

宇宙用ソフトウェア開発検証技術

衛星打上げ用ロケット搭載ソフトウェア の開発事例紹介

1	ロケット搭載ソフトウェアの概要・・・	3
2	搭載ソフトウェアの開発方法……………	6
3	管理標準……………	3 7

1 ロケット搭載ソフトウェアの概要

図1-1 アビオニクス系の機器構成

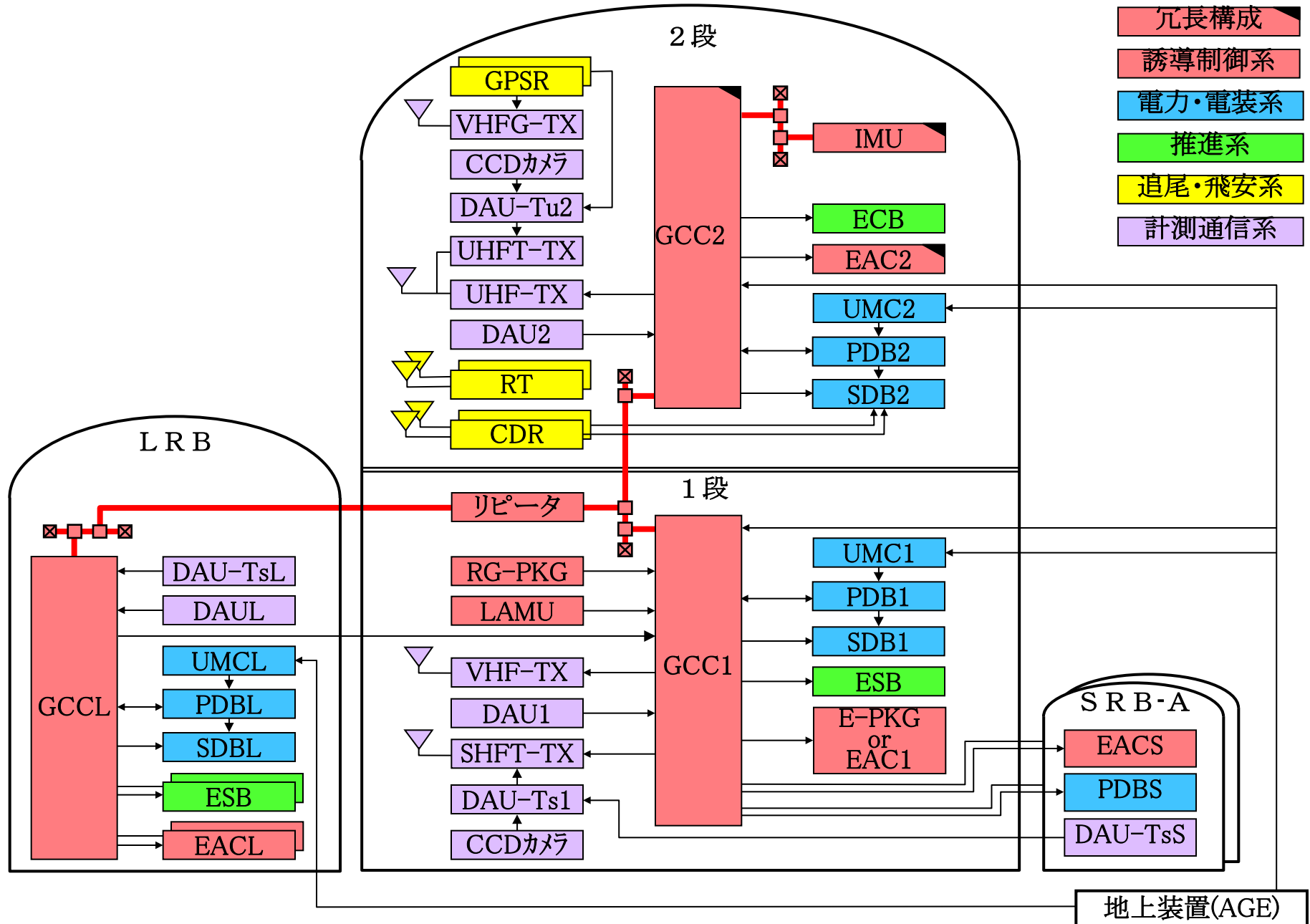


表1-2 搭載ソフトウェアの種類

No	名 称	主 要 機 能
1	搭載ソフトウェア (制御管理モジュール)	2段用 OBS全体の実行制御、姿勢制御、飛行シーケンス制御、2段推進系タンク加圧制御
		1段用 1段姿勢制御、1段飛行シーケンス制御、1段推進系タンク加圧制御
		LRB用 LRBジンバル制御、LRBタンク加圧制御
2	搭載ソフトウェア(航法誘導モジュール)	航法、誘導
3	搭載ソフトウェア(システムモジュール)	リアルタイム OS、入出力ドライバ
4	IMUソフトウェア	センサ・データ処理(ドリフト補償)、初期アライメント
5	2段電動アクチュエータ・ソフトウェア	電動アクチュエータの制御、冗長管理
6	SRB-A電動アクチュエータ・ソフトウェア	電動アクチュエータの制御
7	LRB電動アクチュエータ・ソフトウェア	電動アクチュエータの制御
8	エンジン・コントロール・ボックス・ソフトウェア	2段エンジン点火停止シーケンスの制御
9	エンジン・シーケンス・ボックス・ソフトウェア	1段エンジン点火停止シーケンスの制御
10	アンビリアル・コントローラ・ソフトウェア	地上装置との通信の中継
11	GPS受信機ソフトウェア	飛行状況モニタ用GPS航法

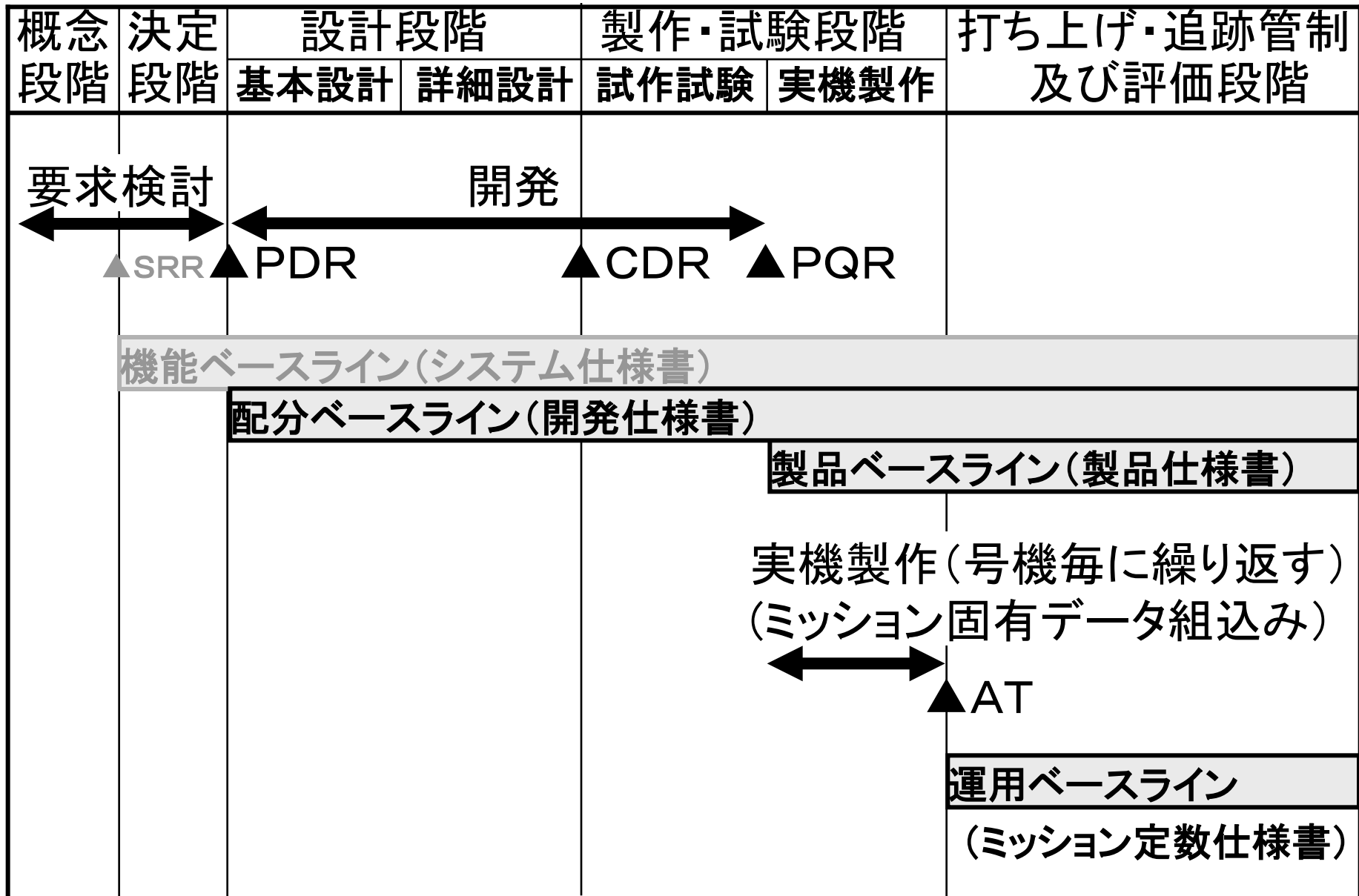
2 搭載ソフトウェアの開発方法

2. 1	開発工程	7
2. 2	文書体系	8
2. 3	主要ソフトウェア・ツール	1 0
2. 4	作業内容	1 5
2. 5	試験の形態	2 3

(注1) ここでいう搭載ソフトウェアは、表1-2に示したNo. 1～No. 3であり、No. 4以降の組込ソフトウェアは除く。

(注2) 検証方法については、ロケットによっては一部異なる方法が採用されており、必ずしもこの限りではない。

2.1 ロケット搭載ソフトウェアの開発工程



2.2 ロケット搭載ソフトウェアの文書体系(1/2)

★開発仕様書

- 要求仕様
- 機能仕様

★インタフェース仕様書

★製品仕様書

- 設計文書
 - 基本設計書
 - 詳細設計書
 - プログラムリスト
- 製造文書
 - 解析実施要領書／手順書
 - 記録媒体仕様書／作成手順書
- 受入試験文書
 - 受入試験計画書
 - 受入試験手順書

搭載ソフトウェアに関する
文書のみ。全体システムに
関する文書は省略。

2.2 ロケット搭載ソフトウェアの文書体系(2/2)

★実機製作における作成文書

- 解析報告書(ミッション固有定数データの設計解析)
- ミッション定数仕様書
- 受入試験実施要領書(試験仕様を含む)
- 受入検査成績書
- 文書パッケージ

★開発試験文書

- モジュール単体(CSU)試験仕様書、試験成績書
- 機能(CSC、CSCI)試験計画書、試験仕様書、試験成績書

★その他(アルゴリズム設計書等)

2.3 主要ソフトウェア・ツール

2.3.1 数学的シミュレーション・プログラム

(SSP: Scientific Simulation Program)

2.3.2 計算機シミュレーション・プログラム

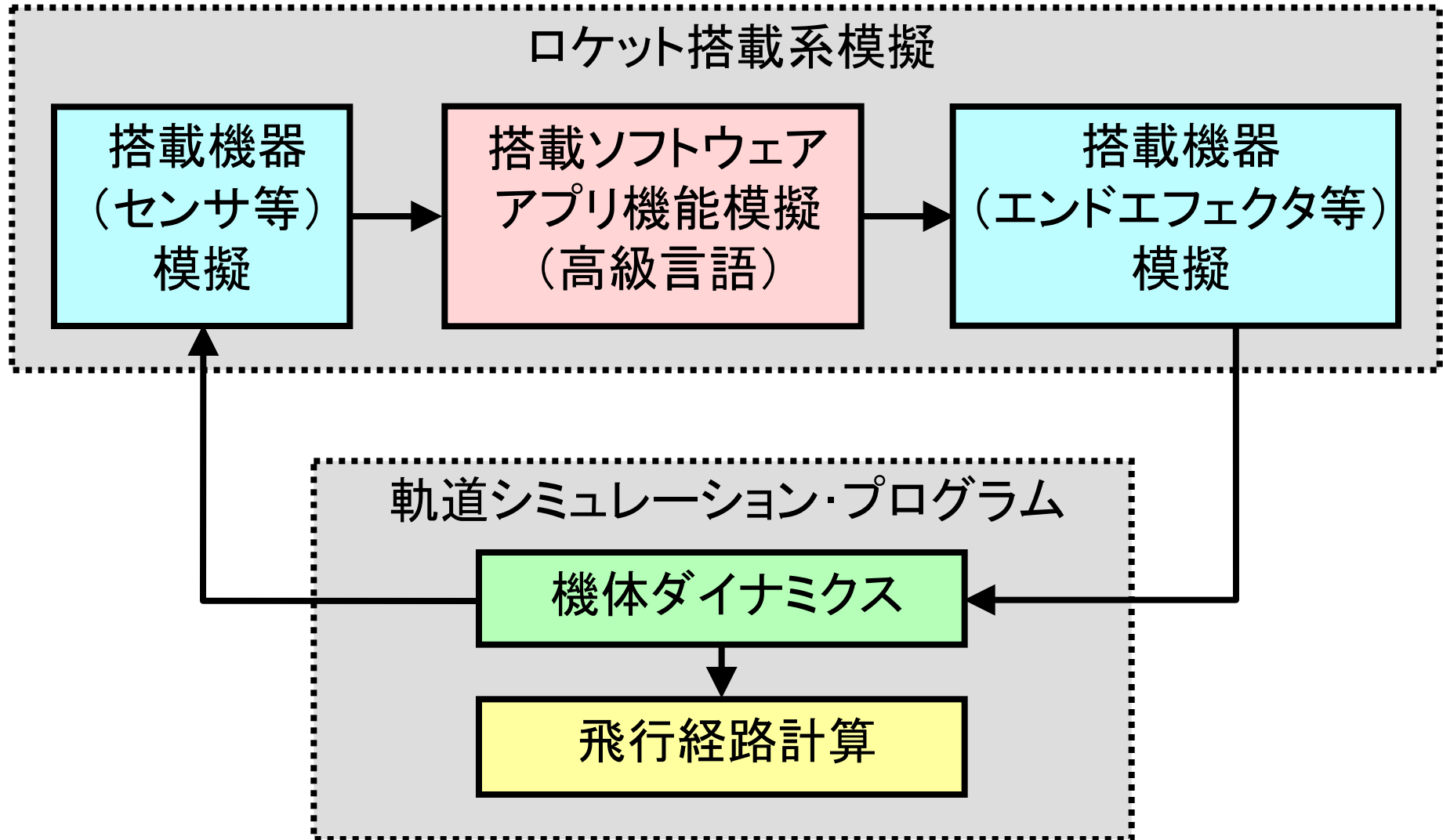
(ICS: Interpretive Computer Simulation)

2.3.1 数学的シミュレーション・プログラム (SSP: Scientific Simulation Program)

- (1) 高級言語で作成(数学モデル、搭載ソフトのプロトタイプ)
- (2) 対象サブシステムの機能シミュレーション(閉ループ)
- (3) 用途

- ◆ アルゴリズム設計、トレードオフ解析
- ◆ 軌道投入精度等のシステム設計解析
- ◆ 搭載計算機に対する要求(CPU速度、メモリ容量)見積もり
- ◆ 搭載ソフトの機能検証における評価基準値作成
- ◆ 打上げ号機毎に行うミッション解析(搭載ソフトウェアに組込むミッション固有定数データの設計解析・検証含む)

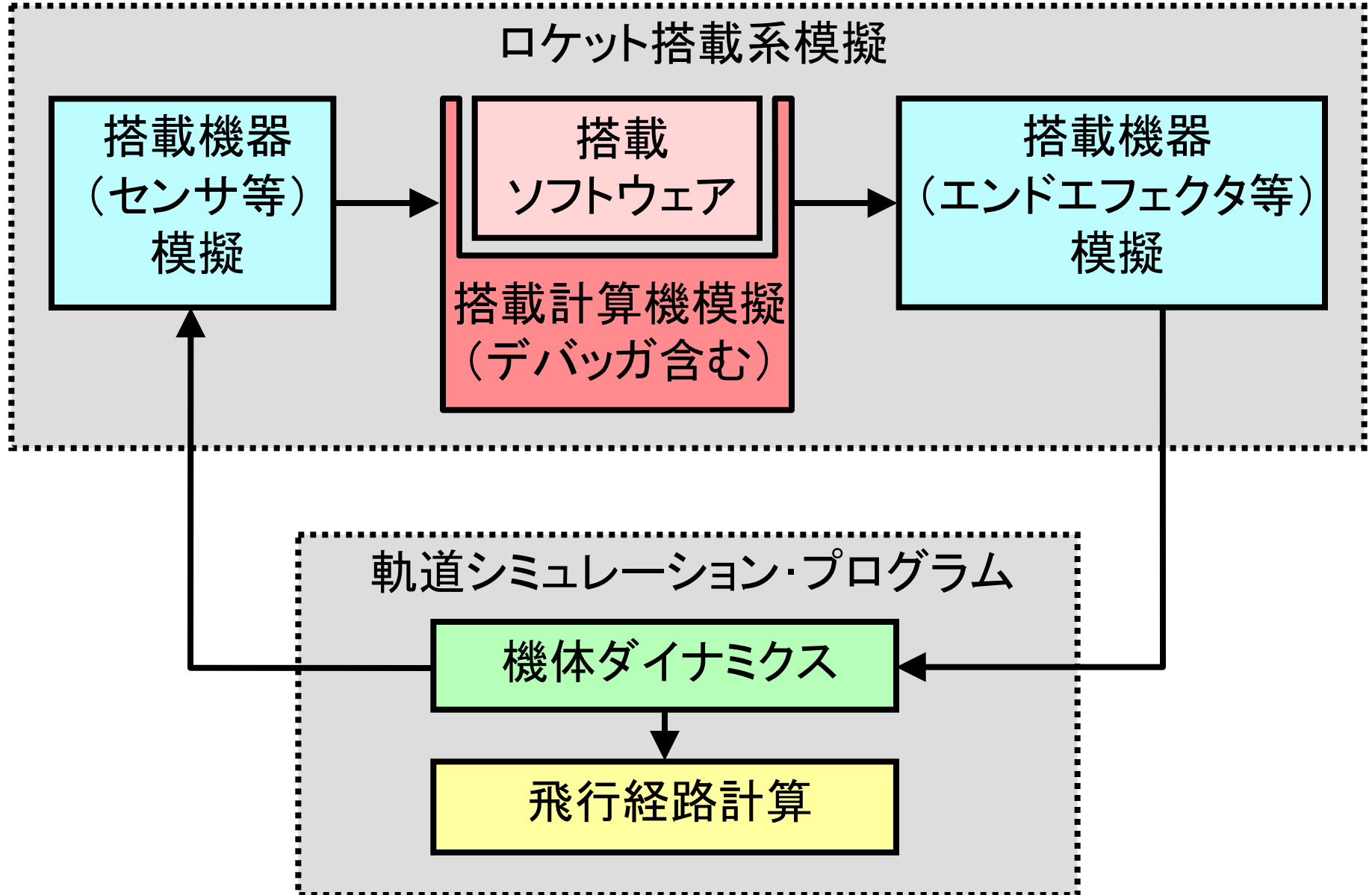
図2.3-1 数学的シミュレーション・プログラム(SSP)



2.3.2 計算機シミュレーション・プログラム (ICS: Interpretive Computer Simulation)

- (1) ソフトウェア・エミュレータ
- (2) デバッグ機能、言語処理系を完備
- (3) 搭載計算機の命令コード(搭載ソフト)を忠実に実行
- (4) 対象サブシステムの機能シミュレーション(閉ループ)
- (5) 用途
 - ◆ 搭載ソフトウェアのプログラミング
 - ◆ 搭載ソフトウェアのデバッグ、機能検証
 - ◆ 搭載ソフトウェアとミッション固有定数データの組込検証

図2.3-2 計算機シミュレーション・プログラム(ICS)



2.4 作業内容

2.4.1 開発段階

2.4.1.1 搭載ソフトウェアに対するシステム要求の定義

2.4.1.2 搭載ソフトウェアの基本設計

2.4.1.3 搭載ソフトウェアの詳細設計

2.4.1.4 搭載ソフトウェアのプログラミング

2.4.1.5 搭載ソフトウェアのユニット(CSU)試験

2.4.1.6 搭載ソフトウェアの機能検証試験

2.4.1.7 アビオニクス系サブシステム試験

2.4.1.8 開発完了の確認

2.4.2 システム統合試験(地上試験機)

2.4.3 実機製作

2.4.3.1 ミッション解析

2.4.3.2 実機用搭載ソフトウェアの製作

2.4.3.3 最新機体特性に基づく最終確認

2.4.1 開発段階

2.4 .1.1 搭載ソフトウェアに対するシステム要求の定義

- (1) 開発目標の設定
- (2) 初期システム概念の検討
- (3) システム要求条件の定義
- (4) システム要求条件のシステム構成品目への配分
- (5) 搭載ソフトウェアに対するシステム要求の詳細化
 - ・要求仕様の定義
 - ・機能仕様の定義(機能設計、方式設計、予備設計)
- (6) 開発仕様書の制定

2.4.1.2 搭載ソフトウェアの基本設計

- (1) モジュール分割
- (2) アルゴリズムの詳細化
- (3) ロジックの設計及び検証
- (4) 基本設計書の作成

2.4 .1.3 搭載ソフトウェアの詳細設計

- (1) データ仕様の設計
- (2) リアルタイム・タスク管理モジュールの設計
- (3) 入出力インタフェース部分のロジック設計
- (4) 詳細な処理ロジックの設計
- (5) 詳細設計書の作成

2.4.1.4 搭載ソフトウェアのプログラミング

- (1) コーディング
- (2) 翻訳
- (3) リンク／ロードモジュール作成
- (4) レビュー及びデバッグ

2.4.1.5 搭載ソフトウェアのユニット(CSU)試験

- (1) 試験計画及び試験仕様を文書に定める
- (2) 各CSUを一つひとつ単独に試験する(作成者が実施)
- (3) 全パス／全分岐条件網羅(が前提だが、作成者まかせ)
- (4) 別途求めた基準値(検査規格)と比較
- (5) 結果を成績書にまとめる(実際は計算機出力の整理程度)

2.4.1.6 搭載ソフトウェアの機能検証試験

- (1) 試験計画、試験仕様及び試験手順を文書に定める
- (2) 個別機能の検証試験(CSC試験)
 - (a) 機能仕様を一つひとつ確認する
 - (通常はCSCI試験に含まれることが多い)
- (3) 統合機能検証試験(CSCI試験)
 - (a) ノミナルケース
 - (b) 例外事象発生ケース
 - (c) 変動要因(誤差源)発生ケース
 - (d) 異常・故障発生ケース
 - (e) 堅固性(ストレス耐性)確認ケース
- (4) 結果を成績書にまとめる

2.4.1.7 アビオニクス系サブシステム試験

- (1) BBM(ブレッド・ボード・モデル)システム試験
- (2) EM(エンジニアリング・モデル)システム試験(地上試験)
- (3) EMシステム試験(飛行機搭載試験)

2.4.1.8 開発完了の確認

- (1) 製品仕様書及び製造図面類の作成
- (2) 実機製作・試験の工程の確認
 - ・システム統合試験用ソフトウェアの製作
 - ・システム統合試験用ソフトウェアの受入試験
- (3) 開発完了の確認審査(PQR相当)
 - ・開発試験結果が良好であること、実機製作・試験(量産)に移行できることを確認

2.4.2 システム統合試験(地上試験機による試験)

- (1) 地上試験機の工場組立(工場設備との噛合わせ含む)
- (2) 地上試験機の射場作業(射場設備との噛合わせ含む)

2.4.3 実機製作

2.4.3.1 ミッション解析

飛行計画の作成、ミッション固有の定数データの設計

- (1) 飛行経路の作成
- (2) 制御系解析
- (3) 誘導解析
- (4) 軌道誤差解析
- (5) 電波リンク解析
- (6) 飛行安全解析

2.4.3.2 実機用搭載ソフトウェアの製作

- (1) ミッション定数仕様書を定める
- (2) ミッション定数のコーディング、点検
- (3) 受入試験の試験仕様及び試験手順を定める
- (4) 搭載ソフトウェア(命令部分)とミッション定数との統合検証
- (5) 収録媒体作成
- (6) 実機用搭載計算機による確認試験
- (7) ミッション定数仕様書及び受入検査成績書を含む文書パッケージを作成し、収録媒体に添付して納入

2.4.3.3 最新機体特性に基づく最終確認

- (1) 最新機体特性を反映した飛行シミュレーション
- (2) ノミナルケース、堅固性確認ケース

2.5 試験の形態

2.5.1 開発段階

2.5.1.1 アルゴリズム設計検証

2.5.1.2 搭載ソフトウェア開発検証

2.5.2 システム試験段階

2.5.2.1 サブシステム試験

2.5.2.2 全段統合システム試験

2.5.3 実機段階

2.5.3.1 実機用製作試験

2.5.3.2 工場組立試験

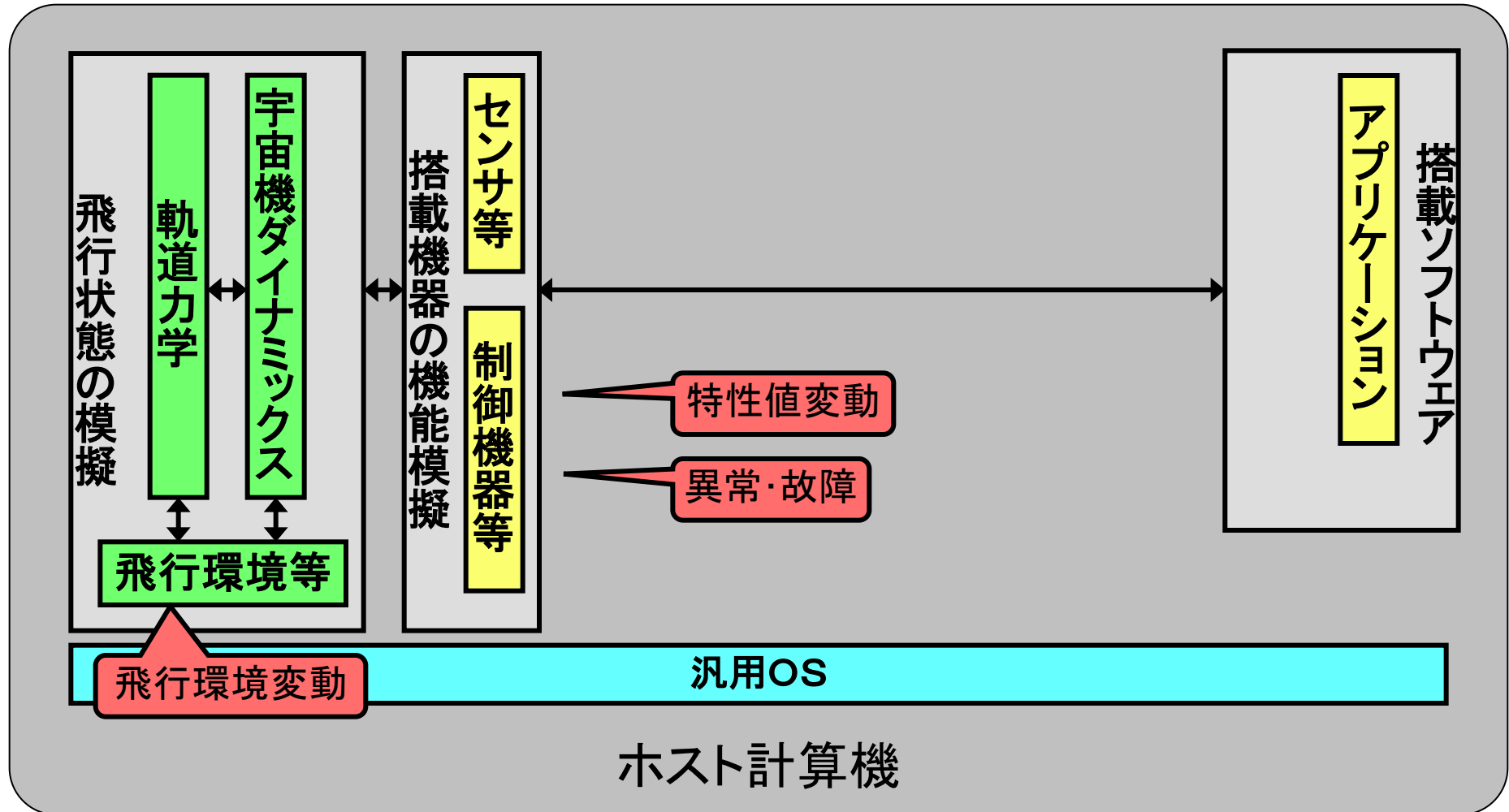
2.5.3.3 射場整備点検

2.5.1 開発段階

2.5.1.1 アルゴリズム設計検証

- (1) 2.3.1項「数学的シミュレーション・プログラム」によるホスト計算機(汎用計算機)を用いた検証環境
- (2) 搭載ソフトウェアのRTOSやI/Oドライバを除いたアプリケーション機能(システム機能)部分について、アルゴリズムのトレードオフ解析や設計検証を行う
- (3) 搭載ソフトウェアをアセンブリ言語で開発する場合でも高級言語で作成
- (4) 飛行環境変動や宇宙機特性値の変動及び異常・故障等を模擬した飛行シミュレーションを実施し、機能・精度を評価

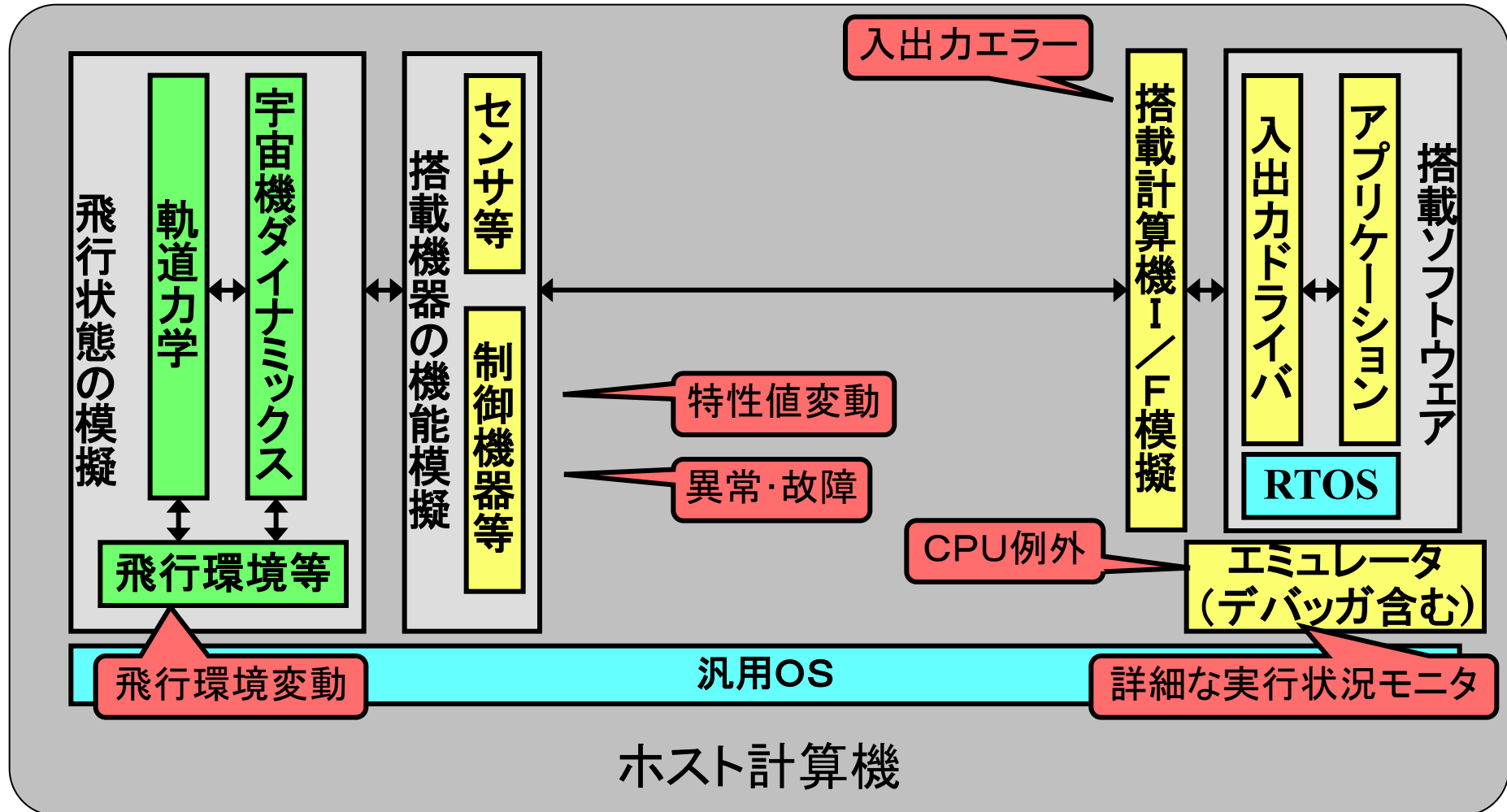
図2.5-1 ホスト計算機による機能模擬方式



2.5.1.2 搭載ソフトウェア開発検証(1／3)

- (1) 2.3.2項「計算機シミュレーション・プログラム」を用いたソフトウェア・エミュレータ方式の検証環境
- (2) ターゲット計算機(実運用に用いる計算機)で実行可能な搭載ソフトウェア(RTOSやI/Oドライバを含む全体)の検証
- (3) ソフトウェア・エミュレータは、ターゲット計算機を忠実に模擬し、ロードモジュールの命令を一つひとつ解釈して実行。変数変動範囲のチェック及び各種デバッグ機能を備える
- (4) 飛行環境変動や宇宙機特性値の変動、異常・故障の発生ケース、RTOSやI/Oドライバの関数戻り値が正常でない全てのケース及び、演算例外等を模擬した飛行シミュレーション

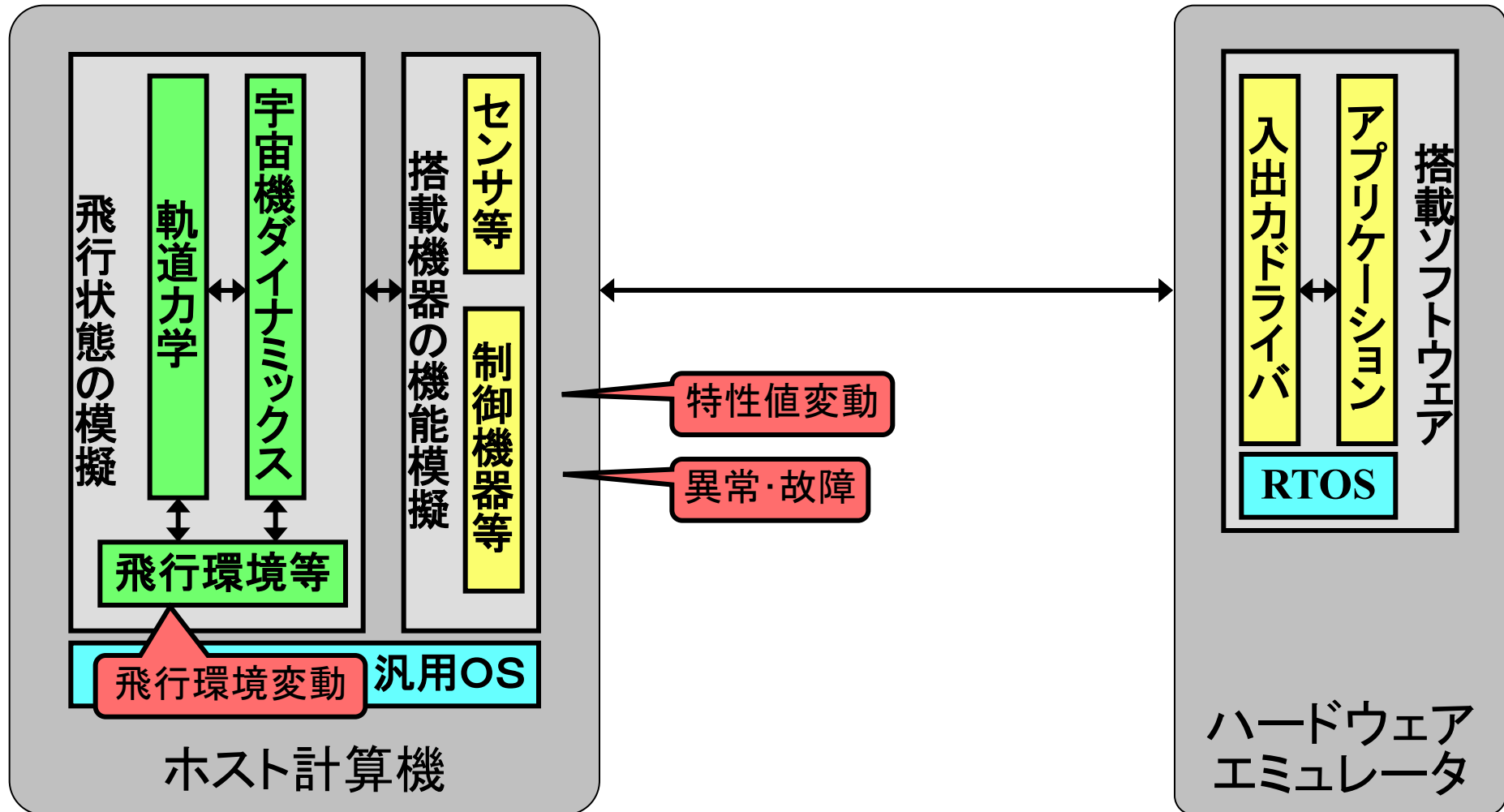
図2.5-2 ソフトウェア・エミュレータ方式



2.5.1.2 搭載ソフトウェア開発検証(2／3)

- (1) ターゲット計算機(実運用に用いる計算機)のプロセッサと同種プロセッサを用いたハードウェア・エミュレータ方式の検証環境
- (2) ターゲット計算機で実行可能な搭載ソフトウェア(RTOSやI/Oドライバを含む全体)の検証
- (3) 飛行環境変動や宇宙機特性値の変動、異常・故障の発生ケース等を模擬した飛行シミュレーション
- (4) RTOSやI/Oドライバの関数戻り値が正常でない全てのケース及び演算例外等の検証は困難

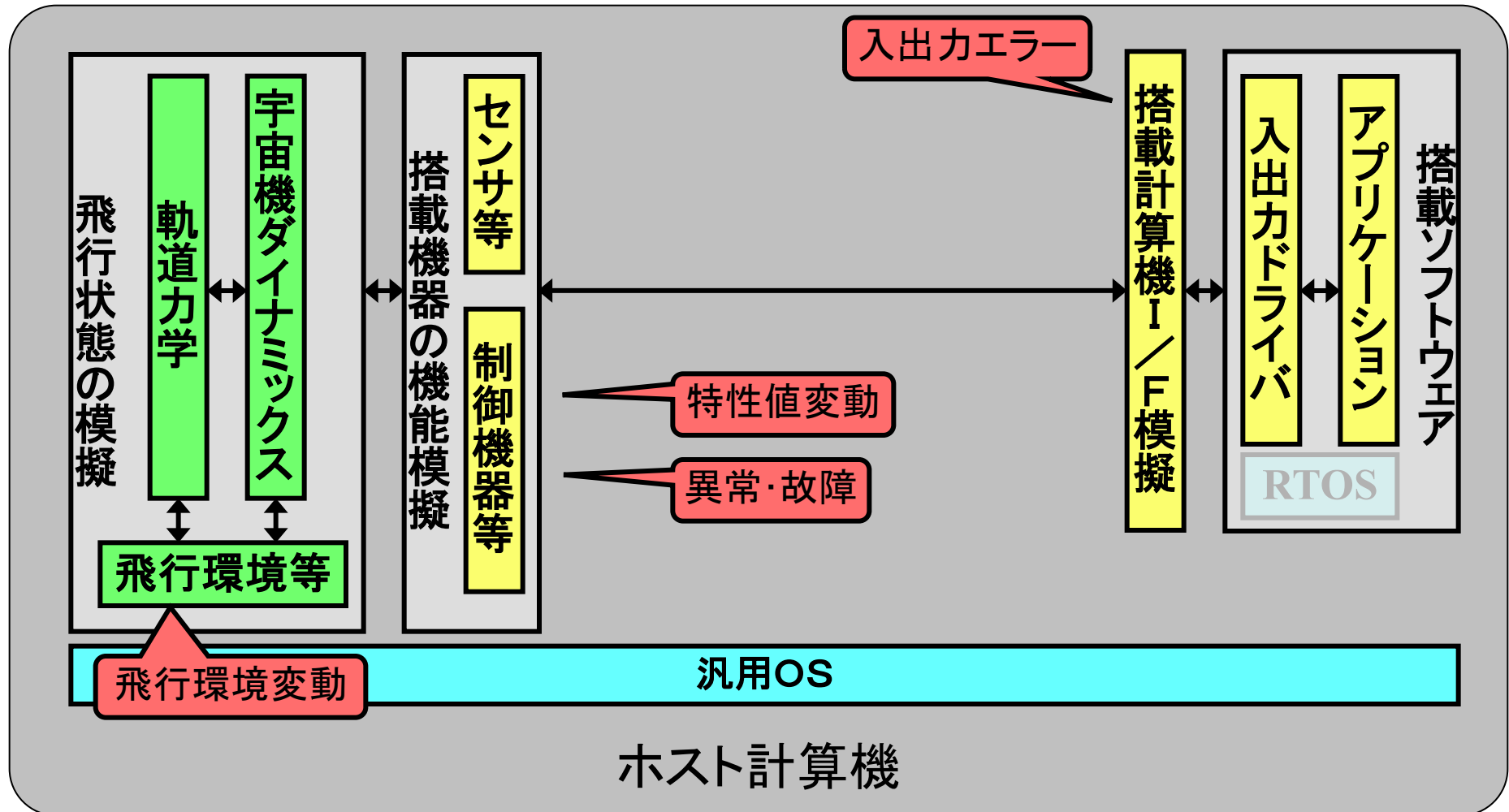
図2.5-3 ハードウェア・エミュレータ方式



2.5.1.2 搭載ソフトウェア開発検証(3／3)

- (1) ホスト計算機(汎用計算機)を用いた検証環境
(フル・ソフトウェア・シミュレーション方式)
- (2) ハードウェア依存のI/Oドライバ含む搭載ソフトウェア(RTOS
除く)の検証
- (3) I/Oドライバがハードウェア・レジスタを参照するところを、
ハードウェア・インタフェースを模擬したメモリの参照に変更
(システム・ジェネレーション時のメモリマップ変更)
- (4) ハードウェア・エミュレータ方式の欠点を補完し、I/Oドライバ
の関数戻り値が正常でない全てのケースを模擬した飛行シ
ミュレーション
- (5) RTOSについても、I/Oドライバと同様に含めるのが望ましい

図2.5-4 フル・ソフトウェア・シミュレーション方式

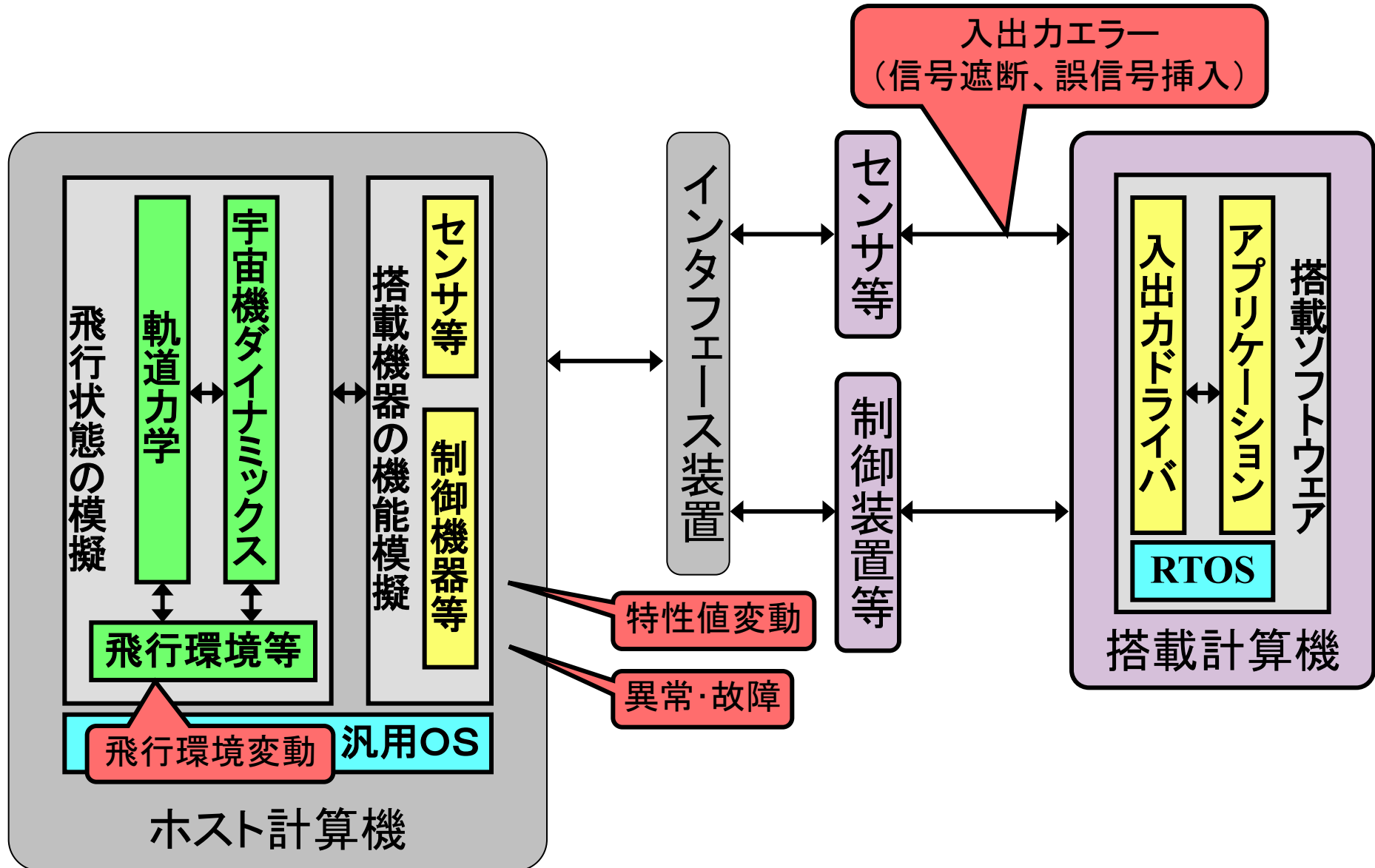


2.5.2 システム試験段階

2.5.2.1 サブシステム試験

- (1) 搭載機器（技術試験モデル等の試作品段階が多い）を組み合わせ、各機器間のインタフェース及び、サブシステム全体の機能・性能を確認する
- (2) 通常はフライト用の設計製作に入る前に行う
- (3) 搭載ソフトウェアは検証試験途上にあることが多いが、実運用段階で想定される飛行経路の案に対応した定数データを組み込んで試験に供する
- (4) 関連機器を一つずつ順次接続してインタフェースを確認し、全体接続後に飛行シミュレーション

図2.5-5 サブシステム試験構成



2.5.2.2 全段統合システム試験

- (1) 搭載機器(搭載ソフトウェア含む)をロケット機体(地上試験用)に順次、組み立てながら点検
- (2) 点検装置はアンビリカル・コネクタ(ロケット機体と地上装置とのインタフェース用)を介し、点検指示と結果データの取得
- (3) 搭載ソフトウェアは点検指示コマンドを受け、ロケット機体各機器に信号を送出(整備点検支援機能)
- (4) ロケット搭載状態での飛行シミュレーションは、搭載ソフトウェア自身が持つ整備点検支援機能による

図2.5-6 工場組立・発射整備点検時の構成

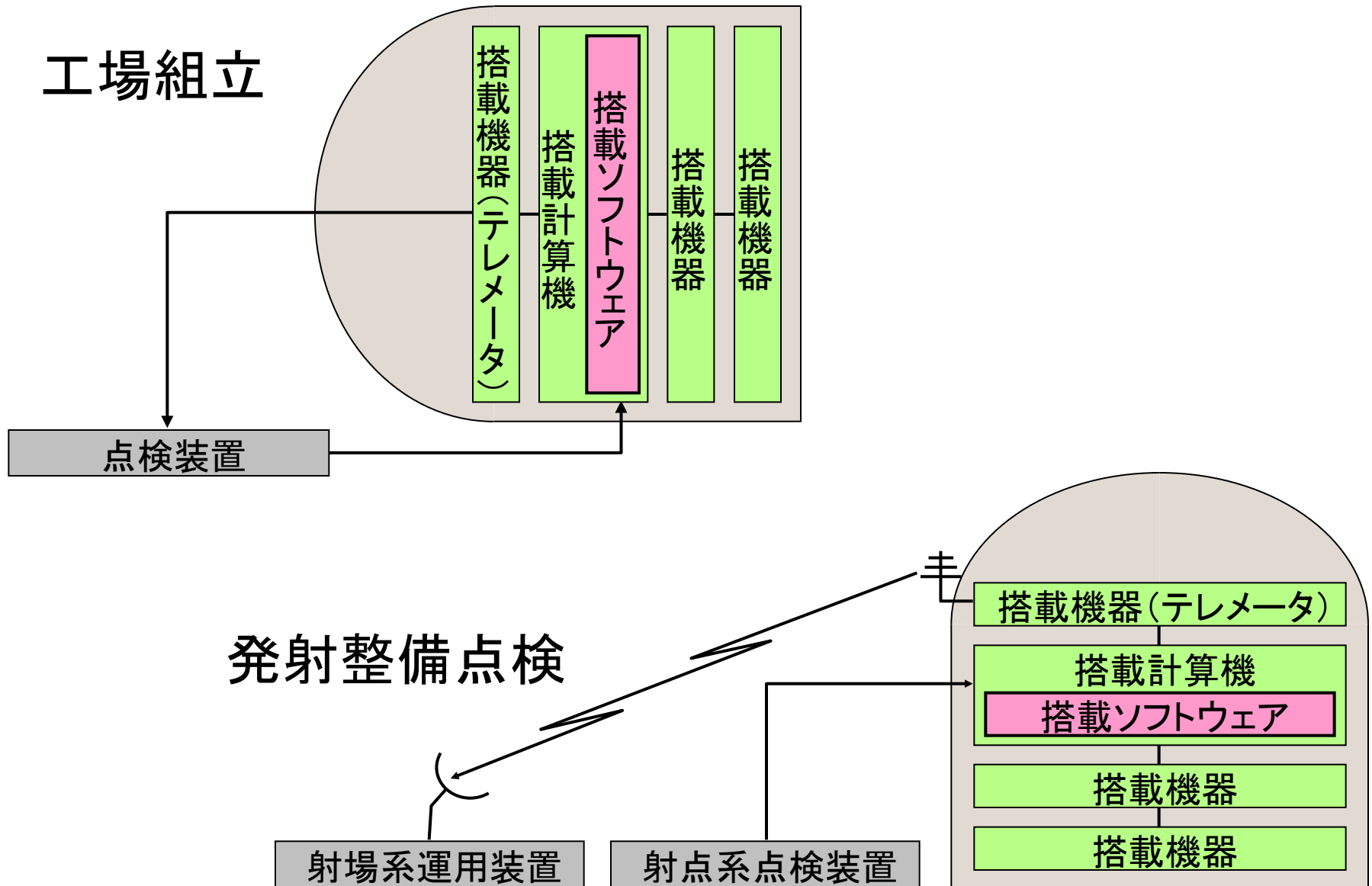
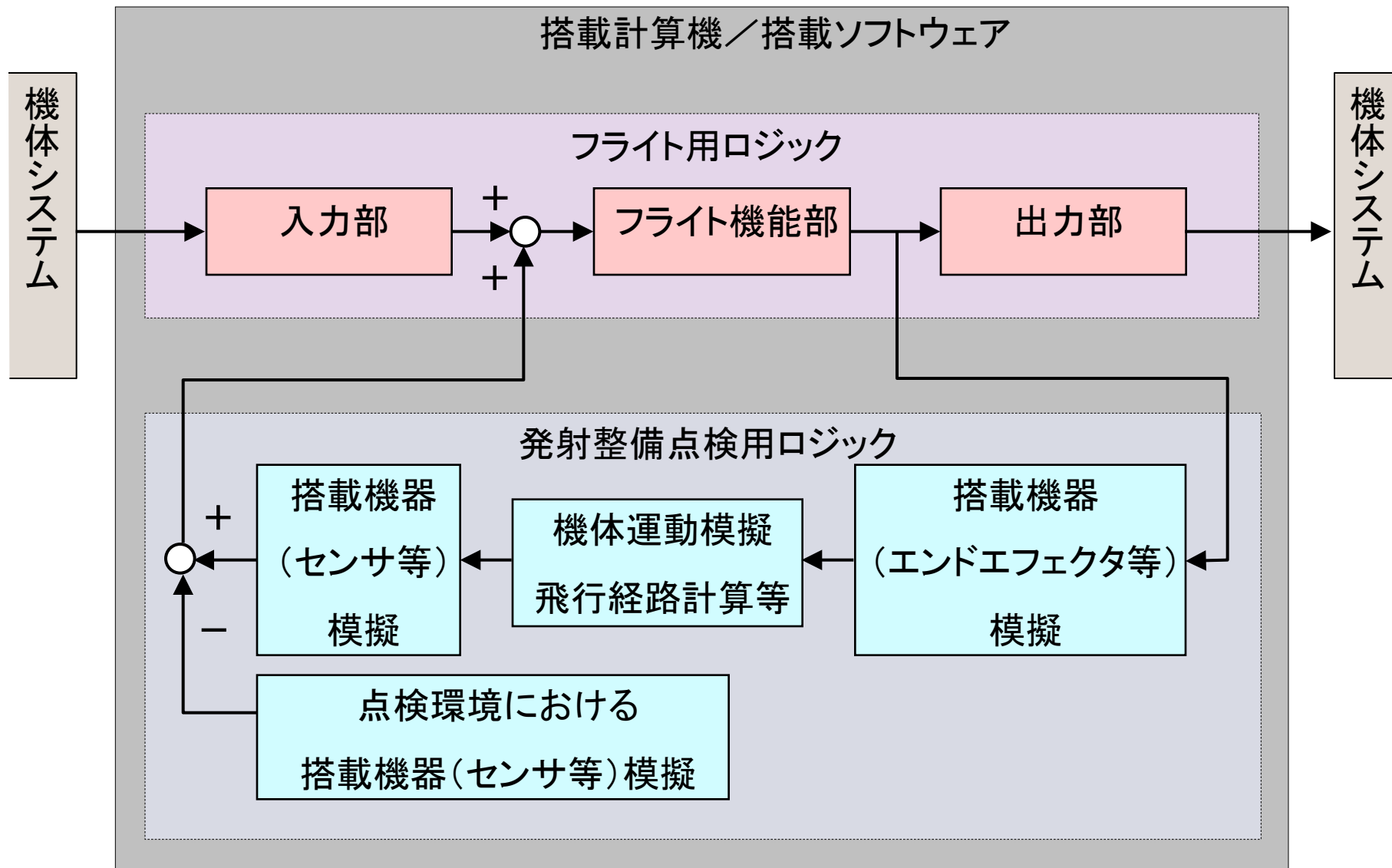


図2.5-7 整備点検における模擬飛行テスト



3 管理標準

宇宙機システム／ハードウェア

◆信頼性プログラム標準

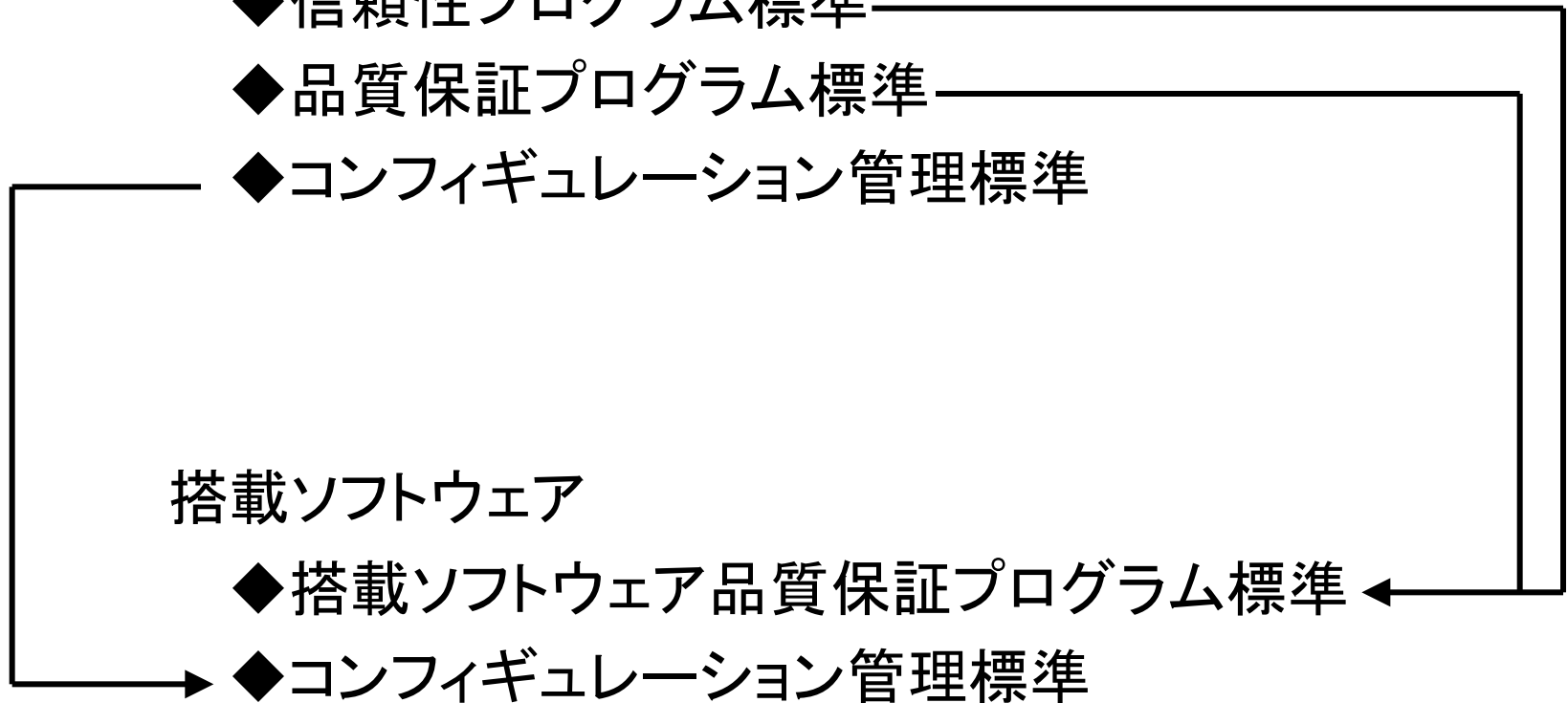
◆品質保証プログラム標準

◆コンフィギュレーション管理標準

搭載ソフトウェア

◆搭載ソフトウェア品質保証プログラム標準

◆コンフィギュレーション管理標準



3.1 信頼性プログラム標準の内容

- (1) 信頼性設計活動及びその管理活動の計画設定に関すること
- (2) 信頼度予測及び信頼性設計解析に関すること
- (3) 設計管理に関すること(＊)
- (4) 設計審査に関すること(＊)
- (5) 不具合及び異常・故障の管理に関すること(＊)
- (6) 品目の管理に関すること(＊)
- (7) 部品・材料等の選定に関すること
- (8) 認定試験・信頼性評価に関すること

(＊) ソフトウェア品質保証プログラム標準に取り込んでいる項目

3.2 コンフィギュレーション管理標準の内容

- (1) コンフィギュレーション(構成)管理の計画設定に関すること
- (2) コンフィギュレーションの識別に関すること(＊)
- (3) 変更管理に関すること
- (4) 記録及び報告に関すること

(＊) ソフトウェア固有の詳細要求は、ソフトウェア品質保証プログラム標準に規定

3.3 搭載ソフトウェア品質保証プログラム標準の内容

- (1) 品質保証活動及びその管理活動の計画設定に関すること
- (2) ソフトウェア開発計画の立案に関すること
- (3) 文書・データの管理に関すること
- (4) 設計技術管理に関すること(設計審査、設計の妥当性確認等)
- (5) 工程管理に関すること
- (6) 検査・試験に関すること
- (7) 不具合管理に関すること
- (8) コンフィギュレーション管理に関すること
- (9) 購買管理に関すること
- (10) 出荷に関すること
- (11) 納入後の維持管理に関すること

3.4 設計の妥当性確認項目の例

(1) 機能要求仕様の全項目と検証項目との突き合わせ

(2) 設計の根拠、データの根拠の確認

(3) 例外要因、変動要因に対する検証

- ◆ 計算機例外、OS／入出力ドライバ関数の例外的な戻り値

- ◆ BIT、FDIR、その他アプリが対応機能を有する異常・故障の要因

- ◆ 飛行環境や機体特性の変動(誤差源)

(4) 搭載ソフトウェアの堅固性確認

(注) BIT : Built In Test

FDIR : Fault Detection Isolation and Reconfiguration

図3-1 ソフトウェア変更管理に係る作業フロー

