単一故障・波及故障防止設計標準

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　適用範囲

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。

現在制定されている設計基準等を順守して宇宙機を設計、製造検査、試験を行えば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る。しかしミッションの確実な成功に向けて、システム的な観点から見ると、必ずしも既存の各種基準の適用のみでは十分でない。このため本基準では単一故障・波及故障に焦点をあて必要となる事項を規定するものである。本標準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が望ましい。

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-004B　信頼性プログラム標準

3　用語の定義及び略語

3.1　用語の定義

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

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

3.2 略語

FMEA	Failure Mode Effect Analysis
FTA	Fault Tree Analysis

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 号軌道上運用異常原因調査の結果、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。

5 要求

5.1 基本要求

（1）単一故障点排除の範囲の決定

・単一故障点の識別、排除の設計を行う範囲は、プロジェクトの規模、達成すべき信頼性等プロジェクトの目的により異なるため、プロジェクトにて決定されなければならない。

（2）単一故障点の排除要求

・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故障により冗長系を失わないように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が望ましい。

（３）単一故障点、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。

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)
除去するに当たっては、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別に規定する検証をしなければならない。

5.2 開発の各段階毎の詳細要求

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、設計・製造・試験の各段階、およびシステム・サブシステム・コンポーネントの単位において、以下に示す項目に従って設計を行うこと。

（１）設計段階

（１－１）（予備設計段階）

単一故障点の識別、排除を行う範囲の決定を行う。

（１－２）（基本設計、詳細設計）

① システム設計

・ 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設定し、単一故障点抽出のベースとなるサブシステム間の接続インタフェースを明確化する。（サブシステム間 I/F 接続要求の設定）。

・システムレベルで FTA（故障の木解析）を行い、故障モードの抽出・そのシステムへの影響を識別し、冗長とすべき対象の決定を行うことが望ましい。

・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。なお、FMEA、FTA の手法の詳細は参考文書 2.2（1）等を参照のこと。

・軌道上で故障が発生し地上コマンドにより故障波及防止の制御をする場合、時間的制約からシステム喪失に結びつく可能性がないか評価すること。

・運用過誤によりシステム喪失の可能性がないか評価して単一故障点防止設計をしなければならない。（例：バッテリー完全放電、姿勢喪失による立て直し不可等）

② サブシステム設計

・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コンポーネント間 I/F　FMEA 等によりサブシステムレベルで内在する単一故障点の可能性を全て識別すること。

・識別に当たっては、サブシステム毎に特有な視点があるのでサブシステム毎に注目すべきことをそれぞれ設定すること。

・システム設計結果のサブシステム間 I/F 接続要求に基づき、当該 I/F 条件を詳細化すること。

・冗長系構成をとることが極めて困難な部分や、冗長系にも係わらず単一故障点排除設計の結果、単一故障により両系を喪失する部位の排除が避けられない時には別項

に規定するリスクの最小化設計等を行わなければならない。

・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的に示すこと

・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最終確認を行うこと。

③ コンポーネント設計

・サブシステム設計での I/F　FMEA 結果をベースに、更にコンポーネント内に入り込んで単一故障により冗長系を喪失させる単一故障点を識別し、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、コネクター、半田付け接続点等を全て含めること）

・上記で単一故障点の排除が極めて困難な場合はリスク最小化設計を行い、設計審査での承認を得ること。

・筐体を一つにした内部冗長コンポーネントは特別な注意をすること。（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）

・寿命に配慮しなければならない機器等は十分な設計余裕をもつように設計すること。

・実装設計が不適切な場合、単一点故障を潜在させる可能性があることを認識すること。

④ その他

・上記の②③の作業は実質的には同時に行い効率化を図ってもよい。
また①②③の作業を繰り返すことにより当該宇宙機の単一故障点が最終的に識別される。

・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）より管理し漏れのないようにすること。クリティカルアイテムの識別に当たってはコンポー

ネントレベルに限定せず、内部冗長を用いている場合には部品レベルまで評価し、必要に応じてCILに追記すること。

・既開発のコンポーネントをベースとした開発を行う場合には、新たに適用する打ち上げ環境、宇宙環境等の条件、また運用条件として問題ないかどうかの再評価が重要である。また、変更点について十分に精査して問題ないことを確認すること。

・冗長設計においてはその切り替え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。

・冗長系で設計されているが、運用系の故障で待機系も動作できなくなるケースあり。（インタフェース不整合、またはある稀な条件下で切り替わらないことあり）
従って、冗長化された部位の一点が故障することにより故障が伝播して冗長系も失うことがないように適切な設計余裕を確保した設計とすること。

・設計マージンの評価が必要な場合には、評価用モデルにより実証すること。（実証に当たっては、評価モデルの妥当性、試験方法の妥当性等を評価すること）。

・設計パラメータ（実効放射率等）の設定においてはその設定の方法について妥当性が評価できるように十分配慮すること。

・寿命評価により設計の妥当性を示す必要がある場合には、必要に応じて適切な寿命試験の実施も考慮することが望ましい

・試験計画の設定においては可能な限り、END-TO-ENDで実施することを考慮すること。また、設計段階から分割するI/Fの設計条件を単純化すること

（２）製造・検査段階

① 製造

・製造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らなければならない。特に新規の工程および変更が

ある場合には配慮すること。

② 検査

・設計段階で作成された「クリティカルアイテムリスト」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。

・輸入品や民生品を使用する場合など上記の検査手法の適用に制約のある場合は、試験による確認や上位のサブアセンブリレベルにて品質が要求を満たしていることが確認できるよう配慮すること。

（３）試験段階

・冗長機能により単一故障点を排除する場合には、冗長系の切り替えなどの機能試験を確実に実施し、単一故障点の見落としがないことを確認すること。

・設計で識別された単一故障点については、最終的にはコンポーネント試験、サブシステム試験、システム試験の各段階で実証し、適切な設計マージンが確保されていることを確認する試験手法を採用すること。また、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。

・試験は最終的にはシステムレベルの END-TO-END 試験により所定の要求に満足していることを確認しなければならない。 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り END-TO-END 試験に代える時には、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 END-TO-END 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、常に意識するように気をつけること

5.3 リスクの最小化設計

（1）設計マージンの確保

① 冗長化による単一故障点の排除・波及故障の防止が適切でない場合（構造・材料等）および単一故障点の排除がプロジェクトの規模や状況により困難な場合には、適切な設計マージンの確保による単一故障・波及故障の防止を図ること。

② 設計にあたっては、単一故障点の故障発生確率を下げるために以下を考慮すること。

- 使用する部品・材料は使用環境に対して十分な余裕を持っていること。
- 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。
- 構成機器の十分な寿命評価がなされていること。
- 電気・電子部品の使用条件（ディレーティング設計等）や実装設計（絶縁設計等）に対しては十分な余裕をとること。
- ハーネスは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に適切な設計マージンを有していること。（波及故障の防止）

③上記の「十分」の程度は別の設計基準によるか、他に適切な基準が存在しない場合にはプロジェクト毎に設定するものとする。但しその場合、その基準の妥当性を示し独立評価の審査を受けなければならない。また設計結果（解析、図面等）の妥当性評価を行うこと。

また、リスクの低減度合いが当該プロジェクトとして許容できることを評価の上決定すること。

（2）その他

・単一故障点として識別されて、除去することができない場合には、当該箇所には単純な構造・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。

5.4 ソフトウエア

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停止防止)

5.5 環境の考慮

単一故障点はそのさらされる環境（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のこと。

5.6 検証

システムの単一故障点が識別・排除されていること、または識別された単一故障点が排除できない場合には適切な設計余裕を有していること、および、システムとして許容可能と設定した故障によりシステムが損失しないことを検証する手段を講ずること。

また、検証計画の策定に当たっては設計通りに製品が製造されていることを検査・試験できることに配慮すること。

（1）解析

・試験による検証が困難な場合は解析による検証を行う。この場合には前提など条件を吟味し、実際の使用条件との差異に注意すること。

（2）検査

・識別された単一故障点（許容された単一故障点を含む）が設計余裕を阻害された製造になっていないか検査し、その証拠を残すこと。

・検査方法が妥当であることを示すこと。

・単一故障点の検査では、リスク許容の条件どおり対象物（外注品を含む）が製造されているか確認すること。

（3）試験

・可能な限り完全性（END-TO-END の試験形態の構築）及び網羅性を確保した形態で宇宙環境を模擬した試験を実施することが望ましい。試験上の制約から解析による検証も含む場合や、分割形態での試験を実施せざるを得ない場合には事前に軌道上環境との違いを十分に識別して検証作業を実施のこと。

・識別された単一故障点は全て試験で問題ないことを確認し証拠を残さなければならならない。

・試験方法は単一故障点の試験として適切であることを、設計部門、品管部門、独立評価部門により承認されなければならない。

・試験により基本的な故障モードを含めて可能な限り多くのモードについて実証すること。併せて故障分離機能の確認も行うこと。

5.7 独立評価

単一故障点の識別のために過去の事例、他のプロジェクトの事例などは有効な視点となり得るため、プロジェクト実施部門とは独立な立場のものによるレビューを実施することが望ましい。

5.8 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。

・冗長系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設計を確実に行うこと。(後の単一点故障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)。

・電源系ではEND-TO-ENDとして電力ソースからペイロード供給系まで電流遮断特性、ハーネス許容電流等に問題がないことを、他のサブシステムまで入り込んで総合電源系FMEA等として行うことが単一故障点･波及故障の防止のためには重要である。

・ソフトとハードを組み合わせたシステムでは、ハード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認識し、その結果を評価・活用することが必要である。

・単に単一故障点ゆえ高信頼性部品を使用するとの対処は注意が必要（部品はブラックボックスでありマージン等が確認できないリスクが存在する。そのため部品評価、インプロセス検査が重要である。）

・太陽電池パドルはたとえ 2 翼でも、1 翼が完全冗長となっていない場合には、展開不良、駆動系不良により 1 翼が使用不能となった場合に、機能を満たせないことが生じる。そのため、片系においても設計余裕の考慮など信頼性に配慮した設計とすること。

・異常発生時に状態をスピーディーに検知し、自動または地上の支援により故障波及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み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。