4) Identification of Safety Requirements
Applicable safety requirements shall be identified to control hazard causes. If applicable safety requirements cannot cover the hazard, a new safety requirement shall be specified.

(5) Elimination/control of hazard causes
Elimination and control of hazard causes shall be performed according to the safety design priority specified in 4.3.1.1.

(6) Verification of the hazard control method
Effectiveness of a method for controlling each hazard cause, as developed in (5) above, shall be reviewed in the safety verification process described in 4.3.3.

4.3.2.1 Hazard classification

On the basis of the following hazard identification, hazard reports shall be prepared according to 4.3.2.4 for ones of hazard levels I and II, and ones of hazard levels III with a likelihood of occurrence A, B, or C applicable.
For hazards outside the range of preparing a hazard report, the basis for identifying that they are outside the scope of preparing a hazard report shall be clearly defined with the hazard analysis table (see Table 4.3.2.3-1, etc.)

(1) Hazard level
Hazard severity is indicated by four levels (I through IV) shown in Table 4.3.2.1-1 and is used to provide the determination criteria for the expected worst case scenario due to human error, adverse environmental conditions, inadequate design, procedural deficiencies, and failure or malfunctioning of systems, subsystems, and/or components.

Table 4.3.2.1-1 Hazard level

Hazard level	Term	Description
I	Catastrophic	Death or severe personal damage Irreversible significant environmental impact Loss of or severe damage to public or third party property Loss of system or launch site facilities
II	Critical	Major personal damage Reversible significant environmental impact Major damage to public or third party property Severe damage to system or launch site facilities
III	Marginal	Minor personal damage Reversible moderate environmental impact Minor damage to public or third party property Major damage to systems
IV	Negligible	Any conditions that causes less damages than Hazard level I to III.

(2) Likelihood of occurrence
The likelihood that a hazard occurs during the life cycle of systems can be indicated in the number of occurrences per unit operating hours, the number of operations, the number of personnel involved, or the number of tasks. In addition, the likelihood of occurrence may be indicated in qualitative terms.Table 4.3.2.1-2 illustrates the classification of the likelihood of occurrence, which may be derived from the analysis of safety data measured from past similar systems.

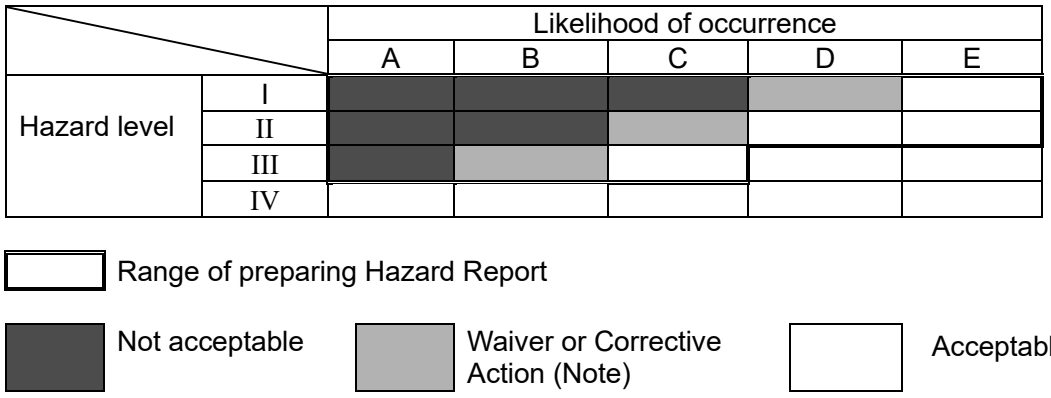
Table 4.3.2.1-2 Likelihood of occurrence

Likelihood of occurrence	Description
A	Frequent / Likely to occur immediately
B	Probable / Probably will occur in time
C	Occasional / May occur in time
D	Remote / Unlikely to occur
E	Improbable / Improbable to occur

4.3.2.2 Risk assessment

The JAXA responsible divisions and/or the contractors shall assess residual risks relating to the systems, which are indicated in the expected severity and the likelihood of occurrence.

Acceptable risk criteria shall be indicated in Fig. 4.3.2.2-1 as a standard.
The JAXA responsible divisions or the contractors may propose its own criteria that are equivalent to the above upon consultation and agreement with the JAXA Safety Division.
It is not only requested that residual risks be within the acceptable risk criteria, but also it is requested that every effort shall be made to minimize the risks under constraint on budget, schedule and so forth.



Note: (1) In the case requiring a decision about acceptance, making the greatest possible efforts made to reduce risks may make the case acceptable.
(2) The likelihood of occurrence shall be evaluated after controlling the hazard.
(3) For hazards with hazard levels I and II, hazard reports shall be prepared in principle even if it becomes out of the scope of the above Preparing Hazard Report after control.

Figure 4.3.2.2-1 Risk allowance evaluation standard

4.3.2.3 Phased hazard analysis

The JAXA responsible divisions and/or the contractors shall conduct hazard analysis in the initial development phase, identify hazards, and establish safety requirements, and then incorporate the results in the design, procedures, operations, and other related activities.
The results of hazard analysis shall be compiled as part of a safety data package and be used as safety review materials specified in 4.2.4. Hazard analysis shall be performed during each phase of development. The content of the hazard analysis to be performed in each phase is defined below.
Hazard analysis shall be reviewed when a design change is made.

(1) Phase 0 hazard analysis
Phase 0 hazard analysis is performed in the conceptual study/definition design phase. The purpose of this analysis is to identyfy system-related hazards and examine control measures in order to prepare a hazard analysis table (refer to Table 4.3.3-1) and establish safety requirements.

The hazard report shall:
a. Specify hazardous portion and location during system operation.
b. Identify a hazardous substance in materials or piece parts that are planned to use.
c. Clearly define hazards that are conceivable to occur in the course of test, transportation, handling, operation, and other relevant activities.
d. Clearly define safety issues relating to interfaces.
e. Estimate the severity of a mishap associated with each hazard.

(2) Phase I hazard analysis
Phase I hazard analysis is performed in the preliminary design phase. The purpose of this analysis is to identify hazards, clarify the impacts and control measures and establish detailed safety requirements in further detail based on the hazards identified in Phase 0 hazard analysis. A hazard report shall be prepared for all hazards that are classified at such a level defined in 4.3.2.1. The hazard report shall:
a. Identify hazard causes and establish appropriate hazard elimination and control measures.
b. Perform hazard analysis relating to system or subsystem interfaces and trade-off studies to optimize conditions between safety and design improvements.
Hazards of subsystems and components shall be considered in hazards analysis, and a hazard report of a system shall be prepared.
c. For high-risk hazards perform FTA (Fault Tree Analysis), and SCA (Sneak Circuit Analysis) and ETA (Event Tree Analysis) as required.
d. Crosscheck the results of hazard analysis with those of the FMEA to ensure complete coverage.
e. Incorporate necessary corrective measures into the design, while considering all safety related design constraints.
f. Clearly define improvements and corrections relating to safety in order to implement them by appropriate methods.

(3) Phase II Hazard analysis
Phase II hazard analysis is performed in the critical design phase. The Phase II hazard analysis shall include a detailed safety assessment by reviewing the results of Phase Ⅰ hazard analysis. The Phase II hazard analysis shall:
a. Ensure that the recommended hazard elimination and control measures are clearly defined and incorporated into the design.
b. Review the results of FTA, SCA, and ETA as required.
c. Select appropriate methods of reducing the frequency of mishap occurrence relating to safety critical parts and materials.
d. Document safety critical technology, design, manufacture, test, operation and other activities and the extent of their influence and incorporate them into maintenance and improvement of safety..
e. Clearly define the verification method.

(4) Phase III Hazard analysis
Phase III hazard analysis is performed in the manufacturing and testing phase. The Phase III hazard analysis shall include a detailed safety assessment by reviewing the results of Phase II hazard analysis. The Phase III hazard analysis shall:
a. Clearly define and document the recommended hazard elimination and control measures relating to system operation.
b. Select appropriate methods of reducing the frequency of occurrence of hazards relating to safety critical operating procedures.
c. Document safety critical system operations and the extent of their influence, and incorporate them into maintenance and improvement of safety.
d. Assess the results of hazard control verification activities.

4.3.2.4 Hazard report

The JAXA responsible divisions and/or the contractors shall document the results of hazard analysis in accordance with the following and submit them timely. A hazard report shall be prepared for all hazards that are classified at such a level defined in 4.3.2.1.

(1) Identify all hazards relating to the systems and list them in the hazard identification summary table using the form shown in Table 4.3.2.4-1 or equivalent.
The hazard report shall be made using the form shown in Table 4.3.2.4-2 or equivalent and shall specify the classification of each hazard, its cause, control measures, and verification methods, accompanied by supporting data as required.

(2) Ensure that the results of hazard analysis performed in (1) above are consistent with the results of FTA, safety requirement compliance detailed review, and other required analyses that have been performed separately.

(3) The hazard report shall be signed by the system safety program manager according to each phase and shall be submitted by a contractor to the JAXA responsible division, or by the JAXA responsible division to the JAXA Safety Division, for confirmation as a safety review document.

(4) The hazard report shall be complete when the hazard is eliminated by a design change or its control method is verified, and it is confirmed that the acceptable risk criteria are satisfied and safety verification is completed.

4.3.3 Safety verification

Safety verification means the process of verifying systems, both hardware and software, satisfies all safety design requirements with the objective evidence(s). This verification is performed by means of test, inspection, analysis, demonstration, and any combination thereof.

When safety verification is conducted according to procedures or processes, it shall be documented as process specifications. When analysis, test and/or inspection is performed, the results shall be compiled into a report. In either case, the document number shall be referred to the applicable hazard report. In the case of similarity analysis, previous verification procedures and requirements referred to shall be studied to verify adequate similarity.

If safety verification items are not closed by the end of Phase III, they shall be recorded in a safety verification tracking log pursuant to the form in Table 4.2.4-2 or equivalent for tracking, which shall be closed and submitted timely.

All data relating to safety verification shall be available at all times.

If the system is found to have a defect after safety verification has been completed and the results have been reported, corrective measures including a follow-up action shall be taken as a process after verification.

4.4 Documentation and Safety Data

Documents to be developed for compliance with this standard are listed in Appendix II.

The JAXA responsible divisions shall consult with the Safety Division with regard to documentation and related actions.

All data relating to documentation and safety verification shall be recorded and be made available at all times.

All the documents shall be kept at all times to show the updated version to the system safety program manager and shall be provided as feedback information for related divisions so as to prevent the recurrence of a defect of repetitive feature and confirm that detailed safety requirements have been satisfied.

The safety documentation shall also be stored and kept accessible for future reference.

Table 4.3.2.3-1　Hazard analysis table　Format example

No.	Hazard title	Hazard outline	Hazard causes	Actions	Hazard level	Likelihood of occurrence	Remarks（HR No）
1							
2							
3							
4							

Note: For hazard on which hazard reports were prepared, describe the hazard report no. (HR No.) also. Likelihood of occurrence is required for Phase I and later only.
Describe hazard outlines and controls for the basis of description, so that hazard level and likelihood of occurrence are understood.
If a hazard level is reduced, make a description in the actions column.

-24-

Table 4.3.2.4-1 Hazard identification summary table Format

System _____

Subsystem _____

Hazard Category / Hazard Type / System, subsystem, component or hazardous item / Or work process name	Extreme temperature		Fire	Explosion/Rupture				Structural Failure		Vibration/Impact/Collision			Corrosion/Contamination			Leak			Electromagnetic interference	Electrical shock/Discharge			Radiation			Noise	Suffocation /Gas poisoning	Fall/Dropping object																
	High temperature/Heating elements	Low temperature/Extremely low temperature	Existence of ignition source Combustible material and oxidizing agent	Pressure systems/ Pressure vessels	Explosives (Solid propellant/pyrotechnics)	Liquid propellant	Explosive atmosphere	Excessive load/Insufficient strength/Fatigue	Hydrogen embrittlement/Stress corrosion	Vibration source/Acoustic noise/Pressure wave	Rotator/Movable mechanism		Biological contamination/Contamination	Corrosive substance/Galvanic corrosion/Dissimilar metals	Fluid compatibility	Loose fittings/Plumbing damage	Deterioration of seals/Permanent sets in seal seats, Malfunctioning of valve		Shield deficiency	Short circuit	Electrostatic	Electrical shock	Ionizing radiation/Radio active substance	Laser, IR, UV, strobe	Radio wave	Continuous noise/Shock wave	Oxygen deficiency/Toxic gas	High-place work/unstable position	Dropped parts or tools	Dropping a hoisted item													
Hazard report No.																																										

Caution: Classify hazard in consideration of the possibility that the following items may cause an accident:
- Human factor
- Software error (input error or bug)
- Natural disaster (earthquake, tsunami, lightning, typhoon, heavy rain, strong wind, etc.)
- Hazardous operation (dangerous object, harmful substance, high-pressure gas, explosive material handling, heavy lifting task)
- Power failure, power recovery

Hazard level

I Catastrophic: Death or severe personal damage,Irreversible significant environmental impact, Loss of or severe damage to public or third party property, Loss of system or launch site facilities
II Critical: Major personal damage, Reversible significant environmental impact, Major damage to public or third party property, Severe damage to system or launch site facilities
III Marginal: Minor personal damage, Reversible moderate environmental impact, Minor damage to public or third party property, Major damage to systems
IV Negligible: Any conditions that causes less damages than Hazard level I to III.

(Note) Add required hazards to blank columns in accordance with system characteristics.

Table 4.3.2.4-2(1/2) Hazard report Format (1)

Hazard report	Hazard Report No.	
System	Date	Prepared /revised by
Subsystem	Phase	
Hazard title		
Applicable Safety Requirements	Hazard classification Hazard level ☐ I ☐ II ☐ III ☐IV Likelihood of occurrence: ☐A ☐B ☐C ☐D ☐E	
Hazard outline		
Hazard causes		
Hazard Controls		
Safety Verification Method		
Status of Verification		

Approval	Contractors	JAXA responsible division	JAXA/Safety Div.
Phase I			
Phase II			
Phase III			

A contractor shall submit to the JAXA responsible division, and the JAXA responsible division shall submit to the safety division.

Table 4.3.2.4-2(2/2) Hazard report Format (2)

Hazard report (continued)	Hazard Report No.
System/Subsystem	

5. Appendix I Definition of terms

[A]

Audit : An action to confirm the effectiveness of system safety program activities of the contractors itself or its supplier.

[C]

CDR (Critical Design Review):
A review conducted when critical design is mostly completed and prior to manufacturing of a prototype model (PM), to confirm that the results of critical design review satisfy the requirements in the contract document or specifications and manufacturing of PM may be commenced, by evaluating manufacturing drawings, specifications, and test results of engineering models (EM).

Component : An assembly of parts, devices and/or structures, which independently performs function during integrated operations of devices (e.g., attitude control device and power distribution device).

Conceptual study : A design phase to establish system concept in the early stage of development.

Configuration : Functional and physical characteristics of a system or component.

[D]

Design for minimum risk:
A design approach that enhances the reliability by applying the concept of safety factor or design margin.

Design review : An organizational activity to evaluate design quality and process of manufacturing, testing, installation, use, and maintenance planned in the product design stage on the basis of the collected objective knowledge in consideration of cost and delivery and to propose improvements, and to confirm that the design phase is ready to be advanced to the subsequent phase. Basically, there are three types of design reviews in compliance with the progress of design; preliminary design review (PDR), critical design review (CDR), and post-qualification test review (PQR).

Development : A development, in a broad sense, performed by JAXA, including the researches and maintenance of systems.

Development manager:
A person responsible for execution of the JAXA projects by collectively managing system specifications, reliability, safety, and content, schedule and cost of development in accordance with the purpose and implementation policy.

Deviation : To verify that conditions of non-conformance to safety requirements satisfies the underlying purpose of the safety requirements, and to approve the conditions as being compliant with the safety requirements.

[E]

ETA (Event Tree Analysis):
An inductive analysis technique to evaluate system failure or disaster by tracing it from an initiating event (e.g. valve rupture, pipe crack or operational error) to an intermediate event, through the functional and operational sequences, to prevent the occurrence of the outcome (e.g., stoppage or rupture of a propulsion system) at each step of the sequences.

[F]

Fail-safe : A design philosophy to retain safety, even if subsystem or component fails or loses its function when trouble occurs.

Fault tolerance design:

A design that prevents an accident caused by a fault or a human error. This is the basic safety requirement used to control hazards.
At hazard level I, the design prevents an accident caused by double failures or double human errors, or by a combination of one failure and one human error.
At hazard level II, the design prevents an accident under one failure or one human error.

Fool-proof : A design philosophy that retains safety, even if human error occurs.

Fracture control : To perform analysis of propagation of crack that may lead to a catastrophic defect and implement preventive measures.
The standard of fracture control involves the application of engineering, quality assurance, manufacturing, and operation engineering.

FTA (Fault Tree Analysis):
An analysis technique to predict qualitative or quantitative failure or identify a cause for a failure by dividing a critical phenomenon of a system or a subsystem into logical elements, eventually to an observable basic element (cause for failure).

[H]

Hazard : The presence of an existing or potential risk situation that may result in a mishap.

Hazard analysis : A technique to assess hazards, systematically and logically, in the applicable systems (including support equipment) and relating to the operation throughout the life cycle.

Hazard causes : Causes of hazard occurrence that make a hazard lead to an incident (e.g. insufficient strength of container that causes leak of thrust agent, malfunction of valves, poor sealing, over pressurization)

Hazard control : In a narrow sense, to reduce the likelihood of occurrence for hazard by using approaches of fault tolerance design or design for minimum risk.
In a broad sense, to add to the above, safety devices, protective devices, warning devices, and techniques using special procedures are included.
In this standard, the broad definition is used except for 4.3.1.

Hazard measures : Measures to eliminate hazard causes, to restrain occurrence of hazard causes, and to restrain damage caused by occurrence of hazard causes (hazard control).

Hazard outline : Outline of hazard including source, mechanism, and outcome that indicates a hazard level.

Hazard report : The document, which contains technical information about the specific hazard obtained throughout the execution of hazard analysis, and which is provided for designer, system safety person, and project person to assess the residual risk(s), followed by getting the development manager’s approval.

Hazard title : A hazard title that implies details of hazard (source, mechanism, and outcome) and allows discrimination from other hazards.

[I]

Incident : Contingent occurrence or a condition that can cause injury, death or illness of personnel, damage to the system, related equipment, or properties, or adverse environmental impacts.

Incident and others : Incident of a failure that affects safety. Permanent event, without any incident or failure, that leads to job-related illness or harmful effect to environment.

Inhibit : A design feature that provides a physical interruption between an energy source operating a function leading to an accident and an operating device, restraining the operating device with a function leading to an accident from operating at an unnecessary time.
For example, a relay or transistor between a battery and a pyrotechnic initiator, a latch valve between a propellant tank and a thruster, etc.

[J]

JAXA responsible division:
(For this standard only) Division conducting research and development or outsourcing work related to systems in JAXA.

[L]

Life cycle : All phases during the existence of system including design, manufacture, test, operation, and disposition.

[M]

Major personal damage:
A non-disabling personal damage with or without lost workdays

Personal damage with lost work days:
Work-related injuries or illnesses, which requires the worker to be away from work from the next day of receiving the damage.

Personal damage without lost work days:
Work-related injuries or illnesses, which do not require the worker to be away from work, after receiving treatment from medical facilities (including the clinic in the office). This also applies to the case where the worker was away from work for a less than a day.

Milestone : An important event scheduled in the project's life cycle or a systems safety program which is used as a control point to measure the progress or effectiveness of the project.

Minor personal damage:
Minor injuries resulting in for the worker to return to work immediately after receiving treatment.

[N]

Non-conformance : An anomalous state of a product where one or more characteristic(s) does not comply with the requirements. It includes failure, deviation, defect, shortage, and malfunction.

[O]

Overall Milestone review:
A review held at each milestone of a program or project, including preliminary design review (PDR), critical design review (CDR), post qualification test review (PQR), and pre-shipment review (PSR).

[P]

PDR (Preliminary Design Review):
A review held prior to the start of the detailed design when the basic design is nearly complete, which confirms that the achievement of preliminary design enables the product to satisfy system specification or development specifications and the preliminary design may be preceded to the detailed design.

Person in charge of system safety:
A person who conducts system safety program activities under the system safety

program manager within a system safety management organization.

PQR (Post Qualification Test Review):
A design review held after the qualification test using PM (prototype model), which has been manufactured in accordance with the applicable manufacturing drawings, specifications, and manufacturing processes. The purpose of this design review is to confirm that PM meets requirements of the development by evaluating the results of qualification test.

Preliminary design : System design to establish development specifications.

Probabilistic risk assessment:
Also called quantitative risk assessment, in other words, a method to express severity and likelihood of occurrence of damage that constitute a risk by using numeric value to indicate the safety level quantitatively on the basis of a model, that is an assessment method to grasp a significant factor rationally.

Projects : Project of JAXA that researches, develops or contracts systems, and organization that corresponds to the project. (Except for projects managed by the Space Basic System Head Office Launch Safety Assessment Office, and Manned system Safety and Mission Assurance Office)

Protective device : A physical barriers that are designed to protect personnel and equipment from a mishap that has been identified as hazard (e.g., casings for rotation objects such as motor, cover guards).

PSR (Pre-Shipment Review):
A review to confirm that systems are ready for delivery to the launch site. To review the results of the acceptance test, quality record, and the status of the corrective activities for non-conformance

[R]

Regulation by law : Industrial safety stipulated by industrial safety-related legislation and labor safety and hygiene legislation applicable in manufacturing sites or handling areas.

Risk : An expression of the probability of a hazardous state occurring. It is a function of the possible frequency of occurrence of mishap and the potential severity of the resulting consequence.

[S]

Safety : The state that hazard is eliminated, minimized, or controlled not to result in a mishap. In other word, the stage that the risk is as lower as acceptable.

Safety critical : A hazard severity identified as I or II. For example, being used as “safety critical operation procedures” or “safety critical parts”.

Safety data package : Documents to verify compliance to safety requirements for: hazard identification summary table, hazard analysis table, hazard report, safety verification data, safety verification tracking log, safety requirements compliance matrix, safety requirements compliance detailed review, and failure data of safety critical function.

Safety device : A device or a system designed to prevent failure or inadvertent operation of the device from causing a mishap.

Safety Division : (For this standard only) The Safety management review organization of head office managing the JAXA responsible division
This refers to the Safety and Mission Assurance Department in a head office without any safety management review organization.

Safety review : This reviews that the systems are compliant with safety requirements in addition

to hazards being classified without omission, evaluates and verifies that control and verification of hazard cause described in hazard report in each development phase, and evaluates and verifies that remaining risks of hazards are at tolerable levels.

Safety verification tracking log:
A document used to appropriately judge and manage the status of completion steps for an unverified item instead of safety verification in a hazard report.

SCA (Sneak Circuit Analysis):
An analytical technique to evaluate hardware and software systems, designed to identify a potential circuit or a state that prevents a required function from being performed or causes a unwanted function to be performed.
SCA are sneak path analysis, digital sneak circuit analysis, and software sneak path analysis, and a suitable analytical technique shall be chosen for the system.

Service : Electricity, water, gas and other utilities that are supplied to a development item

Severe personal damage:
A personal damage that:
- leads to permanent disability to work
- requires long-term treatment
- is disabling injury or illness

Subsystem : An assembly of components that take a major role in a system's function.

Supplier : An individual, a company or an office that conducts a transaction directly with a contractors and supplies a product and/or a service to the contractors under the contract with JAXA. The supplier includes a different division or an affiliate company.

System : A group of personnel, hardware and software, which are organized to perform a specific function.

Systems : (For this standard only) Systems, subsystems and components researched and developed or contracted by JAXA.
In general, a system is the first unit of a division for project activities.

System safety : The application of engineering and management principles, criteria, and techniques to rationally minimize a risk including potential mishaps as much as possible, by optimizing safety with the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle from project planning, production, operation and execution to disposal.

System safety program activity:
A management activity to develop and implement plans and procedures for systematically promoting and conducting activities to ensure system safety.

[T]

Tailoring : An action of modifying requirements in consideration of various conditions of development items to make this standard adaptable.

The contractors : An individual or a company that is in a contractual relationship with JAXA, including contractors counterpart who is engaged in a joint development with JAXA.

Trade-off : To select the most suitable plan from many plans by weighing cost, performance, and other factors.

[V]

Verification : To confirm that both hardware and software meet all design requirements

(including performances and safety requirements) by test, inspection, analysis, demonstration, and any combination thereof.

[W]

Waiver : To consider whether or not to accept the nonconforming status of safety requirements and accept the status only for the device in question.

Warning devices : A device that detects a specific hazardous condition or similar condition timely and generates an appropriate warning signal to caution personnel.

6. Appendix II Prepared documents list

Document title	Item No. referred
System safety program plan	4.2.1(2) and Table 4.2.1-1
Safety data package	4.2.4(4) and Table 4.2.4-1
Hazard identification summary table*	4.3.2.4 and Table 4.3.2.4-1
FTA, RTA, SCA, etc.*	4.3.2.3(2)
Hazard analysis table*	4.3.2.3, Table 4.3.2.3-1
Hazard report*	4.3.2.4, Table 4.3.2.4-2
Safety Requirements compliance matrix	4.2.2, Table 4.2.2-1
Safety verification tracking log (when required)	4.2.2(4), Table 4.2.4-2
Safety requirements compliance detailed review (as required)	4.2.5, Table 4.2.5-1
Safety review manual	4.2.4(3)
Education/Training plan	4.2.6
Record for execution of education/training and participants for training	4.2.6
Audit plan	4.2.7
Audit report	4.2.7
Report on a specific problem/issue	4.2.8
Mishap report/ “hiyari hatto (narrow escape)” report (when required)	4.2.9

Note*: Update always to use as safety design tools from the initial phase of design. Compose the part of safety data package using the latest data at each safety review phase.