General

LAUNCH VEHICLE PAYLOAD SAFETY STANDARD

Rev. D March 20, 2019

Japan Aerospace Exploration Agency

This is an English translation of JMR-002D and does not constitute itself.

Whenever this document conflicts with the original document in Japanese, the original document takes precedence.

Contents

F

Intentionally left blank

1. GENERAL

1.1 Purpose

The purpose of this Standard is to specify integrated requirements for safety management and design that the contractor shall implement 1) to protect human life, properties (of public and third party), and environments from adverse effects of mishap or accident occurrence associated with launch vehicle payload (hereinafter referred to as “payload”) to be launched from Japan Aerospace Exploration Agency (JAXA) Tanegashima Space Center (TNSC) or JAXA Uchinoura Space Center (USC), as well as payload’s Ground Support Equipment (GSE), during the period from delivery to TNSC or USC to through launch site operation and launch and until payload separation from launch vehicle, and 2) to mitigate space debris generation.

Note: For JAXA payloads or the payloads JAXA developed on contract with other organizations, Chapter 5 and 6 of this Standard shall apply.

1.2 Application

This Standard shall be applied to the payload and GSE (hereinafter referred to as the “payload/GSE”) and shall be specified in the contract documents agreed between JAXA and the contractor.

1.3 Responsibility of Contractor

The contractor shall be responsible for taking actions required to ensure the safety associated with payload/GSE in accordance with the requirements of this Standard and the Contract Documents, etc.

1.4 Tailoring

(1) Tailoring of system safety management requirements

System safety management requirements of this Standard may be tailored according to features and characteristics of payload/GSE and based on past domestic and foreign experiences. Contractors shall consult with the safety organization of JAXA for tailoring requirements and rationales, reflect the changes in the system safety program plan (refer to paragraph 4.2.1), and receive approval of JAXA safety review.

(2) Tailoring of safety requirements

Safety requirements (safety requirements for design, operations, and space debris mitigation) cited in the system safety program plan may be tailored according to the features and the characteristics of the payload/GSE and based on past domestic and foreign experiences. Contractors shall consult with the safety organization of JAXA for tailoring requirements and rationales, describe the changes in Table 1.4-1 or an equivalent format, attach the Table to the system safety program plan, and receive approval of JAXA safety review.

2 APPLICABLE DOCUMENTS

The following documents constitute a part of this Standard to the extent specified in this Standard. Latest documents at the time of contract shall be applied as applicable documents. If documents are revised afterward, in principle, the latest versions shall be applied. However, if this cannot be accomplished, contractor shall consult with JAXA.

2.1 Applicable documents

(1) JERG-0-001 “Technical Standard for High Pressure Gas Equipment for Space Use ”

(2) JERG-1-007 “Safety Regulation for Launch Site Operation~~/Flight Control Operation~~”

(3) NPR8715.3　NASA Procedural Requirements, NASA General Safety Program Requirements Chapter 2 “System Safety”

(4) MIL-STD-461　Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference

(5) MIL-STD-882　Department of Defense Standard Practice for System Safety

(6) JMR-003 “Space Debris Mitigation Standard”

(7) CZA-2019029 “Rocket Payload Standard Hazard Report Format”

3. DEFINITION OF TERMS

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

Table 1.4-1 (1/2)　Safety Requirements Tailoring Request Form (1/2)

<table>
<tr><td colspan="2">１．Title</td><td colspan="2">Number

Date</td><td colspan="2">Payload Organization

Section</td></tr>
<tr><td colspan="3" rowspan="2">２．(1)Payload Name

(2) Subsystem Name</td><td>Development Manager</td><td>System Safety Program Manager</td><td>Prepared by</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td colspan="6">３．　Document Title, Document Number , and Paragraph Number to be Tailored</td></tr>
<tr><td colspan="6">４．Differences in safety requirements and controls before and after tailoring
4.1 Differences in safety requirements (Safety requirements changes resulting from tailoring)

4.2 Differences in hazard controls (Hazard control changes resulting from tailoring)

（Use additional sheets if extra space is need）</td></tr>
<tr><td colspan="6">５．Reason for tailoring

（Use additional sheets if extra space is need）</td></tr>
<tr><td colspan="6">６．Rationale why equivalent safety is assured

（Use additional sheets if extra space is need）</td></tr>
<tr><td colspan="5">Decision：　Approval　Approval with conditions　Reexamination　（Circle one）</td><td>JAXA　Safety Organization</td></tr>
<tr><td colspan="5">Reasons, Comments, etc：</td><td>

Date</td></tr>
</table>

Note: This form is a part of the system safety program plan and assessed in the safety review for the system safety program plan. The descriptions of the format shall be coordinated with and confirmed by the safety organization of JAXA beforehand.

Table 1.4-1 (2/2) Safety Requirements Tailoring Request Form (2/2)

１． Title ＜Title＞ (Cotinued)	Number
２． (1) Payload Name (2) Subsystem Name	

4 SYSTEM SAFETY PROGRAM MANAGEMENT REQUIREMENT

4.1 Basic requirements

The contractor shall plan and implement system safety program for safety throughout the process from transporting payload/GSE into Tanegashima Space Center or Uchinoura Space Center, through launch until immediately after satellite/payload separation from the launch vehicle.

This Standard sets forth the following basic requirements for system safety program:

(1) System safety management organization that functions appropriately shall be established to implement system safety program.

(2) Hazards in a system including subsystems, components, etc. shall be identified and controlled throughout the entire life cycle. The contractor shall confirm during the development phase that the minimized risk is at the acceptable level.

(3) Safety requirements shall be established to control hazards, and the cause(s) of each hazard shall be identified to facilitate appropriate controls for each cause.

(4) Safety design shall be verified by test or other appropriate means.

(5) Operating procedures or other similar documents shall include all applicable safety requirements. Operations shall be performed in accordance with the procedures.

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

(7) Safety data shall be maintained current.

(8) Effective system safety program plan (see paragraph 4.2.1) shall be developed to implement system safety based on above requirements. Milestones for system safety programs shall be defined based on the milestones for the entire project, and reflect the key activities of the system safety program, *i.e*. hazard analysis, establishment of safety requirements, safety reviews, establishment of management regulation/procedure, schedule to report, audits, schedule of prepared documents submission and, if required, education/training plans.

4.2 System safety program management

4.2.1 System safety program plan

System safety program plan shall be structured based on sample of contents of Table 4.2.1-1, and safety review shall be required by JAXA. System safety program plan shall be updated at all times.

System safety program plan in accordance with NPR8715.3, MIL-STD-882, or equivalent to these documents with requirements of this Standard incorporated will also be acceptable.

4.2.2 System safety program activities

The contractor shall effectively perform system safety program activities throughout the life cycle to assure the safety; to minimize risks throughout the design, manufacture, test, and operation phases; and to confirm the risks are at an acceptable level.

System safety program activities required for the life cycle are shown in Figure 4.2.4-1. Outline of system safety program activities performed during each phase are described below. System safety program activities shall be started immediately after the contract award at the latest.

Manufacturing and tests that are performed prior to delivery to JAXA launch sites, are exempt from JAXA system safety review.

(1) Conceptual study/definition design phase (Phase 0)

a. Prepare the system safety program plan for application throughout the design, manufacture, test, and operation phases.

b. Phase 0 hazard analysis shall be conducted in order to identify hazards for a system including subsystems and components, etc. and examine for measures to be taken to eliminate or minimize and control hazards, and to identify safety requirements that should be added based on the hazard analysis result in addition to the requirements in Chapter 5 and paragraph 2.1(2) (including tailoring results).

JMR-003 shall be applied to decrease space debris as an international norm. The contractor shall consult with JAXA when applying the equivalent document of JMR-003.

Note: Because “hazard identification” is performed throughout all phases, hazard identification summary in Table 4.3.4-1 shall be developed based on paragraph 4.3.1 in the early phase of design process and updated as design matures.)

c. Safety requirement compliance matrix shall be developed to confirm that design, manufacturing and test, and operation plan comply with safety requirements. The safety requirement compliance matrix format is shown in Table 4.2.4-3.

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

(2) Preliminary design phase (Phase I)

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

b. Phase I hazard analysis shall be conducted. The result of investigation/examination by the Phase I hazard analysis is put into writing, and reflected in a basic design.

c. As required, the system safety program plans shall be maintained/revised.

d. The result of the Phase I hazard analysis shall be documented and reflected in a preliminary design.

(3) Critical design phase (Phase II)

a. Process of (2) above shall be repeated for Phase II.

b. Safety requirement compliance shall be confirmed in the design reviews. When nonconformance with a safety requirement is identified, design shall be modified to meet the safety requirement. If noncompliance cannot be avoided, Noncompliance Report (see paragraph 4.2.5) shall be developed, with consultation with JAXA, ensuring residual risk is within acceptable level. The sheet requires JAXA approval.

(4) Manufacturing/testing phase (Phase III)

a. Process of (3) above shall be repeated for Phase III.

b. Completion of all safety verifications shall be confirmed. Any items which safety verification can be completed only at the launch site shall be recorded in the safety verification tracking log (Table 4.2.4-4 or equivalent), closed item by item prior to related operations, and submitted to JAXA after every closure.

(5) Operation phase

a. The results of Phase III hazard analysis shall be revisited, operating procedures for the launch site and other operating procedures shall be up-dated if required.

b. For safety involved in operations, all operations shall be confirmed to be conducted in accordance with the system safety program plan and operating procedures, as an operational safety stand point.

c. If any hazard is newly identified, investigation/examination shall be conducted in coordination with the reliability program division and quality program division to take required corrective actions

d. If design is modified, requirements for design phase shall be applied.

e. If any system safety related item is modified after Phase III, safety to the design change and the procedure change, and the launch site operation procedures, shall be confirmed.

4.2.3 System safety management organization

The system safety management organization shall be established considering the level of independence from development project organization according to development item and program scale.

The system safety management organization shall be managed per following.

(1) The contractor shall establish a system safety management organization, that has clearly defined responsibility and authority, functions, instructions and reporting, etc., to plan and implement system safety programs

(2) The contractor shall appoint a system safety program manager who is responsible for system safety management for payload/GSE and launch site operations and has knowledge and experience of system safety.

(3) System safety program manager shall have the following authorities and responsibilities:

a. To develop/establish system safety program plan according to the authority of system safety program manager.

b. To establish management procedures required for implementation of system safety program plan.

c. To conduct a review of specifications, procedures and other documents for safety.

d. To promote hazard analysis and safety reviews.

e. To maintain, manage, and efficiently utilize safety data.

f. To coordinate with appropriate sections for safety related issues.

g. To make reports and recommendations for safety directly to a person who is responsible for implementation of payloads/GSE development.

h. To prevent and terminate establishment/revision of project activities and documents that deviate from safety requirements and procedures regarding safety.

i. To terminate and correct safety critical operations that deviate from established procedures

j. To serve as a point of contact with JAXA for safety management.

4.2.4 Safety review

The purposes of safety reviews are to confirm safety requirements for payload/GSE established according to identified hazards, and compliance with those requirements. Safety reviews shall also evaluate identification of hazards and their causes; controls and their verification method; validity of verification results; minimization of residual risks; and acceptability of the residual risks.

The contractor shall perform safety reviews for each phase in accordance with the followings to confirm that activities required in section 4.2.2 have been performed and appropriately incorporated into the design, and required safety data has been prepared.

(1) The system safety program manager or designated alternate shall conduct a safety review to confirm that system safety of payload/GSE is conducted properly and the execution purpose is achieved.

(2) In principle, safety review is conducted four times, one per each development phase; Phase 0, Phase I, Phase II, and Phase III safety reviews.

Phased safety reviews may be integrated depending on the scale of the system, experiences in foreign countries, etc. after coordination with JAXA. Each phased safety review may be conducted as a part of the overall milestone reviews after coordination with JAXA.

(3) Safety reviews shall be conducted based on established safety review plan. The overview of safety review is described in Figure 4.2.4-1 including schedule for each safety review to be performed, purpose of review, documents to be reviewed, and major system safety program activities for each development phase.

(4) Review documents, minutes, action item table, and required support data shall be compiled as a safety data package. The safety data package shall be submitted to JAXA immediately after completion of each safety review and shall be reviewed by JAXA safety review.

(5) All verification items in Payload Safety Verification Tracking Log (4.2.2 (4)) that have not been closed at Phase III safety review requiring closure at the launch site shall be closed and submitted to JAXA along with Payload Safety Compliance Certificate (Table 4.2.4-2) prior to JAXA Launch Readiness Review.

The contractor shall report on launch site's safety management implementation status including its safety activities to JAXA Launch Readiness Review for safety review.

4.2.4-1 Phase 0 Safety Review

The purposes of Phase 0 Safety Review are to clarify issues that have been identified during the preparation of review data, specified in (1) below, regarding payloads/GSE in the conceptual design phase, and to determine an approach for the items to be resolved in the subsequent phases.

The contractor may conduct Phase 0 Safety Reviews as an informal working group type meeting such as technical interchange meeting. However, the contractor must undergo the safety review of JAXA.

(1) Review data requirements

The following data are required for Phase 0 Safety Review:

a. Description of payloads/GSE in the conceptual study/definition design phase and mission scenario of payloads.

b. Description of safety critical subsystems and their operations.

c. Launch site operation scenario.

d. Status (including appropriate support data) of compliance with safety requirements using the form in Table 4.2.4-3, "Safety Requirement Compliance Matrix".

e. Hazard Identification Summary (using the form shown in Table 4.3.4-1, and including appropriate support data).

f. Description of controls/verification methods against hazards which are not required to submit hazard report and safety related issues which are not identified hazard.(Hazard Analysis Table (using the form shown in Table 4.3.3-1, or an any form)).

g. Phase 0 Hazard Report (preferable from an initial phase, though not mandatory).

Standard Hazard Report form (provided by paragraph 2.1 (7)~~attachment 1~~) can be used when hazard controls and verification are applicable to the identified hazards in the form. Unique Hazard Report form (using the form shown in Table 4.3.4-2) shall be used when hazard controls and verification are not applicable to the identified hazards. F

(2) Major items discussed at Phase 0 Safety Review

If Phase 0 Safety Review is conducted, major items discussed are as follows:

a. Overview of the conceptual design of the payloads/GSE and the launch site operations,

b. Descriptions of safety critical subsystems,

c. Exhaustiveness of hazards and hazard causes identification

d. Validity of applicable safety requirements (including tailored requirements if applicable) as well as new requirements added based on hazard analysis.

4.2.4-2 Phase I Safety Review

The purpose of Phase I Safety Review is to formally review the preliminary design of payloads/GSE and the scenario of launch site operations to ensure that they comply with requirements of this Standard and the results of hazard analysis are acceptable.

The following items shall be reviewed for hazard analysis:

a. All hazards and their causes have been identified.

b. Appropriate measures for eliminating, reducing or controlling causes of all hazards have been established.

c. Appropriate safety verification methods have been established.

(1) Review data requirements

Review data required for Phase I Safety Review shall be as follows: (If safety review is conducted as a part of the design review, duplicated data may be omitted from the safety review data, provided that whereabouts of required data are specified. The same rule applies hereinafter.)

a. Latest description of Payloads and mission scenario of payloads.

b. Latest descriptions of safety critical subsystems/components and their operations for payloads, GSE, and related launch operations (The descriptions shall include schematics and block diagrams showing identified safety features, inhibits, etc.).

c. Latest launch site operation scenario.

d. Pyrotechnics data, the results of RF hazard analysis (refer to section 5.5.6).

e. Latest Safety Requirements Compliance Matrix (including appropriate support data).

f. Latest Hazard Identification Summary (using the format shown in Tables 4.3.4-1, and including appropriate support data).

g. Description of controls/verification methods against hazards which are not required to submit hazard report and safety related issues which are not identified hazard.(Hazard Analysis Table (using the form shown in Table 4.3.3-1, or an any form)).

h. Latest hazard reports

Standard Hazard Report form (provided by paragraph 2.1 (7)~~attachment 1~~) can be used when hazard controls and verification are applicable to the identified hazards in the form. Unique Hazard Report form (using the form shown in Table 4.3.4-2) shall be used when hazard controls and verification are not applicable to the identified hazards. F

i. Results of Fault Tree Analysis (FTA), Sneak Circuit Analysis (SCA), etc. (if applicable).

(2) Major items discussed at Phase I Safety Review

Major items discussed at Phase I Safety Review are listed below:

a. Examination of latest payload program milestones and schedules.

b. Overview of the preliminary design of payloads/GSE, and scenario of launch site operations.

c. Description of latest safety-critical subsystems.

d. Description of assessment of the compliance with applicable safety requirements.

e. Results of Phase I hazard analysis.

f. Determination of Phase I Hazard Reports disposition process.

4.2.4-3 Phase II Safety Reviews

The purpose of Phase II Safety Review is to review the critical design of payload/GSE and the scenario of launch site operations to ensure that they comply with requirements of this Standard and the results of hazard analysis are acceptable. The following shall be reviewed for hazard analysis:

a.All hazards have been identified;

b.Appropriate measures for eliminating, reducing, or controlling all hazards have been cleared and implemented.

c.Specific safety verification methods (such as test plans, analysis methods, and inspection requirements) have been determined.

d.Payload/GSE interfaces, launch site operations, procedures, and implementation schedule that were not addressed during Phase I Safety Reviews shall be assessed.

Payload interfaces shall be assessed including those between the launch vehicle and payloads, between the subsystems/components consisting of payload system; and between the payload and associated GSE, launch site facility, and equipment. Additional hazard reports shall be prepared for newly identified hazards.

Hazard analysis shall incorporate the hazards of subsystems and components to develop hazard reports for the system.

(1) Review data Requirements

The following data are required for Phase II Safety Review:

a. Description of latest Payloads and mission scenario payloads.

b. Description of latest safety critical subsystems/components and their operations for payloads/GSE, and related launch site operations. (The description shall include schematic and block diagrams showing safety features, inhibits, etc. The required number of inhibits and controls and their independence shall be clearly identified especially in electrical schematics).

c. Drawings and required stress analysis results of safety critical subsystems/components for payload and GSE.

d. Updated scenario of launch site operations.

e. List of all hazardous operation procedures and description of safety measures procedures for the hazardous operations.

f. Updated pyrotechnics data, and the results of RF hazard analysis (refer to 5.5.6).

g. List of nonconformance and accidents that could have an impact on the safety.

h. Updated Safety Requirement Compliance Matrix (including appropriated support data).

i. Hazard Identification Summary (only when a new hazard is identified, and including appropriate support data).

j. Description of controls/verification methods against hazards which are not required to submit hazard report and safety related issues which are not identified hazard.(Hazard Analysis Table (using the form shown in Table 4.3.3-1, or an any form))..

k. Updated hazard reports

Standard Hazard Report form (provided by paragraph 2.1 (7)~~attachment 1~~) can be used when hazard controls and verification are applicable to the identified hazards in the form. Unique Hazard Report form (using the form shown in Table 4.3.4-2) shall be used when hazard controls and verification are not applicable to the identified hazards.

l. Updated results of FTA, SCA, etc. (if applicable).

m. Status of action items assigned at Phase I Safety Review.

(2) Major items discussed at Phase II Safety Review

The major items discussed at Phase II Safety Review are listed below.

a. Status of action items assigned at Phase I Safety Review.

b. Overview of payloads/GSE, emphasizing design changes implemented after Phase I Safety Review.

c. Assessment of the compliance with safety requirements that should be reflected in the final design of payloads/GSE. (If not complied, methods to correct noncompliance shall be specified. If the noncompliance cannot be eliminated, the rationale for acceptance shall be presented.)

d. Results of Phase II hazard analysis.

e. Determination of disposition process of Phase II Hazard Reports.

4.2.4-4 Phase III Safety Review

The purpose of Phase III Safety Review is to review the final design of payloads/GSE, manufacturing results of payloads/GSE and launch site operations to ensure that they comply with safety requirements of this Standard; the final results of hazard analysis are acceptable; and all hazard verification items are closed.

Verification items that must be conducted at the launch site and were not closed during Phase III Safety Review shall meet requirements in paragraph 4.2.4 (5).

Permission for delivery of payloads to TNSC or USC and start of the launch site operations shall be determined at JAXA safety review meeting.

If contents on JAXA Phase III Safety Review are modified, or additional issues are newly identified, consult with JAXA and conduct the post-Phase III Safety Review, if necessary.

(1) Review data requirements

The following review data are required for Phase III Safety Review.

a. Final description of the as-build Payloads and payload mission scenario.

b. Final description of the configuration of safety critical subsystems and their operations for payload/GSE and related launch site operations. (The description shall include schematics and block diagrams showing identified safety features of the as-built payload and inhibits/controls.).

c. Final drawings and required stress analysis results of safety critical subsystems/components for payload/GSE.

d. Final scenario of the launch site operations.

e. Complete list of all hazardous operation procedures and outline of their safety measures procedures.

f. Complete pyrotechnics data, and the results of RF hazard analysis.

~~g. Summary of all nonconformance and accidents determined to have an impact on launch vehicles or JAXA properties such as facility equipment occurred during fabrication, test, and inspection of Payload/GSE, and their safety assessment.~~

g. Safety assessment reports and summary of noncomformances, for any noncomformances that impact safety, among all the noncomformances that occurred during fabrication, test, inspection of Payload and/or GSE.

h. Safety Verification Tracking Log for safety of payload/GSE and launch site operations (using the form shown in Table 4.2.4-4).

i. Confirmation that payloads have a Pressure Vessel Log Book that addresses the history of pressurization, exposure to fluid, and other applicable data for all pressure vessels of payload.

j. Complete Safety Requirement Compliance Matrix.

k. Hazard Identification Summary (including appropriate support data, only if a new hazard is identified).

l. Description of controls/verification methods against hazards which are not required to submit hazard report and safety related issues which are not identified hazard.(Hazard Analysis Table (using the form shown in Table 4.3.3-1, or an any form)).

m. Complete Hazard Reports (including appropriate support data that contain the final configuration of the as-built payload).

Standard Hazard Report form (paragraph 2.1 (7)~~attachment 1~~) can be used when hazard controls and verification are applicable to the identified hazards. Unique Hazard Report form (using the form shown in Table 4.3.4-2) shall be used when hazard controls and verification are not applicable to the identified hazards.

n. Final results of FTA, SCA, etc. (if applicable).

o. Final Noncompliance Report (using the form at show in Table 4.2.5-1) (Disposition must be completed prior to completion of Phase III Safety Review)

p. The status of action items assigned in Phase II Safety Review.

(2) Major items discussed at Phase III safety review

The major items discussed at Phase III Safety Review are listed below:

a. The status of action items assigned at Phase II Safety Review.

b. Description of hazard analysis emphasizing design modifications and safety verifications performed after Phase II Safety Review.

c. Final assessment of the compliance of the as-built payloads/GSE with safety requirements. (Noncompliance Report shall have been approved by JAXA prior to Phase III Safety Review.)

d. Determination of disposition process of Phase III Hazard Reports.

e. Disposition process for all issues, open items, etc. (There issues and open items shall be recorded in Safety Verification Tracking Log format shown in Table 4.2.4-4 for the final examination to resolve the problems. Previous action items shall be closed prior to completion of Phase III Safety Review.)

Table 4.2.1-1 System Safety Program Plan – Typical Table of Contents

Item	Remarks	Applicable Paragraph
1. General 1.1 Purpose		
1.2 Scope	In case of series/reflight payload, scope and implementation items shall be clalified.	4.2.6
2. Related documents To indicate applicable and reference documents.		
3. Implementation items 3.1 Organization and Implementation system (1) To clearly specify the project manager, the system safety program manager, and related sections. (2) To illustrate the system safety management organization including related sections.	If a direct contract with a supplier is involved, system safety program management for the supplier shall be described.	4.2.3
3.2 System safety review method		4.2.4
3.3 System safety activities in each phase of development (1) To specify hazard analysis, safety requirements, system safety reviews, and other activities for each phase of development. (2) To indicate the 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 identification		4.3.1
3.5 Risk assessment		4.3.2
3.6 Hazard analysis		4.3.3
3.7 Safety requirements (1) Applicable documents (2) Non-applicable items related to the applicable documents, tailored items(*) subject to prior coordination, etc. (3) Additional requirements resulting from hazard analysis (4) Implementation for Japanese laws in case of legal process for government agency.		4.2.2, and others
3.8 Safety verification		4.3.5
3.9 Education/Training		4.2.7
3.10 Mishap investigation and reporting		4.2.9
4. Documents to be developed and safety data		4.4

∗ : Tailored items shall be described using Table 1.4-1.

Table 4.2.4-1 General Outline of Safety Review and Phased System Safety Activities

Type of Safety Review	Review Timing	Primary Purpose of Safety Review	Major Safety Activities in each Development Phase
Phase 0 Safety Review (Note 1)	Upon Completion of Conceptual Study/Definition Design	・To confirm hazards and their causes ・To cofirm applicable safety requirements (including additional requirements per tailoring and hazard analysis.)	・For Phase 0 hazard analysis, hazard, hazard cause, and control identification (Refer to the hazard analysis table (Table 4.3.3-1).) ・Initial identification of applicable safety requirements and establishment of additional safety requirements
Phase I Safety Review	During Preliminary Design Review （PDR）	・To confirm hazards and thier causes ・To confirm hazard control methods ・To confrim verification methods ・To confirm details of safety requirements added as necessary.	・Reconfirming the results of Phase 0 hazard analysis and adding the details to safety requirements as necessary. ・For Phase I hazard analysis - Hazard identification - Identification of causes for hazards - Discussion on hazard control methods - Discussion on safety verification methods (general outline) ・Reconfirming the detailed safety requirements on the basis of the above analytical results
Phase II Safety Review	During the Critical Design Review （CDR）	・To confirm that a hazard control method is implemented in the design ・To confirm that a verification methods is established in detail	・Reconfirming the results of Phase I hazard analysis ・For Phase II hazard analysis - To incorporate the hazard control method into the critical design. - To discuss the safety verification methods in detail. - Hardware/software safety verification tests as required ・Operational proposal and reconfirmof 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	・Assessment/confirmation of consistency between manufacturing and test results and hazard verification ・To confirm that safety verification is incorporated in the operational procedures. ・Confirmation of deviation/waiver handling

Note 1） The controactor may conduct Phase 0 safety review as informally as a working group meeting.

Time(month/year) / Phase / System Safety Program Activity	Conceptual Study/ Definition Design (Phase 0)	Preliminary Design (Phase I)	Critical Design (Phase II)	Manufacture/verification (Phase III)	Operation	Remarks
Overall Milestone — Contractor	Definition Design Review (DDR) ▽	Preliminary Design Review (PDR) ▽	Critical Design Review (CDR) ▽	Post Qualification Review or Pre Shipment Review (PQR or PSR) ▽		
System Safety Program Plan	Preparation Review ▽ ▽	Update/Revision ▽	Update/Revision ▽	Update/Revision ▽	Update/Revision ▽	
Safety Review (Contractor) (JAXA)	Phase 0 Safety Review ▽ ▽	Phase I Safety Review ▽ ▽	Phase II Safety Review ▽ ▽	Phase III Safety Review ▽ ▽	Post-Phase III Safety Review ▽(if necessary) Launch Readiness Review ▽	
Hazard Analysis	Phase 0 Hazard Analysis	Follow-up Reconfirmation				
		Phase I Hazard Analysis				
			Phase II Hazard Analysis	Follow-up Reconfirmation Phase III Hazard Analysis	Follow-up Reconfirmation	
Safety Requirements	Initial identification of safety requirements ▽ Identification of safety requirements ▽	(As necessary) Add details to requirements ▽ Review ▽				
Operation Procedures, etc.				Preparation (Manufacturing・Process Specifications, Test Procedures, etc.)	Preparation (Operation Procedures)	

Figure 4.2.4-1　System Safety Program Activities in the Life Cycle

Table 4.2.4-2 Payload Safety Requirement Compliance Report Form

Payload Safety Compliance Certificate

____

（Payload）

We ________________________ hereby certify that;

（Contractor）

The payload complies with all safety requirements in
JMR-002 (Current issue) Chapter 5,
JERG-1-007(Current issue) Chapter 4, and
JMR-003 (Current issue) Chapter 5.

Approved waivers or deviations are listed below.

Approved： ______________________________ __________

（Contractor） Date

Table 4.2.4-3 Safety Requirement Compliance Matrix

(Safety Requirements Document Title and Document Number with Revision Identification)		Compliance	Non-compliance	N/A	Program ____________	
Paragraph	Requirement Description				Results	Remarks

Table 4.2.4-4　Safety Verification Tracking Log Form

Page　　／

System Name ;

Date ;

Log number	Hazard report number	Safety verification number	Verification Item／Verification confirm method	Restriction to operation of Launch site	Completion plan date	Completion date	Verification result confirmation	note（Procedure number/Title）

4.2.5 Noncompliance Report

If payload/GSE fails to comply with requirements specified in Chapter 5 of this Standard; Chapter 4 of "Safety Regulation for Launch Site Operation~~/Flight Control Operation~~" (paragraph 2.1(2)); and Chapter 5 of "Space Debris Mitigation Standard" (paragraph 2.1(6)) (including tailored or otherwise modified safety requirements); the contractor shall confer with JAXA, examine compliance in detail, record the examination results in the Noncompliance Report (refer to Table 4.2.5-1 for a format), and receive the approval of Deviation/Waiver from the safety review of JAXA.

The contractor shall incorporate the examination results in the safety requirement compliance matrix and update the hazard report if the residual risk falls within the range requiring hazard report development as shown in Figure 4.3.2-1.

4.2.6 Series payloads / Reflight payloads application

4.2.6.1 Series payloads

If payload designed identically or similarly to a payload (including payload elements) previously launched from TNSC or USC is launched, the contractor shall perform the following:

a. Perform assessment of the impact from applicable documents version's differences between old version and new version such as this Standard or safety requirements.

b. Clearly define similarity or difference as a series payload, such as design modification in conjunction with operation purpose change and/or improvement in conjunction with technological renovation, and perform required hazard analysis.

c. If waiver for a payload has been accepted in previous flight, but corrective action has not been taken, Noncompliance Report for the payload shall be re-submitted.

d. Conduct a safety review.

e. To consult with JAXA in advance including above plans after preparing or revising system safety program plan.

4.2.6.2 Reflight payloads

For payload (including payload elements) that has been previously launched from TNSC or USC, the contractor shall specify storage conditions, status of limited life items, details of refurbishment, and other relevant factors, and shall confirm its safety through a safety review.

The contractor shall submit the following data in addition to data in 4.2.6.2.

a. Assessment of limited life items.

b. Descriptions of maintenance, structural inspections and refurbishment, and assessment of safety impact

4.2.7 Education and training

Prior to operations, the contractor shall conduct safety education/training to ensure safety of operations for personnel associated with manufacture, test, and transportation of payload/GSE, and for personnel associated with unpacking, inspection, and assembly test of payload/GSE set-up and handling of GSE, handling of hazardous products, operation on high-elevated place that are performed at TNSC or USC. Education/trainings for personnel s be conducted according to training plans prepared by the contractor that address the following.

(1) Identify equipment, operations, and support tasks that require trainings. JAXA conducting safety education trainings for launch site personnel specified in paragraph 2.1(2), "Safety Regulation for Launch Site Operation~~/Flight Control Operation~~" could be excluded from identified operations.

(2) Specify the need for any qualification.

(3) Education/training plans shall include the following:

a. Hazard classification and causes, expected mishaps, preventive measures, and control methods

b. Procedures, check lists, emergency procedures, etc.

c. Functions and operations of safety devices, protective devices, monitoring equipment, and warning devices (except for JAXA facilities and equipment).

d. Preventive measures for human errors.

(4) Education training shall be designed not only for the contractors and their related persons but also for JAXA workers and their related persons if those persons are determined to be required for trainings, considering peculiarity of payload/GSE.

(5) To prepare a record of participants name and the results of training.

4.2.8 Investigation and reporting of mishap or accident

4.2.8.1 Investigation of mishap or accident

The contractor shall perform investigations if any mishap or accident occurs after delivery of payload/GSE to TNSC or USC, and shall submit required records and data to JAXA section in charge.

4.2.8.2 Reporting of mishap or accident

The contractor shall conduct below.

(1) Report to JAXA section in charge immediately on injury to or death of person, damage to property caused by a mishap or accident on JAXA ground, a mishap or accident causing considerable effect to JAXA ground and surrounding environment, and a mishap or accident which influenced the third party. The mishap or accident shall be documented in the latest format at the time of reporting and the report shall be submitted to JAXA section in charge within 5 working days. If a detailed report is required, the report shall be submitted within 30 days of the mishap or accident.

For "Hiyari-Hatto," an event that could have led to a mishap if any other factors are added (a close call of a mishap), examine the event occurrence situation, cause, etc.; investigate recurrence prevention measures; document the results in the latest format at the time of reporting; and submit the report to JAXA section in charge.

(2) For safety critical mishap or accident occurred prior to delivery of payload/GSE to TNSC or USC, examine the mishap or accident occurrence situation, cause, etc.; and report the results to JAXA section in charge.

For "Hiyari-Hatto," an event that could have led to a mishap if any other factors are added, examine the event occurrence situation, cause, etc., investigate recurrence prevention measures, report to JAXA section in charge.

Table 4.2.5-1 Noncompliance Report Form

<table>
<tr><td colspan="2" rowspan="2">Title</td><td colspan="2">Number</td><td colspan="2">Date</td></tr>
<tr><td colspan="4" rowspan="2">Contractor Name, Section Name</td></tr>
<tr><td colspan="2">Payload Name</td></tr>
<tr><td>Disposition ;
(circle either)</td><td>・Waiver
・Deviation(Compliance)</td><td>Development Manager</td><td colspan="2">System Safety Program Manager</td><td>Prepared by</td></tr>
<tr><td colspan="6">Applicable Safety Requirements</td></tr>
<tr><td colspan="6">Description of Noncompliance</td></tr>
<tr><td colspan="6">Reason for Noncompliance

(Use additional sheets if extra space is need)</td></tr>
<tr><td colspan="6">Relevant Hazard Control (Applicable Hazard Report No:)

(Use additional sheets if extra space is need)</td></tr>
<tr><td colspan="4">Decision</td><td colspan="2">JAXA/Safety Section

Date</td></tr>
</table>

* The contractor shall submit this form to JAXA

* Attach the support materials or data.

4.3 Hazard analysis

4.3.1 Hazard identification

(1) Severity

Severity is indicated using Severity Categories I, II, III, and IV as shown in Table 4.3.1-1 that provides criteria for the expected worst case derived from human error, adverse environment conditions, inappropriate design, defective procedures, defects or malfunctions of subsystems or components, or other factors.

Table 4.3.1-1 Severity Categories

Severity	Terminology	Description
I	Catastrophic	~~Any condition that may cause death or severe injury of third-party(including permanent damage), death or severe permanent damage of personnel, loss of or severe damage to public or thrid partyls private property, loss of system (launch vehicle, payload/GSE) or launch site facilities, and/or serious environmental damage.~~ Death or severe personal damage Irreversible significant environmental impact Loss of or severe damage to public or third party property Loss of launch site facilities
II	Critical	~~Any condition that may cause minor injury of third-party, severe personnel injury, minor damage to public or private property, severe damage to system (launch vehicle, payload/GSE) or launch site facilities, and/or reversible severe environmental damage.~~ Major personal damage*1 Reversible significant environmental impact Major damage to public or third party property Severe damage to launch site facilities *1 Injury or occupational illness requiring definitive/specialty hospital/medical treatment
III	Marginal	~~Any condition that may cause minor personnel injury, minor damage to system (launch vehicle, payload/GSE) or launch site facilities, and/or minor environmental damage.~~ Minor personal damage*2 Reversible moderate environmental impact Minor damage to public or third party property *2 Injury not requiring definitive/specialty hospital treatment
IV	Negligible	Any conditions that causes less damages than Hazard level I to III.~~may cause less than minor personnel injury, minor damage to system (launch vehicle, payload/GSE) or launch site facilities, and/or minor environmental damage.~~

(2) Likelihood of occurrence

The probability of hazard occurrence throughout the life cycle of systems, subsystems, or components can be expressed as the number of potential likelihood of occurrence for the constant unit such as operating hours and the number of activations, personnel involved, or operations.

The possibility of occurrence may be expressed qualitatively (examples are shown in Table 4.3.1-2). This may be derived from analysis of past safety data on similar system and etc.

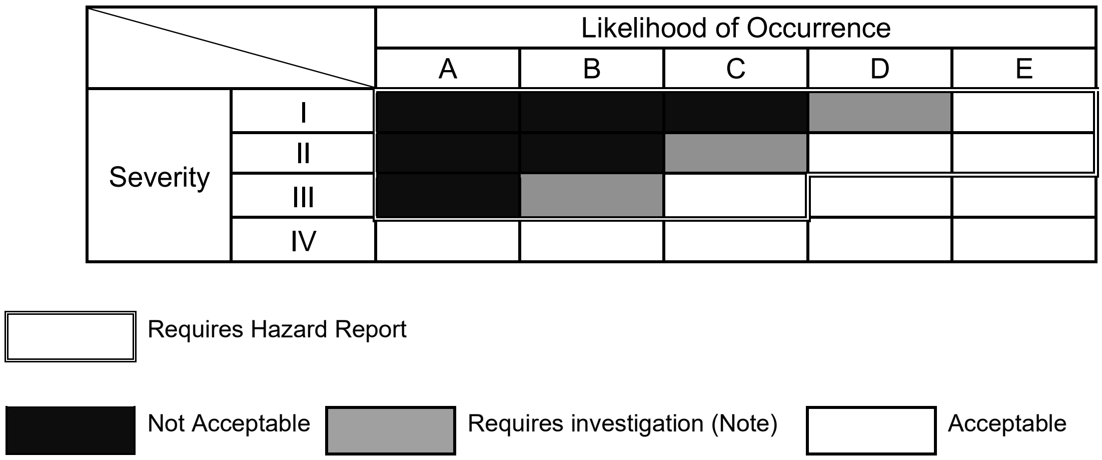
Table 4.3.1-2 Likelihood of Occurrence

Likelihood of Occurrence Classification	Terminology
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 Risk assessment

The risk acceptance criteria shall be in accordance with Table 4.3.2-1. However, if the contractors propose criteria equivalent to the risk acceptance criteria, the contractors shall consult with JAXA on the proposed criteria. If the proposed criteria are approved by JAXA, the criteria may be used as substitute for the risk acceptance criteria.

Although residual risks are within the risk acceptance criteria, that are not sufficient enough, therefore, maximum efforts under limited conditions shall be required to eliminate the risks.



Note: (1) Those requiring investigation maybe accepted when risk is minimized to the extent possible.

(2) Likelihood of occurrence shall be the likelihood with hazard control.

(3) For hazards outside of the range that requires hazard reports, the evidence that hazard reports are not required shall be clearly documented using Hazard Analysis Table (See Table 4.3.3-1.).

(4) For hazards which severity is I or II without hazard controls, hazard reports shall be developed as a rule even when such hazards fall in the range that does not require hazard reports after hazard controls.

Fig.4.3.2-1 Risk Acceptance Criteria

4.3.3 Phased hazard analysis

The contractor shall perform hazard analysis in the early stage of design phase to identify hazards and establish safety requirements to reflect in designs, procedures, operations, etc. The results of this hazard analysis shall be compiled into a safety data package to be reviewed at safety reviews specified in 4.2.4. Therefore, hazard analysis shall be performed during each phase of 0, I, II, III corresponding to each phase of safety reviews shown below. If design is modified, hazard analysis shall be re-performed.

(1) Phase 0 hazard analysis (Conceptual Study/Definition Design Phase)

Phase 0 hazard analysis is performed during conceptual study/definition design phase to identify hazards and hazard causes, and examine controls. The results shall be summarized in the Hazard Analysis Table (refer to Table 4.3.3-1), and applicable safety requirements shall be identified. Phase 0 hazard analysis shall contain the following:

a. Definition of portion and location having a hazardous condition that could occur during system operations.

b. Identification of hazardous substances from materials or parts to be used.

c. Clearly define hazards those are identified during testing, transportation, handling, operation, etc.

d. Clearly define safety issues regarding interfaces.

e. Estimation of expected damage of mishap or accident as a result of hazard. To document hazard causes and controls in the hazard analysis table.

(2) Phase I hazard analysis (Preliminary Design Phase)

The purpose of Phase I hazard analysis is to perform more detailed hazard analysis based on hazards identified during Phase 0 hazard analysis in order to specify identified hazards, impacts, and control and establish detailed safety requirements.

Hazard report shall be developed for hazards that are classified as coverage of hazard report to be prepared as defined in 4.3.2, and the hazard report shall be reviewed as phase progressed. Hazard report shall contain the following:

a. Hazard causes that have been identified and appropriate hazard elimination and control that have been established.

b. To perform hazard analysis regarding interfaces for connection of systems and subsystems and trade-off studies to establish optimum safety conditions for design modification and safety. Hazard analysis shall generate hazard reports for the system incorporating subsystem and component level hazards.

c. To perform FTA (Fault Tree Analysis) for high-risk hazards and, if required, SCA (Sneak Circuit Analysis) and ETA (Event Tree Analysis).

d. To perform crosscheck of the results of hazard analysis with the results of FMEA to ensure complete coverage.

e. To reflect necessary corrective measures in design based on the results of analysis, considering safety related design constraints, etc.

f. To clearly define improvement and corrections of safety in order to conduct them in an appropriate manner.

(3) Phase II hazard analysis (Critical Design Phase)

The purpose of Phase II hazard analysis is to perform detailed safety assessment by re-assessing the results of Phase I hazard analysis as the design progressed during critical design phase. Phase II hazard analysis shall contain the following:

a. To ensure that proposed measures for elimination and control of hazards are clearly defined and incorporated into the design.

b. To re-assess the results of FTA, SCA, and ETA if needed,

c. To select appropriate methods to reduce the frequency of mishap occurrence relating to safety critical parts, materials, etc.

d. To document safety critical technologies, designs, manufactures, tests, operations, and other activities and the scope affected by those activities, and reflect these to safety maintenance and improvement activity.

e. To specify verification methods.

(4) Phase III hazard analysis (Manufacturing/Testing Phase)

The purpose of Phase III hazard analysis is to perform detailed safety assessment of operations by re-assessing the results of Phase II hazard analysis during manufacturing/testing phase. Phase III hazard analysis shall contain the following:

a. To clearly define and document the proposed measures for elimination and control of hazards relating to system operations.

b. To select appropriate methods to reduce the frequency of hazard occurrence relating to safety critical operating procedures.

c. To document safety critical system operations and the scope affected by the operations, and reflect these to safety maintenance and improvement activity.

d. To clarify the verification results of hazard control.

4.3.4 Hazard report

The contractor shall document the results of hazard analysis performed in accordance with the following and submit the documented results at an appropriate time.

(1) After fully understanding configuration, functions, etc. of the payload/GSE, identify all existing or potential hazard causes by considering expected mishaps referring to Hazard Identification Summary in Table 4.3.4-1 or equivalent. Group identified hazard causes by hazard category and fill in the Hazard Identification Summary.

(2) To perform hazard analysis of each hazard identified in (1) above for hazard classification, causes, control methods, and verification methods. The results of hazard analysis shall be described in Hazard Report and shall be updated as phase progressed. Support data shall be attached to hazard report, as applicable. Hazard Report forms are the following.

Standard Hazard Report form (provided by paragraph 2.1 (7)) : using when hazard controls and verification are applicable to the identified hazards in the form.

Unique Hazard Report form (using the form shown in Table 4.3.4-2): using when hazard controls and verification are not applicable to the identified hazards.

(3) The results of hazard analysis performed in section (1) and (2) above shall be consistent with the results of FTA and FMEA, Noncompliance Report (if applicable), and the results of other analysis that have been performed separately.

(4) Hazard report shall be signed per each phase by System Safety Program manager for confirmation, and shall be submitted to JAXA section in charge as safety review data package for confirmation.

(5) Hazard report shall be complete when hazards are eliminated by design, hazard controls are verified, or residual risk meets the risk acceptance criteria with maximum effort, and all safety verifications are completed.

4.3.5 Safety verification

Safety verification is to confirm that hardware and software of payload/GSE satisfy all the safety design requirements by test, inspection, analysis, demonstration, and any combination of these methods using objective evidences. Procedure/process controls used as verification methods shall be compiled into procedure, and analysis/test/inspection used as verification methods shall be compiled into a report, their document numbers, etc. shall be shown in hazard report. For similarity analysis, previous verification procedures and requirements referred shall be studied to adequately evaluate their similarities.

As previously described (4.2.2(4)), open items of safety verification data that are not closed before completing Phase III and transferred to launch site operation to close, shall be recorded in the Safety Verification Tracking Log for tracking and management, closed, and submitted at an appropriate time.

All data associated with safety verification shall be managed to be available at any time.

After verification, the verification results shall be reported, and feedback such as corrective action shall be required as a disposition process if nonconformance has been found.

Table 4.3.3-1 Hazard Analysis Table Form

No.	Hazard Title	Hazard Summary	Cause	Control	Severity	Likelihood	Notes (HR No.)
1							
2							
3							
4							

Note: Hazard Report number shall be recorded when applicable.
Severity shall be entered after Phase I.
Hazard summary and control shall be described clarifying hazard severity and likelihood so that applicable severity and likelihood can be justified.
When severity is decreased, control should include rationale for lower severity.

System :

Subsystem :

Table 4.3.4-1 Hazard Identification Summary

Hazard Category / Hazard Type	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													
System, subsystem, component, other hazardous item, or task./ step title	High temperature/Heating elements	Low temperature/Extremely low temperature	Flammable materials/Oxidant /ignition source	Pressure systems/	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/Dissimilar metals/Galvanic corrosion	Fluid compatibility	Loose fittings/Plumbing damage	Deterioration of seals/Permanent sets in seal seats, Malfunctioning of		Shield deficiency	Short circuit	Electrostatic	Electrical shock	Ionizing radiation/Radio active substance	Laser/IR/UV/Spark	Radio wave	Continuous noise/Impact noise	Oxygen deficiency/Toxic gas	Elevated work/unstable position	Dropped parts or tools	Dropping a hoisted item											
HR No.																																									

Note: Hazards shall be identified considering the accident possibilities due to below.

- Human factors
- Software Error (input error, bug)
- Natural Disaster (Earthquake, Tsunami, Lightning, Typhoon, Sever wind, etc.)
- Hazardous Operations (Handling of dangerous/detrimental materials, high pressure gas, explosive, or transportation of a heavy object)

（Note）An additional hazard maybe entered in a blank column according to system characteristics.

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

Table 4.3.4-2 (1/2) Hazard Report Form (1)

<table>
<tr><td colspan="3">Hazard Report</td><td colspan="2">HR No.</td></tr>
<tr><td colspan="3">System</td><td>Date</td><td>Drafted
/revised</td></tr>
<tr><td colspan="3">Subsystem</td><td colspan="2">Phase</td></tr>
<tr><td colspan="5">Hazard Title</td></tr>
<tr><td colspan="3">Applicable Safety Requirements</td><td colspan="2">Hazard classification

Severity :
☐ I ☐ II ☐ III ☐Ⅳ

Likelihood of occurrence :
☐A ☐B ☐C ☐D ☐E</td></tr>
<tr><td colspan="5">Description of the Hazard</td></tr>
<tr><td colspan="5">Hazard Causes</td></tr>
<tr><td colspan="5">Hazard Controls</td></tr>
<tr><td colspan="5">Safety Verification Methods</td></tr>
<tr><td colspan="5">Status of Verification</td></tr>
<tr><td>Approval</td><td>Contractor</td><td>JAXA Section in Charge</td><td colspan="2">JAXA/Safety Div.</td></tr>
<tr><td>Phase I</td><td></td><td></td><td colspan="2"></td></tr>
<tr><td>Phase II</td><td></td><td></td><td colspan="2"></td></tr>
<tr><td>Phase III</td><td></td><td></td><td colspan="2"></td></tr>
</table>

Table 4.3.4-2 (2/2) Hazard Report Form (2)

Hazard Report (continued)	HR No.
System/Subsystem	

4.4 Documentation and safety data

The following documents shall be developed to implement this Standard. Documents and safety data shall be recorded and managed to be available at any time.

Documents and safety data shall be maintained as latest condition to be shown to system safety program manager and be used to prevent defects having repetitive features and to confirm compliance with detail requirements associated with safety, by feedback to all of related departments

Documents and safety data shall also be stored as safety data for future reference.

Table 4.4-1 Deliverable Documents

Document Title	Applicable Item No.
System safety program plan	4.2.1
Safety data package	4.2.4 (4)
Hazard identification summary*	4.3.4
FTA,SCA,ETA,etc (as necessary)	4.3.3
Hazard analysis table*(as necessary)	4.3.3
Hazard report*	4.3.4
Safety requirement compliance matrix	4.2.4-1
Safety verification tracking log (as necessary)	4.2.2 (4)
Noncompliance Report (as necessary)	4.2.5
Required data for series/reflight payload	4.2.6
Safety review implementation plan	4.2.4 (3)
Education and training plan	4.2.7
Education and training implementation/participants record	4.2.7
Mishap report/"hiyari-hatto" report (as necessary)	4.2.8

Note) * : Keep updated to the latest status from the early stage of design to utilize as a tool for safety design. The latest versions shall be compiled into the safety data package of each phased review.

5. SAFETY DESIGN REQUIREMENTS

For payloads and ground facilities/equipment, domestic (Japanese) laws shall be applied, and the following safety design requirements shall be met.

5.1 General Requirements

This document specifies generic and common safety design requirements. Additional requirements shall be applied if necessary as a result of hazard analysis based on Chapter 4.

5.1.1 Basic requirements for safety design

Failure Tolerant (FT) design shall be applied for safe design of a payload. When the verification data to make an appropriate design on the basis of section 5.1.1.4 can be indicated, Design for Minimum Risk (DFMR) can be applied.

When FT design cannot be applied and DFMR is not practically possible, Probabilistic Risk Assessment (PRA) may be acceptable. Note that a contractor is required to adequately coordinate with JAXA safety section to use PRA.

5.1.1.1 Order of precedence for safety design

Order of precedence for safety design shall be as follows:

(1) Elimination of hazards.

(2) Design to minimize hazards.

(3) Design to control hazards.

(4) Use of safety equipment.

(5) Use of protective equipment.

(6) Use of warning systems.

(7) Hazard controls using special procedures and trainings.

Note) (3) through (7) are collectively referred to as hazard controls.

5.1.1.2 Fault tolerance design requirements

Design shall satisfy the following fault tolerance requirements to lower the likelihood of hazardous event occurrence to the acceptable level by controlling failures and human errors according to the severity of hazard due to the failures and human errors:

(1) Control of catastrophic hazards

Payloads shall be designed to ensure that no two faults, human errors, or combination of fault and human errors may result in a catastrophic hazard ~~death or severe injury of third-party, death of personnel, loss of or severe damage to significant public or private property, loss of systems (launch vehicles, payload/GSE) or launch site facilities, and/or irreversible severe environmental damage.~~

(2) Control of critical hazards

Payloads shall be designed to ensure that no single fault or human error may result in a critical hazard ~~minor injury of third-party, severe personnel injury, minor damage to public or private property, severe damage to systems (launch vehicles, payload) or launch site facilities, and/or reversible severe environmental damage. .~~

F

5.1.1.3 Control of hazardous functions

Potential hazardous events caused by inadvertent activation of hazardous functions as a result of system failure or human error shall be controlled according to the severity of the hazard as follows:

(1) Control of Catastrophic Hazard

Functions that have potential capability of causing a catastrophic hazard shall have a minimum of three independent inhibits between the function and energy source. It is preferable that the ground return for the function circuit is controlled by one of the independent inhibits. At least two of the three required inhibits shall be monitored.

(2) Control of Critical Hazard

Functions that have potential capability of causing a critical hazard shall be controlled by a minimum of two independent inhibits between the function and energy source.

5.1.1.4 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 etc. 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 line and fittingss
- Pyrotechnic devices
- Material compatibility
- Material Flammability
- Some mechanisms

5.1.1.5 Failure propagation

(1) Design shall preclude increase of accident possibilities by primary failure or function loss of the equipment and the function, etc. (including those due to human errors) inducing other failures and such.

(2) Safety critical redundant systems which controls catastrophic and critical accidents shall be separated from each other as much as practically possible or protected to prevent compromise of both systems as a result of unexpected common causes or events. Redundant system circuits to prevent a catastrophic accident must use separate connectors.

5.1.1.6 Safety maintenance function

(1) Fail safe and Foolproof.

(2) Multiple control functions for each hazard shall be independent from each other.

(3) Safety shall be maintained until safing is completed in the events of power supply loss, etc.

5.1.1.7 Special procedures

If hazards cannot be adequately controlled by design or installing safety equipment, protective equipment, or warning systems, payloads shall be designed to ensure that the likelihood of hazard occurrence can be reduced by operations. Safety training for personnel, establishment of appropriate operation procedures, and proper maintenance shall be utilized to control hazards.

5.1.2 Requirements for explosive hazardous atmosphere area

5.1.2.1 Explosive hazardous atmosphere area for liquid propellants

The explosive hazardous atmosphere area for flammable liquid propellants including oxidizer shall be defined as follows:

(1) Within 15 m of container or payload tank filled with a liquid propellant.

(2) Within 15 m of liquid propellants vent ducts.

(3) Within 8 m of equipment, ground facility/equipment, and transfer piping filled with a liquid propellant.

(4) Within 31 m of the launch vehicle filled with a liquid propellant.

(5) All areas of an applicable room of building where handling operation of liquid propellant is in processing or liquid propellants are stored, and their air conditioning systems and a room spatially connected with the air conditioning system.

5.1.2.2 Explosive hazardous atmosphere area for solid propellants and pyrotechnics

Within 3 m of a solid propellants or pyrotechnic.

5.1.2.3 Requirements for electrical equipment used in the explosive hazardous atmosphere area

(1) Electric equipment of the payload shall be provided with explosion-proofing measures such as potting, hermetic sealing, pressurization with inert gases or other necessary method, not to become ignition source in normal operation if it is exposed to the explosive hazardous atmosphere. Electric apparatus may be approved as an explosive protected device if it does not have sufficient electrical capacity and it could not be an ignition source at below the ignition limit of an explosive gas. It shall be consulted with JAXA for detail.

(2) Electrical equipment of GSE used in the explosive hazardous atmosphere area shall be explosion-proofed. Requirement for the explosion-proof equipment shall be referred to related law, such as Ordinance on Industrial Safety and Health, Constructional Requirements for Electrical Equipment for Explosive Atmospheres, Recommended Practices for Explosion-protected Electrical Installations in General Industries, Ministerial ordinance which determines technical standards on electrical installations, and etc. On applying the above regulations, payload operator shall consult with JAXA System Safety Review Panel.~~Sample of explosion-proof requirements for electrical equipment are described in Appendix II~~.

(3) When the requirement in (2) above cannot be met and use of GSE electrical apparatus is essential in the explosive hazardous atmosphere area, use of an explosion-proof room (pressurized room) that has 25 Pa (2.5 mm H_2O) or greater pressure differences than the explosive hazardous atmosphere area, shall be planned and specified in the operation procedures. If the inner pressure is reduced to below that pressure, warning shall be automatically issued.

(4) When the requirement in (3) above cannot be met for a temporarily used device, leakage detectors may be installed in the explosive hazardous atmosphere area, and the monitoring stations may be provided outside the explosive hazardous atmosphere area. The monitoring

stations shall have master switches that can manually or automatically turn off all non-explosion-proof electrical equipment located in the applicable area. When turning off manually, required trainings shall be conducted.

5.1.3 Materials used

The following describes general requirements for materials used in payloads/GSE.

(1) General requirements

Materials shall be evaluated for their characteristics such as mechanical, fractural, flammability, reactivity, harmfulness, compatibility, static-discharge, etc., by test or other methods prior to use, if their material characteristics are not well known.

(2) Harmful materials

Materials such as paintings or adhesives that generate harmful gases in the atmosphere or water under the ground operating environments shall not be used. The use of mercury and mercury compounds shall be prohibited. The use of harmful materials shall be minimized, and necessary treatments shall be taken.

(3) Flammable/combustible materials

The use of flammable/ combustible materials shall be minimized, and those materials shall be used at the appropriate location. Materials that will not easily burn by ignition shall be used.

(4) Electrostatic materials

Materials shall not be charged with electrostatic not to become ignition sources of pyrotechnics or propellants, or not to cause electrical shock to personnel.

(5) Other harmful materials

The contractor shall consult with JAXA for implementation of followings:

a. The experiment payloads/GSE using flammable liquids such as liquefied methane or alcohol shall be designed to prevent the liquids from causing fire.

b. Microbiological experiments payloads using pathogenic bacteria, etc. shall be designed to prevent contamination in any kinds of conditions by sealing containers or compartments and to protect personnel from contacting with the pathogenic bacteria, etc.

c. Life support systems for primates and vertebrate shall be provided with an excrement disposal system to prevent contamination.

d. Biological experiment payloads/GSE shall be designed to allow the removal of dead bodies, etc. to prevent contamination, as well as specific embalming methods.

e. To safely store harmful materials, etc., preservation and storage shall be considered.

5.1.4 Payload flight termination / destruct system installation requirements

(1) When determined to be necessary for safety after coordination with JAXA, a flight termination or destruct system shall be installed on payloads.

(2) The flight termination or destruct system installed on the payload shall be activated by a destruct command sent from the launch vehicle.

(3) Safety design requirements for pyrotechnics related to the flight termination or destruct system installed in payloads shall comply with paragraph 5.5.

5.1.5 Sharp edge

Sharp edges of equipment shall be removed or covered for personnel safety.

5.1.6 Bolt length

Bolts shall be in appropriate length for personnel safety or prevention of interference with other installed equipment.

5.1.7 Prevention of charging

All conducting metal items which are subject to charging shall have a mechanically secure conductive connection to conductive structure. The resistance of the connection shall be less than 1 ohm. Conducting nonmetal items shall have appropriate prevention of charging.

5.2 Structural/mechanical system

5.2.1 Structural analysis

Structural analyses shall be performed for all payload structures to prove that all design factors including strength, stiffness, structural stability, and fatigue limit are satisfied with anticipated loads and environmental conditions. Structural analysis shall include static and dynamic stress analysis and vibration analysis.

5.2.2 Structural design

(1) Following transportation and handling loads shall be considered in payload structural design in addition to the loads applied to payloads during launch and test:

a. Loading and unloading payloads to and from a transportation vehicle.

b. Loads during transportation and moving operation.

(2) All fittings including those used for transportation and handling shall be sufficiently examined for strength and installation methods to clearly specify handling procedures, such as appropriate fastening torque, etc.

5.2.3 Mechanism design

(1) Any payload equipped with movable mechanism such as docking manipulators, scanning antennas, and paddles that may be separated, deployed, expanded, or rotated shall be designed to prevent inadvertent movement during transportation, inspection, handling and launch at the launch site.

(2) The working range of the all movable parts defined in (1) above shall be specified in the interface drawings, launch site operation procedures and other appropriate documents, assuming inadvertent movements.

(3) When using pyrotechnics to release a locking mechanism, the requirements specified in paragraph 5.5 shall be applied.

5.3 Propulsion System

Propellants and other physically or chemically hazardous fluids of the payload shall be used within systems that have been specially designed in accordance with following requirements. Structural design of propulsion system shall be in accordance with the requirements of paragraph 5.2, and design as pressure system shall in accordance with the requirements of paragraph 5.4.

5.3.1 Liquid propellant system

5.3.1.1 Materials

(1) Materials of systems containing hazardous fluids (including seals, lubricants, etc.) shall be compatible with the fluids used under expected operating conditions such as pressure, impact, vibration, and temperature.

(2) Particular attention shall be given to hydrogen embrittlement for systems using hydrogen.

(3) Materials that may be susceptible to low-temperature embrittlement under the operating environment shall not be used.

(4) Materials with high fracture toughness and slow crack propagation rate shall be selected.

(5) Materials such as aluminum alloys where their screw threads are easily destructible shall not be used for fitting that are frequently and repeatedly connected and disconnected.

(6) Appropriate corrosion prevention measures shall be taken.

(7) Materials with a potential for contacting with hazardous fluids in case of leakage shall be nonflammable.

5.3.1.2 Strength

Engines/thrusters shall not yield (excluding the local yields) or undergo detrimental permanent deformation at the load 1.1 times the Maximum Expected Operating Pressure (MEOP) nor burst at the load 1.25 times the MEOP under the expected operating environments. Other portions of the propulsion systems subjected to pressure shall meet strength requirements of paragraph 5.4.

5.3.1.3 System design

(1) Propellant leakage and inadvertent mixture of propellants shall be prevented.

(2) Systems that contain incompatible fluids shall be designed to avoid mixture of the fluids (e.g. oxidizing propellants and fuels, or breathing air and harmful fluids). In particular, connecting portion shall be designed to prevent misconnection and leakage.

(3) For each type of piping, the number of fitting shall be reduced as small as possible to minimize the possibility of leakage.

(4) Inert gases used to pressurize propulsion systems that could be contaminated by propellants shall not contact with contaminating materials or incompatible systems.

(5) Systems using cryogenic fluids shall be designed to avoid clogging at any part of circuits. Thermal insulation shall be installed, if necessary.

(6) Tanks, pressure lines, etc. containing hazardous fluids shall be designed to be cleaned, and purged with an inert gas after use, and may be verified to ensure that cleanliness and contamination levels are below the pre-defined level. This pre-defined level shall be determined considering harmfulness.

(7) Systems using a hazardous fluid shall be able to be pressurized at a blanket pressure using inert gas to maintain cleanliness and prevent outside air from entering.

(8) Components that can be assembled in reverse or that are specified a specific type of fluid shall be clearly identified to prevent from incorrect assembly or the use of a wrong fluid.

(9) Tanks and vessels containing cryogenic propellants shall have pressure relief devices.

(10) All seals and valves used under cryogenic conditions shall not freeze up.

(11) For remote control valves, normal-open or normal-close types of valves shall be selected to automatically recover to the safe position when they lose control power.

(12) Payload shall ~~be able to unload propellants~~ be designed so that propellants can be unloaded safely in case of contingencies, ~~such as like~~ propellant leak from the payload ~~while on the launch vehicle~~

(13) If engines and thrusters have gimbal actuators, mechanical limiters shall be provided to prevent the actuators from exceeding the pre-defined angle.

(14) Engines and thrusters shall be designed to maintain sealing capability against rapid changes in temperature and/or pressure.

(15) In order to prevent hazards due to outflow/leakage of hazardous fluid to the outside, a leakage prevention means, having enough fault tolerance corresponding to the hazard analysis result for the outflow path (leak path), should be secured. In addition, a design with two or more seals in one valve is recognized as a system with two inhibits. ~~Propellant shall not be released to outside only with an operation of one valve. Payload shall have at least three seals for an internal leakage from the valve.~~

(16) The propellant loading/unloading operation shall have enough number of independent controls according to the hazard analysis results.~~Propellant supplying shall be controlled by circuit having at least three independent electrical inhibits.~~

(17) Waste fluids requiring to render harmless shall be collected, through GSE, in a reservoir tank that is capable of neutralizing and draining them. If this is not feasible, they shall be collected in a portable container that is capable of filling the waste liquids into special disposing equipment.

(18) Exhaust gas of hazardous fluid shall be collected in a vent. If environmental contamination is expected at the downstream of the vent, the exhaust gas shall be neutralized or diluted prior to disposition. Vents shall be designed in accordance with the following:

a. Vents shall have sufficient dimensions to accommodate the anticipated volume of exhaust gases to be disposed.

b. Exhaust gases from vents shall not cause any hazard to persons. The terminals of the vents shall be clearly identified.

c. Separate vents shall be provided for incompatible fluids.

d. Systems that drain two or more hazardous fluids from the same vent shall be protected from clogging, reverse flow, or contamination affected by the other system.

e. If an existing vent system at the launch site is used, the discharge rate shall be controlled within the handling capacity of the vent.

5.3.1.4 Electrical requirement

(1) Appropriate measures shall be provided for electrical equipment not to cause explosion of explosive gases when the gases are present surrounding the equipment. If required, explosion-proof provision, such as potting or pressurization by an inert gas shall be provided.

(2) Electrical bonding resistance between metal enclosure of all electrical equipment and their metal mounts, between the mounts and the payload metal structure, and regarding non-electrical metal parts, shall be as follows:

a. 10 mΩ or less between the equipment enclosure and supporting metal structure, including cumulative effect of all faying surface interfaces.

b. 15 mΩ or less between the cable shields and the equipment enclosure, including cumulative effect of all connector and accessory interfaces.

c. 2.5 mΩ or less across individual faying interfaces within the equipment, such as between sub-assemblies or sections.

d. 1 Ω or less between parts made of conductive material and between those parts and the payload's conductive structure.

If payload cannot comply with above requirements, contractor shall document rationale for particular bonding resistance, and shall be accepted by JAXA.

(3) Electrical components shall meet the requirements of electromagnetic compatibility (EMC) specified in MIL-STD-461 “Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference.” If payload cannot comply with above requirements, contractor shall document rationale for particular EMC, and shall be accepted by JAXA.

(4) Operations of propellant supply valves shall be in accordance with requirements of paragraph 5.3.1.3 (16).

5.3.2 Solid-rocket motor

Solid-rocket motors cannot be verified for their functions prior to use, because solid rocket motors are a typical one-shot system that uses an explosive as the propellant. Therefore following safety features shall be considered, during the design phase.

5.3.2.1 Materials

Component materials shall comply with the following requirements, in addition to those in paragraphs 5.3.1.1 (3) through (6):

(1) Combustible materials shall not be used at high-temperature portion of solid rocket motors or near their peripherals. If combustible materials must be used, they shall be thermally insulated.

(2) Materials that may generate electrostatic discharge shall not be used for pyrotechnics.

5.3.2.2 Strength

(1) Motor shall have enough strength to withstand the limit load without any detrimental permanent deformation.

(2) Motor shall have enough strength to withstand the ultimate load without damage such as buckling.

(3) Yield load of combustion chamber shall have safety factor of 1.1 or more against the combined loads considering the maximum expected operating pressure and the maximum flight load. Ultimate load shall have safety factor of 1.25 or more against the above combined loads.

(4) Proof test pressure must be 1.05 times or more of the maximum expected operating pressure.

(5) Strength of the constructed materials shall be used A value or B value of MIL-HDBK-5 “Metallic Materials and Elements for Aerospace Vehicle Structures” for the metallic materials, or the value of MIL-HDBK-17 Part II “Plastics for Aerospace Vehicles Transparent Glazing Materials”. In the case of using other materials, equivalent test shall be performed and the obtained test data shall be used.

5.3.2.3 Electrical requirements

(1) Electrical equipment of solid rocket motors shall comply with the EMC requirements of MIL-STD-461. If equipment cannot comply with above requirements, contractor shall document rationale for safety, and shall be accepted by JAXA.

(2) Electrical bonding resistance between metal enclosure of all electrical equipment and their metal mounts, between the mounts and the payload metal structure and regarding non-electrical metal parts, shall be as follows:

a. 10 mΩ or less between the equipment enclosure and supporting metal structure, including cumulative effect of all faying surface interfaces.

b. 15 mΩ or less between the cable shields and the equipment enclosure, including cumulative effect of all connector and accessory interfaces.

c. 2.5 mΩ or less across individual faying interfaces within the equipment, such as between sub-assemblies or sections.

d. 1 Ω or less between parts made of conductive material and between those parts and the rocket motor's conductive structure.

If payloads cannot comply with above requirements, contractor shall document rationale for particular bonding resistance, and shall be accepted by JAXA.

(3) Grounding wire shall be capable of connection to any single point of solid rocket motor to establish electrical grounding during ground handling and transportation.

5.3.2.4 Handling and transportation

A solid rocket motor shall have a single grounding point with a metallic container during transportation, and have a single grounding point during handling operation.

5.3.2.5 Solid propellants

(1) Selection of propellants

a. Stability

Solid propellants shall be safe under all expected environmental conditions, and quality of the solid propellants shall not be degraded from specification during the required service life period.

b. Characteristics

For selection of solid propellants, characteristics shown in paragraph (4) below shall be considered.

(2) Mechanical strength characteristics

Adhesion strength between the propellant and the insulation and between the insulation and the motor case shall sufficiently withstand all distortions due to expected environments such as thermal condition.

(3) Deterioration resistance

a. Materials that could deteriorate below the specified propellant's performance level during service life shall not be used.

b. Cohesion between the insulation and the propellants shall have required physical characteristic during service life.

(4) Safety characteristics

Before the solid rocket motor development program proceeds, tests and analysis shall be conducted to acquire the following characteristics of propellants:

a. Impact sensitivity

Impact sensitivity of propellants shall be below the acceptable level.

b. Friction sensitivity

A cured propellant shall have low friction sensitivity, and shall not be ignited during normal handling operations.

c. Spark sensitivity

Spark sensitivity shall be low so as not to be ignited by sparks due to ordinary electrostatic discharge of a human body.

d. Spontaneous ignition sensitivity

The propellant shall have high ignition point and shall not be ignited spontaneously in temperature conditions to which the propellant will be exposed. Internal heat generation due to chemical reaction of either curing or deterioration shall not produce strong heat that causes spontaneous ignition.

e. Detonation

Propellants shall not cause detonation due to impact under the expected conditions.

f. Toxicity

Propellants shall not produce volatile gases exceeding allowable concentration.

5.3.3 Ion engines

5.3.3.1 General

(1) Ion engine units shall be stored and handled to meet the conditions required for their operations in vacuum.

(2) Handling and storage conditions for gaseous propellants shall be clearly defined.

(3) When liquid propellants are used, paragraph 5.3.1 shall be applied.

(4) When using harmful propellants, safety shall be considered in the design.

5.3.3.2 Materials

Materials used for propellant storage and supply systems shall be compatible with the propellant and fluids used.

5.3.3.3 Strength

(1) Structures shall not cause permanent deformation for limit loads.

(2) Ultimate loads for the structure shall be equal to or greater than 1.25 times of the limit loads.

5.3.3.4 Electrical requirements

(1) Controllers shall not actuate shut-off valves of the propellant storage and supply systems when electric power is turned on.

(2) Any part that is applied high voltage shall be protected from contacting with other parts.

5.3.3.5 Handling and transportation

(1) Gas replacement prior to propellant loading shall be conducted without decreasing the purity of propellants in the system.

(2) Propellant loading procedures and methods of handling and storage shall be clearly specified.

(3) The protection of electrodes for ion thrusters, the cleanliness in the propellant storage and supply systems, etc. shall be maintained during handling and transportation.

5.4 Pressure System

5.4.1 General requirements

(1) High Pressure Gas Equipment shall be designed in accordance with paragraph 2.1 (1) JERG-0-001 “Technical Standard for High Pressure Gas Equipment for Space Use”. Pressure component that needs to be applied “Industrial Safety and Health Law” shall be in accordance with the law.

(2) Pressure systems shall be designed to maintain in safe conditions at all times during nominal operations (combustion test or countdown) of the systems or when the procedures are paused or incorrectly executed.

(3) Regulator systems equipped with high-pressure tanks shall have pyro valves that are actuated after separation of the payload from the launch vehicle or valves with high or equivalent reliability for unintended operations or internal leak.

(4) Shutoff valves shall be installed as closely as possible to the downstream outlet of pressure vessels or downstream of pressure relief devices when it is provided.

(5) Parts that have a direction for installation shall be designed to avoid being installed in reverse, or shall be clearly identified to avoid incorrect assembly.

(6) Electrical systems related to the pressurized systems shall be designed not to cause ignition during nominal operations, and not to be affected by condensation of gas or vapor from the pressurized systems.

(7) Operational requirements

The following requirements for operating the pressure systems shall be reflected in their design:

a. Systems shall be capable of being monitored from the operation site to check for any anomaly and, if any, its status together with necessary control.

b. Payload shall be able to unload propellants safely in contingency like propellant leak from the payload while on the launch vehicle.

c. For assembly, test or replacement of the equipment associated with pressure vessels, pressure vessels shall be designed to vent the internal fluids

d. Tank, pressure line, etc. shall be designed to be confirmed their contamination/cleanness level is under pre-defined level, and those could be purged by inert gas, if necessary. This pre-defined level shall be considered harmful effect.

5.4.2 Pressure relief devices

Pressure relief devices shall be installed on systems if the system has a pressure source that may exceed the MEOP of the system and its pressure may destruct the components, or if malfunction of a part that causes to exceed MEOP may destruct other part.

(1) Pressure relief devices shall relief the pressure not exceed 110 % of MEOP of systems.

(2) Pressure relief devices shall be installed at as closely as possible to downstream of the pressure source or pressure vessels. However, pressure relief devices may not be required if the system is isolated by pyro-valves or equivalent valves (refer to 5.4.1(3)) that are actuated after separation of the payload.

5.4.3 Quick disconnect (QD) coupling

QD coupling shall meet the requirements of the following:

(1) QD shall have sealing capability under the un-mated conditions in any system pressure

range.

(2) QD shall be designed to minimize the possibility of de-mating or external leakage due to the loads of lateral direction or flow direction under the mated condition.

(3) Hydraulic QD shall be designed to minimize air ingress during QD mating/de-mating.

(4) QD shall be automatically locked during QD mating, and shall be visually inspected its lock/unlock condition easily.

(5) QD shall be designed to avoid mismating.

5.4.4 System layout, etc.

Safety critical equipment shall be arranged to allow the monitoring and operation from a location where safety of personnel is ensured. Pressure systems including GSEhall be designed to allow monitoring from their operating site in the event of hazardous situation. Systems using hazardous fluids shall be located a sufficiently safe distance from personnel or other systems under the pressure loaded conditions.

5.4.5 Hydraulic systems

5.4.5.1 Safety design considerations

(1) Safety devices

Hydraulic systems shall have appropriate relief valves and system vent lines to withstand the MEOP and protect their components.

(2) Temperature control

Appropriate cooling systems shall be provided to hydraulic systems in order to prevent occurrence of nonconformance due to the embrittlement of sealing, carbonization and degradation of hydraulic fluid, valve or servo malfunctions, etc. In addition,fluid temperature shall be visually checked using a thermometer or other means as necessary.

5.4.5.2 Selection of components and hydraulic fluid

(1) Selection of materials

a. Materials shall be selected to prevent reaction between the materials and fluid.

b. When using materials which characteristics are not well known, its compatibility with applicable fluids shall be confirmed by an appropriate test or other means prior to use.

(2) Pressure adjustment

If power-driven hydraulic pump is used, its pressure shall always be regulated to preclude excessive pressure.

(3) System components

System components shall be designed to preclude creating sharp angles or abrupt cross-sectional changes. If this is not possible, the components shall be designed to maintain stress below the limit where stress corrosion of the materials occurs.

(4) Electrical circuits

Electrical circuits shall be installed at the place as far as possible from high-pressure components.

(5) Flexibility

When connecting two sections that are in relative motion, coil tubes, swivel joints, or flexible hoses shall be used.

(6) Selection of hydraulic fluids

Non-flammable (or fire-proofed) fluids shall be used.

5.4.5.3 Bleeding

If necessary, bleed valves shall be installed in the system at a place where air or gases can be properly released. Bleed valves shall be installed at a place where personnel is protected from contacting with fluid that flows out of the valves when activated.

5.5 Pyrotechnics system

5.5.1 General requirements

For designing pyrotechnic systems, special attention to safety design shall be required to prevent destructions, contamination, or ignition of the perimeter equipment due to fragments or other released objects caused by activation, and electro-explosive devices from causing inadvertent ignition. Because pyrotechnics are one-shot items and their function cannot be verified prior to use, confirmation of safety shall be thoroughly performed during design phase.

5.5.1.1 Classification

All pyrotechnics shall be classified as Category A or B on the basis of the following criteria.

(1) Category A

Pyrotechnics that could cause a hazard ~~injury or death of person, damage to JAXA properties such as launch vehicles or facility, payload/GSE or third parties' properties~~ due to a series of events caused by the pyrotechnic energies or pyrotechnics~~. For example,~~ Electro Explosive Device (EED) for firing solid rocket motor, stage separation, and flight termination system, etc. are typical examples of Category A pyrotechnics.

(2) Category B

Pyrotechnics that could not cause a hazard ~~injury or death of person, damage to JAXA properties such as launch vehicles or facility, payload/GSE or third parties' properties~~ due to a series of events caused by the pyrotechnic energies or pyrotechnics. For example, the pyrotechnics unit, purchased as built, which unintended firing does not result in an accident even for the worst case, is a category B unit. F

5.5.1.2 Others

(1) Pyrotechnics firing circuits shall be capable for stray voltage checking prior to electrically connecting. The result of checking shall not exceed 1/10 of the maximum no-fire current or 50 mA, whichever lower. This check, in the first, can be conducted with all powers ON under the equivalent condition to the final launch electrical configuration. In the second, this check can be conducted with all powers OFF, immediately prior to connecting pyrotechnics.

(2) Category A pyrotechnics locations shall be where pyrotechnics can be installed as late as possible in the tests after delivery to a launch site. The locations shall also be accessible for firing circuits wiring as late as possible in the countdown process.

If pyrotechnics cannot comply with above requirements, but in case pyrotechnics is considered as category A only after containing payload in the fairing, contractor shall document rationale and after accepting by JAXA, pyrotechnics may be installed and finally wired at latest period otherwise specified above.

5.5.2 Category A electro-explosive device

(1) The EED shall have the following tolerance characteristics. “No-fire” described herein means that the ignition level is 0.1 % at 95 % of confidence level determined by Bruceton test or equivalent statistic test methods.

a. The EED shall not cause fire or malfunctions when 1A DC is applied for five minutes without an external shunt.

b. The EED shall not cause fire or malfunctions when 1W DC is applied for five minutes without an external shunt.

(2) The EED shall be a single bridge that provides sufficient insulation between the bridge wire and the case to preclude electrostatic discharge around the igniters, considering that human beings could become medium of charge generating. When double bridge wires must be used, a sufficient insulation shall be provided between the bridges. The bridges shall be hermetically sealed to protect them from environmental conditions.

(3) The EED shall not result in nonconformance although discharge of 25 kV from a 500 pF capacitor applied between pin-to-case directly, and applied between the pin-to-pin with a 5000Ω resistance connected to capacitor in series.

(4) The EED main body shall not rupture or produce fragment when operated. Main body (outer case) of EED shall be made of metal or conductive materials.

(5) Carbon bridge wires shall not be used for EED.

(6) Insulation resistance between the pin-to-case shall be equal to or greater than 2 MΩ at 500 VDC.

(7) Explosives and other substances used for the EED shall not be degraded, decomposed, or chemically changed throughout the EED’s service life.

(8) The EED shall not result in spontaneous ignition at either higher temperature condition of 120°C or + 30°C of the maximum expected temperature . If decomposition and deterioration of EED may affect safety, decomposition and deterioration shall not occur under the high temperature environment where temperature range of the–10 degrees Celsius of minimum expected temperature to + 30 degrees Celsius of the maximum expected temperature. The expected temperature shall be pre-defined, considering the worst case.

(9) Shielding caps

a. Shielding caps shall be provided and placed on the EED during transportation, preservation and storage, handling, and installation until the EED is connected to the connectors.

b. Outer shells of shielding caps shall be made of conductive material that provides asan Radio Frequency (RF) shield and makes electrical contact with the EED case.

c. The mating surface between the shielding cap and the EED case shall have no RF gap around the full 360-degree circumference.

d. Shielding caps shall be designed to allow for installation of the EED without removing shield caps from EED. A special torque wrench shall be provided if necessary. When this requirement cannot be met, the contractor shall document that removing shielding caps does not present any safety issue and submit it for JAXA approval.

e. Shorting plugs (caps) shall not be used as a substitute for shielding caps. JAXA’s approval is required for the use of shorting plugs (caps) without shield caps. If shorting plugs (caps) are placed on the EED itself, they shall short-circuit between pin-to-pin and between pin-to-case.

5.5.3 EBW (Exploding Bridge Wire device) and Laser Initiated Device

When using EBW or Laser Initiated , contractor shall consult with JAXA.

5.5.4 Safe & Arm devices

Safe & Arm (S&A) devices shall be provided for Category A firing systems that are used for solid rocket motors or flight termination/destruction system, except for EBW specified in paragraph 5.5.3.

(1) S&A devices shall be electromechanical Safe and Arm devices that have electrical and mechanical safety mechanism.

(2) At the safe position, initiators shall be short-circuited inside the devices, and the explosive train shall be interrupted by mechanical barriers.

(3) At the armed position, firing circuits for initiators shall be connected inside the devices, and mechanical barriers for the explosive train shall be removed.

(4) Switching to the safe and arm positions shall be accomplished by remote control.

(5) Armed and safe position can be monitored by a remote status monitor and also by visual check.

(6) A mechanical lock (safety pin) shall be provided for locking the devices at the safe position to prevent inadvertent transition from the safe position to arm position. The safe position shall be maintained by insertion of safety pins. S&A devices shall be accessible from outside of vehicles as much as possible, considering that safety pins should be removed as late as possible of pre-launch operations.

(7) S&A devices shall be provided with a function to release ARM manually in case of contingency in the ARM position, but shall not be transferred manually to ARM position.

(8) For firing circuits of S&A devices, control circuits and monitoring circuits shall be completely separated, and non-interchangeable connectors shall be used for them.

(9) When resistors is connected to firing circuits for electrostatic discharge, its resistance shall be equal to or greater than 25kΩ.

5.5.5 Power supply

(1) RF energy shall not be used as a power source to fire the EED.

(2) Except for Flight Termination and Destruction Systems, dedicated batteries shall be required for EED subsystems. However, power supply busses that are properly insulated and isolated may be acceptable without dedicated batteries. Isolated power supply bus means a bus line that supplies power exclusively to the EED subsystem, and not to supply power to other loadings.

(3) Ignition circuits shall be designed not to generate sneak circuits or unintentional current leak path due to failure of return circuits and switches.

(4) If loss of power supply or loss of signal could result in injury to person or damage to safety critical systems, redundant circuits shall be provided.

5.5.6 Shields

(1) Firing circuits shall be completely shielded, or at least shielded from the EED to a point where filters or absorptive devices are located to prevent RF from entering into the shielded portion of the system.

(2) RF shielding shall provide a minimum of 85 % of optical coverage ratio. Note that a solid shield rather than a mesh would have 100 % coverage.

(3) Shields shall provide equal to or greater than 20 dB attenuation against the maximum no-

fire power of pyrotechnics, for all expected RF frequency spectrums that comes from launch vehicle (including the launch site) interface conditions and payload/GSE, regardless of the impedance of the power supply or load. Since the maximum no-fire power of pyrotechnics varies depending on the RF frequency and radio wave format, the evaluation should consider the RF environment at the launch site.

(4) Shielding, including termination at the connectors' back face, shall not have any gaps or discontinuities. Connectors shall not reduce shielding capabilities provided by the shielded cables.

(5) Shields terminated at connectors shall be electrically jointed around the full 360° circumference without any gap.

(6) All physically connected metal interfaces in EED and its shielding for a firing system shall be bonded with a DC resistance of equal to or less than 2.5 mΩ. Interface between EED system metal surface and body ground shall be 1Ω or less.

(7) Firing circuits and control circuits shall be shielded from each other. When using electrical parts (semiconductor relays, etc.) which cannot provide electrical isolation to the pyrotechnics ignition circuit or control circuit , effective measures according to its characteristics shall be applied.

5.5.7 Circuits

(1) Firing circuit shall be designed so that final connection between the EED and firing circuits can be performed at the connectors as closely as possible to the EED.

(2) Category A EED firing circuits that do not use S&A devices or EBWs shall have switches, ARM/SAFE plugs, etc., that isolate pyrotechnics from the power supply, with at a place as closely as possible to the EED. ARM plugs (flight plugs) shall be installed at an appropriate location accessible from the outside of the fairing.

(3) Twisted shielded pairs shall be used for wiring in the firing circuits. Splicing of wires or overbraid shields shall be prohibited.

(4) Firing circuits containing EEDs shall be isolated from the EED case and other conductive parts. If a circuit is required to be grounded, there shall be only one interconnection (single point ground) with other circuit. This interconnection shall be at the power source only. Using static bleed resistors of equal to or greater than 10kΩ may be acceptable for single point ground.

(5) Ungrounded circuits that may build up electrostatic charge shall be electrostatically grounded to a structure using static bleed resistors of at least 10kΩ or greater.

(6) EED subsystems shall be designed to prevent unexpected or unintended path due to ground short or nonconformance of solid-state switches, etc.

(7) All insulation resistances shall be equal to or greater than 2 MΩ at a minimum of 500 VDC.

(8) Firing circuits shall be independent from other electrical circuits. In addition, firing circuits contained in distribution boxes shall be independent by separating it from other circuits.

5.5.8 Connectors

(1) Connectors shall be the plug-receptacle type.

(2) Outer shells of connectors shall be made of good conductive metals such as aluminum.

(3) Connectors shall be selected to eliminate the possibility of incorrect mating.

(4) Connectors shall be the self-locking type. Other than self-locking type connectors, lock wiring or other adequate means shall be used to prevent demating.

(5) Connector pins shall be appropriately assigned such that no current exceeding 1/10 of the maximum no-fire current of EED or 50 mA, whichever lower, is generated due to any short-circuits caused by bent pin or contamination.

(6) Only one wire shall be connected to one pin. Connector pins shall not be used as terminals or tie points.

(7) Spare pins shall not be provided for connectors where broken pins may adversely affect firing circuits or control circuits as a safety standpoint.

(8) Separate connectors shall be used for circuits in redundant systems.

(9) Source circuits shall terminate in a connector with female contacts.

(10) Connectors which handle electric firing circuit signals shall be independent from other connectors.

5.6 Electrical system

5.6.1 General requirements

Electrical systems shall be designed in accordance with paragraph 5.1.1.3 and the following:

(1) Safety critical electrical circuits shall not be affected by other circuits or shall not affect other circuits.

(2) Safety critical electrical circuit shall be independent from others.

(3) Electrical equipment and circuit used in explosive hazardous atmosphere area shall be in accordance with section 5.1.2.3.

(4) Safety critical system shall have a design feature to prevent malfunction due to transient change of power supply.

(5) Safety critical system shall have a design feature to prevent malfunction due to momentary power interruption.

(6) Electromagnetic valves shall have a design feature to prevent malfunction due to regenerative electric current from coils.

(7) Appropriate protections shall be provided to prevent electric shock.

5.6.2 Connector

(1) The followings or other methods shall be taken to prevent mismating of connectors.

a. Plugs and receptacles shall be clearly marked or identified with symbols.

b. Plugs and receptacles shall have a shape or a keyway arrangement that is incompatible with nearby plugs to prevent mismating.

(2) As a rule, source circuits shall terminate in a connector with female contacts. Contact resistance between contact and pin while connected shall be reduced to as low as possible.

(3) Connectors used in hazardous environments shall have a system function that is capable of shutting off electrical power before connector is connected/disconnected.

(4) The followings or other methods shall be taken to prevent failure.

a. Back shells of connectors shall be sealed or potted with appropriate materials to prevent insulation failure due to contamination or water. Electrical wires shall be prevented from excessive bending at the fixing portion due to excessive pulling in order to avoid damage from bending.

b. Caps, plugs, covers or other effective means shall be provided to prevent contamination and damage of un-mated connectors.

(5) Connectors used in safety critical circuit shall have locking mechanism. Round shaped connector shall have self-locking mechanism.

(6) When using a locking mechanism that produces torsion force to plugs, receptacles shall be prevented from accidentally rotating during plug installation.

(7) Circuits shall be designed to prevent receptacles or connector located inside or connected to components that contains flammable vapor or liquid from causing explosion due to spark.

(8) Connector pins shall be assigned to prevent short-circuiting of adjacent pins from resulting in a single-point failure. Pins shall also be assigned carefully to ensure that two signals, such as ARM and FIRE signals, which must be operated in series, are not actuated by one signal due to short-circuiting between adjacent pins.

5.6.3 Battery

(1) General requirement

a. Battery cells shall be designed to prevent electrolyte leakage.

b. Battery cells shall be designed to withstand their internal pressure.

c. Battery cases shall be designed to withstand electrolyte substances.

d. Excess space inside the battery case shall be minimized to prevent gas accumulation.

e. Exposed circuit such as relay contact shall not be used inside or near the battery case.

f. Batteries shall be designed to prevent reverse polarity when connecting terminals. Anodes and cathodes shall be clearly identified and marked when using lugs or similar metal fittings.

g. Dissimilar metals that may corrode upon contact shall not be used for connecting the main bus and batteries.

h. The connection between the main bus and batteries shall be protected by proper coating or sealing, etc. to cover terminals and prevent influence of moisture.

i. Types of electrolytes should be clearly indicated on battery cell cases. When it cannot be indicated on a battery case, other methods shall be acceptable. Safe handling procedures shall also be indicated.

(2) Gas permeable battery cell

a. Battery cell shall be designed to minimize leakage of electrolyzed liquids.

b. Wet-cell batteries shall have a proper pressure relief mechanism in each cell.

c. Battery cell shall be designed in consideration of preventing electrolyte from leaking under microgravity conditions.

d. Battery case shall be designed to prevent leakage of electrolyte if pressurized due to overload or an internal short-circuit

e. Vent plugs, when installed, shall be electrically insulated from the cases using proper insulators. Batteries having venting plugs shall have mechanisms to release an accumulated electrolyte (such as porous plugs or stand pipes).

(3) Sealed battery cells

a. Battery cells with 1 MPa or more Maximum Expected Operating Pressure (MEOP) shall be designed in accordance with pressure vessel requirements specified in paragraph 2.1 (1) JERG-0-001“Technical Standard for High Pressure Gas Equipment for Space Use”.(e.g.: nickel-hydrogen battery cell container)

b. Battery cells with lower than 1 MPa MEOP shall have 3.0 or higher Factor of Safety against rupture for the worst inner pressure under nominal operations. Battery cells designed with non-hazardous Leak Before Burst (LBB) shall have 1.5 or higher Factor of

Safety.

c. Sealed battery cells that do not meet the above requirements shall have a pressure relief function that operates at 1.5 times of operating pressure or less.

d. Battery cells shall be demonstrated by test that they can withstand the inner pressure increase due to shorting or an abnormal temperature increase.

(4) Lithium Ion battery (including lithium battery)

~~When using lithium-ion batteries (including lithium battery), contractor shall consult with JAXA.~~

In addition to the above requirements (1) to (3), the following design shall be adopted to prevent ignition and thermal runaway.

a. Design to prevent overcharging.

b. Design to stop charging/discharging when overcurrent occurs due to external short circuit.

c. For internal short-circuiting, take necessary measures including risk minimization design.

F

5.6.4 Circuit protection device

(1) Circuit protection device shall be provided on the power supply side of a subsystem of a payload if any overload in the subsystem can affect other subsystems or other GSE.

(2) A primary circuit and its redundant circuit shall not share the same protection equipment.

(3) Current threshold value and duration of circuit protection shall be selected properly to avoid disturbing the operation of other circuit protection equipment.

5.6.5 Cables and Wires

(1) Through-holes accommodating wiring shall be provided with proper protection measures such as potting and sealing if it is necessary to isolate the inside of electric devices, etc. from the outside to prevent influence of leakage or condensation of flammable gases, vapors or fluids,

(2) Cables, wires and those termination points or fixing portions to connector shall be assembled, arranged and/or fastened so as to minimize stress and to prevent contact with fluid piping, sharp edges and/or sliding surfaces.

(3) Hot stamps shall not be applied to insulators of cables and wires.

(4) Proper shields shall be provided for safety critical systems to prevent failure of other devices, firing of pyrotechnics, damage of communication functions, etc. due to RF radiation from cable or wire. Also, the following design considerations are required:

a. Single or multipoint shield grounds shall be used according to the frequency of the interference signals, length of transmission lines, and relative sensitivity of circuits over high or low impedance fields.

b. Twisted pairs shall be used to reduce electromagnetic coupling below 5 KHz. Highly conductive copper braided shields shall be provided to the twisted pair and shall be grounded to reduce electrostatic coupling.

c. Signal cables used for electrical ignition circuits shall be in accordance with paragraph 5.5.7.

(5) Communications components shall be shielded from electric power components to prevent input of incorrect information to the telemetry data due to incorrect subsystem's status information changed by electrical transient condition.

(6) For power and signal wiring, different cable and wire harnesses shall be used.

(7) Shielding to protect against an induced voltage of 50 KHz or less in frequency shall be connected to all connectors and shall be grounded at one end. Shielding to protect against an induced voltage of greater than 50 KHz shall be connected to all connectors and shall be grounded at both ends.

(8) Wire-to-wire splicing is not permitted. If this is not possible, rationale for acceptability as a safety standpoint shall be documented and shall be approved by JAXA. For wiring of pyrotechnics, splice shall be prohibited. (refer to paragraph 5.5.7)

(9) Single wires shall not be used at a location expected to wire breakage due to bending.

(10) Cable rooting shall be designed in consideration of flexibility and length of cables, protection from damage, and proper space to enable easier connection/disconnection of connectors.

(11) Wire insulation shall meet the requirements related to the ambient environment in which it is used, non-flammability, and chemical compatibility.

(12) If stress due to fastening or bending, etc, could be applied to fluorocarbon resin coated wires, short-circuit caused by damage of coating shall be considered.

5.6.6 Control circuits

(1) Each circuit in the equipment for safety critical redundant systems (multiplex control circuit) shall be independent from others.

(2) Components of safety critical redundant system shall not be routed through common cables or connectors.

(3) Components of safety critical redundant system shall not receive power through the same bus circuits or protection circuits.

(4) Redundancy shall be considered when relays are used in a safety critical control system.

(5) Component having self-test circuits shall indicate actual system response, as well as indicating generation of commands and test signals.

(6) Indicators to monitor system status shall indicate actual responses, such as operation result of commanded device, as well as the status of generation of commands or power consumption.

(7) Control circuits shall have check and verify function for responses of individual circuits.

(8) Safety critical redundant control circuits shall have self-check functions.

(9) Heater circuits that could result in temperature run-away during operation shall be designed to be fail-safe.

(10) Equipment shall be turned to a safe condition in case of shutdown of input, overvoltage or insufficient voltage.

(11) System using heating equipment shall be studied to have manual reset capabilities, and redundant automatic heater shut-off capabilities.

(12) Bleed-down circuits shall be provided for the circuits having capacitors that may discharge current at a hazardous level.

(13) Latching relays and similar circuits shall be designed to prevent inadvertent operation due to transient voltage.

(14) Should heaters be used for thermal control of components, independent circuits shall be provided separately for temperature detection, temperature control, and overheating protection operation.

(15) Electrical and electronic devices that contain or are exposed to flammable gases, vapors or fluids shall be explosion-proofed.

(16) Circuit breakers and switches used to control emergency devices and circuits shall have protective measures against inadvertent operation.

(17) Status monitoring capabilities of the equipment shall not be lost in case of loss of power to the control circuit.

(18) Limits for operating range and function shall be specified in design.

5.6.7 Power circuits

(1) Power system overload protection device shall be capable of protecting the GSE from any damage resulting from malfunction of the power system.

(2) The wiring of the primary electric power bus and that of the redundant electric power bus shall not be routed through a common connector in order to prevent propagation of a failure occurring in the connector.

(3) Except when antenna and transmission units are operating, the outer surface voltage of the RF radiation equipment shall be kept at ground level to prevent personnel injury due to accumulated electrostatic charge or electrostatic charges generated by incorrect connections.

(4) The DC return shall be connected to a single-point ground of the structure.

(5) Payload structures shall be electrically bonded to transfer the maximum current safely to the single-point ground of the payload or other applicable structures.

5.7 RF Radiation system

(1) Systems, subsystems and components shall be designed to have proper Electromagnetic Compatibility (EMC) to prevent malfunction, anomalies and failures due to electromagnetic interference by RF radiation, etc.

(2) Pyrotechnic firing circuits and other important equipment shall be arranged in place and be shielded properly to exclude influence of RF radiation.

(3) Proper arrangement of component locations and shields or establishment of Keep-Out Area to reduce RF level, considering objects to be protected, shall be provided for RF equipment whose electric field intensity and electric power density from RF radiation exceeds the hazardous level for human body. ~~Table 5.7-1,~~ Enforcement Regulation for Radio Law, Ordinance Regulating Radio Equipment, Protection Guideline, Notification, and etc., shall be referred as electromagnetic field intensity for human body. F

~~Table 5.7-1 Electromagnetic Field Intensity to Humans Body (average time of six minutes) Requires Human Protection~~

~~Frequency~~	~~Effective Electric Field Intensity (V/m)~~	~~Effective Magnetic Field Intensity (A/m)~~	~~Electric Flux Density (mW/cm²)~~
~~10 KHz to 30 KHz~~	~~> 275~~	~~> 72.8~~	
~~30 KHz to 3 MHz~~	~~> 275~~	~~> 2.18/Frequency[MHz] (72.8 to 0.728)~~	
~~3 MHz to 30 MHz~~	~~> 824/Frequency[MHz] (275 to 27.5)~~	~~> 2.18/Frequency[MHz] (0.728 to 0.0728)~~	
~~30 MHz to 300 MHz~~	~~> 27.5~~	~~> 0.0728~~	~~> 0.2~~
~~300MHz to 1.5 GHz~~	~~>1.585×(Frequency [MHz])^1/2 (27.5～61.4)~~	~~>(Frequency [MHz])^1/2／237.8 (0.0728～0.163)~~	~~> Frequency[MHz]/1500~~
~~1.5GHz to 300GHz~~	~~> 61.4~~	~~> 0.163~~	~~> 1~~

F

5.8 Ionizing Radiation

Contractor shall consult with JAXA if payloads (including experiment payloads) emitting ionizing radiation or containing radioactive materials such as X-ray or γ-ray generator are used.

If the usage is accepted, the following requirements shall be satisfied.

(1) Radiation generation equipment shall be designed to have shields, interlocks, fail-safe systems and limit switches.

(2) Radiation systems shall be designed to protect personnel, facilities and equipment from exposure to extreme temperatures, high voltage, harmful vapors, harmful gases, or radiation.

(3) Designs shall meet the following requirements for radioactive materials.

a. Radioactive materials shall be completely sealed using materials that are not susceptible to coherent radiation or shall be housed in containers to eliminate detrimental effects due to radiation leakage.

b. Sealing for radioactive materials shall withstand damage resulting from ground or space environments, mishaps or mishandling.

c. Components associated with radioactive materials shall be replaceable without damaging the sealing for the radioactive materials.

(4) The following preventive measures shall be incorporated in design to minimize the risk of radioactive material leakage or influences resulting from leakage:

a. Radioactive materials shall be kept in properly shielded, safe and reliable storage rooms for radiation sources designated by JAXA.

b. Spare shielded containers shall be provided to temporarily store radioactive materials in the case of mishaps.

c. Double shields shall be provided for all components and equipment containing radioactive materials to prevent secondary leakage.

d. Radiation sources for flight systems shall be installed as late as possible in the launch site processing.

5.9 Optical and laser radiation Systems

5.9.1 General requirements

(1) Optical systems shall be designed to prevent eye injuries by beams of hazardous intensity and hazardous wavelength.

(2) Areas where beams of hazardous wavelength are generated shall have proper protective measures for burns due to ultraviolet or infrared radiation. Quartz glass windows, and openings or covers made of quartz glass shall not be used without proper protective measures,

(3) Pulse or other high-energy laser systems which could cause loss of sight or burns shall not be used unless proper measures are taken to prevent all laser beams and their reflections that leak from equipment from irradiating human eyes and harming bodies (also refer to paragraph 5.9.2).

(4) Optical systems shall control the light intensity and spectral wavelength at direct-view eyepieces within a safe range for preventing visual damage.

5.9.2 Lasers

(1) Stoppers, locking mechanisms and shields shall be provided to prevent laser beams from irradiating personnel, other equipment, structures, etc.

(2) Laser equipment shall be designed so that it's electric supply can be turned off before it is removed from its installed position.

(3) Laser emission equipment and reflection equipment shall be designed to be fixed to prevent optical axis from moving to the unexpected direction by vibration from the launch or inadvertent contact during maintenance.

(4) Laser equipment shall be designed to keep voltage of all exposed exterior parts, surfaces, shields, and the like at ground potential.

(5) In general, quartz glass should not be used for flash tubes. If it must be used, proper plastic or tempered glass shields shall be used to absorb ultraviolet radiation. Quartz glass may be used as flash tube housing if the amount of ultraviolet radiation is indicated when the housing is opened.

(6) Laser equipment shall have shutter systems or inhibits operated by multiple commands to prevent inadvertent beam generation.

(7) Laser beams and their reflections can endanger personnel or ignite flammable substances. Therefore, laser systems shall be designed so that their output can be measured in completely shielded conditions.

(8) To minimize radiation hazards to person, laser systems shall be designed to allow as many adjustments and systems checks as possible with their beam shut off.

(9) Strong and well-known coating shall be used to prevent lens surfaces from overheating and melting due to internal reflection caused by coating deterioration.

(10) Laser systems operating at the high power level where contamination of optical apparatus due to dusts, vapors, or fingerprints may cause potential hazard shall be designed to prevent occurrence of optical contamination due to adjustment or maintenance operations at the launch site.

(11) Laser systems shall be designed to completely contain laser beams and prevent them from irradiating eyes when focusing and measuring output.

(12) Filters suitable for the operating wavelength shall be installed on the eyepieces for observing laser beams.

(13) Low-energy lasers such as He-Ne lasers shall be used to align the target and optical systems.

(14) Laser systems using harmful chemicals and/or cryogenic substances shall have shut-off valves to control leakage in the case of broken pipes.

5.10 Ground Support Equipment (GSE)

GSE shall meet requirements specified in section “5.1”, and the following requirements:

5.10.1 Transportation and handling equipment

(1) The following GSE are included in the transportation and handling equipment and shall be designed to comply with applicable safety requirements.

a. Material Handling Equipment (MHE)

Slings (ropes, spreader bars, hooks, and ring links), trucks, dollies, loaders, forklifts, auxiliary equipment (jacks, bracing devices, wheel stopper, towing rings, etc.), portable shelters, and protective covers

b. Cranes, etc.

Cranes, derricks, hoists and hydrasets

c. Transporter

Frames, transportation container, shipping container and transportation motor vehicle, road trailers

d. Handling structure

Spin-table, portable launch platform, etc.

(2) Minimum safety factors and proof load requirements

Transportation and handling equipment shall satisfy a minimum safety factor and proof load requirements specified as follows.

a. The minimum safety factor for lifting devices

- The minimum safety factor for lifting devices shall comply with Industrial Safety and Health Act.
- The minimum safety factor except for lifting devices shall be 3 for permanent deformation under static load condition, and 2 for permanent deformation under dynamic loads which exceed 1.5 times the rated load.

b. Proof test load

- For the equipment designed not based on agency or industrial standards, proof test shall be performed at twice the rated loads.
- For the equipment manufactured and maintained based on industrial standards (JIS, ANSI / ASME), proof test loads specified in industrial standards may be used.
- Equipment for lifting and supporting a person shall be capable of performing all design functions even under proof test load conditions.

(3) Frames, shipping containers and transportation vehicles shall be confirmed that they are adequate to be used, and that induced load from transportation are less than allowable value

of payloads.

(4) Sharp edges shall be removed or covered(in accordance with section 5.1.5).

(5) Bolts shall have the appropriate length (in accordance with section 5.1.6).

(6) The center of gravity shall be analyzed to prevent falling, tumbling or collapse of equipment or other mishap due to loss of balance when hoisting, transporting or conducting similar operation.

(7) Transportation and handling equipment shall be electrically grounded and bonded appropriately to protect persons from injury and to prevent damage from lightning strikes.

5.10.2 Electrical and electronic equipment

5.10.2.1 Selection of materials and combination of dissimilar metals

(1) Materials shall be selected to satisfy safety, reliability and compatibility requirements under the expected equipment operating conditions.

(2) Flammable materials should not be used for equipment structures.

(3) Glass fiber materials shall not be used for external covers of cables, wires or other equipment in order to prevent skin irritation.

(4) Materials selected shall neither generate harmful, corrosive, flammable or explosive gases nor cause fire under the expected operating conditions.

(5) Dissimilar metals shall not be used in a part where they constantly contact each other. Should dissimilar metals be used, proper measures shall be taken to prevent galvanic corrosion on the contacting surface.

5.10.2.2 Circuits and components

(1) Wiring and cables

a. Wiring insulation materials shall have long life with low degradation of electrical properties and shall not be degraded of physical properties under the expected operating conditions.

b. Insulation materials shall withstand constant usage under the low-temperature and high-temperature environmental conditions shown below, provided they are shielded from radiation heat caused by direct sunshine, etc.

(a) Low-temperature condition -5°C

(Ambient temperature during operation/non-operation)

(b) High-temperature condition 52°C(75°C)*

(Maximum temperature during operation/non-operation)

[*For exothermic items, increased temperature of 23°C is added to the ambient temperature of 52°C.]

c. Proper conductor diameters shall be selected to ensure that sufficient conductivity can be maintained when ambient temperature increases.

d. Cable insulation materials or contact point material for current carrying parts of wiring equipment shall be self-extinguishing when either of the following events occurs, even in the violent oxidizing process:

(a) When ignition sources are removed; or

(b) When conductors melt due to a large current resulting from short-circuiting of circuits or equipment failure.

e. When connecting power supply cables to terminals of a power supply panel, use round crimp-style terminals on the distal ends of the cables to keep the cables securely in position when screws become loose.

(2) Connection points

a. Terminals

(a) Sufficient insulation gaps or partitions shall be provided to prevent corona discharge and deterioration of insulation resistance under adverse environmental conditions such as high temperature, vapor condensation, low atmospheric pressure, and a saline atmosphere.

(b) Protective covers and the like shall be provided for terminals that are located near devices frequently accessed for operation, terminals that may cause electric shock/short-circuit due to human contact or inclusion of foreign objects, or terminals of circuits whose performance may be reduced due to dust, water droplets and contamination.

b. Connectors

(a) Two or more connectors to be installed adjacent to each other within one device shall have different alignment pins or keyways to prevent mismating or provide other appropriate means.

(b) Connectors shall have receptacle contacts on the power supply side and pin contacts on the load side.

(c) Un-mated connectors shall have protective caps and the like to protect them from dust, water droplets, and contamination.

(3) Grounding

a. General

(a) RF radiation equipment shall be designed and assembled to ensure that its exterior surfaces and shields voltage are kept at ground potential except when antenna and transmitter are operating.

(b) Insufficient grounding or hazardous high voltage shall be prevented in design.

(c) The earth ground shall not be used as a part of the circuit. A current return path shall be routed inside the equipment or through inter-equipment cables.

(d) Shields shall not be used as a return path, except for coaxial cables.

(e) Frames and/or cases of portable tools or equipment shall be automatically grounded when plugs or receptacles are connected.

(f) Grounding wires shall have sufficient current-carrying capacity and their impedance shall be reduced to restrict voltage level increasing from ground and to ensure operation of over-current protection devices in the circuits. Unused wiring in a long bundled harness shall be grounded to discharge floating and electrostatic charges.

b. Grounding to chassis

(a) For grounding to chassis or frames by soldering, ground wires shall be soldered to terminal lugs or to a dedicated location on the chassis or frame. For grounding to chassis or frames by fastening, grounding terminals shall be fastened to tapped holes or through holes in the chassis or frame using screws, nuts, and lock washers.

(b) For steel chassis or frames, plating or tin coating shall be applied around the screw holes to keep them corrosion resistant.

c. Shields

(a) Shields of wires and cables shall be grounded to chassis or frames in accordance with processes specified (3) b above.

(b) Shields shall be designed not to contact with exposed powered parts or to be grounded at other than the specified grounding points on the chassis or frame.

(c) End of shield shall be kept far enough from exposed portions of the core wire to prevent short-circuits and arcing between the core wire and shield. The shield end shall be positioned within 25 mm from the exposed portion of the core wire, with crimping or rings etc, in order to maintain sufficient shielding.

(4) Overload protection

a. General

(a) Protective devices shall be provided to prevent any overload in GSE from affecting the payload.

(b) Fuses, circuit breakers and other protective devices shall be installed in primary circuits to prevent fire, explosion, and overheating.

(c) Test and inspection equipment shall be protected from overload current and incorrect operation.

(d) Fuses, circuit breakers, and the like shall be used to open a power supply line to a failed circuit.

(e) Protective devices shall be installed on the load side of main power supply switches except for those activated by measuring neutral point voltage.

(f) Protective devices shall be the longer trip time type for the power supply side, and the shorter trip time type for the load side.

(g) Three-phase motor shall have protection circuit for loss of a phase not to activate all three phase as a result of single-phase failure.

b. Circuit breakers

(a) Circuit breakers shall have reset buttons and switching levers that can be easily operated.

(b) Circuit breakers shall allow visual checking of their trip status.

(c) Circuit breakers shall be capable of tripping when their levers are held to the "ON" side.

5.10.2.3 Protection of human body

(1) General

a. High-energy systems shall be designed to minimize the risks of skin burns and injury due to electric discharge and RF radiation.

b. Hazards, such as skin burns caused by touching an electrically overheated surface or a part heated by transfer of high temperature, injuries due to fire caused by overload electric equipment, and electric shocks caused by contacting high voltage (30V or more (direct current or effective value of alternate current)),shall be controlled.

c. Appropriate protective measures, such as doors and covers, shall be provided to prevent person from accidentally contacting a part to which 30 V (direct current or effective value of alternate current) or more is applied during operation.

d. Devices shall be turned off when they are installed, relocated, and replaced.

e. Main power switches of equipment shall be capable of cutting off the power supply of the equipment and shall be clearly identified.

(2) Interlocks

a. Electrical interlock mechanisms shall be provided to equipment that fails or causes hazards when operated improperly.

b. Interlock mechanisms shall be selected and designed according to the following guidelines.

(a) Interlock mechanisms shall be provided to protective doors, safety covers, or the like of the parts if personnel may contact to portion that is applied voltage of equal to or greater than 70 V (direct current or effective value of alternate current) during planned adjustment, maintenance, etc.

(b) No interlock mechanisms are required on systems that are applied voltage of 70 V to 500 V (direct current or effective value of alternate current) if barriers or guards are provided.

(3) Shorting rods

a. Storable Shorting rods shall be provided for devices that may accumulate some of electric charge causing electric shocks even if power is turned off.

b. Devices without storable shorting rods shall have ground studs for connecting portable shorting rods.

c. Storable shorting rods shall be connected to ground studs on the main frame of the devices using flexible copper stranded wire covered with a transparent sleeve.

d. Connection to ground studs shall not become loose. Resistance to the ground shall not be high.

e. Devices with ground studs only shall facilitate quick connection and disconnection of portable shorting rods with the grounding studs.

(4) Safety guards

a. Contacts, terminals, and the like which have an electric potential of 30 V to 500 V (direct current or effective value of alternate current) from ground shall have partitions or guards to prevent accidental human contacts.

b. Partitions may have access holes for maintenance and testing. However, internal components operated at equal or greater than 500 V or more shall be an enclosed type that is completely shielded from other internal components.

c. As partitions and guards may be removed for various purposes, appropriate high-voltage hazard signs with the maximum applied voltage information shall be displayed in a clearly visible place.

(5) High-voltage marking

a. Contacts, terminals, and similar components to which 500 V (direct current or effective value of alternate current) or more is applied shall be clearly marked with "危険，高圧（Danger, High Voltage) - (maximum applied voltage) V". The marking shall be in black letters on a white background with a proper symbol indicating "Danger."

b. Markings shall be clearly visible and placed near hazardous parts of the equipment.

(6) High-voltage protection

The equipment that need to be measured a voltage of 300 V (direct current or effective value of alternate current) or higher during operation and maintenance shall have test points to allow measurement at a relatively low voltage.

(7) Discharging devices

High-voltage circuits and capacitors shall have discharging devices, unless they can discharge their voltage to 30 VDC within two seconds after the power is turned off. Discharging devices shall turn off power automatically to reduce voltage to 30 VDC within two seconds when the high voltage containment case or rack is opened.

(8) Momentary overrides

a. Circuits for which instantaneous power cut-off is not desirable shall have momentary-on override switches on the front panels to allow manual operation prior to interlock.

b. An override switch shall automatically be disengaged when a door or cover with the override switch is returned to the initial position. The override switch, whether the switch is turned on or automatically turned off, shall not cause instantaneous interruption of power to the equipment

(9) Temperature

a. The exposed surface of the equipment that may be touched by person shall not exceed 60°C in normal ambient temperature conditions.

b. The temperature of front panels shall not exceed 45°C in normal ambient temperature conditions.

(10) Inspection doors

a. If inspection doors need to be installed near hazardous machines or electric parts, lighting devices shall be provided inside, with a mechanism to turn the light on or off that is controlled by the inspection door open/close. In addition, clearly identifiable warning signs shall be displayed on the front of the inspection doors.

b. Edges of inspection doors shall be protected with molded plates, rubber, textile, or plastic to prevent injuries to hands or arms.

c. Safety interlock mechanisms shall be provided for inspection doors for high voltage equipment.

d. If any work need to be performed on operating equipment and devices with its interlock mechanisms released, the interlock mechanism shall be automatically recovered by closing the inspection door upon completion of the work.

e. Driver guide mechanisms and the like shall be provided for adjusting portion located near sections with high voltage applied, thereby preventing screw drivers and other tools from accidentally contacting high voltage areas.

f. Where glass does not meet durability requirements including stress, quick-open type metal doors shall be provided.

g. Openings and doors shall be made of materials capable of preventing electromagnetic interference of the component or other equipment, if necessary.

h. The sign specified in paragraph 5.10.2.3(5) shall be provided near each inspection door.

(11) Mechanical protection

a. Protection devices, etc. shall be provided to prevent personnel from touching movable parts such as gears and fan belts while equipment is in operation.

b. Cabinets, doors, etc. shall not have any sharp edges.

c. Covers with doors or hinges shall have rounded corners and a mechanism to secure them in the open position.

d. Mechanisms to prevent drawers or rack equipment from sliding out or falling shall be provided to prevent damage to devices and injury to person.

e. Critical switches and controllers shall be located at where they cannot be activated by accidentally contact by person.

f. Piping and joints for lubricant and pneumatic pressure or wiring and electrical connectors for measuring instruments shall be designed to prevent misconnection.

g. Color coding or marking shall be used only when a fool-proof design cannot be implemented.

5.10.2.4. Other considerations

(1) Overload bypass devices or equivalent shall be installed on meters to prevent excessive voltage or current from being generated at the terminals due to equipment failure.

(2) Equipment with cathode ray tube displays shall be designed to prevent injury due to their rupture.

(3) Equipment cooling and ventilation

a. Ventilation hole shall be arranged and shaped to prevent foreign objects from entering into and contacting a high-voltage part.

b. Partitions or internal ventilation hole shall be provided, as required, to prevent overheating of components.

c. Ventilation fans shall be provided if necessary. Fan design shall adequately consider electromagnetic interference, power supply, and cooling since fans generally consume much electrical energy and generate much heat.

(4) Static Electricity

a. If one material used in combination with others insulation material, provision shall be made to prevent generation of static electricity due to friction of the materials.

b. If electrostatic is accumulated high voltage instead of being discharged, occurrence of sparks due to electrostatic discharge shall be prevented.

c. Equipment and devices shall be grounded to prevent accumulation of electrostatic charge.

(5) Accessibility

a. If the inspection doors of the equipment do not have latches or hinges, the unit shall be removed or replaced by opening a single inspection door.

b. Parts requiring visual inspection (e.g. operating time recorder) shall be inspected without removing the panels or other parts.

5.10.3 RF radiation equipment

RF radiation equipment of GSEhall meet the requirements in paragraph 5.7.

5.10.4 Ionizing Radiation equipment

X-ray and γ-ray inspection equipment of GSEhall meet the safety requirements specified in paragraph 5.8 concerning radioactive radiation to protect personnel, facilities and equipment.

5.10.5 Optical equipment

Optical equipment of GSEhall meet the requirements in paragraph 5.9

5.10.6 Propellant equipment

5.10.6.1 Materials

(1) Materials and components used for systems containing hazardous fluids shall be compatible with the fluids used in operation. Similar consideration shall be taken for non-metallic materials, especially lubricants and materials for acoustic insulation.

(2) Materials with high fracture toughness and a slow rate of crack propagation shall be selected.

(3) Screws with threads that are easily broken, such as those made of aluminum alloy, shall not be selected for joints that are frequently connected and disconnected.

(4) Appropriate corrosion prevention measures shall be taken.

5.10.6.2 Strength

(1) Safety factors shall be determined by dividing burst stress by maximum operating stress (for tanks, burst pressure divided by MEOP).

(2) Safety factors for devices shall be equal to or greater than 4 unless otherwise authorized by JAXA.

(3) Gas pressure shall never exceed the MEOP.

(4) Devices located downstream with a reduced pressure shall withstand the upstream pressure or they shall have safety valves, rupture disks, or the like which shall operate at or below a pressure 110% of the MEOP of the downstream device.

(5) The maximum operating stress shall be calculated considering shapes; manufacturing standards (tolerance, surface roughness, inspections, and variations); pressure; temperature gradients; temperature changes; assembly conditions; weight; environments; and stress, temperature, corrosion in the dynamic operating conditions, etc.

5.10.6.3 System design

(1) Propellant leakage and accidental mixing of propellants shall be prevented.

(2) For a circuit that uses incompatible fluids, fluid mixing shall be prevented. (For example, oxidizing propellants and reducing propellants, or breathing air and harmful fluid.) In particular, joints (e.g. union joints) shall be designed to prevent incorrect connection and leakage.

(3) Pipes shall be designed to minimize the number of joints to minimize risks of leakage.

(4) Non-condensing gases shall be used in cryogenic propulsion systems.

(5) Circuits using cryogenic fluids shall be free from clogging.

(6) Circuits using a hazardous fluid shall be purged by inert gas after use.

(7) Circuits using a hazardous fluid shall be capable of preventing contamination (for leakage, and effect from outside).

(8) Fixed or portable storage tanks shall be capable of operating while the fluid flows at the MEOP and shall have manual shut-off valves at an easily accessible location on branching circuits.

(9) For remote control valves, normal-open type or normal-close type valves shall be selected to recover to the safe position when causing hazards due to loss of control power.

(10) Waste fluids shall be collected in reservoir tanks capable of neutralizing and draining them safely. If this is not feasible, they shall be collected in portable containers that can feed the waste liquids into special disposing equipment.

(11) Gaseous exhaust of hazardous fluids shall be collected in vents. Should any environmental pollution is expected downstream of the vent, exhaust gases shall be neutralized or diluted prior to disposal.

(12) Systems containing hazardous fluids shall be designed considering hazardous characteristic of the systems such as corrosion by fluids and harmfulness, together with characteristic such as stress corrosion in pressure systems. Leak tests shall be performed at the launch site prior to their use.

(13) Devices shall be installed where they can withstand mechanical stress. High-pressure lines shall be installed where there is no risk of danger to person. If necessary, protection measures shall be provided.

(14) Proper ventilation shall be considered for hazardous fluids. When exhausting the large amount of hazardous fluids into the atmosphere, the hazardous fluids shall be combusted or diluted to prevent harmful influence due to atmospheric pollution.

(15) Automatic pressure reducing devices shall be installed on storage equipment which has an operating pressure exceeding 1/4 of the burst pressure and on fluid systems that expected pressure increase exceeding 1/4 of the burst pressure.

(16) If a burst can cause critical or catastrophic hazards due to pressure excess, two types of automatic pressure reducing devices having different operational functions shall be provided.

(17) The use of flexible hoses shall be minimized. If flexible hoses must be used, handling specification shall be clearly defined. The operating pressure shall be 1/4 the design burst pressure or less. A proof pressure test shall be conducted at a pressure of 1.5 times the MEOP or more.

(18) Each piping or container shall have identification tags or signs attached that bear identification number, maximum expected operating pressure, and fluids used.

(19) Instruments/instrumentation equipment

a. Operating points shall be selected to be 1/2 to 2/3 of the full scale.

b. Remote control shall be employed to protect personnel from unnecessary exposure to the site for circuit operations or operating condition checks.

c. Control panels shall be designed to allow for operators to safely operate.

(20) Components that can be assembled in reverse or that are specified to use a specific type of fluid shall be clearly identified to prevent from incorrect assembly or the use of a wrong fluid.

(21) Some pressure vessels, pipings, etc. for high-pressure gas used in the propulsion GSE, and some equipment handling hazardous fluids are subject to regulations or permit/approval under Japanese laws. The contractor shall prepare necessary data.

(22) GSE shall be <u>designed so that propellants can be unloaded from payload</u> ~~able to unload payload propellants~~ safely in <u>contingencies</u>~~y situations~~<u>, such as</u> ~~including~~ propellant leak from the payload~~ while the payload is still installed on the launch vehicle~~. F

(23) Transportation/handling equipment shall be electrically grounded and bonded for human body protection and for mitigation of lightning damage.

(24) Non-shatterable materials shall be used for the window of on-site indicators.

(25) For cryogenic fluids, specific prevention measures for cryogenic brittleness shall be provided. This prevention measures shall be provided for all cryogenic piping systems especially whose temperatures are less than 90.3 K (liquefied temperatures of oxygen at atmospheric pressure).

5.10.7 Hydraulic equipment

5.10.7.1 General requirements

(1) MEOP and temperature limits

a. Piping

Flow paths shall be free from obstructions that reduce the optimum flow rate of working fluids and cause excessive pressure and power loss. System components shall be designed to ensure that a single component failure will not cause back pressure to the system. The effects of the MEOP on the viscosity of working fluids shall be considered.

b. Temperature

Cooling systems shall be provided to keep the working fluids within a normal operating temperature range if high temperature of working fluids could cause hazard.

5.10.7.2 Selection of components and working fluids

(1) Selection of materials

Plated materials shall not be used for piping, because plated materials are susceptible to exfoliation. Copper shall not be used as it can react with various substances, and aluminum alloys and stainless steel shall be used.

(2) Pressure adjusting and regulator valve

Hydraulic system pressures shall be adjusted to avoid pump overloading to maintain and adjust the required system pressure, and supply the required pressure for subsystems. Pressure regulator valve shall be installed downstream of pumps to prevent the system pressure exceeding the downstream structural limits, or when subsystems are required for lower pressure.

(3) System piping

a. Piping

Straight piping shall not be used to reduce strain caused by vibration, thermal expansion, and thermal shrinkage.

b. Flexible hoses

Flexible hoses may be used in the following cases:

(a) To isolate the system from vibration or shock

(b) To connect components which make interactive motions

(c) If fixed piping is not feasible

c. Fixing high-pressure pipes

High-pressure pipes shall be appropriately fixed to prevent rupture caused by fastening or loosening.

(4) Selection of working fluids

Working fluids shall be selected based on an evaluation of the entire system from the viewpoint of operating functions and compatibility of working fluids. In the process, consideration shall be given to the following factors.

a. Effects of working fluids related to the performance of operating elements.

b. Potential effects of operating oils such as corrosion or deterioration on non-moving elements such as coatings, seals, hoses, and piping.

c. Potential of improper handling of working fluids which causes any adverse effects on components, operating parameters, ambient conditions, and working fluids themselves.

d. Low flammable working fluids shall be used for high pressure hydraulic systems or at the areas where fire could occur.

5.10.8 Pressurizing equipment

For pressurizing equipment design, contractor shall consult with JAXA regarding to legal regulation such as Japanese Law.

5.10.8.1 Safety design considerations

(1) System analysis

Structural analysis shall be performed for all significant pressurized systems.

(2) Proof test pressure, etc.

Proof test pressure and design burst pressure shall be in accordance with High Pressure Gas Safety Law. Summary of the law are described below:

Proof test pressure

Transportable pressure vessel; (MEOP) x 5/3

Others; (MEOP) x 1.5

Nonconformance of systems shall not occur at this pressure level.

Design burst pressure (MEOP) x 4

Systems shall not be ruptured at this pressure.

(3) Compatibility of materials

All materials used for pressurized systems shall be selected from materials that are certified to have compatibility with pressurized fluid to prevent chemical reactions between the materials and the pressurized fluids.

(4) ~~Emergency~~ Contingency measures

The GSE shall ensure that the payload pressure system shall be safely depressurized in case of contingencies~~y situations,~~such as ~~including~~ propellant leak from the payload while the payload is still installed on the vehicle.

6. LAUNCH SITE OPERATION SAFETY REQUIREMENTS

Safety requirements for launch site operations shall be in accordance with paragraph 2.1(2) JERG-1-007 “Safety Regulation for Launch Site Operation~~/Flight Control Operation~~.”

Appendix I DEFINITION OF TERMS

(See Chapter 3 of this Standard.)

The terms used in this Standard are defined below.

[A]

Arm/safe plug

Connectors and related devices to provide electrical connection or insulation for the firing circuits of pyrotechnics used in the payload by mating/demating.

[B]

Bleed valve

A valve used for discharging fluid to maintain normal operation of system. I.e. air bleed valve.

Bruceton Test

Statistical technique to determine reliability of pyrotechnics by random measuring using Up-and-down method.

[C]

~~Catastrophic Hazard~~

~~Hazard that could cause death or severe injury of third-party (including permanent injury to a person), death or severe and permanent injury of personnel, loss of or severe damage to public or third-party's private property, loss of system (launch vehicle, payload/GSE) or launch site facilities, or serious environmental impacts.~~

~~Critical Hazard~~

~~Hazard that could cause minor damage of third-party, severe personnel damage, minor damage to public or third-party's private property, severe damage to system (launch vehicle, payload/GSE) or launch site facilities, or severe environmental impacts~~

F

Contractor

An individual, organization, or company developing payload/GSE or performing launch site operations under contract/agreements with JAXA.

[D]

Deterioration

Degrading characteristics of material or equipment performance as a result of its use or time consuming.

Deviation

Approval given to the condition not meeting safety requirement after confirming that the condition satisfies the intent of the safety requirement.

[E]

EBW (Exploding Bridge Wire device)

An explosive device that has bridge wire designed to be exploded or decomposed by high-energy electric discharging, and which uses as igniter for the initiator.

EED (Electro-Explosive Device)

Electro-Explosive Device

Electromagnetic Compatibility (EMC)

An ability of system or related subsystem/components to perform its function without degradation under any electromagnetic environments to be exposed during all mission lifetime.

Explosive hazardous atmosphere area

An area where is expected to be leaked or discharged explosive gas or vapor, etc. The electric equipment used in this area must be explosion-proof.

Explosive train

The path to transfer the energy produced by EED.

[F]

Fail-safe

Design concept that ensures safety even if a subsystem, component, etc. fails and loses its function.

Failure

The inability of a system, subsystem, component or part to perform its required function within specified constraints, under specified conditions and for a specified duration.

Fault tolerant design

Design that prevents a failure or human errors from resulting in an accident. Basic safety requirement to control hazards. For severity I hazards, design shall prevent accidents after two failures, or two human errors, or the combination of one failure and one human error. For severity II hazards, design shall prevent accident after one failure or one human error

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 to a system or a subsystem into logical elements, eventually to an observable, basic element (cause for failure).

Fool-proof

A design to prevent human errors or to maintain safety after human errors.

[G]

Ground Support Equipment (GSE)

The ground equipment necessary for handling, testing and inspecting a payload.

[H]

Harmful Propellant

Propellant that vapor or gas causes physical disorders such as skin disorder, nerve disorder, asphyxiant, carcinogenic, or toxic disorder.

Hazard

An existing or potential condition that can result in a mishap.

Hazard analysis

A technique to assess, systematically and logically, hazards associated with payload/GSE throughout the life cycle.

Hazard Cause

Cause that leads a hazard to an accident. (e.g., container structure deficiency that leads to propellant leak, malfunction of propellant valves, and deficient seals.)

Hazard control

In strict sense, reduction of likelihood of occurrence of a hazard by failure tolerance design or design for minimum risk.

In broader sense, safety device, protective device, warning systems, special procedures and training are included.

In this Standard, except for paragraph 5.1.1, the broader meaning is applied.

Hazard Report

A report that is documented technical information as a result of hazard analysis, and is developed for risk assessment by designer, project member, and for approval of residual risk by responsible person for the project.

Hazard Summary

Hazard description that explains a hazard (including source, mechanism, and outcome,) and specifies severity.

Hazard Title

Title that can be indicative of content of hazard (source, mechanism, outcome), and distinguishable from other hazard

Hazardous Atmosphere:

An atmosphere where harmful or explosive gas/vapor is present, or an atmosphere expected to be oxygen deficient condition such as closed volume.

Hazardous fluid

Fluids including harmful materials, liquid propellants, liquid oxygen, oxidants like gaseous oxygen, or any other exothermic reacting fluids.

Hazardous operation

Any operation that handles hazardous products, etc. or is performed in a hazardous environment and that is designated as hazardous by JAXA.

Hazardous products

Hazardous products include explosives, high pressure gases and hazardous materials as well as materials similar to hazardous materials.

Hermetic seal

The sealing of a part, component, etc. which physically isolates the inside from the outside, and does not allow gas passage.

Hiyari-Hatto

Both Hiyari and Hatto are Japanese expression usually used in not so serious situation of “be startled at” or “take fright at”. Hiyari-Hatto means an event that could have led to a mishap or accident. Note: In English, “close call” is a similar expression. “Close call” means that unplanned occurrence in which there is no injury/damage but under similar circumstances could have resulted in a reportable mishap.

[I]

Incompatible fluids

Fluids, which will cause a mishap or induce a mishap as a result of accidental mixture, i.e., mixing oxidizing propellant and reducing propellant or breathing air (including ventilation equipment) and toxic fluid.

Inhibit

Any physical method that interrupts energy to initiate hazardous functions, installed to prevent unintended operation of hazardous functions. e.g, relays in electrical circuits, shut-off vales in piping.

Interlock

A function that monitors the state of a specific event, variables and physical parameters and transmits signals to control equipment connected thereto, upon detecting any abnormality, so as to terminate the system operation and to prevent the occurrence of any mishap, failure, and condition causing mishap or malfunction.

[L]

Launch Readiness Review

Review to confirm completion of launch processing operations for space craft, etc. and readiness for shift to launch count down. This review is conducted by JAXA.

Launch Site Operation

Launch processing operation of launch vehicles or payload/GSE and operations of facility/equipment performed at Tanegashima Space Center.

Leak Before Burst

Design to prevent bursting of a pressure vessel when the pressure vessel fails by causing the pressure vessel to leak first.

[M]

Manipulator

The multi-joint and multi-freedom robotic arm that is used for replacing of unit, assembling, berthing, etc. (on orbit).

Maximum Expected Operating Pressure (MEOP)

The maximum pressure that is expected to be applied to components of pressure system under the operational environment.

Milestones

Important events that are scheduled within the life cycle of a project and are utilized as control points for tracking the progress or effectiveness or achievement of payload/GSE development, etc.

Mishap

An unexpected event that causes injury, death or illness of person and/or loss or damage to system (launch vehicles, payload/GSE), related facility or property, environment effect.

Mishap, etc.

Mishap or “Hiyari-Hatto” (dangerous incident that could have led to a mishap). It includes constant event that affect operator’s occupational disease or harmful effect to environment, even if no mishap nor “Hiyari-Hatto”.

[N]

Nonconformance

A condition where one or more characteristic of parts, material, or service used for components does not comply with specified requirements. It includes failure, discrepancy, defect, and malfunction.

[O]

Override

To allow the specific control to have the priority over the normal control.

[P]

Payload (launch vehicle payload)

A cargo which is launched by a launch vehicle to space. In this Standard, the cargo is unmanned hardware and includes sub-systems and components constituting a payload.

Person (corresponding to “Jin-in” in Japanese version)

In this Standard, the term of “person” is used to mean personnel (shown below), public citizen and/or visitor inside/outside TNSC.

Personnel (corresponding to “yoin” in Japanese version)

In this Standard, personnel mean definitely the people of JAXA, contractors, or other organizations who are engaged in specific operations.

Potting

To fill a compound in a part of an electric circuit, etc. or an entire volume of inside a component to shield it so that explosive gas or flame generated by explosion may not propagate to other area.

Pre-Shipment Review (PSR)

A review to confirm that systems can be delivered to a launch site. Acceptance test results, quality records, anomaly dispositions and such are reviewed.

Pressure System

A system consisting of pressure vessel, components and piping to connect these, etc.

Pressure Vessel

A vessel which stores high pressure gas inside. High pressure gas is defined as follows,
(1) compressed gas at pressure equal to or greater than 1 MPaG at normal temperatures, and of which pressure is “in substance” equal to or greater than 1 MPaG. Or compressed gas which pressure will get to equal or greater than 1 MpaG at 35℃. (except compressed acetylene gas)

(2) liquified gas at pressure equal to or greater than 0.2 MPaG at normal temperatures, and of which pressure is “in substance” equal to or greater than 0.2 MPaG. Or liquefied gas of which temperature will be equal to or lower than 35℃ at the pressure of 0.2 MpaG.

Where, pressure “in substance” means that the pressure to which the gas will reach theoretically by temperature rise, excluding mechanical pressurization or chemical change.

Protective device

(1) Devices, etc. (cover, protection wall) to be designed as part of ground facility/device to prevent hazardous condition in case that component and/or function are inadvertently operated or in out of control.

(2) Device, etc. to prevent unintentional operation or access to hazardous portion.

Purge

To load inert gas such as nitrogen gas or helium gas into a tank, piping, or the like to discharge any propellant remaining inside or to prevent the entrance of the outside air.

Pyro-valve

A valve which state is switched open or close by the pyrotechnics operation.

[R]

Receptacle

Female part of an electric connector.

Risk

Product of hazard severity and likelihood of occurrence.

[S]

Safety

The state that hazards are eliminated, minimized or controlled not to lead mishap/accident, i.e. risk level is low as acceptable.

Safe/Arm Device

A device that prevents inadvertent operation (on ground) of pyrotechnics used for ignition for solid rocket motor, separation of first/second stage or flight termination system of launch vehicle.

Safety critical

Any condition that identified hazard severity is I or II.

e.g., “safety critical” operational procedure, “safety critical” parts.(Refer to Table 4.3.1-1)

Safety Data

Hazard identification summary table, Hazard analysis table, Hazard report, Safety verification data, Safety verification tracking log, Safety requirements compliance matrix, failure data and other necessary data of safety-critical functions, document that confirms compliance with safety requirements

Safety Device

Devices or systems to be designed to prevent hazardous condition in case that component and/or function are inadvertently operated or in out of control.

Safety requirement compliance matrix

A matrix to demonstrate and verify the compliance of a payload with safety requirements.

Safety Review

A review to confirm whether a payload, GSE, and launch site operation comply with the safety requirements, to confirm all hazards are identified, and also to assess and confirm that residual risk of identified hazards are acceptable by assessing and confirming controls of identified hazard causes and their verification at each development phase.

Safety Verification Tracking Log

A document used to track verification of controls specified in the hazard reports that can be completed only at the launch site. This document complements safety verification confirmation during hazard report review. It is used to properly manage and confirmn verification items until completion.

SCA (Sneak circuit analysis)

An analytical technique to evaluate hardware and software systems, developed to identify a potential circuit or a state that prevents a required function from being performed or causes an undesired function to be introduced. SCA consists of sneak path analysis, digital sneak circuit analysis, software sneak path analysis and so on, and suitable analytical techniques shall be chosen for the system.

System Safety

Application of engineering and management principles, criteria, and techniques to rationally minimize 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.

Stray voltage

The voltage measured to check for the stray current.

Swivel joint

Piping joint having freedom of rotating.

[T]

Tailoring

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

[U]

<u>Union joint</u>

A threaded joint used for connecting the ends of two pipes, eliminating the need for turning either pipe for joining.

[V]

<u>Vent</u>

Equipment that has an opening to drain an unnecessary or used fluid or gas into the air. The opening is called a vent port.

[W]

<u>Waiver</u>

Permission for condition that cannot comply with safety requirement based on confirmation that safety risk is acceptable.

F

~~Appendix II Explosion-proof Requirements for Electric Equipment in Explosive Hazardous Atmosphere Area~~

~~Based on the specifications of the “User’s Guide for Explosion-Protected Electrical Installations in General Industries (explosion-proofing for gas, 1994)”, types of explosion-protected electrical equipment of ground support equipment/device used in explosive hazardous atmosphere areas (referred to as "hazardous areas" in the above guide) and considerations in selecting such equipment are summarized below. Details are specified in the guide and latest “Specification for Explosion-protected Electrical Apparatus” or “Technical Regulation” (see note) that are Japanese Law related to the guide. The details necessary for actually applying the requirements shall be consulted with JAXA.~~

~~(Note) “Technical Regulation” was revised in 1996, after establishment of the guide.~~

~~(1) Explosion-proof, structure types~~

~~a.Flameproof explosion-proof structure~~

~~An enclosed structure that can withstand internal pressure of any occurring gas explosions, and that will not ignite external explosive gases. Temperature rise at outside surface of enclosure which contacts an explosive gas shall not exceed the appropriate values specified according to the ignition category.~~

~~b.Oil-immersed explosion-proof structure~~

~~A structure in which electrical equipment which may generate sparks or arcs is immersed in insulation oil so that explosive gases existing above the surface of the oil will not be ignited. Temperature rises of oil at parts that may contact an explosive gas and at oil surface shall not exceed the appropriate values specified according to the ignition category.~~

~~c.Pressurized explosion-proof structure~~

~~A structure that is maintained internally at an overpressure by a pressurizing protective gas (clean air or inert gases) so as to prevent the introduction of explosive gases. Temperature rise of any external surface of the enclosure, associated ducts, and exhausts that may contact an explosive gas shall not exceed the appropriate values specified according to the ignition category. Structures are classified as continuous, compensating, or hermetically sealed types according to how over-pressure is maintained.~~

~~d.Increased safety explosion-proof structure~~

~~A structure in which additional measures are applied so as to increase protection against the possibility of excess temperature and electric sparks where such abnormalities shall not occur in normal service. The temperature rise of any part composing an electrical apparatus to which explosive gases are accessible shall not exceed the appropriate values specified according to the ignition category.~~

~~e.Intrinsically safe explosion-proof structure~~

~~A structure with electrical and structural characteristics verified by ignition tests or in other ways by authorized organizations to be incapable of igniting explosive gases by sparks or high-temperature parts produced either normally or in specific fault conditions.~~

~~f. Special explosion-proof structure~~

~~Any structure other than a through e above which has been verified to prevent igniting explosive gas by testing or other ways by authorized organizations.~~

~~(2) Explosive gas classification~~

~~When selecting explosion-proof electrical equipment, consider the risk level of the explosive gas with regard to vessel strength, vessel gaps, high temperature areas, etc. of the~~

F

~~explosion-proof structures specified in (1) above. Risk levels of explosive gases are categorized according to the explosion grade and ignition categories. Followings are sample of categorization in accordance with “Specification for Explosion-protected Electrical Apparatus”.~~

~~a. Explosion grades~~

~~The three explosion grades in Table II-1 are divided according to the minimum gap which permits flame propagation in the test using a standard test vessel.~~

~~Table II-1 Explosion Grades~~

~~Explosion Grade~~	~~The Minimum Gap Which Permits Flame Propagation at a Flame Path Length of 25mm (G)~~
~~1~~	~~0.6mm < G~~
~~2~~	~~0.4mm < G ≤ 0.6mm~~
~~3~~	~~G ≤ 0.4mm~~

~~b.Ignition Categories~~

~~Six ignition categories are defined in Table II-2 according to the ignition temperature of explosive gas.~~

~~Table II-2 Ignition Categories~~

~~Ignition Category~~	~~Ignition Temperature (T)~~
~~G1~~	~~T > 450°C~~
~~G2~~	~~300°C < T ≤ 450°C~~
~~G3~~	~~200°C < T ≤ 300°C~~
~~G4~~	~~135°C < T ≤ 200°C~~
~~G5~~	~~100°C < T ≤135°C~~

~~(3) GSE-related explosion-proof requirements~~

~~The explosion-proof requirements for hazardous products are stated below. Consider the following requirements when designing and selecting GSE for hazardous operations.~~

~~a.For explosives, nitrogen tetroxide (NTO), and oxygen~~

~~GSE shall have an enclosed structure.~~

~~b.For hydrogen~~

~~GSE shall satisfy explosion grade 3 and ignition category G1 requirements.~~

~~c.For hydrazine~~

~~GSE shall satisfy explosion grade 2 and ignition category G3 requirements.~~

~~d.Two or more hazardous products present~~

~~The most severe conditions of explosion grades and ignition category of all hazardous products present shall be applied.~~

~~Notes~~

1. ~~The oxygen and hydrogen requirements mainly apply to launch vehicles. These requirements are stated as references since there will be few payload operations in which GSE is used near payloads (around launch pad) during or after propellant loading to launch vehicle.~~

2. ~~"Explosives" here refers to solid motors and pyrotechnics including explosive bolts. It does not include powder or explosive dust which may be ignited by electric equipment.~~

F

~~Attachment-1 Standard Hazard Report form~~

F

~~**JAXA Payload**~~	~~**Hazard Title**~~	~~**A.Review Phase**~~	~~**B.Date**~~
~~**Standard Hazard Report**~~	~~**Standard Hazard**~~		

~~**C. Payload Name**~~	~~**D. Launch Vehicle**~~

~~**E.Approval**~~	~~**Contractor**~~	~~**Payload Organization**~~	~~**JAXA/Safety Devision**~~
~~**Phase I**~~			
~~**Phase II**~~			
~~**Phase III**~~			

~~**F.Hazard Description**~~	~~**G. Hazard Control**~~	~~**H. Applicability**~~	~~**I. Verification Method, Reference Document, Status.**~~
~~HR-1 Ignition in Explosive hazardous atmosphere~~ ~~1.1 Flight Equpment:~~	~~a) Meets all of the following.~~ ~~a)-1 Gas-explosion proof design (except for type of protection "n") in accordance with Japanese law:"Constructional Requirements for Electrical Equipment for Explosive Atmospheres". (Explosion proof design for cable/connector between electrical components should be considered. Examples for gas-explosion proof design are potting, hermetic sealing, pressurization with inert gases, or designs described in JMR-002, Appendix II).~~ ~~a)-2 Appropriate grounding/bonding to prevent ESD.~~ ~~a)-3 Any portion acting as a catalyst for hydrazine, such as rust, is eliminated.~~	☐	

~~JAXA Payload~~	~~Hazard Title~~	~~A.Review Phase~~	~~B.Date~~
~~Standard Hazard Report~~	~~Standard Hazard~~		

	~~b) Meets all of the following.~~ ~~(Non-exposion proof equipments, cables or connectors (D-sub connector, etc.) are acceptable if these meets the following.)~~ ~~b)-1 payload is unpowered by demating battery and so on in explosive hazardous atmosphere during propellant loading or unloading operation. (Mis-operation needs to be considered if interface by operator exists.) Or payload does not exist in explosive hazardous atmosphere during propellant loading or unloading operation for other payloads.~~ ~~b)-2 Normal payload functions do not cause ignition of propellant leaked from payload(including other payload). (Failure modes need not be considered.)~~ ~~Note: If item b)-2 can be complied, payload can be powered under all of the launch site environment, except under the environment of item b)-1 below.~~ ~~b)-3 Integrity of electrical equipment is verified after vibration/impact test. (Chattering needs to be prevented if unsealed relay is connected to battery.)~~ ~~Note:This paragraph shall be applied when inadvertent power supply is credible due to chattering of relay (such as latching relay) used as inhibit against hazardous function.~~	☐	

F

~~**JAXA Payload**~~		~~**Hazard Title**~~	~~**A.Review Phase**~~	~~**B.Date**~~
~~**Standard Hazard Report**~~		~~**Standard Hazard**~~		
	~~b)-4 Appropriate grounding/bonding to prevent ESD.~~ ~~b)-5 Any portion acting as a catalyst for hydrazine, such as rust, is eliminated.~~			
~~1.2 AGE/GSE~~	~~a) AGE/GSE is not used under explosive hazardous atmosphere. (No verification required.)~~ ~~b) Meets all of the following.~~ ~~b)-1 Explosion proof design in accordance with JMR-002, para 5.1.2.~~ ~~b)-2 Any portion acting as a catalysit for hydrazine, such as rust, is eliminated. Inspection before operation is acceptable as a hazard control.~~ ~~c) Operation in accorddance with JERG-1-007. (AGE/GSE is used inside pressurized explosion-proofed room, etc.)~~ ~~4.1.1.2 Hazardous operation~~ ~~4.1.2 Hazardous atmosphere~~ ~~Note: Summary of compliance with requirements for launch site operation shall be attached.~~	~~□~~ ~~□~~ ~~□~~		
~~1.3 Operation at explosive hazardous atmosphere.~~	~~a) Operation is not conducted under explosive hazardous atmosphere. (No verification required.)~~	~~□~~		

F

~~JAXA Payload~~		~~Hazard Title~~	~~A.Review Phase~~	~~B.Date~~
~~Standard Hazard Report~~		~~Standard Hazard~~		
~~Note: This item is applicable if operation is conducted under explosive hazardous atmosphere.~~	~~b) Operation in accordance with JERG-1-007.~~ ~~4.1.1.2 Hazardous operation~~ ~~4.1.2 Hazardous atmosphere~~ ~~4.1.8.2 Protective equipment~~ ~~Note: Summary of compliance with requirements for launch site operation shall be attached.~~	☐		
~~HR-2 EMC~~ ~~Note1: Scope of susceptibility assessment is limitted to safety critical function.~~ ~~Note2: EMC assessment shall be conducted if inadvertent power-on during launch is credible even under cold launch mission.~~	~~a) EMC testing to verify compliance with ICD for operated environment.~~ ~~b) EMC analysis to verify compliance with ICD for operated environment.~~	☐ ☐		
~~HR-3 Electrical Shock~~	~~a) Voltage of battery or GSE/AGE is less than 30V DC/AC. Or COTS equipment powered from commercial 100V power supply is used under rated condition.~~	☐		

F

F

~~JAXA Payload~~	~~Hazard Title~~	~~A.Review Phase~~	~~B.Date~~
~~Standard Hazard Report~~	~~Standard Hazard~~		
	~~b) Meets all of the following.~~ ~~b)-1 Design to eliminate exposed high voltage surface greater than 30V. (Unmated powered connecter pin shall be considered.).~~ ~~b)-2 Appropriate grounding/bonding to prevent electrical shock.~~ ~~(This shall be applied to equipments that has internal high voltage source even without exposed high voltage surface.)~~ ~~c) Operation in accordance with JERG-1-007.~~ ~~4.1.1.2 Hazardous operation~~ ~~4.6 Electricity/electron related operation~~ ~~Note: Summary of compliance with requirements for launch site operation shall be attached.~~	~~☐~~ ~~☐~~	
~~HR-4 Personnel or equipment fall during operation in high places~~ ~~4.1 operation in high places~~ ~~Note: Safety assessment for design of high place platform shall be~~	~~a) Operation in high places higher than 2m is not conducted. (No verification required.)~~ ~~b) Operation in accordance with JERG-1-007.~~ ~~4.1.1.2 Hazardous operation~~ ~~4.1.8.2 Protective equipment~~	~~☐~~ ~~☐~~	

~~**JAXA Payload**~~		~~**Hazard Title**~~	~~**A.Review Phase**~~	~~**B.Date**~~
~~**Standard Hazard Report**~~		~~**Standard Hazard**~~		
~~addressed at unique hazard report.~~	~~4.1.8.7 Operation at high elevation~~ ~~Note1: Summary of compliance with requirements for launch site operation shall be attached.~~ ~~Note2: COTS equipment or existing GSE/AGE shall be confirmed if it can be operated under rated condition.~~			
~~4.2 falling protection of equipments~~	~~a) Tools are not used in high places. Or operations with tools are conducted in non hazardous area. (No verification required.)~~ ~~b) Operation in accordance with JERG-1-007.~~ ~~4.1.8.4 Tool control~~	☐		
~~HR-5 Falling or collision of lifted heavy items during handling operation~~ ~~Note: Safety assessment for design of handling GSE shall be addressed at unique hazard report.~~	~~a) Lifting/hoisting operation for equipment exceeding 20kg is not conducted at launch site. (No verification required.)~~ ~~b) Meets all of the following.~~ ~~b)-1 The load per person during handling operation is less than 20kg.~~ ~~b)-2 Operation in accordance with JERG-1-007.~~ ~~4.1.1.2 Hazardous operation~~ ~~4.1.8.2 Protective equipment~~ ~~4.1.8.4 Tool control~~	☐ ☐		

F

~~JAXA Payload~~	~~Hazard Title~~	~~A.Review Phase~~	~~B.Date~~
~~Standard Hazard Report~~	~~Standard Hazard~~		

	~~4.2 Transporting, transferring, and handling equipment~~ ~~Note1: Summary of compliance with requirements for launch site operation shall be attached.~~ ~~Note2: COTS equipment or existing GSE/AGE shall be confirmed if it can be operated under rated condition.~~		
~~HR-6 Battery rupture, electrolyte leakage~~ ~~6.1 COTS Li-Ion Battery~~ ~~Note: As used herein, COTS Li-Ion Battery is complied with UN Recommendations.~~ ~~Note: Summary of battery specification and its configuration on payload shall be attached.~~	~~a) COTS Li-Ion Battery is not used. (No verification required.)~~ ~~b) Meets all of the following.~~ ~~b)-1 Li-Ion Battery is complied with CSA-108024 "Guidelines for Safety Design of Commercial Li-ion Batteries for Spaceflight Applications in Small Satellites" to verify the cell integrity against internal short, leakage, insulation or environment test.~~ ~~b)-2 external short~~ ~~Meets b)-2-1 OR b)-2-2.~~ ~~b)-2-1 Cell shall have at least two over current protection function (PTC, separator shutdown, etc.) for Battery External Short.~~ ~~b)-2-2 Double insulation/isolation on load side~~	~~☐~~ ~~☐~~	

~~JAXA Payload~~	~~Hazard Title~~	~~A.Review Phase~~	~~B.Date~~
~~Standard Hazard Report~~	~~Standard Hazard~~		

	~~b)-3 Overcharge~~ ~~b)-3-1 Battery is not charged after propellant loading or installation to launch vehicle.~~ ~~b)-3-2 Battery is not charged after opening fairing because Solar Array Panels are not exposed.~~		
~~6.2 COTS NiMH Battery~~ ~~Note: Summary of battery specification and its configuration on payload shall be attached.~~	~~a) COTS Ni-MH Battery is not used. (No verification required.)~~ ~~b) Meets all of the following.~~ ~~b)-1 Battery is not charged under exposed condition.~~ ~~b)-2 external short~~ ~~Meets b)-2-1 OR b)-2-2.~~ ~~b)-2-1Overheat due to short circuit does not affect to surrounding components (such as pyrotechnic, propellant).~~ ~~b)-2-2 Double insulation/isolation on load side~~	☐ ☐	
~~HR-7 Asphyxiation due to lack of oxygen~~	~~Meets a) or b), and meet c) if applicable.~~ ~~a) The operation under potential oxygen-deficient atmosphere in the launch site is not conducted. (No verification required.)~~ ~~b) Operation in accordance with JERG-1-007. 4.1.1.2 Hazardous operation~~	☐ ☐	

~~JAXA Payload~~		~~Hazard Title~~	~~A.Review Phase~~	~~B.Date~~
~~Standard Hazard Report~~		~~Standard Hazard~~		
	~~4.1.2.2 Other requirements for hazardous atmosphere area~~ ~~Note: Summary of compliance with requirements for launch site operation shall be attached.~~ ~~c) All of the following operations are applied when operation with SCAPE suit is conducted.~~ ~~c-1) Redundant breathing air supply system.~~ ~~c-2) Inspection of breathig air supply system before operation.~~ ~~c-3) Evacution after loss of air supply function.~~	 ~~□~~		
~~HR-8 Noise~~	~~a) The operation under noisy environment in the launch site is not conducted. (No verification required.)~~ ~~b) Operation in accordance with JERG-1-007.~~ ~~4.1.1.2 Hazardous operation~~ ~~4.1.8.2 Protective equipment~~ ~~4.1.6 Acoustic noise~~ ~~Note: Summary of compliance with requirements for launch site operation shall be attached.~~	~~□~~ ~~□~~		
~~HR-9 Personel injury due to hot or cold surface~~	~~a) There is no extreme high or low temperature portion on payload, AGE, etc.(No verification required.)~~ ~~b) Design to Eliminate exposed high or low temperature surface.~~	~~□~~ ~~□~~		

F

~~JAXA Payload~~	~~Hazard Title~~	~~A.Review Phase~~	~~B.Date~~
~~Standard Hazard Report~~	~~Standard Hazard~~		

	~~c) Operation in accordance with JERG-1-007.~~ ~~4.1.1.2 Hazardous operation~~ ~~4.1.8.2 Protective equipment~~ ~~Note: Summary of compliance with requirements for launch site operation shall be attached.~~	~~□~~	
~~HR-10 Laser~~ ~~Note: Laser that is categorized as class 3 in JIS C6802(Japanese law) shall be addressed in unique hazard report.~~	~~a) Lazar is not used on payload, AGE, etc.(No verification required.)~~ ~~b) Design, operation in accordance with JIS C6802.~~	~~□~~ ~~□~~	
~~HR-11. Sharp edge, corner, protrusion.~~ ~~Note: This item is applicable to newly developed hardware. COTS hardware is excluded because it is certified as a commercial product.~~	~~Meets a) or b), and meet c) if applicable.~~ ~~a) Burr is removed in accordance with inhouse specification. (No verification is required if hardware is mamufactured under appropriate quality control.)~~ ~~b) Design to eliminate sharp edge, corner or protrusion.~~ ~~c) Appropriate operational control (cover, PPE, etc) is specified if design control is not feasible.~~	~~□~~ ~~□~~	
~~HR-12. Earthquake~~	~~a) Operation in accordance with JERG-1-007.~~ ~~4.1.1.4.4 Tidal wave and earthquake~~	~~□~~	

F

~~**JAXA Payload**~~		~~**Hazard Title**~~	~~**A.Review Phase**~~	~~**B.Date**~~
~~**Standard Hazard Report**~~		~~**Standard Hazard**~~		
~~Note: Safety assessment for newly developed GSE shall be addressed at unique hazard report.~~	~~b) When operation in high places over 2m or handling operation for items of over 20kg is conducted, meet the following.~~ ~~- Design to prevent falling, dropping, moving or collision of payload, AGE or personel caused by Earthquake. Also, appropriate operational procedure is specified.~~ ~~Note: COTS equipment or existing GSE/AGE shall be confirmed if it can be operated under rated condition.~~	☐		
~~13. Overheat or damage of wires~~	~~a) Battery is not used. (No verification required.)~~ ~~b) Wires are complied with CSA-112051 "Interpretation of Requirements for Safety Design (Wire Sizes) of Electric Systems"~~	☐ ☐		
~~14. Unique Hazard~~	~~Unique hazard is a hazard that is not identified above or cannot be applied the hazard control methods specified in this form.~~ ~~a) Structural failure of flight equipment~~ ~~b) Inadvertent operation of pyrotechnic device~~ ~~c) Inadvertent deployment of deployable mechanism.~~ ~~d) Rupture and/or explosion of pressure system~~ ~~e) Leakage and/or explosion of propellant~~ ~~f) Rupture, explosion and/or fire of battery~~ ~~g) Falling and/or dropping due to inadequate design of handling equipment for heavy material~~	☐ ☐ ☐ ☐ ☐ ☐ ☐		

F

~~JAXA Payload~~		~~Hazard Title~~	~~A.Review Phase~~	~~B.Date~~
~~Standard Hazard Report~~		~~Standard Hazard~~		
	~~h) Falling of personnel and/or tools due to inadequate design of high elevation platform~~ ~~i) Leakage of harmful fluids~~ ~~j) Excessive Levels of RF radiation~~ ~~Note: Add unique hazard below if identified other than the above hazards.~~	☐ ☐ ☐		

F

~~Instruction of JAXA Standard hazard Report~~

~~This form mainly addresses hazards and its controls which is commonly applicable to any payload. The following are instruction of this form.~~

F

~~A. Review Phase~~

~~Fill in review phase for system to be reviewed.~~

~~B. Date~~

~~Fill the issue date or revised date of this form.~~

~~C. Payload Name~~

~~Fill the name of system to be reviewed.~~

~~D. Launch Vehicle~~

~~Fill the name or flight number of launch vehicle to be installed the payload.~~

~~E. Approval~~

~~Before submitting SDP to JAXA safety review secretariat, this form must be signed by the project director or system safety program manager in "Contractor" and "Payload Organization" column of the appropriate phase with date. Refer to the approval column of previous phase HR, then type up the name and date in column of previous phase.~~

~~F. Hazard Description~~

~~If the hazard shown in this form is identified at the system to be reviewed, it can be documented on this form as a standard hazard.~~

~~Hazards which are not identical to HR-1 ~ HR-12 shall be documented on form specified in JMR-001 or JMR-002. In this case, check the check-box of relevant items a) ~ j) at "13. Unique Hazard" and describe hazard report number in "Verification Method, Reference Document, Status" column. Add item k) or higher if identified hazard is not identical to item a) ~ j).~~

~~Note: The number of unique hazard report may be 100 or higher. (To distinguish between unique hazard report and standard hazard report number (2 digits).)~~

~~**G. Hazard Control**~~

~~This column addresses the hazard control that is acceptable as a control for standard hazard. Safety of the hazard is determined as acceptable if this hazard control is applied to the payload.~~

F

~~**H. Applicability**~~

~~Check the applicable box for each hazard and hazard control consistent with the design of the payload. Double click the check box and select ON as default setting, and then you can check the box.~~

~~One of the hazard controls needs to be applied if there is no note such as "Meets all of the following" (All of controls need not be applied.) If there is a note such as "Meets all of the following", all of controls need to be applied, or develop unique hazard report if not appropriate.~~

~~**I. Verification Method, Reference Document, Status.**~~

~~Refer to particular test reports by document number and title. Indicate the status of the activity.~~

Attachment 2 Design Standards to implement Design for Minimum Risk

Design for minimum risk can be applied if the verification data to make a design on the basis of the following design standard specified by JAXA etc. can be indicated. Latest version of the documents should be applied.

(1) Structure

JERG-2-230 Structural Design Standards

CSA-110010 Precautions Related to Structural Safety Design and Verification when Ti-6Al-4V Material Fasteners are Used

CSA-111030 Concept of structural strength verification in launch vehicle payload safety analysis

CSA-112023 Guideline for control of Stress Corrosion Cracking on H-IIA piggyback small satellites

(2) Pressure vessels, Pressurized piping and joints

JERG-0-001 Technological Standard for High-Pressure Gas Equipment for Space Use

The High Pressure Gas Safety Law

(3) Pyrotechnic devices

JMR-002 LAUNCH VEHICLE PAYLOAD SAFETY STANDARD

section 5.5 Pyrotechnics system

(4) Material compatibility, Material flammability

JMR-002 LAUNCH VEHICLE PAYLOAD SAFETY STANDARD

section 5.1.3 Materials used

section 5.3 Propulsion System

section 5.4 Pressure System

section 5.10 Ground Support Equipment (GSE)

(5) Some mechanisms

CSA-111006 System Safety for Launch Vehicle Payload Mechanisms

CSA-112040 Safety checklist for Non-metallic Lock-wire design of the small satellite

(6) Explosive Hazardous Atmosphere

CSA-109009 Interpretations of “JMR-002B 5.2.2.3 Requirements for Electrical Equipment Used in an Explosive Hazardous Atmosphere”

(7) Electrical system

JERG-2-213 Insulation Design Standards

CSA-108024 Guidelines for Safety Design of Commercial Li-ion Batteries for Spaceflight Applications in Small Satellites

CSA-112026 Interpretation of safety requirement for JMR-002B 5.6.3 Lithium-ion batteries

CSA-112051 Interpretation of Requirements for Safety Design (Wire Sizes) of Electric Systems

(8) Other adequate Standards whose implementation can reduce the risk as low as acceptable.