限定なし

# 単一故障・波及故障防止設計標準

平成３０年３月３０日　　Ａ 改訂
平成２２年７月２８日　　制定

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

本標準は宇宙機システムに内在する単一故障点の故障及び波及故障によりシステムを喪失するリスクを最小化するための設計・製造検査・試験標準について定めるものである。

## 1.2 適用範囲

この設計標準は、以下の場合に適用する。

(1) 契約書、調達仕様書等でこの標準が呼び出された場合

(2) 契約の相手方が、この標準に基づいた設計を実施したい旨申し出て、機構がこれを認めた場合

(3) 機構の提案要求書に引用する場合

なお、本標準の適用にあたっては、ミッション達成のために冗長系を採用する宇宙機、また、一つの故障が発生しても可能な限りの多くのミッション機器を生かしたいマルチミッション搭載の宇宙機に適用することを想定している。

本標準では、既存の設計標準等を順守して宇宙機を設計、製造検査、試験を行うことでほとんどの単一故障点の排除および故障リスクを下げることは基本的に可能と考えられるが、ミッションの確実な成功に向けて、個々の設計標準の隙間を見落とすことが無いようあらためてシステム的な観点から単一故障・波及故障に焦点をあてて設計結果等を見直すことを意図した要求事項を規定している。

本標準に規定される要求事項は、プロジェクトの規模によりその適用項目の違いはあるものの、単一故障・波及故障防止のために考慮すべき事項を網羅している。

# 2 関連文書

## 2.1 適用文書

以下の文書は、本標準の定める範囲において、本標準の一部とする。尚、本標準と適用文書間で矛盾が生じた場合は、本標準の規定を優先する。

(1) JMR-004 信頼性プログラム標準

(2) JERG-2-212 ワイヤディレーティング設計標準

# 3 用語の定義及び略語

## 3.1 用語の定義

適用文書 2.1(1)によるものの他に本標準で用いる用語の定義は以下の通り。

①単一故障　　：一つの機器の故障のモードにより、システム、サブシステムあるいは機器の喪失に至る故障。

②単一故障点　：単一故障となりうる故障モードの発生する部位、あるいは機器。SFP ともいう。

③波及故障　　：故障が連鎖、あるいは他のコンポーネント・サブシステムに影響する故障。

④サバイバビリティ：運用中に発生した異常事象に対して、全損せずに地上コマンドによる復旧作業と故障発生時の HK データをダウンリンクできるような機能を維持しつづける能力のこと。必要な電力余裕と姿勢、通信確保ができる能力のこと。

⑤内部冗長　　：同一の筐体（連結されて一筐体と扱う場合を含む）の中で冗長構成がとられていること。完全複数構成になっている場合や、部分的に複数構成になっている場合などがある。

⑥冗長性　　：手段の一部が故障してもアイテムは故障とならない性質。必要な機能・性能に対してアイテムが保有する機能・性能の倍率によって実現される性質。

### 3.2 略語

| | |
|---|---|
| FMEA | Failure Mode and Effects Analysis |
| FTA | Fault Tree Analysis |
| CIL | Critical Item List |
| SFP | Single Failure Point |
| FDIR | Fault Detection, Isolation and Recovery |

## 4 一般要求事項

宇宙機は多くの部品より構成されており、一つの部品の故障によりシステムが全損し極めて大きな影響を及ぼすことがある。従って可能な限り冗長化を図り単一故障点を最小化し信頼性を高める必要がある。

また、「みどり 2 号」、「ひとみ」の軌道上運用異常では、故障の波及により衛星システムが喪失しミッションの達成が出来なかったことから、単一故障のみならず波及故障の防止もミッション喪失を防ぐために重要であることが改めて認識された。

単一故障・波及故障によるシステム喪失のリスクを低減するためには、設計のみに注目するだけでは完全でなく、製造段階での検査及び試験に至るまでの一連の流れの中で適切に対処することが重要である。また、単一プロジェクトでの成否を糧に、不断の知見の蓄積によって、洞察力を高めることが高信頼性システムを生み出すうえで重要である。

# 5 要求

## 5.1 基本要求

（1）冗長系採用可能範囲の決定

・サブシステム、コンポーネントを複数搭載（または内部冗長）することで冗長系を構成することはプロジェクトの規模、達成すべき信頼性、サクセスクライテリア、運用等、プロジェクトにより異なるため、各プロジェクトにて決定されなければならない。

（2）単一故障点の排除

・冗長系が必要と決定された宇宙機システムおよびその一部は、本標準により単一故障点の排除を行うこと。

・冗長系不要と決定された宇宙機システムおよびその一部は、本標準 5.3 項で規定するリスク最小化設計をすること。

（3）単一故障・波及故障防止設計等の進め方

・冗長系が必要と決定された宇宙機システムおよびその一部の、単一故障点、波及故障防止設計は、次の順序で行うこと。

① 単一故障点の抽出・識別（設計段階）

冗長系が必要と決定された宇宙機システムまたはその一部の設計にあたっては、内在する全ての単一故障点を抽出し識別すること。

識別された単一故障点でのリスクに対する対策は設計初期に衛星開発での対策及び運用での対策を明確にし、それぞれの設計への前提条件にすること。

② 単一故障点の可能な限りの除去（設計段階）

識別された単一故障点は、原則として冗長化によって排除すること。（注 1）

ただし、冗長化の採用が困難な場合は、代替機能による補償やシステム全体の安全モード化等の対策を採用する事も考慮すること。また、冗長化を採用した場合においても切り替え機能の不全、インタフェース部分の波及故障、共通要因による同時故障等、冗長化の効果が阻害される可能性について十分な評価を実施すること。

（注 1）

除去に当たっては、当該プロジェクトとして許容されたリソースの制約の下でミッションサクセスの向上を目的とし、識別された故障のミッションへの影響に応じた対策を講じることができる。

③ 単一故障点許容の妥当性評価・決定（設計段階）

単一故障点の除去が困難な場合にはリスク最小化設計（5.3 項）を行うこと。

④ ③に対する検査・試験による確認（製造検査・試験段階）

単一故障点、波及故障防止に係わる全ての部位はクリティカル品目として 5.3 項に規定する管理をしなければならない。

（4）サバイバビリティの検討

・残存する単一故障点のみならず、冗長系を採用した系統においてもシステム的に重大と考えられる故障モードが発生した場合について、サバイバビリティの観点で評価・検討を行うこと。

・真の冗長性が保たれていない場合は、冗長構成の有効性を再検討し、設計変更やリスク受容などを判断すること。一見して冗長構成になっているような系統でも、場合によって真の冗長性が保たれない場合があることも考えられ、例えば、システムリソース不足などの能力不足、待機系の立上げ時間中や FDIR におけるモード変換時の運用も考慮する必要がある。

## 5.2 各設計段階の詳細要求

単一故障点を識別・排除し、単一故障・波及故障を防止するために、各設計段階でシステム・サブシステム・コンポーネントのレベル別に、以下に示す項目を実施すること。

### 5.2.1 予備設計段階

サブシステム、コンポーネントを複数搭載（または内部冗長）することで冗長系を構成する範囲の決定を行う。この範囲の特定は、各プロジェクトのリソース、信頼性要求、安全性要求、サクセスクライテリア等と整合するように総合的に検討して決定すること。この際、複数搭載して冗長系を構成することが、必ずしも冗長性を確保したことにならないことを注意すること。

システム的に重大と考えられる故障モードに対するサバイバビリティについて、サクセスクライテリアとシステムリソースを考慮して検討すること。必要なサバイバビリティ確保のためのシステムオプションを明確にすること。

### 5.2.2 基本設計、詳細設計段階

①システムレベル

（1）単一故障点の把握

・ システム機能系統図により各サブシステム間の接続関係を確認することは単一故障点抽出のベースとなる。加えて電源系統図、機器配置図等可能な限り実体配置、実体配線に近い図面を用いて単一故障点となり得る部位を把握すること。

・コンポーネントレベル、その構成要素レベルの FMEA またはサブシステム設計のインタフェース FMEA からシステムレベルへの影響を評価し、単一故障点の抽出を行うこと。

（2）エマージェンシー対応設計

・単一故障点で予想される故障が発生した場合に自動的に SAFE モードまたは FDIR によってサバイバビリティを確保し、原因究明のため HK データ保存が可能なシステムとすること。最初の故障によって 2 次的に引き起こされる波及故障についても考慮の上、ミッション軌道における可視性に基づいて地上コマンドによる復旧作業と故障発生時の HK データをダウンリンクできるように必要な電力余裕と姿勢、通信確保ができること。

（3）運用ミス対策

・　単一のコマンドミスなどの運用ミスによりシステム喪失の可能性がないか ETA などを用いて評価して該当する運用については多重ゲート化、オペレーションミスを防止するツール、コマンド設計、運用手順検証による運用上の対策をとること。

・軌道変更、姿勢変更のマヌーバは不具合発生時のリスクが高い運用であるため、可視域での運用を前提にすること。ミッション要求との関係でやむ負えない場合は、ハイリスクな運用としてサバイバビリティの検討対象として含めること。

（4）電源バス故障分離の実装設計

・電源バスは、低インピーダンスで接続されているため、サブシステムを越えて電力供給源（太陽電池パドル等）から各種負荷まで END-TO-END としてとらえることが重要である。負荷短絡などの故障モードに対して、故障分離機能（過電流保護、電流制限機能、ヒューズなど）の配置、しきい値、ハーネス許容電流等に問題がないことをシステム全体として総合的に確認すること。

（5）冗長系切替え時間制約の対応

・システムレベルの FMEA において、冗長系の切り替え時間、タイミング設定がクリティカルな故障モードの有無を検討すること。クリティカルな故障モードに対して

は、冗長系切替え時間等の要求事項を設定し、関連する機器等に配分するとともにシステムとして検証すること。

② サブシステム設計

（1）単一故障点の把握

・当該サブシステムを構成する全てのコンポーネント及び他のサブシステムの関連するコンポーネントを要素としたインタフェース FMEA 等によりシステム、サブシステムレベルで内在する単一故障点を全て識別すること。

・冗長構成をとった場合も、接続の仕方、配置によって冗長性を阻害されることがある。たとえば、冗長となる信号が同一リレーや同一コネクタを経由して配信されている場合や同一ハーネス束に束ねられている場合のように物理的／熱的に故障伝搬する構成の場合は冗長性が阻害されることがある。これらの潜在的な単一故障点を識別するため実体配線図、レイアウト図等を用いて電気的、機械的な故障モードを意識して精査すること。

・冗長系については確実に切り替わるかどうか、想定できる限りの故障モードを想定して解析を実施すること

③ コンポーネント設計

（1）単一故障点の把握

・内部冗長機器の場合は、コンポーネント内に入り込んでインタフェース FMEA 等を行い、冗長系を喪失させる潜在的な単一故障点が無いような設計を行うこと（コンポーネントに属するハーネス、コネクタ、半田付け接続点等を全て含めること)。また、内部冗長コンポーネントは筐体を一つにしたことに着目した特別な注意をはらうこと（例：波及故障防止のために十分な空間分離。共通ハーネスの冗長化等)。

（2）クリティカルアイテム管理

・上記の結果で単一故障点が残存する場合は、単一故障点に対してクリティカルアイテムとしてリスク最小化設計を行うこと。

5.2.3 その他留意事項等

・実装設計が不適切な場合、単一故障点を潜在させる可能性があることを認識するこ

と。

・設計段階で識別された単一故障点はクリティカルアイテムリスト（CIL）として管理し漏れのない対策を講じること。クリティカルアイテムの識別に当たってはコンポーネントレベルよりは、部品、デバイス、接続箇所などのレベルで評価すること。

・冗長設計においてはリレー等の切り替え箇所が単一故障点となりうることを注意すること。

・偶発故障ではなく設計に起因するような故障には、冗長設計という考え方では対応できない点に注意すること。すなわち、一方の系で生じた故障が、設計に起因する共通の原因により他方の系にも生じて、結果的にいずれの系も機能を損失することがあることに配慮すること。

・ソフトウエアを搭載する制御装置を冗長化する場合には、ソフトウエアバグの内在有無を十分に確認すること。（同じバグの内在による両系機能の喪失防止）

・単一故障点は、さらされる環境（打上げ時の音響振動、宇宙での熱真空環境、宇宙放射線環境等の外部環境及び宇宙機自体の有する電磁誘導環境、機械的特性、熱環境等の誘導環境）を十分に考慮して設計すること。特に設計パラメータ（実効放射率、熱膨張率等）については非線形性、ヒステリシス特性や高温側・低温側で特性が異なる場合などがありうるので、設計に用いた値の妥当性が確認できるような評価試験データの収集あるいは試験による実測などを考慮すること。

・ワイヤハーネスについては、適用文書 2.1(2)に基づき束線数に応じたディレーティングを適切にとること。

・設計審査等では設計要求の妥当性確認のみならず、設計結果（解析、図面）により適切に設計されていることをその分野の有識者により確認しなければならない。確認ではプロジェクト実施部門とは独立な立場のものによる確認を行うこと。

### 5.3 クリティカルアイテムの管理

（1）リスク最小化設計

① 冗長化が不可能な場合（構造等）、故障発生確率を下げるため、設計マージンを確保すること。

・ 部品・材料は使用環境に対して適切な余裕を持ち、適切なディレーティング設計等を適用すること。
・ 構造・熱設計においては適切な設計マージンを持っていること。
・ 機構設計においては可動部分に対して適切な設計余裕を有すること。
・ 構成機器の寿命評価がなされ、寿命余裕を持っていること。
・ 電気・電子部品の実装設計（部品接着等の固定方法、絶縁空間の確保や二重絶縁化などの絶縁設計等）については必要な余裕をとること。
・ 下流の短絡により上流の共通ハーネスが損傷しないよう、故障個所を分離できる保護機能を入れること（波及故障の防止)。

②その他

・単一故障点は単純な構造・機構とすることを配慮し、信頼性を確保すること。
・可能な限り、すでに軌道上で実証され、技術成熟度の高い部品・コンポーネントの採用をすること。
・実装設計においては、製造後に適切な状態（間隔、形状、配置など）に施工されたことを確認できるよう中間検査や最終検査での検査性を考慮すること。また、これらのポイントは、検査段階の検査ポイントとして明確にすること。

（２）製造・検査段階

① 製造

・CIL に記載された製造時の要注意点について、管理することが必要である。特に適用される工程が特殊工程またはそれに準ずる工程では、品質が工程自体に依存するため、工程 FMEA 等により品質向上を図ること。特に新規工程および４M（作業者－Man，設備・治工具－Machine，部品・材料－Material，作業方法－Method）に変更がある場合には工程確立が必要である。

② 検査

・設計段階で作成された CIL により製造工程での検査ポイントを明確にして全て検査しなければならない。

・組み立てが進んだ段階に識別された検査部位が検査できない事がないように、検査ポイントの設定をすること。

・後の試験段階で試験検証が不可能な場合には、検査段階が最終との認識で適切な検査を実施し証拠を残すこと。

・検査方法は単一故障点の検査として適切な方法でなければならない。

・当該検査方法は、検査部門、設計部門により承認されなければならない。また独立な立場のものによる確認を受けなければならない。検査結果の確認についても同様とする。

（３）試験段階

・CIL 記載の要注意ポイントを確実に確認すること。冗長系を採用している場合は、組合せに抜けがなくなるように切り替えなどの機能試験を確実に実施し、冗長系が確実に動作することを検証すること。

・故障の予兆を検知できるパラメータが存在する場合は、適切な管理幅を設定し、各試験を通して特性値管理を行うこと。

・冗長系の評価のため、システムレベルの END-TO-END の視点を持って、試験により冗長系が所望の動作をおこなうことを確認すること。この時の END-TO-END 試験構成については、想定した単一故障に対して適切なものとなるように配慮されている必要がある。やむを得ず分割試験の積み上げによる場合は、END-TO-END の視点から、積み上げにより生じるリスクが十分低いことを確認すること。
また、それぞれの試験がカバーできていない実運用時に生じうる事象は何であるか、END-TO-END の視点から常に意識するように気をつけること。

### 5.4　その他考慮すべき事項

（１）設計・試験に関する事項

・システム設計、サブシステム設計、コンポーネント設計の各設計間のコンフィギュレーション管理は密に行い、設計変更等にともなう単一故障点設計への反映漏れがないように進めること。

・冗長性を完全にするにはサブシステム設計におけるコンポーネント設計者との協働作業に大きく依存することを認識して設計すること。

・冗長化設計は基本設計でほぼ決定されることから、この段階での単一故障点対策を確実に行うこと（後の単一故障点に係わる設計変更発生を未然に防止できインパクトを最小化できる）。

・ソフトウェアとハードウェアを組み合わせたシステムでは、ハードウェアの単一故障により異常な命令等に遷移してシステム喪失にならないような検証も必要である。

・詳細 FMEA はその実施方法により、解析結果に大きな差がでることを認識し、その結果を評価・活用することが必要である。

・単一故障点に使用する部品については、内部構造、動作原理などを確認し、高信頼性部品であることを保証できる部品を採用すること。

・太陽電池パドルは、2 翼では完全冗長とはなっていないので、展開不良、駆動系不良は致命的な故障モードである。このため、太陽電池パドルの駆動・機構系において設計余裕（トルクマージンなど）の確保を確実に行うこと。

・電力異常、姿勢異常など衛星喪失につながる異常発生時に衛星の状態をスピーディーに検知し、FDIR 等の自動対策を適用し、安全化措置を講じること。加えて地上の支援により波及的な事象の悪化を防止できる適切な手段を講じること。

・波及故障に対応した設計になっているかどうかを確認するため、故障の波及シナリオを時系列的に見て評価することは有効である。

・FDIR などで、ある単一故障により予想外のループに遷移して、宇宙機の機能に大きな影響を及ぼさないように設計すること。

・システム設計において識別された故障モードへの対策として冗長化という視点だけではなく、故障を許容するシステムとするという視点も波及故障によるミッション喪失を防止するには有効である。

・製造欠陥を識別することに配慮した検査を実施すること。

（2）他ミッション・過去の不具合事例等の参照

・故障モードの識別に当たっては過去のミッションにおいて発生した事例を参照すること。

・地上試験における不具合でミッション喪失に結びつく可能性があった不具合事例を整理し参照すること。