JSASS-2022-4259

2D04　火星衛星探査計画 MMX ミッションロバスト化のための航法誘導制御ソフトウェア独立検証

○大野剛，吉川健人，巳谷真司，木下貴博，今田高峰(宇宙航空研究開発機構)

Independent Verification and Validation of Guidance, Navigation and Control System Software for Robust Mission Execution of Martian Moons eXploration (MMX)

Go Ono, Kent Yoshikawa, Shinji Mitani, Takahiro Kinoshita, Takane Imada (JAXA)

Key Words: MMX, GN&C, FTA, FDIR, IV&V

Abstract

The Martian Moons eXploration (MMX) is a mission to achieve sample return from one of the Martian moons, Phobos, for the first time in the world. In this paper, the independent verification and validation of a guidance, navigation and control (GN&C) software for robust mission execution of MMX is summarized.

1.　はじめに

火星衛星探査計画 Martian Moons eXploration (MMX)は，火星衛星からの世界初のサンプルリターンミッションである[1]．2024 年度の打上げを目標として検討を進めている．参考までに，火星衛星フォボスへの降下着陸時のイメージを図 1　フォボス地表面への降下着陸時 (想像図)に示す．

図 1　フォボス地表面への降下着陸時 (想像図)

探査機システムの航法・誘導・制御(GN&C)は，全ミッション期間中に必要不可欠なサブシステムである，また，そのソフトウェア設計は，火星周回軌道投入やフォボスへの降下着陸等のクリティカル運用を成功させる上で，特に重要である．MMX プロジェクトでは，最重要なミッションであるサンプルリターンの成功確率を高めるための検討活動を「ミッションロバスト化」と称し，探査機システム，ミッション機器，地上システム等の全構成システムを対象に，種々の検討を行っている[1]．本稿では，その検討内容について，探査機システム開発企業が設計する GN&C ソフトウェアに対して，JAXA が実施する独立検証活動を中心に紹介する．

2.　Fault Tree Analysis(故障の木解析)

MMX ではフォボスからのサンプルリターンを目指すため，ロケット打上から火星圏への到着，火星圏での滞在，フォボスへの降下着陸，地表面でのサンプル採取，地球帰還，カプセル分離までを完遂しなければならない．ミッション期間中に多数の運用が計画されており，クリティカル運用は下記の通り定義・分類されている[1]．

・ワンチャンスイベント：往復伝播時間である 40 分間探査機が何もしないと探査機全損，または，ミッションフェールとなる異常が発生する運用．

・タイムクリティカルイベント：運用時間等の制約により対応に十分な対応時間が確保できない運用．

これらの運用の中から，特に新規性・難易度が高いと識別されるものを対象に，Fault Tree Analysis(FTA，故障の木解析)を実施した．各運用の失敗をトップ事象とした仮想的な FTA 解析を行うことで，不具合事象発生の経路を事前に明確化し，安全性・信頼性向上のための対策を取ることが目的である．探査機システム，ミッション機器，地上システム，全てを組み合わせた総合システムとして運用する主体は JAXA であり，各構成要素を横断的に確認することは，ミッションロバスト化における重要な観点の一つである．全 6 つの FTA のトップ事象，および，対応する運用を表 1 に示す．

表 1　FTA

トップ事象	対応する運用
軌道投入に失敗	・火星周回軌道投入 ・デイモスフライバイ ・火星周回軌道脱出
モジュール分離に失敗	・往路モジュール分離 ・探査モジュール分離
低高度 QSO 周回中に QSO 離脱(共軌道への離脱, または, フォボスへの衝突)	・QSO 周回 ・QSO 遷移
ローバ分離に失敗	・ローバ分離
サンプリングに失敗	・降下 ・接地・着陸・滞在 ・離陸・上昇
カプセル回収に失敗	・カプセル分離 ・カプセル回収・輸送

各 FTA は，トップ事象を起点とし，それに至る要因事象を列挙する一般的な手法で検討し，コンポーネント単位に落とし込むまで分析した．誌面の都合上，全てを示すことはできないが，参考として「軌道投入に失敗」の FTA の一部を図 2，図 3 「軌道投入に失敗」FTA の一部に示す．トップ事象を起点に，失敗に至るフェーズに分けた後，不具合事象から探査機システムや地上システムの機能，運用対応へ分解している．そして，末端の要因事象に対して，設計・試験・検査・運用の段階で取れる対処をまとめた．末端の要因事象は探査機システム，地上システム，運用に関連するものに分類できる．以下にそれぞれの分析結果を概略的に示す．

・探査機システム : 要因事象の多くは，サブシステム(GN&C 系，推進系，通信系等)のコンポーネント異常であり，MMX 信頼性設計の仕様通り，冗長設計とされていること，あるいは，十分な信頼性を根拠にシングル設計とされていることを確認した．GN&C ソフトウェアの FDIR 設計や，その他機器等の解析条件，試験条件等に考慮すべき詳細を識別し，引継事項とした．

・地上システム : 基本的に全て冗長設計であり，異常を地上で識別可能である．

・運用 : 運用中に取り得る対処を識別し，運用設計や文書へ反映した．

本解析を通じて，上記のような対策を確認すると共に，各システムへの仕様配分を行った．

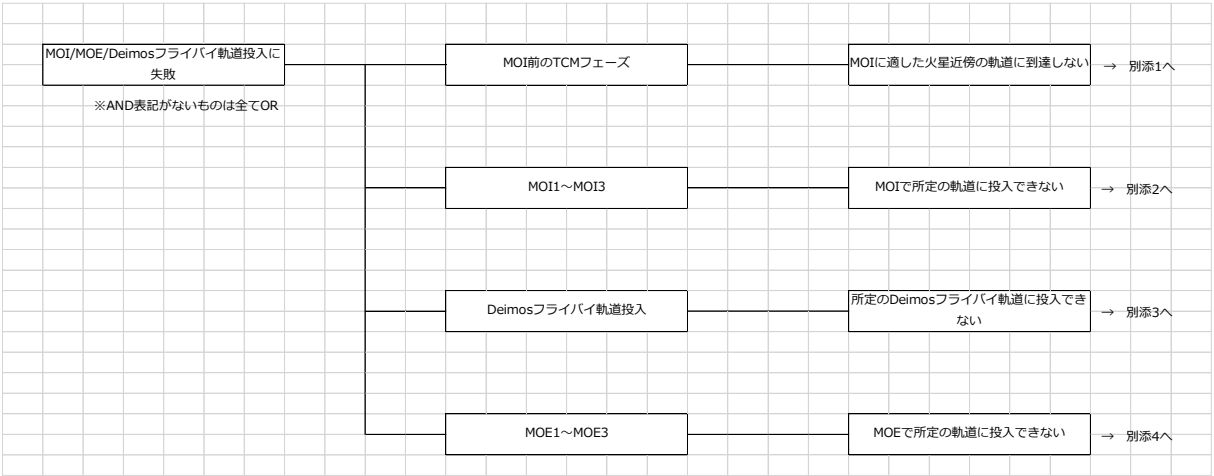

図 2　「軌道投入に失敗」FTA の一部(1/2)

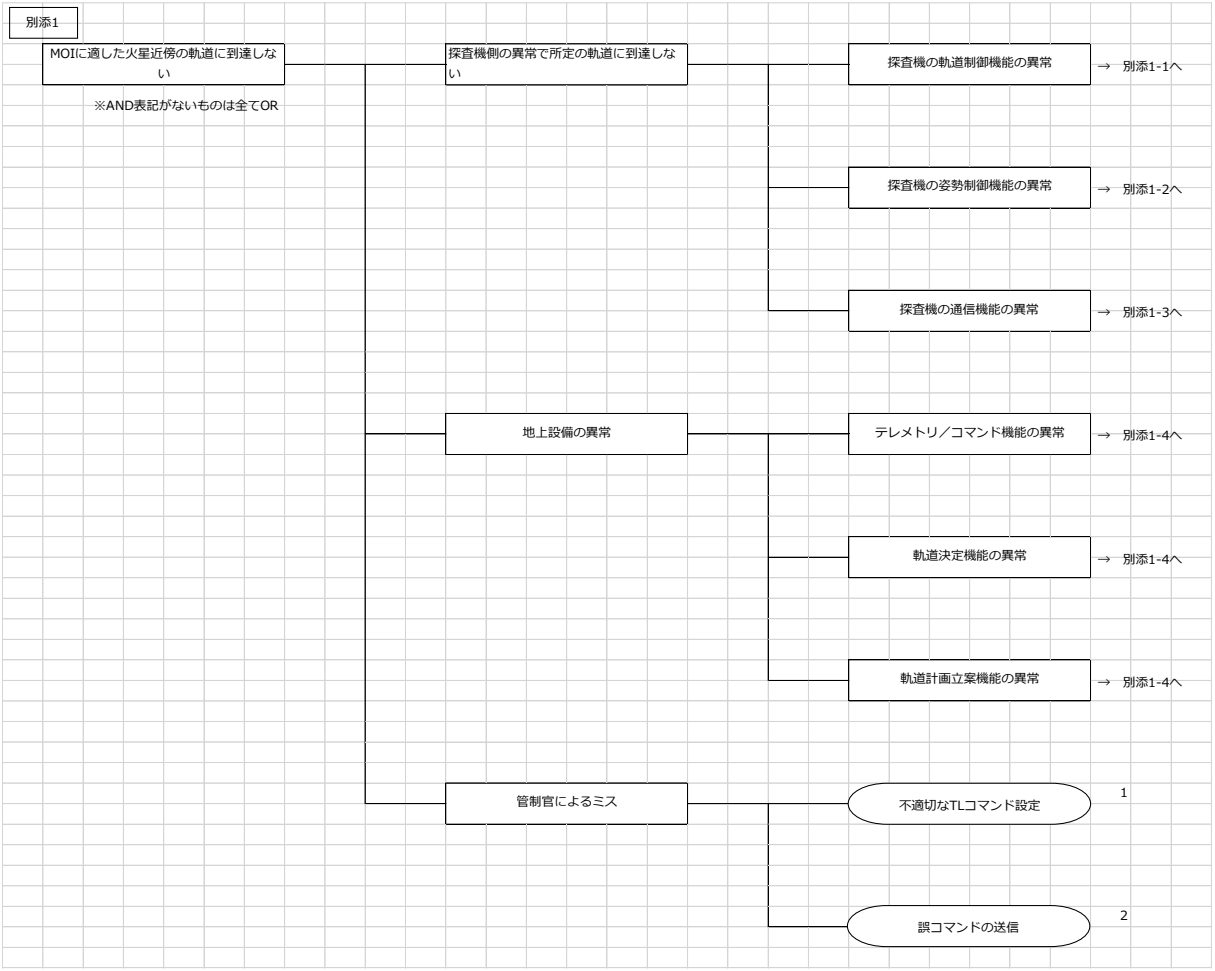

図 3　「軌道投入に失敗」FTA の一部(2/2)

3.　FDIR 独立検証

次に，JAXA が実施した FDIR 独立検証活動について紹介する．GN&C 系が司る最も重要な機能の一つである FDIR 設計に対し，早期から独立検証を行ってきた．これまで JAXA が運用してきた宇宙機の知見を活用・反映すべく，探査機システム開発企業が設計する内容に対し提言する活動である．

本活動内容の一つとして，GN&C 系航法センサの過大値異常，一定値異常，変化率異常，ドリフト異常，シフト異常を体系的に想定することが挙げられる．各異常の概念図を図 4 に示す．

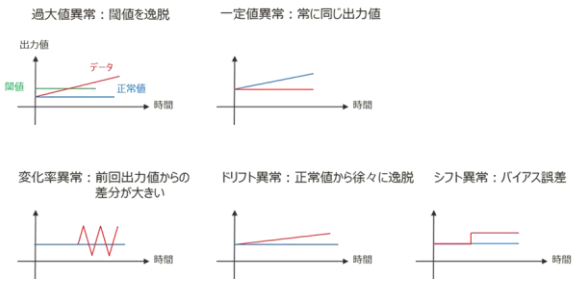

図 4　航法センサの異常

これら 5 種類の異常を想定する航法センサの対象は，IMU(ジャイロ)，IMU(加速度)，STT，ALT の 4 つとした[1]．つまり 5×4 の表として，各センサが各異常を示した際に，FDIR 設計として検知可能であるか，対処可能であるか，を網羅的に確認した．設計反映の結果，閾値や前回値，参考値との比較により異常を検知し，冗長系切替により対処することを基本方針とした．

4. Independent Verification and Validation(ソフトウェア独立検証・有効性確認)

最後に, ソフトウェアの Independent Verification and Validation(IV&V，独立検証・有効性確認)について紹介する(本項での IV&V が意味するものは，所謂「ソフトウェア IV&V」であり,「ミッションロバスト化」のような広義の独立検証活動ではない)．一般的な IV&V 同様, 探査機システム開発請負組織が必要な管理活動, 評価, 解析等を実施していることを前提に, 独立した第三者組織が，搭載ソフトウェアを客観的に評価し, 潜在する問題点の識別, 問題点解決に向けたフォローアップを実施するものである．探査機の安全性，信頼性，保全性，品質確保・向上に貢献することが目的である. MMX における IV&V の実施体制を図 5 に示す.

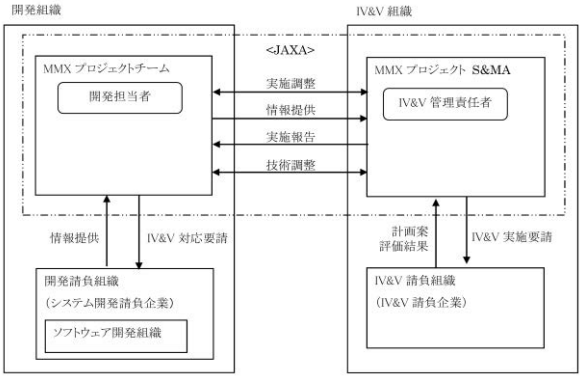

図 5　IV&V 実施体制

IV&V では一般的に, プロジェクトチームが持つ漠然とした懸念を起点に分析を始める．MMX では，前述したワンチャンスイベント，タイムクリティカルイベントが重要な運用であるため，これらに関わる懸念を挙げることから開始した．その後，IV&V 請負組織により，保証シナリオ(運用やソフトウェアの前提，特徴，懸念に関わる情報を整理した一覧表)が作成され，検証の観点や深さを明確化した.

この時, 多数の保証シナリオが作成され, 作業規模から現実的な数に絞り込む必要があった．全ての保証シナリオはクリティカル運用に関わる懸念に基づいており, いずれも重要な内容であるため, 絞り込みには苦心した．考慮すべき観点として挙げたものを以下に示す.

・探査機喪失：探査機喪失に繋がる懸念を優先する
・オフノミナル処理 : 異常検知後の復帰処理・運用継続処理等，オフノミナル処理を優先する
・MMX 固有 : 惑星間軌道・着陸・接地・離陸等, MMX 固有の処理を優先する
・環境依存 : フォボス環境依存である懸念を優先する
・偽陰性 : 偽陽性によりアボートする懸念より, 偽陰性により異常対処されない懸念を優先する

これらを複合的に考慮しつつ, 最終的には, プロジェクトチームメンバーが重要と考える保証シナリオを選定した．選定したものの概要を表 2　に示す.

表 2　検証対象として選定した保証シナリオ概要

保証対象	対象 ソフトウェア
火星周回軌道投入および火星周回軌道脱出時に, 姿勢異常を誤検知し(偽陽性)，1 故障にも関わらず, 安全化処置を実行するリスクがある.	GNFS
火星周回軌道投入および火星周回軌道脱出時に, 姿勢異常を検知できず(偽陰性)，姿勢異常にも関わらず, 安全化処置を実行しないリスクがある.	GNFS
垂直降下への切替時(高度約 2km)において, CAM-W で撮像した画像データ，画像航法データ，ALT 高度データに他サブシステムの干渉(タンク液剤の振動)や必要な環境情報の不足・間違いや変化等があり, 期待する推定位置や制御ΔV が出力できないリスクがある.	IMGFS，GNFS
入力情報に誤り(偽陽性)があり，接地していないにもかかわらず接地したと判定されてしまうリスクがある.	GNFS

検証スコープが大きくなり過ぎないよう，火星周回軌道投入および火星周回軌道脱出運用では姿勢異常に，降下着陸運用では垂直降下への切替と接地判定に焦点を当てることとした. また, 検証対象となるソフトウェアは, 画像航法系ソフトウェア(IMGFS)と航法誘導制御系ソフトウェア(GNFS)である．表 2 に示すリスクが実際に潜在するのか，具体的な問題と解決方法は何であるか，を下記の観点で検証する.

・上位仕様との整合性確認 : 上位仕様と評価対象仕様が整合していることを確認する

・インタフェースの整合性確認:インタフェース仕様が，サブシステム及びミッション機器側のインタフェース仕様と整合していることを確認する.
・状態遷移の完全性及び一貫性確認:動作モード及び制御状態等の遷移条件に矛盾及び抜けがないことを確認する.
・故障検知, 分離, 及びリカバリ(FDIR)の完全性確認:発生し得る故障及び検出処理とリカバリ処理に対して，処理条件の抜けや誤りがないことを確認する.
・処理タイミングの妥当性:想定しないタイミングでのイベント発生により，ソフトウェアの機能が損なわれるような処理タイミングが内在しないことを確認する.
・試験仕様の網羅性 : ソフトウェア設計仕様書, インタフェース仕様書に基づき試験仕様を識別し，計画された試験仕様との比較において，ソフトウェア機能の確認漏れが無いことを確認する.

検証作業は未了であるが, 現時点において, ソフトウェアの要求仕様書や設計仕様書への上位仕様反映漏れ, 不明確なインターフェース仕様, 不具合発生時のオフノミナル処理に関する指摘が挙がり，成果が得られている.

5. おわりに

MMX プロジェクトでは, 最重要なミッションであるサンプルリターンの成功確率を高めるための検討活動を「ミッションロバスト化」と称し，探査機システム, ミッション機器, 地上システム等の全構成システムを対象に, 種々の検討を行っている. 本稿ではその中でも，GN&C ソフトウェアに関する内容を中心に概説した. 設計反映等の形で成果を挙げており, 今後も独立検証活動を継続していく予定である.

6. 謝辞

4 項で述べた IV&V について, 過去の知見から有益なアドバイスを数多く頂いている JAXA 研究開発部門第三研究ユニットの石濱直樹氏，大久保梨思子氏，IV&V 請負組織として活動頂いている HIREC 株式会社殿に対しまして, MMX プロジェクト一同謝意を表します.

参考文献

1) 川勝他 : 火星衛星探査計画 MMX の概要と開発状況，2D01，第 66 回宇科連，2022.
2) 吉川他 : 火星衛星探査計画 MMX の総合システム詳細設計とミッションロバスト化検討，2D03，第 66 回宇科連，2022.
3) 安光他:火星衛星探査計画 MMX の運用詳細設計，2D05，第 66 回宇科連，2022.
4) 大野他 : 火星衛星探査計画 MMX 航法誘導制御系の基本設計，2B06，第 65 回宇科連，2021.