General

LAUNCH VEHICLE PAYLOAD SAFETY STANDARD

Rev. E, 24 November, 2022

Japan Aerospace Exploration Agency

This is an English translation of JMR-002E and does not constitute itself.
Whenever this document conflicts with the original document in Japanese, the original document takes precedence.

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

Contents

1. General

1.1 Purpose

The purpose of this Standard is to specify integrated requirements for safety management and design that the payload responsible organization (hereinafter referred "PL organization") shall implement to protect human life, properties (of public and third party), and environments from adverse effects of mishap occurrence associated with launch vehicle payload (hereinafter referred to as "payload") to be launched from Japan Aerospace Exploration Agency (JAXA) Tanegashima Space Center or JAXA Uchinoura Space Center (hereinaftere referred to as "Kagoshima Space Centere (KSC)"), as well as payload's Ground Support Equipment (GSE), during the period from delivery to KSC to through launch site operation and launch and until payload separation from launch vehicle.

1.2 Application

PL organization using KSC shall apply this standard for their payload and GSE (hereinafter referred to as the "payload/GSE") by defining in documents such as the contract between the PL organization and JAXA.
This standard is not applied to operations where safety can be ensured only by complying with laws and prescriptive regulations (such as requirements for occupational safety based on the Japanese Industrial Safety and Health Act). PL organization must be responsible for ensuring the safety of their own personnel while complying with relevant laws, regulations and JAXA standards.
Especially, the PL organization which plans operation in KSC shall comply with the "Safety Regulation for Launch Site Operation" (JERG-1-007).

Note: For payloads to which JMR-001 "System Safety Standard" is applied, the requirements of JMR-001 take precedence over those in Chapter 4 of this standard.

1.3 Responsibilities of each organization

PL organization has the following responsibilities.

(1) Taking necessary measures to ensure safety related to payload/GSE in accordance with this standard.
(2) Submitting the documents for safety review specified in this standard to the JAXA Safety and Mission Assurance Department by the specified date before safety review panel.
(3) Completing the safety review process specified in this standard.

JAXA has the following responsibility.

(1) Confirming that the safety review documents submitted by the PL organization are compliant with this standard by the prescribed date.

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. PL organization shall consult with the JAXA Safety and Mission Assurance Department for tailoring requirements and rationales, reflect the changes in the system safety program plan (refer to section 4.2.1), and receive approval of JAXA system safety review panel described in section 4.6.
(2) Tailoring of safety requirements
Safety requirements 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.
PL organization shall consult with the JAXA Safety and Mission Assurance Department for tailoring requirements and rationales, describe the changes in Format 1 or an equivalent format, attach the Table to

the system safety program plan, and receive approval of JAXA system safety review.

2. Applicable documents

The following documents constitute a part of this Standard to the extent specified in this Standard. The applicable documents shall be the latest version available at the time of application, and the applicable version shall be indicated in the system safety program plan.

2.1 Applicable documents

(1) JERG-0-001 "Technical Standard for High Pressure Gas Equipment for Space Use "
(2) CZA-2018029 "Launch Vehicle Payload System Safety Program Plan/Safety Data Package Template"
(3) JERG-1-007 "Safety Regulation for Launch Site Operation"

2.2 Reference documents

(1) NPR8715.3 "NASA Procedual Requirements, NASA General Safety Program Requirements Chapter 2. System Safety"
(2) MIL-STD-882 "Department of Defense Standard Practice for System Safety"
(3) CZC-117001 "System Safety Review Panel Management Procedure"

3. Terms and definitions

For the purposes of this standard, the following terms and definition apply.

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

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.

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).

Ground Support Equipment (GSE)
The ground equipment necessary for handling, testing and inspecting a payload.

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 a mishap. (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 fault tolerant design or design for minimum risk. In broader sense, safety device, protective device, warning systems, special procedures and training are included. In this Standard, the broader meaning is applied.

Hazard report
A report that is documented technical information as a result of hazard analysis related to payload/GSE, 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 hazards

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

Inhibit
Any physical method that interrupts energy to initiate hazardous functions, installed to prevent unintended operation of hazardous functions. Inhibits are used as a means of implementing fault tolerant design. Examples of inhibits include relays in electrical circuits, shut-off vales in piping.

Launch Site Operation
Launch processing operation of launch vehicles or payload/GSE and operations of facility/equipment performed at KSC.

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.

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.

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)
Personnel (shown below), public citizen and/or visitor inside/outside KSC.

Personnel (corresponding to “yoin” in Japanese version)
The people of JAXA, PL organization who are engaged in specific operations.

PL organization
An organization of individuals, groups, companies, or insutitutions that conduct payload/GSE development, launch site operations, and etc. If the launch is to be performed by a launch transportation service provider, the organization includes the above and the launch transportation service provider.

Potting
To fill a compound in a part of an electric circuit 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.

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 of 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
A physical barrier that is designed to protect personnel and equipment from a mishap that has been identified as hazard (e.g., casings for rotation objects such as motor, cover guards).

Pyro-valve
A valve which is switched open or close by the pyrotechnics operation.

Reflight payload
A Payload (including payload elements) that has been launched from the KSC in the past are recovered and re-launched at the same launch site.

Risk
Product of hazard severity and likelihood of occurrence.

Safe and Arm Device
A device with electrical and mechanical safety mechanisms that prevents inadvertent operation (on ground) of pyrotechnics that are mainly used for ignition for solid rocket motor.

Safety
The state that hazards are eliminated, minimized or controlled not to lead mishap, i.e. risk level is low as acceptable.

Safety critical
Any condition that identified hazard severity is I or II. e.g., “safety critical” operational procedure, “safety critical” parts.

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 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.

Series payload
A follow-on payload of the same or similar* design as a payload (including payload elements) launched from KSC in the past.
*Payload for which past hazard analysis can be applied. In other words, the design related to safety is the same, past hazard analysis including safety verification results (excluding those related to manufacturing) can be applied, and only minor changes need to be evaluated.

Special procedures
If hazard control is insufficient by design, or by installation of a safety device, protection device or warning device, the likelihood of a hazard occurring needs to be reduced by operation. In this case, hazard control is implemented through personnel education and training, appropriate operational procedures, and necessary maintenance.

Stray voltage
The voltage measured to check for the stray current.

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.

Tailoring
An action of modifying the requirements into a requirement that is appropriate for the applicable target, by selecting or modifying the requirements in consideration of the various conditions of the applicable target.
Warning devices
A device that detects a specific hazardous condition or similar condition timely and generates an appropriate warning signal to caution personnel.

4. System safety requirements

4.1 Basic requirements

The PL organization shall plan and implement system safety program considering the following requirements for safety from payload/GSE arrival to KSC, launch site operations, and to payload separation from the launch vehicle after launch.

This Standard sets forth the following basic requirements:

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

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

(3) For each hazard, the cause of the hazard shall be identified, and hazard control shall be set for each cause. As an exception, from the payload handover to the launch vehicle, the period of joint operations with the launch vehicle, to the payload separation from the launch vehicle after launch, safety measures required based on the results of launch vehicle hazard analysis shall be implemented.

(4) Effectiveness of hazard control shall be verified by test, inspection, analysis or other appropriate means.

(5) Operating procedures, education/training plans, etc., shall include necessary hazard controls. Operations shall be performed in accordance with the procedures.

(6) System safety program plan (see section 4.2.1) and Safety data package (see section 4.5) shall be maintained and managed.

(7) 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, schedule of prepared documents submission.

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 reference documents (1) (2), or equivalent standards will also be acceptable. The format of the applicable document (2) is also acceptable.

Table 4.2.1-1 System safety program plan – Typical table of contents

Item	Remarks	Applicable Psection
1. General 1.1 Purpose		
1.2 Scope	From payload/GSE arrival to KSC, launch site operations, and to payload separation from the launch vehicle after launch	1.1 1.2
2. Related documents To indicate applicable and reference documents.	The applicable edition shall be described. Tailoring shall be described, if any.(*) If requirements other than JMR-002 (e.g., foreign standards) are applied, identified standards shall be described.	1.4 and other sections
3. Implementation items		

3.1 Organization and implementation system (1) To clearly specify the project manager, the system safety program manager, the person in charge, and related sections. (2) To illustrate the system safety management organization including related sections.	If the contractor is included in the system safety program management, the contractor shall be described. The division of responsibilities for statutory procedures to public offices shall be described.	4.2.3
3.2 System safety review method	The integration of the safety review phase or the implementation of safety reviews for series payloads/reflight payloads shall be described, if any.	4.6
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 4.6-1 Fig. 4.2.2-1

*: Tailored items shall be described using Format-1.

4.2.2 System safety program activities

The PL organization 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 4.2.2-1. Outline of system safety program activities performed during each phase are described below.

(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 during the conceptual study/definition design phase and the results documented.
   c. If tailoring safety requirements, the content of the tailoring shall be specified.

(2) Preliminary design phase (Phase I)
   a. Phase I hazard analysis shall be conducted during the preliminary design phase and the results documented.
   b. If any item that does not comply with safety requirements, the redesign shall be done to comply with the safety requirements. If it is difficult to comply with the safety requirements, a noncompliance report form (see section 4.3.1.9) shall be prepared by clarifying that the residual risk is at an acceptable level, and the contents shall be approved by the safety review by JAXA. The same shall apply to Phase II and III.

(3) Critical design phase (Phase II)
   a. Phase II hazard analysis shall be conducted during the critical design phase and the results documented.

(4) Manufacturing/testing phase (Phase III)
   a. Phase III hazard analysis shall be conducted during the manufacturing/testing phase and the results documented.

(5) Operation phase (after Phase III)

a. The results of phase III hazard analysis shall be revisited, if necessary.
   - If any hazard is newly identified, go back to the required phase and perform the hazard analysis.
   - If the design is to be changed, it shall be implemented from the identification of safety requirements again.
   - When making changes to the procedures, reconfirm that they reflect the necessary hazard controls.

b. To ensure the safety of operations, all operations shall be confirmed to be conducted in accordance with the system safety program plan and operating procedures.

(6) Series payload/reflight payload system safety program activities

If the PL organization wishes to streamline the hazard analysis and safety review process for a series payload or reflight payload to be launched on the same launch vehicle as in the past, the PL organization shall:

a. Provide justification being a series payload/reflight payload in the system safety program plan. System safety program activities for multiple series payloads may be managed in a single system safety program plan.

b. Evaluate the impact of differences between the old and new versions of applicable documents and safety requirements.

c. Perform the hazard analysis shown in section 4.3.1.11.

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 PL organization 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 PL organization 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 package.

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 Safety and Mission Assurance Department regarding system safety management.

Time(month/year) / Phase / System safety program activity		Conceptual study/ Definition design (Phase 0)	Preliminary design (Phase I)	Critical design (Phase II)	Manufacturing/ Verification (Phase III)	Operation	Remark
Overall milestone	PL organization	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		Phase 0 safety review ▽	Phase I safety review ▽	Phase II safety review ▽	Phase III safety review ▽	Post-Phase III safety review ▽(If necessary)	
Hazard analysis		Phase 0 hazard analysis	Phase I hazard analysis	Phase II hazard analysis	Phase III hazard analysis		
Safety requirements		Initial identification of safety requirements ▽ Identification of safety requirements ▽	(As necessary) Add details to Requirements /Review ▽ ▽				
Operation procedures and other procedures					Preparation (Manufacturing/Process specifications, Test Procedures, etc.)	Preparation (Operation Procedures)	

Figure 4.2.2-1 System safety program activities in the life cycle

4.3 System safety engineering

4.3.1 Hazard analysis

The PL organization shall conduct hazard analysis from the early design phase, identify hazards, establish hazard control methods, and reflect these methods in design procedures, and operations.

4.3.1.1 Subject of hazard analysis

(1) Applicable period

The applicable period for hazard analysis is during the payload launch site operations from the arrival of the payload to the KSC to the payload handover to the launch vehicle. After the payload handover to the launch vehicle, during the period of joint operations with the launch vehicle until the separation of the payload from the launch vehicle after launch, the safety requirements established based on the results of the launch vehicle hazard analysis shall be applied.

(2) Treatment of laws, regulations of Japan, and safety rules/standards of JAXA

As described in section 1.2, cases in which safety can be ensured only by compliance with laws, regulations of Japan, and safety rules/standards of JAXA (e.g. personnel safety based on the Occupational Safety and Health Law) are not included in the hazard analysis.

4.3.1.2 Hazard identification

After fully understanding the configuration, functions, etc. of the payload/GSE to be covered, assuming possible mishaps, all potential and actual hazard sources shall be identified, and the results shall be listed in the hazard identification summary table shown in Format-2 or similar other table. The severity and likelihood of occurrence shall be determined with reference to the following.

As a result of hazard identification, hazard reports shall be prepared for severity I and II, the causes of the hazard shall be eliminated/controlled, and the acceptability of the residual risk indicated in section 4.3.1.6 shall be evaluated.

Severity III and IV are acceptable with normal design, manufacturing, and operation. Hazard reports need not be prepared. For hazards that are outside the scope of hazard report preparation, the rationale for being outside the scope shall be clarified in a hazard analysis table (Format-3) or similar analysis.

a. Severity

Severity is indicated using Severity categories I, II, III, and IV as shown in Table 4.3.1.2-1 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 4.3.1.2-1 Severity categories

Severity	Terminology	Description
I	Catastrophic	Death or severe personal damage Irreversible significant environmental impact Loss of or severe damage to public or third party property Loss of launch site facilities

II	Critical	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	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 cause less damages than Hazard level I to III.

b. 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 4.3.1.2-2). For example, this may be derived from analysis of past safety data on similar system.

Table 4.3.1.2-2 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

4.3.1.3 Identification of the hazard cause

For the hazards identified in section 4.3.1.2, hazard causes shall be extracted considering the target hardware, software, operation, human error, interface, and environmental conditions. As a reference, it is also effective to cross-check with FMEA as well as the FTA.

4.3.1.4 Elimination/control of hazard causes

For severity I and II, the hazard causes identified in section 4.3.1.3 shall be eliminated or controlled. Elimination/control of hazard causes shall be performed in accordance with the following safety design priorities.

(1) Design to eliminate hazard.
(2) Design to minimize hazard.
(3) Design to control hazard.

4.3.1.5 Design to control hazard

In the designing to hazard controls of payload/GSE as specified in section 4.3.1.4 (3), basically, fault tolerant (FT) design shall be applied. When the verification data to make an appropriate design on the basis of section

4.3.1.5.2 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 applied. If PRA is used, the PL organization shall coordinate with JAXA Safety and Mission Assurance Department prior to the safety review.
Chapter 5 of this standard contains examples of general hazard control methods that can be applied when conducting the hazard analysis in Chapter 4. Payload/GSE shall implement hazard control with reference to these examples. For hazards that cannot be covered in Chapter 5, hazard controls shall be implemented individually.

4.3.1.5.1 Fault tolerant design requirements (explanation provided in Attachment-2)

Design shall satisfy the following fault tolerant requirements to lower the likelihood of occurrence to the acceptable level by controlling hazards according to the severity:
(1) Control of catastrophic hazards
Payload/GSE shall be designed to ensure that any combination of two faults, two human errors, or single fault and single human error will not result in a catastrophic hazard.
(2) Control of critical hazards
Payload/GSE shall be designed to ensure that single fault or single human error will not result in a critical hazard.

Supplement 1: When implementing this section, consider the following:

- The fault tolerant design shall be implemented with the required number of independent inhibits between the energy source and hazardous functions, or means other than inhibits.
- The design shall preclude increase of mishap 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.
- The design shall prevent loss of multible hazard controls at the same time due to common causes or events.
- Safety critical redundant systems which controls catastrophic and critical hazards shall be separated from each other as much as practically possible or protected to prevent compromise of both systems.
- If a operation is required to activate the hazard control, the operation shall be taken into account in the procedure.

Supplement 2: When implementing this section, consider the following for functions that must be kept in operation to ensure safety:

- Prevent the creation of new hazards as well as the inability to maintain safe conditions.
- Prepare for power supply interruptions, etc. and maintain safety until restoration.

Supplement 3: Basically, fault tolerant design shall be implemented as part of the design of payload/GSE, butmethods (1) through (4) may be used in the rollowing order of priority. For definitions, see Section 3.

(1) Use of safety devices.
(2) Use of protective devices.
(3) Use of warning devices.
(4) Application of hazard control relying on special procedures

4.3.1.5.2 Design for minimum risk

If the verification data for proper design based on the design standard specified by JAXA and etc. (see

Attachment-1) can be indicated, design for minimum risk can be applied. The design shall be managed by considering sufficient design margins, safety factors, and appropriate selection of material and EEE parts. When design standard other than Attachment-1 are used as a basis, The PL organization shall coordinate with JAXA Safety and Mission Assurance Department prior to the safety review. Design for minimum risk is usually applied to the following.

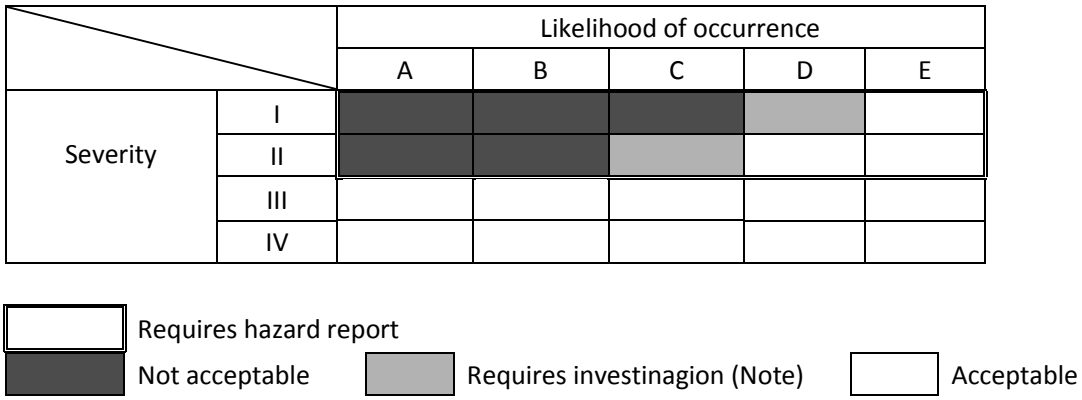
- Structures • Pressure vessels • Pressurized line and fittings • Pyrotechnic devices
- Material compatibility • Material flammability • Some mechanisms

4.3.1.6 Residual risk assessment

For severity I and II, the residual risk as a result of the eliminate/control of the hazard cause shall be evaluated, and a determination of acceptability shall be made based on Figure 4.3.1.6-1. For the severity I, the likelihood of occurrence E, and for the severity II, the likelihood of D or E are acceptable.

If the PL organization propose criteria equivalent to the risk acceptance criteria, the PL organization shall coordinate with JAXA Safety and Mission Assurance Department prior to the safety review. 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, 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.

Figure 4.3.1.6-1 Risk acceptance criteria

4.3.1.7 Safety verification

The effectiveness of the control methods for the hazard causes described in section 4.3.1.5 shall be confirmed by 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. The identification information such as their document numbers shall be shown in hazard report.

For the hazard analysis for series payload/reflight payload, previous verification procedures and requirements referred shall be studied to adequately evaluate their similarities.

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 (SVTL, Format-4) for tracking and management. In addition, the completion and submission dates of the verification items shall be

set in advance, and the results of the items shall be submitted to the JAXA Safety and Mission Assurance Department by the set dates. If the effectiveness of the hazard control depends on the launch configuration, launch configuration settings shall be tracked by SVTL.

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.

4.3.1.8 Hazard report

(1) If the results of hazard identification in section 4.3.1.2 indicate that a hazard is within the scope of reporting, a hazard report shall be prepared.

(2) If a separate hazard report is created for each subsystem or component, it shall be shown that the hazard report is valid when evaluated as a system.

(3) The hazard report shall include an analysis of the applicable safety requirements (Capter 5 of this standard and any additional requirements), hazard classification, description of the hazard, hazard causes, hazard controls, safety verification methods, and shall indicate the status of verification.

(4) The hazard report shall be accompanied by supplementary explanatory material outlining the hazard controls, safety verification methods, and safety verification results.

(5) The format of the hazard report shall be as follows:
- For general hazards, the format in Applicable Document (2) can be used.
- For unique hazards that do not correspond to the above, prepare a report using Format-5 or similar other format.

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

4.3.1.9 Noncompliance Report (NCR)

If payload/GSE fails to comply with requirements specified in hazard reports, the PL organization shall coordinate with JAXA Safety and Mission Assurance Department, examine compliance in detail, record the examination results in the noncompliance report (Format-6), and receive the approval from the safety review of JAXA. The noncompliance report shall be linked to the hazard report.

4 3.1.10 Phased hazard analysis

The 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 shall be performed during conceptual study/definition design phase to identify hazards and hazard causes, and examine hazard controls with reference to Chapter 5 of this standard. In addition to Chapter 5, other applicable requirements shall be identified, if any. The results shall be summarized in the Hazard Identification Summary (Format-2) and the Hazard Analysis Table (Format-3). 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 that are identified during testing, transportation, handling, operation, and etc.
d. Clearly define safety issues regarding interfaces.

e. Estimation of expected damage of mishap 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.

The hazard report shall be developed for hazards that are classified as coverage of hazard report to be prepared as defined in 4.3.1.2, and the hazard report shall be reviewed as phase progressed. Hazard report shall contain the following:

a. To identify hazard causes and to establish appropriate hazard elimination and control.
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 catastrophic/critical hazards. Cross checking with FMEA (Failure Mode and Effects Analysis) to prevent omissions is also effective.
d. To reflect necessary corrective measures in design based on the results of analysis, considering safety related design constraints.
e. 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 in hazard reports and incorporated into the design.
b. To re-assess the results of FTA 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 in hazard reports, and reflect these to safety maintenance and improvement activity.
e. To specify verification methods in hazard reports.

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

The purpose of Phase III hazard analysis is to perform detailed safety assessment of operations by reassessing 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 in hazard reports.
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 in hazard reports and reflect these to safety maintenance and improvement activity.

d. To clarify the verification results of hazard control in hazard reports, and those safety verifications that can only be confirmed at the launch site shall be documented in the safety verification tracking log (Format-4, or equivalent format) and individually close prior to operation.

4.3.1.11 Hazard analysis of series payload/reflight payload

The purpose of series payload/reflight payload hazard analysis is to perform a safety assessment compared to the baseline payload hazard analysis. This hazard analysis shall contain the following:

(1) All design changes (including parts and software) and changes in operational conditions and procedures, to the baseline payload shall be identified, and their impact on the hazard analysis of the series payload/reflight payload shall be assessed.

(2) The impact on the series payload/reflight payload hazard analysis for all anomalies/failures in the baseline payload shall be evaluate. Anomalies/failures related to safety-critical systems shall be corrected.

(3) Tests, inspections, etc. on the newly produced hardware shall be conducted to reverify the effectiveness of the hazard control established in the past. This is mainly based on environmental conditions, taking into account new operational scenarios, and includes, if necessary, a review of past analysis and verification items.

(4) Safety requirement noncompliances in the baseline payload shall be reconfirmed as to their basis of acceptance and corrected if necessary.

(5) For reflight payload, the life limited items, maintenance, structural inspection, and safety impact of refurbishment shall be evaluated.

4.4 Compliance assessment of safety measures required based on the results of launch vehicle hazard analysis

During the period of joint operations with the launch vehicle from the payload handover to the launch vehicle to the separation of the payload from the launch vehicle, the launch vehicle identifies payload-related hazard causes and this information is provided to the PL organization. The PL organization shall conduct the following:

(1) To establish hazard controls to prevent the occurrence of the presented hazard causes.

(2) To confirm the effectiveness of the established hazard controls by safety verification.

(3) To document the results of the compliance assessment of the safety measures required based on the results of launch vehicle hazard analysis in the prescribed format provided by the launch vehicle.

(4) If there is a specific payload-related hazard cause other than the hazard causes identified by the launch vehicle, it is necessary for the launch vehicle to conduct an additional hazard analysis. The PL organization shall coordinate with the launch vehicle the measures to be taken, and then coordinate with JAXA Safety and Mission Assurance Department prior to the safety review.

4.5 Safety data package

The result of the hazard analysis shall be compiled into a safety data package, which shall be used as a document for the safety review described in section 4.6. Typical table of contents of safety data package is shown in table 4.5-1.

Table 4.5-1 Safety data package – Typical table of contents

Item	Remarks	Applicable section
1. General 1.1. Purpose		

1.2. Scope		4.3.1.1 4.3.1.2
2. Related documents	To indicate applicable and reference documents.	
3. Description of the payload/GSE 3.1. Basic information of the payload/GSE	Main specifications, payload appearance (launch and on-orbit configuration)	
3.2. Overview of design and function of the payload/GSE	At a minimum, provide the information necessary to understand the hazard analysis in section 4 (e.g. system configuration block diagram) Details on functions used for hazard control shall be attached in hazard report.	
3.3. Flowchart of the launch site operation and description of each task	At a minimum, provide the information necessary to understand the hazard analysis in section 4. Operations that require hazard control shall be identified.	
4. Hazard analysis result		4.3.1
4.1. Hazard identification summary		4.3.1.2
4.2. Hazard analysis table		4.3.1.2
4.3. FTA or other analysis	Only if there are catastrophic/critical hazards.	4.3.1.3 4.3.1.10
4.4. Hazard report	Only if there are catastrophic/critical hazards. Details on functions used for hazard control (schematic and block diagram showing inhibits, etc.) shall be attached in hazard report.	4.3.1.8
4.5. Compliance assessment of safety measures required based on the results of launch vehicle hazard analysis	Phase II and III only	4.4
4.6. Safety verification tracking log (SVTL)	Only if there are safety verification items that has not been completed at the time the Phase III HR is prepared.	4.3.1.7 4.3.1.10
4.7. Noncompliance report (NCR)	Only if there are requirement noncompliance. NCR shall be associated with the hazard report.	4.3.1.9

4.6 System safety review

The PL organization shall undergo system safety review by JAXA 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. General outline of safety review is shown in table 4.6-1.

The objective of the JAXA system safety review is to prevent major damage to JAXA's facilities and equipment, and damage to other person than operating personnel in the regulated area. To achieve this objective, the following will be assessed. The occupational safety of the personnel of the PL organization is not included in the scope of the JAXA system safety review as described in section 1.2.

- The compliance with the safety reqiurements set according to the hazard identified in relation to the payload/GSE during the period of payload operations from the arrival of the payload to the KSC to the payload handover to the launch vehicle is confirmed. And identification of hazard and its causes, controls, verification methods, verification results, and acceptability of minimized the risk that cannot be eliminated (residual risk) are also evaluated.

- The compliance with the safety measures required based on the results of launch vehicle hazard analysis during the period of joint operations with the launch vehicle from the payload handover to the launch vehicle to the separation of the payload from the launch vehicle is evaluated.

(1) In general, safety review is conducted four times for the payload/GSE developed by JAXA, one per each development phase; Phase 0, Phase I, Phase II, and Phase III safety reviews. However, if the PL organization judges that the development risk is sufficiently small, phased safety reviews may be integrated depending on the scale of the system, experiences in foreign countries, etc. The method of integration is expected as three times for Phase 0/I, II, and III, twice for Phase 0/I/II, and III, and once for Phase 0/I/II/III. Each phased safety review may be conducted as a part of the overall milestone reviews after coordination with JAXA.

(2) The system safety review of JAXA is conducted in accordance with the reference document (3). The overview of safety review is described in table 4.6-1 including schedule for each safety review to be performed, purpose of review, documents to be reviewed.

(3) Based on table 4.6-1, a system safety program plan and a safety data package shall be submitted to the JAXA Safety and Mission Assurance Department by the designated date before the safety review is conducted.

(4) Compliance assessment of safety measures required based on the results of launch vehicle hazard analysis shall be evaluated by launch vehicle safety review (the PL organization only submit document to launch vehicle) or during this safety review.

(5) If there are any changes or additions to the contents of the Phase III safety review, the PL organization shall coordinate with the JAXA Safety and Mission Assurance Department, and post-Phase III safety review shall be conducted as necessary.

Table 4.6-1 General outline of safety review

Type of safety review	Review timing	Purpose of review	Review documents
Phase 0 safety review	Upon completion of conceptual study/definition design	a. To confirm hazards and their causes b. To confirm applicable safety requirements (including additional requirements per tailoring and hazard analysis.)	a. System safety program plan b. Safety data package
Phase I safety review	During preliminary design review (PDR)	a. To confirm hazards and their causes b. To confirm hazard control methods, verification methods c. To confirm safety requirements added as necessary.	a. System safety program plan b. Safety data package
Phase II safety review	During critical design review (CDR)	a. To confirm that a hazard control method is implemented in the design b. To confirm that a verification methods is established c. To confirm the compliance with safety measures required based on the results of launch vehicle hazard analysis	a. System safety program plan b. Safety data package (The description shall include schematic and block diagrams showing safety features, fault tolerant (FT) designs, and etc. The required number of FTs and its controls and their independence shall be clearly identified especially in electrical schematics)
Phase III safety review	During development completion review	To determine that it is acceptable to begin launch site operations with hazards at the KSC, the following is confirmed. a. To confirm that safety verification has been completed b. To confirm the compliance with safety measures required based on the results of launch vehicle hazard analysis (verification results) c. To confirm the appropriateness of transfer to the SVTL for verifications that have not been completed which can only be verified at the launch site d. To confirm that all action items are closed	a. System safety program plan b. Safety data package (The description shall include summary of noncomformances that impact safety, and its safety assessment among all the noncomformances that occurred during fabrication, test, inspection of Payload/GSE)
Series payload /Reflight payload safety review	During critical design review (CDR) or, during development completion review	a. To confirm if any design changes, launch site/launch operations, or launch site/launch failures affect each phase of the baseline payload hazard analysis b. To confirm the results of difference (delta) of hazard analysis for the phase affected	a. System safety program plan b. Safety data package ・ The description shall include changes to the baseline payload and their impacts to the safety, for each package section. ・ The description shall include items in the baseline payload hazard report that need to be reverified and new items that need to be verified. ・ (Reflight payload only) The description shall include safety impact evaluation for life limited items, maintenance, structural inspection, and refurbishment.

Note 1) For the safety review of a series payload/reflight payload, a single Phase delta II/III review is nomally expected, including design changes. (If the hazard identification changes, a Phase delta I review is also required)

5. Hazard analysis guidelines

Section 5.1 through 5.8 of this chapter present typical hazard analyses that have been authorised in the past safety reviews of payloads. The hazard analysis in chapter 4 should be perfomed in consideration of these sections. Although this does not preclude hazard analysis using methods other than those in this chapter. Hazard analysis shall be performed comprehensively, not limited to the contents of this chapter, and safety measures shall be considered for each identified hazard. In particular, hazard analysis shall be conducted separately for pathogens that cause biohazards, ionizing radiation sources, and cryogenic fluids.

5.1 Prevention of fire and explosion hazard at the launch site (explanation provided in Attachment-2)

At the launch site,

A) A fire/explosion hazard occurs when the ignition source of the payload/GSE ignites in an explosive hazardous atmosphere (defined in JERG-1-007) is formed by leakage of flammable propellant or the presence of exposed solid propellant/pyrotechnic device.

B) A fire/explosion hazard occurs by mixing flammable propellant and oxidizer.

C) A fire hazard occurs when JIS C 6802 (IEC 60825-1) class 4 laser become ignition source.

This hazard is generally considered as a catastrophic hazard because fire and explosion can result in death or injury of person and loss of launch site facility and equipment. Appropriate hazard controls should be implemented to prevent this hazard. The following are typical measures: A) is prevented by (2) and (3) of this section, B) is prevented by (4), and C) is prevented by (5).

(1) As hazard analysis, flammable propellants and exposed solid propellants/pyrotechnic devices, oxidizers, and ignition sources that require hazard control in the payload/GSE are identified, respectively.

(2) Payload/GSE that is introduced into an explosive hazardous atmosphere are designed or operated so that they do not become ignition sources during normal use (failure need not be considered). The following are typical measures.
   a. For payload electrical equipment to be energized in explosive hazardous atmosphere, explosion proof measures such as potting, hermetic seals, and pressurization with inert gas are taken to prevent the equipment from becoming an ignition source. The electrical capacity of the electrical equipment is sufficiently small and below the ignition limit of the explosive gas to prevent it from becoming an ignition source is also an effective explosion proof measure. In addition, electrical equipment that is not explosion proof is not energized.
   b. For GSE electrical equipment to be energized in explosive hazardous atmosphere is “gas-explosion protection” in accordance with the national regulation “Constructional Requirements for Electrical Equipment for Explosive Atmospheres” or IEC 60079. When non-explosion proof equipment is brought into an explosive hazardous atmosphere, measures is taken in accordance with JERG-1-007.
   c. Payload/GSE is designed so that there are no exposed energized parts that can be touched by person. If there are exposed energized parts such as plasma thrusters, these are not energized in an explosive hazard atmosphere.
   d. Exposed electric heating wires are not energized in an explosive hazard atmosphere.
   e. Solid propellant/pyrotechnic device is not ignited in an explosive hazard atmosphere.
   f. Payload/GSE are bonded and grounded to prevent the generation of static electricity in an explosive hazardous atmosphere.
   g. For payload/GSE that are to be brought into an explosive hazardous atmosphere, nonflammable materials are used in areas where they may touch flammable propellants. And the existing of rust in such areas is avoided.

(3) Leakage of flammable propellants is prevented according to section 5.4 (2) through (7). When a two fault tolerant design is applied for leakage, there is no need to consider a failure with respect to contact between the leaked flammable propellant and the ignition source, and only consider normal state. In the case of taking additional measures to prevent contact between the leaked flammable propellant and the ignition source, the two fault tolerant design in section 5.4 (2) can be replaced as one fault tolerant.

(4) The two fault tolerant design (blocked by bulkheads, valves, etc.) is applied for mixing of flammable propellant and oxidizer. The design that prevents mixing due to mishandling during filling operation is also applied. (Use of different pipe diameters, placement of port connections in different positions and phases, etc.)

(5) For class 4 lasers, design and operate in accordance with JIS C 6802 (IEC 60825-1)

5.2 Prevention of pressure system burst hazard at the launch site

At the launch site, this hazard is generally considered as a catastrophic hazard because payload/GSE pressure system burst hazard can result in death or injury of person and loss of launch site facility and equipment. Appropriate hazard controls should be implemented to prevent this hazard. The following are typical measures:

(1) As hazard analysis, pressure systems that require hazard control in the payload/GSE are identified.
(2) Pressure system is applied design for minimum risk in accordance with JERG-0-001 and national law "High Pressure Gas Safety Act". In addition, the following are considered.
    a. The pressure design is considered assuming a pressure increase in the worst thermal environment due to failure such as heater malfunction, or leakage to the low-pressure side (consider two failures of a valve etc.).
    b. The two fault tolerant design is applied against overpressurization caused by incorrect operation procedures, such as incorrect operation of manual valves. When a pressure relief device is used as a failure tolerant design, the upstream of the device should not be disabled by a valve or other functions.
(3) Pressurization operation is performed in accordance with JERG-1-007 at the launch site.

5.3 Prevention of lithium-ion battery rupture hazard at the launch site (explanation provided in Attachment-2)

At the launch site, this hazard is generally considered as a catastrophic hazard because payload/GSE lithium-ion battery rupture hazard can result in death or injury of person and loss of launch site facility and equipment. Appropriate hazard controls should be implemented to prevent this hazard. The following are typical measures:

Note that the rupture of a lithium-ion battery of 100 Wh or less as a battery assembly is not considered as a catastrophic hazard or a critical hazard outside of an explosive hazardous atmosphere, but a rupture in an explosive hazardous atmosphere is considered a catastrophic hazard. Rupture of a Ni-MH battery is not considered as a catastrophic hazard or a critical hazard because of its low energy density.

(1) As hazard analysis, lithium-ion batteries that require hazard control in the payload/GSE are identified.
(2) Battery is designed not to rupture due to the following causes:
    a. Internal short of a cell
    b. External short of a cell
    c. Overcharge
    d. Use in abnormal temperature environments caused by thermal control system failure

5.4 Prevention of toxic material leakage hazard at the launch site

At the launch site, leakage hazard of toxic material such as propellants (hydrazine, MMH, etc.) and oxidizers (MON3, NTO, etc.) is generally considered as a catastrophic hazard because this hazard can result in death or injury of person and contamination of launch site facility and equipment. Appropriate hazard controls should be implemented to prevent this hazard. The following are typical measures:
The severity of toxic damage for propellants, oxidizers, and etc. other than those listed above should be considered on a case-by-case basis.

(1) As hazard analysis, toxic materials that require hazard control in the payload/GSE (Including post treatment after filling) are identified.
(2) All possible paths of leakage are identified, and leakage for each path should be prevented as follows:
    a. Two fault tolerant design is applied for the release operation of valves. that shut off the leakage path of toxic materials, taking the following into consideration.
        I. Two fault tolerant design is applied for valves and other outflow paths (leak paths). Note that "valve with two or more seals" and "a pyrovalve" can be regarded as equivalent to one fault tolerant design.

II. The electrical controls that operate the above valves, etc., related to the fault tolerant design should be designed to open by three independent signals.
III. If the control measures to prevent leakage differ for different phases of the launch site operation, two fault tolerant design for each phase should be shown.

b. Two fault tolerant design with three seals, or design for minimum risk with metal seals are applied against leakage of toxic materials from pouring and draining valves, etc.

(3) Filling operation of toxic materials is performed in accordance with JERG-1-007 at the launch site.
(4) Fluid compatible materials are used for tanks, pipes, etc. filling toxic materials (including pressurized gas pipes that may be contaminated by propellants).
(5) Cleanliness-controlled fluids are used to prevent foreign matter from being entrapped in valves.
(6) In the case of lifting operations (including payload lifting operations after propellant filling) for tanks loaded with toxic materials, the design should have appropriate margins for lifting equipment and lifting points of payload. The "industrial Safety and Health Law, Safety Ordinance for Cranes" requires a minimum safety factor of 6 for wire rope and 5 for other types.
(7) The design as a pressure system satisfies section 5.2.

5.5 Prevention of inadvertent RF radiation hazard at the launch site (explanation provided in Attachment-2)

At the launch site, RF radiation hazard more than a predetermined intensity can result in injury to personnel. The severity of this hazard is determined by the following:

Step 1 (Determination of a marginal/negligible hazard)

If any of the following A) through C) are satisfied, the hazard is considered to be a marginal/ negligible hazard.

A) Frequencies of electromagnetic radiation source is below 6 GHz, and antenna power of electromagnetic radiation source is at or below 20 W. (Assuming that no person other than the PL organization personnel approach within 10cm of the electromagnetic radiation source.)
B) Calculation result of the safe distance (electromagnetic field range with the intensity below the guideline value) in accordance with the "Guidelines for safe distance calculation"(1) meets the following a or b. (Safe distance may be calculated taking duty cycle into account for pulse beam. Use appropriate reflection coefficient considering inadvertent radiation.)
   a. No person other than the PL organization personnel is physically able to access the area within the safe distance according to the launch site operations scenario or configuration of equipment, and etc.
   b. The safe distance is within 1.4 m and the access of person other than the PL organization personnel is limited to incidental.
C) Calculation result of the safe distance in accordance with the "Guidelines for safe distance calculation" (2), (3), and (4) in this order shows that no person is physically able to access within the safe distance.

"Guidelines for safety distance calculation"

(1) "The Radio Radiation Protection Guidelines for Human Exposure to Electromagnetic Fields" (hereinafter referred to as RRPG) Table 2: Electromagnetic Field Strength Guidelines for General Environment (Condition G) (Average Time: six Minutes)
(2) RRPG, Table 1: Electromagnetic Field Strength for Controlled Environment (Condition P) (Average Time: six Minutes)
(3) RRPG, Supplementary Guidelines II, (1) Guidelines for Cases of Non-uniform or Partial-body Exposure
- Use these guidelines when human body is exposed to electromagnetic field non-uniformly or partially.
(4) RRPG, Table 5: Basic Guidelines

Step 2 (Determination of a critical/catastrophic hazard)

Hazards not identified as marginal/negligible hazards are catastrophic hazards if the human body is exposed to an average of 200 W or more over a six minutes period, and critical hazards if less than 200W.

In addition, appropriate hazard controls should be implemented to prevent hazards. The following are typical measures:

(1) As hazard analysis, RF radiation sources that require hazard control in the payload/GSE are identified.
(2) The required number of fault tolerant design should be implemented against inadvertent radiation of RF

in each phase at the launch site.

(3) In the case of intentional RF radiation at the launch site, operational restrictions such as keep out zone to the safety distance is set.

5.6 Prevention of inadvertent actuation of pyrotechnic devices hazard at the launch site

At the launch site, for the pyrotechnic devices used in the retention and release mechanisms of solar array paddles, etc., inadvertent actuation is generally not considered a catastrophic or critical hazard. (While onboard a launch vehicle, follow the instructions of the launch vehicle separately).

If an inadvertent actuation of pyrotechnic devices results in death or injury of person or damage to the launch site facility and equipment and is considered a catastrophic or critical hazard, appropriate hazard controls should be implemented to prevent this hazard. The following are typical measures:

(1) As hazard analysis, pyrotechnic devices that require hazard control in the payload/GSE are identified.

(2) The required number of fault tolerant design should be implemented against inadvertent actuation of pyrotechnic devices in each phase at the launch site.
   a. For a catastrophic hazard, the design should have a minimum of three independent inhibits to the energy source. At least two of the three inhibits should be designed to be monitored.
   b. For a critical hazard, the design should have a minimum of two independent inhibits to the energy source.

(3) An electro-explosive device (EED), should be confirmed that it does not cause fire or malfunctions when 1 A DC and 1W DC are applied for five minutes without an external shunt. “No-fire” means that the ignition level is 0.1 % at 95 % of the confidence level determined by Bruceton test or equivalent statistic test methods.

(4) For the EED, shields should be provided equal to or greater than 20 dB attenuation against the maximum no fire power of pyrotechnics, for all expected RF frequency spectrums that come from the 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.

(5) When EED is used, pyrotechnics firing circuits are checked for stray voltage prior to electrically connecting. The result of checking should not exceed 1/10 of the maximum no-fire current or 50 mA, whichever is lower.

In addition, solid rocket motors and pyrotechnic devices used in solid rocket motors are particularly high-risk items, and the following measures are generally taken.

(6) For pyrotechnic devices used for ignition of solid rocket motors, the measures described in section 5.6 (2) through (5) are taken. For (2), one of the three independent inhibits shall be a safe and arm device with electrical and mechanical safety mechanisms. In the case where a device other than an EED such as laser ignition detonator is used for ignition of a solid rocket motor, the necessity of a safe and arm device is individually considered.

(7) The solid rocket motor is designed to be physically and chemically resistant in the handling environment (friction, vibration, shock, human static electricity, EMC, temperature, humidity, etc.)

(8) The solid rocket motor is secured against static electricity by bonding and grounding.

5.7 Treatment of hazards related to the safety of personnel in the PL organization

At the launch site, the following hazards are generally considered to be hazards to the safety of personnel of the PL organization. These hazards are not required to establish hazard controls because the severity of the hazards to person other than personnel of the PL organization, and the launch site facility and equipment is generally considered to be marginal or negligible hazards. But the PL organization should take responsibility for their own personnel safety.

(1) Electric shock

(2) Fall while operation at height

(3) Falling of heavy objects during transportation of heavy objects

(4) Lack of oxygen

(5) Noise injury
(6) Injury from hot or cold surfaces
(7) JIS C 6802 (IEC 60825-1) class 4 or less injury due to use of lasers (except as an ignition source in explosive hazardous atmospheres)
(8) Injury from sharp edges, corners, and protrusions
(9) Injury caused by unintended movement of mechanisms (solar array paddles, antennas, etc.)

6. Inherent safety design requirements irrelevant to hazard analysis (explanation provided in Attachment-2)

This chapter is inherent safety design requirements irrelevant to hazard analysis in chapter 4 and the results of compliance assessment shall be submitted separately.

(1) The payload/GSE shall be designed so that the pressure system can be safely depressurized and the propellants (hydrazine, MMH, etc.), oxidizers (MON3, NTO, etc.) can be safely discharged in case of anomalies such as in case of leakage of propellants, oxidizers, etc. from the payload.

Attachment 1 Design Standards to implement Design for Minimum Risk

“Design for minimum risk" is applicable in the following items, if the design conforms to the design standards specified by JAXA in each item and verification data are provided. The latest version of the documents shall be applied.

(1) Structure
- JERG-2-320 Structural Design Standards
- Users’ manual of each launch vehicle

(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 Act

(3) Pyrotechnic devices
- JMR-002 Launch Vehicle Payload Safety Standard Section 5.6 Prevention of inadvertent actuation of pyrotechnic devices hazard at the launch site

(4) Some mechanisms
- CZA-2018029 Launch Vehicle Payload System Safety Program Plan/Safety Data Package Template

(5) Explosive hazardous atmosphere
- JMR-002 Launch Vehicle Payload Safety Standard Section 5.1 Prevention of fire and explosion hazard at the launch site, “Detail explanation”
- National regulation “Constructional Requirements for Electrical Equipment for Explosive Atmospheres”
- IEC 60079 Series
- JERG-1-007 Safety Regulation for Launch Site Operation

(6) Electrical system
- JERG-2-213 Insulation Design Standards
- JMR-002 Launch Vehicle Payload Safety Standard Section 5.3 Prevention of lithium-ion battery rupture hazard at the launch site

(7) Other adequate Standards whose implementation can reduce the risk as low as acceptable.

Attachment 2 Detail explanation of each section

4.3.1.5.1 Fault tolerant design requirements, explanation part 1

1. Purpose

This section clarifies its interpretation of control system independence with respect to 4.3.1.5.1 Fault tolerant design requirements.

Note that this section does not preclude other means to ensure safety.

<Background>

When multiple inhibits are controlled by a computer-based control system (hereinafter referred to as a "CBCS"), they are not necessarily independent inhibits. However, there are currently many cases where multiple inhibits are controlled by a CBCS, and this was frequently discussed in the JAXA System Safety Review Panel. In such cases, if the design of the CBCS is evaluated and it is confirmed that there is a certain degree of independence in the control of each inhibit, the CBCS is considered to be effectively equivalent to an independent inhibit and is evaluated as equivalent to a fault tolerant design. It was necessary to clarify these individual evaluations.

<Definition>

A CBCS is a control system that uses computer hardware, software, and firmware to receive input information, process that information, and provide output in order to perform a defined task.

Here, control by a CBCS is defined as consisting of (1) an inhibit release command, (2) a command issuing device, (3) a command relay device, and (4) a command execution device (see Figure 1), where each device is assumed to be equipped with a computer and software.

2. Scope of application

This section is applied to the control system of electrical inhibits that prevent malfunctions of hazardous equipment in launch vehicle payloads (e.g., malfunctions of deployed objects such as solar array paddles and antennas, inadvertent RF radiation, leakage of toxic substances).

(This does not apply to the independence of control systems related to unintended shutdown of equipment that must continue to operate for hazard control. If applicable systems exist, they should be coordinated with the JAXA Safety and Mission Assurance Department.)

3. Interpretation

A CBCS that controls multiple inhibits can be evaluated to guarantee a certain degree of independence if it satisfies the following points.

Figure 1 Definition of Terms

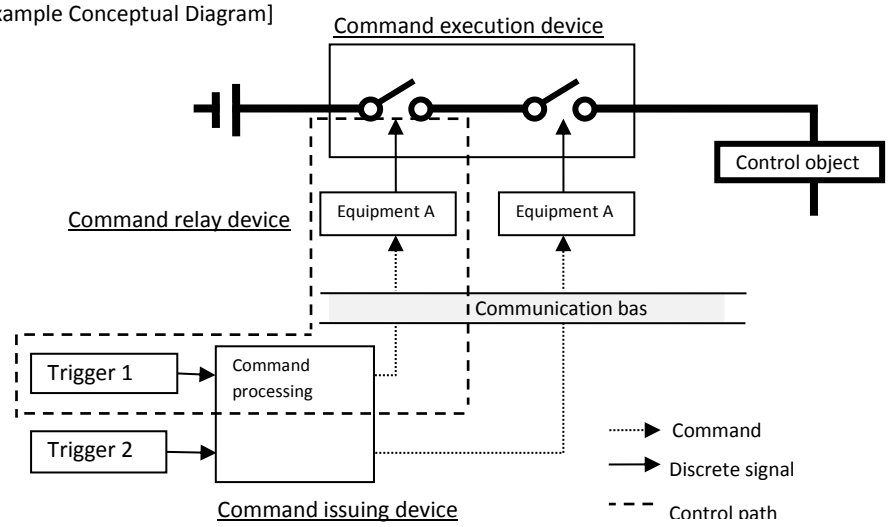
The definitions of "command issuing device," "command relay device," and "command execution device" used in this document are as follows. A conceptual diagram of a typical CBCS design is also shown below.

Command issuing device: A device that processes signals received by a certain trigger and sends commands or signals to release inhibits to the command execution device.

Command relay device: A device that relays and processes commands or signals received from the command issuing device and sends the command or signal to the command execution device.

Command execution device: A device that processes and executes commands or signals received from the command issuing device or command relay device.

[CBCS Design Example Conceptual Diagram]



3.1 Independence design guidelines for each component

(1) Inhibit release command

(a) Uniqueness of identification of inhibit release command

In an environment where commands are represented by bit patterns, each inhibit release command has its own unique bit pattern to prevent unintended inhibits from being released due to errors in command sending and receiving other than inhibit release commands.

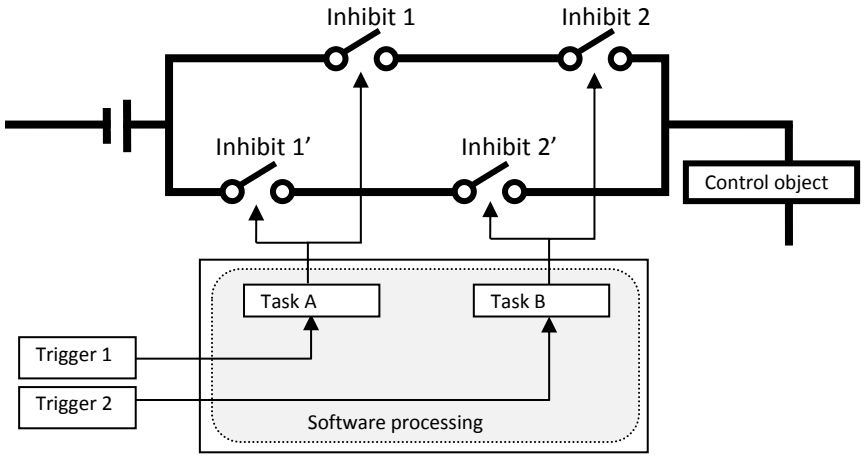
(b) Uniqueness of correspondence between inhibit release command and inhibit

A single inhibit release command releases one specific inhibit. (However, if the circuit to be controlled has a redundant system from the standpoint of reliability, etc., one command may be used to cancel one inhibit for each system.)

The concept of this is illustrated in Figure 2.

Figure 2 Example of uniqueness of correspondence between inhibit release command and inhibit in Section 3.1(1)(b)

An example of the uniqueness of the correspondence between inhibit release commands and inhibits is shown below. The command issuing device releases inhibit 1,1' by trigger 1, and releases inhibit 2,2' by trigger 2. Here, different commands must be used to cancel inhibit 1 and inhibit 2 (the same applies to inhibit 1' and inhibit 2'). However, since inhibit 1 and inhibit 1' are redundant in terms of reliability, the commands to cancel inhibit 1 and inhibit 1' can be common (the same applies to inhibit 2 and inhibit 2').



(c) Communication independence of inhibit release command

When sending inhibit release commands, each communication command is sent at a different timing using a separate communication frame.

(2) Command issuing device for inhibit release

(a) Considerations for inhibit release commands

Design any of the following (a-1) through (a-3), or a combination of several of them.

(a-1) Software design with isolated command issue control paths

Software that issues multiple inhibit release commands for the same hazard has a separate control path for each command. A separated control path is a control path (logical flow (see Figure 1)) that gives functional independence to each command and does not affect other command issuing processes in the event of any failure or operational error as well as during normal operation. In addition, refer to Section 3.2 to guarantee the independence of the command issuing process. The concept of this is shown in Figure 3.

(a-2) Software design to prevent command issuance under independent conditions

If (a-1) above cannot be satisfied (e.g., multiple inhibit release commands for the same hazard are issued by a common process based on time series (timeline processing, etc.) and cannot be judged to be separate control paths), to prevent unintended processing from starting and subsequent command issuance, the design requires conditions independent of this processing (e.g., determination of satellite separation, rate dumping completion or sun acquisition). The number of these conditions shall be sufficient to achieve fault tolerance. In order to ensure that the command issuance is not executed with a single fault, the independence indicated in section 3.2 shall be guaranteed for this condition processing. The concept of this is shown in Figure 3.

Figure 3 Independence of control systems using computers

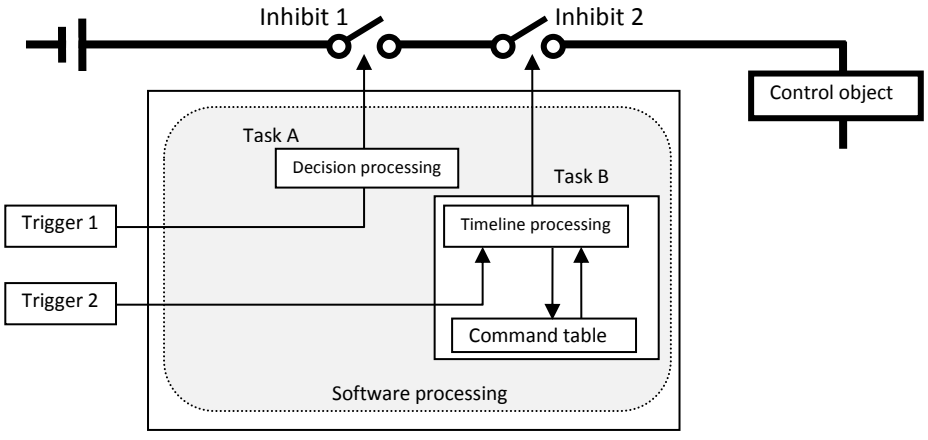
The following is an example of a power and control subsystem that prevents unintended operation of hazardous equipment due to electrical failure for a critical hazard (1FT is required). Note that triggers 1 and 2 are established by independent Hardware. An example of the application of the contents explained in Section 3.1(2) (a-1), (a-2) is shown as a conceptual diagram. In each section, the design "no two inhibits are simultaneously released by any one failure" in the inhibit control system is implemented. Similarly, in the case of a catastrophic hazard, a design in which "no three inhibits are simultaneously released by any two failures" shall be implemented. For reference, examples of noncompliance are shown below each compliance example.

Example of compliance to Section 3.1(2)(a-1)

Although two inhibits are controlled by a single software process, the tasks that perform these controls are independent (Tasks A and B are evaluated to be independent of each other according to Section 3.2) and the control paths are separated. The respective inhibit release processing operations are shown below.

Task A: Sends an inhibit 1 release command by the decision process in software according to the trigger 1 condition.

Task B: Starts timeline processing according to the trigger 2 conditions, calls a stored command from the command table, and sends an inhibit 2 release command.

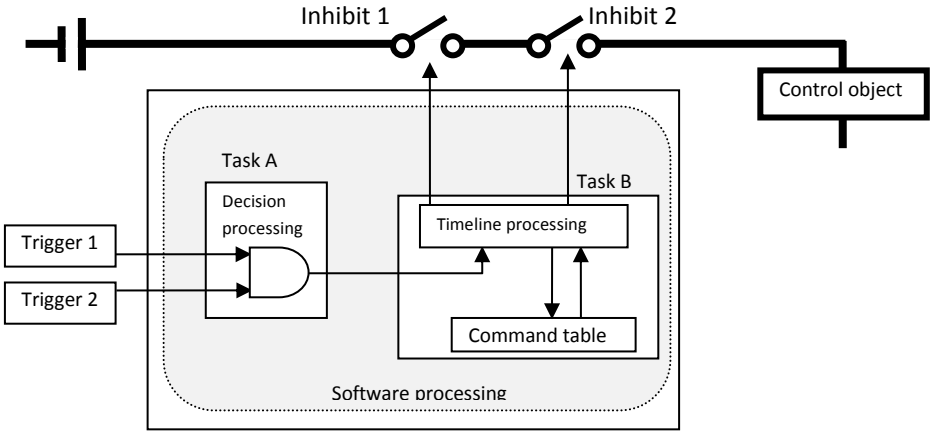


Example of **noncompliance** with section 3.1(2)(a-1)

Two inhibits are controlled by a single software process, and tasks A and B, which control these inhibits, are not independent and do not have separate control paths. Therefore, a single point of failure exists (one failure of task A or B may cause inhibits 1 and 2 to be released). The inhibit release process operation is shown below.

Task A: Outputs a decision signal to Task B by the logical product of triggers 1 and 2.

Task B: Starts timeline processing based on the signal from Task A, calls the stored command from the command table, and sends the inhibit 1 and inhibit 2 release commands.

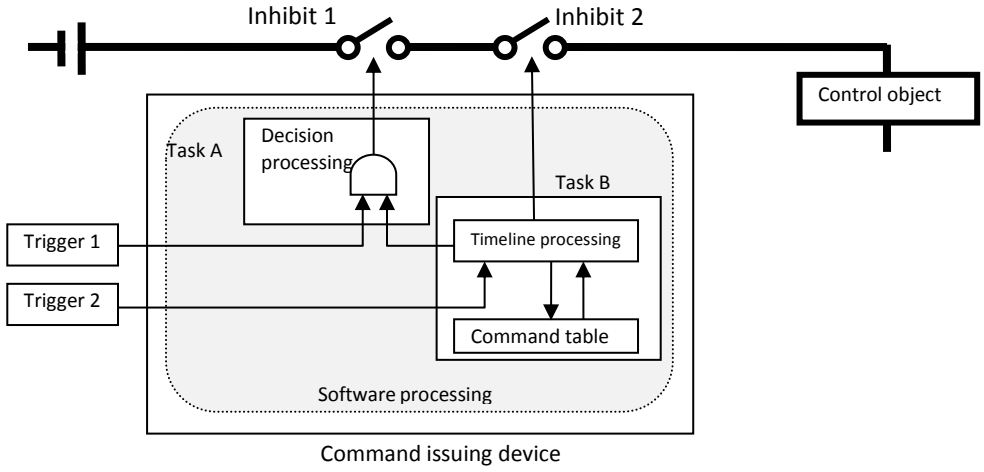


Example of compliance to Section 3.1(2)(a-2)

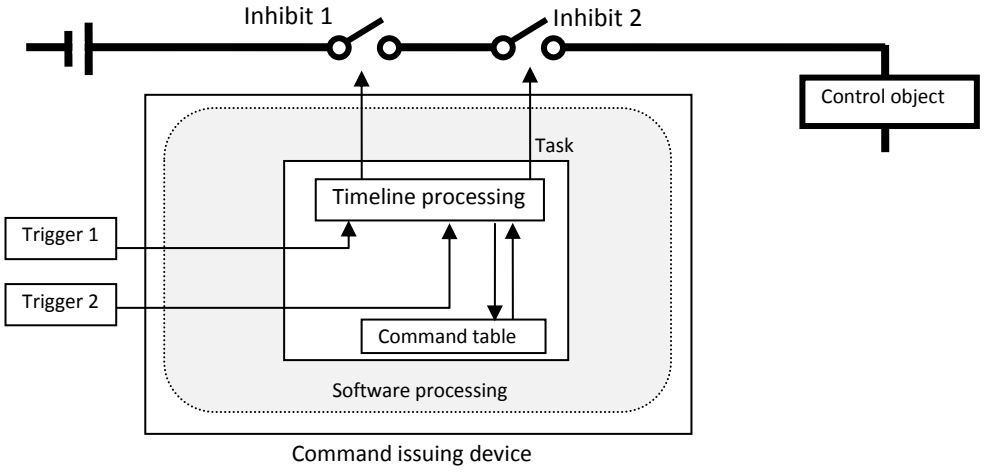
Since the command to release inhibit is issued in the same timeline process of Task B, the control paths are not independent of each other, but the inhibit 1 release process is a logical product of the trigger 1 decision and the timeline process, and the command issuance is prevented by conditions independent of the timeline process that issues the command. (For example, even if timeline processing is executed due to the failure of trigger 2, the issuance of the inhibit 1 release command is prevented by trigger 1.) This decision process of Task A is evaluated for independence according to Section 3.2.

Task A: Receives the inhibit 1 release command from the timeline processing of Task B and sends the command according to the trigger 1 condition (trigger 1 prevents the sending of the inhibit 1 release command).

Task B: Starts timeline processing according to the trigger 2 condition, calls the stored command from the command table, and sends the inhibit 1 and inhibit 2 release commands.



Example of **noncompliance** with section 3.1(2)(a-2)
The software process to release inhibits ((1) and (2) below) is performed in a common task (timeline processing), and since there is no independent condition to prevent timeline processing, the design has a single point of failure (one failure in the task could release inhibits 1 and 2).
(1) Trigger 1 condition starts timeline processing, calls a stored command from the command table, and sends an inhibit 1 release command.
(2) Starts timeline processing according to the trigger 2 condition, calls a stored command from the command table, and sends an inhibit 2 cancel command.



(a-3) Software design that does not register inhibit release commands
A design in which a certain inhibit release command is not registered in the equipment of the launch vehicle payload (e.g., inhibits release is achieved only by sending commands from the ground). In this case, any failure will not generate such a command (there is no stored command and no inhibit release command will be issued due to a failure).

(b) Consideration for the order and timing of inhibit release
If the order or timing of inhibit release may cause a hazard, do not issue inhibit release commands in the order or timing that causes the hazard.

(3) Command relay device for inhibit release
(a) Prohibition of command expansion
Device that relays multiple inhibit release commands of the same hazard sends only the received commands downstream and does not expand them into multiple inhibit release commands.

(b) Consideration for the order and timing of inhibit release

If the order or timing of inhibit release may cause a hazard, inhibit release commands received in the order or timing that causes a hazard are rejected and not sent downstream.

(4) Command execution device for inhibit release

(a) Prohibition of command expansion

A device that executes multiple inhibit release commands for the same hazard will only release the inhibit that corresponds to the received command and will not release multiple inhibits.

(b) Consideration for the order and timing of inhibit release

If the order or timing of inhibit release may cause a hazard, inhibit release commands received in the order or timing that causes a hazard are rejected and the corresponding inhibit is not released.

3.2 Software design to ensure command issuance independence

Software that issues multiple inhibit release commands for the same hazard shall have an independent process for issuing each command.

Here, an independent software process is one that does not affect other command issuing processes, not only during normal operation, but also in the event of any failure or operational error. In particular, when assuming a failure of the CBCS, it is necessary to determine through evaluation of the specific software design that "there is no failure mode that could accidentally issue other inhibit release commands, or a design where this mode is acceptable."

Specifically, if any of the following applies, it is judged that a certain degree of independence of command issuance is guaranteed by the software design, but the final judgment as to whether the system has required number of fault tolerance shall be made from a comprehensive perspective in conjunction with Section 3.1.

(1) Task-level independence

When multiple inhibits are controlled by different tasks (*) and their respective inhibit release conditions are not identical. Note that additional evaluation against common faults is required in the following cases

(*) A task here refers to a running program with unique computer resources. The term "task" used here is a general one, so if different terms are used depending on the processing system used by the target to be evaluated, these should be read accordingly.

(a) Evaluation of inter-process communication

When inter-process communication (shared memory, sockets, various synchronizations, etc.) is performed between tasks that perform inhibit control, these multiple inhibits should not be released

as an effect of the failure mode involving the inter-process communication process.

(b) Evaluation of common designs

If multiple tasks with inhibit control utilize a common function or code, it should be indicated that multiple inhibits will not be released as an effect of the failure mode involving these functions or codes.

(2) Function-level independence

When task-level independence of (1) cannot be achieved (multiple inhibits are controlled by a single task), but they are processed by different functions and their respective inhibit release conditions are not identical. Note that additional evaluation for common faults is required in the following cases.

(a) Evaluation of shared variables between functions

If there is a variable shared by multiple functions (a global variable), it should be indicated that multiple inhibits will not be released as an effect of the failure mode related to that variable.

(b) Evaluation of common designs

If multiple functions that perform inhibit control utilize a common library function or code, it should be indicated that multiple inhibits will not be released as an effect of the failure mode involving these library functions or codes.

Appendix: Examples for implementation of fault tolerance design by hardware

In this appendix, guidelines are presented for implementing a fault tolerant design as a system when multiple inhibits are controlled by the CBCS, instead of using a software design. Figure A-1 shows the concept of this design. Figure A-1 also shows an example of a system that does not comply with this design and does not satisfy 1FT design as a reference.

Figure A-1 Design to prevent issue/execution of commands by hardware

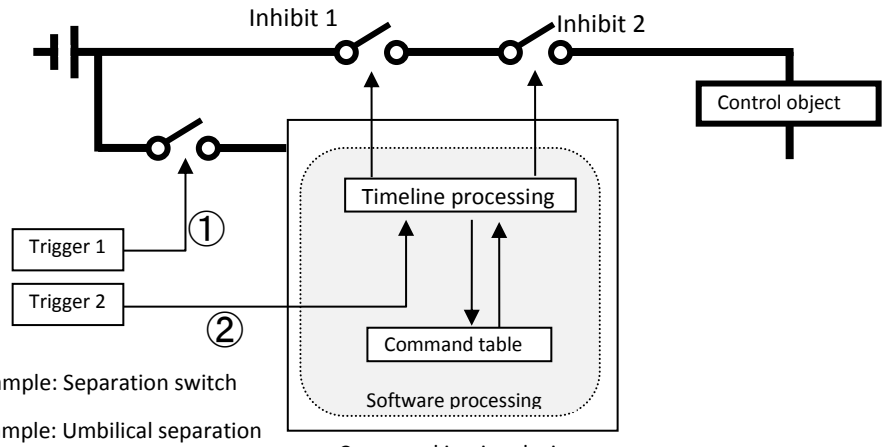
(a) Example of prevention of inhibit release by hardware

The software process within the command issuing device that releases inhibit 1 and 2 is common, but command issuance is prevented by hardware, and the system satisfies 1FT. Inhibits 1 and 2 are released only when two hardware failures occur: (i) unintended power-on of the command issuing device and (ii) malfunction of the command issuing device. (Triggers 1 and 2 are implemented by independent hardware)

①Power on of command issuing device by trigger 1 condition

②The trigger 2 condition initiates timeline processing, calls the stored command from the command table, and releases inhibits 1 and 2.

Note: An inhibit is a disconnecting device installed between the control object and the energy source, so a relay that disconnects power to command issuing device is not an inhibit to the control object.



Trigger 1 Example: Separation switch

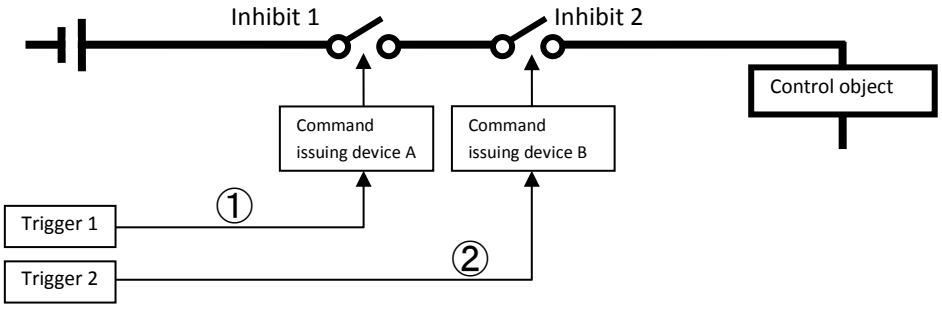
Trigger 2 Example: Umbilical separation signal

(b) Example of a design with independent hardware

The devices that process inhibit release commands and downstream devices are independent for each inhibit and satisfy the 1FT.

①Trigger 1 condition causes command issuing device A to send an inhibit 1 release command

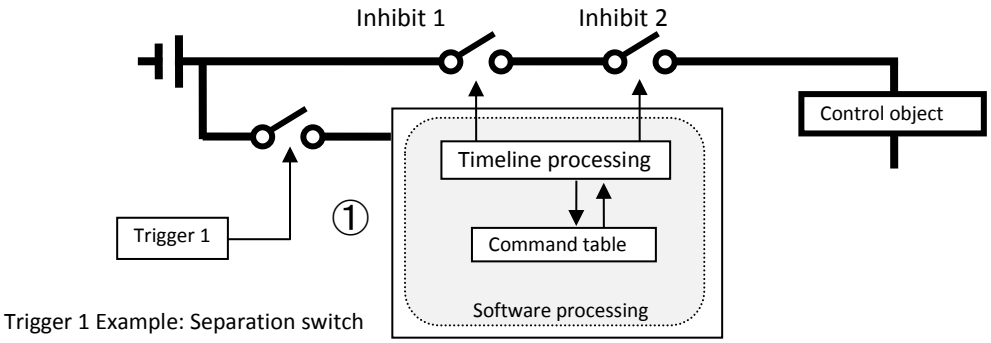
②Trigger 2 condition causes command issuing device B to send an inhibit 2 release command



Example of 1FT Design Failures

The software process within the command issuing device to release inhibit 1 and 2 is common, and since inhibit 1 and 2 are released by one failure of trigger 1, 1FT is not established.

①Power on of the command issuing device by the trigger 1 condition starts the timeline processing, calls the stored command from the command table, and releases inhibits 1 and 2.

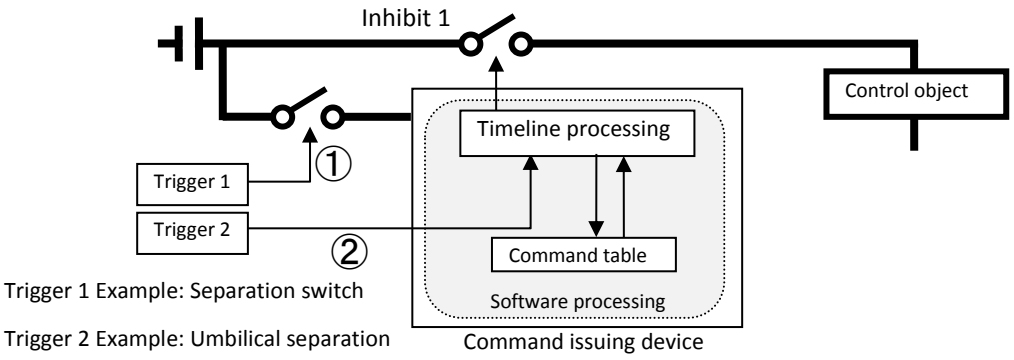


Example of 1FT Design Failures

The inhibit control line satisfies the 1FT according to the concept in (a), but does not satisfy the 1FT because there is only one inhibit installed between the control object and the energy source (a relay that interrupts the power supply of a command issuing device does not count as an inhibit). Therefore, the design below has an insufficient number of inhibits because, for example, a single fault, a short circuit in inhibit 1, could cause the control object to operate.

①Power on of command issuing device by trigger 1 condition

②The trigger 2 condition initiates the timeline processing, calls the stored command from the command table, and releases inhibit 1.



(a) Designed to prevent issue/execution of commands by hardware

A design that provides a condition by hardware that prevents the issuing/execution of the command in the device that processes the inhibit release command or in downstream devices. The conditions shall be independent of the computer issuing the inhibit release command and its software

processing. The number of conditions shall be sufficient to achieve fault tolerance.

(b) Hardware independent design

A design in which the devices that process inhibit release commands and downstream devices are independent for each inhibit.

4.3.1.5.1 Fault tolerant design requirements, explanation part 2

1. Purpose

This section clarifies the timing to check the soundness of a fault tolerant design consisting of inhibits.
Note that this section refers to electrical inhibits, and mechanical inhibits are outside the scope.
Note that this section does not preclude other means to ensure safety.

<Background>

- Since small satellites are “cold-launch”, it is impossible to monitor inhibits during launch. Therefore, the soundness of the inhibit confirmation is ensured by checking the inhibit prior to launch. On the other hand, some “hot-launch” satellites can monitor the inhibit constantly during launch. Thus, the monitoring method varies according to the condition of each satellite, and it was then necessary to ascertain whether real-time monitoring during launch is necessary and also to establish the monitoring method.
- When the FET is used as the inhibit, the monitoring circuit for direct confirmation of the status of the inhibit will be complicated (which may degrade the mission reliability). In some missions, verification of the feedback in the driving line of the FET SW is regarded as monitoring of the inhibit (particularly because it is difficult to monitor inhibits on the return side using the FET). It was then necessary to discuss whether such an indirect confirmation method is acceptable as monitoring.

2. Interpretation

The following are examples of how to verify the soundness of inhibits according to configuration and other conditions. Note that real-time monitoring during launch is required for inhibits when an emergency response is needed in the event of an anomaly.

[Prerequisites]

All of the conditions listed below are applicable to "the period when mitigation of a hazard by using the inhibits is required" (in other words, checking of the state of the inhibits during "the period when mitigation of a hazard by using the inhibits is not required" is not necessary, since safety is ensured regardless of the state of the inhibits during such a period).
In principle, required number of inhibits must be functioning during "the period when mitigation of a hazard by using the inhibits is required."

(Configuration 1)

If all inhibits and control circuits validated on the ground are maintained throughout the launch, real-time monitoring of inhibits need not be performed.

In this condition, the configuration of devices that contribute to hazard mitigation is not changed during the period in which hazards are controlled by the inhibits, and the possibility of occurrence of hazards owing to failures of all inhibits is very low. A real-time measure for an emergency response is not required and real-time monitoring during launch is not necessary to be performed. It is sufficient to monitor inhibits at an appropriate time (such as when performing the final setting of the configuration of the inhibits).

In addition, monitoring of inhibits after verification is not required when a failure or a change in the status of the inhibits or their control circuits is not expected after the inhibits have been verified on the ground. In this case, indirect confirmation of the status of the inhibits is acceptable if it is considered to be equivalent to direct confirmation.

This case is applicable to many satellites, as inhibits are not disabled during the flight of a launch vehicle.
For instance, in the case of confirmation of the status of the inhibits through checkout for avionics at the launch site, monitoring of the inhibits need not be performed after the status confirmation (under the assumption that the environmental resistance of the inhibits is verified in advance through tests such as the vibration test). In this case, it is acceptable to confirm the soundness of the inhibits through an indirect method such as verification of conduction to a hazardous function with two inhibits removed.

(Configuration 2)
Inhibit monitoring is not required if the following two conditions are met (checking the status at the launch site is also not required)

I. When a potential energization failure mode is excluded (for example, when there is another inhibit in addition to the required inhibit)
II. When the control circuit of an inhibit is disabled (i.e., the power supply to the control circuit is interrupted so that a failure of the circuit will not result in removal of the inhibit)

Another inhibit in addition to the required inhibit can increase reliability and reduce the likelihood of a hazardous function being activated. In addition, with the control circuit disabled, a hazardous function is not activated unless the inhibits themselves fail at the same time. Accordingly, monitoring of the inhibits is not required (the act of monitoring itself is not necessary). (Source: AFSPCMAN 91-710 vol.3, 12.8.3.5, and NSTS 1700.7B 202.1c (3))

(Configuration 3)

If the configuration of equipment that contributes to hazard mitigation is changed during launch (as indicated in the prerequisites, in principle, the required number of inhibits shall not be released), real-time and direct monitoring of inhibits is required.

Providing a means for real-time monitoring of inhibits is required in order to confirm (monitor) that control over a hazardous function is effective in real-time before changing the configuration of the devices that contribute to hazard mitigation. In this case, it is also required that the areas monitored are directly able to check the state of the inhibits in order to correctly recognize the state of the inhibits within a limited period of time (Examples of such parts include the monitored contact point of the mechanical relay and the position sensor of the valve; indirect monitoring, including the feedback from the driving line of the inhibits, is not acceptable).

Real-time monitoring is not required for many satellites, since the configuration of the devices that contribute to hazard mitigation is usually not changed before the separation of the satellite from a launch vehicle. Whether real-time monitoring is required should be determined using the cases below as a reference.

<Case of the requirement of the United States Air Force> Source: AFSPCMAN91-710 vol. 3

The state of the inhibits for a solid rocket motor, command destruct system, and liquid propellant is required to be monitored directly in real-time as the state changes upon the launch of a launch vehicle.

<Case 1 of the space shuttle program> Source: NSTS 1700.7B 202.1

In a mission in which a satellite with a solid rocket motor is separated from the Orbiter, real-time monitoring of two of the three electrical inhibits for the solid rocket motor is required if the safe and arm device (SAD) is removed before the satellite reaches a safe distance.

(2FT design is established in the three electrical inhibits as hazard controls other than the SAD, as the SAD is removed in this situation. In this regard, however, the removal of SAD results in the removal of the physical barrier in the ignition circuit to the rocket motor, which is considered to be a change in the configuration of the important safe device (see Figure 1).)

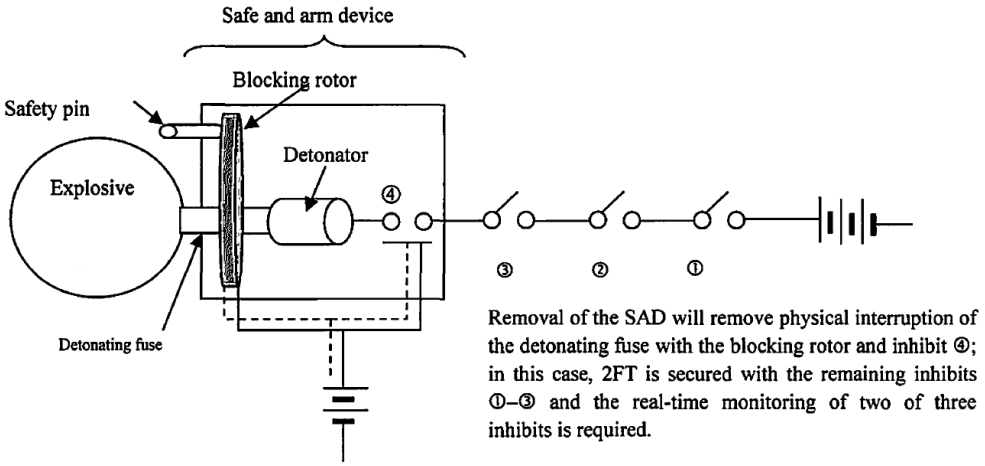


Figure 1 Example of safe and arm device of payload on a space shuttle

<Case 2 of the space shuttle program> Source: NSTS1700.7B 202.2

In a mission in which a satellite with liquid propellant is separated from the Orbiter, real-time monitoring of two of the three electrical inhibits for the remaining two flow control valves (shutoff function) is required when opening the isolation valve to activate a small thruster for attitude control prior to the satellite reaching a safe distance when it is separated from the Orbiter. (i.e., the distance at which the jet of a large thruster would not cause any problem) (see Figure 2).

(Jetting of a large thruster prior to the separation of the satellite from the Orbiter before the satellite reaches a safe distance is deemed to be a catastrophic hazard, so the propulsion system is required to have at least three mechanical devices (such as an isolation valve) to prevent the propellant flow. In addition, at least three electrical inhibits are required for an electrical failure.

The isolation valve is opened for activating of the small thruster for attitude control at a distance (which is normally 50-100 m) at which the shuttle is not affected by a jet of the small thruster or a small amount of leakage of the propellant. In other words, as 2FT design is required against inadvertent firing of a large thruster, it has to be controlled by three electrical inhibits. For internal leakage from the sealing, it is considered that a large amount of leakage of the propellant is prevented by the two flow adjustment valves other than the isolation valve; thus, opening of the isolation valve prior to the satellite reaching a safe distance is acceptable.)

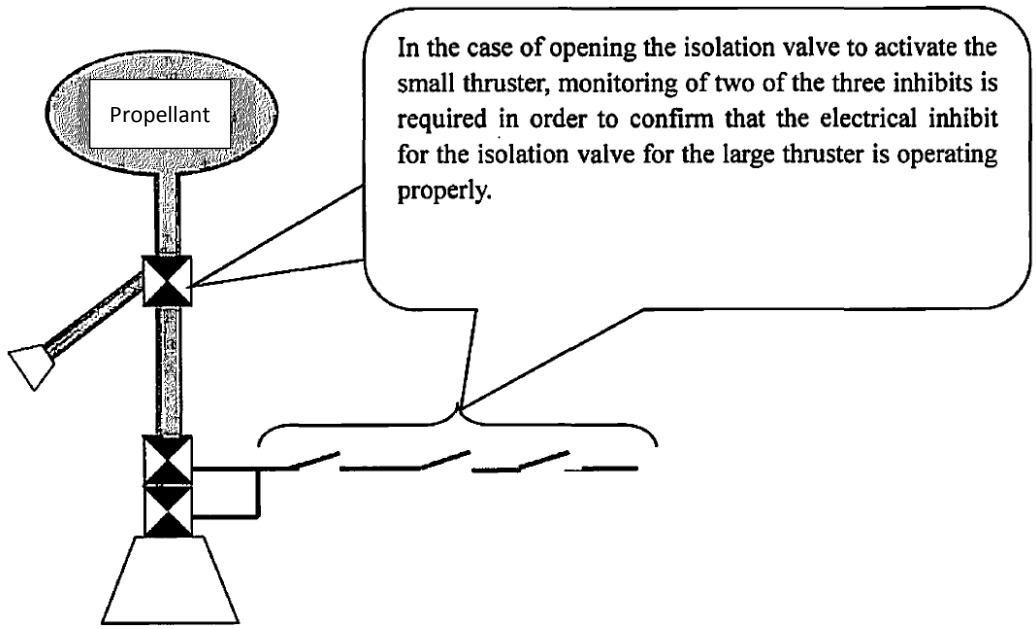
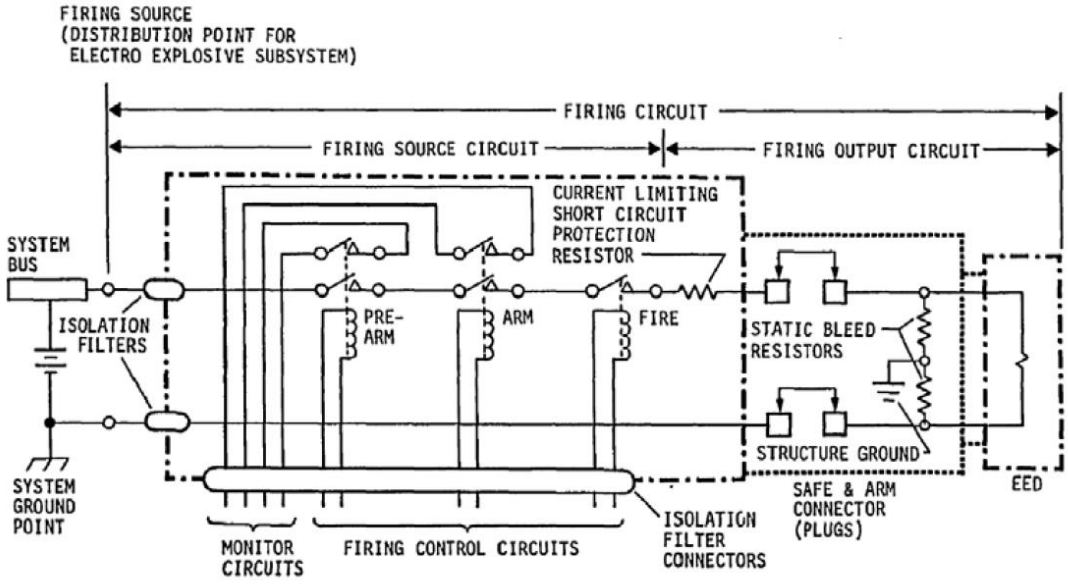


Figure 2 Example of inhibits for propulsion system of payload on a space shuttle

Examples of a method for "checking the state of the inhibits directly" are listed below:

(a) Method using a relay (Source: MIL-STD-1576)

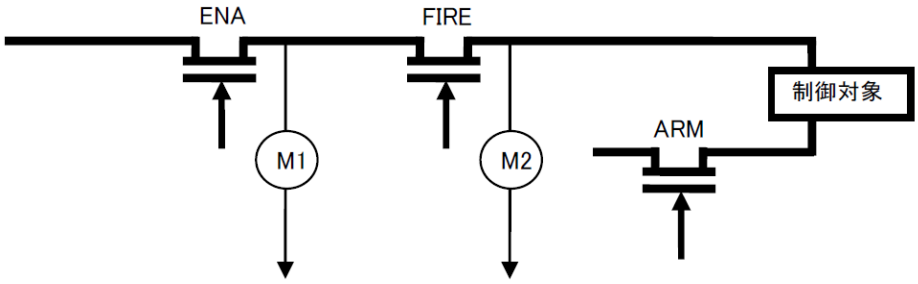
The mechanical contact point of the relay is monitored. Although the conduction of the inhibits is not monitored, it is accepted as a" direction confirmation" method with a failure mode of relay.



(b) Method using a semiconductor SW

The constant monitor M1 is monitored. After ENA is closed and it is confirmed with M2 that FIRE is

effective as an inhibit, ARM is closed Then, FIRE is closed



3. Rationale

In JMR-002, the requirement for the monitoring of inhibits is specified on the basis of the safety requirements established by the United States Air Force and NASA's manned system, and this interpretation is based on these requirements. (See below)

AFSPCMAN 91-710 vol.3

5.3. WR OSC Controls, Monitors, and Communication Lines:

5.3.2. At a minimum, the controls, monitors, and communication needs listed below are required at the launch complex OSC. These items are general in nature and may vary depending on the launch vehicle configuration. The monitor circuit shall be designed so that the actual status of the critical parameters can be monitored rather than the command transmittal. It is important that this console not have any FTS command transmittal functions.

5.3.2.1. FTS safe and arm status for all FTS safe and arm devices.

5.3.2.2. Ignition safe and arm status for all solid rocket motor safe and arm devices.

5.3.2.3. Launch vehicle liquid propulsion system inhibits and propellant tank pressure status (psig).

12.8.3. Flight Hardware Hypergolic Propellant System Valves:

12.8.3.5. Remotely controlled valves shall provide for remote monitoring of open and closed positions during prelaunch operations. Monitoring of remotely controlled, pyrotechnically operated valve open and closed positions shall not be required if the function power is deenergized (in other words, an additional fourth inhibit is in place between the power source and the three required inhibits) and the control circuits for the three required inhibits are disabled (in other words, no single failure in the control circuitry will result in the removal of an inhibit) until the hazard potential no longer exists).

13.3.6. Ordnance Electrical and Optical Monitoring, Checkout, and Control Circuits:

13.3.6.1. All circuits used to arm or disarm the firing circuit shall contain means to provide remote electrical indication of their armed or safe status.

13.3.6.1.1. These inhibits shall be directly monitored.

13.3.6.1.2. GSE shall be provided to electrically monitor arm and safe status of the firing circuit at all processing facilities including launch complexes up to launch.

NSTS 1700.7B

201.1c Monitors. Monitors are used to ascertain the safe status of payload functions, devices, inhibits and parameters. Monitoring circuits should be designed such that the information obtained is as directly related to the status of the monitored device as possible. Monitor circuits shall be current limited or otherwise designed to prevent operation of the hazardous functions with credible failures. In addition, loss of input or failure of the monitor should cause a change in state of the indicator. Monitoring shall be available to the launch site when necessary to assure safe ground operations. Notification of changes in the status of safety monitoring shall be given to the flight crew in either near-real-time or real-time.

201.1c(1) Near-Real-Time Monitoring. Near-real-time monitoring (NRTM) is defined as notification of changes in inhibit or safety status on a periodic basis (nominally once per orbit). NRTM may be accomplished via ground crew monitored telemetry data. Switch talk backs shall not be used as the only source of safety monitoring when the hazard exists during crew sleep periods.

201.1c(2) Real-Time Monitoring. Real-time monitoring (RTM) is defined as immediate notification to the crew. RTM shall be accomplished via the use of the Orbiter failure detection and annunciation system or by ground crew monitored telemetry data. An exception to this would be where RTM is necessary only during payload operations. Under these conditions, switch panel talk back monitoring is acceptable. Real-time monitoring of inhibits to a catastrophic hazardous function is required when changing the configuration of the applicable payload system or when the provisions of paragraph 204 are implemented for flight crew control of the hazard. If ground monitoring is used to meet real-time monitoring, a continuous real-time data link (containing the applicable safety parameters) must be assured by the payload and continuous communications between the flight and ground crews must be established and maintained during the required period.

201.1c(3) Unpowered Bus Exception. Monitoring and safing of inhibits for a catastrophic hazardous function will not be required if the function power is deenergized (i.e., an additional fourth inhibit is in place between the power source and the three required inhibits) and the control circuits for the three required inhibits are disabled (i.e., no single failure in the control circuitry will result in the removal of an inhibit) until the hazard potential no longer exists.

201.3 Functions Resulting in Catastrophic Hazards. A function whose inadvertent operation could result in a catastrophic hazard must be controlled by a minimum of three independent inhibits, whenever the hazard potential exists.

One of these inhibits must preclude operation by an RF command or the RF link must be encrypted. In addition, the ground return for the function circuit must be interrupted by one of the independent

inhibits. At least two of the three required inhibits shall be monitored (paragraph 201.1c).
If loss of a function could cause a catastrophic hazard, no two credible failures shall cause loss of that function.

202.1 Solid Propellant Rocket Motors.
202.1d Monitoring. Monitoring requirements are a function of the design and operations as follows:
202.1d(1) No Rotation of the S&A Prior to a Safe Distance. The capability to monitor the status of the S&A device and one electrical inhibit in near real-time is required until final separation of the payload from the Orbiter. No monitoring is required if the payload qualifies for the unpowered bus exception of paragraph 201.1c(3).
202.1d(2) S&A Will be Rotated to Arm Prior to a Safe Distance. Prior to rotation of the S&A and separation of the payload from the Orbiter, the flight or ground crew must have continuous real-time monitoring to determine the status of the S&A and to assure that two of the three electrical inhibits are in place (paragraph 201.1c(2)).
202.2 Liquid Propellant Propulsion Systems.
202.2a(4) Monitoring. At least two of the three required independent electrical inhibits shall be monitored by the flight or ground crew until final separation of the payload from the Orbiter. The position of a mechanical flow control device may be monitored in lieu of its electrical inhibit, provided the two monitors used to meet the above requirement are independent.
Either near real-time or real-time monitoring will be required as defined in paragraphs 201.1c(1) and 201.1c(2). One of the monitors must be the electrical inhibit or mechanical position of the isolation valve.
Monitoring will not be required if the payload qualifies for the unpowered bus exception of paragraph 201.1c(3). If the isolation valve will be opened prior to the payload achieving a safe distance from the Orbiter, all three of the electrical inhibits that will remain after the opening of the isolation valve must be verified safe during final predeployment activities by the flight or ground crew.

5.1 Prevention of fire and explosion hazard at the launch site, explanation

1. Purpose

The following is a detail explanation of "5.1 Prevention of fire and explosion hazard at the launch site" Note that this section does not preclude other means to ensure safety.

2. Explanation of 5.1 (2) a.

This section explains in detail the sentence "The electrical capacity of the electrical equipment is sufficiently small and below the ignition limit of the explosive gas to prevent it from becoming an ignition source is also an effective explosion proof measure."

2.1. Assessment methods for the ignition limit of an explosive gas

It can be assessed that the electrical equipment could not be an ignition source at below the ignition limit of the explosive gas by using reference curve shown in Technical recommendations of the National Institute of Occupational Safety and Health "Recommended Practices for Explosion-Protected Electrical Installations in General industries" (hereinafter referred to as "Recommended Practices") Part 6 Equipment protection by type of protection "i" attachment A. The premise of this assessment is that the temperature range of the environment exposed to the electrical equipment is within the temperature range (from -20°C to + 60°C) as defined in Recommended Practices. (For the other cautionary note, see section 2.2)

Explosion-proof design is not mandatory when it can be assessed that the electrical equipment could not be an ignition source at below the ignition limit of the explosive gas.

<Information>

The assessment by using figure A.1 to A.6 in Recommended Practices is substituted for the confirmation by "assessment standard for Intrinsically-safe explosion-proof structure"i": spark ignition test (test to confirm no ignition capability in the circuit)". In spark ignition test in Group IIC, mixed gas composition for explosion test is specified, and this is the composition rate which provides minimum igniting energy within Hydrogen combustion range (4.0 to 75 vol % (under 1 atm)). Thus, change of gas condensation will be covered within this test to be complied with.

2.2. Supplemental information for implementation of Recommended Practices

2.2.1. Standard for hydrazine and methanol based on Recommended Practices

Ignition limit evaluation requires clarification of the target explosive gas group. Recommended Practices do not include standards for hydrazine and methanol, however, assuming the worst-case, Group IIC (*1) of the category of electrical equipment can be applied for hydrazine and methanol.

(*1) Definition of Group (Recommended Practices Part 1 General)

Group II: Electrical equipment used in an explosive atmosphere at the places except for the mine which is affected by the firedamp. Electrical equipment in Group II is classified into more specific categories based on the characteristics of the explosive atmosphere in which electrical equipment is used. (These categories are based on maximum experimental safety gaps or minimum igniting currents of an explosive atmosphere in which electrical equipment is used (See IEC 60079-20-1). The categories of Group II are the followings:

IIA: Propane, etc. / MESG ≥ 0.9 mm or MIC > 0.9 (*2)

IIB: Ethylene, etc. / 0.55 mm < MESG < 0.9 mm or 0.5 ≤ MIC ≤ 0.8 (*2)

IIC: Hydrogen, etc. / MESG ≤ 0.5 mm or MIC < 0.45 (*2)

MESG: maximum experimental safety gaps

MIC: minimum igniting currents

Group IIC is defined as the category with the lowest ignition energy (i.e., most easily ignited) of the gases to which it is exposed. All ignition energies below the threshold defined in Group IIC are also distinguished in Group IIC.

2.2.2 Implementation of Recommended Practices to Space environment

As the Recommended Practices assumes a ground environment (temperature -20°C to +60°C, atmospheric pressure 80 to 110 kPa, oxygen concentration about 21% by volume) as described in Part 1 General, the concept of applying the Recommended Practices to the temperature and depressurization environment after launch of a launch vehicle is summarized below.

- For temperature conditions, it is necessary to confirm that the post-launch temperature environment is included in the assumed temperature range of the Recommended Practices individually.
- Since ignition is less likely to occur in a depressurized environment than in atmospheric pressure, evaluation based on the Recommended Practices assuming atmospheric pressure can be a safe evaluation for depressurized environments (*2).

(*2) Rationale for evaluation of depressurized environment being on the safe side compared to evaluation at atmospheric pressure

The minimum ignition energy becomes significantly smaller as the pressure increases, but conversely increases under reduced pressure, making ignition less likely. (From ”High pressure gas safety technology for beginner revision 10” issued by The High Pressure Gas Safety Institute of Japan, p. 41). In addition, the combustion reaction becomes unable to continue as the ambient air pressure decreases (From “Combustible Science” Toshisuke Hirano section 3.2.3).

2.2.3 Extrapolation of Ignition Limit Curves of "Recommended Practices"

All of the origins of the coordinate axes in figure A.1 to A.6 of Recommended Practices are a certain value (not zero). Ignition limit curve can be extended with negative correlation if a point less than the origin wants to be used. (*3)

(*3) Rationale that voltage and current can be extrapolated with negative correlation

The amount of added energy is the condition of ignition when ignition is occurred by increasing temperature of the gas locally with spark like chattering.

(The threshold of ignition of hydrazine is defined as energy (several mJ) in AIAA SP-084-1999 Fire, Explosion, Compatibility, and Safety Hazards of Hypergols – Hydrazine issued by American Institute of Aeronautics and Astronautics)

3. Explanation of 5.1(2) d.

The following is an explanation of the sentence "Exposed electric heating wires are not energized in an explosive hazard atmosphere."

This sentence is written out of concern that exposed electric heating wires, such as nichrome wires used to burn out non-metallic wires used for holding and releasing mechanisms of small satellites may cause a local temperature increase that reaches the temperature upper limit (*4) of explosion-proof electrical equipment for flammable substances (liquid propellants, etc.). (Since electric heating wires do not normally produce sparks when heated, a mode in which a flammable substance that has reached its flash point burns due to sparks is not assumed.) On the other hand, heaters for catalytic layers used in large satellites generally do not reach temperatures high enough to reach the temperature upper limit of explosion-proof electrical equipment before payload separation, and thus do not require thermal analysis or other evaluation (heater temperatures during on-orbit operation are not considered here). If there is a heat source other than "exposed electric heating wire" that could be the temperature upper limit of the explosion-proof electrical equipment, it should be identified and controlled as a hazard.

(*4) The ignition temperature of hydrazine is 270°C and that of monomethylhydrazine (MMH) is 194.4°C. According to the Recommended Practices, it says "the temperature upper limit for electrical equipment of explosion-proof construction is approximately 80% of the lower limit of the ignition temperature corresponding to the respective ignition degree, minus the reference ambient temperature limit of 40°C." For example, in the case of MMH, the ignition degree is G4 (ignition temperature greater than 135°C and less than 200°C), and a temperature rise of up to 70°C is allowed.

5.3 Prevention of lithium-ion battery rupture hazard at the launch site, explanation

1. Purpose

This section explains the details of "Prevention of lithium-ion battery rupture hazard at the launch site." Note that this section does not preclude other means to ensure safety.

2. Method to determine the severity of lithium-ion battery rupture hazard

Battery ignition or rupture can cause injury to person and damage to ground equipment. The severity caused by lithium-ion battery ignition or rupture that falls under 1) and 2) below is considered a marginal/negligible hazard outside of the explosive hazardous atmosphere of the launch site, and therefore a hazard report is not required.

1) A single lithium-ion battery incorporated in the equipment with a watt-hour rating of 20 Wh or less
2) A single lithium-ion battery pack incorporated in a device with a watt-hour rating of 100 Wh or less.

In the explosive hazardous atmosphere of the launch site, all lithium-ion battery ignition or rupture will cause a fire, so the severity is considered a catastrophic hazard. The treatment of lithium-ion battery ignition or rupture while onboard a launch vehicle depends on the hazard analysis of the launch vehicle.

[Supplement 1] Following the fact that lithium-ion batteries that meet all the requirements of 1) and 2) above in the IATA Airline Dangerous Goods Regulations, 62nd Edition (2021), which stipulates the capacity of lithium-ion batteries that can be carried in an aircraft, can be exempted from the application of dangerous goods transportation (treated as non-dangerous goods), the above evaluation was made because the risk of rupture and ignition of lithium-ion batteries outside the explosive hazardous atmosphere of the launch site is considered to be smaller than that inside the cabin of an aircraft.

[Supplement 2] Evaluation of lithium-based energy storage devices other than lithium-ion batteries
Some lithium-based energy storage devices (lithium-ion capacitors, ionic liquid lithium-ion rechargeable batteries, etc.) other than lithium-ion batteries covered in these guidelines have been shown to have superior safety characteristics with less thermal runaway than lithium-ion batteries. At this time, safety design guidelines have not been established for these batteries because the application for space use has not been defined. If such batteries are to be used, the application

requirements are determined in coordination with the JAXA Safety and Mission Assurance Department.

[Supplement 3] Evaluation of nickel-metal hydride (Ni-MH) rechargeable batteries
Hazards such as rupture or leakage of electrolyte from Ni-MH batteries are not identified as a catastrophic or critical, so a hazard report is not required. However, it is necessary to confirm that there are no hazards due to overheating.

3. General approach to hazard control and safety verification methods
The general concept of the hazard control method and safety verification method when drafting a hazard report for a lithium-ion battery rupture is shown below.

3.1. Hazard cause (1) Internal short of a cell
3.1.1. Hazard control method
(1) Design and manufacturing of cells without internal short.

3.1.2. Safety verification method
*(1-1) Confirm that cells were made in accordance with the standard by a certificate of a UN 38.3 UN Recommendation transport test or a certificate of a UL1642, etc. In case of cells certified by a space agency, confirm that the cells have been certified by the agency
*(1-2) Confirm no change in battery charge/discharge characteristics before and after environmental tests (vacuum test, vibration test, etc.) of the payload on board condition (or battery assembly) by test report or other documents

* If JAXA-developed cells are used, it has already been verified and no additional verification is required (and subsequent items as well).

[Supplemental]
Internal short cannot be completely controlled by inspection such as X-ray inspection or process control during manufacturing. When using commercial cells, it is necessary to evaluate not only their track record on the ground, such as compliance with UN recommendations, but also their performance in the launch environment and space environment conditions. The same philosophy is used in NASA's CREWED SPACE VEHICLE BATTERY SAFETY REQUIREMENTS (JSC-20793).

3.2. Hazard cause (2) External short of the cell
3.2.1. Hazard control method

(2) Design and manufacturing without short-circuit on the battery load side.
Select either (2-1) or (2-2)
(2-1) Preparing two protection functions inside or outside of the cell against short-circuit outside the cell. (e.g. protection functions inside of the cell: separator shutdown function, PTC, fusible link, etc. protection functions outside of the cell: fuse, etc.)
The part where short-circuit is assumed in the path between the cell and the external protection function is double-insulation as shown in (2-2), because the external protection function doesn't work in the short-circuit of this path. In the case of a battery consisting of multiple cells in series, the protection function may be considered to be the same as the number of cells.

[Supplemental]
A load side short is counted as the first failure, so two protection functions should be prepared inside or outside the cell, as an implementation of a two-failure tolerant design.

(2-2) Double-insulation the load side.

[Supplemental]
Double-insulation on the load side is performed in accordance with Section 5.2 of the Design Standard Insulation (JERG-2-213A). Double insulation is considered to be extremely unlikely to cause short circuits and can be regarded as a design for minimum risk.
Examples of insulation include spatial isolation (a distance of at least 1 mm between conductors), covered wires, tapes (Kapton tape, polyester tape, etc.), resin sheets, etc.

Double-insulation lines can be applied to primary power bus lines and battery lines (including internal battery power lines, cell cases, battery housing, and battery output lines). When said lines pass through the board, it is necessary to show that double-insulation is established on and inside the board as well. In addition, sharp edges should be removed and wires should be properly rigged to prevent damage to wire sheathing and other insulation materials due to vibration, shock, etc.

When a switch is used for separation detection, if it can be shown that chattering due to launch vibration or factors other than launch vibration (e.g., mounting error, conductive contamination) will not cause a short circuit in said switch, a short circuit in the said switch is considered extremely unlikely to occur, so the scope of application of double-insulation may be upstream of the switch.

Usually, there are parts that cannot be double-insulated, such as FETs. In this case, failure tolerant design is applied. In other words, even if a double failure occurs, the battery should not rupture.

Specifically, for areas that cannot be double-insulated, the maximum current should be calculated assuming two failures, and it should be shown that the maximum current is within the battery's rating. Alternatively, the battery's rupture should be prevented even in the event of an external short circuit by using a protection function (2-1) in the battery or an overcurrent shutdown function such as a fuse. Alternatively, double-insulation of wiring harnesses within the range of two failures for FETs, etc., may be used.

3.2.2. Safety verification method

*(2-1-1) Confirm the design of protection functions by drawing or other documents.
Confirm that protection functions are installed in the proper location by drawings or other documents. Also confirm that the double-insulation between the battery and the external protective function is installed.

*(2-1-2) Confirm that protection functions work by functional test or other methods.
Confirm the effectiveness of the protection function by the following means

- The appropriate external short resistance value assumed in the system design should be set and an external short test should be conducted to demonstrate that the protection function is effective. When verifying the protection function possessed by a cell, the protection function should be confirmed using a battery with the same timing and the same part number purchased from the same supplier as the flight item.
- The battery should be confirmed by a catalog or other means to have been certified in accordance with UN 38.3 or UL1642, and the certification number of the battery should be indicated. This can be assumed that one protection function has been verified. However, in this case, even if the battery has multiple protection functions inside, they are not individually confirmed, i.e., they are considered to be a single protection function, and the verification data for another protection function should be shown. (If verification based on UL standards has not been conducted, indicate the test items and test conditions corresponding to UL standards and the data sheet or test data for the overcurrent protection function.)

*(2-2-1) Confirm the design of double-insulation by drawing or other documents.
*(2-2-2) Confirm the installation of double-insulation by inspection or other methods.

- After environmental tests with an onboard condition (vacuum test, vibration test, etc.), confirm that double-insulation is in place and that there are no sharp edges at the wire rigging points by visual inspection.

- The maximum current for the parts that are not double-insulated should be calculated using the drawings and circuit resistance, assuming a two-fault. The analysis should then show that it is within the battery rating.

[Supplemental]
When space isolation is selected as one of the double-insulations, it should be shown that space insulation is secured based on the pattern diagram and actual measurement of the substrate. For patterns inside the substrate laminate, it is sufficient if the spatial isolation is 1 mm or more, including the thickness direction. Care should be taken not to overlook insulation considerations with through holes.

3.3. Hazard cause (3) Overcharge/Over-discharge

3.3.1. Hazard control method

(3-1) The charging system should be provided with an overcharge prevention function (anomaly detection and power shutdown function) and the following should be considered.
1FT design against overcharging when charging outside the explosive hazardous atmosphere at the launch site, and 2FT design when charging inside the explosive hazardous atmosphere or while the payload is on board the launch vehicle.
In principle, temperature sensors are not used as overcharge monitors because temperature sensors are often unable to detect rapid temperature changes inside cells due to overcharging in real time. If it is necessary to use a temperature sensor, the temperature sensor should be correlated to the cell temperature.
(3-2) Prevent overcharge due to voltage variations in each cell. Since battery total voltage monitoring may not detect single-cell overcharge due to cell variations, one means of overcharge prevention function should be each cell voltage monitoring. Alternatively, battery total voltage monitoring should be performed with cell voltage variations under control (single-cell anomalies can be confirmed).
(3-3) Since recharging after over-discharge can be a hazard cause, do not use batteries below the voltage recommended by the cell/battery pack manufacturer or established in qualification tests for over-discharge. In the unlikely event that the voltage falls below the voltage range, do not continue to use the battery.

[Supplement]
The primary concern with lithium-ion batteries is overcharging (short-circuit has internal energy only, but energy continues to be supplied externally when charging). Since commercial chargers are generally not designed to be 2FT design, additional control measures should be added for use in

charging in explosive hazardous atmospheres. Note that NASA's unmanned spacecraft is also required a 2FT design against overcharging.

3.3.2 Safety verification method

(3-1-1) Confirm proper FT design by drawing or other documents

(3-1-2) Confirm that the protection functions work properly by functional test or other methods

*(3-2) Confirm the results of cell variation control by inspection or other methods

(3-3) Confirm battery voltage before charging (only if there is a charging operation at the launch site)

[Supplement]

In managing charging capacity, since battery voltage fluctuates with charging current and temperature, charging capacity should be specified by the product of current and time, in addition to monitoring voltage.

[Supplement]

Regarding over-discharge. Over-discharge itself is not a safety issue, but problems such as over-charge occur during subsequent recharging (when recharging a battery that contains cells with abnormally low voltage due to over-discharge, other cells in series will be over-charged). If it is confirmed that, at least at the launch site, no functional tests or other operations are planned in which the battery is completely discharged, and that safety measures such as cell monitoring and cell variation control are taken to prevent overcharging, it is not necessary to consider a special safety design for over-discharging. When battery charging operations are planned at the launch site, the voltage should be measured before charging to confirm that there is no voltage drop beyond the expected level.

3.4. Hazard cause (4) Use in abnormal temperature environments caused by thermal control system failure

3.4.1. Hazard control method

Select either (4-1) or (4-2).

(4-1) Design environmental temperature below the guaranteed battery temperature even under a worst-case condition (after two failures of the heater driver circuit).

(4-2) 2FT design against the heater ON.

[Supplemental]

For failures due to secondary factors such as heater overheating, the strength design of commercial batteries is dependent on the manufacturer, so it is necessary to design two failure tolerances on the heat source side.

3.4.2. Safety verification method

(4-1) Confirm that the temperature is below the guaranteed battery temperature by thermal analysis. (Considering after two failures of the heater drive circuit.)

(4-2-1) Confirm 2FT design by drawing or other documents

(4-2-2) Confirm that 2FT design is valid by functional test or other methods

Appendix A: Definition of Terms

(1) Cell

A cell consists of positive/negative plates, separators, electrolytic solution, and a container that makes up battery.

(2) Battery

Battery is made of one or more cell(s) with added control circuit and made into a package.

(3) PTC (Positive temperature coefficient)

Positive temperature coefficient is an element with great resistance variance with an ability to shut down electric current by unlimited resistance when reaching a certain temperature.

(4) UN Recommendations

United Nations Recommendations on the Transport of Dangerous Goods, an International transportation standard of dangerous goods developed by dangerous goods transportation specialists committee to secure safe international transportation of dangerous goods via land, sea, and air.

(5) UL (Underwriters Laboratories Inc.)

A safety certification organization in the United States. UL sets standards for functionality and safety for materials, parts, equipment, tools, and end products, formulates evaluation methods, and conducts actual evaluation tests. When a product passes these tests, it is allowed to use the UL certification mark.

(5) JAXA completed development cell

A lithium-ion battery for space use, registered as a JAXA completed development component.

5.5 Prevention of inadvertent RF radiation hazard at the launch site, explanation

1. Purpose

"5.5 Prevention of inadvertent RF radiation hazard at the launch site" is based on Japanese regulations including "The Radio Radiation Protection Guidelines for Human Exposure to Electromagnetic Fields" (hereinafter referred to as RRPG). This section describes the methods to assess compliance with Japanese regulations in performing RF radiation hazard analysis.

The scope of this section is limited to electromagnetic radiation sources installed on the spacecraft that have the following characteristics:

- Electromagnetic radiation sources with frequencies above 300 MHz (bands mainly for amateur wireless band, S band, and K band), and
- Electromagnetic radiation sources may be operated at launch sites.

Electromagnetic radiation exposure to heart pacemaker wearers is out of the scope of this section. (The Japanese regulation, "RRPG," does not cover heart pacemaker wearers.) Should the possibility of exposure to heart pacemaker wearers arise, separate considerations should be made.

Note that this section does not preclude other means to ensure safety.

<Background>

Frequent debates have occurred in the past safety reviews regarding the thresholds of different hazard severity categories (I, II, and III). This section provides guidelines for safe distance calculation and the criteria for hazard severity.

2. Rationales

2.1 Scope of this section

Evaluation methods described in section 5.5 mainly consider thermal effects. RRPG stipulates the prevention of stimulation effects on human body from contact current and induced current. However, the frequency range at or above 300 MHz covered in this section is out of the scope of RRPG. (Paragraph 3.3.1, "1991 RRPG)

2.2. Rationale for Step 1 A)

Step 1 A) is intended for screening for safety evaluation of systems such as small satellites.

The screening threshold values calculated based on the Electromagnetic Field Strength Guidelines of RRPG, depending on conditions, may be lower than the values calculated based on the Basic Guidelines. On the other hand, in Step 1 A), the minimum acceptable values that meet the Basic Guidelines, the backbone of RRPG, are used as the threshold values. Electromagnetic radiation sources are accepted as low-power sources if the Basic Guidelines is met, even if the Electromagnetic Field Strength Guidelines is not.

The Basic Guidelines is used since one of the Basic Guidelines uses Specific Absorption Rate (SAR) as a criterion, irrelevant of antenna types, offering the advantage to require antenna output only (The Electromagnetic Field Strength Guidelines requires to consider antenna types and gains and unique judgment for each antenna).

(1) Rationale for 6 GHz in Step 1 A)

The Basic Guidelines paragraph 4.b requires consideration to limit the power density incident to the eye (6-minnutes average value) to be at or less than 10 mW/cm2 for the frequency range of 6 GHz and above. On the other hand, for electromagnetic radiation sources below 6 GHz, consideration for optical incident power density is not required, and SAR for the entire body, 0.4 W/kg (6-minnutes average value) per the Basic Guidelines 1, may be used. Thus, electromagnetic radiation sources at and above 6 GHz have thresholds that take not only antenna power but also gain into consideration, and its hazard severity cannot be identified in Step1 A). Identifying hazard severity of electromagnetic radiation sources at and above 6GHz is performed in Step 1 B) C) and subsequent steps.

Note: The 2011 Consultation Report No. 2030 on "The way Partial-body Absorption Guidelines ought to be" extended the scope of the Partial-body Absorption Guidelines to 6 GHz. For both whole-body averaged SAR and local SAR specified here, the previous reference value from 100 kHz to 3 GHz is now applicable from 100 kHz to 6 GHz, and the threshold value is revised from 3 GHz to 6 GHz.

(2) Rationale for 10 cm distance from the electromagnetic radiation source in Step 1 A)

10cm was determined according to the definition of space in the Partial-body Absorption Guidelines in paragraph 4.2 (3) of the 1997 RRPG. Operational environment in launch site is the “controlled environment (work environment)” per RRPG. Therefore, electromagnetic radiation source output was established by the following evaluation.

(3) Rationale for 20 W in Step 1 A)

The spaces separated by 10 cm or more from the electromagnetic radiation sources were evaluated based on the Basic Guidelines. Because the spaces several wavelengths away from the antenna are evaluated for the whole-body exposure, SAR for the whole body, 0.4 W/kg (6-minnutes average value) per the Basic Guidelines is applied. Presuming a person weighing 50 kg, the acceptable value is 20 W（=0.4 [W/kg] x 50[kg]）. This evaluation is conservative as it is the exposure to the total power output from antenna.

2.3. Rationale for Sep 1 B) and C)

Use the following process to apply RRPG (paragraph 3.1.5 of 1990 RRPG and paragraph 4.2 of 1997 RRPG). Step 1 B) and C) were set based on this process.

1. The order of evaluation of the safety distance calculation indicated in Step 1 B) and C)

Controlled environment is where actual circumstances of radio wave use are acknowledged, subjects for protections are identifiable, and necessary measures such as calling for caution are implementable; general environment is where these are not satisfied. The evaluation process introduced in Step 1 B) and C) are based on the underline policy of paragraph 3.1.5, "Application procedures for the radio-radiation RRPGs" of 1990 RRPG.

(1) When the space is distant enough from the electromagnetic radiation source (having a uniform electromagnetic field), general condition (Condition G) is applied for evaluation.

(2) When the above (1) is not satisfied, controlled environment (Condition P) is applied for evaluation of electromagnetic field strength.

General environment is applied to the environment where adequate control per RRPG is not implemented. In this environment, generally speaking, radiation is not measured frequently, measurement points are not covered enough, or surrounding conditions are changing including the circumjacent objects or buildings which scatter radiation. Thus, the electromagnetic field strength is predicted to increase to about two holds even if the radiation source does not change. General environment considers these uncertainties and applies additional safety margins compared to controlled environment as 5 folds for power density (2.23 holds for electrical field or magnetic field) (Appendix 1, paragraph 2.1.2, 1990 RRPG).

For launch site operations, evaluation can be made for controlled environment. However, evaluation shall be made for general environment first to avoid troublesome evaluation considering issues such as reflection waves in the unique working environment of the launch site.

(3) When the space is in a non-uniform electromagnetic field or near-field, the evaluation shall be conducted by RRPG, II Supplementary Guidelines, (1) Non-uniform or partial-body electromagnetic field exposure.

When safety distance is around tens of centimeters, Electric Field Strength Guidelines, which most consider whole body exposure, are not actually applicable; Supplementary Guidelines, which consider cases where radio wave is non-uniform or exposure is partial, are used as main guidelines.

During operations of electromagnetic radiation sources installed in the satellites, the body parts exposed to electromagnetic sources are expected to be extremities. No operations that require for operators to stay in the proximity of the electromagnetic radiation sources more than 6 minutes are expected.

(4) When the above administrative guidelines are not met, evaluate using the Basic Guidelines.

Table 1 below lists related guidelines. Even if safety distance from the electromagnetic radiation sources (current density becomes 1 mW/cm2) is 50 cm, the Basic Guidelines (i.e., 25 W/kg for body surface and extremities) may be applied to the space within the safety distance. If the safety distance becomes as short as 25 cm, current density becomes 4 mW/cm2, which does not exceed the Basic Guidelines (25 W/kg) considering the surface area of the extremities of operators.

Table 1 Frequencies with the most severe condition amongst frequency ranges subject to this document

RRPG for 3GHz range (6 minutes average)

	Electric Field Strength Guidelines	Supplementary Guidelines		Partial-body Absorption Guidelines	Basic Guidelines	
		Body surface	Eyes	Extremities	Body surface and extremities	Eyes
Condition G/ General environment	1 mW/cm2	4 mW/cm2	2 mW/cm2	4 W/kg	25 W/kg	10 mW/cm2
Condition P/ Controlled environment	5 mW/cm2	50 mW/cm2	10 mW/cm2	10 W/kg		
Note		(Reference only as these guidelines are not for extremities)		(Reference only as these guidelines are for portable devices)		(Reference)

2. Rationale for 1.4 m in Step 1 B)

The safety distance threshold value of 1.4 m calculated in Step 1 B) b. was derived based on the electromagnetic radiation source output acceptable value 20 W calculated in Step 1 A) using the following conditions. Gain with no change; reflection co-efficient, K, as 2.56 (when transmitting frequencies is at or above 76MHz, considering reflection from the large ground); acceptable current density as 0.2 mW/cm2. When inversely calculated from this safe distance, the radiation source can

be considered as a marginal/negligible hazard by limiting access to incidental accesses, since the value exceeding acceptable antenna output shown in Step 1 A) is allowed depending on the conditions.

2.4. Rationale for Step 2

The threshold value for catastrophic cases shall be whole body SAR, 4 W/kg, 6 minute average. This is the worst value of the ranges resulting in biological effects (4 to 8 W/kg) based on the rat experiments conducted by the U.S. and other countries. (This is based on paragraph 1.1 of Appendix 1 of 1990 RRPG. 0.4 W/kg in the Basic Guidelines was derived using this value applying safety coefficients.) Thus, for a person weighing 50kg, radiation emission (6 minutes average) of 200 W（4 W/kg x50 kg = 200 W） is a catastrophic hazard.

Limiting exposure time to electromagnetic waves increases the acceptable value of electromagnetic radiation source output, making it one of the hazard controls.

When the frequency of an electromagnetic radiation source reaches 300MHz or above, the dominant effect on human body is thermal. The Guidelines is taking consideration the thermal effects including about one degree increase in deep body temperature when exposed to radio wave (6 minute average). Exposure to radio waves is not time critical in terms of thermal effects. RRPG also states that the radio wave strength exceeding the RRPG itself does not mean an immediate adverse effect on health, since RRPG uses safety coefficient and considers other issues (Paragraph 6.2 (1) of 1997 RRPG). Therefore, evacuation within a reasonable time ensures the hazard will not lead to a loss of life, making it one of hazard controls.

3. Reference Documents

This document was developed mostly based on below.

Telecommunications Technology Council Report No. 38 "the Radio Radiation Protection Guidelines for Human Exposure to Electromagnetic Fields" (June, 1990)

Telecommunications Technology Council Report No. 89 "the Radio Radiation Protection Guidelines for Human Exposure to Electromagnetic Fields" (April 1997)

The above guidelines were compiled based on the researches of numerous literatures and overseas laws and regulations.

This document also incorporates the results of discussions with the experts.

Appendix A: Definition of Terms (Excerpts from "the Radio Radiation Protection Guidelines for Human Exposure to Electromagnetic Fields (June, 1990))

(1) Radio Radiation Protection Guidelines for Human Exposure to Electromagnetic Fields

Guidelines that recommend the requirements to meet for ensuring the safety of radio use so that any individual exposed to radio radiation (limited to the frequency range between 10 kHz and 300 GHz) is protected from any undesirable biological effect of the radiation.

(2) Basic Guidelines

Guidelines intended for evaluation of safety to human body, based on the various biological functions (e.g., thermal stress due to body temperature increase, electrical current stimulation, and high frequency wave burns) when exposed to an electromagnetic field.

(3) Administrative Guidelines

Guidelines intended for actual evaluation using measurable physical quantities (e.g., electric field strength, magnetic field strength, current density, current, and specific absorption rate) to show compliance with the Basic Guidelines. Administrative Guidelines are composed of the Electromagnetic Field Strength Guidelines, Supplementary Guidelines, and Partial-body Absorption Guidelines.

(4) Electromagnetic Field Strength Guidelines

Guidelines intended for evaluation of safety of the spaces based on applicable electric field strength, magnetic field strength, and current density.

(5) Partial-body Absorption Guidelines

Guidelines intended for use in cases where part of the human body is subject to concentrated exposure to an electromagnetic field associated with electromagnetic radiation from a wireless device being used in the extreme proximity to the human body.

(6) Supplementary Guidelines

Guidelines intended for detailed evaluation per Basic Guidelines when Electromagnetic Field Guidelines is not satisfied. This Guidelines relax or exclude the application of the Electromagnetic Field Strength Guidelines based on exposure conditions to electromagnetic fields (i.e., non-uniformly, partially, on the surface), applicable biological functions (i.e., contact current and induced current), and radiation source attribution (i.e., antenna power and frequency range) when these parameters are explicit.

(7) Controlled environment

Environment where human body exposure to electromagnetic field is acknowledged, its radiation source is identified, and controls are provided appropriately.

(8) General environment

Environment with unknown factors where human body exposure to electromagnetic field is not properly acknowledged and controls are not provided appropriately. One example is the case where residents are exposed to electromagnetic fields in the general housing environment. Thus, in the applicable guidelines, acceptable values are lower for general environment compared to controlled environment. General environment corresponds to Condition G in 1990 RRPG.

(9) Specific Absorption Rate (SAR)

The electric power absorbed by the unit mass of the human tissue exposed to an electromagnetic field. Whole-body SAR is the average of SAR in the entire body; Partial-body SAR is the average of SAR for 1 g or 10 g of the arbitrary tissue of a body part.

(10) Distant field

The electromagnetic field separated farther than both $2D^2/\lambda$ or $\lambda/2\pi$ from the electromagnetic radiation sources, having no reflection or scatter. D is the maximum dimension of antenna: λ is a free space wave.

Appendix B: Guidelines in "the Radio Radiation Protection Guidelines for Human Exposure to Electromagnetic Fields" (Excerpts from 1990 RRPG and 1997 RRPG)

• Basic Guidelines (Paragraph 3.3, Table 5 in 1990 RRPG)

1. The whole-body averaged SAR over any given 6-minute period must not exceed 0.4 W/kg.
2. At frequencies between 10 kHz and 100 kHz, the induced current density in the tissue must not exceed 0.35 x 10-4 f[Hz] mA/cm2.
3. The current flowing in from the outside the body, such as contact current, must not exceed 10-3f[Hz] mA (average time < 1 second) at frequencies between 10 kHz and 100 kHz, or 100 mA (average time: 6 minutes) at frequencies between 100 kHz and 100 MHz.
4. In addition to 1, 2, and 3 above, the following conditions should also be taken into account:

(a) Even though the whole-body averaged SAR over any given 6-minute period is below 0.4 W/kg, the SAR for any 1 gram of tissue (average time: 6 minutes) should not exceed 8 W/kg (25 W/kg for the skin surface and extremities).

(b) At frequencies at or above 3 GHz, the power density incident to the eye must not exceed 10mW/cm2 (average time: 6 minutes).

• Administrative Guidelines (1997 RRPG)

I. Electromagnetic Filed Strength Guidelines

Table 1: Electromagnetic Field Strength Guidelines for Controlled Environment

(Condition P) (Average Time: 6 Minutes)

Frequency f	rms electric field strength E [V/m]	rms magnetic field strength H[A/m]	Power density S[mW/cm2]
10 kHz～30 kHz	614	163	
30 kHz～3 MHz	614	$4.9f[MHz]^{-1}$ （163 – 1.63）	
3 MHz～30 MHz	$1842f[MHz]^{-1}$ （614 – 61.4）	$4.9f[MHz]^{-1}$ （1.63 – 0.163）	
30 MHz～300 MHz	61.4	0.163	1
300 MHz～1.5 GHz	$3.54f[MHz]^{1/2}$ （61.4 - 137）	$f[MHz]^{1/2}$／106 （0.163 - 0.365）	f[MHz]／300 (1 – 5)
1.5 GHz～300 GHz	137	0.365	5

Table 2: Electromagnetic Field Strength Guidelines for General Environment

(Condition G) (Average Time: 6 Minutes)

Frequency f	rms electric field strength E [V/m]	rms magnetic field strength H[A/m]	Power density S[mW/cm2]
10 kHz～30 kHz	275	72.8	
30 kHz～3 MHz	275	$2.18f[MHz]^{-1}$ （72.8 - 0.728）	
3 MHz～30 MHz	$824f[MHz]^{-1}$ （275 - 27.5）	$2.18f[MHz]^{-1}$ （0.728 - 0.0728）	
30 MHz～300 MHz	27.5	0.0728	0.2
300 MHz～1.5 GHz	$1.58f[MHz]^{1/2}$ （27.5 - 61.4）	$f[MHz]^{1/2}$／237.8 （0.0728 - 0.163）	f[MHz]／1500 (0.2 – 1)
1.5 GHz～300 GHz	61.4	0.163	1

II. Supplementary Guidelines

(1) Supplementary Guidelines for cases of non-uniform or partial-body exposure

<table>
<tr><td></td><td>10 kHz-300 MHz</td><td>300 MHz-1 GHz</td><td>1 GHz-3 GHz</td><td>3 GHz-300 GHz</td></tr>
<tr><td>Spatial average of electromagnetic field strength</td><td colspan="4">Controlled environment: Table 1 is applied.
General environment: Table 2 is applied.</td></tr>
<tr><td rowspan="2">Spatial maximum of electromagnetic field strength</td><td></td><td colspan="2">Other than extremities:
Controlled env.: 20 mW/cm2
General env.: 4 mW/cm2</td><td>Skin surface:
Controlled env.:
50 mW/cm2
General env.:
10 mW/cm2</td></tr>
<tr><td></td><td></td><td>Head:
Controlled env.:
10 mW/cm2
General env.:
2 mW/cm2</td><td>Eyes:
Controlled env.:10mW/cm2
General env.:2mW/cm2</td></tr>
<tr><td>Relevant space</td><td>Space occupied by the human body and separated by 20 cm or more from electromagnetic radiation sources and metallic objects</td><td colspan="3">Space occupied by the human body and separated by 10 cm or more from electromagnetic radiation sources and metallic objects</td></tr>
<tr><td>Average time</td><td colspan="4">6 minutes</td></tr>
</table>

III Partial-body Absorption Guidelines

Scope: Applicable to frequency range between 100 kHz and 3 GHz

Applicable equipment: Applicable to small radio equipment used in proximity to the human body. The distance from the electromagnetic field radiation source is within 20 cm at frequencies between 100 kHz and 300 MHz and within 10 cm for frequencies between 300 MHz and 3 GHz.

	Controlled environment	General environment
Whole-body SAR	0.4 W/kg	0.08 W/kg
Partial-body SAR	For any 10-g tissue 10 W/kg 20 W/kg (extremities)	For any 10-g tissue 2 W/kg 4 W/kg (extremities)

6 Inherent safety design requirements irrelevant to hazard analysis, explanation

This is a requirement for safe depressurization and propellant and oxidizer discharge in case of anomalies such as propellant or oxidizer (hydrazine, MMH, MON3, NTO, etc.) leakage from the payload. This is an inherent safety design requirement not based on hazard analysis, which requires additional emergency measures based on past discussions that even if a two-failure design was established as a result of hazard analysis, the possibility of minor leakage still cannot be ignored.

Until the JMR-002C version, the design had to be capable of both depressurization and propellant and oxidizer discharge while the payload is loaded on the launch vehicle. However, in the JMR-002D version, it was discussed that if depressurization can be performed while the payload is loaded on the launch vehicle, the amount of leakage will be reduced and the payload can be safely moved, the location of propellant and oxidizer discharge became be selected (e.g., while the payload is onboard or after it is returned to the satellite maintenance area).

In the JMR-002E version, in consideration of the actual situation in the U.S. and France, as well as user feedback, we have deleted the requirement that depressurization should be performed in the "launch vehicle onboard condition" to allow for more flexible operation of depressurization. This allows the user to choose the location of the depressurization (e.g., while the payload is onboard or after it is returned to the satellite maintenance area). One of the reasons for the revision is the opinion that if depressurization operation actually occurs while the payload is onboard in the launch vehicle, it is anticipated that the personnel will have to enter the fairing using a diving board in a leaking propellant, oxidizer, etc., to depressurize the payload, a highly dangerous operation, and that a requirement that implicitly requires such a task should be avoided. Revision E allows the PL organization to choose the location and procedure for depressurization and discharge of propellant, oxidizer, etc. In the past, there was a design constraint to provide a depressurization port for the payload in a direction accessible to personnel while the payload is loaded on the launch vehicle, but if it is safe to depressurize the payload after moving to the satellite maintenance area, this design constraint will be eliminated.

The actual operational procedures in the event of a leak of propellant, oxidizer, etc. while the payload is on board the launch vehicle depend on the design and operation of the launch vehicle, so the feasibility should be confirmed with each launch vehicle.

Format-1 Safety Requirements Tailoring Request Form (1/2)

1. Title	Number Date	PL organization Section

2. (1) Payload name (2) Subsystem name	Development Manager	System Safety Program Manager	Prepared by

3. Document title, document number, and section number to be tailored

4. Differences in safety requirements and controls before and after tailoring 4.1 Differences in safety requrirements (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 needed)

5. Reason for tailoring (Use additional sheets if extra space is needed)

6. Rationale why equivalent safety is assured (Use additional sheets if extra space is needed)

Decision: Approval Approval with conditions Reexamination (Circle one)	JAXA Safety and Mission Assurance Department
Reasons, Comments, etc. :	Date

Note: This format 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 JAXA Safety and Mission Assurance Department beforehand.

Format-1 Safety Requirements Tailoring Request Form (2/2)

1. Title (Continued)	Number
2. (1) Payload name (2) Subsystem name	

Format-2 Hazard Identification Summary

System name : ___________________

Subsystem name : ___________________

Hazard Category Hazard Cause System, Subsystem, component, other hazardous item, or task/step title	Fire/Explosion							Rupture		Leakage of toxic materials						Radiation																									
	Presence of ignition source, etc.	Laser (JIS C 6802(IEC 60825-1) class 4	Static electricity	Explosives (Solid propellants/pyrotechnics)	Rust, etc.	Flammable liquid propellant	Mixing of propellants and oxidizers	Pressure systems/Pressure vessels	Lithium ion battery	Loose joints, damaged piping, etc.	Deteriorated seals, worn seals, valve malfunctions	Fluid incompatibility	Foreign matter mesh in valves, etc.	Falling of tanks with toxic materials	Pathogens, etc.	RF	Ionizing radiation/Radioactive materials																								
Hazard report No.																																									

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

- Human factors
- Software error (input error, bug)
- Hazardous operations (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.

Format-3 Hazard Analysis Table

No.	Hazard Title	Hazard Summary	Cause	Control	Severity	Likelihood	Note (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.

Format-4 Safety Verification Tracking Log (SVTL) 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)

Format-5 Hazard Report

<table>
<tr><td>Hazard Report</td><td colspan="2">Hazard Report No.</td></tr>
<tr><td>System</td><td>Date</td><td>Drafted/revised</td></tr>
<tr><td>Subsystem</td><td colspan="2">Phase</td></tr>
<tr><td colspan="3">Hazard Title</td></tr>
<tr><td>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="3">Description of the Hazard</td></tr>
<tr><td colspan="3">Hazard Causes</td></tr>
<tr><td colspan="3">Hazard Controls</td></tr>
<tr><td colspan="3">Safety Verification Methods</td></tr>
<tr><td colspan="3">Status of Verification</td></tr>
</table>

Format-5 Hazard Report

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

Format-6 Noncompliance Report (NCR)

<table>
<tr><td colspan="2">Title</td><td>Number</td><td>Date</td></tr>
<tr><td colspan="2" rowspan="2">Payload Name</td><td colspan="2">PL organization name, Section name</td></tr>
<tr><td>Development Manager</td><td>System Safety Program Manager</td><td>Prepared by</td></tr>
<tr><td>Disposition ;</td><td></td><td></td><td></td></tr>
<tr><td colspan="4">Applicable Safety Requirements</td></tr>
<tr><td colspan="4">Description of Noncompliance</td></tr>
<tr><td colspan="4">Reason for Noncompliance
(Use additional sheets if extra space is need)</td></tr>
<tr><td colspan="4">Relevant Hazard Control (Applicable Hazard Report No.:)
(Use additional sheets if extra space is need)</td></tr>
<tr><td colspan="3">Decision</td><td>JAXA/Safety Section
Date</td></tr>
</table>

*Attach the support materials or data.