限定なし

ロケットペイロード安全標準

２０２２年　１１月　２４日　E改訂

宇 宙 航 空 研 究 開 発 機 構

免責条項

ここに含まれる情報は、一般的な情報提供のみを目的としています。JAXA は、かかる情報の正確性、有用性又は適時性を含め、明示又は黙示に何ら保証するものではありません。また、JAXA は、かかる情報の利用に関連する損害について、何ら責任を負いません。

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.

発行

〒305-8505 茨城県つくば市千現 2-1-1

宇宙航空研究開発機構 安全・信頼性推進部

JAXA（Japan Aerospace Exploration Agency）

目次

1. 総　則

1.1 目　的

本標準は宇宙航空研究開発機構（以下、「機構」という。）種子島宇宙センター及び内之浦宇宙空間観測所（以下、「鹿児島宇宙センター」という。）から打上げられるロケットペイロード（以下、「ペイロード」という。）、及びその地上支援装置（以下、「ＧＳＥ」(Ground Support Equipment)という。）の鹿児島宇宙センターへの搬入から射場作業、打上げを経てロケットからペイロードの分離までに生ずる事故等から人命及び財産（公共や第三者の私有財産）を守ると共に環境を保護する為、ペイロードの担当組織（以下、「PL担当組織」という。）が実施すべき安全管理及び安全設計について、統一的な要求事項を定めることを目的とする。

1.2 適　用

鹿児島宇宙センターを利用するPL担当組織は、ペイロード及びＧＳＥ（以下、「ペイロード等」という。）に関して、本標準を契約書等に呼び出して適用すること。

ただし、法令の遵守のみで安全を確保できる作業（労働安全衛生法に基づく要員の安全確保等）については、適用対象外とする。すなわち、PL担当組織の要員の安全確保については関連する法令及び機構基準を遵守しつつPL担当組織自らの責任において対応すること。

また、鹿児島宇宙センターにおける作業安全要求については「射場運用安全技術基準」(JERG-1-007)に従う必要がある。

注）JMR-001「システム安全標準」が適用されるペイロードは、本標準の4章の部分はJMR-001の要求が優先される。

1.3 各組織の責任

PL担当組織は以下の責任を有する。

(1) 本標準に従い、ペイロード等に係る安全を確保するために必要な処置を講じる。
(2) 本標準で定められた安全審査用文書を、安全審査実施前の所定の期日までに安全・信頼性推進部へ提出する。
(3) 本標準で定められた安全審査プロセスを完了する。

機構は以下の責任を有する。

(1) PL担当組織から提出された安全審査文書が本標準に適合していることを所定の期日までに確認する。

1.4 テーラリング

(1)　システム安全管理要求のテーラリング

本標準のシステム安全管理要求事項はペイロード等の特徴、特性に応じて、また国内外の実績を評価して修整して適用することができる。この場合、PL担当組織は、安全・信頼性推進部と修整部分及び修整理由について協議し、テーラリングの内容等をシステム安全プログラム計画書（4.2.1項）に反映し、4.6項に示す機構のシステム安全審査で承認を受けること。

(2)　安全要求のテーラリング

システム安全プログラム計画書で適用とした安全要求事項は、対象とするペイロード等の特徴、特性に応じて、また国内外の実績を評価して修整して適用することができる。PL担当組織は、安全・信頼性推進部と修整部分及び修整理由について協議し、テーラリングの内容を様式1又は同等の様式で示し、システム安全プログラム計画書に添付し、4.6項に示す機構のシステム安全審査で承認を受けること。

2. 適用文書等

下記の文書は本標準に規定する範囲において、この本標準の一部をなすものである。適用文書は適用時点の最新版とし、システム安全プログラム計画書に適用版を明記すること。

2.1 適用文書

(1) JERG-0-001 「宇宙用高圧ガス機器技術基準」
(2) CZA-2018029 「ロケットペイロード システム安全プログラム計画書/安全データパッケージテンプレート」
(3) JERG-1-007 「射場運用安全技術基準」

2.2 参考文書

(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 「システム安全審査部会運営要領」

3. 用語の定義

本標準の用語の定義を示す。

圧力システム

圧力容器、機器及びこれらを継ぐ配管などによって構成されるシステム

圧力容器

内部に高圧ガスを貯蔵する容器。ここでいう高圧ガスとは、

(1) 常用の温度において圧力(ゲージ圧）が1.0 [MPa]以上となる圧縮ガスであって現にその圧力が1.0 [MPa]以上であるもの、又は温度35℃において圧力1.0 [MPa]以上となる圧縮ガス（圧縮アセチレンガスを除く）。
(2) 常用の温度において圧力が0.2 [MPa]以上となる液化ガスであって現にその圧力が0.2 [MPa]以上であるもの、又は圧力が0.2 [MPa]となる場合の温度が35℃以下である液化ガス。

安全

ハザードが事故等に至らないように、除去、最小化又は制御されている状態。即ち、リスクが許容できるレベルまで低い状態

安全上クリティカルな

識別されたハザードの被害の度合いがⅠ又はⅡの危険を有している状態をいう。例えば、安全上クリティカルな運用手順とか、安全上クリティカルな部品等の使い方をする

安全審査

ペイロード、ＧＳＥ及び射場作業がペイロードの安全要求事項に適合していることを含め、ハザードが漏れなく識別され、ハザードレポートに記載のハザード 原因の制御及びその検証について、各開発段階において評価・確認し、ハザードの残存リスクが許容できるレベルにあることを評価・確認するための審査

安全装置

装置の故障、誤使用がハザードとして識別された事故を引き起こさないよう防止する装置、又はシステムの総称

インヒビット
　事故に繋がる機能について要求しない時にその機能が動作することを抑制するため、事故に繋がる機能を動作させるエネルギ源との間に設ける物理的な遮断であり、故障許容設計の実現の手段として用いられる。電気回路におけるリレー、配管における遮断弁等がインヒビットの具体例である。

ＦＴＡ(Fault Tree Analysis)
　故障の木解析。システム等にとって致命的な事象を出発点として、これを論理的に要素に分解して行き、最終的に観測可能な基本要素（故障原因）にまで細分化することで、定性的又は定量的な故障の予測、又は故障原因調査を行う解析手法

警報装置
　特定の安全でない状態又はそれに近い状態をタイムリーに検出して、適切な警報信号を発生して要員に警告するための装置

故障
　システム、サブシステム、機器、部品が規定の期間中、規定の条件下で、規定の制約の範囲内で要求される機能を果たすことができなくなること

再飛行ペイロード
　過去に鹿児島宇宙センターから打上げられたペイロード（ペイロードエレメントを含む）が回収され、同一射場で再度打上げられるもの

事故
　人員の負傷、死亡、疾病、システム（ロケット、ペイロード／ＧＳＥ）、関連設備、財産の損傷、環境への悪影響をもたらすような不慮の出来事をいう

事故等
　事故及びヒヤリ・ハット（危うく事故等になりそうになった事象）これらがなくても要員の職業病や環境への有害な影響をもたらす恒常的な事象を含む

射場作業
　鹿児島宇宙センターにおいて実施されるロケット、ペイロード等の整備作業及び設備・装置などの運用作業

システム安全
　プロジェクト等の事業遂行に関する計画立案から整備、運用･実施、撤収に至るシステムのライフサイクルの全段階を通じて、運用効果、スケジュール、及びコストへの配慮の下に安全を最適化し、事故等のリスクを合理的に可能な限り小さくするため、工学及び管理の原理、基準及び手法を用いること

シリーズペイロード
　過去に鹿児島宇宙センターから打上げられたペイロード（ペイロードエレメントを含む）と同一又は類似※の設計の後続機ペイロード。
※過去のハザード解析が適用できるペイロード。すなわち、安全に係る設計が同一ものであり、安全検証結果（製造に係るものを除く）も含めて過去のハザード解析が適用でき、軽微な変更部分についてのみ評価すればよいものである。

人員
　要員及び鹿児島宇宙センター内外の住民及び見学者

ストレイ電圧
　迷走電流の有無を確認するために計測される電圧

セーフアーム装置
　固体ロケットモータの点火等に用いられる火工品の地上での誤作動を防ぐための電気的及び機械的な安全機構を有する装置

地上支援装置（ＧＳＥ）
　ペイロードのハンドリング、試験、点検などに必要な地上装置

テーラリング
　適用対象の諸条件を考慮して、要求事項を取捨選択又は修整して、適用対象に見合った要求書に変更する行為

特別の手順
　設計によっても安全装置、保護装置又は警報装置の設置によってもハザードの制御が不十分な場合、ハザードの発生の可能性を運用で低減できるようにすること。また、要員の教育訓練、適切な作業手順の設定及び必要な保全等によってハザード制御を図ること。

パイロバルブ
　火工品の作動によって開閉状態が切替えられる弁

ハーメティックシール
　部品又は機器等において内部と外部が機械的に隔離され、気体の流通のできない封止

ハザード
　事故をもたらす要因が顕在又は潜在する状態をいう

ハザード解析
　ペイロード／ＧＳＥに係わるハザードを、ライフサイクルのすべてのフェーズに亘って体系的かつ理論的に評価する手法

ハザード概要
　ハザードの内容（source、mechanisum、outcome）を含み、被害の度合いが分かるハザードの概要

ハザード原因
　ハザードが事故に至るための要因発生の原因となるもの（例えば、推薬の漏洩の原因となる容器の強度不足、推薬弁の誤作動、シール不良など）

ハザード制御
　狭義の意味では、故障許容設計、リスク最小化設計の手法を用いて、ハザードの発生の可能性を低減させることをいう。また広義の意味では、このほかに、安全装置、保護装置、警報装置、特別な手順などによる手法を含む。なお、本標準では一般に広義の意味で使用している。

ハザードタイトル
　ハザードの内容（source、mechanisum、outcome）を想像でき、他のハザードと区別できるタイトル

ハザードレポート
　ペイロード／ＧＳＥに係わる個々のハザードに関して、設計担当者、安全担当者及びプロジェクト担当者のリスク評価を受け、ひいては開発実施責任者に残存リスクに対する承認を得るために、ハザード解析で実施された技術情報を文書化したもの

不具合
　機器等に使用される部品、材料又は役務において、１つ以上の特性が規定された要求と合致しない状態。故障、不一致、欠陥及び機能不良を含む

ブルーストンテスト（Bruceton Test）
　火工品の信頼度をUp-and-down method（上下変動法）で試行錯誤的に測定し統計的に求める方法

ペイロード（ロケットペイロード）
　ロケットにより宇宙に打上げられる積荷。本標準では無人の積荷とし、それを構成するサブシステム、機器を含める

PL担当組織
　ペイロード／ＧＳＥの開発、射場作業等を実施する個人、団体、企業、又は機構の組織。打上げ輸送サービス事業により打上げを行う場合は、上記のものに打上げ輸送サービス事業者を含めた組織。

保護装置
　ハザードとして識別した事故から人命等を保護するための物理的バリア等。例えば、モータ等の回転体に対するケーシング、囲いガード等

ポッティング
　電気回路等の一部又は機器内部の全体に対して、他の部分との間に爆発性ガス又は爆発による火炎が移行するのを防止するため、コンパウンドを充填して遮断すること

マイルストーン
　ペイロード／ＧＳＥの開発等の進捗状況、有効性の測定又は達成の管理点として活用するため、プロジェクトのライフサイクル上に予定した重要なイベント

要員
　当該作業に従事する機構及びPL担当組織などの担当者

リスク
　予想される被害の度合いと事故発生の可能性を掛け合わせたもの

4.　システム安全要求

4.1 基本要求事項

　PL担当組織は、ペイロード等の鹿児島宇宙センターへの搬入から射場作業、打上げを経てロケットからペイロードの分離までの安全について以下の要求事項を考慮しシステム安全プログラムを計画し、実行しなければならない。
　本標準における基本的な要求事項は次のとおりである。

(1) システム安全プログラムの遂行にあたっては、安全管理組織を確立すること。
(2) サブシステム、コンポーネント等を含むシステムとしてのハザードを識別、管理し、リスクを最小化すると共に許容レベルにあることを開発の段階で確認すること。
(3) 各ハザードに対して、その原因を把握し、原因毎にハザード制御を設定すること。ただし、ペイロードをロケットに引渡して以降、打上げを経てロケットからペイロードの分離までのロケットとの共同作業期間中においては、ロケットのハザード解析結果に基づいて求められる安全対策を行うこと。
(4) ハザード制御の有効性を試験、検査、解析等により検証すること。
(5) 作業手順書、教育・訓練計画書等に必要なハザード制御を盛り込み、これらの手順書等に基づいて確実に作業を実施すること。
(6) システム安全プログラム計画書(4.2.1項)と安全データパッケージ(4.5項)を維持／管理すること。
(7) 全体プロジェクトのマイルストーンに関連付けて、システム安全プログラムのマイルストーンを設定し、システム安全プログラムの主要な活動であるハザード解析、安全要求の設定、安全審査、管理規定／手順等の制定、報告等の実施時期、作成文書の提出時期を明確にすること。

4.2 システム安全プログラム管理

4.2.1 システム安全プログラム計画書

システム安全プログラム計画書の構成は表4.2.1-1の目次を標準とし、機構の安全審査を受けること。また常に最新化すること。

システム安全プログラム計画書は、参考文書(1) (2)又はこれらと同等の基準に基づいて作成されたものに本標準の要求を盛り込んだものでもよい。また、適用文書(2)の様式を用いることができる。

表4.2.1-1 システム安全プログラム計画書 目次の標準

項目	備考	該当項
1. 総則 1.1 目的		
1.2 適用範囲	鹿児島宇宙センターへの搬入から射場作業、打上げを経てロケットからペイロードの分離まで	1.1 1.2
2. 関連文書 適用文書、参考文書を示すこと。	適用版の指定を記載すること。 テーラリングがある場合、記載すること。（*） JMR-002以外の要求（海外基準等）を適用する場合は識別して記載すること。	1.4等
3. 実施内容 3.1 組織と体制 (1) プロジェクトマネージャ、システム安全プログラム責任者、担当者、関連部門を明示すること。 (2) 関連部門を含めシステム安全管理組織を図示すること。	システム安全プログラム管理に契約相手方が含まれる場合は相手方の体制を含むこと。 公官庁への法定手続きの役割分担も含むこと。	4.2.3
3.2 システム安全審査の方法	統合する審査フェーズ、シリーズペイロード／再飛行ペイロードの安全審査実施があれば記載すること。	4.6

3.3　各開発段階におけるシステム安全業務 (1) 開発段階ごとにハザード解析、安全要求及びシステム安全審査等について規定すること。 (2) システム安全プログラムマイルストーンに上記各業務の実施時期を図示すること。		表4.6-1 図4.2.2-1

＊：テーラリングがある場合は、様式1に記載して示すこと。

4.2.2　システム安全プログラム活動

PL担当組織は、ペイロード等に係る安全を確保し、設計、製造・試験及び運用段階を通じリスクを最小化し、許容レベルにあることを確認するため、ライフサイクルを通じてシステム安全プログラム活動を効果的に実施すること。

なお、図4.2.2-1にライフサイクルにおけるシステム安全プログラム活動を、また以下に各段階におけるシステム安全プログラム活動の概要を示す。

(1) 概念／予備設計段階（フェーズO）
- a. 設計、製造・試験及び運用段階を通したシステム安全プログラム計画書を作成すること。
- b. 概念／予備設計段階においてフェーズOハザード解析を実施し、結果を文書化すること。
- c. 安全要求をテーラリングする場合は、その内容を定めること。

(2) 基本設計段階（フェーズⅠ）
- a. 基本設計段階においてフェーズⅠハザード解析を実施し、結果を文書化すること。
- b. 安全要求に合致できない事項が生じた場合には安全要求に適合するように設計の見直しを行うこと。適合し難い場合には残存リスクが許容できるレベルであることを明確にして安全要求適合性詳細検討書（4.3.1.9項）を作成し、その内容について機構の安全審査で承認を受けること。フェーズⅡ、Ⅲについても同様とする。

(3) 詳細設計段階（フェーズⅡ）
- a. 詳細設計段階においてフェーズⅡハザード解析を実施し、結果を文書化すること。

(4) 製造・試験段階（フェーズⅢ）
- a. 製造・試験段階においてフェーズⅢハザード解析を実施し、結果を文書化すること。

(5) 運用段階（フェーズⅢ以降）
- a. 要すればフェーズⅢハザード解析の結果を見直すこと。
  - ・ ハザードが新たに識別された場合は、必要なフェーズに戻ってハザード解析を行うこと。
  - ・ 設計を変更する場合は、改めて安全要求の識別から実施すること。
  - ・ 手順書を変更する場合は、必要なハザード制御が反映されていることを再確認すること。
- b. 作業の安全を確保するため、システム安全プログラム計画書及び手順書等に基づき作業が行われていることを確認すること。

(6) シリーズペイロード／再飛行ペイロードのシステム安全プログラム活動

PL担当組織は、シリーズペイロードまたは再飛行ペイロードを過去と同一ロケットで打上げる場合について、ハザード解析及び安全審査の効率化を希望する場合、以下を実施すること。
- a. システム安全プログラム計画書にシリーズペイロード／再飛行ペイロードであることの根拠を示すこと。連続する複数機のシリーズペイロードのシステム安全プログラム活動を1つのシステム安全プログラム計画書で管理しても良い。
- b. 標準等適用文書や安全要求に関して、適用する版の新旧相違等による影響評価を行うこと。
- c. 4.3.1.11項に示すハザード解析を実施すること。

4.2.3　システム安全管理組織

システム安全管理組織は、その開発プログラムの内容、規模に応じて開発プロジェクトの組織体制との独立性を勘案して設定すること。

システム安全管理組織の運営に関しては以下によること。

(1) PL担当組織はシステム安全プログラムを計画し実行するため、責任と権限、機能、指示及び報

告等を明確にしたシステム安全管理組織を設定すること。

(2) PL担当組織はペイロード等及び射場作業におけるシステム安全管理に関して責任を持ち、システム安全についての知識、経験を備えたシステム安全プログラム責任者を任命すること。

(3) システム安全プログラム責任者は、以下の権限及び責任を持つものとする。

a. システム安全プログラム責任者の権限に応じて、システム安全プログラム計画書を制定又は作成すること。
b. システム安全プログラムの実行に必要な管理要領を設定すること。
c. 仕様書、手順書等について安全に関する審査を行うこと。
d. ハザード解析及び安全審査を推進すること。
e. 安全データパッケージの維持、管理及び有効利用を図ること。
f. 安全に係る重要な問題点について、関係部門と調整し解決を図ること。
g. ペイロード等の開発の実施責任者に対し、安全に関する報告及び勧告を直接行えること。
h. 安全要求及び安全に係る手順から逸脱するプロジェクト活動及びプロジェクト文書の制定／改訂を阻止及び中止できること。
i. 確立した作業手順から逸脱する安全上クリティカルな運用を中断し、是正できること。
j. システム安全管理に関し、安全・信頼性推進部との窓口となること。

実施年月(西暦) / 開発段階 / システム安全プログラム活動		概念／予備設計（フェーズO）	基本設計（フェーズⅠ）	詳細設計（フェーズⅡ）	製造・試験（フェーズⅢ）	運用	備考
全体マイルストーン	PL担当組織	予備設計審査（DDR）▽	基本設計審査（PDR）▽	詳細設計審査（CDR）▽	認定試験後審査又は出荷前審査（PQR又はPSR）▽		
システム安全プログラム計画書		作成 審査 ▽ ▽	維持/改訂 ▽	維持/改訂 ▽	維持/改訂 ▽	維持/改訂 ▽	
安全審査		ﾌｪｰｽﾞ0安全審査 ▽	ﾌｪｰｽﾞ Ⅰ安全審査 ▽	ﾌｪｰｽﾞ Ⅱ安全審査 ▽	ﾌｪｰｽﾞ Ⅲ安全審査 ▽	ﾌｪｰｽﾞ Ⅲ後の安全審査 ▽（必要に応じ）	
ハザード解析		ﾌｪｰｽﾞ 0ﾊｻﾞｰﾄﾞ解析					
			ﾌｪｰｽﾞ Ⅰﾊｻﾞｰﾄﾞ解析				
				ﾌｪｰｽﾞ Ⅱﾊｻﾞｰﾄﾞ解析	ﾌｪｰｽﾞ Ⅲﾊｻﾞｰﾄﾞ解析		
安 全 要 求		安全要求初期設定 ▽ 安全要求設定 ▽	（必要に応じて）要求の詳細化 見直し ▽ ▽				
作業手順書等					作成 (製造・試験作業手順書、	運用作業手順書等）	

図4.2.2-1　ライフサイクルにおけるシステム安全プログラム活動

4.3 システム安全工学

4.3.1 ハザード解析

PL担当組織は設計段階初期からハザード解析を行い、ハザードを識別するとともにハザード制御方法を設定しそれらを設計、手順、運用等へ反映させること。

4.3.1.1 ハザード解析の対象

(1)対象期間

ハザード解析の対象は鹿児島宇宙センターへの搬入からペイロードをロケットに引渡すまでのペイロード単独射場作業期間中とする。ペイロードをロケットに引渡して以降、打上げを経てロケットからペイロードの分離までのロケットとの共同作業期間中においては、ロケットのハザード解析結果に基づいて設定された安全要求に従うこと。

(2)法令及び機構の安全規程／基準類の扱い

1.2項の通り、法令及び機構の安全規程／基準類の順守のみで安全を確保できる場合（労働安全衛生法に基づく要員の安全確保等）はハザード解析の対象外とする。

4.3.1.2 ハザード識別

対象とするペイロード等について、それらの構成、機能等を十分理解した上で、予想される事故等を想定し、全ての顕在又は潜在するハザード源を抽出した後、ハザード毎に識別し、その結果を様式2に示すハザード識別まとめ表等に記載すること。被害の度合いと発生の可能性は以下を参考に決定すること。

ハザード識別の結果、被害の度合いⅠ、Ⅱのハザードは必ずハザードレポートを作成し、ハザード原因の除去／制御を行い、4.3.1.6項に示す残存リスクの許容可否を評価すること。

被害の度合いⅢ、Ⅳのハザードは通常の設計、製造、運用を実施することで許容可能。ハザードレポートは作成しなくてもよい。ハザードレポート作成の範囲外にあるハザードについては作成範囲外となる根拠をハザード解析表（様式3）等で明確にしておくこと。

a. 被害の度合い(Severity)

被害の度合いは表4.3.1.2-1に示す通り被害の度合いⅠ、Ⅱ、Ⅲ及びⅣで表し、これらは人的過誤、環境条件の厳しさ、設計の不適切、手順の欠陥、システム、サブシステム又はコンポーネント等の欠陥や機能不良等から予想される最悪結果についての判断基準を示すものであること。

表4.3.1.2-1　被害の度合い

被害の度合い	用　語	説　明
Ⅰ	破局 (Catastrophic)	死亡・重度の人的被害 深刻な環境への影響 公共の財またはサービス、第三者財産の喪失や重大な損害 JAXA射場施設・設備等の喪失
Ⅱ	重大 (Critical)	軽度の人的被害 重大な環境への影響 公共の財またはサービス、第三者財産の軽度の損害 JAXA射場施設・設備等の重大な損傷
Ⅲ	限界・局所的 (Marginal)	軽微な人的被害 公共の財またはサービス、第三者財産の軽微な損害 軽度の環境への影響
Ⅳ	無視可能 (Negligible)	Ⅰ～Ⅲをもたらさない程度のもの

b. 発生の可能性

システム、サブシステム又はコンポーネント等の計画されたライフサイクルにおける被害発生の可能性は、それらの作動時間、作動回数、関与する人数、作業回数等の一定の単位に対する潜在発生可能数として表すことができる。

そのほか、発生の可能性を定性的に表すこともでき、その例を表4.3.1.2-2に示す。これらは過去の類似システム等のデータを解析することにより導き出すことができる。

表4.3.1.2-2　発生の可能性

発生の可能性	説　　明
A	しばしば発生する　(Frequent / Likely to occur immediately)
B	たまに発生する　（Probable / Probably will occur in time）
C	まれに発生する　（Occasional / May occur in time）
D	ほとんど発生しない　（Remote / Unlikely to occur）
E	ほとんど全く発生しない　（Improbable / Improbable to occur)

4.3.1.3　ハザードの原因の識別

4.3.1.2項で識別したハザードに対して、対象となるハードウエア、ソフトウエア、運用、人的過誤、インタフェース、環境条件を考慮してハザード原因の抽出を行うこと。なお、参考として、FTA手法だけでなく、FMEAとクロスチェックを行うことも効果的である。

4.3.1.4　ハザード原因の除去／制御

被害の度合いⅠ、Ⅱについては、4.3.1.3項で識別したハザードの原因を除去または制御すること。ハザード原因の除去／制御は以下の安全設計の優先順位に基づき実施すること。

(1) ハザードの除去
(2) ハザードを最小化する設計
(3) ハザードを制御する設計

4.3.1.5　ハザードを制御する設計

4.3.1.4項(3)のペイロード等のハザードを制御する設計においては、基本的に故障許容設計によること。ただし、4.3.1.5.2項により適切に設計し検証データを示すことができる場合は、リスク最小化設計(Design for Minimum Risk)によることができる。

なお、故障許容設計が適用できずリスク最小化設計にもより難い場合は、確率論的なリスク評価によることができる。ただし、この手法をとる場合、PL担当組織は安全審査実施前に安全・信頼性推進部と調整すること。

本文書の5章は、4章のハザード解析を実施する際に適用可能な一般的なハザード制御方法の事例を記載している。ペイロード等は、これらを参考にハザード制御を実施すること。5章でカバーできない場合には、個別にハザード制御を検討すること。

4.3.1.5.1　故障許容設計要求（添付2に解説有り）

事故の被害の度合いに応じて、ハザードを制御し発生の可能性を少なくして許容できるレベルにするため、次の故障許容設計要求を満足すること。

(1)　破局（カタストロフィック）ハザードの制御

２つの故障、２つの人的過誤、又は１つの故障と１つの人的過誤のいかなる組み合わせによっても破局（カタストロフィック）ハザードに至らない設計とすること。

(2)　重大（クリティカル）ハザードの制御

単一の故障又は単一の人的過誤により重大（クリティカル）ハザードに至らない設計とすること。

補足１：本項の実行に当たって、以下を考慮すること。

- ハザードの制御には、エネルギ源との間に必要数の独立したインヒビットを設けるか、インヒビット以外の方法で故障許容設計を成立させること。
- 機器・機能等の１次故障・機能喪失等(人的過誤によるものを含む)が他の故障等を誘発し、事故発生の可能性の増大をもたらさない設計とすること。
- 共通の要因によって同時に複数のハザードの制御を喪失することの無い設計とすること。
- 破局的な事故や重大な事故を防止する安全上重要な冗長系は実現可能な限り互いに離すか保護することにより、予期しない事象により一方に被害があっても他方の機能が損なわれないようにすること。
- ハザードの制御の有効化に手順を要する場合は、その手順を手順書に反映すること。

補足２：本項の実行に当たって、安全を確保するために作動状態を維持する必要がある機能については以下を考慮すること。

- 安全な状態を維持できなくなるだけでなく、新たなハザードを生じることを防ぐこと。
- 電源供給等の途絶に対し、安全化対応ができるまで安全が維持できること。

補足３：故障許容設計はフライト品やGSEの設計の一部として達成されることを基本とするが、以下の優先順位で(1)から(4)の方法を用いても良い。各定義については用語の定義を参照。

(1) 安全装置の使用
(2) 保護装置の使用
(3) 警報装置の使用
(4) 特別の手順によるハザード制御

4.3.1.5.2 リスク最小化設計

機構等が設定した設計基準等(添付１)に基づき適切に設計したことを検証データをもって示すことができる場合、リスク最小化設計とすることができる。十分な設計マージン、安全係数、適切な材料及び部品の選定等によって設計を管理すること。機構等が設定した設計基準等以外を根拠とする場合は安全審査実施前に安全・信頼性推進部と調整すること。リスク最小化設計が適用される分野としては、下記が挙げられる。

- 構造体　• 圧力容器　• 圧力配管及び継ぎ手　• 火工品　• 材料適合性
- 材料可燃性　• 一部のメカニズム（機構品）

4.3.1.6 残存リスク評価

被害の度合いⅠ、Ⅱについては、ハザード原因の除去／制御を実施した結果として、残存するリスクの評価を行い、その許容可否判定を図4.3.1.6-1に基づいて行うこと。被害の度合いⅠについては発生の可能性E、ⅡについてはDまたはEに低減されたことをもって許容可能とする。

PL担当組織が同等の基準を提案する場合は安全審査実施前に安全・信頼性推進部と協議し、合意がなされた場合は、それをもってリスク許容判定基準とすることができる。

なお、残存リスクは単にリスク許容判定基準内に収まっていれば良いとするものではなく、制約条件の下で最大限の努力をして、その低減に努めること。

		発生の可能性				
		A	B	C	D	E
被害の度合い	Ⅰ					
	Ⅱ					
	Ⅲ					
	Ⅳ					

：ハザードレポート作成の範囲
：許容できない　：許容可否判断要（注）　：許容可能

注)①許容可否判断要についてはリスクの低減に最大限の努力を払った場合許容の可能性あり。
②発生の可能性のレベルは、ハザードの制御がなされた後のものであること。

図4.3.1.6-1　リスク許容判定基準

4.3.1.7　安全検証

4.3.1.5項で検討したハザードの原因の制御方法の有効性を安全検証で確認すること。検証とは試験、検査、解析、デモンストレーション及びこれらの組み合わせにより、ペイロード等のハードウエア又はソフトウエアがすべての安全設計要求を満足していることを客観的証拠で確認することである。

検証手段として手順／工程管理を用いる場合は手順書に、解析／試験／検査を用いる場合は報告書にまとめ、ハザードレポートに文書番号等を示すこと。

シリーズペイロード／再飛行ペイロードのハザード解析では、参照対象となった以前の検証手順、検証要求を調査してその類似性を十分に評価すること。

なお、フェーズⅢ終了時に未了であってその検証が射場作業に持ち越される安全検証の未処理事項は、安全検証追跡ログ（SVTL）（様式4）に記録して追跡管理すること。さらに、予め処置の完了日及び提出日定め、定められた期日までに処置した結果を安全・信頼性推進部に提出すること。ハザード制御の有効性が打上げコンフィギュレーションに依存する場合には、打上げコンフィギュレーション設定が適切に行われたことをSVTLで確認する。

検証に係るすべてのデータは常に利用できるよう管理すること。

また、検証を行った後はその結果を報告し、不具合が発見されたときには検証後の処理として是正措置をとる等のフィードバックを行うこと。

4.3.1.8　ハザードレポート

(1) 4.3.1.2項のハザード識別の結果、ハザードレポート作成の範囲であった場合、ハザードレポートを作成すること。
(2) サブシステム、コンポーネント毎に個別でハザードレポートを作成した場合、システムとして評価した場合もそのハザードレポートが有効であることを示すこと。
(3) ハザードレポートでは、適用される安全要求（本標準5章及びその他追加の要求）、ハザードの分類、ハザードの概要、ハザード原因、ハザード制御方法、安全検証方法についての解析を行い、安全検証ステータスを示すこと。
(4) ハザードレポートにはハザード制御方法、安全検証方法、安全検証結果の概要についての補足説明資料を添付すること。
(5) ハザードレポートの様式は以下による。
- 適用文書(2)の様式に示されるハザード制御・安全検証を適用可能なハザードは、当該様式を用いることができる。

・ 上記に該当しないハザードは様式5等を用いてレポートを作成する。

(6) ハザードレポートは、ハザードが設計によって除去されるか制御手段が検証され、最大限の努力の上、リスク許容判定基準を満足し、全ての安全検証の完了（クローズ）が確認された時点において完了する。

4.3.1.9 安全要求適合性詳細検討書(NCR)

PL担当組織はペイロード等がハザードレポートにて適用した要求事項に合致できない場合には安全・信頼性推進部と協議の上、安全要求適合性について詳細に検討し、安全要求適合性詳細検討書（様式6）にその検討内容を示し、機構の安全審査で承認を受けること。

安全要求適合性詳細検討書はハザードレポートから呼び出すこと。

4 3.1.10 各フェーズにおけるハザード解析

ハザード解析は安全審査のフェーズに対応して、以下に示すフェーズ0～Ⅲの各段階において実施すること。なお、設計変更等が生じた場合、ハザード解析を見直すこと。

(1) フェーズ0ハザード解析（概念／予備設計段階）

フェーズ0ハザード解析は概念／予備設計段階において実施し、本標準の5章を参考にハザード及びハザード原因を識別したうえで対応策の検討を行うこと。5章に加えて他設計標準等の要求を引用する必要がある場合はそれらについても識別すること。これらの結果は、ハザード識別まとめ表（様式2）、ハザード解析表（様式3）に纏めること。その内容は次のとおりである。

a. システムの運用において考えられるハザードを有する部位、場所を明らかにすること。
b. 使用予定材料、部品等で特にハザードを有する物質を識別すること。
c. 試験、運搬、取扱い、運用等で考えられるハザードを明確にすること。
d. インタフェースに関する安全上の問題を明確にすること。
e. ハザードに対して予想される事故等の程度を明らかにし、ハザードの原因、その対応策を設定し、ハザード解析表に記載すること。

(2) フェーズⅠハザード解析（基本設計段階）

フェーズⅠハザード解析は基本設計段階においてフェーズ0ハザード解析で識別したハザードに基づき、より詳細にハザード解析を行い、ハザードの識別、影響の及ぶ範囲、対応策を明らかにするとともに設定すること。

また、4.3.1.2項でハザードレポート作成範囲に該当すると分類された範囲のハザードについてはハザードレポートを作成し、フェーズの進展に伴って見直すこと。その内容は次のとおりである。

a. ハザード原因の識別をするとともに、ハザードの除去策又は制御策が適切に設定されていること。
b. システム、サブシステム等の接続についてはインタフェースに関係するハザード解析を実施するとともに、設計の改善と安全について必要なトレードオフを行い最適条件を定めること。なお、ハザード解析においてはサブシステム、コンポーネントのハザードを考慮し、システムとしてのハザードレポートとすること。
c. 破局／重大ハザードについてはFTA (Fault Tree Analysis) を行うこと。FMEA (Failure Mode and Effects Analysis)と相互チェックを行い、漏れを防ぐことも効果的である。
d. 解析結果に基づき、安全に関係する設計上の制約条件等について考慮しつつ、必要な改善策を設計に反映させること。
e. 安全の改善、是正は適正な方法で実施できるよう明確にしておくこと。

(3) フェーズⅡハザード解析（詳細設計段階）

フェーズⅡハザード解析は詳細設計段階において、フェーズⅠハザード解析の結果を設計の進展に伴って見直すことにより安全の詳細評価を行うもので、その内容は次のとおりである。

a. ハザードの除去、制御に関する処置内容がハザードレポートに明確に記載され、設計上実現されていること。
b. 必要に応じてFTAの結果を見直すこと。
c. 安全上クリティカルな部品や材料等について事故発生頻度を低下させるべき適正な手段を選定すること。
d. 安全上クリティカルとなる技術、設計、製造、試験、運用等、及びそれらが影響する範囲についてハザードレポートに明文化し、安全の維持、改善に反映させること。
e. 検証手段をハザードレポートに明示すること。

(4) フェーズⅢハザード解析（製造・試験段階）

フェーズⅢハザード解析は製造・試験段階において、フェーズⅡハザード解析の結果を見直すことにより運用に関する安全の詳細評価を行うもので、その内容は次のとおりである。

a. 運用上のハザードの除去、制御に関する処置内容を明確にし、ハザードレポートに明文化すること。
b. 安全上クリティカルな運用手順等についてハザードの発生頻度を低下させるべき適正な方法を選定すること。
c. 安全上クリティカルとなる運用及びそれらが影響する範囲についてハザードレポートに明文化し、安全の維持、改善に反映させること。
d. ハザード制御の検証結果をハザードレポートに明確化し、全ての安全検証が終了したことを確認すること。なお、ハザードの安全検証の完了を射場のみでしか確認できないものは、安全検証追跡ログ（様式4、または同等な様式）に記載してフォローして個々に運用前にクローズすること。

4.3.1.11 シリーズペイロード／再飛行ペイロードのハザード解析

シリーズペイロード／再飛行ペイロードのハザード解析は、ベースラインとなるペイロードのハザード解析と比較して安全評価を行うもので、その内容は次のとおりである。

(1) ベースラインとなるペイロードに対して、設計変更（部品やソフトウエアを含む）及び運用条件や手順の変更を全て識別し、シリーズペイロード／再飛行ペイロードのハザード解析への影響を評価すること。
(2) ベースラインとなるペイロードにおける全ての異常・不具合に対し、シリーズペイロード／再飛行ペイロードのハザード解析への影響を評価すること。安全上クリティカルなシステムに関連する異常・不具合は是正すること。
(3) 新たに製作したハードウエアに対する試験・検査等を実施し、過去に設定されたハザード制御の有効性を再検証すること。これは、新たな運用シナリオを考慮した環境条件等に基づくものであり、必要であれば、過去の解析検証事項に対する見直しも含む。
(4) ベースラインとなるペイロードの安全要求不適合事項は、その受入れ根拠を再確認し、必要であれば是正すること。
(5) 再飛行ペイロードについては、有効寿命品目の評価、保全、構造検査、改修の安全への影響の評価を実施すること。

4.4 ロケットのハザード解析結果に基づいて求められる安全対策に対する適合性評価

ペイロードをロケットに引渡して以降、打上げを経てロケットからペイロードの分離までのロケットとの共同作業期間中においては、ロケットがペイロード起因のハザード原因を識別し、ロケットか

らペイロード側に提示する。PL担当組織は以下を実施すること。

(1) 提示されたハザード原因を発生させないためのハザード制御方法を実施すること。
(2) 実施したハザード制御方法の有効性を安全検証で確認すること。
(3) ロケットのハザード解析結果に基づいて求められる安全対策に対する適合性評価結果をロケットから提示される所定のフォーマットに記入すること。
(4) ロケットから示されたハザード原因以外のハザード原因がある場合は、別途ロケット側がハザード解析を実施する必要があるため、ロケット側と調整を実施した後に、これに対する処置について安全審査実施前に安全・信頼性推進部と調整すること。

4.5 安全データパッケージ

ハザード解析結果は安全データパッケージに取り纏め、4.6項に示す安全審査の審査資料とすること。安全データパッケージの構成は表4.5-1を標準とする。

表4.5-1 安全データパッケージ 目次の標準

項目	備考	該当項
1. 総則 1.1. 目的		
1.2. 適用範囲		4.3.1.1 4.3.1.2
2. 関連文書	適用文書、参考文書を示すこと。	
3. ペイロード等の説明 3.1. ペイロード等の基本情報	主要諸元、ペイロード外観図（打上げ時、軌道上コンフィギュレーション）	
3.2. ペイロード等の設計及び機能の概要	4項のハザード解析を理解するのに必要な情報（システム構成ブロック図等）を最低限記載する。 ハザード制御に用いる機能等の詳細はハザードレポートの添付に示すこと。	
3.3. 射場作業フロー及び各作業の内容	4項のハザード解析を理解するのに必要な情報を最低限記載する。 ハザード制御を要する作業を識別すること。	
4. ハザード解析結果		4.3.1
4.1. ハザード識別まとめ表		4.3.1.2
4.2. ハザード解析表		4.3.1.2
4.3. FTA等	破局/重大ハザードがある場合のみ	4.3.1.3 4.3.1.10
4.4. ハザードレポート	破局/重大ハザードがある場合のみ。 ハザード制御に用いる機能等の詳細(インヒビット等が示されたスケマティック及びブロック図)を添付に示すこと。	4.3.1.8
4.5. ロケットから求められるハザード制御に対する適合性評価	フェーズⅡ、Ⅲのみ	4.4
4.6. 安全検証追跡ログ(SVTL)	フェーズⅢにてログへ移管する検証項目がある場合のみ	4.3.1.7 4.3.1.10

4.7.　安全要求適合性詳細検討書(NCR)	要求不適合がある場合のみ ハザードレポートから呼び出すこと。	4.3.1.9

4.6　システム安全審査

PL担当組織は4.2.2項に要求する活動が確実に実施され、設計に適切に反映され、かつ必要な安全データが整備されていることを確認するため、機構のシステム安全審査を受審すること。安全審査プロセスの概要を表4.6-1に示す。

機構のシステム安全審査の目的は、機構の施設設備の大きな損害と規制エリアに存在する直接の作業者以外の被害を防ぐことである。この目的を達成するために以下を評価する。なお、PL担当組織の要員の労働安全については、1.2項に示す通り、機構のシステム安全審査の対象外としている。

- 鹿児島宇宙センターへの搬入からペイロードをロケットに引渡すまでのペイロード単独作業期間中にペイロード等に関係して識別されたハザードに応じて設定された安全要求、及びそれに対する適合性を確認するとともに、ハザード及びハザード原因の識別、制御、その検証方法、更には検証結果の妥当性及び除去しきれないリスク（残存リスク）最小化の内容や許容性を評価する。
- ペイロードをロケットに引渡して以降、打上げを経てロケットからペイロードの分離までのロケットとの共同作業期間中において、ロケットのハザード解析結果に基づいて求められる安全対策への適合性を評価する。

(1) 機構が開発するペイロード等については各開発段階毎に、フェーズ0、及びフェーズⅠ～Ⅲ安全審査の４回の審査を受審することを基本とするが、システムの規模や国外での実績等開発上のリスクが十分小さいとPL担当組織が判断した場合は、各フェーズ安全審査を統合して実施することができる。統合の方法はフェーズ0／Ⅰ、Ⅱ、Ⅲの3回、フェーズ0／Ⅰ／Ⅱ、Ⅲの2回、フェーズ0／Ⅰ／Ⅱ／Ⅲの1回が想定される。また、各フェーズ安全審査は、機構と調整のうえ全体マイルストーン審査に含め実施することができる。

(2) 機構のシステム安全審査は、参考文書(3)に基づき実施される。安全審査の概要として各安全審査の実施時期、審査の主目的、審査文書を表4.6-1に示す。

(3) 表4.6-1に基づいて、システム安全プログラム計画書と安全データパッケージを、安全審査実施前の所定の期日までに安全・信頼性推進部へ提出すること。

(4) ロケットのハザード解析結果に基づいて求められる安全対策への適合性は、PL担当組織がロケット側安全審査の中で評価を受けるか、もしくは本安全審査の中で評価を受けること。

(5) フェーズⅢ安全審査にかけた内容の変更や追加事項等が発生した場合は、安全・信頼性推進部と協議し、必要に応じてフェーズⅢ後の安全審査を実施すること。

表4.6-1　各開発段階における安全審査の概要

安全審査	審査実施時期	審査の主目的	審査文書
フェーズ0 安全審査	概念／予備設計 完了時	a. ハザードとその原因の識別の確認 b. 適用する安全要求の確認（テーラリング、ハザード解析による追加要求がある場合はそれを含む）	a. システム安全プログラム計画書 b. 安全データパッケージ
フェーズⅠ 安全審査	基本設計審査時 （PDR 時）	a. ハザードとその原因の識別の確認 b. ハザード制御方法、ハザード検証方法の確認 c. 必要に応じて詳細化された安全要求の確認	a. システム安全プログラム計画書 b. 安全データパッケージ
フェーズⅡ 安全審査	詳細設計審査時 （CDR 時）	a. ハザードの制御方法の設計への反映結果の確認 b. 詳細な検証方法の設定の確認 c. ロケットから求められるハザード制御に対する適合性の確認	a. システム安全プログラム計画書 b. 安全データパッケージ（識別された安全上の特徴、故障許容性等が示されたスケマティック及びブロック図を含むこと。特に電気スケマティックについては、要求される数の故障許容性及びその制御の必要な数、及びそれらが互いに独立であることが明確に識別出来なければならない。）
フェーズⅢ 安全審査	開発完了審査時	鹿児島宇宙センターにおいて、ハザード源を有する射場作業を開始してよいことを決定するために以下を確認する。 a. ハザードの検証完了の確認 b. ロケットから求められるハザード制御に対する適合性の確認（検証） c. 射場でしか確認できないため未了となった検証については、安全検証追跡ログへの移行の妥当性確認 d. 全アクションアイテムクローズの確認	a. システム安全プログラム計画書 b. 安全データパッケージ（ペイロード等の製作、試験及び検査において発生した不具合等の内、安全に影響を与えると判断される不具合等のサマリ及びそれらの安全評価を含むこと）
シリーズペイロード／再飛行ペイロードの安全審査	詳細設計審査時 （CDR 時） または、開発完了審査時	a. 設計変更、射場/打上げ運用、並びに射場/打上げの不具合のいずれかがベースラインとなるハザード解析の各フェーズに影響を及ぼすか否かの確認 b. 影響を及ぼすフェーズについて差分（Δ）のハザード解析実施結果の確認	a. システム安全プログラム計画書 b. 安全データパッケージ ・ パッケージ各項目のベースラインペイロードに対する変更点とその影響評価を含むこと。 ・ ベースラインペイロードのハザードレポートの安全検証項目のうち、再検証する項目、及び新たに検証が必要となった項目を識別すること。 ・ （再飛行ペイロードのみ）有効寿命品目の評価、保全、構造検査、改修の安全への影響の評価を含むこと。

注１）シリーズペイロード／再飛行ペイロードの安全審査は、設計変更点を含んでフェーズΔⅡ／Ⅲの１回の審査が通常想定される。（ハザードの識別が変更される場合はフェーズΔⅠの実施も必要である。）

5. ハザード解析のガイドライン

本章の5.1項～5.8項は過去のペイロードの安全審査で実績のある典型的なハザード解析を示す。これらを考慮して、4章のハザード解析を実施すること。なお、本章以外の方法でのハザード解析を妨げるものではない。ハザード解析は、本章の内容に限らず網羅的に実施し、識別された各ハザードに対して安全対策を検討すること。特に、バイオハザードを引き起こす病原菌等、電離放射線源、極低温流体については個別でハザード解析を検討すること。

5.1 射場における火災・爆発ハザードの防止（添付2に解説有り）

射場において、

A) 可燃性推進薬の漏洩や、露出した固体推進薬／火工品の存在によってJERG-1-007に定義される爆発性危険雰囲気が形成された状態でペイロードやGSEの点火源が発火することで、火災・爆発ハザードが発生する。

B) 可燃性推進薬と酸化剤の混合により火災・爆発ハザードが発生する。

C) JIS C 6802(IEC 60825-1)クラス4レーザが着火源となり火災ハザードが発生する。

火災・爆発は人員の死傷や射場施設設備の喪失につながるため、このハザードは通常、破局ハザードとみなされる。このハザードを防ぐために適切なハザード制御を実施すること。以下が典型的な対策である。A）については本項(2)(3)により、B）については本項(4)により、C）については本項(5)により防止する。

(1) 本ハザードに対するハザード解析として、ペイロード及びGSEにおいて、ハザード制御が必要な可燃性推進薬および露出した固体推進薬／火工品、酸化剤、点火源をそれぞれ識別する。

(2) 爆発性危険雰囲気に持ち込まれる、ペイロード及びGSEが通常の使用（故障を考慮する必要は無い）において点火源とならない設計又は運用を行う。以下は典型的な対策である。

   a. 爆発性危険雰囲気で通電するペイロードの電気機器に対して、通常の使用では点火源とならないようポッティング、ハーメティックシール、不活性ガスによる加圧などの必要な防爆対策を行う。対象とする電気機器の電気容量が十分小さく、対象爆発性ガスの点火限界以下で点火源となり得ないものも有効な防爆対策である。また、防爆対策が行われていない電気機器は通電しない。

   b. 爆発性危険雰囲気で通電するGSEの電気機器は、国内法規「電気機械器具防爆構造規格」またはIEC 60079におけるガス蒸気防爆構造とする。非防爆機器を爆発性危険雰囲気に持ち込む場合は、JERG-1-007に従った対応を行う。

   c. ペイロード及びGSEに、人が触れる部分に露出した通電部が無い設計とする。プラズマスラスタ等、露出した通電部がある場合、爆発性危険雰囲気において当該部分を通電しない。

   d. 爆発性危険雰囲気において露出した電熱線等を通電しない。

   e. 爆発性危険雰囲気において火工品、固体推進薬を着火しない。

   f. 爆発性危険雰囲気においてペイロード及びGSEをボンディングや接地することにより静電気の発生を防止する。

   g. 爆発性危険雰囲気に持ち込まれるペイロード及びGSEについては、可燃性推進薬と接触する可能性のある箇所に不燃性の材料を使用する。また、当該箇所における錆の発生を防止する。

(3) 可燃性推進薬の漏洩は、5.4項(2)～(7)により防止する。漏洩に対して2故障許容設計がなされる場合、漏洩した可燃性推進薬と点火源との接触に関して故障を考慮する必要は無く、通常の使用において点火源にならなければ良い。漏洩した可燃性推進薬と点火源との接触を防ぐための処置を別途とる等の場合には、5.4項(2)の2故障許容は1故障許容に読み替える。

(4) 可燃性推進薬と酸化剤の混合に対して2故障許容設計とする。（隔壁、バルブ等により遮断）また、充填時の誤操作により混合しない設計とする。（異なる配管径の使用、ポート接続場所を異なる位置・位相に配置する等）

(5) クラス4レーザについてはJIS C 6802(IEC 60825-1)に従った設計・運用を行う。

5.2 射場における圧力システム破裂ハザードの防止

射場において、ペイロードやGSEの圧力システムの破裂ハザードは人員の死傷や射場施設設備の喪失につながるため、このハザードは通常、破局ハザードとみなされる。このハザードを防ぐために適切なハザード制御を実施すること。以下が典型的な対策である。

(1) 本ハザードに対するハザード解析として、ペイロード及びGSEにおいて、ハザード制御が必要な圧カシステムを識別する。
(2) 圧カシステムについてはJERG-0-001や高圧ガス保安法に則ったリスク最小化設計を行う。また、下記についても考慮する。
    a. ヒータ等の故障によるワースト熱環境における圧力上昇や低圧側へのリーク（バルブ等の2故障までカウント）した場合を想定した耐圧設計とする。
    b. 手動弁の誤操作等の誤った運用手順設定による過加圧に対して2故障許容設計とする。故障許容設計として圧カリリーフ装置を用いる場合、装置の上流をバルブ等で無効にしない。
(3) 射場で圧力システムの加圧作業を実施する場合、JERG-1-007に従った作業を行う。

5.3 射場におけるリチウムイオンバッテリ破裂ハザードの防止（添付2に解説有り）

射場において、ペイロードやGSEのリチウムイオンバッテリの破裂ハザードは人員の死傷や射場施設設備の喪失につながるため、このハザードは通常、破局ハザードとみなされる。このハザードを防ぐために適切なハザード制御を実施すること。以下が典型的な対策である。

なお、組電池として100Wh以下のリチウムイオンバッテリの爆発性危険雰囲気以外での破裂は破局ハザードや重大ハザードとみなされないが、爆発性危険雰囲気における破裂は破局ハザードとみなされる。また、Ni-MHバッテリはそのエネルギ密度が小さいことから、破裂が破局ハザードや重大ハザードとみなされない。

(1) 本ハザードに対するハザード解析として、ペイロード及びGSEにおいて、ハザード制御が必要なリチウムイオンバッテリを識別する。
(2) バッテリについては以下に示すような原因により破裂しない設計とする。
    a. セル内部の短絡
    b. セル外部の短絡
    c. 過充電
    d. 熱制御系の故障に起因する異常な温度環境での使用

5.4 射場における毒性物質漏洩ハザードの防止

射場において、推進薬や酸化剤等の毒性物質（ヒドラジン、MMH、MON3、NTO等）の漏洩ハザードは有毒ガス吸引等による人員の死傷や毒性物質による射場施設設備の汚染につながるため、このハザードは通常、破局ハザードとみなされる。このハザードを防ぐために適切なハザード制御を実施すること。以下が典型的な対策である。

なお、上記以外の推進薬や酸化剤等についての毒性の被害の度合いは個別に検討すること。

(1) 本ハザードに対するハザード解析として、ペイロード及びGSE（充填後の後処置含む）において、ハザード制御が必要な毒性物質を識別する。
(2) 毒性物質が存在するタンク等から、システム外に漏洩する可能性がある経路を全て識別し、以下のように各経路に対して漏洩を防止する。
    a. 毒性物質の漏洩経路を遮断するバルブ等の解放操作に対して以下を考慮した2故障許容設計とする。
        I. バルブ等の流出経路（リークパス）に対して2故障許容設計とする。なお、「バルブ内に2つ以上のシールを有するバルブ」や「パイロバルブ等」は1故障許容相当とみなせる。
        II. 故障許容設計に関連する上記バルブ等を操作する電気的制御については、独立した3つの信号により開となる設計とする。
        III. 射場作業のフェーズによって漏洩防止に対する制御手段が異なる場合は、各フェーズにおける2故障許容設計を示す。
    b. 毒性物質の注排弁等からの漏洩に対して3つのシールによる2故障許容設計、または金属シールによるリスク最小化設計とする。
(3) 射場で毒性物質の充填作業を実施する場合、JERG-1-007に従った作業を行う。
(4) 毒性物質を搭載するタンク等（推進薬によって汚染される可能性のある加圧ガス用流路含む）に流体適合性がある材質を用いる。

(5) バルブ等に異物の噛み込み防止のため、清浄度管理された流体を使用する。
(6) 毒性物質を搭載したタンク等について吊り作業（推進薬充填後の衛星吊り作業も含む）を行う場合は、吊具、吊り点について適切なマージンがある設計とする。「労働安全衛生法　クレーン等安全規則」にて吊り具に対する最小安全係数はワイヤロープに対しては6、それ以外に対しては5が要求される。
(7) 圧力システムとしての設計は5.2項を満足する。

5.5　射場における電波誤放射ハザードの防止（添付2に解説有り）

射場において、所定の強度を超える電波の誤放射ハザードは人員の傷害につながる。このハザードの被害の度合いは以下により決定する。

ステップ1 （限定・局所的ハザードの判定）

以下A)～C)のいずれかを満足する場合、限定・局所的ハザードとみなす。

A) 電波放射源の周波数：6GHz 未満かつ、電波放射源の空中線電力：20 W 以下である。（PL担当組織以外の人員が電波放射源の10cm以内に近づかないという前提）
B) 「安全距離算出に使用する基準」(1)の基準に基づき、安全距離(電磁界強度指針以下の電磁界強度となる範囲)を求め、以下a.b.のいずれかを満足する場合。（デューティを考慮した安全距離の算出をしてもよい。また、意図せぬ放射も条件に考慮して、適切な反射係数を使用する。）
   a. 射場作業シナリオ、機器のコンフィギュレーション等により、安全距離以内にPL担当組織以外の人員が物理的にアクセスしえない
   b. 安全距離が1.4m 以内、かつPL担当組織以外の人員の安全距離以内へのアクセスが偶発的な場合のみである
C) 「安全距離算出に使用する基準」(2), (3), (4)の順に安全距離を算出し、求められた安全距離以内に人員が物理的にアクセスしえない

「安全距離算出に使用する基準」

(1) 「電波防護指針 表2:一般環境(条件G)における電磁界強度（平均時間6分間）の指針値」
(2) 「電波防護指針 表1:管理環境(条件P)における電磁界強度（平均時間6 分間）の指針値」
(3) 「電波防護指針 II.補助指針 (1)人体が電磁界に不均一又は局所的にさらされる場合の指針」
(4) 人体が電磁界に不均一または局所的にされられる場合は、本指針に基づき評価する。
(5) 「電波防護指針 表5 基礎指針」

ステップ2（重大ハザード/破局ハザードの判定）

ステップ1で限定・局所的ハザードと判定されない場合、人体が6分間に平均して200W以上の照射を受ける場合は破局ハザード、それ以下であれば重大ハザードとみなす。

また、ハザードを防ぐために適切なハザード制御を実施する。以下が典型的な対策である。

(1) 本ハザードに対するハザード解析として、ペイロード及びGSEにおいて、ハザード制御が必要な電波放射源を識別する。
(2) 射場での各フェーズにおける電波の誤放射に対して必要な数の故障許容設計とする。
(3) 射場で意図的に放射する場合、求められた安全距離への立ち入り規制等による運用制約を設定する。

5.6　射場における火工品誤着火ハザードの防止

射場において、太陽電池パドル等の保持解放機構に用いられている火工品の誤着火については射場においては破局ハザードや重大ハザードとみなされないことが通常である。（ロケット搭載状態での火工品の誤着火については別途ロケットの指示に従って対応する。）

仮に、火工品の誤着火ハザードが人員の死傷や射場施設設備の破損につながり、破局または重大ハザードとみなされる場合、このハザードを防ぐために適切なハザード制御を実施すること。以下が典型的な対策である。

(1) 本ハザードに対するハザード解析として、ペイロード及びGSEにおいて、ハザード制御が必要な火工品を識別する。
(2) 射場での各フェーズにおける火工品の誤着火に対して必要な数の故障許容設計とする。
   a. 破局ハザードに対しては、エネルギ源との間に最小限３つの独立したインヒビットを持つ設計とする。なお、グランドリターン回路は上記インヒビットの内の１つにより制御することが望ましい。３つのインヒビットの内、少なくとも2つはモニタが出来る設計とする。
   b. 重大ハザードに対しては、エネルギ源との間に最小限2つの独立したインヒビットを持つ設計とする。
(3) 電気起爆装置(EED)について、外部シャントなしで1A DC,1W DCをそれぞれ5分間通電あるいは負荷したとき、発火又は機能不良にならないことをブルーストンテスト(Bruceton test)又は同等の統計的試験方法により信頼水準95%において発火レベルが0.1%であることで確認する。もしくは、NASA Standard Initiator等、規格に基づいたものを使用する。
(4) EEDについて、ロケット側のインタフェース条件（射場を含む）、及びペイロード等の予測される全てのRF周波数スペクトラムに対して電源及び負荷側のインピーダンスにかかわらず、火工品の最大不着火電力の少なくとも20dB以上の減衰を与えるシールドを設ける。EEDがコネクタに結線されるまで、シールドキャップを取り付けておく。火工品の最大不着火電力は、RFの周波数、電波の形式によって異なるので、射場におけるRF環境を考慮した評価を行う。
(5) EEDを使用する場合、火工品の結線を行う前に火工品点火回路のストレイ電圧チェックを行い、火工品の最大不着火電流の1/10又は50mAのいずれか低い値以上の電流を生じないことを確認する。

なお、固体ロケットモータ及び固体ロケットモータに使用する火工品については、特にリスクの高いアイテムであり、典型的には以下の対策をとる。
(6) 固体ロケットモータの着火に使用する火工品について、5.6項(2)-(5)までの対応をとる。ただし、(2)については、３つの独立したインヒビットのうちの１つを電気的及び機械的な安全機構を有するセーフアーム装置とする。なお固体ロケットモータの着火にEED以外（レーザ着火起爆装置等）を用いる場合は、セーフアーム装置の使用について、個別に検討を実施する。
(7) 固体ロケットモータ本体について、取り扱い環境（摩擦、振動、衝撃、人の静電気、EMC、温度、湿度等）で物理的化学的に耐性のある設計とする。
(8) 固体ロケットモータ本体について、ボンディングや接地により静電気を防止する。

5.7 PL担当組織の要員の安全確保に係るハザードの位置づけ

射場において、PL担当組織の要員の安全確保に係るハザードとしては、一般的に以下が想定される。これらについては通常、PL担当組織の要員以外の人員及び射場施設設備に対する被害の度合いとしては限定・局所的ハザード以下とみなされるため、本標準におけるハザード制御は求められないが、PL担当組織自らの責任において対応すること。

(1) 感電
(2) 高所作業中の転落
(3) 重量物運搬中の重量物の落下
(4) 酸欠
(5) 騒音による負傷
(6) 高温、低温表面による負傷
(7) JIS C 6802(IEC 60825-1)クラス4以下レーザ使用による負傷（爆発性危険雰囲気における点火源としてを除く）
(8) 鋭利な端部、角、突起物による負傷
(9) 可動機構（太陽電池パドルや可動アンテナ等）の意図しない動作による受傷

6. ハザード解析によらない固有の安全設計要求（添付2に解説有り）

本章は4章のハザード解析とは無関係に要求される固有の安全設計要求であり、個別に適合性評価結果を提出すること。

(1) ペイロードからの推進薬や酸化剤等（ヒドラジン、MMH、MON3、NTO等）の漏洩時等の異常時に備えて、圧力システムを安全に減圧するとともに、推進薬や酸化剤等を安全に排出できるようにペイロード、GSEを設計すること。

添付１　リスク最小化設計を適用可能な条件となる設計基準等

以下に示す機構等が設定した設計基準等に基づき適切に設計したことを検証データをもって示すことができる場合リスク最小化設計とすることができる。文書は適用時の最新版を用いること。

（１）構造体
- ■JERG-2-320 構造設計標準
- ■各ロケットのユーザーズマニュアル

（２）圧力容器、圧力配管等
- ■JERG-0-001 宇宙用高圧ガス機器技術基準
- ■高圧ガス保安法

（３）火工品
- ■JMR-002 ロケットペイロード安全標準 5.6 射場における火工品誤着火ハザードの防止

（４）一部のメカニズム(機構品)
- ■CZA-2018029　ロケットペイロード システム安全プログラム計画書/安全データパッケージテンプレート

（５）爆発性危険雰囲気
- ■JMR-002 ロケットペイロード安全標準　5.1 射場における火災・爆発ハザードの防止　補足
- ■「電気機械器具防爆構造規格」
- ■IEC 60079 Series
- ■JERG-1-007射場運用安全技術基準

（６）電気系
- ■JERG-2-213 絶縁設計標準
- ■JMR-002 ロケットペイロード安全標準 5.3 射場におけるリチウムイオンバッテリ破裂ハザードの防止

（７）その他、その内容が妥当であり受け入れ可能なリスクまで低減できることが確認できる基準

添付２　各項目の解説

4.3.1.5.1　故障許容設計要求　解説その1

１．目的

4.3.1.5.1　故障許容設計要求に関して、その制御系の独立性に対する解釈を明確にする。
なお、本解釈の通りではない他の方法で安全を確保することを妨げるものではない。

＜背景＞

複数のインヒビットを、計算機を用いた制御系（以下、「CBCS」（Computer-Based Control System）と言う）によって制御する場合、それらは独立なインヒビットであるとは必ずしも言えない。しかし、現在、CBCSにより複数のインヒビットを制御する事例が多くあり、システム安全審査部会で頻繁に議論になった。そこではCBCSの設計を評価することにより、各インヒビットの制御に一定の独立性があることが確認できれば、独立したインヒビットによるものと実効的に同等と見なし、故障許容設計相当として評価してきた。これら個々の評価を明確化する必要があった。

＜定義＞

CBCSとは、定められた仕事を遂行するために、入力情報を受け取り、その情報を処理して出力を与える計算機のハードウェア、ソフトウェアおよびファームウェアを利用する制御システムのことである。
ここではCBCSによる制御を、(1) インヒビット解除コマンド、(2) コマンド発行機器、(3) コマンド中継機器、及び、(4) コマンド実行機器から構成されるもの（図１参照）と定義し、各機器は計算機及びソフトウェアを搭載するものとする。

２．　適用範囲

ロケットペイロードのハザーダスな機器の誤動作（太陽電池パドルやアンテナ等展開物の誤展開、電波誤放射、毒性物質漏洩等）を防止している電気的インヒビットの制御系に対して適用する。
（ハザード制御のために動作し続ける必要がある機器の意図せぬ停止に関連する制御系の独立性については適用外である。該当システムが存在する場合は別途、JAXA安全・信頼性推進部と調整すること。）

３．解釈

複数のインヒビットを制御するCBCS は以下の点を満足すれば、一定の独立性を担保できると評価できる。

図1　用語の定義

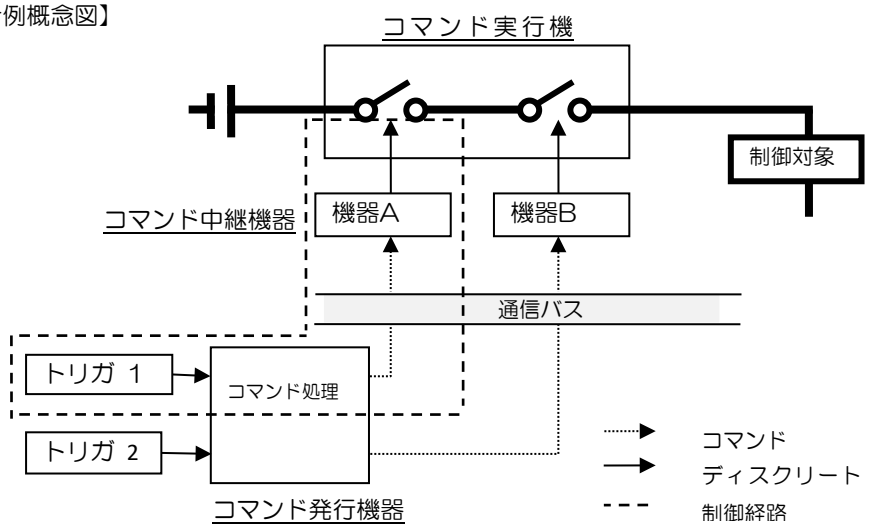
本文中で使用される「コマンド発行機器」、「コマンド中継機器」及び「コマンド実行機器」の定義を以下に示す。また、一般的なCBCS設計例の概念図を以下に示す。

「コマンド発行機器」…あるトリガによって受信される信号を処理し、インヒビットを解除するためのコマンドまたは信号をコマンド実行機器に向けて送信する機器。

「コマンド中継機器」…コマンド発行機器から受信されるコマンドまたは信号の中継及び処理を行い、コマンドまたは信号をコマンド実行機器に送信する機器。

「コマンド実行機器」…コマンド発行機器またはコマンド中継機器から受信されるコマンドまたは信号を処理し、実行する機器。

【CBCS設計例概念図】



３．１ 各構成要素に対する独立性の設計指針

(1) インヒビット解除コマンド

(a) インヒビット解除コマンドの識別の固有性

コマンドがビットパターンで表現される環境では、インヒビット解除コマンド以外のコマンド送受信の誤りなどにより意図していないインヒビットが解除されることを防ぐため、インヒビット解除コマンドはそれぞれ固有のビットパターンを持つ。

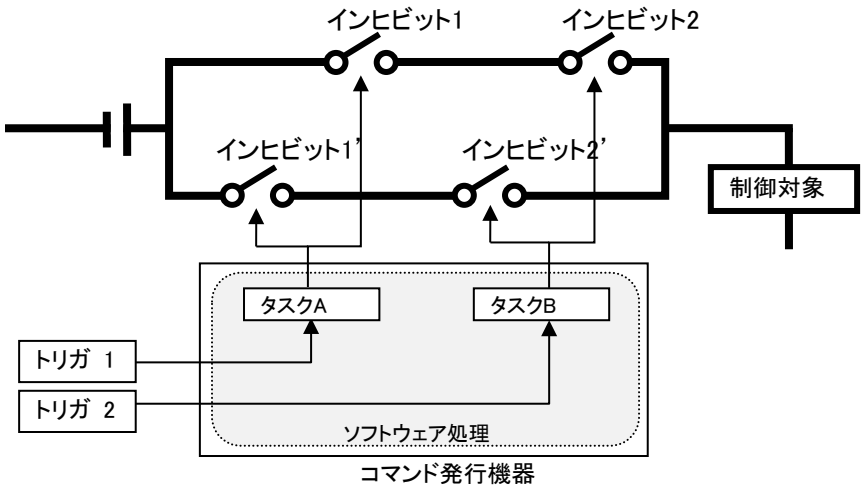
(b) インヒビット解除コマンドとインヒビットの対応の一意性

1 つのインヒビット解除コマンドは、特定の1 つのインヒビットを解除するものである。（ただし、信頼性の観点から制御対象の回路に冗長系を持たせる等の場合は、1 つのコマン

ドにより系毎に1 つのインヒビットを解除して良い。）
本対応の概念を図2 に示す。

図2　3.1(1)(b)項インヒビット解除コマンドとインヒビットの対応の一意性の例

下記に、インヒビット解除コマンドとインヒビットの対応の一意性の例を示す。コマンド発行機器はトリガ1によってインヒビット1,1’を解除し、トリガ2によってインヒビット2,2’を解除する。ここで、インヒビット1及びインヒビット2を解除するコマンドはそれぞれ異なるものを使用しなければならない（インヒビット1’及びインヒビット2’についても同様）。ただし、インヒビット1及びインヒビット1’は信頼性の観点から冗長の関係にあるため、インヒビット1及びインヒビット1’の解除コマンドは共通でも構わない（インヒビット2及びインヒビット2’についても同様）。



(c) インヒビット解除コマンドの通信上の独立性
インヒビット解除コマンドを送信する際は、通信コマンド毎に個別の通信フレームにより異なるタイミングで送信する。

(2) インヒビット解除コマンドを発行する機器
(a) インヒビット解除コマンドへの配慮
以下の(a-1)～(a-3)のいずれか、もしくはいずれかを複数組み合わせた設計を行う。

(a-1) 分離されたコマンド発行制御経路を持つソフトウェア設計
同一のハザードの複数のインヒビット解除コマンドを発行するソフトウェアは、コマンド毎に分離された制御経路を持つ。分離された制御経路とは、各コマンドに対して機能的な独立性を与える制御経路（論理的な流れ（図1 参照））であり、通常動作時のみならず、いかなる故障やオペミスが生じても他のコマンド発行処理に影響を及ぼさないものである。なお、コマンド発行処理の独立性を保証するために３．２項を参考にすること。本対応の概念

を図3 に示す。

(a-2) 独立な条件でコマンド発行を抑止するソフトウェア設計
上記 (a-1)を満足できない場合（例えば、同一のハザードに対する複数のインヒビット解除コマンドが、時系列に基づく共通の処理（タイムライン処理等）により発行され、分離された制御経路とは判断できない場合）、意図しない処理の開始とその後のコマンド発行を抑止するため、この処理から独立した条件（衛星分離、レートダンピング完了または太陽捕捉の判定など）を必要とする設計とする。この条件の数は、故障許容を実現するのに十分なものとする。なお、コマンド発行が単一故障で実行されないために、この条件処理については３．２項で示される独立性を保証すること。本対応の概念を図3 に示す。

図3 計算機を用いた制御系の独立性　概念図

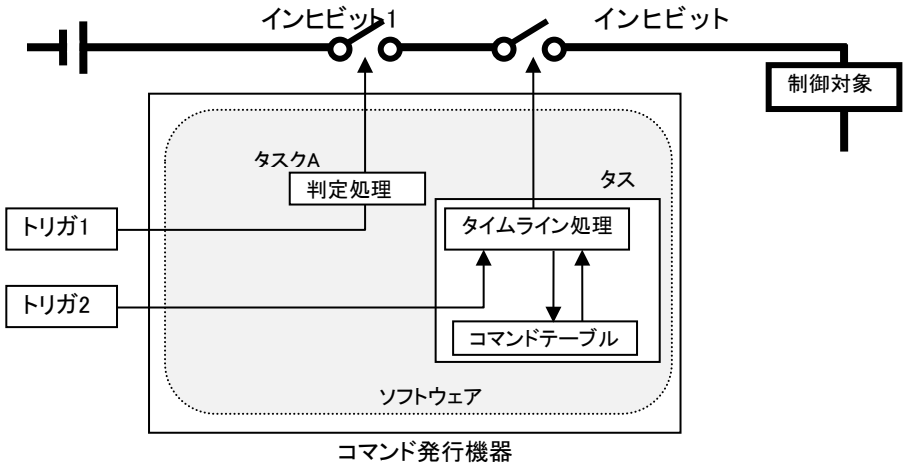
以下は、重大ハザード（1FTが要求される）に対して、電気的な故障によるハザーダスな機器の意図しない動作を防止している電源系、制御系の一例である。なお、トリガ1、2は独立したH/Wで実現されている。本文3.1(2)項(a-1),(a-2)で示される内容を適用した場合の例を概念図として示す。各項ともに、インヒビットの制御系において、「いかなる1つの故障によっても2つのインヒビットが同時に解除されない」設計を実現している。破局ハザードの場合も同様に、「いかなる2つの故障によっても3つのインヒビットが同時に解除されない」設計を実現すること。なお、参考として、各適合例の下に不適合例を示す。

3.1(2)(a-1)項の適合例

1つのソフトウェア処理によって2つのインヒビットが制御されているが、これらの制御を行うタスクは独立しており（タスクA及びBは互いに独立であることが３．２項に従って評価されている）、制御経路が分離している。それぞれのインヒビットの解除処理動作を以下に示す。

タスクA：トリガ1条件によるソフトウェア内の判定処理によって、インヒビット1解除コマンドを送信する

タスクB：トリガ2条件によってタイムライン処理を開始し、コマンドテーブルからストアードコマンドを呼び出し、インヒビット2解除コマンドを送信する

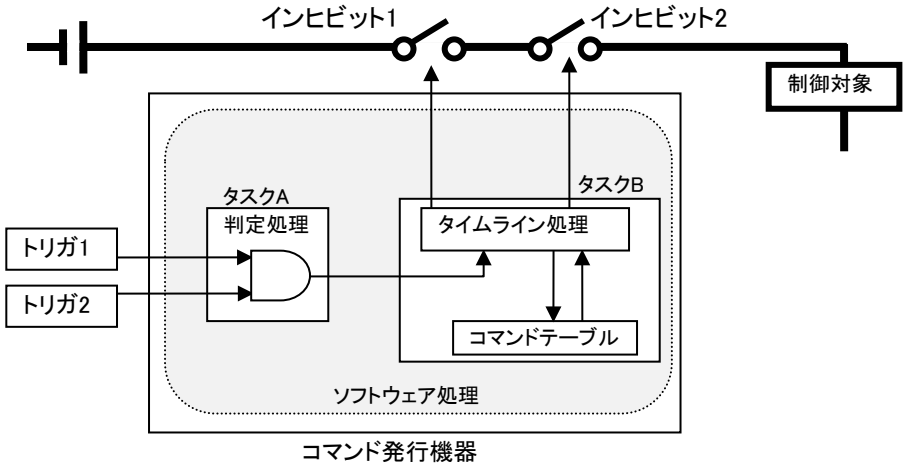


3.1(2)(a-1)項の<u>不適合例</u>

1つのソフトウェア処理によって2つのインヒビットが制御されており、これらの制御を行うタスクA及びBは独立しておらず、制御経路が分離していない。このため、単一故障点が存在する（タスクAまたはBの1故障によってインヒビット1及び2が解除される可能性がある）。以下にインヒビット解除処理動作を示す。

タスクA：トリガ1及び2の論理積によってタスクBに判定信号を出力する。

タスクB：タスクAからの信号によってタイムライン処理を開始し、コマンドテーブルからストアードコマンドを呼び出し、インヒビット1及びインヒビット2解除コマンドを送信する。

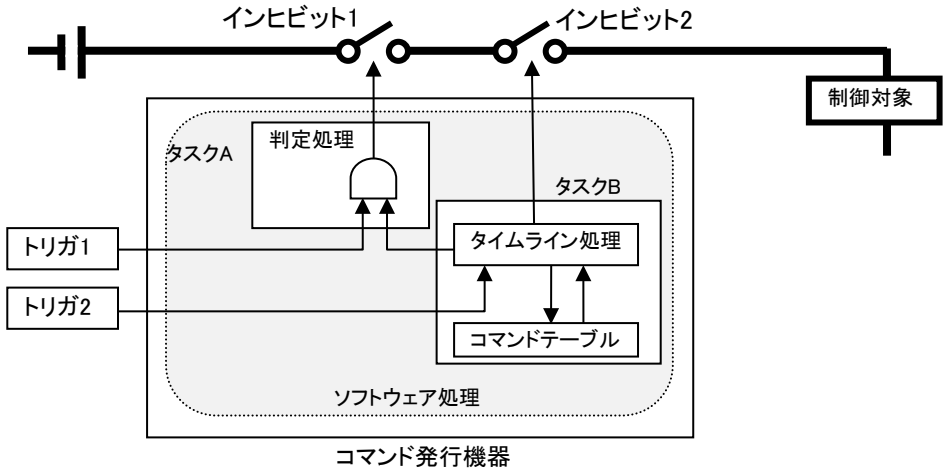


3.1(2)(a-2)項の適合例

インヒビットを解除するコマンドがタスクBの同一のタイムライン処理で発行されるため、制御経路は互いに独立してはいないが、インヒビット1解除処理がトリガ1判定とタイムライン処理との論理積となっており、コマンド発行を行うタイムライン処理とは独立した条件によってコマンド発行を抑止する設計となっている（例えば、トリガ2の故障によりタイムライン処理が実行されても、インヒビット1解除コマンドの発行はトリガ1によって抑制されている）。このタスクAの判定処理は３．２項に従って独立性が評価されている。

タスクA：タスクBのタイムライン処理からインヒビット1解除コマンドを受け取り、トリガ1条件によってコマンドを送信する（トリガ1がインヒビット1解除コマンドの送信を抑制している）

タスクB：トリガ2条件によってタイムライン処理開始し、コマンドテーブルからストアードコマンドを呼び出し、インヒビット1及びインヒビット2の解除コマンドを送信する

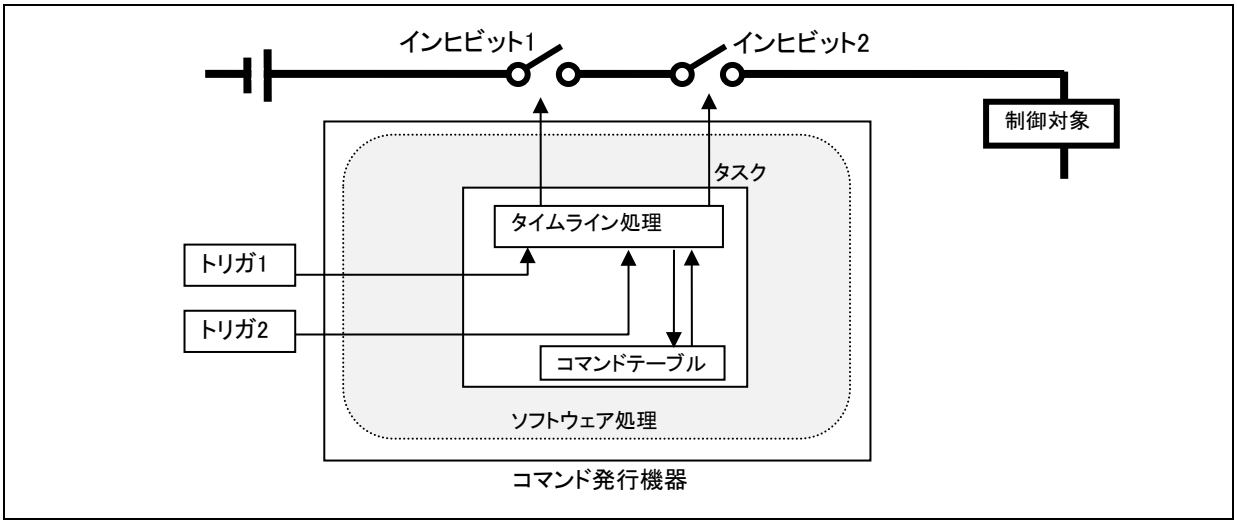


3.1(2)(a-2)項の**不適合例**

インヒビットを解除するソフトウェア処理（以下の(1)及び(2)）を共通のタスク（タイムライン処理）で行っており、タイムライン処理を抑止する独立した条件が存在しないため、単一故障点が存在する設計となっている（タスクの1故障によってインヒビット1及び2が解除される可能性がある）。

(1)トリガ1条件によってタイムライン処理開始し、コマンドテーブルからストアードコマンドを呼び出し、インヒビット1解除コマンドを送信する

(2)トリガ2条件によってタイムライン処理開始し、コマンドテーブルからストアードコマンドを呼び出し、インヒビット2解除コマンドを送信する



(a-3) インヒビット解除コマンドを登録しないソフトウェア設計
あるインヒビットの解除コマンドをロケットペイロードの機器に登録しない設計とする（例：地上からのコマンド送信のみで実現される）。この場合、いかなる故障が生じても当該コマンドが生成されない（ストアードコマンドは存在せず、故障によってインヒビット解除コマンドが発行されることはない）ことを示す。

(b) インヒビット解除の順序及びタイミングへの配慮
インヒビット解除の順序またはタイミングによりハザードを生じる可能性がある場合、ハザードを生じる順序またはタイミングでインヒビット解除コマンドを発行しない。

(3) インヒビット解除コマンドを中継する機器
(a) コマンド展開の禁止
同一ハザードの複数のインヒビット解除コマンドを中継する機器は、受信したコマンドだけを下流側に送信し、複数のインヒビット解除コマンドに展開しない。

(b) インヒビット解除の順序及びタイミングへの配慮
インヒビット解除の順序またはタイミングによりハザードを生じる可能性がある場合、ハザードを生じる順序またはタイミングで受信したインヒビット解除コマンドを棄却し、下流側に送信しない。

(4) インヒビット解除コマンドを実行する機器
(a) コマンド展開の禁止
同一のハザードの複数のインヒビット解除コマンドを実行する機器は、受信したコマンド

に該当するインヒビットだけを解除し、複数のインヒビットを解除しない。

(b) インヒビット解除の順序及びタイミングへの配慮
インヒビット解除の順序またはタイミングによりハザードを生じる可能性がある場合、ハザードを生じる順序またはタイミングで受信したインヒビット解除コマンドを棄却し、該当するインヒビットを解除しない。

３．２ コマンド発行の独立性を保証するソフトウェア設計

同一のハザードの複数のインヒビット解除コマンドを発行するソフトウェアは、コマンド毎にその発行に関する独立した処理を持つ必要がある。
ここで、独立したソフトウェア処理とは、通常動作時のみならず、いかなる故障やオペミスが生じても、他のコマンド発行処理に影響を及ぼさないものである。特に、CBCS の故障を想定した場合は、「誤って他のインヒビット解除コマンドを発行してしまう故障モードが存在しないか、または、許容される設計である」ことを、具体的なソフトウェアの設計の評価を通じて判断する必要がある。
具体的には、以下のいずれかに該当する場合は、ソフトウェア設計によりコマンド発行の独立性が一定程度保証されていると判断するものとするが、必要な数の故障許容相当とする最終的な判断は、３．１項と合わせて総合的な見地から行わなければならない。

(1) タスクレベルの独立
複数のインヒビットが、それぞれ異なったタスク(*)により制御され、それぞれのインヒビット解除条件が同一でない場合。ただし、以下の場合は、共通故障に対する付加的な評価が必要である。
(*) ここで言うタスクとは、固有の計算機資源を持つ、実行中のプログラムのことである。ここで用いる「タスク」は一般的なものであるので、評価対象の利用する処理系によって異なる用語が使用されている場合は、適宜これらを読み替えること。

(a) プロセス間通信に関する評価
インヒビット制御を行うタスクの間でプロセス間通信（共有メモリやソケット、各種の同期など）が行われる場合、プロセス間通信処理が関係する故障モードの影響として、複数のインヒビットが解除されることがないことを示す。

(b) 共通の設計に関する評価
インヒビット制御を行う複数のタスクが共通の関数やコードを利用する場合、これらの関数やコードが関係する故障モードの影響として、複数のインヒビットが解除されることがないことを示す。

(2) 関数レベルの独立

(1)のタスクレベルの独立が実現できないが（複数のインヒビットが一つのタスクにより制御されるが）、それぞれ異なった関数により処理が行われ、それぞれのインヒビット解除条件が同一でない場合。ただし、以下の場合は、共通故障に対する付加的な評価が必要である。

(a) 関数間共有変数に関する評価

複数の関数により共有される変数（グローバル変数）がある場合は、その変数に関係する故障モードの影響として、複数のインヒビットが解除されることがないことを示す。

(b) 共通の設計に対する評価

インヒビット制御を行う複数の関数が共通のライブラリ関数やコードを利用する場合、これらのライブラリ関数やコードが関係する故障モードの影響として、複数のインヒビットが解除されることがないことを示す。

付録： ハードウェアで故障許容性を保証する設計例

ここまで、CBCS で複数のインヒビットを制御する場合のソフトウェアに対する設計指針について示した。ここでは、CBCS で複数のインヒビットを制御する場合に、ソフトウェア設計によらず、システムとして故障許容設計とする指針を示す。また、本設計の概念を図A-1に示す。なお、参考として、本設計に適合せず1 故障許容設計を満足しない例も図A-1 に示す。

図A-1　ハードウェアでコマンドの発行/実行を抑止する設計

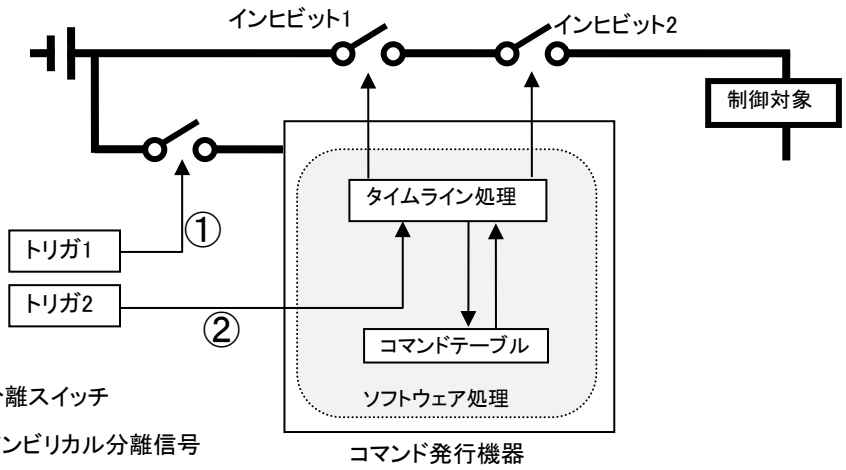
(a)ハードウェアによるインヒビット解除の抑制例

　インヒビット1,2を解除するコマンド発行機器内のソフトウェア処理は共通であるが、H/Wによってコマンド発行を抑制しており、システムとして1故障許容を満足している。(i)コマンド発行機器の意図せぬ電源投入、(ii)コマンド発行機器の誤動作という２つのH/W故障が生じて初めて、インヒビット1、2が解除される。（トリガ1、2は独立したH/Wで実現されている）

　①トリガ1条件によるコマンド発行機器の電源投入

　②トリガ2条件によってタイムライン処理を開始し、コマンドテーブルからストアードコマンドを呼び出し、インヒビット1,2を解除する。

　*インヒビットとは制御対象とエネルギー源との間に設置される遮断装置のことであるため、コマンド発行機器の電源を遮断するリレーは、制御対象に対するインヒビットではない。

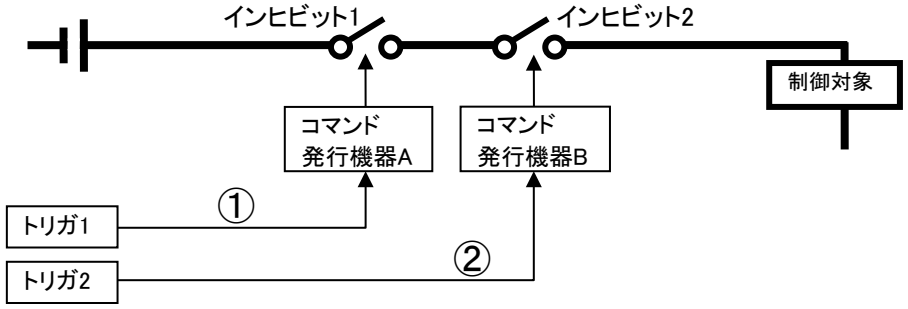


(b)ハードウェアが独立している設計例

インヒビット解除コマンドを処理する機器及び下流側の機器が、各インヒビット毎に独立しており、1故障許容を満足している。

①トリガ1条件によって、コマンド発行機器Aがインヒビット1解除コマンドを送信する

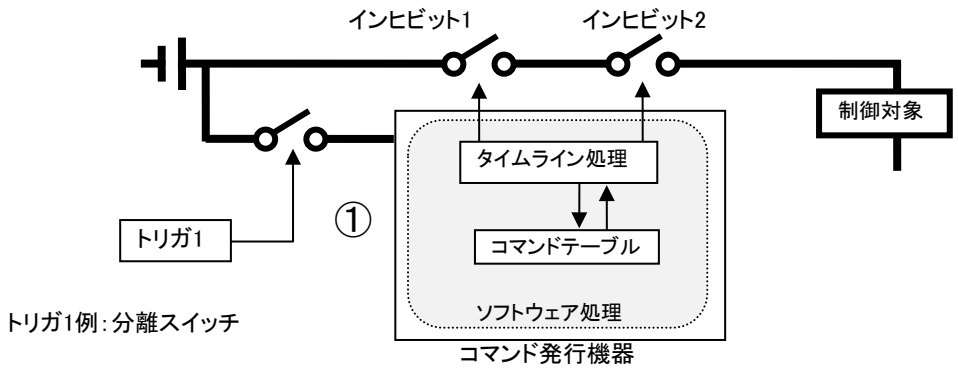
②トリガ2条件によって、コマンド発行機器Bがインヒビット2解除コマンドを送信する



<u>1故障許容を満足できていない例</u>

インヒビット1,2を解除するコマンド発行機器内のソフトウェア処理は共通しており、トリガ1の1故障によってインヒビット1,2が解除されるため、1故障許容を満足していない。

①トリガ1条件によるコマンド発行機器の電源投入によって、タイムライン処理を開始し、コマンドテーブルからストアードコマンドを呼び出し、インヒビット1,2を解除する

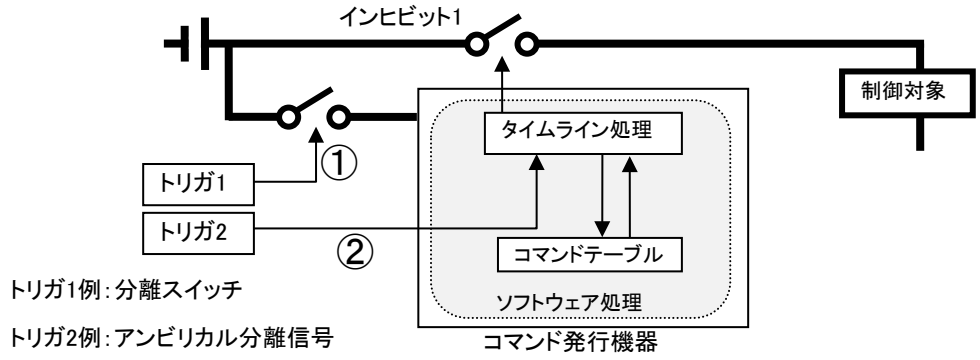


1故障許容を満足できていない例

インヒビット制御ラインは(a)の考え方により1故障許容を満足しているが、制御対象とエネルギー源との間に設置されるインヒビットが1つしかないため、1故障許容を満足していない（コマンド発行機器の電源を遮断するリレーはインヒビットとは数えられない）。よって下記設計は、例えばインヒビット1の短絡という1故障で制御対象が動作してしまう可能性があり、インヒビットの数が足りない設計となっている。

①トリガ1条件によるコマンド発行機器の電源投入

②トリガ2条件によってタイムライン処理を開始し、コマンドテーブルからストアードコマンドを呼び出し、インヒビット1を解除する。



(a) ハードウェアでコマンドの発行/実行を抑止する設計

インヒビット解除コマンドを処理する機器または下流側の機器において、コマンドの発行／実行を抑止する条件をハードウェアで実現する設計。この条件は、インヒビット解除コマンドを発行する計算機及びそのソフトウェア処理とは独立したものとする。また、条件の数は故障許容を実現するのに十分なものとする。

(b) ハードウェアが独立している設計

インヒビット解除コマンドを処理する機器及び下流側の機器が、インヒビット毎に独立している設計。

4.3.1.5.1　故障許容設計要求　解説その2

１．目的

故障許容設計を成立させるためのインヒビットについて、その有効性を確認するタイミングを明確にする。なお、本資料は電気的なインヒビットについて言及しており、機械的なインヒビットは本資料の対象外とする。なお、本解釈の通りではない他の方法で安全を確保することを妨げるものではない。

背景

- 小型衛星等はコールドロンチであるため、打上げ中はインヒビットのモニタが不可能である。このため、ロケット搭載前にインヒビット確認を実施することで、その有効性を担保している。一方、ホットロンチの衛星では、打上げ中のインヒビットの常時モニタが可能な場合もある。このように衛星によってインヒビットのモニタ手段が異なっているため、打上げ中のリアルタイムモニタの必要性及びモニタ手段について整理する必要があった。
- インヒビットとしてFET を使用する場合は、直接インヒビットのステータスを確認するモニタ回路は煩雑となるため（ミッション信頼度を低下させる場合がある）、FET SW の駆動ラインのフィードバックを確認することでインヒビットを検証するミッションもある（特に、FET を用いたリターン側のインヒビットのモニタを実現する手段は困難であるため）。このような間接的な確認手段を受け入れ可能かどうか整理する必要があった。

２．解釈

以下に、コンフィギュレーション等の条件に応じたインヒビットの有効性確認方法の例を示す。なお、インヒビットに打上げ中リアルタイムモニタが必要となるのは、異常時等に緊急対応する必要がある場合である。

【前提】

以下に示される全ての条件は、「ハザードに対してインヒビットによる抑制が必要な期間中」を対象とする（「ハザードに対してインヒビットによる抑制が不要な期間」はインヒビットの状態によらず安全が確保できているため、インヒビットの状態確認は不要である）。

「ハザードに対してインヒビットによる抑制が必要な期間中」は、「必要数のインヒビットが機能している状態であること」が原則である。

(コンフィギュレーション1)

地上で有効性が確認された全てのインヒビット及び制御回路の状態が打上げ中維持される場合、インヒビットのリアルタイムモニタは実施しなくてもよい。

本条件ではハザードをインヒビットで制御している期間中にハザードの制御に寄与する機器等のコンフィギュレーションを変更することはないため、全てのインヒビットの故障によるハザード顕在化の可能性は非常に低い。よって、異常時に緊急対応するためのリアルタイムの対応が必要な状況ではなく、打上げ中リアルタイムモニタを実施しなくてもよい。インヒビットのコンフィギュレーションを最終設定するタイミング等でインヒビットの有効性を確認すればよい。

また、地上でインヒビットを検証した後にインヒビット及びその制御回路の故障や状態変化が想定されない場合は、検証実施後のインヒビットのモニタは不要である。
なお、この場合、直接的な確認と同等と認められる方法であれば、インヒビットの状況は間接的な確認でも受け入れられる。

多くの衛星の場合、ロケット飛翔中はインヒビットを解除しないため、本項を適用すればよい。
例えば、射場でのアビオニクス系チェックアウト等でのインヒビットのステータス確認を実施する場合は、当該ステータス確認後のインヒビットモニタは不要とすることができる（振動試験等で事前にインヒビットの耐環境性を検証できていることが前提）。なおこの場合、２つのインヒビットを解除した状態でのハザーダスな機能への導通確認など間接的な手法でインヒビットの健全性を確認することでも受け入れられる。

(コンフィギュレーション2)
以下の2 つの条件を満たす場合インヒビットモニタは不要（射場でのステータス確認も含めて不要）。

I. 想定される通電故障モードが排除されている場合（必要数＋1のインヒビットが存在する場合等）
II. インヒビットの制御回路が無効となっている場合（制御回路が電源遮断されており、回路の故障でインヒビットが解除されることのないこと）

必要数+1のインヒビットを加えることにより信頼度を高め、ハザーダスな機能が作動する可能性を低くできること、及び、制御回路を無効にすることでインヒビットそのものが同時に故障しない限り、ハザーダスな機能が動作しない状況と言えるため、インヒビットモニタは不要（モニタ行為そのものが不要）とすることができる。（出典:AFSPCMAN91-710 vol.3 12.8.3.5, NSTS1700.7B 202.1c(3)）

(コンフィギュレーション3)
ハザードの抑制に寄与する機器のコンフィギュレーションを打上げ中に変更する場合

（前提で示した通り、原則、必要数のインヒビットの解除は許されない。）インヒビットのリアルタイムかつ直接モニタが必要

ハザードの抑制に寄与する機器のコンフィギュレーションを変更する前に、ハザーダスな機能に対する制御が有効であることをモニタする必要があるため、インヒビットをリアルタイムでモニタをできる手段を設ける必要がある。また、この場合、限られた時間内で確実に状態把握を行うため、モニタ箇所はインヒビットの状態を直接確認する部分であることも必要である。（例：メカニカルリレーの接点モニタ、バルブの位置センサ、等。インヒビット駆動ラインのフィードバック等の間接的なモニタは受け入れられない）。
多くの衛星では、ロケット分離以前にハザードの抑制に寄与する機器のコンフィギュレーションを変更しないため、リアルタイムモニタは必要ではない。以下の事例を参考に、リアルタイムモニタの要否を確認すること。

<米国空軍要求の事例> 出典: AFSPCMAN91-710 vol.3
ロケット固体モータや指令破壊系、液体推進薬等のインヒビットはロケット打上げに伴いインヒビットの状態の変更が行われるため、ステータスはリアルタイム及び直接状態を確認できるモニタが要求される。

<スペースシャトルプログラムの事例1> 出典：NSTS1700.7B 202.1
オービタから固体ロケットモータを搭載した人工衛星を放出するミッションにおいて、オービタから放出された衛星が安全な距離に達する前にSafe & Arm Device(SAD)を解除する場合、固体ロケットモータに対する電気的3 つのインヒビットのうち2 つのインヒビットのリアルタイムモニタが要求されている。
（この状況下ではSAD は解除されるため、SAD を除いて他のハザード制御として電気的な3 つのインヒビットで2 故障許容を確保している。ただし、SAD 解除によりロケットモータへの点火回路における物理的遮蔽が解除されるため、安全上重要な機器のコンフィギュレーション変更と見なされる(図１参照)。）

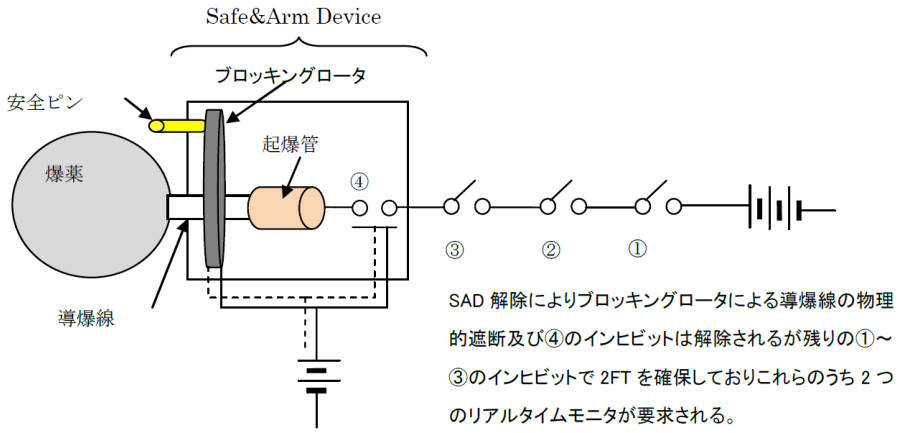


図 1 スペースシャトル搭載ペイロードの Safe & Arm Device 例

<スペースシャトルプログラムの事例2> 出典：NSTS1700.7B 202.2

オービタから液体推進薬を搭載した人工衛星を放出するミッションにおいて、オービタから放出された衛星が安全な距離（大径スラスタを噴射しても問題ない距離）に達する前に小径姿勢制御スラスタ駆動のため遮断弁を開放する場合、残り2 つの流量調整弁(遮断機能あり)に対する電気的な3 つのインヒビットのうち2 インヒビットのリアルタイムモニタが要求されている（図2 参照）。

（オービタから放出された衛星が安全な距離に達する前に大径スラスタが噴射することは破局ハザードとみなされるため、推進システムには少なくとも3 つの機械的な推進薬遮断機器（遮断弁等）が要求される。また、電気的故障に対して少なくとも3 つの電気的インヒビットが要求されている。

小径姿勢制御スラスタ駆動のための遮断弁開放は、小径スラスタ噴射、及び、推進薬の少量リークが発生してもシャトルに影響のない距離（通常50～100 メートル）で実施される。つまり、大径スラスタ誤噴射は依然2 故障許容が要求されるため電気的な3 つのインヒビットにより制御される必要がある。一方、シールからの内部漏洩については遮断弁以外の残り2 つの流量調整弁で推進薬の大量リークは制御されていると判断されるため、安全な距離の前の遮断弁開放は認められている。）

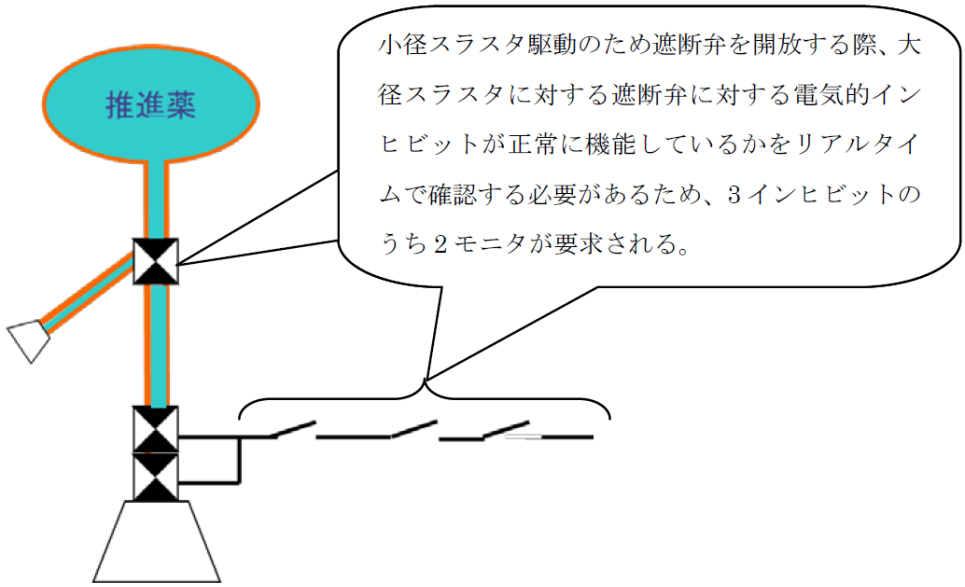
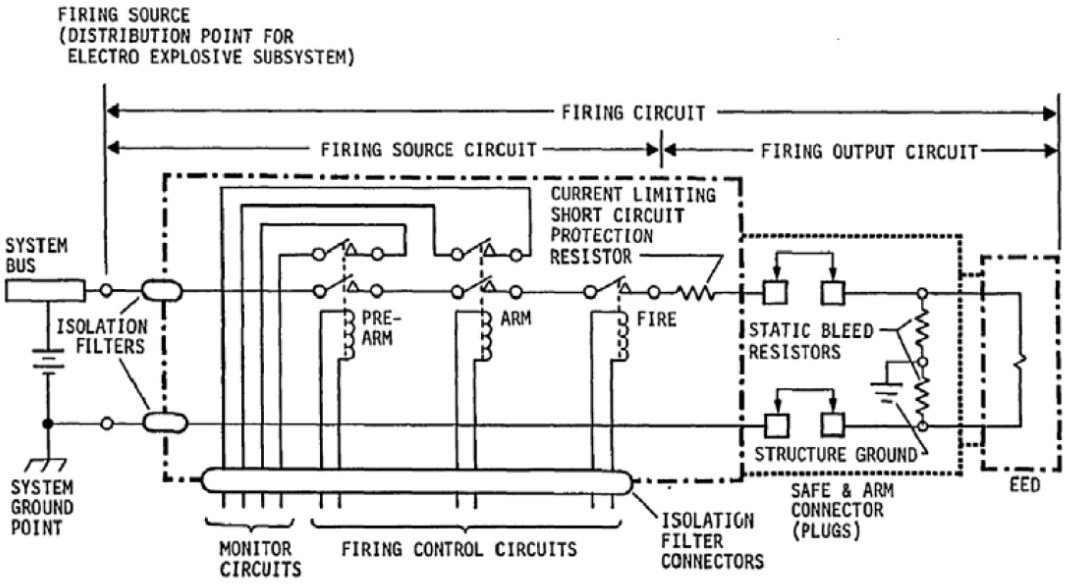


図 2 スペースシャトル搭載ペイロードの推進システムに関するインヒビットの例

「インヒビットの状態を直接確認する」手段の例を以下に示す。

(a) リレーを用いた例（出展：MIL-STD-1576）

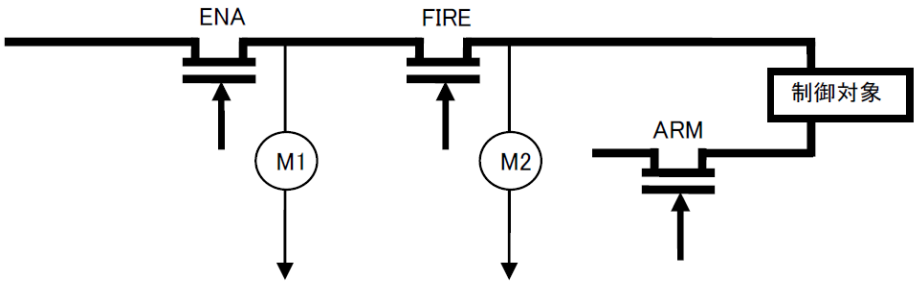
リレーのメカニカル接点をモニタしている。インヒビットの導通までモニタしていないが、リレーに故障モードを想定し、「直接確認する」手段として認めている。



(b) 半導体SW を用いる例

常時モニタM1 を監視する。ENA をクローズし、M2 によりFIRE がインヒビットとして有

効であることを確認した後に、ARM をクローズする。その後、FIRE をクローズする。



３．根拠

・JMR-002 におけるインヒビットのモニタの考え方は、米国空軍の安全要求やNASA 有人システムを参考に設定したものであり、本解釈もこれらの要求を根拠としている。（以下参照）

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 射場における火災・爆発ハザードの防止　解説

１．目的

「5.1 射場における火災・爆発ハザードの防止」の詳細を解説する。なお、本解説の通りではない他の方法で安全を確保することを妨げるものではない。

２．5.1(2)a.の解説

「対象とする電気機器の電気容量が十分小さく、対象爆発性ガスの点火限界以下で点火源となり得ないものも、有効な防爆対策として認められる」についての詳細を解説する。

２．１．点火限界評価

労働安全衛生総合研究所技術指針「工場電気設備防爆指針（国際整合技術指針）」（以下、「防爆指針」と略称）第6編 本質安全防爆構造”i” 付属書A 本安回路の評価　に規定される基準曲線を用いて、対象の電気機器が対象爆発性ガスの点火限界以下であることを評価する。評価においては、対象の電気機器がさらされる温度環境が防爆指針で規定される温度範囲（-20℃～+60℃）内であることを前提とする（その他注意点等は２．２項参照）。
本評価により、対象爆発性ガスの点火限界以下であることが示された場合、防爆設計は必須ではない。

＜参考情報＞
「防爆指針」第6編 本質安全防爆構造”i” 付属書A 図A.1～図A.6 による評価は、本質安全防爆構造”i”における評価基準：火花点火試験(回路に点火能力がないことの確認試験)による確認を代替するものである。グループIIC の火花点火試験は爆発性試験用混合ガス組成の使用が指定されており、これは水素の燃焼範囲(4.0～75vol%(1 気圧下))のうち、最小着火エネルギーを与える混合比である（ガス混合比に対する最もワーストな評価）。すなわち、本試験に適合すれば、ガスの濃度変化は包含される。

２．２． 防爆指針の適用に関する補足情報

２．２．１ ヒドラジンやメタノールの防爆指針上の取り扱い

点火限界評価には、対象爆発性ガスのグループを明確にする必要がある。防爆指針においてヒドラジンやメタノールはどのグループに区分されるかは不明であるが、最悪ケースを想定して電気機器の区分の基準のグループIIC(※1)を適用すればよい。

(※1)グループの定義について(「防爆指針」第1 編 総則より)
グループII：坑気の影響を受ける鉱山以外の爆発性ガス雰囲気が存在する場所で使用する電気機器。グループII の電気機器は、それを使用しようとする爆発性雰囲気の性質に応じて細分類する(この細分類は、電気機器を設置しようとする爆発性ガス雰囲気の最大安全隙間又

は最小点火電流値に基づいている(IEC60079-20-1 参照)。グループII の細分類は、次のとおりである。

IIA：代表ガスは、プロパン / MESG ≧ 0.9 mm or MIC > 0.9

IIB：代表ガスは、エチレン / 0.55mm < MESG < 0.9 mm or 0.5 ≦ MIC ≦ 0.8

IIC：代表ガスは、水素 / MESG ≦ 0.5 mm or MIC < 0.45

MESG : maximum experimental safe gaps (最大安全隙間)

MIC : minimum igniting currents (最小点火電流値)

グループIIC はさらされる気体の着火エネルギーが最小の（＝最も着火しやすい）カテゴリとして定義されている。また、グループIIC で定義される閾値以下の着火エネルギーは全てグループIIC に区別される。

２．２．２ 防爆指針の宇宙環境への適用に関する考え方

防爆指針は、第1編総則に記載されている通り、地上環境（温度 -20℃～+60℃、大気圧 80～110kPa、酸素濃度 体積分率約21％）を想定しているため、ロケット打上げ後の温度・減圧環境下に防爆指針を適用するための考え方を以下に整理する。

- 温度条件については、個別に「防爆指針」の前提温度範囲に打ち上げ後の温度環境が包含されていることの確認が必要。
- 減圧環境下では大気圧より発火は起こり難くなることから、大気圧を前提とした「防爆指針」で評価しておけば減圧環境に対して安全側の評価となる(※2)。

(※2)減圧環境の評価が大気圧での評価に対して安全側になる根拠

最小発火エネルギーは、圧力の増大とともに著しく値が小さくなるが、逆に減圧下では増大して発火が起こりにくくなる。（初級 高圧ガス保安技術第10 次改訂版（高圧ガス保安協会発行）p.41 より）。また、燃焼は、周辺気圧の低下に伴い燃焼反応の継続ができなくなる（平野敏右著「燃焼学」 3.2.3 着火に及ぼす圧力と温度の影響）。

２．２．３ 防爆指針の点火限界曲線の外挿について

「防爆指針」 第6編 本質安全防爆構造”i” 付属書A 図A.1～図A.6 の原点は全てある値となっているが（ゼロではない）、当該数値よりも小さい値の場合の取り扱いとしては、電圧と電流は負の相関で外挿すればよい(※3)と考える。

(※3) 電圧と電流は負の相関で外挿できる根拠

チャタリングのような電気火花で局所的にその空間にある気体の温度を上昇させて着火する現象は、加えたエネルギーの量が着火の条件となるため。（AIAA SP-084-1999 Fire, Explosion, Compatibility, and SafetyHazards of Hypergols – Hydrazine において規定されるヒドラジンの着火閾値もエネルギー（数mJ）で規定されている。）

３．5.1(2)d.の解説

「爆発性危険雰囲気において露出した電熱線等を通電しない。」について解説する。
これは、小型衛星等の保持解放機構等に用いられるテグスを焼き切るためのニクロム線等露出した電熱線が、可燃性物質（液体推進薬等）に対する防爆構造の電気機器の温度上昇限度(※4)に達するような局所的な温度上昇をもたらすことを懸念しての記述である。（電熱線は通常加熱により火花を生じるわけではないため、引火点に達した可燃性物質が、火花により燃焼するモードは想定しない。）一方で、大型衛星で使用される触媒層用ヒータ等は一般的にペイロード分離前までに防爆構造の電気機器の温度上昇限度に達するような高温にはならないため、個別の熱解析等の評価は不要である（ここでは、軌道上運用時のヒータ温度については考慮不要）。なお、「露出した電熱線」以外に防爆構造の電気機器の温度上昇限度となりうる熱源が存在する場合には、ハザードとして識別し、制御する必要がある。

(※4)ヒドラジンの発火温度は270℃、モノメチルヒドラジン（MMH）の発火温度は194.4℃である。工場電気設備防爆指針によると、「防爆構造の電気機器の温度上昇限度は、それぞれの発火度に対応する発火温度の下限値の約80%から基準周囲温度の限度40℃を差引いた値である。」とされている。例えばMMHの場合、発火度はG4（発火温度135℃超過200℃以下）であり、70℃までの温度上昇が許容されている。

5.3　射場におけるリチウムイオンバッテリ破裂ハザードの防止　解説

１．目的

「5.3　射場におけるリチウムイオンバッテリ破裂ハザードの防止」の詳細を解説する。なお、本解説の通りではない他の方法で安全を確保することを妨げるものではない。

２．リチウムイオンバッテリ破裂ハザードの被害の度合いの考え方

バッテリの発火、破裂は、作業者への傷害、地上設備が損傷に至る。下記 1)、かつ 2)に該当するリチウムイオンバッテリ発火、破裂の被害の度合いは、射場の爆発性危険雰囲気外において限定・局所的ハザードと整理されるため、ハザードレポート起草不要である。

1) 機器に組み込まれたリチウムイオン単電池 1 個のワット時定格値が 20 Wh 以下
2) 機器に組み込まれたリチウムイオン組電池 1 個のワット時定格値が 100 Wh 以下

射場の爆発性危険雰囲気においては全てのリチウムイオンバッテリ発火、破裂は火災を引き起こす原因となるため、被害の度合いを破局ハザードとする。また、ロケット搭載中のリチウムイオンバッテリ発火、破裂についての扱いは、ロケットのハザード解析による。

【補足 1】航空機持ち込み可能なリチウムイオンバッテリ容量を規定する「IATA 航空危険物規則書 第 62 版（2021）」において上記 1)2)の要件を全て満たすものは、危険物輸送の適用除外を受けられる（非危険物扱い）ことに倣い、射場の爆発性危険雰囲気外でのリチウムイオンバッテリの破裂・発火リスクは、航空機のキャビン内よりも小さいと考えられるため、上記の整理とした。

【補足 2】リチウムイオンバッテリ（二次電池）以外のリチウム系蓄電デバイスについて

本ガイドラインで扱うリチウムイオンバッテリ（二次電池）以外のリチウム系蓄電デバイス（リチウムイオンキャパシタ、イオン液体リチウムイオン二次電池など）には、リチウムイオンバッテリ（二次電池）に比べて熱暴走しにくく安全性に優れることが示されているバッテリもあるが、現時点では宇宙用の用途が定まっていないため、安全設計のガイドラインの策定に至っていない。当該バッテリを使用する場合は、安全・信頼性推進部と調整し、適用要求等を決定すること。

【補足 3】ニッケル水素(Ni-MH)充電池について

Ni-MH 電池の破裂・電解液の漏洩などのハザードは識別されないため、ハザードレポートの起草は不要。ただし、過熱による安全上の影響がないことを確認する必要がある。

３．ハザード制御方法と安全検証方法の一般的な考え方
リチウムイオンバッテリ破裂について、ハザードレポートを起草する場合のハザード制御方法と安全検証方法の一般的な考え方を以下に示す。

３．１．ハザード原因(1)セル内部の短絡
３．１．１．ハザード制御方法
(1)内部短絡が無いセルの設計・製造

３．１．２．安全検証方法
＊(1-1)UN 勧告（UN 38.3 国連勧告輸送試験）適合品または UL1642 認証品の認証番号等により、規格に基づいたセルであることを確認する。宇宙機関認定セルの場合、その機関が認定したことを確認できれば良い。
＊(1-2) 打上げ環境下でセル内部の短絡を生じるセルを排除するために、衛星搭載状態（またはバッテリ組立）の環境試験（真空試験、振動試験等）前後におけるバッテリ充放電特性に変化の無いことを示す。

＊マークの検証は、JAXA 開発完了セルを使用する場合は既に検証済みであり、追加の検証は不要。（以降の項目も同様）

【補足】
内部短絡は、X 線検査などの検査や製造時の工程管理などでは完全に制御できるものではない。UN 勧告等に準拠しているなどの実績によることも必要であるが、民生用バッテリで実績のない打上げ環境や宇宙環境の条件での評価が必要である。なお、NASA 有人宇宙機搭載バッテリガイドライン（JSC-20793）でも同じ思想である。

３．２．ハザード原因(2)セル外部の短絡
３．２．１．ハザード制御方法
(2) バッテリ負荷側短絡が無い設計・製造。
(2-1)または(2-2)のどちらかを選択する。
(2-1)セル外部の短絡に対して、2 つの保護機能をセル内部または外部に持つ（セルの保護機能の例：セパレータシャットダウン機能、PTC、ヒュージブルリンク等、セル外部の保護機能の例：ヒューズ等）。ただし、セルと外部保護機能間の経路に短絡が想定される部位は(2-2)に示す二重絶縁する（当該箇所の短絡が生じた場合、外部保護機能は機能しないため）。なお、複数セルを直列構成するバッテリでは、セルの個数分の保護機能を有していると考えてよい。

【補足】
負荷短絡の故障を 1 故障目と数え、セルまたは外部に合わせて 2 つの保護機能を確保することで、2 故障許容設計とする。

(2-2)負荷側を二重絶縁する。

【補足】
負荷側の二重絶縁は絶縁設計標準(JERG-2-213A) 5.2 項に従い行う。二重絶縁を行うことにより短絡が極めて起こりにくいと考えられ、これはリスク最小化設計とみなせる。
絶縁の実施例としては、空間絶縁（導電物間の距離を 1mm 以上開ける。）、線材被覆、テープ（カプトンテープ、ポリエステルテープ等）、樹脂シート等がある。
なお、二重絶縁ラインは 1 次電源バスラインおよびバッテリライン（バッテリ内部の電力ライン、セルケース、バッテリ筐体およびバッテリ出力ラインを含む）に適用できる。当該ラインが基板を経由する場合は、基板上・内部でも二重絶縁が成立していることを示す必要がある。また、振動や衝撃等でワイヤ被覆等の絶縁材が損傷することがないように、シャープエッジを除去し適切にワイヤを艤装する。

分離検知にスイッチを使用する場合、打上振動によるチャタリングや打上振動以外の要因（例：取り付け誤差、導電性コンタミ）で当該スイッチが短絡することがないことを示せれば、当該スイッチの短絡は極めて起こりにくいと考えられるため、二重絶縁の適用範囲は、当該スイッチの上流とすればよい。

通常、FET 等、二重絶縁できない部分がある。この場合、故障許容設計が適用される。つまり、二重故障が生じても、バッテリの破裂、発火が生じないようにすることである。具体的には、二重絶縁できない箇所に関しては、2 故障を想定した最大電流を算出し、最大電流がバッテリの定格内であることを示すこと。もしくはバッテリ内の保護機能(2-1)、ヒューズ等の過電流遮断機能を用いて、外部短絡発生時でも、バッテリの破裂、発火を防止すること。あるいは、FET 等に対して 2 故障を想定した範囲のワイヤハーネス類を二重絶縁することでもよい。

３．２．２．安全検証方法
＊(2-1-1)図面等による保護機能の確認
図面等により、保護機能が適切な位置に設置されていることを確認する。また、バッテリと外部保護機能間の短絡が二重絶縁されていることも確認する。

＊(2-1-2)機能試験等による保護機能の確認
以下のような手段で保護機能の有効性を検証する。

- システム設計で想定される適切な外部短絡抵抗値を設定し、外部短絡試験を実施することで保護機能が有効であることを示す。セルが有する保護機能を検証する場合は、フライト品と同タイミング、同一業者から購入した同一部品番号のバッテリを用いて保護機能を確認する。
- UN 38.3 または UL1642 に基づいた検証に認証済みのバッテリであることをカタログ等で確認し、当該バッテリの認証番号を示す。これにより、1 つの保護機能が検証されたこととできる。ただし、この場合はバッテリ内部に複数の保護機能を有していても個別に検証できていない、すなわち単一の保護機能と考え、もう一つ別の保護機能の検証データを示す必要がある。（UL 基準に基づいた検証が実施されていない場合、UL 基準に相当する試験項目および試験条件と、過電流保護機能のデータシートもしくは試験データを示す。）

＊(2-2-1)図面等による二重絶縁箇所の確認
＊(2-2-2)現品検査等による二重絶縁の施工結果の確認

- 衛星搭載状態での環境試験（真空試験、振動試験等）後に二重絶縁が適切になされていること、およびワイヤ艤装箇所にシャープエッジがないことを目視検査で確認する。
- 二重絶縁されない箇所については二重故障を想定した最大電流を図面および回路抵抗を用いて算出すること。そして、バッテリの定格内であることを解析で示す。

【補足】
二重絶縁のひとつとして特に空間絶縁を選択する場合には、パターン図及び基板の実測などから空間絶縁が確保されていることを示す。基板の積層内部中のパターンについては厚さ方向も含めて空間的に 1mm 以上あれば良い。スルーホールとの絶縁検討を忘れがちなため注意する。

３．３．ハザード原因(3)過充電／過放電
３．３．１．ハザード制御方法
(3-1)充電系統には過充電防止機能（異常検知、電源遮断機能）を設け、以下を考慮する。
爆発性危険雰囲気区域及びロケット搭載状態で充電する場合は過充電に対して 2 故障許容設計とする。射場設備内での爆発性危険雰囲気以外で充電する場合は 1 故障許容設計とする。なお、過充電によるセル内部の急激な温度変化を温度センサでリアルタイムに検知で

きない場合が多いため、温度センサは過充電モニタとして原則使用しないが、用いる必要がある場合は、温度センサがセルの温度に相関するものとする。
(3-2)各セルの電圧ばらつきによる過充電を防ぐ。バッテリの全電圧モニタは、セルのばらつきにより単セルの過充電の検知とならない場合もあるため、過充電防止機能の 1 つの手段は各セル電圧モニタとする。もしくは、セルの電圧のばらつきを管理した状態（単セルの異常が確認できる状態）で、バッテリ全電圧モニタを行う。
(3-3) 過放電後の再充電はハザード原因となり得ることから、過放電に対しては、電池がセル／電池パック製造業者の推奨する電圧または認定試験で確立された電圧以下で使用しない。万が一、電圧範囲を下回った場合は継続使用しない。

【補足】
リチウムイオンバッテリ（二次電池）で最も懸念すべき事項が過充電である（短絡は内部エネルギーのみであるが、充電時は外部からエネルギーが供給され続ける）。民生充電器は、一般的に 2 故障許容設計となっていないため、爆発性危険雰囲気での補充電に使用するためには、追加の制御手段を付加する必要がある。なお、NASA の無人機においても、充電器に対しては 2 故障許容設計が要求されている。

３．３．２．安全検証方法
(3-1-1)図面等による適切な故障許容設計の確認
(3-1-2)機能試験等による過充電防止機能が適切に動作することの確認
＊(3-2)検査記録等によるセルのばらつき管理結果の確認
(3-3)射場にて充電作業がある場合、充電前のバッテリ電圧の確認

【補足 1】
充電容量の管理にあたり、バッテリ電圧は充電電流や温度で変動するため、充電容量は電圧でのモニタに加えて、電流と時間の積で規定する。

【補足 2】
過放電について。過放電自体は安全上の問題ではなく、その後の充電時に過充電等の問題が発生する（過放電により異常に電圧降下したセルを含むバッテリを充電する場合、直列の場合他のセルが過充電状態となる）。少なくとも射場では完全放電するような機能試験等の運用は計画されないこと、過充電防止の観点で各セルモニタ、セルのばらつき管理等の安全対策が取られることを確認できれば、過放電に対して特別な安全設計は考慮する必要はない。射場でバッテリの充電作業を計画する場合、充電前に電圧測定し想定以上の電圧降下が生じていないか確認する。

３．４．ハザード原因(4)熱制御系の故障に起因する異常な温度環境での使用

３．４．１．ハザード制御方法

(4-1)または(4-2)どちらかを選択。

(4-1)最悪状態（ヒータ駆動回路の 2 故障後など）でもバッテリ保証温度以下である設計

(4-2)2 故障が生じてもヒータが ON にならない設計

【補足】

ヒータ過熱等の 2 次的要因による故障に対しては、民生用バッテリの強度設計は製造メーカに依存するため、熱源側で 2 故障許容設計とする必要がある。

３．４．２．安全検証方法

(4-1) 最悪状態（ヒータ駆動回路の 2 故障後など）を想定した熱解析によりバッテリ保証温度以下であることを確認する。

(4-2-1) 図面等で 2 故障許容設計を確認する。

(4-2-2) 機能試験等で故障許容設計が有効であることを確認する。

付録 A　用語の定義

(1) セル

正負極板、セパレータ、電解液、容器で構成されたもので、バッテリの構成要素の一つ

(2) バッテリ

一つ又は複数のセルに制御回路を付加しパッケージングしたもの

(3) PTC (Positive temperature coefficient)

PTC 素子は温度変化に対する抵抗変化の大きい素子であり、ある温度に達すると抵抗が無限大となり、電流を停止させる機能を備えている。

(4) UN 勧告

「国際連合危険物輸送勧告」。「危険物輸送に関する勧告」ともいう。

国際間の危険物の陸海空の安全輸送確保のため、危険物輸送専門家委員会が策定した危険物の国際間輸送基準。

(5) UL(Underwriters Laboratories Inc.）

アメリカ合衆国の安全認証機関。

材料･部品･装置・道具類などから最終製品まで、機能と安全性の規格基準を設定し、同時に評価方法を策定、実際に評価試験を実施する。これらの試験に合格した際には、UL 認証マークの使用を認める。

(5) JAXA 開発完了セル

JAXA の開発完了コンポーネントに登録されている宇宙用リチウムイオン電池。

5.5 射場における電波誤放射ハザードの防止　解説

１．目的

「5.5 射場における電波誤放射ハザードの防止」は国内法規「電波防護指針」等の法規に基づいている。電波放射に関連する安全解析において、法規の適合性評価について解説する。
本資料の対象は、以下に該当する人工衛星に搭載される電磁放射源に限定する。

- 電磁放射源の周波数300MHz 以上（アマチュア無線帯、S バンド・K バンド帯等が主な対象）
- 射場作業における電磁放射源の運用

また本解釈は、心臓ペースメーカ装着者等への電磁放射曝露は対象外である（国内法規「電波防護指針」においても心臓ペースメーカ装着者は対象外となっている）。心臓ペースメーカ装着者等への電磁放射曝露の可能性がある場合は、別途検討すること。
なお、本解釈の通りではない他の方法で安全を確保することを妨げるものではない。
＜背景＞
過去の安全審査部会において、ハザードの被害の度合い（I, II, III）の閾値の具体化について議論があった。そのため、安全距離の算出とそれに関連した被害の度合いの判断基準を整理する必要があった。

２．根拠

２．１ 本書の適用範囲

5.5項の評価方法は、主に熱的影響を考慮したものである。防護指針では、接触電流、誘導電流等の人体への刺激作用を防止するための指針も示されているが、本資料で扱う300MHz以上の周波数帯では、これらは評定とならない。（平成2 年防護指針 3.1.1 項）

２．２ ステップ1 A)の根拠

ステップ1 A)では、小型衛星等の安全評価を行ううえでのスクリーニングを意図している。スクリーニングの閾値を算出するにあたり電波防護指針の電磁波強度指針等を用いると、条件によっては出力許容値が基礎指針から算出した数値より厳しい数値となる場合もある。一方、ステップ 1 A)では、電波防護指針の考え方の根拠である基礎指針を用いることで最低限守るべき許容値を閾値とする方針とし、電磁波強度指針等を満足できなくても基礎指針を満足できれば低電力の電磁放射源としてみなした。
なお、基礎指針のうち一つは全身平均比吸収率（SAR : Specific Absorption Rate）を基準としており、アンテナの種類等によらず、アンテナからの出力のみに注目できる利点もあるため、閾値として採用した（電磁波強度指針等を用いるとアンテナの種類や利得等を考慮する必要があり、アンテナ毎にユニークな判断が必要なため）。

(1) ステップ1 A)の6GHzの根拠

基礎指針4.b によると、6GHz 以上の帯域においては、眼への入射電力密度（6 分間平均）が10mW/cm2 以下であることの考慮が必要である。一方、6GHz 未満の電磁放射源では、眼への入射電力密度は特別に考慮する必要はなく、基礎指針1 の全身SAR：0.4W/kg（6 分間平均）を適用すればよい。よって、6GHz 以上の電磁放射源は、空中線電力だけでなく利得も考慮した閾値となり、ステップ1 A)ではハザードの度合いの識別はできない。そのため、6GHz 以上の電磁放射源はステップ1 B) C)でハザードの度合いの識別をする。

注：平成23年 諮問第2030号「局所吸収指針の在り方」に関する答申により、局所吸収指針の対象が6GHzまで拡張された。ここで規定される全身平均SAR、局所SARともに、従来の100kHz～3GHzまでの基準値が100kHz～6GHzまで適用されることとなったため、閾値を従来の3GHzから6GHzに修正した。

(2) ステップ1 A)の電磁放射源からの距離10cm の根拠
10cm の規定は、「平成9 年 防護指針 4.2 (3)項」局所吸収指針の適用される空間の定義より設定した。射場作業環境は、電波防護指針における「管理環境（職場環境）」が適用できるため、これに基づき以下の評価により電磁放射源の出力を設定した。

(3) ステップ1 A)の20W の根拠
電磁放射源から10cm 以上の空間の評価は、基礎指針に基づいて評価した。アンテナから数波長の距離があると、全身暴露の条件で評価できるため、基礎指針の全身SAR：0.4W/kg（6分間平均）が適用できる。50kgの人間を想定すると、20W（=0.4 [W/kg] x 50[kg]）まで許容できる。なお、これはアンテナ全出力の暴露であるため、安全側の評価となっている。

２．３ ステップ1 B) C)の根拠

防護指針の適用手順は以下である（平成2 年防護指針, 3.1.5 項、平成9 年防護指針4.2 項）。ステップ1 B) C)は、この考えに適合させている。

１、 ステップ1 B) C)で示される安全距離算出の評価順序
電波利用の実情が認識されていると共に、防護対象を特定することができる状況下にあり、注意喚起など必要な措置の対応が可能な場合は管理環境、これが満たされない場合は一般環境として扱う。ステップ1 B) C)で示した以下の評価順序は、「平成2 年電波防護指針 3.1.5 防護指針の適用手順」の考え方を引用した。

(1) 電磁放射源より十分遠方（対象とする空間の電磁界が均一）である場合、電磁界強度指針 一般環境(条件G)における電磁界強度を適用した評価を行う。

(2) (1)が満たされない場合、電磁界強度指針 管理環境(条件P)における電磁界強度に基づき評価する。

一般環境は、防護指針に照らした管理が十分になされてない等の環境に適用される。この環境では、一般的に測定が頻繁に行なわれるわけではなく、測定点が十分に網羅されていなかったり、電波を散乱する周辺の物体や建物などの状況が変化すること等によって、放射源が変わらなくても電磁界強度が2 倍程度まで変化することが想定される。一般環境では、このような不確定さを考慮し、管理環境に比べて電力密度で5 倍（電界強度又は磁界強度で2.23 倍）の安全率を付加的に考慮されている（平成2 年防護指針，付録１, 2.1.2 項）。
射場作業では管理環境に基づく評価によることもできるが、射場のユニークな作業環境における反射波などを考慮した煩雑な評価を回避するため、先ず一般環境に基づく評価を実施する。

(3) 対象とする空間の電磁界が不均一又は近傍界である場合、「電波防護指針 II.補助指針 (1) 人体が電磁界に不均一又は局所的にさらされる場合の指針」を適用した評価を行う。
安全距離が数十ｃｍ前後となると、全身暴露を主に考慮した電界強度指針は実質適用とならず、電波が不均一／局所的にさらされる場合の「補助指針」が主な評定となる。人工衛星で搭載される電磁放射源の射場での扱いを考慮すると、この場合に電磁放射源にさらされる人体の部位は四肢であると考えられる。なお、6 分以上電磁放射源近傍に滞在し続ける作業は想定できない。

(4) 上記管理指針が満たされていない場合、基礎指針に基づき評価を行う。
表1 に、関連する指針を示す。仮に、電磁放射源からの安全距離(電力密度が1mW/cm2 となる距離)が50cm であっても、それ以内では基礎指針（体表と四肢に対し25 W/kg）を満足できれば良い。仮に25cm まで接近すると電力密度は4mW/cm2 であるため、作業員の四肢の表面積を考慮すると基礎指針（25 W/kg）を超えることはない。

表 1 本書の対象とする周波数帯で最も条件が厳しい周波数：3GHzにおける電波防護指針（6 分間平均）

	電界強度指針	補助指針		局所吸収指針	基礎指針	
		体表	眼	四肢	体表と四肢	眼
条件 G/一般環境	1 mW/cm2	4 mW/cm2	2 mW/cm2	4 W/kg	25 W/kg	10 mW/cm2
条件 P/管理環境	5 mW/cm2	50 mW/cm2	10 mW/cm2	10 W/kg		
備考		（四肢以外の指針のため参考）		（携帯端末向け指針のため参考）		（参考）

２、ステップ1 B) b. 1.4mの根拠
ステップ1 B) b.で示される安全距離の閾値1.4m は、ステップ1 A)の電磁波放射源出力の許容

値20W を用いて次の条件（利得G=1 倍、反射係数K=2.56(大地面の反射を考慮し、送信周波数が 76MHz 以上の場合)、許容電力密度 0.2 mW/cm2）で算出した。この安全距離から逆算した場合、条件によってはステップ1 A)で示した許容出力値を超えるアンテナ出力の場合も許容されることになるため、「偶発的なアクセス」に制限することで限定・局所的ハザードとみなせる。

２．４ ステップ2 の根拠

破局ハザードの閾値は全身平均SAR：4W/kg@６分間平均とする。これは米国等のラット実験の結果、生体に影響がでた値（4～8W/kg）のワースト値である（平成2 年 防護指針 付録 1, 1.1 項が根拠）。基礎指針の0.4W/kg は、この値に安全係数等を加味した値である）。これより、50kg の人員であれば、200W（4W/kg × 50kg = 200 W）の電波放射（6 分平均）であれば破局ハザードとする。

電磁波の曝露時間を制限することにより、電磁放射源の出力の許容値を緩和することができ、ハザード制御の一部とすることができる。

電磁放射源の周波数が300MHz 以上であれば、人体に対する熱作用が支配的である。指針の規定は、6 分間平均の電波暴露時に人体の深部体温が約1 度上昇する等の影響を考慮したものであるため、熱作用の観点では電波への暴露はタイムクリティカルな事象ではない。また、防護指針の規定には安全係数等が考慮されているものであるため、電波の強さが、防護指針を超えたからと言って、それだけで直ちに健康に影響があるものではないとの記述がある（平成9 年防護指針 6.2 (1)）。よってある程度の時間内に退避することができれば人員の死亡に至るレベルではないため、ハザード制御とみなせる。

３．関連文書

本書は、主に以下に基づいて作成した。

諮問第38号「電波利用における人体の防護指針」（平成2年6月）

諮問第89号「電波利用における人体防護の在り方」（平成9年4月）

上記指針は、多くの文献、海外法規の調査の結果、纏められたものである。

また、本書は専門家との討議による知見も反映している。

付録A： 用語の説明 （「平成9 年度 電波防護指針」からの抜粋）

(1) 電波防護指針

電波利用において人体が電磁波（周波数の範囲は10kHz から300GHz までに限る。）にさらされるとき、その電磁波が人体に好ましくないと考えられる生体作用を及ぼさない安全な状況であるために推奨される指針のことをいう。

(2) 基礎指針

人体が電磁界にさらされるとき人体に生じる各種の生体作用（体温上昇に伴う熱ストレス、

電流刺激、高周波熱傷等）に基づいて、人体の安全性を評価するための指針をいう。

(3) 管理指針

基礎指針を満たすための実測できる物理量（電界強度、磁界強度、電力密度、電流及び比吸収率）で示した、実際の評価に用いる指針のことをいう。管理指針はさらに電磁界強度指針、補助指針及び局所吸収指針から構成される。

(4) 電磁界強度指針

対象とする空間における電界強度、磁界強度、電力密度によって、当該空間の安全性を評価するための指針をいう。

(5) 局所吸収指針

主に身体に極めて近接して使用される無線機器等から発射される電磁波により、身体の一部が集中的に電磁界にさらされる場合において、基礎指針に従った詳細評価を行うために使用する指針をいう。

(6) 補助指針

電磁界強度指針を満足しない場合において、基礎指針に従った詳細評価を行うために使用する指針をいう。電磁界にさらされる状況（不均一、局所、表面など）、対象とする生体作用（接触電流及び誘導電流）、電波発射源の属性（空中線電力及び周波数帯）が明らかな場合、これらの状況に基づき電磁界強度指針の適用を緩和又は除外する形で表した指針である。

(7) 管理環境

人体が電磁界にさらされている状況が認識され、電波の放射源を特定できるとともに、これに応じた適切な管理が行える条件を指す。

(8) 一般環境

人体が電磁界にさらされている状況の認識や適正管理等が期待できず、不確定な要因があるケース（環境）を指す。一般の居住環境等において住民が電磁界にさらされているケース等がこれに該当する。

このため適用する指針においては一般環境は管理環境に比べ厳しい値となっている。一般環境は、平成２年の電波防護指針の条件Ｇに該当する。

(9) 比吸収率（SAR：Specific Absorption Rate）

生体が電磁界にさらされることによって単位質量の組織に単位時間に吸収されるエネルギー量をいう。

SAR を全身にわたり平均したものを「全身平均ＳＡＲ」、人体局所の任意の組織1g または 10g にわたり平均したものを「局所ＳＡＲ」という。

(10) 遠方界

電磁波源からの距離が、2D2/λ又はλ/2πのいずれよりも遠い領域にあり、反射又は散乱がない状態の電磁界をいう。ここで、D はアンテナの最大寸法、λは自由空間波長とする。

付録B： 電波防護指針の各指針（「平成2 年度 電波防護指針」、「平成9 年度 電波防護指針」からの抜粋）

・基礎指針 （平成2 年防護指針 3.3 項 表5）

1 全身平均 SAR の任意の6分間平均値が、0.4W/kg 以下であること。
2 10kHz から 100kHz までの周波数では、組織内の誘導電流密度が 0.35 ×10−4f[Hz]mA/cm2 以下であること。
3 10kHz から 100kHz までの周波数では、接触電流などが体外からの流入電流が 10−3f[Hz]mA 以下（平均時間＜1秒間）であること。また、100kHz から 100MHz までの周波数では、100mA 以下(平均時間6分間)であること。
4 上記の(1)(2)及び(3)に加え、次の点に関して注意事項として考慮すること。
(a) 全身平均 SAR の任意の6分間平均値が 0.4W/kg 以下であっても、任意の組織 1g 当りの SAR（6分間平均値）が 8W/kg（体表と四肢では 25W/kg）を超えないことが望ましい。
(b) 3GHz 以上の周波数においては、眼への入射電力密度(6分間平均)が 10mW/cm2 以下とすること。

・管理指針 （平成 9 年防護指針）

I. 電磁界強度指針

表1：管理環境（条件P）における電磁界強度（平均時間6分間）の指針値

周波数 f	電界強度の実効値 E [V/m]	磁界強度の実効値 H[A/m]	電力束密度 S[mW/cm^2]
10kHz～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)	
30MHz～300MHz	61.4	0.163	1
300MHz～1.5GHz	3.54f[MHz]$^{1/2}$ (61.4 − 137)	f[MHz]$^{1/2}$／106 (0.163 − 0.365)	f[MHz]／300 (1 − 5)
1.5GHz～300GHz	137	0.365	5

表2：一般環境（条件 G）における電磁界強度（平均時間6分間）の指針値

周波数 f	電界強度の実効値 E [V/m]	磁界強度の実効値 H[A/m]	電力束密度 S[mW/cm^2]
10kHz～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)	
30MHz～300MHz	27.5	0.0728	0.2
300MHz～1.5GHz	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)
1.5GHz～300GHz	61.4	0.163	1

II. 補助指針

(1)人体が電磁界に不均一又は局所的にさらされる場合の指針

<table>
<tr><td></td><td>10kHz–300MHz</td><td>300MHz–1GHz</td><td>1GHz–3GHz</td><td>3GHz–300GHz</td></tr>
<tr><td>電磁界強度の空間的平均値</td><td colspan="4">管理環境：表 1　適用
一般環境：表 2　適用</td></tr>
<tr><td rowspan="2">電磁界強度の空間的最大値</td><td></td><td colspan="2">四肢以外：
管理：20mW/cm^2
一般：4mW/cm^2</td><td>体表：
管理：50mW/cm^2
一般：10mW/cm^2</td></tr>
<tr><td></td><td></td><td>頭部：
管理：10mW/cm^2
一般：2mW/cm^2</td><td>眼：
管理：10mW/cm^2
一般：2mW/cm^2</td></tr>
<tr><td>適用する空間</td><td>電磁放射源、金属物体から 20cm 以上離れた人体の占める空間</td><td colspan="3">電磁放射源、金属物体から 10cm 以上離れた人体の占める空間</td></tr>
<tr><td>平均時間</td><td colspan="4">6分間</td></tr>
</table>

III 局所吸収指針

適用範囲：　本指針は、周波数 100kHz から 3GHz までに適用できる。

対　　象：　身体に近接して使用する小型無線機等に適用できる。

主に、周波数 100kHz 以上 300MHz 未満で、電磁放射源との距離 20cm 以内

周波数 300MHz 以上 3GHz 未満で、電磁放射源との距離 10cm 以内

	管理環境	一般環境
全身平均SAR	0.4W/kg	0.08W/kg
局所SAR	任意の組織 10g 当たり 10W/kg 20W/kg（四肢）	任意の組織 10g 当たり 2W/kg 4W/kg（四肢）

6　ハザード解析によらない固有の安全設計要求　解説

ペイロードからの推進薬や酸化剤等（ヒドラジン、MMH、MON3、NTO等）の漏洩等の異常時に備えて、減圧・推進薬や酸化剤等排出を安全に実施するための要求であり、これはハザード解析の結果、推進薬や酸化剤等の漏洩に対して2故障許容設計が成立したとしても、なお微小漏洩の可能性は排除できないという過去の議論から、緊急時の追加対策を求める、ハザード解析によらない固有の安全設計要求である。

JMR-002C版までは、ロケットに搭載した状態において減圧・推進薬や酸化剤等排出両方を実施できる設計とする必要があったが、JMR-002D版においては、ロケット搭載状態で減圧を実施できれば、推進薬や酸化剤等の漏洩量が低減され安全に移動できると想定されることが整理されたため、推進薬や酸化剤等の排出場所については選択（ロケット搭載状態のまま、または衛星整備エリアへ返送後など）できるようになった。

JMR-002E版においては、さらに、米国および仏国における実態、ユーザからの声を考慮し、減圧についてもより柔軟な運用が可能になるよう、減圧を“ロケット搭載状態”にて実施すべきという記載を削除した。これにより、減圧場所についても（ロケット搭載状態のまま、または衛星整備エリアへ返送後など）選択できるようになった。ロケット搭載状態において実際に減圧作業が発生した場合、作業者が、推進薬や酸化剤等が漏洩した状態のフェアリング内にダイビングボードで侵入し、減圧するという危険度が高い作業が予想され、このような作業を暗に求めるような要求は避けるべきという意見も、改定理由の1つである。E改定によって、減圧・推進薬や酸化剤等を排出する場所や手順はPL担当組織が選択できることになり、従来はロケット搭載状態で人がアクセスできる方向にペイロードの減圧ポートを設ける設計上の制約があったが、衛星整備エリアに移動してから減圧することが安全上可能であれば、この設計上の制約は無くなる。

ペイロードがロケットに搭載された状態で推進薬や酸化剤等が漏洩した場合の実際の作業手順は、ロケットの設計や運用に依存するため、各ロケットに実現性について確認する必要がある。

様式１　安全要求に関するテーラリング申請書

１．題名	番号 年　月　日	ペイロード担当組織名称	
２．(1)対象のペイロードの名称 (2)サブシステムの名称	実施責任者	汉安ﾌﾟﾛ責任者*	作成
３．　テーラリングの対象となる適用文書名･文書番号とその安全要求の項番号			
４．テーラリング内容と適用文書の安全要求内容及び対応策の比較 4.1安全要求内容の比較（テーラリング有りと無しの比較） 4.2安全要求に基づく安全対策（ハザード制御）内容の比較（テーラリング有りと無しの比較） （本欄で不足の場合は次葉以降に適宜追加のこと）			
５．テーラリングを必要とする理由 （本欄で不足の場合は次葉以降に適宜追加のこと）			
６．同等の安全を確保できる理由の説明 （本欄で不足の場合は次葉以降に適宜追加のこと）			
判定：　承認　コメント付承認　再検討　（選択）			機構／安全部門
理由･コメント等：			年　月　日

注）本書はシステム安全プログラム計画書の一部をなし、記載内容はシステム安全プログラム計画書の安全審査の中で審査される。なお､内容については事前に機構の安全部門と調整・確認のこと。

＊：汉安ﾌﾟﾛ責任者；システム安全プログラム責任者

様式 1　安全要求に関するテーラリング申請書

１．題名 ＜テーラリングの題名＞　（続き）	番号
２．(1)対象のペイロードの名称　　(2)サブシステムの名称	

様式2　ハザード識別まとめ表

システム名　　：＿＿＿＿＿＿＿＿

サブシステム名：＿＿＿＿＿＿＿＿

ハザード カテゴリ	火災・爆発							破裂		毒性物質の漏洩						放射																									
ハザード原因 / システム サブシステム コンポーネント 又は ハザーダスアイテム 又は、作業工程名称	点火源等の存在	レーザ(JIS C 6802(IEC 60825-1)クラス4	静電気	火薬類（固体推進薬・火工品）	錆等	可燃性の液体推進薬	可燃物・酸化剤の混合	圧力システム・圧力容器	リチウムイオンバッテリ	結合部のゆるみ・配管等の破損	シール劣化・へたり・弁機能不良	流体適合性不良	バルブ等の異物噛み込み	毒性物質搭載タンク吊上時の落下	病原菌等	電波	電離放射線・放射性物質																								
ﾊｻﾞｰﾄﾞﾚﾎﾟｰﾄNO.																																									

注意：以下の事項等によって、事故が発生する可能性も考慮して、ハザードを識別すること。
- 人的過誤（ヒューマンファクタ）
- ソフトウェアエラー（入力ミス・バグ）
- 危険作業（危険物、有害物質、高圧ガス、火薬類等取扱い、重量物運搬）

<被害の度合い>
- Ⅰ　破局　：死亡・重度の人的被害／深刻な環境への影響／公共の財またはサービス、第三者財産の喪失や重大な損害／ＪＡＸＡ射場施設・設備等の喪失
- Ⅱ　重大　：軽度の人的被害／重大な環境への影響／公共の財またはサービス、第三者財産の軽度の損害／ＪＡＸＡ射場施設・設備の重大な損傷
- Ⅲ　限界・局所的　：軽微な人的被害／公共の財またはサービス、第三者財産の私有財産の軽微な損害／軽度の環境への影響
- Ⅳ　無視可能　：Ⅰ～Ⅲをもたらさない程度のもの

(注) 空欄にはシステムの特性に応じて必要なハザードを追記すること

様式3　ハザード解析表

No.	ハザードタイトル	ハザード概要	ハザード原因	対応策	被害の度合い	発生の可能性	備考 (HR No)
1							
2							
3							
4							

注）ハザードレポートを作成したハザードに対してはハザードレポート番号（HR　No）も記載のこと。
なお、発生の可能性の記載はフェーズⅠ以降でよい。
被害の度合いや発生の可能性が分かるようにハザード概要と制御を記載し、その根拠とすること。
被害の度合いを低減をした場合には、その対応策の欄で説明すること。

様式4　安全検証追跡ログ(SVTL)

ページ　／

システム等の名称；

作成/改訂日；

ログ番号	ハザードレポート番号	安全検証番号	検証アイテム／検証確認方法	射場等の運用に対する制約	完 了予定日	完了日	検証確認結果	備考（手順書番号／タイトル）

様式5　ハザードレポート

<table>
<tr><td colspan="2">ハザードレポート</td><td colspan="2">ハザードレポート番号</td></tr>
<tr><td>システム名</td><td>日付</td><td>作成／改訂</td></tr>
<tr><td>サブシステム名</td><td colspan="2">プログラムフェーズ</td></tr>
<tr><td colspan="3">ハザードタイトル</td></tr>
<tr><td>適用される安全要求</td><td colspan="2">ハザードの分類

被害の度合い：
□Ⅰ　□ Ⅱ　□ Ⅲ　□Ⅳ

発生の可能性：
□A　□B　□C　□D　□E</td></tr>
<tr><td colspan="3">ハザードの概要</td></tr>
<tr><td colspan="3">ハザード原因</td></tr>
<tr><td colspan="3">ハザード制御方法</td></tr>
<tr><td colspan="3">安全検証方法</td></tr>
<tr><td colspan="3">安全検証ステータス</td></tr>
</table>

様式5　ハザードレポート

ハザードレポート（　続　き　）	ハザードレポート番号
システム名／サブシステム名	

様式 6　安全要求適合性詳細検討書(NCR)

<table>
<tr><td colspan="2">適合性詳細検討項目名称</td><td>番号</td><td colspan="2">日付</td></tr>
<tr><td colspan="2" rowspan="2">ペイロードの名称</td><td colspan="3">PL担当組織の名称、部門名</td></tr>
<tr><td>開発実施責任者</td><td>システム安全
プログラム責任者</td><td>作成</td></tr>
<tr><td>処置；</td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="5">適用する安全要求</td></tr>
<tr><td colspan="5">要求事項に合致できない内容</td></tr>
<tr><td colspan="5">安全要求に合致できない理由

（本欄で不足の場合は添付等で説明のこと）</td></tr>
<tr><td colspan="5">安全要求対象ハザードへの対応策　（対応するハザードレポートの番号；　　）

（本欄で不足の場合は添付等で説明のこと）</td></tr>
<tr><td colspan="4">判定</td><td>機構／安全部門

年　月　日</td></tr>
</table>

・補足資料、データ等を添付のこと。