JMR-001B

システム安全標準

平成　２０年　　３月　２７日　B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。）が研究開発及び受託するシステム、サブシステム及びコンポーネント等（以下、「システム等」という。）に関係する事故等から人命、財産及びシステム等を守るとともに環境を保護するため、システム等に係るハザードを識別し、設計、製造・試験及び運用段階を通じて適切な手段によりハザードを除去、又は最小化及び制御して安全を確保するよう、機構において研究開発及び受託を行う部門（以下、「機構担当部門」という。）並びに契約の相手方（受託及び共同研究開発する場合の契約、協定等の相手方を含む。以下、「契約の相手方」という。）が実施すべき標準的な要求事項について規定することを目的とする。

１．２　範囲

１．２．１　適用

機構担当部門及び契約等に定める場合の契約の相手方は、法令及び機構の安全規程類の遵守のみで安全を確保できる場合を除き、機構の研究開発（契約の相手方に委託等を行う場合を含む。）又は受託するシステム等に関して本標準を適用すること。また、本標準に準拠するシステム安全プログラム計画書を作成し、必要な安全審査を受けてシステム安全活動を実施すること。

１．２．２　実施部門の責任

機構担当部門及び契約の相手方は、安全に係わる法令による規定を順守するとともに、本標準に準拠して安全を確保するために必要な処置をとる責任を有する。

１．２．３　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、対象とするシステム等の特徴、特性に応じて修整して適用することができる。機構担当部門は事業計画書等で定めるシステム安全審査のレベルに応じて機構担当部門の属する本部等の安全部門（安全部門のない本部については安全・信頼性推進部）及び安全・信頼性推進部（以下、これらを「安全部門」という。）と修整部分及び修整理由について協議し、システム安全プログラム計画書に反映し機構の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（安全設計要求、運用安全要求及びスペースデブリ要求）事項は対象とするシステム等の特徴、特性に応じて修整して適用することができる。機構担当部門は機構安全部門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表 1.2.3-1 の様式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機構の安全審査で承認を受けること。

２．関連文書

２．１　適用文書

本標準に規定される範囲で以下の文書を適用する。適用文書は最新版を使用することとし、それによりがたい場合は安全・信頼性推進部と協議すること。

(1) NPR8715.3　NASA Procedual Requirements NASA General Program Requirements Chapter 2, System Safety

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

(3) JMR-002　ロケットペイロード安全標準

(4) JMR-003　スペースデブリ発生防止標準

(5) JERG-1-007　射場・飛行運用安全技術基準

(6) JERG-1-006　ロケットシステム開発安全技術基準

３．用語の定義

本標準で使用する用語の定義を付属書Ｉに示す。

４．要求事項

４．１　基本要求事項

機構担当部門､及び調達仕様書等で指定された範囲において契約の相手方は､システム等の設計、製造・試験及び運用段階を通じてシステム安全を実施するため、有効なシステム安全プログラムを初期段階に計画し、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､的確に機能するシステム安全管理組織（4.2.3 項）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全ライフサイクルを通じて識別、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各段階で確認すること。（4.3.2 項）

(3) ハザードを制御するため安全要求を設定するとともに､各ハザードに対してその原因を把握し、各原因毎に対応策（4.3.1 項）を講じること。

(4) 安全設計を試験等により検証すること。（4.3.3 項）

(5) 作業手順書等に必要な安全手順が確実に盛り込まれていること､及び作業がこれらの手順書等に基づいて完全に実施されていることの確認を行うこと。（4.2.4 項）

(6) システム安全プログラム活動の成果を文書化すること。（4.4 項）

(7) 安全データを維持／管理すること。（4.4 項）

(8) 以上を踏まえ、システム安全を実施するための効果的なシステム安全プログラム計画書（4.2.1 項）を作成すること。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、監査、作成文書の提出時期、及び必要に応じ教育・訓練計画を明確にすること。

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

機構担当部門及び調達仕様書等に指定された範囲において契約の相手方は、本標準の要求を満足する「システム安全プログラム計画書」を作成すること。システム安全プログラム計画書は、機構担当部門にあっては安全部門の、契約の相手方にあっては機構担当部門の安全審査を受けること。機構担当部門に対する安全審査は機構の規程によること。

機構担当部門及び契約の相手方は、システム安全プログラム計画書を常に最新化すること。

(1)　システム安全プログラム計画書の構成は表 4.2.1-1 を標準とし、安全審査を受けること。

(2)　契約の相手方のシステム安全プログラム計画書は、NPR8715. 3、MIL-STD-882 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。

表 1.2.3-1(1/2)　安全要求に関するテーラリング申請書　様式（1）

<table>
<tr><td colspan="2">1．題名</td><td>番号

年　月　日</td><td colspan="3">ｼｽﾃﾑ等の担当組織名称</td></tr>
<tr><td colspan="2" rowspan="2">2．(1)対象システム等の名称

(2)サブシステムの名称</td><td>実施責任者</td><td>ｼｽ安ﾌﾟﾛ責任者*</td><td>作成</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td colspan="5">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</td></tr>
<tr><td colspan="5">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）</td></tr>
<tr><td colspan="5">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）</td></tr>
<tr><td colspan="5">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）</td></tr>
<tr><td colspan="2" rowspan="2">判定：承認　　コメント付承認
再検討　　（選択）
理由･コメント等：</td><td>機構／安全部門</td><td colspan="2">機構担当部門</td></tr>
<tr><td></td><td>担当部門責任者</td><td>ｼｽ安ﾌﾟﾛ責任者*</td></tr>
<tr><td colspan="2"></td><td>年　月　日</td><td>年　月　日</td><td>年　月　日</td></tr>
</table>

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。

＊：ｼｽ安ﾌﾟﾛ責任者；システム安全プログラム責任者

表 1.2.3-1(2/2)　安全要求に関するテーラリング申請書　様式（２）

１．題名（続き）	番号
２．(1)対象のシステム等の名称　　(2)サブシステムの名称	

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	契約の相手方は以下を追加する。 1.3　契約上の他の要求事項との関係 1.4　契約者の責任 1.5　機構の行為	
2.　関連文書 適用文書、参考文書を示す。		
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。 (2) 関連部門を含め、システム安全管理組織を図示する。 (3) 契約品目を含む場合、契約の相手方に実施させる部分と機構担当部門が実施する部分との関係を明確にする。	機構の場合、関連部門とは機構担当部門、安全部門を指す。 供給業者と直接取引する場合は、そのシステム安全プログラム管理についても記述する。	4.2.3
3.2　システム安全審査の方法		4.2.4
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。 (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。		表 4.2.4-1 図 4.2.2-1
3.4　ハザード識別		4.3.2.1
3.5　リスク評価		4.3.2.2
3.6　ハザード解析		4.3.2.3
3.7　安全要求 (1) 適用文書等（システム等が該当する場合、JMR-002 の 5 章、JERG-1-007 の 4 章、JMR-003 の 5 章、JERG-1-006 等の適用を含む） (2) 適用文書に対する明確な非該当項目、事前調整によるテーラリング項目等（*） (3) ハザード解析に基づく追加要求 官庁への法定手続きを実施する場合の国内法規対応方法　等		4.2.2 等
3.8　安全検証		4.3.3
3.9　教育・訓練		4.2.6
3.10　監査		4.2.7
3.11　報告		4.2.8
3.12　事故等の調査と報告		4.2.9
4.　作成文書及び安全データ		4.4

＊：テーラリング項目がある場合は、表 1.2.3-1 の様式でその内容等を示すこと。

４．２．２　システム安全プログラム活動

機構担当部門及び契約の相手方は、システム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を示す。

システム安全プログラム活動は概念設計／計画決定段階の初期から開始すること。

(1) 概念設計／計画決定段階（フェーズ０）

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. フェーズ０ハザード解析を実施し、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の識別及び対応策の検討を行い、その結果に基づき JMR-002 の 5 章、JERG-1-007 の 4 章、JMR-003 の 5 章、JERG-1-006 等（テーラリングがある場合にはそれを含むこと。）の他に追加すべき安全要求の設定を行うこと。

（注；「ハザードの識別」は全フェーズに一貫して実施するので、4.3.2.4 項及び表 4.3.2.4-1 のハザード識別まとめ表を設計の初期段階から作成し、設計の進捗に従って改訂していくこと。）

c. 安全要求適合マトリクスを作成し、システム等の設計、製造・試験、及び運用の計画が安全要求に合致していることを確認すること。表 4.2.2-1 に安全要求適合マトリクスを示す。

d. フェーズ０ハザード解析で調査／検討した結果は文書化し、概念／予備設計に反映させること。

(2) 基本設計段階（フェーズⅠ）

a. 本フェーズの初期にフェーズ０ハザード解析の結果を見直し、必要に応じて安全要求の詳細化を行うこと。

b. フェーズⅠハザード解析を実施しハザードを識別し、影響の及ぶ範囲や対応策について検討を行い、その結果に基づき詳細な安全要求の見直し、及び安全要求適合マトリクスの改訂を行うこと。

c. フェーズⅠハザード解析で調査／検討した結果は文書化し、基本設計に反映させること。

d. 必要に応じ、システム安全プログラム計画書の維持／改訂を行うこと。

(3) 詳細設計段階（フェーズⅡ）

a. フェーズⅡハザード解析を実施し、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とともに、安全の詳細評価を行うこと。また、設計の基本的及び詳細な安全要求との適合性を確認すること。

b. フェーズⅡハザード解析で検討した結果は文書化し、詳細設計に反映させること。

c. 必要に応じ、ハードウェア、ソフトウェアによる安全に係る確認試験、操作、運用に関する提案及び安全要求適合マトリクスの改訂を行うこと。

d. 必要に応じ、システム安全プログラム計画書の維持／改訂を行うこと。

e. 安全要求適合性については設計審査において確認されるが、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。もし、どうしても適合できない場合には、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を作成し、その内容について機構担当部門にあっては機構の安全審査組織、契約の相手方にあっては機構担当部門と協議し、機構の安全審査で承認を得ること。

(4) 製造・試験段階（フェーズⅢ）

a. 必要に応じ、フェーズⅡハザード解析の結果を見直すこと。

b. 製造、試験及び射場等の運用に係る作業手順書等を作成し、維持／改訂を行うこと。

c. 製造、試験及び射場等の運用でハザードを有する工程について、作業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。

d. ハザードが新たに識別された場合は、信頼性プログラム及び品質プログラムと協調して調査／検討を行い、必要な是正措置を行うこと。

e. フェーズⅢハザード解析を実施し、ハザード制御の検証結果を明確化すること。また、解析結果に基づき運用に係る下記事項を含む作業手順書等を作成するとともに、作業手順書と詳細な安全要求との適合性を確認すること。

（ⅰ）安全装置、設備に対する要求事項、それらの機能欠陥を検出するのに必要な保全手順

（ⅱ）運用及び保全時の警告、注意、特別手順並びに緊急処置

（ⅲ）取扱い、貯蔵、輸送及び保全の手順

f. 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結果の確認を現地でしかできないものは、安全検証追跡ログ（表 4.2.4-2、又は同等な様式）に記載し、フォローして運用前にクローズすること。

g. 必要に応じ、システム安全プログラム計画書の維持／改訂を行うこと。

(5) 運用段階

a. フェーズⅢハザード解析の結果を見直すとともに、必要に応じて射場等の運用作業手順書等を見直すこと。

b. 運用に係る安全について、システム安全プログラム計画書及び作業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。

c. ハザードが新たに識別された場合は、信頼性プログラム及び品質プログラムと協調して調査／検討を行い、必要な是正措置を行うこと。

d. 設計変更が行われた場合は設計段階からの要求が適用される。

４．２．３　システム安全管理組織

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) 機構担当部門の長及び契約の相手方の長はそれぞれ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。

なお、システム安全管理組織は、独立性を勘案するとともにシステム等の内容・規模に応じて設定することができる。

(2) 機構担当部門の長及び契約の相手方の長はそれぞれ、システム等の設計、製造・試験及び運用段階を通じてシステム安全に責任を持ち、システム安全に関する知識、経験を備えたシステム安全プログラム責任者をシステム等に応じて任命すること。

(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. 安全に係る重要な問題について、関係部門と調整し解決を図ること。

f. プロジェクト等の開発実施責任者に対し、システム安全プログラムに関する実施状況等の報告及び勧告を直接行えること。

g. 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／改定を阻止及び中止できること。

h. 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。

実施年月(西暦) / 開発段階 / システム安全プログラム活動		概念設計／計画決定（フェーズ０）	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	機構担当部門、契約の相手方	ｼｽﾃﾑ要求審査 ｼｽﾃﾑ定義審査 ▽ (SDR) ▽	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) ▽		
	機構審査	ﾌﾟﾛｼﾞｪｸﾄ移行審査 ▽ ｼｽﾃﾑ定義審査 ▽	▽		開発完了審査 ▽	最終確認審査 ▽	
システム安全プログラム計画書		作成 ▽	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	同左見直し				
			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	同左見直し(必要に応じ) ﾌｪｰｽﾞⅢﾊｻﾞｰﾄﾞ解析	同左見直し	
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・試験作業手順書等	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

表 4.2.2-1　安全要求適合マトリクス

(安全要求の文書名、改訂符号付き文書番号)		適合	不適合	N／A	プログラム名称；	
項目	要　求　事　項				結　果	備　考

４．２．４　安全審査

安全審査の目的は、システム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、制御方法、制御の検証方法、並びに検証結果の妥当性を評価することである。また、除去しきれないリスク（残存リスク）に対しては最小化の内容や許容性を評価することである。

機構は機構の規程に基づき安全審査を実施すること。

契約の相手方は以下により安全審査を実施すること。

(1) システム安全プログラム責任者又は選出された者が安全審査を主催し、システム等のシステム安全が適切に実施され、その実施目的が達成されていることを確認すること。

(2) システム等の各開発段階毎に、原則としてフェーズ０安全審査､フェーズⅠ安全審査､フェーズⅡ安全審査及びフェーズⅢ安全審査の４回に分けて実施すること。なお、システムの規模等により、各フェーズ安全審査はプロジェクト等と調整のうえ、統合して実施することができる。また、各フェーズ安全審査はプロジェクト等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。

(3) 安全審査実施要領を定め、それに基づき実施すること。

(4) 各安全審査の審査文書、議事録、アクションアイテム表、及び必要な補足説明資料等は安全データパッケージとして取り纏め､各安全審査終了後速やかにプロジェクト等へ提出すること。

なお、機構担当部門等は安全審査にオブザーバとして参加できるものとする。

また、表 4.2.4-1 に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、及び各開発段階での主要なシステム安全プログラム活動を示す。

４．２．５　安全要求適合性詳細検討書

システム安全プログラム活動（4.2.2 項）で作成した安全要求適合マトリクス（表 4.2.2-1）によってシステム等の安全要求に対して合致できない事項が識別された場合、要求事項に合致できない理由と代替方策及び安全要求の意図を保証しうる根拠等について安全要求適合性詳細検討書（様式は表 4.2.5-1 又は同等の様式による。）にその検討内容を示し、機構の安全部門と協議の上、機構の安全審査でデビエーション／ウェーバの承認を得ること。また、検討内容はハザードレポートに反映すること。

表 4.2.4-1　安全審査と各開発段階におけるシステム安全活動の概要

安全審査	審査実施時期	審査の主目的	審査文書（注２）	各開発段階での主なシステム安全活動
フェーズ０ 安全審査 （注１）	概念／予備設計完了時	ハザード及びハザード原因の確認 （表 4.3.2.3-1 ハザード解析表参照） 適用する安全要求の確認	システム／サブシステム・コンフィギュレーション及び運用に関する説明記述文書 システムについてのハザードの識別及び対応策の検討文書 安全要求（テーラリング、ハザード解析による追加要求がある場合にはそれを含む）	フェーズ０ハザード解析として ハザードの識別、その原因の識別及びその対応策の検討 （表 4.3.2.3-1 ハザード解析表参照）、安全要求の初期設定及び安全要求設定
フェーズⅠ 安全審査	基本設計審査時 （ＰＤＲ時）	ハザード及びハザード原因の確認 ハザード制御方法の確認 検証方法の確認 必要に応じて詳細化された安全要求の確認	システム／サブシステム・コンフィギュレーション及び運用に関する説明記述文書 安全上重要なシステム／サブシステムと運用に関し安全設計上の特徴、インヒビット等の独立性が識別できるスケマティック及びブロックダイヤグラムを含んだ説明記述文書 ハザードレポート取纏めにあたって実施したトレードオフスタディ及び特別な検討結果文書 ハザードレポート、補足資料及びＦＴＡ 詳細化された安全要求	フェーズ０ハザード解析結果を見直し、必要に応じて詳細な安全要求の設定 フェーズⅠハザード解析として ハザード識別 ハザード原因の識別 ハザード制御方法の検討 検証方法（概要）の検討 上記解析結果に基づき詳細化された安全要求の見直し
フェーズⅡ 安全審査	詳細設計審査時 （ＣＤＲ時）	ハザードの制御方法が設計上実現されていることの確認 検証方法の詳細が設定されていることの確認	システム／サブシステム・コンフィギュレーション及び運用に関する説明記述文書 安全上重要なシステム／サブシステムと運用に関し、安全上の特徴、インヒビット等が識別できるスケマティック及びブロックダイヤグラムを含んだ説明記述文書 ハザードレポート、補足資料及びＦＴＡ 詳細な安全要求 フェーズⅠ安全審査のアクションアイテムの処置状況文書	フェーズⅠハザード解析結果の見直し フェーズⅡハザード解析として ハザードの制御方法の詳細設計への反映 検証方法の詳細検討 必要に応じ、ハードウェア、ソフトウェアの安全確認試験 運用提案及び詳細な安全要求の見直し 安全検証が製造手順書及び試験手順書等に反映されていることの確認
フェーズⅢ 安全審査	機構の開発完了審査時	検証が完了していることの確認 アクションアイテムがすべてクローズしていることの確認	システム／サブシステム・コンフィギュレーション及び運用に関する説明記述文書 安全上重要なシステム／サブシステムとその運用の最終的なコンフィギュレーションを明確にする説明記述文書 製造が完了したシステムの安全上の特徴、及び独立のインヒビット／コントロールが識別できるスケマティック及びブロックダイヤグラムを含む ハザードレポート、補足資料及びＦＴＡ 解析、検査、試験及びデモンストレーション等安全検証データ （図面、解析書、試験報告書、製造記録等） 安全要求適合性詳細検討書 安全検証追跡ログ　（注３） フェーズⅡ安全審査のアクションアイテムの処置状況文書	製造及び試験結果のハザード検証との整合性評価／確認 安全検証が運用に係る作業手順書等に反映されていることの確認 デビエーション／ウェーバの処理状況の確認

注１）フェーズ０安全審査は、通常ワーキンググループミーティングの形式等で実施される非公式な安全審査でもよいが、機構の安全審査を受けること。

注２）審査対象文書の詳細は本表を基準に、契約の相手方にあっては機構担当部門と、機構担当部門にあっては安全部門と事前調整し決定のこと。

なお、審査対象文書は現フェーズの最新コンフィギュレーションに基づき作成／維持のこと。

注３）フェーズⅢハザードレポートに対する安全検証のオープン事項は表 4.2.4-2 又は、同等の様式に示す安全検証追跡ログに記録すること。

表 4.2.4-2　安全検証追跡ログ　様式　　ページ ___ ／___

システム等の名称;_____　　作成/改訂日 ;_____

ログ番号	ﾊｻﾞｰﾄﾞﾚﾎﾟｰﾄ番号	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）
1								
2								
3								
4								

表 4.2.5-1　安全要求適合性詳細検討書　様式

<table>
<tr><td colspan="2">適合性詳細検討項目名称</td><td colspan="2">番号</td><td>日付</td></tr>
<tr><td colspan="2" rowspan="2">システム等の名称</td><td colspan="3">機構担当部門／契約の相手方の名称</td></tr>
<tr><td rowspan="2">開発実施責任者</td><td rowspan="2">システム安全
プログラム責任者</td><td rowspan="2">作成</td></tr>
<tr><td>処置；
（該当する方に〇）</td><td>・デビエーション（適合）
・ウェーバ</td></tr>
<tr><td colspan="5">適用する安全要求</td></tr>
<tr><td colspan="5">要求事項に合致しない内容</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 rowspan="2">判定</td><td colspan="2">プロジェクトマネジャ等
実施責任者</td><td colspan="2">システム安全
プログラム責任者</td></tr>
<tr><td colspan="4">機構／安全部門</td></tr>
</table>

備考：契約の相手方の場合は機構担当部門へ、また機構担当部門の場合は安全部門へ提出すること。
　　補足資料、データ等を添付のこと。

４．２．６　教育・訓練

技術者、技能者、操作及び保安要員等が行う作業により人命やシステム等の安全が損なわれる恐れのある場合は、作業・操作及び支援作業に先立って教育・訓練を実施すること。

この教育・訓練は教育・訓練計画書に基づいて実施すること。

これらの教育・訓練では、次のことを考慮すること。

(1) 訓練を必要とする設備、作業、支援作業を識別すること。
(2) 資格の必要性の有無を明らかにすること。
(3) 教育・訓練計画には、次のことが含まれること。
  a. ハザードの種類、原因、予想される事故、防止策、抑制策
  b. 手順書、点検表、緊急措置手順等
  c. 安全装置、保護装置、監視、警報装置等の機能と操作
  d. 人的過誤（ヒューマンエラー）の防止策
(4) 教育･訓練参加者及び結果の記録を作成すること。

４．２．７　監査

システム安全プログラムの実施状況について監査計画書を作成し、それに基づいて監査を実施すること。

また、システム安全プログラムの適用を要求した供給業者に対して、監査を実施すること。

監査の実施に際しては、以下を考慮すること。

(1) 監査は実施要領書、手順書等を用いて行うこと。
(2) 監査はシステム安全プログラムに精通した者を含むチームにより実施すること。
(3) 監査はシステム安全プログラム活動の有効性を確認するため、文書、作業、品目等の審査を含むこと。
(4) 監査は定期的に実施すること。
  また、現状の作業を有効に評価するため、必要に応じて抜き打ち又は臨時監査を実施すること。
(5) 問題点及び不具合の是正に対する勧告を含んだ監査報告書を、システム安全プログラム責任者に提出すること。
  また、問題点及び不具合が確実に是正されたことを確認し、システム安全プログラム責任者に報告すること。
(6) 監査報告書はシステム安全プログラム文書として維持管理すること。

４．２．８　報告

システム安全に影響が生ずるような状況の変化があった時、機構担当部門は安全部門に、契約の相手方は機構担当部に報告書を提出すること。

報告書には以下を含めること。

〔問題事項〕

(1) システム安全に関する問題点及び是正処置
(2) システム安全プログラム活動に影響を与えた決定事項、実施事項、及びそれが品目の安全に及ぼすと予想される影響の説明
(3) 予想されるシステム安全プログラムの遅延スケジュールとその影響

４．２．９　事故等の調査と報告

契約の相手方及び機構担当部門は、以下の対応をしなければならない。

(1) 機構敷地内での人員の負傷若しくは死亡及び物損事故、機構敷地内外の環境への著しい影響を与える事故、及び第三者に影響を与えた事故について、契約の相手方は機構担当部門に対して直ちに報告すること。

事故についての報告書は提出時における機構の最新の様式に記載し、5 作業日以内に機構に提出すること。
詳細な報告が要求される場合は事故等の発生日から 30 日以内に提出すること。
また、何らかの要因が加われば上記事故につながる恐れのあるヒヤリ・ハット(危うく事故等になりそうになった事象)が発生した場合は、その発生状況、原因等を調査及び確認し、再発防止対策を検討したうえで提出時における機構の最新の様式に記載し、機構担当部門は機構の安全部門に、契約の相手方は機構担当部門に報告すること。

(2) 機構敷地への搬入前に発生した安全上クリティカルな事故等について、機構敷地内で類似の工程がある場合は、その発生状況、原因等を調査及び確認し、機構に報告すること。
また、何らかの要因が加われば上記事故につながる恐れのあるヒヤリ・ハットが発生した場合は、その発生状況、原因等を調査及び確認し再発防止対策を検討したうえで、機構担当部門に報告すること。

４．３　システム安全工学

４．３．１　安全設計の原則

システム等の安全設計においては、基本的に故障許容設計によること。ただし、4.3.1.4 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は契約の相手方にあっては機構担当部門と、機構担当部門にあっては安全管理審査組織と十分に調整のこと。

４．３．１．１　安全設計の優先順位

安全設計の優先順位は次によること。

(2)　ハザードを除去する設計
(3)　ハザードを最小にする設計
(4)　ハザードを制御する設計（狭義）
(5)　安全装置の使用
(6)　保護装置の使用
(7)　警報装置の使用（非常処置と関連させること）
(8)　特別の手順及び／又は訓練に依存するハザード制御方法の適用

(注：本標準の 4.3.1 項を除く他の項では、一般に(3)から(7)の全てをハザード制御と称している。)

４．３．１．２　故障許容設計

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に、次の故障許容設計要求を満足すること。

(1)　２重の故障、１つの故障と１つの人的過誤の組合わせ、及び２重の人的過誤が破局的な事故を引き起こさないこと。
(2)　１つの故障又は１つの人的過誤が重大な事故を引き起こさないこと。

４．３．１．３　事故につながる機能発揮の抑制（ハザーダス機能の抑制）

事故につながる機能を有するものについて、要求しない時にその機能が故障や人的過誤によって動作することを抑制し､その発生の可能性を許容レベルにするため、以下の要求を満足すること。

(1) 破局的な事故を引き起こす潜在的な能力のある機能に対しては、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こと。なお、機能の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。
要求される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こと。
(2) 重大な事故を引き起こす潜在的な能力のある機能に対しては、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こと。

４．３．１．４　リスク最小化設計

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。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。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(Pyrotechnic Device)
・材料適合性
・材料可燃性
・一部のメカニズム（機構品）

なお、構造的破壊が破局的なあるいは重大な事故となる場合は、構造物、圧力容器、ファスナ、荷重支持部材などはフラクチャコントロールの基準を設定すること。

４．３．１．５　故障等伝播の拡大防止

機器・機能等の一次故障・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拡大をもたらさない設計とすること。

４．３．１．６　安全維持機能

(1) フェイルセーフ及びフールプルーフであること。
(2) 個々のハザードに対する複数の制御機能は相互に独立であること。
(3) 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。

４．３．１．７　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システム等を設計すること。

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。

４．３．２　ハザード解析

ハザード解析はシステム等及びその運用に係るハザードをライフサイクルの全てに亘って、体系的かつ論理的に識別・評価する手法である。

なお、ハザード解析はシステム等のライフサイクルで遭遇する最悪の環境条件を考慮して実施のこと。また、ハザード解析の実施にあたっては、過去のプロジェクトからの教訓等を十分に取り入れること。

ハザード解析の解析ステップを図 4.3.2-1 に示す。

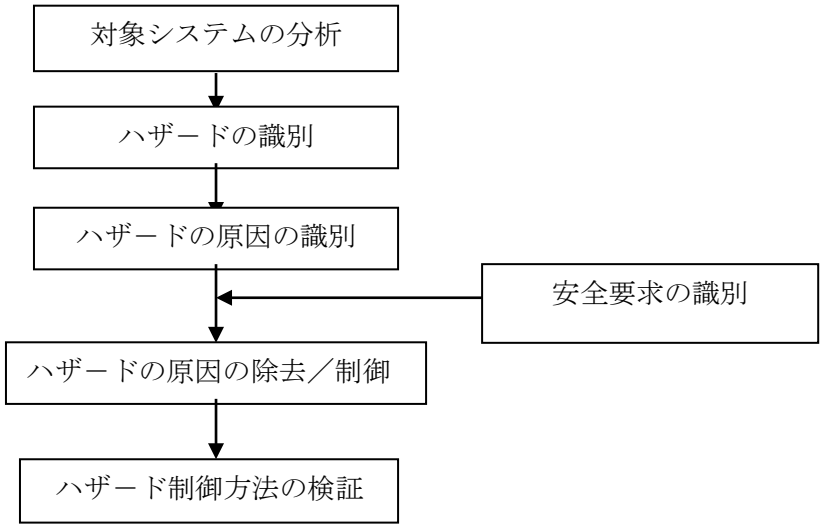


図 4.3.2-1　ハザード解析の解析ステップ

(1) 対象システムの分析

システムの安全性を評価するに際しては、対象システム、運用、ミッション、環境条件及び他システムとのインタフェース等を十分理解している必要がある。

(2) ハザードの識別

上記(1)項で実施した「対象システムの分析」をベースに、ハザードをエネルギ源、環境、運用等に着目して識別し、その内容、発生フェーズ、被害の度合い及び発生の可能性を明確にすること。

なお、被害の度合いは 4.3.2.1(1)項に、また発生の可能性は 4.3.2.1(2)項に基づき、明確にすること。

(3) ハザードの原因の識別

上記(2)項で識別したハザードに対し、対象となるハードウェア、ソフトウェア、運用、人的過誤、インタフェース、環境条件を考慮して、ハザードの原因の抽出を行うこと。

この時、ＦＴＡ（Fault Tree Analysis）手法を活用するとともに、ＦＭＥＡ（Failure Modes and Effects Analysis）とクロスチェックを行うこと。

(4) 安全要求の識別

ハザードの原因を制御するために適用する安全要求を識別すること。適用する安全要求でカバーできない場合には、新たに安全要求を設定すること。

(5) ハザードの原因の除去／制御

ハザードの原因の除去／制御は、4.3.1.1 項の安全設計の優先順位に基づき実施すること。

(6) ハザード制御方法の検証

上記(5)項で検討したハザードの原因の制御方法の有効性を、4.3.3 項の安全検証で確認すること。

４．３．２．１　ハザード識別

以下に示すハザードの識別の結果、被害の度合いⅠ、Ⅱのもの、及び被害の度合いⅢでかつ発生の可能性Ａ、Ｂ、Ｃに該当するものは、4.3.2.4 項に基づきハザードレポートを作成すること。

なお、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（表 4.3.2.3-1 参照）等で明確にすること。

(1) 被害の度合い

被害の度合い(Severity)は表 4.3.2.1-1 に示すとおりレベル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、設計の不適性、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4.3.2.1-1　被害の度合い

被害の度合い	用　語	説　明
Ⅰ	破局 (Catastrophic)	第三者の死亡や重度の人的被害（重度の永久的な人的障害を含む)、要員の死亡や重度の永久的な人的障害、公共や第三者の私有財産の喪失や重大な損傷、システムや射場施設の喪失又は深刻な環境への影響をもたらすものをいう
Ⅱ	重大 (Critical)	第三者の軽度の人的被害、要員の重度の人的被害、公共や第三者の私有財産の軽度の損傷､システムや射場施設の重大な損傷､又は重大な環境への影響をもたらすものをいう
Ⅲ	限界・局所的 (Marginal)	要員の軽度の人的被害、システム等の軽度の損傷、又は軽度の環境への影響をもたらすものをいう
Ⅳ	無視可能 (Negligible)	要員の軽度の人的被害やシステム等の軽度の損傷、又は軽度の環境への影響をもたらさない程度のものをいう

(2) 発生の可能性

システム等の計画されたライフサイクルにおけるハザードの発生の可能性は、それらの作動時間、作動回数、関与する人数、作業の回数等の一定の単位に対する発生回数として表すことができる。その他、発生の可能性を定性的に表すことができ、その例を表 4.3.2.1-2 に示す。これらは過去の類似システム等の安全データを解析することにより導き出すことができる。

表4.3.2.1-2　発生の可能性

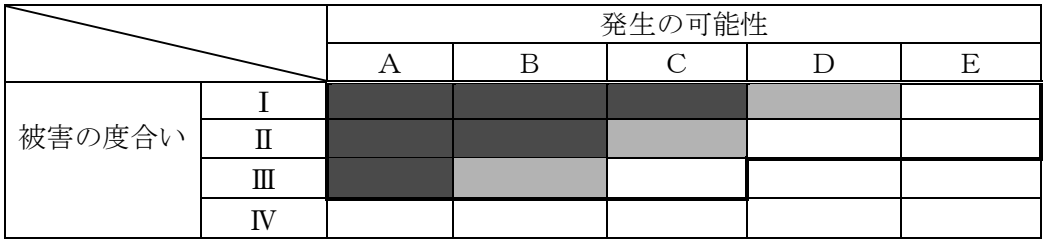
発生の可能性	説　明
A	しばしば発生する (Frequent / Likely to occur immediately)
B	たまに発生する （Probable / Probably will occur in time）
C	まれに発生する （Occasional / May occur in time）
D	ほとんど発生しない （Remote / Unlikely to occur）
E	ほとんど全く発生しない （Improbable / Improbable to occur）

４．３．２．２　リスク評価

機構担当部門及び/又は契約の相手方は、システム等に係る残存リスクを評価すること。
リスクは予想される被害の度合いと事故発生の可能性で表すこと。

リスク許容判定基準は、標準として図 4.3.2.2-1 によること。
ただし、同等の基準を提案する場合は機構の安全部門と協議し、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、予算やスケジュール等の制約条件の下で最大限の努力を払って、その低減に努めること。



；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）　；許容範囲

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。
③ハザードの制御前の被害の度合いがⅠ又はⅡのハザードについては、制御後に上記ハザードレポート作成の範囲外となった場合にも原則としてハザードレポートを作成すること。

図 4.3.2.2-1　リスク許容判定基準

４．３．２．３　各フェーズでのハザード解析

機構担当部門及び／又は契約の相手方は開発の初期段階からハザード解析を行い、ハザードを識別するとともに安全要求を設定し、それらを設計、手順、運用等へ反映させること。

このハザード解析結果は安全データの一部として取りまとめ、4.2.4 項の安全審査文書とすること。従って、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はハザード解析を見直すこと。

(1) フェーズ０ハザード解析

フェーズ０ハザード解析は概念／予備設計段階において行うもので、システムについてのハザードの識別並びに対応策の検討を行いハザード解析表（表 4.3.3-1 を参照）に纏めるとともに、安全要求を設定すること。

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. ハザードに対する予想される事故等の程度を明らかにすること。

(2) フェーズ Ⅰ ハザード解析

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詳細な安全要求を設定すること。

また、4.3.2.1 項で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. リスクの大きいハザードについては、ＦＴＡ(Fault Tree Analysis)、必要に応じてＳＣＡ(Sneak Circuit Analysis)、ＥＴＡ(Event Tree Analysis)等を行うこと。
d. ハザード解析はＦＭＥＡと相互チェックを行い、漏れを防ぐこと。
e. 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。
f. 安全性の改善、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

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、制御に関する提案処置内容が明確になり、設計上実現されていること。
b. 必要に応じてＦＴＡ、ＳＣＡ 、及びＥＴＡ等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文書化し、安全の維持、改善に反映させること。
e. 検証手段を明示すること。

(4) フェーズ Ⅲ ハザード解析

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、制御に関する提案処置内容を明確にし、かつ文書化すること。
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文書化し、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明確化すること。

４．３．２．４ ハザードレポート

機構担当部門及び／又は契約の相手方は下記によりハザード解析結果を文書化し、適切な時期に提出すること。なお、ハザードレポートを作成するハザード範囲は 4.3.2.1 項に示す。

(1) システム等について、すべてのハザードを抽出し、表 4.3.2.4-1 又は同等の様式によりハザード識別まとめ表を作成すること。

また、識別されたハザードについて、そのハザードの分類、原因、制御方法及びその検証方法について表 4.3.2.4-2 又は同等の様式によりハザードレポートを作成し、必要に応じて補足説明資料を添付すること。

(2) 上記(1)項で実施したハザード解析結果は、これとは別に実施したＦＴＡ、安全要求適合性詳細検討書、その他必要な解析結果との整合をとること。

(3) ハザードレポートは各フェーズごとにシステム安全プログラム責任者の確認のサインを受けた上で安全審査文書として契約の相手方にあっては機構担当部門へ、機構担当部門にあっては機構安全部門へ提出し、確認を受けること。

(4) 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方法が検証され、最大限の努力の上、リスク許容判定基準を満足していること及び安全検証の完了が確認された時点において完了する。

４．３．３　安全検証

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、システム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。類似性解析では、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終了時に未決であってその検証が射場における作業に持ち越される安全検証データの未処理事項は、表 4.2.4-2 又は同等の様式に示す安全検証追跡ログに記録して処置を追跡、管理しクローズさせて、適切な時期に提出すること。

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フィードバック等の是正措置をとること。

４．４　作成文書及び安全データ

本標準を実行する上で作成すべき文書を付属書Ⅱに示す。

機構担当部門等は文書作成あるいは処置に当たり安全部門と協議を行うこと。

文書及び安全検証に係るすべてのデータは、常に利用できるように記録し管理すること。

これらは、システム安全プログラム責任者へ最新の状態を提示できるようにするとともに、関連する部門に漏れなくフィードバックさせ、反復性の性質をもつ欠陥の防止及び安全に関する詳細な要求事項に一致していることを確認するために使用すること。

また、これらは将来に対する安全データとして保管すること。

表 4.3.2.3-1　ハザード解析表　様式例

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。
被害の度合いの低減をした場合には、その対応策の欄で説明すること。

表 4.3.2.4-1　ハザード識別まとめ表　様式

システム名　　：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

サブシステム名　：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

ハザードカテゴリ / ハザード・タイフ / 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	極端な温度		火災	爆発・破裂				構造破壊		振動・衝撃・衝突			腐食・汚染			漏洩			電磁干渉	電撃・放電			放射			騒音	窒息・ガス中毒	墜落・落下物 墜落・落下														
	高温・発熱体	低温・極低温	点火源等の存在 可燃物・酸化剤	圧力システム・圧力容器	火薬類（固体推進薬・火工品）	液体推進薬	爆発性雰囲気	過荷重・強度不足・疲労	水素脆性・応力腐食	加振源・音響・圧力波	回転体・可動機構		生物学的汚染・コンタミ	腐食性物質・電解腐食・異種金属	流体適合性	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		シールド不良	短絡	静電気	感電	電離放射線・放射性物質	レーザ・IR・UV・閃光	電波	連続騒音・衝撃音	酸欠・有毒ガス	高所作業・不安定姿勢	部品・工具の落下	吊上物の落下											
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。
- ヒューマンファクタ（人的過誤）
- ソフトウェアエラー(入力ミス・バグ)
- 天災（地震、津波、雷、台風、大雨、強風等）
- 危険作業（危険物、有害物質、高圧ガス、火薬類等取扱、重量物運搬）
- 停電、電力復旧

＜被害の度合い＞
- Ⅰ　破局　　：第三者の死亡や重度の人的被害(永久的な人的障害を含む)、要員の死亡や重度の永久的な人的障害、システムの喪失、環境への深刻な影響をもたらすもの
- Ⅱ　重大　　：第三者の軽度の人的被害、要員の重度の人的被害、システムの重大な損傷、環境への重大な影響をもたらすもの
- Ⅲ　限界・局所的：要員の軽度の人的被害、システムの軽度な損傷、環境への軽度な影響をもたらすもの
- Ⅳ　無視可能　　：要員の軽度の人的被害やシステムの軽度な損傷、環境への軽度な影響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

表 4.3.2.4-2（1/2）　ハザードレポート　様式（１）

ハザードレポート		ハザードレポート番号
システム名	日付	作成／改訂
サブシステム名	プログラムフェーズ	
ハザードタイトル		
適用される安全要求	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	
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		
安全検証ステータス		

承　　認	契約の相手方	機構担当部門	機構／安全部門
フェーズ Ⅰ			
フェーズ Ⅱ			
フェーズ Ⅲ			

契約の相手方の場合は機構担当部門に、また機構担当部門の場合は安全部門に提出すること。

表 4.3.2.4-2（2/2）　ハザードレポート　様式（２）

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	

５．　付属書Ⅰ　用語の定義

［あ行 ］

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に係わるものをいう
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

安全検証追跡ログ：ハザードレポートの安全検証の完了の未確認事項に関してハザードレポートの安全検証確認に替わり、その完了までの状況を適切に管理、確認するための文書

安全審査　：システム等が安全要求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

安全データパッケージ：
ハザード識別まとめ表、ハザード解析表、ハザードレポート、安全検証データ、安全検証追跡ログ、安全要求適合マトリクス、安全要求適合性詳細検討書、安全上クリティカルな機能の故障データ等の、安全要求との適合性を確認する文書

安全部門　：（本標準に限った表記）機構担当部門の属する本部の安全管理審査組織
安全管理審査組織のない本部等については安全・信頼性推進部を指す

インヒビット　：事故に繋がる機能を有する作動装置について、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作動装置の間に設ける物理的な遮断機能
例えば、電気回路におけるリレー、配管における遮断弁等

ＥＴＡ（Event Tree Analysis）：
システムの故障あるいは災害の引金となる基本事象（例えば、弁の破損、配管のクラック、誤操作等）からスタートし、最終的なトップ事象（例えば、推進系の推力停止、推進系の破裂等）に発展する迄の中間事象を機能、運用シーケンスを追ってたどり、最終的なトップ事象の発生をいかにして阻止するかを、それぞれの機能、運用シーケンスの段階で検討を行う帰納的な解析手法

ウェーバ　：安全要求に合致しない状態について許容可否を検討し、当号機に限り許可すること

ＳＣＡ（Sneak Circuit Analysis）：
この解析はハードウェアシステム及びソフトウェアシステムを評価する解析手法の１つであり、要求された機能を発揮させなくしたり、要求されない機能を引き起こす潜在的な回路及び状態を識別することを目的とする
　この解析手法にはスニークパス解析、ディジタルスニーク回路解析、ソフトウェアスニークパス解析等があり、適用システムに対してこれらの解析のうち適切な解析が使われる

ＦＴＡ（Fault Tree Analysis）：
故障の木解析をいう
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、または故障原因調査を行う解析手法

［か行］

概念設計　：開発の最初の段階、すなわち概念段階において可能性のある複数個のシステムについてシステム概念を設定するための設計

監査　：自社又は供給業者のシステム安全プログラム活動の有効性を確認するための行為

開発　：機構が実施する広義の開発をいい、システム等の研究及び維持を含む

開発実施責任者　：プロジェクト等の目的、遂行方針に沿って開発を的確に実施するためシステムの仕様、信頼性、安全性、開発業務の内容、時期、費用等を総合管理し、プロジェクト等の開発責任を有している人、プロジェクトマネージャ等

確率論的なリスク評価：定量的リスク評価ともいう。即ち、安全の度合いを定量的に表現するためにモデルに基づきリスクを構成する被害の度合いと発生確率を数値を用いて表現する方法で、重要と考える要因を合理的に掴む評価方法

機構担当部門　：（本標準に限った表記）機構においてシステム等に関する研究開発又は受託を行う部門

供給業者　：機構との契約のもとで契約の相手方と直接取引を行い、契約の相手方に対して物品等を供給する個人、会社又は事業所
同一企業内の他事業部又は協力会社も含む

契約の相手方　：機構と契約を行なう個人又は法人
機構と共同開発する場合の協定の相手方も含む

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

基本設計審査（PDR :Preliminary Design Review）：
基本設計がほぼ終了し詳細設計に着手する前に実施されるもので、基本設計の成果がシステム仕様書、開発仕様書などを満足する製品の実現が可能であり、詳細設計に移行できる状態であることを確認する審査

検証　：試験、検査、解析、デモンストレーション及びこれらの組合せにより、ハードウェア又はソフトウェアがすべての設計要求（性能及び安全の要求等を含む）を満足していることを確認すること

コンポーネント　：いくつかの部品、デバイス及び構造体を組合わせたもので、機器の全体運用中で独立した機能を遂行するもの。例えば、姿勢制御機器、電力分配器等

コンフィギュレーション：
システム又は構成品目の機能的及び物理的特性

故障許容設計　：故障又は人的過誤があっても事故に至らないようにする設計であり、ハザードを制御するために用いる基本的な安全要求である
被害の度合いがⅠのハザードの場合は２重の故障、又は２重の人的過誤、又は１つの故障と１つの人的過誤の組合せがあっても事故に至らないようにする設計
また、ハザードの被害の度合いがⅡのハザードの場合は、１つの故障又は１つの人的過誤があっても事故に至らないようにする設計

［さ行 ］

サービス　：品目のインタフェース先から供給される電力、水、ガス等

サブシステム　：システムの中で主要な機能を占めるもので、それ自身が複数のコンポーネントから構成されるもの

システム　：人間、ハードウェア、ソフトウェアの集まりであって、特定の諸機能を果たすために組織されているものをいう
一般にシステムはプロジェクト活動の第１分割単位である

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

システム安全プログラム活動：
システム等の安全を確保するための活動をシステマチックに推進・実施するための計画や手順等の立案、実行を行う管理活動

システム安全担当者：
システム安全管理組織の中でシステム安全プログラム責任者の下でシステム安全プログラム活動を推進している担当者

システム等　：(本標準に限った表記) 機構の研究開発及び受託するシステム、サブシステム、コンポーネント等

事故　：人員の負傷、死亡、疾病、システム等、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

事故等　：事故及び安全に影響を及ぼす不具合。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

出荷前審査（PSR: Pre-Shipment Review）：システム等の射場への搬出が可能であることを確認する審査。受入試験結果、品質記録、不具合の処置状況等を審査

詳細設計審査（CDR: Critical Design Review）：
詳細設計がほぼ終了しプロトタイプモデル（PM）の製造に移行する前に実施されるもので、詳細設計を実施した成果である製造図面、仕様書、エンジニアリングモデル（EM）の試験成果などを評価して、詳細設計の成果が契約書、技術仕様書などの要求条件を満足し、PM の製造に移行できる状態であることを確認する審査

設計審査　：製品の設計段階で、設計品質及びそれを具現化するために計画された製造、試験、据付け、使用、保全などのプロセスについて、コスト及び納期を考慮しながら客観的知識を集めて評価し、改善点を提案するとともに、次の段階へ移行し得る状態にあることを確認する組織活動
基本的には設計の進捗に合わせ「基本設計審査（PDR）」、「詳細設計審査（CDR）」及び「認定試験後審査（PQR）」の３種類がある

全体マイルストーン審査：プログラム又はプロジェクトのマイルストーンに開催される審査で、基本設計審査（PDR）、詳細設計審査（CDR）、認定試験後審査（PQR）、出荷前審査（PSR）をいう

［た行 ］

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

デビエーション　：安全要求に合致しない状態について、その安全要求の意図を満足することを確認し、安全要求適合として承認すること

トレードオフ　：複数の案から費用、性能等を比較検討して、最適案を決定すること

［な行］

認定試験後審査（PQR: Post Qualification Review）：
プロトタイプモデル（PM）用の製造図面、仕様書、製造工程に基づいて PM を製造し、認定試験を実施した後に行われる審査
認定試験結果を評価して、製品が開発仕様書の要求条件を満足しており、設定された製造図面、仕様書及び製造工程が確立していることを確認する

［は行 ］

ハザード　：事故をもたらす要因が顕在又は潜在する状態

ハザード解析　：対象システム（支援機器等を含む）及び運用に係るハザードを、ライフサイクルの全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　：ハザードの内容が分かるような source、mechanism、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ハザード要因発生の原因となるもの（例えば、推薬漏洩の原因となる容器の強度不足、弁の誤作動、シール不良、過加圧など）

B

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
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、5.1.1 項を除いて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、mechanism、outcome）が想像でき、他のハザードと区別できるようなハザードのタイトル

ハザード対応策　：ハザード原因をなくする、ハザード原因の発生の可能性を抑制する、又はハザード原因の発生によるダメージを抑制するための方策（ハザード制御）

ハザードレポート：個々のハザードに関して設計担当者、システム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るために、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

ハザードの制御　：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、4.3.1 項を除いて一般に広義の意味で使用している

不具合　：１つ以上の特性が要求と合致しない又は異常な物品の状態
故障、偏差、欠陥、不足及び機能不良を含む

フェイルセイフ　：サブシステム、コンポーネント等に不具合が生じたとき、その機能が失われても、安全性が保持されるように配慮する設計思想

フールプルーフ　：人的過誤(ヒューマンエラー)が起こり得ないような、又は人的過誤によっても安全性が確保されるよう配慮する設計思想

フラクチャコントロール（破壊制御）：
致命的欠陥に繋がるクラック進展の解析を行い、その防止を行うこと
これを扱う基準は工学、品質保証、製造、運用技術等多岐に亘るものが適用される

プロジェクト等　：システム等を研究開発又は受託する機構のプロジェクト及びプロジェクトに準ずる組織（ただし、宇宙基幹システム本部打上安全評価室、及び同・有人システム安全・ミッション保証室が所掌するプロジェクトを除く）

法令による規定　：製造地又は取り扱う地域に適用される産業安全関連法規、及び労働安全衛生法規で規定される産業安全をいう

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

［ま行 ］

マイルストーン　：進捗状況、有効性の測定又は将来業務の計画や方向付けのための管理点として活用するために、プロジェクトのライフサイクル又はシステム安全プログラム上に予定した重要なイベント

［や行 ］

予備設計　：開発仕様書を設定するための予備的なシステム設計

［ら行 ］

ライフサイクル　：設計、試験、製造、運用及び処分を含んだシステムの存続する間のすべてのフェーズ

リスク　：被害の期待値。即ち、ハザードで識別した安全の度合いを予想される「被害の度合い」と「発生の可能性」で表したもの

リスク最小化設計：安全係数や設計マージンなどの概念を適用して信頼性を高めた設計をすること

６．　付属書Ⅱ　作成文書リスト

文書名	該当項目
システム安全プログラム計画書	4.2.1(2)、表 4.2.1-1
安全データパッケージ	4.2.4(4)、表 4.2.4-1
ハザード識別まとめ表*	4.3.2.4、表 4.3.2.4-1
FTA,RTA,SCA 等*	4.3.2.3(2)
ハザード解析表*	4.3.2.3、表 4.3.2.3-1
ハザードレポート*	4.3.2.4、表 4.3.2.4-2
安全要求適合マトリクス	4.2.2、　表 4.2.2-1
安全検証追跡ログ（必要な場合）	4.2.2(4)、表 4.2.4-2
安全要求適合性詳細検討書（必要な場合）	4.2.5、　表 4.2.5-1
安全審査実施要領書	4.2.4(3)
教育・訓練計画書	4.2.6
教育・訓練実施／参加者記録	4.2.6
監査計画書	4.2.7
監査報告書	4.2.7
報告書（問題事項）	4.2.8
事故報告書、ヒヤリ・ハット報告書（必要な場合）	4.2.9

注）＊：設計の初期段階から安全設計のツールとして活用するために常に最新化すること。
各安全審査段階で最新のもので安全データパッケージの一部を構成すること。