

## 15-A-18

# ロケットエンジンにおける モデルベース信頼性評価技術の構築と試行<sup>1</sup>

### 1. 概要

宇宙輸送システムはひとたび点火されて地上を離れたら、そのミッション終了まで機能を停止することが許されない。当然、修理もできない。文字通り一発勝負である。ロケットエンジンはその推進機能を担う中核のシステムであり、非常に高い信頼性が要求される。

これまでのロケットエンジンは開発時に膨大な回数の燃焼試験を行い、その過程で顕在化した不具合は徹底的に対処するという実証主義により信頼性を確保してきた。しかし、このような開発プロセスには大きく2つの課題がある。

1つは今後有人宇宙輸送等にも使用できるような高い信頼性を有するロケットエンジンを実現するためには、その信頼度を評価するために多数の大規模なシステム実証試験（エンジン燃焼試験）が必要となり、試験にかかる費用・時間が莫大になること、もう1つは試験で不具合を洗い出し設計に立ち戻って対処をすることにより、追加の開発コストや期間が非常に大きくなることである。

このような課題に対しては、上流の設計段階で十分な設計検証を行うことが重要であり、有効な手法の1つとして、自動車をはじめとする民生分野において広く行われているシミュレーション技術を活用したモデルベース開発がある。これは、ロケットエンジンの信頼性設計・検証に関する課題についても同様に有効であると考え、我々はモデルベースの信頼性評価技術<sup>2</sup>の構築と試行を実施した。

モデルベースの信頼性評価技術は、設計と並行してモデルを用いた設計検証を行うことにより設計で信頼性を効率的に作り込むこと、及び、大規模な信頼性試験をモデルを用いた設計検証と小規模な要素試験で代替することを可能とする。これにより設計品質を向上し手戻りを予防し信頼性試験規模を抑制する。開発の効率化に加え定量的な信頼度評価までもモデルベースに取り込もうとする点が広く行われているモデルベース技術の狙いと相違である。

本事例ではこのモデルベースの信頼性評価技術について紹介すると共に、次世代ロケット

<sup>1</sup> 事例提供: 国立研究開発法人 宇宙航空研究開発機構 研究開発部門 田口 元 氏

<sup>2</sup> 本取り組みで言う「モデルベース」とは SysML (System Modeling Language) / UML (Unified Modeling Language) 等の仕様モデルや制御開発で扱うプラントモデルのみならず、CAE (Computer Aided Engineering) やシミュレーションを使った開発全般を指している。特に本取り組みでは扱う特性が信頼性であるため、信頼性に関わる故障シナリオといった論理モデルと故障現象を評価する CAE といった物理モデルの両方を「モデルベース」の範囲に含めている。

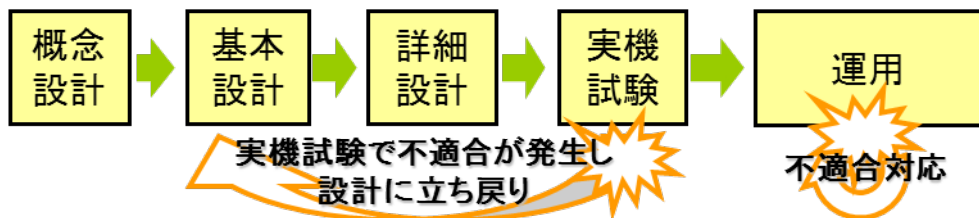
エンジン（LE-X）技術実証プロジェクトにおける適用試行事例を紹介する。なお、本取り組みを含むロケットの信頼性向上の取り組みの全体概要については参考文献[1]を参照されたい。

## 2. 取り組みの目的

### 2.1. 解決すべき課題

これまでのロケットエンジン開発は未知の技術領域へのチャレンジという性格が強く、その開発は実証的なプロセスとならざるを得なかった。そのようにして一步步着実に技術獲得を進めた結果、1990年代にはH-IIロケットの主エンジンであるLE-7において主エンジン国産化を実現するに至った。

しかし、LE-7エンジンの開発を振り返ってみた時、開発後期での不具合により大きな手戻りが発生し開発経費の増大や計画遅延が発生する等、開発プロセス上、改善を要する点があった。また、開発が完了し、改良型であるLE-7Aエンジンも含め、実用段階に移行した後も不具合発生とその対処がしばしば発生し、場合によっては打上げコストにも影響を及ぼしているという状況がある（図15-A-18-1）。



### 不適合の6～7割は設計起因

#### ◆LE-7/7Aエンジンの実績

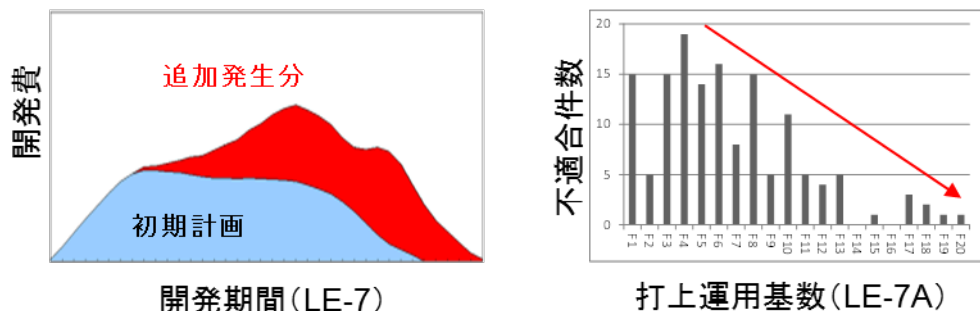


図 15-A-18-1 現行エンジン開発・運用における信頼性の課題

これらの要因となった不具合を分析したところ、開発時不具合、運用時不具合のいずれにおいても設計に起因する不具合が6～7割を占めていた。特に、製造・運用・使用条件等のばらつきに起因する故障モードに対して設計段階で十分な識別と対処ができていなかったの

ではないかということ、及びこれらに加えて複雑な機器の組合せによるシステムでは複合・連鎖事象等に対する十分な識別が困難な部分があり、これまでの単純な FMEA (Failure Mode and Effect Analysis) 等の手法に依存した故障モード識別方法では限界があったということが課題として識別された。

また、実証的なプロセスでは設計・試作段階で識別できていない故障モードについては大規模なシステム実証試験(エンジン燃焼試験)により不具合の識別と対策を行う事となるが、この実証試験用の供試体は実機相当の製品で非常に高価なものとなるため供試体を多数確保することが難しく、限られた予算・期間の中でばらつきと全ての故障モードの検証を行うには限界があるということも課題として識別された。

## 2.2. 本取り組みの目標

以上のような課題を踏まえ、本取り組みの実施に際して目標を以下の通り設定した。

- ① 開発後期段階や運用段階での不具合を低減させるために、開発初期段階で故障モードを網羅的に識別・対処し、運用や部品などのばらつきも考慮した新たな設計手法の構築
- ② 高い信頼性を確保するために、開発段階で十分なばらつきの確認、故障モード毎の検証を大規模な実証試験によらず効率的に実施する方法の構築

## 3. 対象システムと適用技術・手法

### 3.1. 対象の概要と適用工程

本取り組みは、次期ロケットへの適用を目指して研究が進んでいた次世代ロケットエンジン「LE-X」に対して行われた。LE-X エンジンとは低コスト・高信頼性を両立させた液体酸素／液体水素を推進薬とするロケットエンジンであり、これまで日本が上段エンジンの開発で獲得した簡素でロバストなエンジンサイクル（エキスパンダーブリードサイクル<sup>3</sup>）と 1 段エンジンの開発で獲得した高圧・大推力エンジン技術の融合を目指したエンジンであり、研究の主な目的は、大推力エキスパンダーエンジンという世界に類を見ないエンジンの実現性を見極めるために特にリスクが高いコンポーネントについて試作試験を行って技術実証する事であった。

LE-X 技術実証の活動範囲が上記範囲であるため、本取り組みは主としてエンジンのコンポーネント設計からコンポーネント試験にかけて行っている。また、プロセス自体がまだ確性されたものではないため、LE-X エンジンの設計・開発は従来ながらの試作試験プロセスで行いこれと並行する形で新しい手法の構築・試行（3.2 参照）を実施している。

ロケットエンジンについて簡単に特徴を述べると、動作環境は非常に過酷で物理現象は複

---

<sup>3</sup> 燃焼室を冷却し高温化した推進薬によりタービンを駆動する方式のうち、タービンを駆動した後のガスを燃焼させず排気する方式

雑であるが、機能としてはそれほど複雑ではない。動作環境について言えば、燃焼ガスの温度は約  $3000^{\circ}\text{C}$  となり一般的な金属材料は溶けてしまうため燃焼室を中空溝構造の壁とし、その溝内に推進薬となる約  $-250^{\circ}\text{C}$  の液体水素（液体酸素は約  $-200^{\circ}\text{C}$ ）を流して冷やすことにより構造を維持している（再生冷却方式）。また、燃焼室の冷却に使用された液体水素は熱交換で得たエネルギーにより推進薬を燃焼室（約 120 気圧）に送り込むためのターボポンプを駆動する。消費される推進薬は毎秒ドラム缶約 3 本分にものぼり、これらの推進薬が燃焼室で燃焼反応を経て約  $4\text{km/s}$  の噴出ガスとなってロケット機体を推進する。一方で基本機能はエンジンの一連のシーケンスを実現する「予冷」「点火」「燃焼」「停止」の 4 機能のみといって良く、自動車エンジンのような複雑な制御機構が必要となる機能は現時点では有していない。

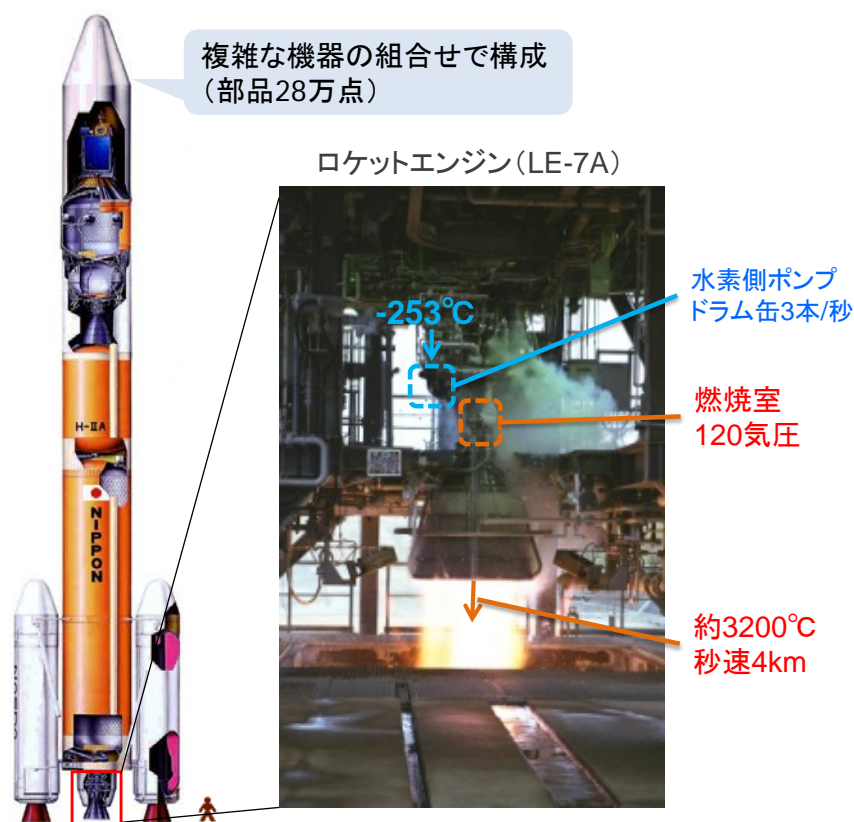


図 15-A-18-2 ロケットエンジン (LE-7A) の概要

### 3.2. 方法論（どんな技術・手法を用いて実施したか）

先述の課題に対しては、上流の設計段階で十分な設計検証を行うことが重要であり、有効な手法の1つとしてシミュレーション技術を活用したモデルベース開発が自動車をはじめとする民生分野において広く行われている。ロケットエンジンの信頼性設計・検証に関する課題についても同様にモデルベース開発は有効であると考え、我々はモデルベースの信頼性評価技術の構築を行う事とした。

具体的には先述の2つの課題に対して、以下の2つの手法をモデルベース中心に行うこととした

- ① 網羅的故障モード識別・対応設計
- ② 数値解析・要素試験中心の検証

図 15-A-18-3 モデルベースの信頼性設計・検証プロセスの概要にプロセスの概要を示す。以下、それぞれの手法について方法論を記述する。

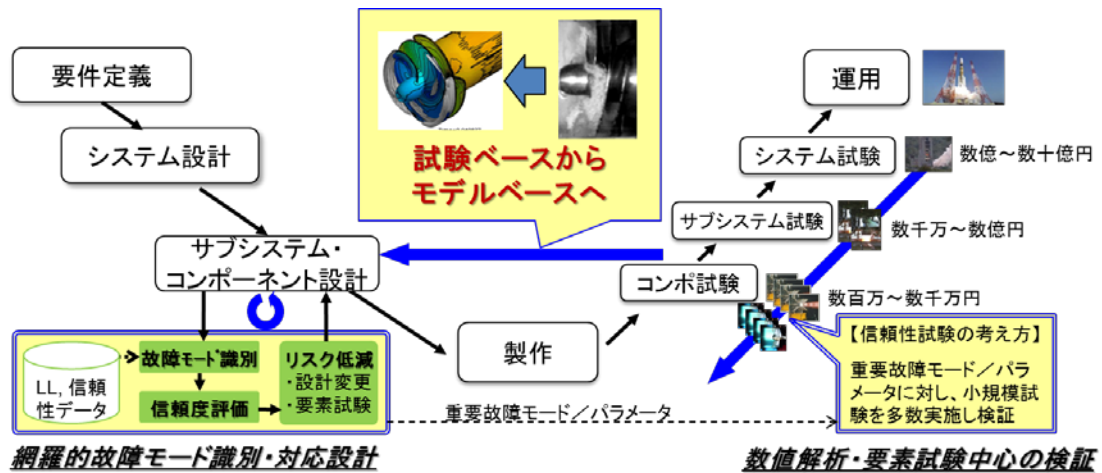


図 15-A-18-3 モデルベースの信頼性設計・検証プロセスの概要

#### (1) 網羅的故障モード識別・対応設計

信頼性評価をモデルベースで進めると一口に言っても、故障に関する全ての物理現象を表す非常に確からしいモデルの存在を前提にすることはできない。そのため現状のモデルベース開発においては、設計で考慮すべき信頼性に関わる頂上事象(例えば、エンジン性能未達や破裂・制御不能等)をモデルで評価できる粒度(=故障モード)に分解した上で網羅的に識別することが必要になる。

信頼性の分野からリスク/安全性の分野で起きている事に少しだけ目を転じると、主に原子力や有人宇宙の分野において、システム安全に関する分析手法として、確率論的リスク評価 PRA (Probabilistic Risk Assessment) が活用されている。PRA とはシステムのリスクをハザードシナリオと言われる論理モデルを用いて定量的かつ網羅的・体系的に分析するための秩序立てられた方法論であり、宇宙分野においては1986年のチャレンジャー号事故以降、NASA (アメリカ航空宇宙局) が PRA を適用し従来のアポロ計画で用いていた定性的な FMEA や FTA (Fault Tree Analysis) による評価を補うものとして有用性が認識され、その後宇宙ステーションをはじめ主要なプロジェクトに適用が広がってきている。

このような状況を踏まえ、信頼性の分野においても設計で考慮すべき最終事象について PRA 手法を参考に運用シナリオから想定される故障シナリオを網羅的・体系的

に展開し、関連する故障モードに分解する手法を構築することとした。これにより頂上事象に関連する故障モードを網羅的・体系的に識別することが可能になるとともに、故障モード発生時の影響を故障シナリオという形でたどることが可能となる。なお、故障シナリオは PRA と同様に解析可能なモデルとしてブール代数式に基づく論理モデルとして表現することとし、数学モデルへ変換して最終事象の確率算出等の定量的解析が実行可能なものとした。

さらに、故障モード識別の網羅性を向上させるためには、故障モードを軸に多様な視点の故障モード識別手法を組み合わせることが有効であると考え、これまでの膨大な開発実績や知見および他国や他産業における失敗事例を故障モードを軸に整理し直し体系化した“故障モードライブラリ”や“Lessons Learned データベース”を整備し、新規エンジン開発時に行う FMEA の効率化と漏れ抜け防止を図ることとした。

これにより、時系列 (ESD (Event Sequence Diagram) <sup>4)</sup>、トップダウン (FTA)、ボトムアップ (FMEA)、リストアップ (故障モードライブラリ)、そして有識者によるレビューという多様な視点で故障シナリオおよび故障モード識別を行うことによりその網羅性を確保することとした (図 15-A-18-4)。このような多様な視点で故障シナリオや故障モードを既存のツールにより整合をとりつつ実施することは困難を極めるため、実行環境として支援システムの整備も並行して進めることとした (3.3 を参照)。

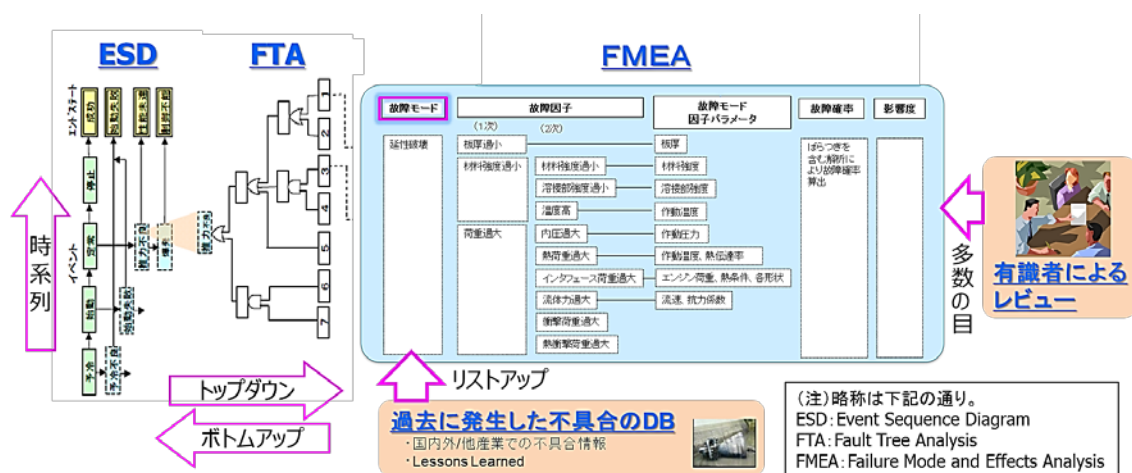


図 15-A-18-4 網羅的故障モード識別手法の概要

## (2) 数値解析・要素試験中心の検証

従来の多数回の試験による信頼性検証は供試体数の確保が問題であった。これに対

<sup>4</sup> ESD は PRA で用いられる技法の 1 つで事象の進展を時系列にグラフ表現する図法。ロケットのように状態や構成が時々刻々変化する場合に特に有効な技法。類似の技法に ETA (Event Tree Analysis) があるが、ETA が末広がり (特に一度分岐して別れたパスが再度合流することはない) の記述を強いられるのに対し、ESD は許容する等の柔軟性が確保されたものとなっている。

応するため製造や運用で想定される「ばらつき」に対しては数値解析的に評価し、その数値解析結果の確からしさについて数値解析結果に対する寄与度の大きな因子を特定した上で小規模な試験により検証するアプローチを採ることとした。「ばらつき」に対する評価を行うため、数値解析は確率論的に行う事となる。このような手法として主に構造分野で用いられている、確率論的設計解析手法 PDA (Probabilistic Design Analysis) がある。具体的には、網羅的に識別された故障モードそれぞれに対し、その現象・メカニズムを踏まえたモデルを構築し、そのモデルを構成している因子のばらつきを確率分布として考慮しモンテカルロ法等を用いて統計サンプリングを行う事により、その故障モードの発生確率を評価する。故障モード毎の発生確率が求まれば (1) で作成した故障シナリオに代入することにより PRA と同じ計算方法によりシステム信頼度 ( $=1 - \text{システム故障確率}$ ) を算出することが可能となる。

これらの評価結果について、故障モード毎の発生確率が許容値を上回るような大きな確率となっている場合には、設計や運用条件を見直す等のフィードバックを行うことにより効率的に信頼性を作り込むことが可能となる。

しかし、上記のような数値解析による信頼性評価においては用いているモデルが正しければその結果は信用できるものとなるが、もし、そうではなかった場合、試験時に不具合が発生することが避けられないだけでなく、数値解析の結果が間違った設計結果を導出する等の有害な作用を及ぼす場合も考えられる。そのため、このような物理／数学モデルベースの設計解析手法においては、用いられるモデルや評価式は十分な試験データに裏打ちされたものであることが前提となる。しかし、実際の開発においては新規エンジンの開発が過去の実績の範囲内で行われることはほとんどなく、設計段階において十分に妥当性確認されたモデルの存在を前提とすることは事実上困難である。

このような“モデルの妥当性問題”に対しては、モデルの不確かさを定量的に把握した上で、それが全体設計に与える影響をマネジメントしつつ開発を行う工学的アプローチを構築することにより対応することとした[2]。具体的には、モデルの不確かさを定量化する手法として計測分野で用いられている不確かさ定量化手法を参考にモデルの不確かさを“モデルの精度”と“その精度評価のサンプル数（妥当性確認試験の実績数）”で表し、これを考慮した信頼度評価を行うこととした (図 15-A-18-5)。これによりモデルベースの信頼度評価結果は従来の PDA による 1 点の数値 (点推定) ではなく区間 (区間推定) で表されることとなる。これらの評価が設計フェーズでできるようになることで、信頼度の区間推定の幅に対し感度の高い故障モードやその因子の絞り込みが可能となり、設計信頼度の推定精度を上げる (= 区間推定の幅を狭める) ための効率的な信頼性試験計画を立案することが可能となる。



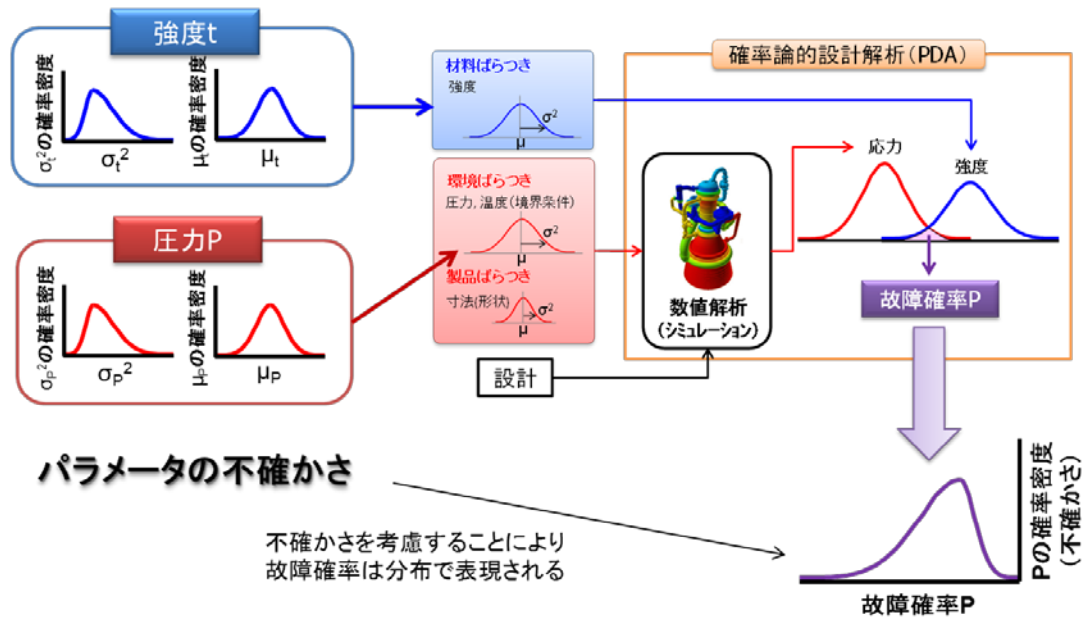


図 15-A-18-5 モデルの不確かさを考慮した PDA

### 3.3. 解決のための着眼点、手法・ツール等

3.2. (1) で述べたような多数の視点で故障シナリオや故障モードを整合をとりながら識別・整理することは手作業や既存ツールでは非常に困難を極めるため、実行環境として支援システムの「高信頼性開発マネジメントシステム “SQRAM” (System of Quantitative Risk Assessment and Management)」を整備した (図 15-A-18-6)。SQRAM は主に開発者が自分の PC で使用することを想定したフロントエンドの解析ツール「高信頼設計支援ツール “SQRAM-leaf”」と、信頼性データ等 (過去の不適合情報や教訓情報等) を蓄積し提供するデータベース「高信頼性開発情報基盤 “SQRAM-ROOT”」および統計的データ解析や不確かさ定量評価を行う「数理統計解析ツール “SQRAM-STAT”」の 3 つの要素から構成されている。SQRAM-leaf は、FMEA 作成/編集、故障シナリオ (FTA/ESD) 作成/編集、最小カット集合/リスク指標計算、信頼度配分/システム信頼度積算の機能を有し、これらの作業を一貫して効率的に実行する機能を提供する。これらの作業は開発プロセスを通して繰り返し実行されるが、その際に重要なことは、過去や進行中の開発で発生した不適合やそれに対してとった設計上の対処を漏れ・抜けなく設計に反映することと、解析に使用するデータの品質を確保することである。SQRAM-STAT はモンテカルロ法等を用いた統計サンプリングや不確かさ定量評価解析および、設計感度解析等を行う事により故障モードの評価および効果的・効率的な設計修正/試験計画の立案を支援する。また、SQRAM-ROOT は開発プロセスを通してこれらのデータを管理するプラットフォームを提供し、SQRAM-leaf や STAT とシームレスに連携することでモデルベースの開発プロセスを全フェーズにわたって支援する。



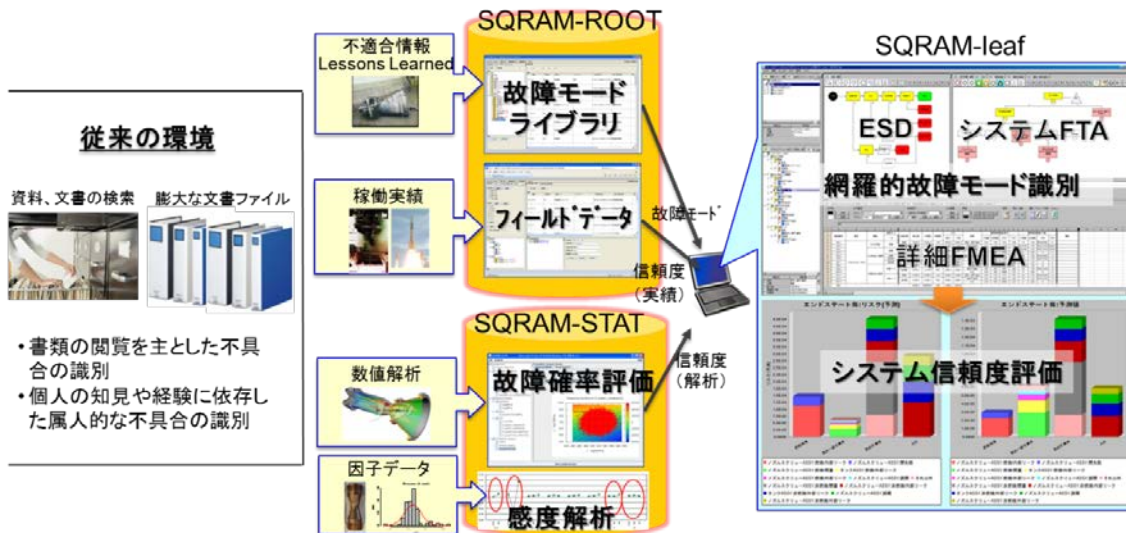


図 15-A-18-6 高信頼性開発マネジメントシステム “SQRAM” の概要

## 4. 取り組みの実施、及び実施上の問題、対策・工夫

### 4.1. 計画、準備

信頼性確保にかかわる活動は、ともすると設計とは一線引いた独立性が確保された組織（例えば品質保証を担当する組織）が実施しがちであるが、「3. 対象システムと適用技術・手法」に述べたような作業は設計作業そのものであるため、エンジン設計の専門家と情報・計算工学技術の専門家が一体となったチームを組み、LE-X エンジンの設計・製造委託先である三菱重工業株式会社とともに実施する体制が取られた。

活動の計画としては、既述の通り、モデルベースの信頼性評価技術自体がまだ確立されたものではないため、LE-X エンジンは従来ながらの試作試験プロセスで設計・開発を進めることとし、これと並行する形で新しい手法の構築・試行するアプローチを採ることとした。これは LE-X 技術実証活動のリスクマネジメントの観点からはやむを得ないアプローチであるが、信頼性評価技術の実証としては効果を実績で評価できないという点で非常に悩ましい。大規模システムにおける開発手法に関わる技術実証の難しいところである。

### 4.2. 実施（具体的取り組み内容、活動）

実施した作業フロー図を図 15-A-18-7 に示す。作業としては、まず、これまでの日本のロケットエンジン開発・運用における不具合事例の整理と Lessons Learned の整理から着手した。また、国内の事例だけでなく、米国スペースシャトル主エンジンの不具合事例等、他国・他産業における事例も可能な限り集めることとした。これらの約 1000 件以上のデータを分析し、エンジンのコンポーネントに発生しうる故障モードを定義し、それぞれの不具合事例／Lessons Learned を故障モードで紐付けることにより故障モードライブラリを体系的に整理した。

上記作業を行っている間に LE-X エンジンの基本設計案ができあがったため、次に、この基本設計案に対し 3.2. (1) で述べた故障シナリオ解析／FMEA を実施し故障モードの網羅的な識別を行った。FMEA に対しては、先に整理した故障モードライブラリを用いてこれまでに存在が認知されている故障モードの漏れ抜けの防止を図った。これらの手法の結果として、以下が得られた。

- ・ 従来の FMEA における故障モードの識別数に比べると設計初期段階にも関わらず 1.5 倍以上の故障モード数を識別することができた。今回新たに識別された故障モードを見てみると従来の FMEA では作成時にエキスパートジャッジによりロケットエンジンでは発生しないと判断され記載されていないものが殆どと考えられるが、中には考慮されてしかるべき故障モードもあった。
- ・ 故障モードライブラリを用いることで設計者が FMEA から過去の不具合事例とその際にとられた設計対処等を容易に参照することが可能となり、これまで得た知見を新規エンジン設計に結びつけ、より開発の確実化・効率化を図るスパイラルアップ効果が確認されている。

次に、識別された故障モードそれぞれに対し、数値解析によりその発生確率を評価することとした。しかし、現実的に時間やリソースに限りのあるプロジェクト活動において数十～数百件程度の故障モードの全てを詳細・高精度な数値解析で、しかも確率論的に評価することは難しい。そのため、故障モードそれぞれに対して定量的な評価を実施する前に定性的な評価を行い、それに基づいて故障モード毎の定量評価方針を決めていくこととした。具体的には、故障モード毎にその現象・メカニズムの把握度合や設計基準の有無（ある場合には、その基準の実績）およびこれまで設計で使用してきている評価ツール・手法の実績等を評価し、これまでの手法でも十分に信頼性を確保できていると考えられる故障モードについては PDA によらずとも良いものとした。また、製造工程の品質管理や検査により除去が可能と判断した故障モードについては工程設計への要求とすることを前提に評価対象外とすることとした。これらのスクリーニングを行った上で故障モードに対して故障確率を評価した作業の結果、以下の知見が得られた。

- ・ システム全体の故障確率に対し寄与度の大きな故障モードは数十～数百の故障モードのうち高々 10 件程度であった。

これらの寄与度の大きな故障モードを重要故障モードと識別し、重点的に発生確率や発生時の影響を低減する対処を検討するため、感度・寄与度解析により故障現象・メカニズムにおける支配因子の把握を行った。一般的に 1 つの故障現象・メカニズムに関連する因子は数十に及ぶが、支配的な因子は高々数個に絞られることが多く、ほとんどの重要故障モードで支配因子として浮かび上がってきたのは「解析モデルの精度」や「材料特性値のばらつき」であった。これらの分析結果から、何の因子をどの程度改善すれば良いかを把握し、合理的なリスク低減計画を立案することができた。

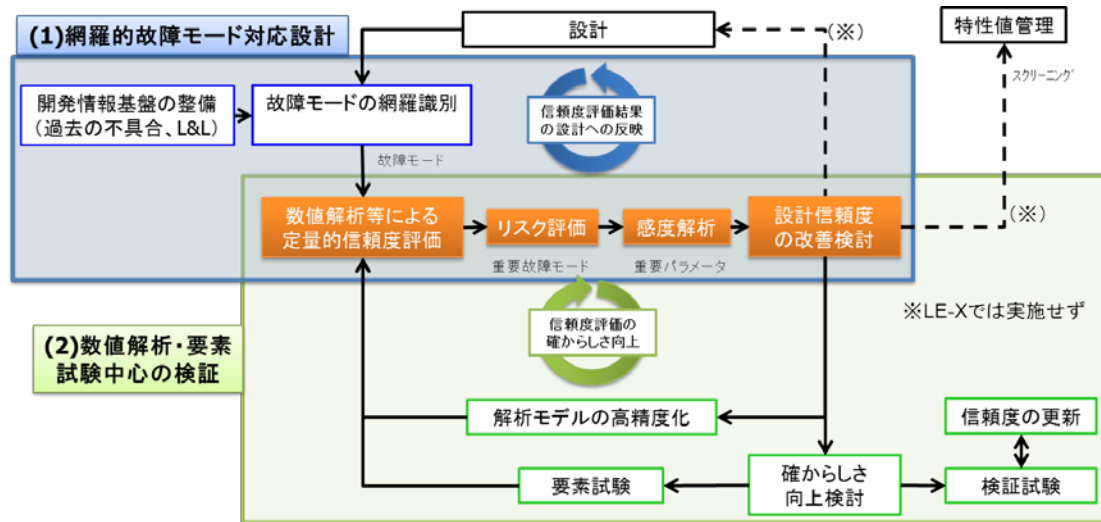


図 15-A-18-7 モデルベースの信頼性設計・検証プロセスの作業フロー

次に、モデルベースで求めた信頼度の不確かさを評価した。例えば、ある故障モードでは故障確率の期待値が  $10^{-5}$  のオーダーであるのに対し 95%信頼水準値は  $10^{-1}$  のオーダーとなり、無視できない不確かさを有していた。これらの不確かさの要因を感度解析により分析し、支配的な因子を把握した結果、支配因子として共通的に浮かび上がってきたのは「解析モデル」及び「環境条件」の根拠データ数の不足からくる不確かさであった<sup>5</sup>。これらの分析結果から、信頼度の不確かさを低減するために必要な解析モデル精度や環境条件根拠データ数の積み増し試験とその回数を検討し、試験計画の立案を行った。その結果、従来のように試験のみで信頼性を検証するのではなくモデルベースで評価した結果の不確かさを試験で低減することにより信頼性を検証するアプローチとすることで、従来の開発プロセスに比べて試験規模は相当の効率化が可能となるという試算結果が得られた。特にこの効果は信頼度要求がこれまで以上に高い場合に顕著であり、例えば、信頼度要求値  $R_{req}=0.99983$  という従来よりも1桁以上高いエンジン信頼度要求（ロケットシステムの信頼度を0.999と仮定した場合にロケットエンジンに想定される信頼度配分值）が課された場合、従来の手法ではエンジン燃焼試験回数が5,000回以上必要と試算されるのに対し、本手法では可能な限り要素試験レベルでの検証を試みるため材料・要素試験数は膨大となるが高価なエンジン燃焼試験回数が少数となる。材料・要素試験とサブスケール試験<sup>6</sup>はエンジン試験に比べれば単価が低いため、試験に要するコストで見ると大幅に安くすることができることになる（図 15-A-18-8）。

<sup>5</sup> 本取り組みでは解析精度や環境条件（例えば燃焼温度）は分布として与えられる。例えばこれらの分布が正規分布の場合、分布の母数は平均値  $\mu$  と分散  $\sigma^2$  であり、これらの値は試験等で計測されたデータに基づいて推定される。推定に用いるデータ数が多ければ平均値  $\mu$  と分散  $\sigma^2$  の推定値は確からしいものとなるが、データ数が少なければその推定値は不確かなものとなる。これが信頼度の推定を不確かなものとしている要因となる

<sup>6</sup> 縮尺形状、または実機大サイズの特定位部のみ抜き出した試験供試体を用いて、ある特定の物理事象について相似則が成り立つような条件で行われる試験

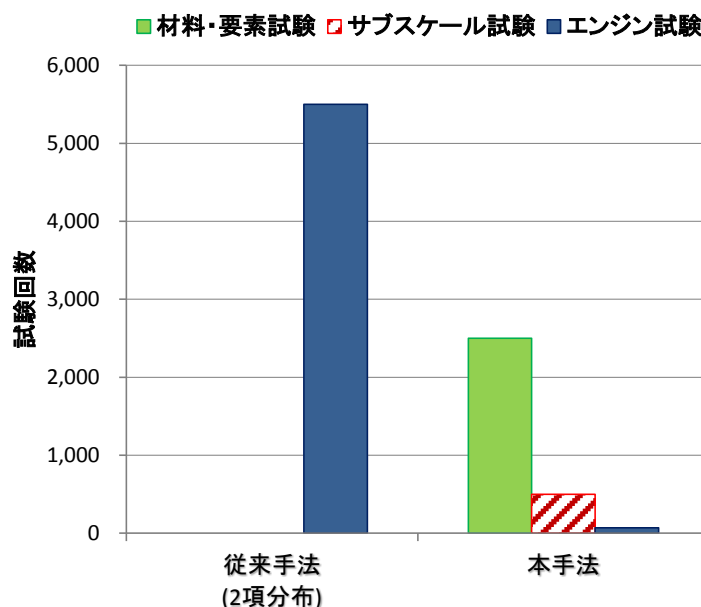


図 15-A-18-8 信頼性試験規模の試算結果[3]

## 5. 達成度の評価、取り組みの結果

「開発後期段階や運用段階での不具合を低減させるために、開発初期段階で故障モードを網羅的に識別・対処し、運用や部品などのばらつきも考慮した新たな設計手法の構築」並びに「高い信頼性を確保するために、開発段階で充分なばらつきを確認、故障モード毎の検証を大規模な実証試験によらず効率的に実施する方法の構築」という活動の目標に対し「網羅的故障モード識別・対応設計」および「数値解析・要素試験による検証」というアプローチにより解決することを試みた。これらのアプローチの根幹をなす技術はシステム信頼度を論理モデルと物理モデルを上手く組み合わせて設計パラメータ（形状や環境条件）からなるモデルとして表現し、分析や定量評価するモデルベースの信頼性評価技術である。

これらの技術をベースとして構築した網羅的故障モード識別・対応設計手法（3.2.（1））を LE-X 技術実証活動において適用した結果、故障モード識別数は従来手法に比べて 1.5 倍以上を識別することができた。今回新たに識別された故障モードを見てみると従来の FMEA では作成時にエキスパートジャッジによりロケットエンジンでは発生しないと判断され記載されていないものが殆どと考えられるが、中には考慮されてしかるべき故障モードもある等、時系列・トップダウン・ボトムアップ・リストアップ・レビューという多様な視点で故障モード識別の網羅性向上を図る方法は非常に有効であった。これにより、識別された故障モードに対して設計で対処（不適合未然防止）を行うことが可能となり、確実に手戻り量が削減されることが期待できる。

同様に、構築した数値解析・要素試験による検証手法（3.2.（2））を LE-X 技術実証活動において適用した結果、従来の試験のみで信頼性を検証する手法と比べて信頼性試験の規模

(コスト)は大幅に安くできるという試算結果を得た。ただし、実際には現状ではモデル自体が存在しない故障モードも少なからず存在することも判明しており、これらの故障モードについては現象・メカニズムを把握しモデル化する活動が必要となるが、これらのモデル化に要するコストを考慮しても従来手法よりも費用は安くできると試算されており、当初の課題に対してモデルベースの信頼性設計・検証手法は有効なアプローチであることが確認された。

## 6. 考察と今後の取り組み

3.1 で述べたように、ロケットエンジンの動作環境は非常に過酷で物理現象は複雑であるが、機能としてはそれほど複雑ではない。そのため、今回の取り組みにおいては主に物理設計・検証の比重が大きかったが、情報処理システムの信頼性・安全性の向上にとっても全く無関係ということではなく、むしろ今後大きく意識せざるを得ない状況になっていくと考えている。

特に制御系の組込みシステムについてはハードウェアとソフトウェアを切り離して考えられない状況になってきており、システムの高信頼化を考える上ではハードウェアとソフトウェアを包含した「システムの視点」をもつ必要がある。例えば、エンジンコントローラーのような組込みシステムはプラントの動特性を表す物理モデルに基づき設計されることが多いが、プラントの動特性がどの程度ばらつき得るのか、さらにはプラント動特性モデルのもつ不確定性はどの程度あるのかといった事がエンジンコントローラーの信頼性や安全性に大きく関わってくるものとなる。

モデルベースの信頼性評価技術は、今後、ロケットや衛星の搭載機器や宇宙機システムそのものへ適用範囲を拡げて行くことを検討している。その中で、今回の取り組みで構築した手法と、今回の取り組みの中では手を付けられなかった機能設計やシステム設計に対するモデルベース手法（SysML や 1D-CAE ツール等）を融合させ、システム開発のみならず運用まで包含するようなモデルベースの信頼性評価技術の構築に取り組んでいきたい。

参考文献

- [1] 沖田耕一：新版信頼性ハンドブック 第V部 E-3 ロケットの信頼性向上策、日本信頼性学会（編）、一般財団法人日本科学技術連盟、2014
- [2] 田口元ほか：不確かさをを用いた液体ロケットエンジンの新しい信頼性設計・評価プロセス、計算工学講演会論文集 Vol.19、2014
- [3] 中島章ほか：液体ロケットエンジンにおける信頼度検証に必要な試験規模算出の試行、一般財団法人日本科学技術連盟 第43回信頼性・保全性シンポジウム Session10-1、2013
- [4] NASA : Probabilistic Risk Assessment Procedure Guide for NASA Managers and Practitioners, NASA/SP-2011-3421 2nd Edition, 2011

掲載されている会社名・製品名などは、各社の登録商標または商標です。

独立行政法人情報処理推進機構 技術本部 ソフトウェア高信頼化センター (IPA/SEC)