C3-1-1 商用ロケット開発における 形式検証の必要性と基盤研究への期待

インターステラテクノロジズ（株）
シニアフェロー　森岡 澄夫
https://www.istellartech.com/

本発表のテーマ

- 民間宇宙開発が活発化.
- 商用ではテストの費用・時間に強い制約.
- しかし安全確保は妥協できない.
- レアケース・バグでも致命的問題に成り得る.

- **形式検証に改めて着目.**

発表の構成

- **民間宇宙開発（NewSpace）の進展と，商用ロケットの登場**
- ロケット制御システム（アビオニクス）の難しさ
- 形式検証の適用が望ましい設計対象と，要調査事項

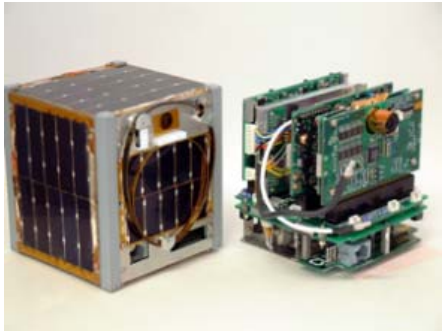
NewSpace：民間主導の宇宙開発

■ 宇宙船，ロケット，人工衛星などを民間開発．最近10年で急速に進展．

写真出典1：https://www.newsweekjapan.jp/stories/world/2018/04/post-9957.php
写真出典2：https://universemagazine.com/en/spacex-stops-production-of-crew-dragon-spacecraft/
写真出典3：https://ja.wikipedia.org/wiki/%E3%83%95%E3%82%A1%E3%83%AB%E3%82%B3%E3%83%B3%E3%83%98%E3%83%93%E3%83%BC#/media/File:Falcon_Heavy_Side_Boosters_landing_on_LZ1_and_LZ2_-_2018_(25254688767).jpg

衛星の小型化と低価格化

- 2000年代のキューブサット登場で始まる.
  - サイズ： 10cm～, 1kg～
  - 日本は技術的先駆者（東大等）.
  - 衛星は電子装置そのもの.



東京大学中須賀研究室 XI-IV
https://www.space.t.u-tokyo.ac.jp/nlab/project.html

※すべてが小型衛星になるわけではなく,
大型衛星向きのアプリケーションもある.
例： 放送（BS/CS）・測位（GPS）

通信
全地球インターネット
衛星電話回線
政府（安全保障）
民間（SpaceX, Amazon, OneWeb）

リモートセンシング
カメラやレーダーで地球を観測
政府（安全保障・科学）
民間（Axelspace, planet, Black sky, Orbital Insight）

安全保障
早期警戒・宇宙天気予想・
地球近傍物体監視
政府（内閣官房, 防衛省）

情報収集
狭帯域通信・データ収集
民間（Spire, SwarmTechnologies）

テクノロジ
新技術の実証実験
民間・政府宇宙機関 (JAXA)・大学

科学
宇宙物理学・天文学
政府機関・研究所 (JAXA)・大学

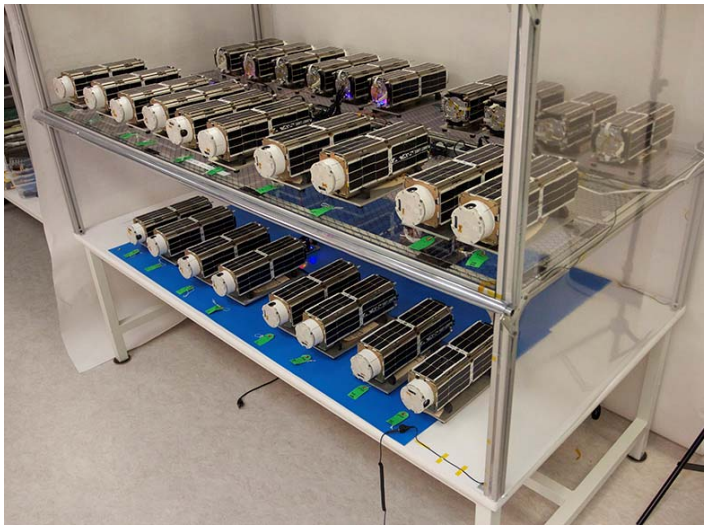
軌道上サービス
軌道上製造・ラストマイル
政府宇宙機関・民間 （Northrop Grumman, Momentus, Astroscale）

衛星の多数化

- 目的：　通信網，地球観測，測位.
- コンステレーション：　低軌道（LEO）に100～10000機オーダで投入.

SpaceX スターリンク通信網

Figure： http://www.telegiz.com/articles/22701/20170505
/spacex-constellation-4-425-satellites-will-make-musk-internet.htm



Planet Labs Inc. Dove観測網

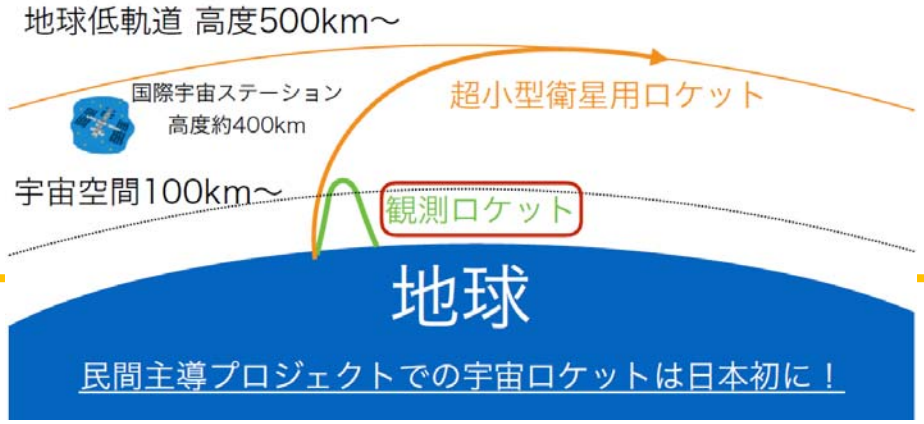
Figure: https://www.planet.com/company/approach/

175機以上

弊社で開発中の低価格ロケット

観測ロケット MOMO
(2019年5月に宇宙到達，7回打ち上げ)

衛星打上げロケット ZERO
(開発中)



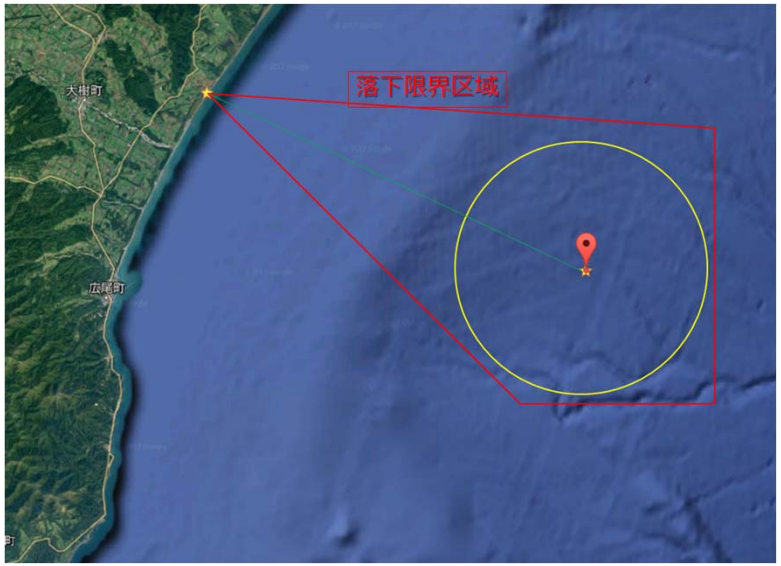
発表の構成

- 民間宇宙開発（NewSpace）の進展と，商用ロケットの登場
- **ロケット制御システム（アビオニクス）の難しさ**
- 形式検証の適用が望ましい設計対象と，要調査事項

安全は低コスト化よりも優先

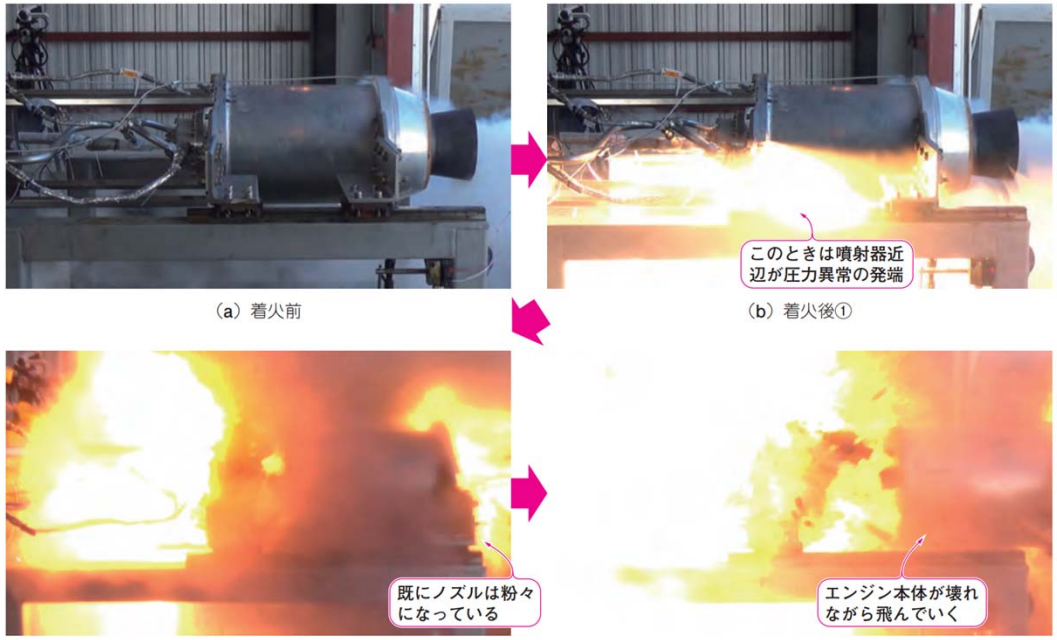
- 優先度1：　**安全確保**

- 優先度2：　主ミッションの達成
- 優先度3：　付随ミッションや広報の達成



重要機能1： エンジン起動・停止制御

- 動作：　10ミリ秒精度でバルブや点火器を操作.
- 要注意：　コマンド**発行順とタイミング**にきわめて敏感.
- 要注意：　温度・圧力・ポンプ回転数などを**見落としなくリアルタイム**監視.

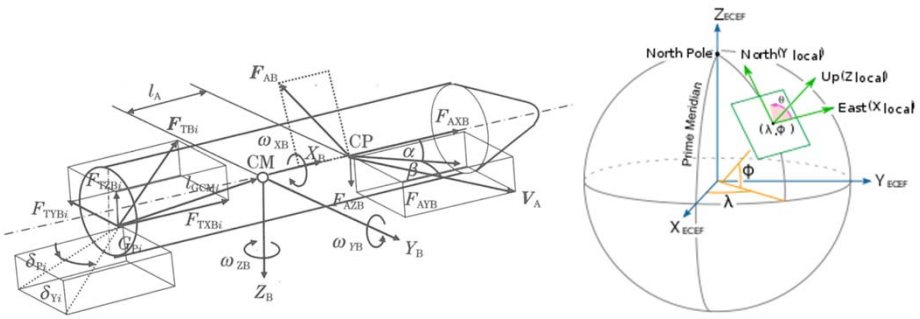


(a) 着火前　(b) 着火後①　(c) 着火後②　(d) 着火後③

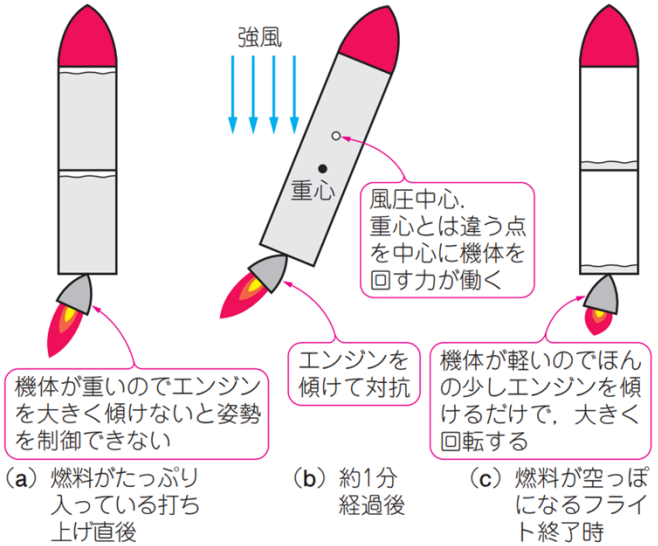
出典 CQ出版社 トランジスタ技術スペシャルNo.155「宇宙ロケット開発入門」,
https://cc.cqpub.co.jp/lib/system/doclib_item/1363/

重要機能2： 誘導制御

- 動作： 姿勢や現軌道を計測し，これからの軌道を選定し，エンジン方向を調整.
- 要注意： 複雑な座標変換，**特殊な数値体系**の利用．（クォータニオン）
- 要注意： ジャイロ出力の微積分や，制御ループ実行の**時間精度，演算精度**.
- 要注意： 様々に変化するロケット内外状況を**網羅した制御設計**.



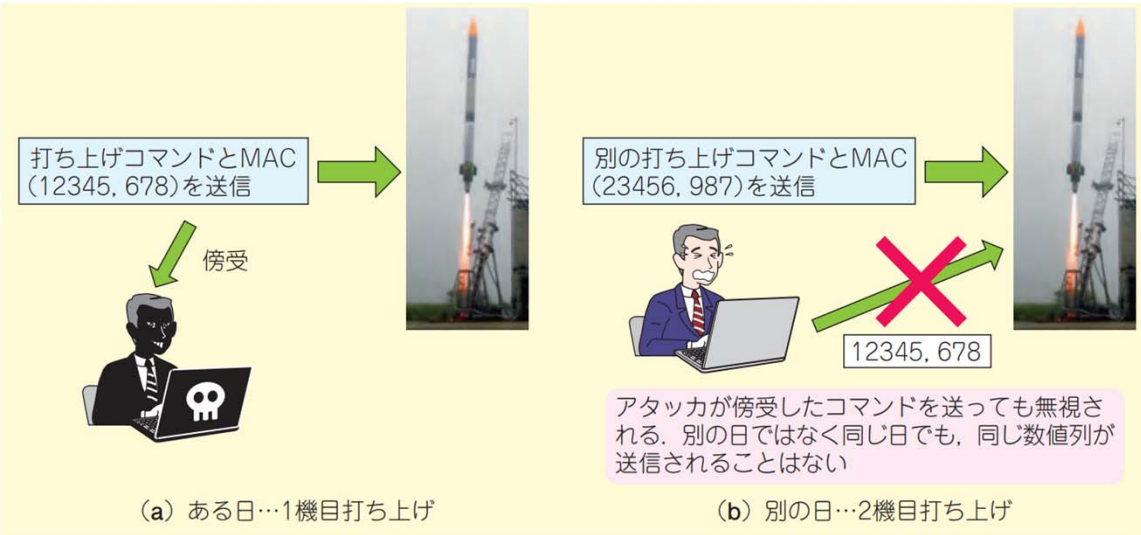
	座標名	原　点	備　考
慣性座標	地球中心慣性座標系（ECI座標）	地球の中心	x：$t=0$において赤道と経度0°の交線方向 y：$t=0$において赤道と東経90°の交線方向 z：地球自転軸方向
運動座標	地球中心回転座標系（ECEF座標）	地球の中心	x：赤道と経度0°の交線方向 y：赤道と東経90°の交線方向 z：地球自転軸方向
	局所水平座標系（NED座標）	機体質量の中心	x：局所水平面において北方向 y：局所水平面において東方向 z：局所水平面において地球中心方向（下方向）
	機体座標系（Body座標） OpenTsiolkovskyでの定義	機体質量の中心	x：機軸方向，機体ノーズ方向＋（ロール軸） y：ピッチ軸 z：ヨー軸
その他	緯度経度高度 LLH	–	緯度 経度 高度



出典 CQ出版社 トランジスタ技術スペシャルNo.155「宇宙ロケット開発入門」，
https://cc.cqpub.co.jp/lib/system/doclib_item/1363/

重要機能3： 地上～機体間通信

- 機能： GO/NO-GOのアップリンク，機体位置／姿勢情報のダウンリンク．
- 要注意： **セキュアな通信プロトコル．**（秘匿，認証，可用性などの達成）



出典 CQ出版社 トランジスタ技術スペシャルNo.155「宇宙ロケット開発入門」，
https://cc.cqpub.co.jp/lib/system/doclib_item/1363/

NICT 国立研究開発法人 情報通信研究機構

NICTについて　研究紹介　研究成果　オープンイノベーション・IDI　採用

トップ ＞ 広報 ＞ プレスリリース ＞ 2021年 ＞ 観測ロケットMOMOv1で情報理論的に安全な実用無線通信に成功

観測ロケットMOMOv1で情報理論的に安全な実用無線通信に成功

2021年8月17日

国立研究開発法人情報通信研究機構
インターステラテクノロジズ株式会社
法政大学

ポイント

- 観測ロケットMOMOv1から地上局に飛行状況を伝送する実用チャネルでセキュア通信の実証実験
- 開発した情報理論的に安全な通信セキュリティ技術の動作確認に実用速度（512 kbps）で成功
- 小型宇宙機の飛行の安全確保に不可欠な伝送データの保護に寄与

国立研究開発法人情報通信研究機構（NICT、理事長: 徳田 英幸）サイバーセキュリティ研究所、インターステラテクノロジズ株式会社（IST、代表取締役: 稲川 貴大）及び法政大学（総長: 廣瀬 克哉）は、共同で開発した小型衛星・小型ロケット用通信セキュリティ技術を観測ロケットMOMOv1に搭載し、2021年7月31日（土）、機体から地上局に飛行状況を伝送する実用チャネルにおいてセキュア通信の実証実験に成功しました。

本研究の目標は、小型宇宙機の乗っ取り防止による飛行の安全確保と、小型宇宙機から伝送される飛行状況や学術的・商業的価値の高いデータの保護のため、第三者によるなりすまし・改ざん・盗聴を防ぐことです。本実験によって、通信の秘匿・認証を最も高いセキュリティである情報理論的安全性で実現できることを実用速度（512 kbps）で確認しました。本成果は、小型宇宙機の飛行の安全確保等に不可欠な伝送データの保護に寄与します。

https://www.nict.go.jp/press/2021/08/17-1.html

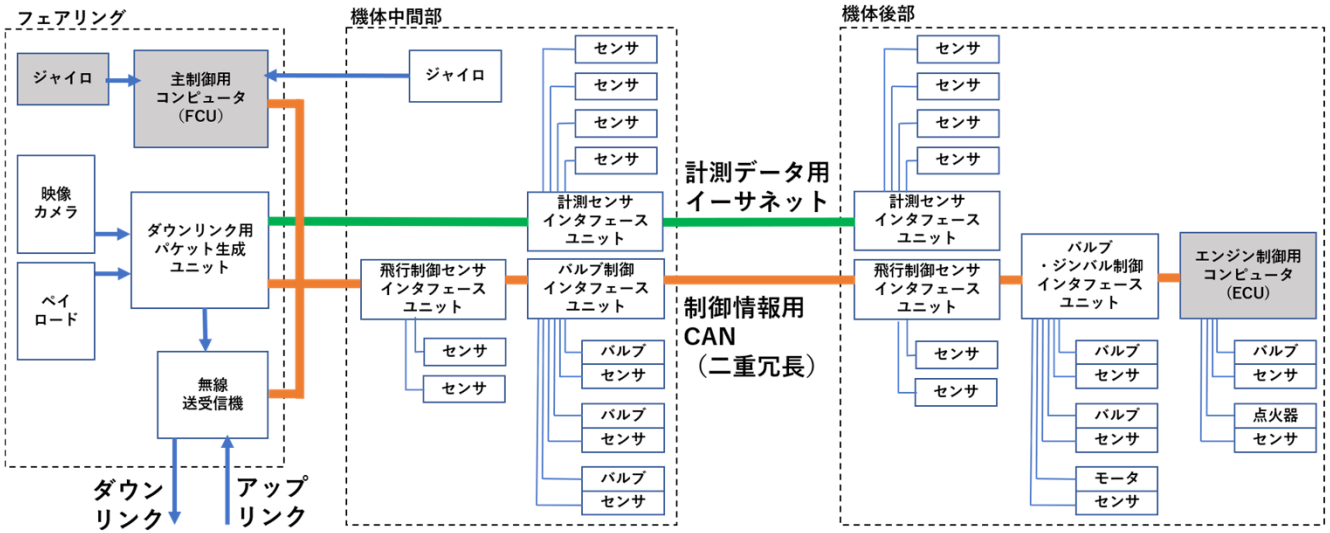
回避しなければならない重大トラブルの例

- 人命や第三者財産への被害.
- 地上局での機体見失い.
- 打上げや飛行の中断不能.

自社設備への被害は，相対的には許容範囲

アビオニクスのハード基本構成

- 数百点のセンサを入力，数十個のアクチュエータを出力とする制御系.
- 数十個のマイクロプロセッサによる，リアルタイム分散制御系.



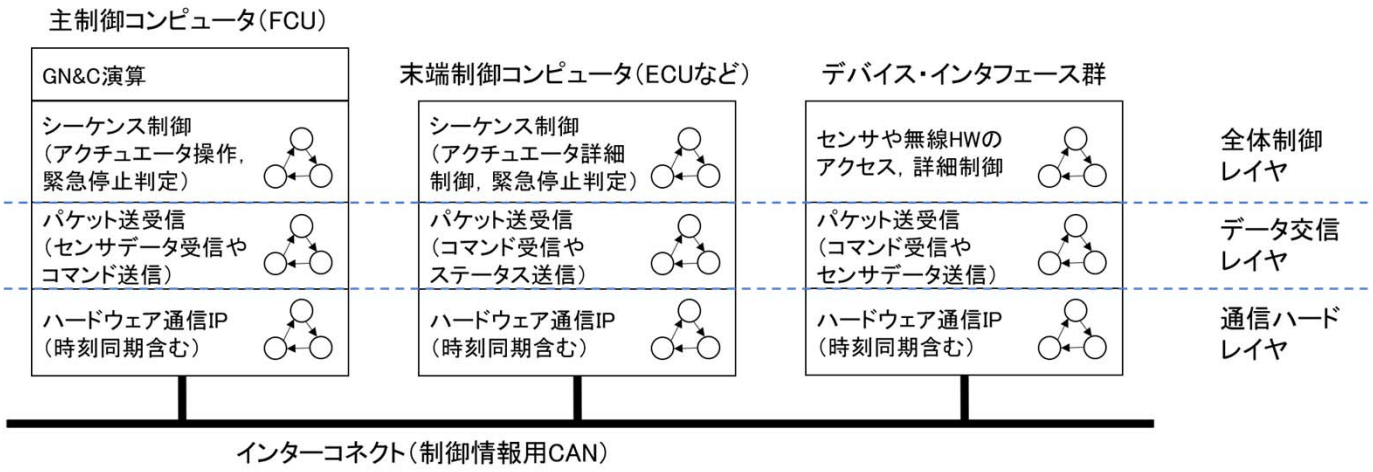
出典 https://app.journal.ieice.org/trial/105_4/k105_4_275/index.html

アビオニクスのソフト基本構造

■全体制御と末端デバイス制御が，機体内に分散配置.

- ■ 即応性確保： モータやセンサなど細かい制御は，末端で行う.
- ■ 安全性向上： 全体制御やインターコネクトが故障しても，末端で安全処置.

■各ノードはFSMの階層構造.



出典 森岡，酒井，"観測ロケットMOMOを事例としたアビオニクス処理への形式検証適用の基礎検討,"
日本航空宇宙学会 第66回宇宙科学技術連合講演会, 1N06, 2022.

アビオニクス由来の事故例(1)

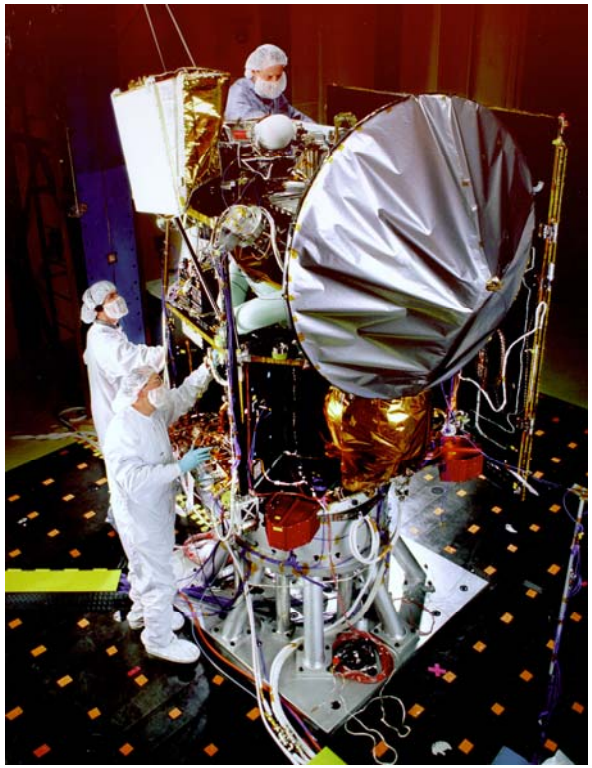
■ **細かい実装ミス１つ**がミッション喪失に直結．回復余裕も少ない．

1996.06.04 アリアンV
変数オーバフローで例外発生し，
ハングアップで制御喪失，空中分解

2013.07.02 プロトンM
姿勢検知センサの取り付け方向を
間違え，地上へ向かって飛ぶ

出典 https://www.esa.int/ESA_Multimedia/Images/2009/09/Explosion_of_first_Ariane_5_flight_June_4_1996
https://www.rt.com/news/proton-m-rocket-takeoff-crash-514/

アビオニクス由来の事故例(2)



1999.09.23 Mars Climate Orbiter
メートル法とヤード・ポンド法の
取り違えで火星着陸失敗

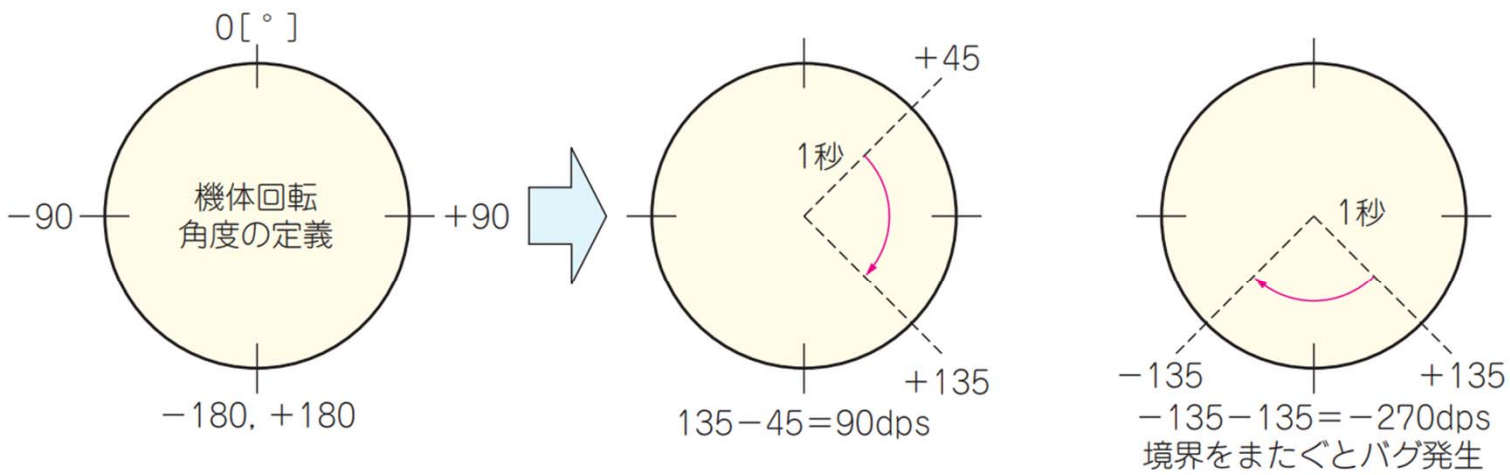
出典　https://en.wikipedia.org/wiki/Mars_Climate_Orbiter#/media/File:Mars_Climate_Orbiter_during_tests.jpg

- 起こしやすいミス.
  - ＋－符号取り違え.
  - 座標系・単位系の取り違え.
  - センサ誤動作など異常ケースに対する対処漏れ.
  - センサ取り付けや配線の間違い.

開発試験中に起きたバグの例(1)

■ 姿勢制御演算において.

- ■ 角度の微分計算を間違い，PID制御が異常になった.
- ■ 大半の入力値内で正しく計算し，実機でも起きにくい.



(a) 角度は−180〜+180° で定義されている

(b) 角度変化の差分から角速度が計算できる

(c) 角速度の計算を誤るコーナ・ケース

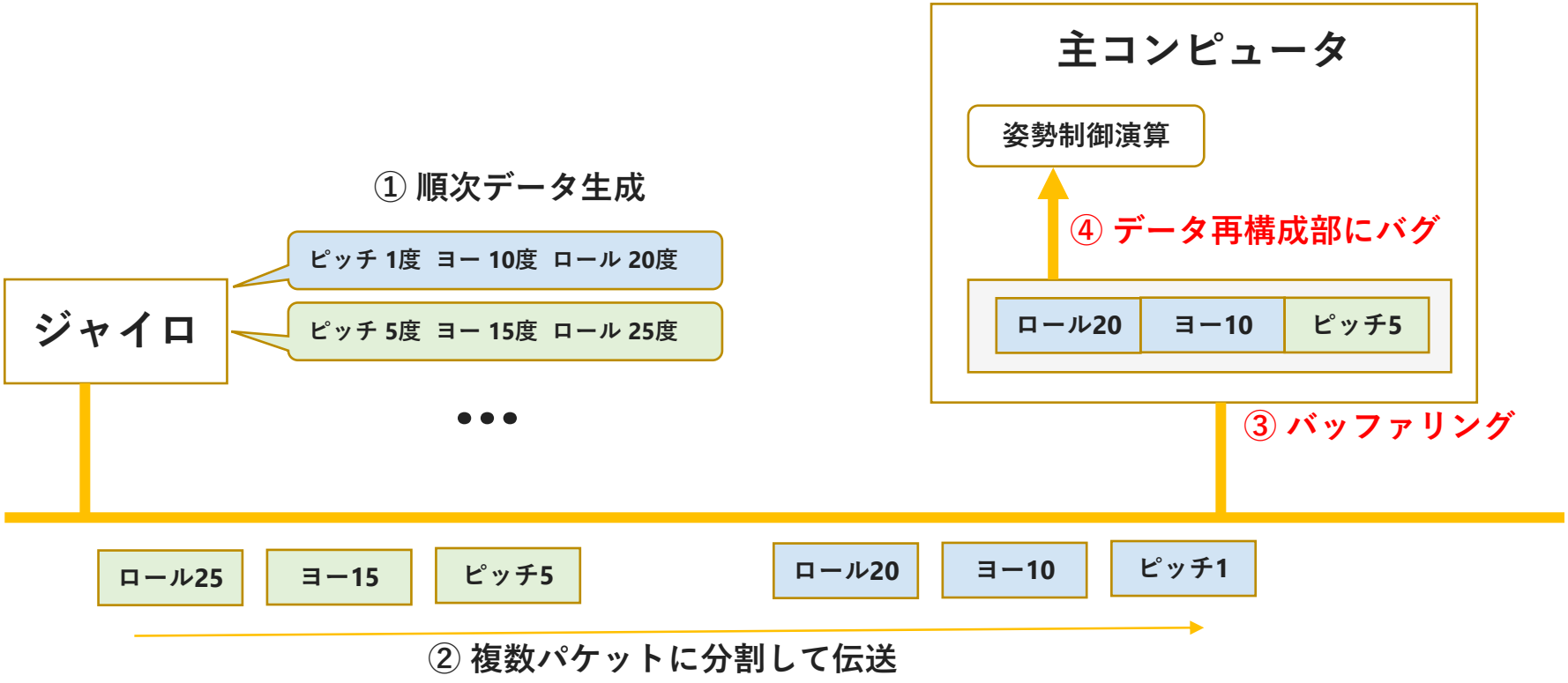
出典 CQ出版社 トランジスタ技術スペシャルNo.155「宇宙ロケット開発入門」,
https://cc.cqpub.co.jp/lib/system/doclib_item/1363/

開発試験中に起きたバグの例(2)

- 同じく姿勢制御演算において.
  - div **0**, asin(1.0…0**1**), atan(**0**,x) など禁止演算が発生.
    - 仕様中の数式では起きなくても，計算機上では発生.
    - 特異点近傍（姿勢が "垂直" など）で起きやすい.
  - 機体実機とシミュレーションの結果食い違い.
    - 機体とシミュレータで浮動小数点精度が異なり，誤差が蓄積.
  - センサ値の固定小数点表現のビット数が不足，演算結果が不正に.
  - 変数のsign/unsignedを取り違え，INT_MAX近辺で演算結果が不正に.

開発試験中に起きたバグの例(3)

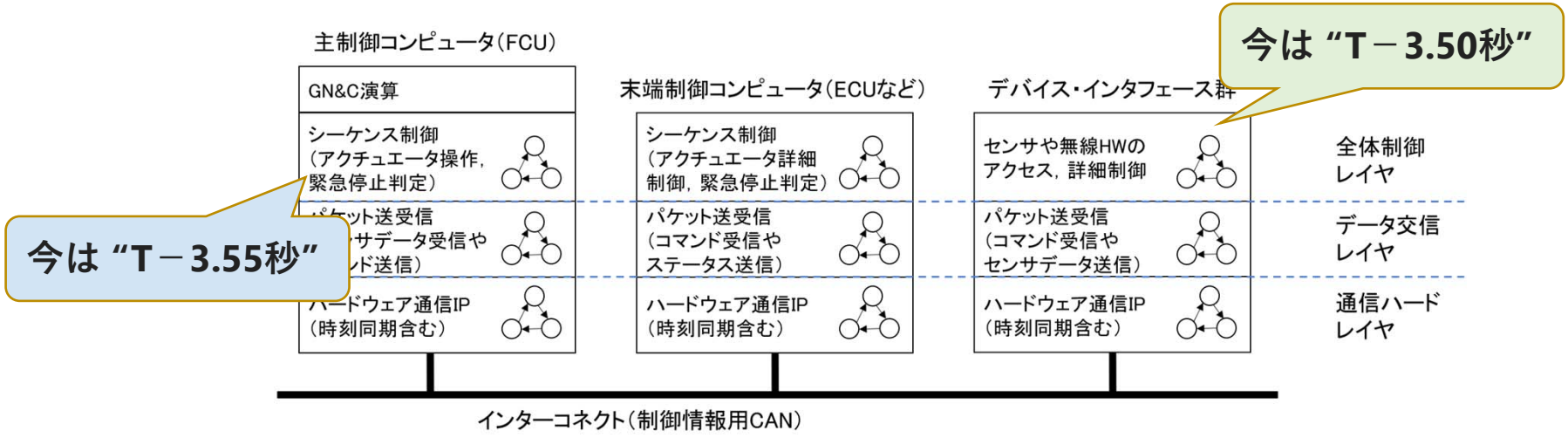
■ インターコネクト処理のバグにより，姿勢データが不正に.



開発試験中に起きたバグの例(4)

■ 旧設計において.

- ■ 各FSMで「時刻」が食い違い，シーケンス実行の食い違いが発生.
- ■ 同期頻度の不足と，各FSMのオシレータ誤差蓄積が根本原因.

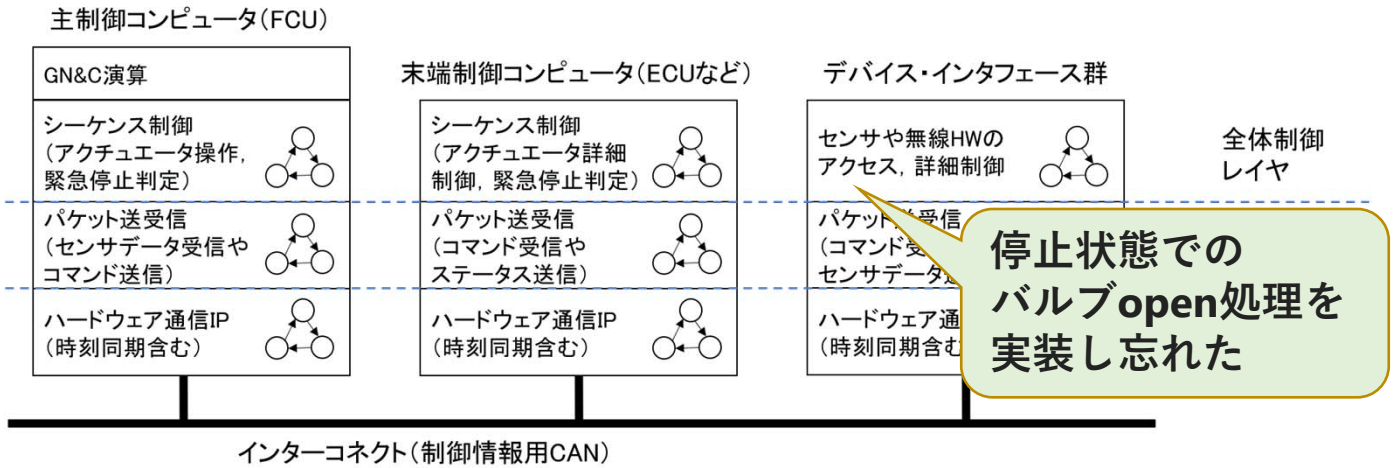


出典　森岡，酒井，"観測ロケットMOMOを事例としたアビオニクス処理への形式検証適用の基礎検討,"
日本航空宇宙学会 第66回宇宙科学技術連合講演会, 1N06, 2022.

開発試験中に起きたバグの例(5)

■ 旧設計において.

■ 地上での緊急停止模擬試験で，液体酸素タンクの開放バルブが制御不能に.
■ バルブ制御FSMのバグと，テストケース漏れが根本原因.



出典　森岡，酒井，"観測ロケットMOMOを事例としたアビオニクス処理への形式検証適用の基礎検討,"
日本航空宇宙学会 第66回宇宙科学技術連合講演会, 1N06, 2022.

厄介なトラブルの基本性質

- **信頼度成長曲線の収束期**であり，発生頻度が低く，再現や原因特定が難しい.
- 発生も原因も**予想できていない**ため，テスト計画に組み込まれていない.
- **機械動作や物理事象と関係**するため，テストの立案／環境構築／実施が困難.
- しかし重要度は高く，甚大な被害につながり得る.

- **（万能でないことは認識しつつ）形式検証への期待**

発表の構成

- 民間宇宙開発（NewSpace）の進展と，商用ロケットの登場
- ロケット制御システム（アビオニクス）の難しさ
- **形式検証の適用が望ましい設計対象と，要調査事項**

検証観点からの機能分類

- リアルタイム分散制御と数値演算に大別される.
- 形式検証の現状と利用可能性をサーベイ中.

基本機能	検証の観点から見た分類
シーケンス制御	リアルタイム分散制御
誘導制御	数値演算
安全管理（飛行継続判定・中断）	リアルタイム分散制御
通信	数値演算 セキュリティ
センシング	数値演算
アクチュエータ制御	リアルタイム分散制御

形式検証が望ましい項目 1

- **機体制御の 実装ミスやタイミング異常の発見，同期ずれへの耐性評価**
  - とくに，**異常（故障）発生時に，予想外の危険状態に到達しない**こと．
    - たとえば「どのようなタイミングでセンサが異常検知しても，安全状態になる」．
    - 「いつインターコネクトが切れても，停止不能とならない」．
  - **異常系については，実機ではテスト環境を作りにくい or テスト実施が危険.**

対象装置	対象機能	詳細検証項目	形式検証 手法の候補	適用すべき 設計開発段階
全体	アクチュエータの 操作指令	・指令順の正しさ ・指令送信の最大遅延 ・指令伝搬の最大遅延	並列時間オートマトン群 の記号実行と，遅延積算	基本設計仕様
		・危険（禁止）状態への不達 ・異常（禁止）コマンドの拒否	並列時間オートマトン群 上のモデルチェッキング	
主制御 コンピュータ (FCU)	センサを使った 緊急停止判断	・判定漏れの非存在 ・不要（過剰）判定の非存在 ・データ異常への全対応	制御レイヤ・オートマトン 上のモデルチェッキング	詳細設計仕様 または実装後

現時点での調査や課題

- 全FSMないし対応レイヤ間の積マシンを構成し，時間オートマトン上でのモデルチェッキングを実施することになると予想.

- 処理系は Uppaal （CTL）が第一候補.

  - NuSMV, SPINも候補ではあるが，時間的挙動を可読性よく書けるか懸念.
  - 専用モデルチェッカの構築もあり得る.

- 課題（現在，対応検討中） … 一般的モデルチェッキングと同様.

  - プロパティ／FSM／メッセージング等の**記述容易性，可読性**.
  - 実用時間内で検証可能な設計規模. … **状態爆発**を回避できるか？
  - **故障シナリオの組み込みやすさ**.

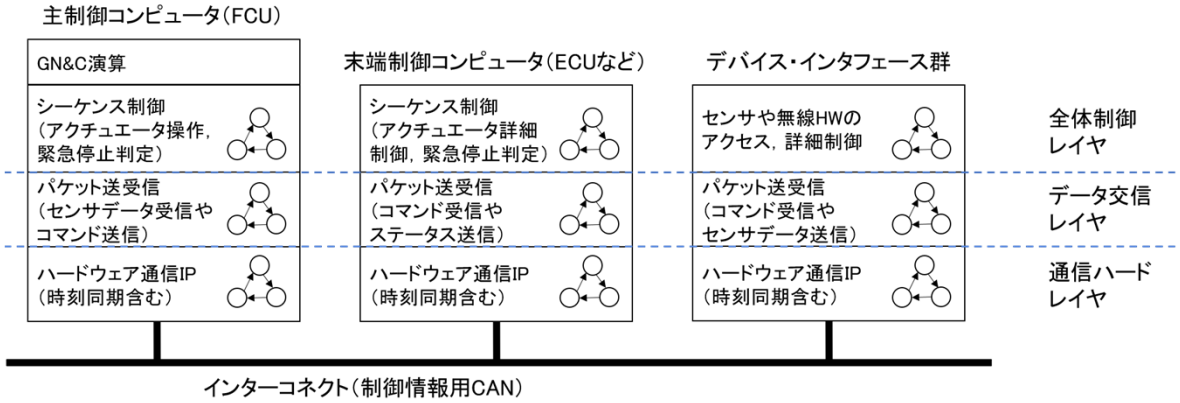
補足： 限定的な検証でも価値は高い

- 形式検証の能力限界から，以下の可能性がある．
  - 実装コードを直接検証できず，縮小記述や異言語での検証になる．
  - 一部プロパティの検証にとどまる．
  - 厳密には現実と合致しない仮定．　例：「同期ずれが一切起こらない」
- しかし，一部事項だけでも**100%**検証できれば，高い価値がある．
  - トラブル原因調査時に，その範囲を明確に排除でき，分析が容易になる．
  - クリティカル動作だけでも検証できていれば，安全性は高まる．

補足： 設計を検証に合わせることも可能

■ 2021年： 不確実動作を減らし，動作解析容易な設計に改良した.

- ■ 各ノードが**頻繁に時刻同期**を取り，基本的に**等速動作**.
- ■ 遷移が**離散時間**間隔.
- ■ ノード間の全メッセージ交換が，**静的にスケジュール**されている.



■ 動的検証，形式検証のいずれに対しても，検証空間を狭めるうえで有効.

出典　森岡，酒井，"観測ロケットMOMOを事例としたアビオニクス処理への形式検証適用の基礎検討，"
日本航空宇宙学会 第66回宇宙科学技術連合講演会, 1N06, 2022.

形式検証が望ましい項目 2

■ 誘導制御演算の機能正当性／演算精度／実行時間保証

- ■ 現在はモンテカルロ・シミュレーションが主なテスト手法.

- ■ **一部故障や不測異常からの自動回復**シナリオを，網羅的に検証したい.
- ■ 将来，飛行経路の**動的探索** （カーナビと同様）を導入したら，網羅的検証が必要.

- ■ 演算精度： **任意の**センサ入力時系列に対し精度が保たれるか，確証を取りたい.
- ■ 実行時間： 同上.

現時点での調査や課題

- 手法選定以前に 検証条件や仕様記述方法が決定できておらず，課題.

  - たとえば「エンジン不調や，それによる軌道逸脱からのリカバリ動作」
    - 自然言語での曖昧な要求を，形式論理で扱える段階に明確化できていない.
    - どの形式論理を用いるべきか，分析しきれていない.

- アルゴリズム機能検証についての研究はある程度見受けられるが，演算精度や時間精度の検証手法の報告は**意外に少ない**.

  - 汎用検証手法を構築しにくく，個別対応になりやすいのが理由？
  - 制御系の一般的な要件であり，ニーズがニッチという訳ではない.

形式検証が望ましい項目 3

■ 通信や数値演算で利用する下位プリミティブ・ライブラリ

- ■ 誘導制御演算： クォータニオン演算や座標変換，三角関数，浮動小数点演算.
- ■ 通信処理： RS符号やLDPC符号などのECC，AESなどの暗号.

- ■ それぞれ，アルゴリズム正当性検証や，実装における精度検証などが必要.

■ これらは一般にも多用され重要だが，形式検証の報告は意外に少ない.

- ■ 整数や有理数上の一階述語論理のサブクラスについては，決定手続きがある.
- ■ 有限体上の一階述語論理についても，決定手続きの報告がある.

- ■ クォータニオン演算の決定手続きや，三角関数実装の検証例などは見当たらない.
- ■ 古くは Pentium の SRT除算バグで，Intelが形式検証利用を検討した事例はある.

補足： 演算の機能検証の難しさ

■ 一般に数値演算については，ブラックボックスとして総当たりする動的検証は不可能.

■ 形式検証，あるいはホワイトボックスとしてのテストを行うとしても，以下が問題となる.

- 演算処理に何かしらの**規則や構造**がないと，テストケースの絞り込みやコーナケースの導出ができない.
- 「正しい演算」の**仕様定義**を，誤りなくコンパクトに行えない場合がある.
（「**仕様記述の複雑さ・規模が実装と変わらず，仕様を間違える**」問題）
- 例： GF(2^128) の乗算回路や除算回路を検証する方法は？

形式検証が望ましい項目4

■ コンパイルなど抽象度変換の等価性検証.

- **ソースコードを検証しても，最終的に実機で動作させるバイナリが等価でない**と困った状況になる.
- ディジタル回路の論理合成については，ASIC(LSI)で古くから実用化されている等価性形式検証の導入を検討中.
- ソフトウェアのコンパイラについては，等価性検証のツールは存在せず， 現状でギブアップ.
- それでもファジングの研究には期待している.

まとめ

- 動的検証では実施コストやカバレッジに限界.
- レアケース・バグが重大事故につながり得る.
- 形式検証を，部分的であってでも併用したい.
- 調査した範囲内では，**意外に研究報告が少ない**.

- **形式検証の基盤研究の活性化を期待しています**.

参考文献（従来研究など）

- 森岡澄夫，稲川貴大，"民間宇宙ロケット用アビオニクス機器に対する諸要求と実現,"電子情報通信学会誌 小特集 極限環境の計測を支える回路とシステム技術，Vol.105, No.4, pp.275-280, 2022.
- 内閣府宇宙開発戦略推進事務局: 人工衛星等の打上げ用ロケットの型式認定に関するガイドライン改訂第2版，令和元年9月14日，http://www8.cao.go.jp/space/application/space_activity/documents/guideline2.pdf
- B.Dutertre and V.Stavridou, "Formal requirements analysis of an avionics control system," IEEE Trans. on Software Engineering, Vol. 23, Issue 5, pp.267-278, May 1997. DOI: 10.1109/32.588520
- J.V.Deshmukh, K.Havelund and I.Perez (eds.), "NASA Formal Methods," Proc. of the 14th Intl. Symposium, NFM 2022, May 2022.
- インターステラテクノロジズ株式会社，"トランジスタ技術SPECIAL No.155 宇宙ロケット開発入門," CQ出版, ISBN 9784789846950, 2021.
- NASA JPL "Mars Climate Orbiter Mishap Investigation Board Phase I Report," Nov. 10, 1999. https://llis.nasa.gov/llis_lib/pdf/1009464main1_0641-mr.pdf
- J.L.Lions, "ARIAN5 Flight 501 Failure," http://sunnyday.mit.edu/nasa-class/Ariane5-report.html
- Nuseibeh, Bashar, "Ariane 5: Who Dunnit?," IEEE Software. No.14, Vol.3, pp.15-16, May 1997. doi:10.1109/MS.1997.589224. S2CID 206482665
- 吉岡信和，田辺良則，田原康之，長谷川哲夫，磯部祥尚，"モデル検査による設計検証," コンピュータソフトウェア，Vol.31, No.4, pp.40-65, 2014.
- Y.Wang, "Research on the Execution Time Analysis Technology of the Worst Case System in Real Time System," Proc. of 2017 9th Intl. Conf. on Measuring Technology and Mechatronics Automation (ICMTMA), 2017. doi:10.1109/ICMTMA.2017.0102
- S.Yuan, Y.Li,, Y.Chen and C.Wang, "Time Synchronization Accuracy Verification for Multi-Sensor System," Proc. of 2021 Intl. Conf. on Artificial Intelligence, Big Data and Algorithms (CAIBDA), May 2021. doi:10.1109/CAIBDA53561.2021.00012
- B.F.Adiego et al., "Modelling and Formal Verification of Timing Aspects in Large PLC Programs," Proc. of the 19th World Congress The Intl. Federation of Automatic Control, pp.3333-3339, 2014. doi:10.3182/20140824-6-ZA-1003.01279
- NuSMV (SMV): a new symbolic model checker https://nusmv.fbk.eu/
- Spin: https://spinroot.com/spin/whatispin.html
- UPPAAL: https://uppaal.org/
- S.Y.Park and N.I.Cho, "Fixed point error analysis of CORDIC processor based on the variance propagation," 2003 IEEE Intl. Conf. on Acoustics, Speech, and Signal Processing (ICASSP'03), 2003. doi:10.1109/ICASSP.2003.1202429
- V.D.Thai, T.T.Quan, T.V.Le and B.T.Ngo, "An Approximation-Based Abstract Interpretation Framework for Formal Verification of Floating-Point Programs," 2012 IEEE RIVF Intl. Conf. on Computing & Communication Technologies, Research, Innovation, and Vision for the Future, 2012. doi:10.1109/rivf.2012.6169864
- S.Boldo and J.C.Filliatre, "Formal Verification of Floating-Point Programs," 18th IEEE Symposium on Computer Arithmetic (ARITH '07), 2007. doi:10.1109/ARITH.2007.20
- M.Tang, X.Zeng, K.Song and J.Liu, "Error Analysis on Floating-Point Arithmetic in C Programming Language Library Functions," 2013 Fourth Intl. Conf. on Emerging Intelligent Data and Web Technologies, 2013. doi:10.1109/EIDWT.2013.134
- A.Jorgensen, A.Masters and R.Guha, "Assurance of Accuracy in Floating-Point Calculations - A Software Model Study," 2019 Intl. Conf. on Computational Science and Computational Intelligence (CSCI), 2019. doi:10.1109/CSCI49370.2019.00091
- Rei Ueno, Naofumi Homma, Takafumi Aoki and Sumio Morioka, "Hierarchical Formal Verification Combining Algebraic Transformation with PPRM Expansion and Its Application to Masked Cryptographic Processors," IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E100-A, No.7, pp.1396-1408, 2017. doi:10.1587/transfun.E100.A.1396
- Sumio Morioka, Yasunao Katayama and Toshiyuki Yamane, "Towards Efficient Verification of Arithmetic Algorithms over Galois Fields GF(2^m)," Proc. of the 13th Intl. Conf. on Computer Aided Verification (CAV'01), LNCS Vol.2102, pp.465-477, July 2001. doi:10.1007/3-540-44585-4_45
- Rei Ueno, Kotaro Okamoto, Naofumi Homma and Takafumi Aoki, "An Efficient Approach to Verifying Galois-Field Arithmetic Circuits of Higher Degrees and Its Application to ECC Decoders," 2014 IEEE 44th International Symposium on Multiple-Valued Logic, DOI: 10.1109/ISMVL.2014.33
- Cooper, D. C., "Theorem Proving in Arithmetic without Multiplication," in B. Meltzer and D. Michie, eds., Machine Intelligence Vol.7. Edinburgh University Press pp.91-99, 1972.
- Oppen, Derek C., "A 2^2^2^pn Upper Bound on the Complexity of Presburger Arithmetic," J. Comput. Syst. Sci. 16 (3): 323-332. doi:10.1016/0022-0000(78)90021-1, 1978.
- Y. Umezawa and T. Shimizu, A formal verification methodology for checking data integrity," Design, Automation and Test in Europe DOI: 10.1109/DATE.2005.15
- 森岡澄夫，酒井一美，"観測ロケットMOMOを事例としたアビオニクス処理への形式検証適用の基礎検討," 日本航空宇宙学会 第66回宇宙科学技術連合講演会, 1N06, 2022.