第 4 章　有人信頼性管理技術

1.　序論

日本実験棟「きぼう」は、国際宇宙ステーション（ISS ： International Space Station）計画に参加してから 20 年以上かけて開発してきた我が国初の有人宇宙システムである。ISS では、宇宙飛行士の安全を確保するため、人工衛星やロケットより有人宇宙システム特有の高い信頼性が要求される。また、宇宙飛行士が故障機器を交換することによりシステムの信頼度を維持することが可能となり、人工衛星やロケットが行っている信頼度予測とは違った設計概念が「きぼう」では必要となる。本章では、これらの設計及び管理技術と共に、その開発結果について述べる。

2.　有人宇宙システム特有の信頼性管理技術

日本が ISS 参加を決定した当時、JAXA（当時、NASDA）には、安全要求に基づいた明確な 2 故障許容（2FT : 2 Fault Tolerance）要求はロケットの指令破壊受信機等、一部にしか適用されていなかった。その後、日本が ISS に参加したことに伴い、ISS の故障許容要求を JAXA の安全要求に取込むように内容の見直しが行われた。このため、現在は人工衛星やロケットに対して、射場作業やロケット飛翔中の 2 故障許容が要求されている。これに加えて、「きぼう」では宇宙飛行士を致命傷から守るために、軌道上でも 2FT を実現した高いシステム信頼性が要求されている [1)]。しかも、この 2FT 設計は、単純に同じ機器を 3 重冗長にする設計ではなく、二つの故障、二つの操作ミス、もしくはそれぞれ一つずつの組合せによって、宇宙飛行士の死傷、宇宙機、装置や設備の喪失を引き起こす可能性のある要因（ハザード）にならないことが要求されている。

また、「きぼう」は有人であるが故に、軌道上で機器を修理、交換することが可能である。このため、従来、人工衛星やロケットで行ってきた設計寿命時の残存確率を求める信頼度予測とは異なった概念が「きぼう」では必要となる。機器の故障率に基づき交換補用品数を設定することにより、信頼度を維持するという設計手法が適用されている。また、宇宙飛行士が軌道上で交換を行うことから、部品故障以外に人為故障による信頼度の低下が起こり得る。このため、人為故障の可能性を除去するシステム及び機器の設計が必要となる。

3.　有人信頼性管理技術

3.1　2 故障許容（2FT）要求

ISS では、宇宙飛行士に対する安全を確保するため、ハザードを度合いに応じて二つのカテゴリに分類している。宇宙飛行士の身体に障害を残す又は致命傷となるハザードはカタストロフィックハザードと識別され、2FT が要求される。また、宇宙飛行士の身体に障害を残すもしくは致命傷までには至らない場合などはクリティカルハザードと

This document is provided by JAXA

識別されている。この場合、1FT が要求されている[1)]。

こうしたハザードの識別には、故障モード及び影響解析（FMEA）の手法が用いられた。

2FT を実現するためには、ISS の全体管理を行うコンピュータ、ソユーズの姿勢制御用コンピュータ、スペースシャトル等のように、単純に同じ機能の機器を 3 重冗長にする方法がある。

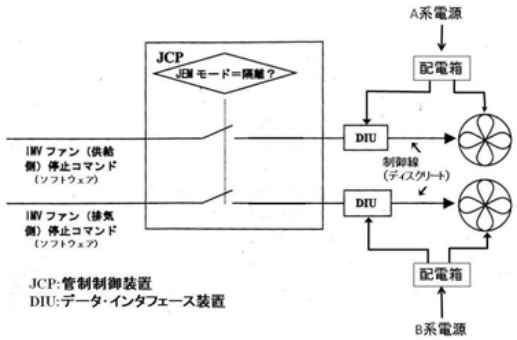
しかし、2FT が要求されるすべての機器を 3 重冗長にすると、システム規模が増大する。そこで、ISS では、対象機器追加以外の方法、すなわち機能で代替することにより、2FT を実現している。

例えば、「きぼう」と米国の第 2 結合部（Node2）間の棟間通風換気（以下 IMV）機能の停止は、二酸化炭素の蓄積による宇宙飛行士の二酸化炭素中毒につながるため、カタストロフィックハザードと識別されており、2FT が要求される。IMV 機能は、「きぼう」への供給側と排出側の 2 系統の IMV ファンにより実現している。ここでは、IMV ファン自身の故障だけでなく、系統全体としての故障も考え、系統の独立性も確保されなければならない。第 1 図に示すように、供給側は A 系電源、排出側は B 系電源から給電する設計となっており、供給側と排出側の IMV ファンは独立性を確保している。また、「きぼう」では、起動／停止の制御も同様に供給側は A 系電源をもつデータ・インターフェース装置によって行い、排出側は B 系電源を持つデータ・インターフェース装置によって行う設計となっている。この設計により、システムの片系停電が発生した場合でも、両系を失うことはない。

また、ハードウェアだけでなく、ソフトウェアコマンドについても、第 1 図に示す通り、送信系路の独立性を確保している。つまり、一つの誤コマンドで両系の IMV ファンを停止させてしまうことはなく、両系を遮断するためには、必ず二つのコマンドが必要となる。

さらに、「きぼう」の管制制御装置（JCP）は、「きぼう」が隔離状態にある時以外は IMV ファン停止コマンドを受信してもリジェクトする設計となっている。

2 系統の IMV ファンに加えて必要な残り一つのハザードに対する制御機能は、「宇宙飛行士の退避」により与えている。ただし、これを制御と扱うには条件があり、二酸化炭素の濃度の上昇時間が IMV ファンの停止の検出時間に対して非常に長いこと、各系統停止時に警報によって宇宙飛行士へ通報できる設計となっていること、「きぼう」から別の棟へ退避する通路が確保されていることが条件となっている。「きぼう」はこれらの条件を満足して 2FT を確保していることが確認されている[2)]。



第 1 図　IMV ファンの系統独立性

3.2 信頼度維持の設計

人工衛星では、信頼度解析を行い、要求される運用期間において所定の残存確率を確保できるようにシステムを設計するのに対して、「きぼう」では宇宙飛行士が機器の修

This document is provided by JAXA

理・交換を行うことによって、信頼度を維持できることが大きく異なっている。

これにより、「きぼう」に要求される運用期間より平均故障間隔（MTBF）の短い機器も搭載が可能となる。

「きぼう」では、事後保全により信頼度を維持するため、故障率からミッション期間中に必要な補用品の数を算出し、補用品の調達計画を策定した。本項では、その考え方について述べる。

3.2.1 故障事象の考え方

故障率の考え方は、一般的に第 1 表に示す 3 パターン [3] がある。「きぼう」のシステム機器は、高信頼性部品を使用しているため、初期故障は取り除かれていると判断でき、また、その部品個々の寿命も長いことから、故障率は一定と判断した。これらの条件から、故障率は CFR 形を採用した。

第 1 表　故障事象のモデル

DFR 形（Decreasing Failure Rate）	故障率減衰形、初期故障形
CFR 形（Constant Failure Rate）	故障率一定形、ランダム故障形
IFR 形（Increasing Failure Rate）	故障率増加形、集中故障形

CFR 形においては、故障はランダムに発生すると考えて、故障率（λ）は一定であることから、以下の通り、MTBF の逆数により表現できる。

$$\lambda = 1/\mathrm{MTBF} \qquad (1)$$

3.2.2 ランダム故障における故障率算出式

ランダム故障は、ポアソン分布となり、r 個の故障率 $P(r)$ は、以下の式で表現できる [3]。

$$P(r) = (\lambda T)^{r} e^{-\lambda T}/r! \qquad (2)$$

T：運用期間

$r!$：r 階乗

e：指数

（2）式から、運用時間（T）における信頼度 Q を以下の通り求めることができる。

$$Q = 1 - \Sigma P(r) \qquad (3)$$

信頼度 Q を、例えば「70％以上にしたい」場合、

$$0.7 < Q = 1 - (P(0) + P(1) + P(2) \ldots + P(r))$$

の計算を行う。その収束結果が

$$0.7 < 1 - (P(0) + P(1) + P(2))$$

という関係を成立させた場合、「信頼度 70％以上を保持するためには 2 個の補用品が必要である」と判断する。

3.2.3 MTBF の扱い

一般的に、MTBF の期待値は単一構成なら 1 を、二重冗長構成なら 1.5 を、待機冗長構成なら 2 を機器単体の故障率（λ）に乗じた下記の式で算出することができる [3]。

$$\left.\begin{array}{ll} \text{単　　一}: & \mathrm{MTBF} = 1/\lambda \\ \text{二重冗長}: & \mathrm{MTBF} = 3/2 \times 1/\lambda \ (=1.5/\lambda) \\ \text{待機冗長}: & \mathrm{MTBF} = 2 \times 1/\lambda \ (=2/\lambda) \end{array}\right\} \quad (4)$$

「きぼう」のシステム機器の評価においても、これらの算出方法に則した MTBF の期待値を用いた。また、MTBF の期待値の算出には、まず、部品点数法により、機器稼働状態及び機器休止状態での故障率（λ）を算出し、次にこのλを（4）式に代入して、機器稼働時の MTBF を MTBF（HOT）、機器休止状態での MTBF を MTBF（COLD）として求めた。

This document is provided by JAXA

3.2.4 運用時間の扱い

運用時間（thot）は、n 個の機器に対して、稼動率 A、運用年数を $_{top}$ とすると、

$$t_{hot} = n \times A \times t_{op} \quad (5)$$

で表わされる。

また、休止時間は

$$t_{cold} = n \times (1\text{-}A) \times t_{op} \quad (6)$$

となる。

ここで、運用年数（$_{top}$）は、「きぼう」のフライト時期（船内系システム：2008 年と船外実験プラットフォーム：2009 年）及び米国のステーション計画終了時期（2015 年）を考慮し、船内系システム搭載機器の運用年数を 8 年、船外実験プラットフォーム搭載機器の運用年数を 7 年とした。ただし、MTBF が運用年数に満たない等、稼働率を求められない場合は、MTBF を設計の前提であった当初計画の運用年数（船内系システム搭載機器 10 年、船外実験プラットフォーム搭載機器 9 年）で除して稼働率とした。

稼動率（A）は、一般に故障時間と稼働時間から求めるが、「きぼう」では、故障までの時間を算出するため休止時間と稼働時間から算出している。また、連続運転が必要な系統の稼働率は冗長構成および実運用状態を想定して単一構成及び 2 重冗長は 1、待機冗長構成は 0.5 とした。これらを第 2 表にまとめた。

第 2 表　稼働率の算出条件と結果

運　転	冗長構成	稼働率の予測	稼働率
連　続	単一、2 重冗長	可能	1
連　続	待機冗長	可能	0.5
間　欠		可能	予測値
上記以外		不可能	MTBF/運用年数*
*：　当初計画の運用年数使用（船内系システム搭載機器 10 年、船外系システム搭載機器 9 年）			

3.2.5 係数λT（故障率×運用期間）の扱い

故障確率 P（r）を算出する際、（2）式のλT は、以下の通りとなる。

$$\lambda T = \lambda' \times t_{hot} + \lambda'' \times t_{cold} \quad (7)$$

ただし、

λ'：（4）式で求めた MTBF（HOT）を（1）式に代入して求めた値

λ''：（4）式で求めた MTBF（COLD）を（1）式に代入して求めた値

t_{hot}：（5）式による。

t_{cold}：（6）式による。

3.2.6 必要な補用品の個数算出結果

「きぼう」の搭載機器について、故障している機器がない確率を 80%あるいは 90%に設定して必要な補用品の個数を算出することは可能であるが、高確率になればなるほど必要な補用品の個数が増加し調達費用が膨大となる。

そこで、「きぼう」のシステム機器としては、既に開発された人工衛星や宇宙機器の信

This document is provided by JAXA

頼度の最低ラインの設定実績等を考慮し、故障している機器がない確率を 70%に設定した。

この方針に従い、(7) 式で求めた値を (2) 式に代入し、3.2.2 項の手順に従って、必要な補用品の個数を求めた。その結果の一部を第 3 表に示す。

この結果に基づき、補用品の調達計画を立案し、この計画を実行中である。また、軌道上の故障状況によって、随時、補用品の調達計画に反映していく予定である。

第 3 表　補用品必要数の算出結果

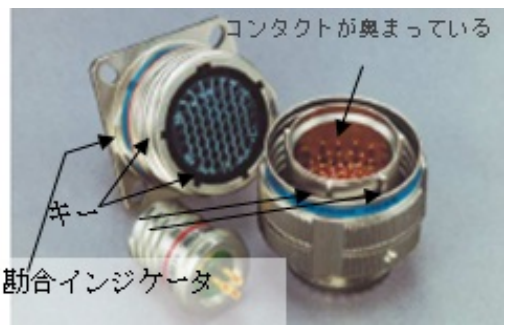
機器名称	MTBF (HOT) [年]	使用数	冗長	稼働率	補用品必要数
データ・インターフェース装置 I 型	14.8	6	無	1	4
配電箱 II 型	46.5	7	無	1	2
JEM 管制制御装置基幹部	5.6	2	待機冗長	0.5	1
空気調和装置制御部	10	2	2 重冗長	1	1

3.3 人為故障の除去

「きぼう」の安全・開発保証要求書 [4] に、部品のランダム故障以外の故障の原因の一つとして人為的な故障が挙げられている。

「きぼう」では、軌道上組立、機器交換時等のミスによって、システムに人為故障を起こし、信頼性を下げることがあってはならない。このため、軌道上での宇宙飛行士による機器の交換が、容易で、安全かつ確実に実施できるように、軌道上交換単位（ORU : Orbital Replaceable Unit）に装置を分割すると共に、交換機器に対しては様々な設計上の工夫がなされている [5]。

例えば、ORU 及びシステム側ハーネスのコネクタは、ORU に複数のコネクタがある場合、誤って接続されないように、それぞれのコネクタの形状やキーを変えている。また、コンタクトピンの曲りやインサートの破損を防ぐためにコネクタシェルの勘合後にコンタクトが勘合する Scoop Proof 型を使用すると共に、締付け不足による接触不良を無くすためにカラーバンドによるインジケータ付きを使用した（第 2 図参照）。

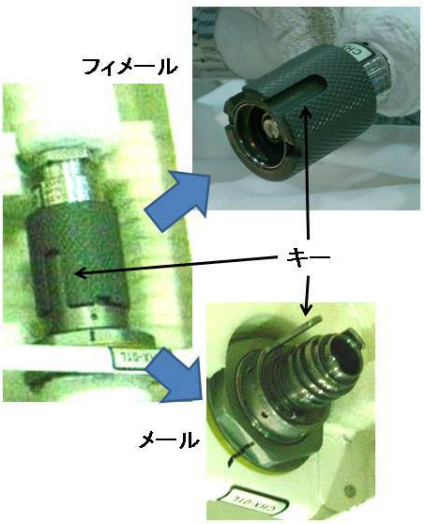


第 2 図　コネクタの特徴

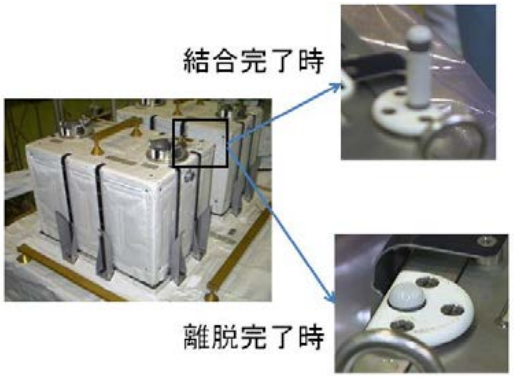
This document is provided by JAXA

また、流体用コネクタ（QD : Quick Disconnect）についても、搭乗員による操作が必要な場合には、誤接続されないように独自のキー溝がついた QD を使用すると共に、ORU の艤装設計として Blind Access を禁止している（第 3 図参照）。

また、船外実験プラットフォームのシステム機器のように、宇宙飛行士が船外活動で取付け／取外しを行う ORU は、第 4 図のような脱着のインジケータ機構をもっている。これにより、宇宙飛行士の誤認によるシステムの不適合を防ぎ、システムの信頼度低下を防ぐことができる。システムの二次構造への ORU 取付用ファスナへのツールアクセスには、視認性とツールのクリアランスを確保するように要求されており [5]、締付け不足等の人為ミスによって、ISS の姿勢や軌道変更時に ORU が浮遊するカタストロフィックハザードにならないよう設計されている。



第 3 図　QD のキー



第 4 図　船外実験プラットフォーム用 ORU の着脱インジケータ

4. まとめ

「きぼう」では、有人宇宙システム特有の取組みとして、2FT 要求実現、信頼度維持設計及び人為故障除去等により、信頼性を向上させる技術の実現および管理を実施してきた。こうした技術は、宇宙ステーション補給機（HTV）などに応用されている。

本技術の構築にあたり、ご尽力をいただいた関係各位に深謝する。

This document is provided by JAXA