Vol.2016-CVIM-202 No.4
2016/5/12

人工衛星システムの信頼性確保 ～耐故障設計を中心に～

植田泰士[†1]　片平真史[†1]　鈴木新一[†1]

概要：人工衛星や探査機などの宇宙機システムは多くが非修理系であることから一発勝負の中での高い信頼性確保が必要となる．その信頼性を確保するための方策の一つとして，クリティカルな異常が発生した場合には自律的に故障を検知し，故障を分離し，正常状態へ回復させる耐故障設計が多くの宇宙機システムには導入されている．これまでそのような宇宙機システムの機能の実現，あるいは宇宙機システムの開発プロセスにおいて，コンピュータビジョン技術が直接的に活用される局面は少ないが，本稿では，コンピュータビジョン研究者による今後の宇宙機システムへのコンピュータビジョン技術応用検討の一助となることを期待し，陸域観測技術衛星 2 号（ALOS-2）を主な題材として耐故障設計の考え方などを紹介する．

Ensuring dependability of a satellite system - focusing on fault tolerant design -

YASUSHI UEDA[†1]　MASAFUMI KATAHIRA[†1]
SHINICHI SUZUKI[†1]

1. はじめに

人工衛星や探査機など一般的な宇宙機システムと地上で動作するロボット等を比較した場合，宇宙環境等の特殊性に依存して下記のような様々な差異が存在する．

- 打上げ時
  - ロケットから受ける激しい振動・音響・衝撃環境に耐えなければならない．
- 軌道上
  - 国際宇宙ステーション等の有人システムを除き，故障したハードウェアは**修理できない**．
  - 高真空環境：熱対流がないこと，材料の蒸発・凝着などへの対策が必要．
  - 微小重力環境：浮遊物によるショートなどが生じない対策が必要．
  - 太陽光環境：システムから常に太陽光が見えるとは限らないためエネルギー獲得タイミングは限られる．また熱入力量も大きく変化するため，昼夜の温度差に耐える対策や，紫外線等による熱制御材の劣化等も考慮する必要がある．
  - 放射線環境：銀河宇宙線や太陽フレア等による高エネルギー粒子が電子部品に衝突しても誤動作しないように対策が必要．
  - スペースデブリ（宇宙ごみ）環境：地球近傍に多量に存在するスペースデブリ衝突対策が必要．
  - 通信環境：常に地上から通信可能な場所にシステムが存在するとは限らない．また深宇宙空間においては通信遅延量も大きく，回線幅も狭い．

また JAXA の宇宙機システムの開発にはおいては，その役割から下記特徴も加わることとなる．

- **システムは全て一品もの開発**であり，二度同じものは作れない．
- 新規技術開発要素を多く含むことなどから開発に要する期間も長く、開発コストも大きい．
- 経年劣化が生じる中で長期動作保証が必要（実利用性確保や深宇宙航行時間）．

以上から，JAXA における宇宙機システム開発は，一発勝負の中で成功するために,限られた期間とコストの中で,宇宙環境等の特殊環境にも耐え得る，高い信頼性を有するシステムを如何に開発するかが，高い性能の実現とともにあわせて重要な点となる．

このような宇宙機システムの実現，あるいはその開発プロセスにおいて，コンピュータビジョン技術（画像からの被写体世界の認識・理解）が直接的に活用される局面はまだ少ないが，本稿では，今後，コンピュータビジョン研究者によって，コンピュータビジョン技術を活用したより高度な宇宙機システムの実現が図られていくことを期待し，応用先のシステムがおかれる場の理解の一助するため，信頼性確保の観点から JAXA で採っている方策を紹介する．

2. 信頼性確保方策

2.1 概要

JAXA では宇宙機システムの信頼性を確保するために様々な方策が，設計・製造・試験・打上げ・運用の全ライフサイクルにわたって採られ，そのプロセスや基準となる

†1 国立研究開発法人宇宙航空研究開発機構
Japan Aerospace Exploration Agency（JAXA）

設計の標準化が図られている[1]．本項では，その代表的な方策を示す．なお達成すべき信頼性は，プロジェクトの規模や目的により異なるため、プロジェクトごとに決定されるものであるであるが，主に実利用に供される JAXA の大型衛星を前提として述べる．

(1) 設計

上記前提において近年採られている基本的な設計思想は

- 1 フェイル・オペラティブ：1 故障でもミッションを維持させる
- かつ 2 フェイル・セーフ：2 重故障が発生してもシステムを安定した状態で生存させる

である．これを実現するため設計として下記方策をとっている．

① 冗長化

2003 年 環境観測技術衛星（みどり II）の太陽電池パドルの発生電力が 6kw から 1kw に減少し、衛星との交信ができなくなり運用を断念する事象が発生した．原因としては電力伝送機能の異常によるものと推定されているが，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[*1] のみならず波及故障[*2] 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ている[2]．このことから電力・通信制御系統など構成する電子機器などにランダム故障が想定される系統においては機器の冗長化を原則行う．また機器間の配線も冗長化し，相互の主系・従系をクロスストラップで接続することなどにより，単一故障で他の機器の冗長系を失うような影響が波及しないよう単一故障点[*3] を排除するアーキテクチャを採る．

計算機については冗長系の構成方法として，多数決冗長系，待機冗長系のどちらも採る場合がある．前者は，1 系統に故障が発生しても，機能性能を完全に維持した状態で運用することができるが，システムが複雑化し検証難易度やコストは上昇する．後者は，システムが比較的単純であるが，一時的な機能低下，復帰させるための運用が必要となるため，システムの特性に応じた選択となる．

その他さらに別の機器で他の機能を補完させる機能冗長を加えることもある（2.2 項参照）．

② 自律的な故障検知・分離・回復（FDIR：Failure Detection Isolation and Recovery）、誤り訂正

宇宙機システムは，常に地上から通信可能な場所にシステムが存在するとは限らないとともに，異常が発生した場合に状況が悪化する前に即座に対処をうつ必要があるため，自律的に故障を検知し，故障を分離し，冗長系へ切り替えるなどにより機能の回復を図る機能を持たせる（2.2 項参照）．

なおメモリ等のデータについては，誤り訂正符号による誤り検出と訂正が図られている．

③ 軌道上不確定性に対するマージン確保

機器の筐体や衛星の構体，あるいは大型のアンテナなど冗長化策を選択できない部位もある．このような部位に対しては，構造・機構・熱などの観点から軌道上の不確定性を考慮した適切な設計マージンを確保することによりリスクを最小化させる方策を採る．

(2) 解析等による設計検証

前項で述べたマージンが十分確保されているかは，様々な設計解析を元に判断を行う．解析観点としては，軌道解析，熱解析，構造解析，通信解析，姿勢制御解析，電力解析，データ収支解析，放射線解析，故障解析，寿命解析，信頼度解析など多岐に渡る．詳細は本稿では述べないが，主としてシステムがおかれる状況の最悪条件を考慮し，その状態でも機能性能を維持できるかを各解析により判断する．

またその結果として妥当な設計であることについては，独立的な立場の評価者を交えた開発フェーズごとのマイルストーン審査（図 1 参照）を経ながら段階的詳細化を行うプロセスにてリスクの最小化を図る．

図 1 JAXA におけるシステム開発プロセス
Figure 1 System development process in JAXA

(3) 試験等による検証

故障発生時のシステム喪失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，製造段階での製造ばらつき，人的過誤も起こり得ることや新規技術開発要素を多分に含むため設計時に想定していた解析前提が正しいかを検証する必要があるため，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となる．

*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 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 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

① 検査

宇宙機システムは膨大な点数の部品で構成されるが，その一つ一つの部品の品質が欠如してもシステムの機能を果たせなくなる可能性があるため部品単位からその製造手順を含めて，検査や品質管理を行う．ここには，溶接、はんだ付、熱処理、表面処理等など，外観検査や寸法検査のような通常の方法による製品の検査だけでは、製品の品質を保証することができない工程も含まれ，放射線透過検査や超音波探傷検査などによる非破壊検査なども行い，信頼性は末端から積み上げていくこととなる．また全ての品質記録が適切に残され管理されていることにより，開発中に問題が発生した際にも原因を究明することが可能となる．

② 試験

″Test as You Fly，Fly as You Test″[6]の原則の下，製造した機器やシステムは，宇宙機システムがさらされる環境を地上で可能な限り模擬し，環境負荷を与えた上で，設計意図通りの機能性能が発揮されていることを確認し，必要な特性を計測する．この中では 1 項で示した様々な環境を模擬した下記のような試験を行う．

- 打上げ環境を模擬した試験
  - 振動試験
  - 音響試験
  - 衝撃試験
- 軌道上環境を模擬した試験
  - 熱真空試験（図 3 参照）
  - 放射線試験
  - 電磁適合性試験
  - 寿命試験など

なおこれらの試験は，システム全体が組みあがって初めて実施するのではなく，システム構成要素から段階的に実施していくものである（図 2 参照）．

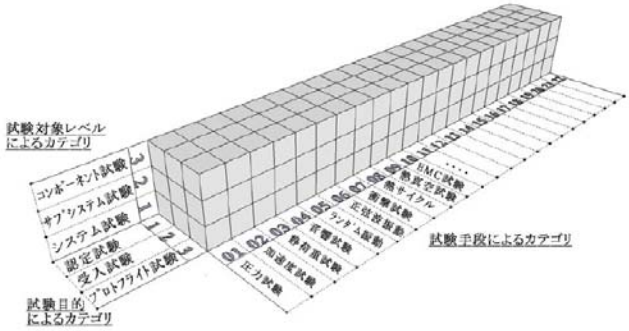

図 2　試験体系モデル[3]

Figure 2　Model of a test system for spacecraft

図 3　熱真空試験

Figure 3　Thermal vacuum test

2.2 耐故障設計事例：陸域観測技術衛星 2 号（ALOS-2）

2.1 項の信頼性確保方策のうち，宇宙機システムの特徴がより強い，冗長化・FDIR に関する耐故障設計について，陸域観測技術衛星 2 号（ALOS-2）を題材に，具体的な耐故障設計の考え方を示す．

陸域観測技術衛星 2 号（ALOS-2）は，防災機関における広域かつ詳細な被災地の情報把握，国土情報の継続的な蓄積・更新，農作地の面積把握の効率化，森林観測を通じた地球温暖化対策など、多岐に渡るミッションを目的として，JAXA が開発し 2014 年 5 月 24 日に打上げ，現在軌道上で運用中の衛星である（図 4 参照）．観測機器としては、高性能マイクロ波センサ「フェーズドアレイ式 L バンド合成開口レーダ PALSAR-2」を搭載する．

図 4　ALOS-2 衛星システム外観

Figure 4 the ALOS-2 system in launch configuration

(4) システム構成

ALOS-2 のシステム構成を図 5 に示す（図中の用語は参考文献[6]参照）.

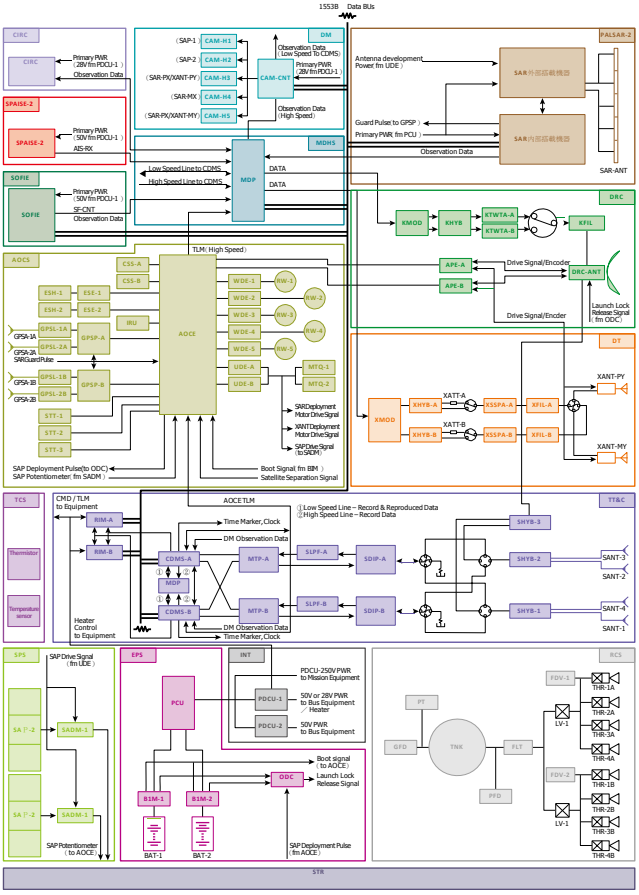

図 5 ALOS-2 システム構成
Figure 5 Block diagram of the ALOS-2 system

(5) 冗長化設計と FDIR

本システムは，そのミッションの重要性から 2.1 項で述べた設計思想同様，1 フェイル・オペラティブ，2 フェイル・セーフのシステムとなっている.

① 同一設計物による冗長

図 5 に示す各機器の名称に「-A」「-B」が付与されている通り，原則全ての機器が冗長化されている.（図中で「-A」「-B」がないものは，機器の内部冗長化が図られている．ただし一部の技術実証目的の機器を除く）.

例えば，ALOS-2 の前号機では太陽電池パドルは進行方向左側に長く延びた 1 翼方式であったが，ALOS-2 ではレーダが衛星下面にあり視野の問題がないため，2 翼方式にし，片翼が故障して発生電力が半分になった場合にも，電力負荷を削減し限定的な観測運用を行う縮退モードによってミッションを継続できる設計となっている.

② 機能冗長

2.1 項で触れた通り，別の機器で他の機器の機能を補完させる機能冗長性を持たせることがある．つまり全く異なる設計間で，同様の機能を実現させることとなる．ALOS-2 において機能冗長が実現されているのは下記の 2 点となる.

a) 姿勢･軌道制御系サブシステム（AOCS:Attitude and orbit control system）:

例えば姿勢制御に際し，アクチュエータ制御量を算出するために姿勢決定を行うにあたり，慣性基準装置*4 を使えば，角速度積分による姿勢伝播で姿勢が求まることとなるが，必ずバイアス誤差が生じるため，他センサによりバイアス推定と姿勢誤差修正を行う必要がある．ここに対し，ALOS-2 では定常時は恒星センサ*5 を用いて高精度な姿勢決定を行っているが，同時に太陽センサ*6．地球センサ*7 も有しており，恒星センサに万一異常が発生した場合にはいつでもその代替を図ることが可能となっている．またアクチュエータについても機能冗長を持つ.

b) 衛星-地上間通信ルート：

衛星の状態を通知する情報（HK テレメトリ）は，S バンドアンテナ経由でも X バンドアンテナ経由（高速回線）でも地上へダウンリンクさせることが可能となっている．また観測を行ったミッションデータのダウンリンクについても，X バンドアンテナ経由または中継衛星用アンテナ経由のダウンリンクが可能であり機能冗長が図られている.

(6) FDIR

① システムレベル

システム全体の FDIR を司っているのは図 5 中における CDMS（Command & Data Management System）となる．CDMS にてシステム内全体の各機器の温度，電圧，バッテリ残量，ステータス値等を常時チェックしている（CDMS 自身は従系に監視させる）．それらのモニタ項目において，万一正常域からはずれた場合，CDMS は各機器に対し

・異常な機器を切り離し，その冗長系を起動
・システムが生存するために必須ではない機器を OFF し電力消費を抑える

*4 IRU（Inertial reference unit）：複数のジャイロスコープを組み合わせて衛星 3 軸の角速度成分を検出する装置
*5 STT（Star tracker）：高感度の 2 次元 CCD や CMOS センサと高性能マイクロプロセッサを使い，複数の恒星のパターン認識と統計処理により恒星の放射する可視光から慣性空間での衛星の姿勢を高精度に検出する装置
*6 SS（Sun Sensor）：太陽の放射する可視光から太陽方向を検出する装置
*7 ESA（Earth Sensor Assembly）：地球の大気（水、CO2)が放射する赤外線を検出し地球方向を検出する装置

・より安全な姿勢，および制御方式に移行させ電力を確実に確保する
・送信機を起動し，衛星の状態を地上に常時発信し，確実に地上から状態が分かるようにする

などの指令を送る（ただし異常の項目と度合いによって，措置内容は異なる）．これによりシステムとしてセーフティな状態へ自動移行し，セーフティを維持した上で人間が原因究明と対処を検討することが可能な設計となっている．

② サブシステムレベル

システムレベルで上記の FDIR が存在する一方であらゆる異常に対し，全てシステム全体をセーフティに落とすとした場合，衛星システムとしてのサービス可用性を下げかねないとともに定常状態へ戻すための運用負荷も大きいことから，サブシステムレベルで耐え切れる異常はサブシステムで措置する考え方となっている．

サブシステムレベルで最も高い自律性を有するのが AOCS である．AOCS は前述の機能冗長を有していることもあるが，そもそも姿勢の喪失は，電力喪失，通信断絶につながり，「短時間」の異常でシステムの生死に直結する可能性のある極めてクリティカルなサブシステムであるため，自サブシステム内で即座に異常な機器の冗長系への切り替え，機器再起動，使用するセンサ組み合わせの変更等を図る．よって異常の程度が軽微である場合は，観測ミッションを中断することなく運用することも可能であり，高いレジリエンス性を有するシステムとなっている．

2.3 衛星システムへのコンピュータビジョン技術の活用について

今後，衛星システムへ高度なコンピュータビジョン技術を活用することを考えた場合，前項までに述べた信頼性確保の観点などから，活用を検討する際に考慮すべきであろう主な制約条件を示す．ただし衛星システムのアーキテクチャが今後も進化していく中で，その前提は変わる可能性はあることに注意されたい．

① 検証可能性とデータ量の少なさ：

システムの信頼性を確保するため，機能の検証可能性を十分担保する必要がある．仮に機械学習のような帰納的手法を適用した場合，演繹的な妥当性判断が難しいと想定されるため，実証主義的な立証を図る以外の手段はないと思われる．一方，宇宙機システムのおかれる環境は総じてスモールデータである．実証可能機会の少なさや，システムリソースに限りがあることから実証用のデータが限られているとともに，深宇宙探査等であれば撮像対象物やその環境条件は，目的地到達後に初めて得られるデータとなる．これらを踏まえてリスクを最小化するための方策を同時に検討する必要がある．

② 計算機能力：

計算機環境としては，放射線の影響を受けにくい部品（MPU、メモリ）を使用しなければならないとともに，熱対流がないことから排熱能力に限界があるため，CPU は低発熱・低消費電力である必要があり，民生品に比べると相対的にスペックも低い*8．画像データ量や処理内容にもよるが，画像データをオンボードリアルタイム処理するには FPGA ハードウェア処理等が必要となる．

③ 通信レート：

システム内通信レートとしては，バス通信型アーキテクチャ衛星における制御用低速バス（1553B 等）は 1Mbps 以下，SpaceWire や個別のミッション観測データ系用高速インタフェース（RS422，LVDS 等）では～数百 Mbps である．また衛星システム～地上間での通信レートは，地球近傍の ALOS-2 で最大 800Mbps（打上げ時，地球観測衛星で世界最高速度）であるが，電波は距離の二乗に反比例し弱まるため深宇宙探査機となるとその通信レートは激減する．このように地上の計算機通信レートとはオーダが異なるため，この点も制約となり得る．

3. おわりに

本稿では，コンピュータビジョン研究者に対するコンピュータビジョン技術の応用先である宇宙機システムの理解の一助するため，信頼性確保の観点から JAXA で採っている方策を紹介した．

宇宙機システムは，様々な制約を受けるシステムではあるが，逆に様々な制約条件が存在するからこそより高度に自律的な認知・判断がなければ高度なミッションを実現しえない場合もあるフィールドである．今後，コンピュータビジョン技術を活用したより高度な宇宙機システムの実現が図られていくことを期待する．

謝辞 本稿作成に際し，助言を頂いた JAXA 片山 保宏氏，同 山元 透氏に謹んで感謝の意を表する．

参考文献

[1] 宇宙航空研究開発機構, JMR-004C 信頼性プログラム標準,

*8 現国産宇宙用 MPU：64bit, 320MIPS 相当

2015.
[2] 宇宙航空研究開発機構, JERG-2-120 単一故障・波及故障防止設計標準, 2010.
[3] 宇宙航空研究開発機構, JERG-2-130 宇宙機一般試験標準, 2012.
[4] 浜崎敬，衛星システムのディペンダビリティとディペンダブル VLSI への期待，ディペンダブル VLSI システムワークショップ, 2011.
[5] " Test as You Fly, Fly as You Test, and Demonstrate Margin". http://llis.nasa.gov/lesson/1196
[6] "だいち 2 号". http://fanfun.jaxa.jp/countdown/daichi2/files/daichi2.pdf