宇宙開発における信頼性管理

市田　嵩

1. はじめに

システムや機器の開発，製造に関する積極的な信頼性管理の方法が議論されはじめたのは米国においては1950年代のはじめからであるが，多くの試行錯誤を経て1963年ごろ一応の体系づけができ，米軍の「信頼性プログラム要求事項(MIL-R-27542，現在のMIL-STD-785の前身)とか，NASAの「信頼性プログラム規定(NPC250-1，現在のNHB・5300・4(1A)の前身)がガイドラインとして，また，実際に軍やNASAとの製造請負契約の条項として使用されるようになった．これらは，宇宙開発においては，各種の人工衛星，アポロ，惑星探査，スペース・ラブなどのプログラムに実施され発展をみたが，宇宙開発以外の分野でも多くの成果が得られている．

一方，わが国では1950年代末ごろから一部識者の間で信頼性の検討がはじめられ，その後の技術革新，高度成長にともなって，その重要性が認識されはじめ，信頼性の技術が一般産業界に広く取り入れられるようになった．アメリカの軍・宇宙関係の規格やハンドブックは大いに参考にされているが，実際に導入された分野は，鉄道，放送，通信，航空，輸送機器，プラント，耐久消費財などそれぞれの企業努力によるもので，主として個別的に有効と考えられる技術・手法が導入定着されたものと考えられる．ここに，日本的な信頼性に対する考え方や方法が形成されつつあることはここ数年の「信頼性・保全性シンポジウム」[1]などに発表された多くの企業の実施例に見られるところである．わが国の宇宙開発も当然，このような国内の産業基盤の上に成立するものであるが，複雑大規模のシステム開発であり，いわゆるプロジェクト・タイプの開発の典型であり，組織的，体系的な管理がぜひ必要で，その一環として信頼性管理の必要性のもっとも高い分野であろう．次節以下にも述べるような特殊な条件もあるが，宇宙開発で実施された信頼性管理の考え方や手順は，ほかの分野にも参考となると思われる．すなわち，新しい試みが特殊なシチュエーションの下ではじめられても，それが，むしろstate of the artを向上させる引金にもなり，効果が認められると，一般に応用されるようにもなるものと思われる．ここに，主として実用衛星の開発・打ち上げで実施されている信頼性管理について述べ，一般の参考に供したい．

2. 各国の人工衛星打ち上げ実績[2]

1975年7月に米国とソ連の共同のアポロ・ソユーズ試験計画(ASTP)が終わり，最近では米国の火星探査機(バイキング1号)に関する報道が行なわれている．また1980年代の再使用可能の宇宙輸送システムをめざして計画が進められている．このような月・惑星探査機や有人宇宙船の打ち上げ

© 日本オペレーションズ・リサーチ学会．無断複写・複製・転載を禁ず．

国は米国とソ連にかぎられている．

一方，人工衛星を自国で開発したロケットにより打ち上げた国は仏，日，英，中の諸国である．仏は1965年以来ディアマンA，BおよびB-P4などのロケットで1974年までに6個（ほかに独と共同で2個）の人工衛星を独自に打ち上げて成功しているが，1971年に1回，1973年に2回の失敗を経験している．また，英国は1971年にブラックアローにより技術開発衛星を打ち上げて成功したが，それにつづく計画は中止されている．このほかに欧州ロケット開発機構（ELDO）がヨーロッパ7カ国参加のもとに1962年に設立され，ヨーロッパⅠ号計画，Ⅱ号計画およびⅢ号計画を進めてきたが，Ⅰ号計画は3回の打ち上げにすべて失敗し，Ⅱ号計画も1971年打ち上げに失敗し，これらによりⅡ，Ⅲ号計画は放棄されるにいたり，現在は欧州宇宙研究機構(ESRO)と合併され，1975年より新しい機関の欧州宇宙機関（ESA）の1部門となっている．

人工衛星を開発し，あるいはこれを他国に製作を発注し，米国またはソ連に打ち上げを依頼した国としては，英，仏，カナダ，伊，独，豪，オランダ，スペイン，印度の諸国のほか，国際的なものとして仏・独共同，NATO，ESRO(現ESA) INTELSAT などがある．

米国におけるロケット打ち上げの実績は，1958～1973年末までに747の打ち上げに対し，成功は636回で成功率は約85%であるが，1963年ごろからは約90%を上下している．もちろん，この間に人工衛星の重量も増大し，ロケットも改修が重ねられている．人工衛星打ち上げ初期の成功率は，アトラス・アジーナは30回で約60%，ソー・アジーナは60回で約70%，スカウトは24回で約60%となっている．

3. 宇宙開発における信頼性設計思想

宇宙開発関係で，信頼性に関する議論でよく出てくる言葉がたくさんある．これらをいくつか紹介すると，おのずから，そこに宇宙開発における信頼性の考え方があらわれてくるように思われる．これらはかならずしも信頼性用語ではなく，ほかの分野でもよく使われていることは読んでいただけばおわかりのことと思う．

(1) state of the art：現在の技術レベルのことであるが，現在の知識，技術，技能，部品，材料などで達し得る最高の技術能力の意味に用いられ，開発しようとしているシステムなりそのサブ・システムあるいはコンポーネントに state of the art を超えるものがあるかないか，もしあれば，どこか，というような検討が開発の初期に十分行なわれる必要がある．

(2) feasibility study：feasibility は実現の可能性と言ってよいであろう．しかし，これは期間，予算，state of the art などの現実の条件の下での可能性であって，原理的にできるできないの問題だけではない．一般に，経験豊かな技術者やマネジャーほど feasibility について厳格な考え方を持つものである．逆に言えば，経験の少ない人ほど原理的に正しければなんでもできてしまうような錯覚を起こしやすい．feasibility をできるだけ客観的にたしかめることが feasibility study である．開発初期（構想段階または概念段階と言う）での信頼性の仕事も feasibility study に重点がある．

(3) mission profile：ロケットの飛行計画を図表で示し，主要なイベントごとに，その時分，実施するオペレーション，受ける環境のストレス(温度，気圧，振動，衝撃，音響など)を記述したもので，基本設計時にはすでに詳細なものが必要である(あとで変更はありうるとしても)．

(4) reliability program plan（信頼性プログラム計画書）：信頼性プログラムを実行するための計画書である．信頼性プログラムの要求事項についてはあとで述べるが，わが国では言葉の上の問題ではあるが，program と program plan が混同されているように思われる．plan は最初に

© 日本オペレーションズ・リサーチ学会．無断複写・複製・転載を禁ず．

つくられるが，program はミッションが終わるまで終わらない．

(5) conservative design：保守的な設計であるが，これが推奨される．これは，金に糸目をつけず贅沢な設計をすることのように考えている人がいるが，けっしてそのような意味ではない．要するに risk の少ない設計をすることである．たとえば，私が1967年にインテルサットⅢ（通信衛星）プロジェクトへ参加したときは，関係した下請負契約品は電源部であったが，設計方針としてIC（集積回路）や多層プリント基盤は用いないということであった．これらの部品は当時すでにわが国でも実用されはじめていたが，重量，寸法などに問題がないのに好んでそのような新しいものを使用するより，それまでに人工衛星で実績のあるディスクリートなトランジスタおよびその回路を用いることにしたのである．要するに，実証された技術や部品・材料をできるだけ用いて，ミッション達成を第一義として設計を進めてゆくことである．したがって，つぎのような言葉がよく出てくる．

(6) existing hardware：説明の要もないであろう．現在アメリカで，人工衛星打ち上げに使用されているロケットは，スカウト，デルタ，アトラス／センター，タイタン／センター，タイタンⅢC，の5機種であり，これらの原形はいずれも1950年代末から1960年代初頭に開発されたものである（もちろんその後改良，拡張がたびたび行なわれている）．できるだけ既存の物を活用してゆこうということは，システム設計の基本であろう．したがってその方法の1つとして

(7) cluster：たとえば，既存のエンジンを2個用いて従来より大きな推力を得る．

(8) experience retention：経験の維持．世代はつぎつぎと変わってゆく．新人は先輩の経験を踏み台にして新しい開拓を行なわなければならない．短期間に先人の経験を身につけなければならない．先輩の失敗を2度繰り返えしてはならない．方法としては，教育，訓練，データの収集，配布．結局，目新しいことはないが，それらを確実にやっていかなければならない．

(9) redundancy：理論的には，フォン・ノイマン，シャノン，ムーア，といった人々が1950年代に解析法を示していて，今もいろいろのシステムに多用され，理論的な研究も，さらに進められているが，つぎのことが残るのは避けられない．

(10) single failure point：その1カ所(point)が故障すればシステムとして重大な影響を受けるような点を言う．ちょうど，アキレスの腱やジーグフリートの1枚の葉の跡のようなところである．アポロでは冗長設計が徹底的に行なわれたが，一方，この残された single failure point の管理が信頼性の重点管理目標となった．これを設計時点で発見する手法としてつぎの手法がよく用いられる．

(11) FMECA (failure mode, effect, and criticality analyses)：この手法はわが国でも広く利用されるようになった．システムを構成する各コンポーネントや部品について，その故障モードを調べ，それぞれの故障モードによるシステムへの影響を列記し，その重大さを評価し，要すれば対策を記入することである．

(12) trade-off：重量，寸法，消費電力と信頼性との trade-off というようにこの言葉は用いられる．設計審査(後述)の重要なチェック・ポイントである．

(13) compatibility：システムの中のサブシステムやコンポーネントが相互に干渉せず，調和を保ってそれぞれ機能を果たす性質であるが，とくに電磁的な妨害は机上の計算だけでは確認が困難なものである．

(14) idiot proof, fool proof：フール・プルーフ設計．

(15) maintainability：保全性，修理可能な系，機器，部品などに備わる保全の容易さをあらわす

© 日本オペレーションズ・リサーチ学会．無断複写・複製・転載を禁ず．

度合または性質である．よく，信頼性のテキストなどにも保全性の不要なものの例としてロケットや人工衛星があげられているが，実際にはロケット・人工衛星にもぜひ必要な性質である．これらは，工場で組み立てられたあと，各種のシステム試験を受け，分解され輸送され，再び射場で受入試験ののち，サブ・システムごとの試験があり，その後整備塔で全段の組み立ておよびチェック・アウトが行なわれる．この間厳しいスケジュールの中で点検，手入，調整，修理，改修などの作業が繰り返えされるのが現実である．保全性を細分すれば，accessibility (接近性)，モジュール化，取付・取外の容易さ，試験の容易さなどにわけられる．また，広い意味の保全性としては予備機，予備品の問題が重要である．したがって，つぎのような用語が用いられる．

(16) refurbish：とくに，人工衛星の開発では1970年ごろまでは，技術モデル，プロトタイプ，実機(フライト・モデル)と3段階にわけて，それぞれ製作・試験を行なうのが普通であった．プロトタイプについては認定試験(qualification test)を実施し，機能および耐環境性が確認されるが，ストレスは実際に加わると考えられるレベルより6db(2倍)上げるのが標準である．認定試験に合格すれば，そのとおりの設計で新しい実機の製作に移るのである．実際には，スケジュールの都合で認定試験完了前に実機の製造がはじめられることが多いが，最終的には実機のコンフィギュレーションはプロトタイプの認定試験完了時とまったく同じにならなければならない．このプロトタイプは，そのまま保管されたり，博物館に寄付されたりしていたが，最近ではプロトタイプをrefurbish して(劣化のある部品を取り替え，再組立，再調整を行なって)，実機として用いるようになった．これをプロト・フライト・モデルと言う．予備機に用いられたり，1号機として打ち上げられたりする．前にも述べたが，人工衛星の打ち上げ実績によれば成功率はかならずしも高くないので，実用衛星では予備機を準備することは必要である．

(17) dormancy：人工衛星を長期間保存したのちに打ち上げることも有りうるし，また，ロケットは数機同時につくっておき，順次使用することもある．地上の打ち上げ設備も，わが国では打ち上げ時期が年2回であるので dormancy(休眠)期間がある．これらの休止期間中の処置とか取扱いについて，信頼性，経済性の面からの検討がされている．

4. システム開発手順

システム開発において，段階(phase)を定め，段階ごとに仕事の区切りをつけてプロジェクトを進めていくことが大切で，その大要を示したものに米空軍の AFR375-1 "System Program Management" とか NASA の NHB7121-2 "Phased Project Planning" などよく知られている．宇宙開発事業団でも昭和46年に「システム開発手順」を人工衛星打ち上げ用大型ロケットの開発のために定めているが，人工衛星開発に対してもそれに準じた手順で進められ，昭和50年9月人工衛星「きく」，ついで51年3月「うめ」を打ち上げた．以下にこれらのプロジェクトの各段階の主要作業と信頼性管理との関係の概要を記しておく[3]．

4.1 概念段階(構想段階)

(1) 目的

特定のミッションを満足し，性能・コスト・スケジュール上からみて可能性ある複数個のシステム概念を選定する．

(2) 主要作業内容

a．環境の制約条件の調査解析を行なう．

b．目的とするミッションの特性解析を行なう．

c．システムの特性解析を行なう．

d．各サブシステムの概略機能性能の解析を行なう．

e．主要コンポーネントなどの可能性の検討を行なう．

© 日本オペレーションズ・リサーチ学会．無断複写・複製・転載を禁ず．

f．開発方法，コンポーネント構成など数種の概念(内容，期間，経費など)の設定を行なう．

(3) 信頼性関連作業

上記 c, e 項に関連して feasibility study を行なう．

4.2 決定段階

(1) 目的

システム概念(数種)をさらに1つのシステムとし，設計要求仕様書を固める．

(2) 主要作業内容

a．選定されたシステム概念について代替分析を行ない，その結果適当なものを選び，それぞれについて予備設計を行なう．

b．これにもとづき最適のシステムを選定し，基本設計要求仕様を決定する．

c．これにもとづいて提出されたプロポーザルを検討し，メーカーを決定する．

(3) 信頼性関連作業

メーカーにプロポーザルを提出させるための信頼性のガイドライン(契約締結後は要求事項となる)作成およびこれにしたがって提出されたプロポーザルの中の信頼性プログラム計画書の審査を行なう．プロポーザルの主要な内容は，(i) 全般の管理体制 (ii) サブシステムのプロジェクト管理組織 (iii) 管理のための情報と統制の体制 (iv) 設備・施設 (v) 主要職員の経歴

これらのプロジェクトマネジメントの下のプログラム計画書としては (i)設計・開発計画 (ii) 試験計画 (iii) 製造計画 (iv) 品質プログラム計画 (v) 信頼性プログラム計画 (vi) コンフィギュレーション管理計画 (vii) 物品資材購入計画などである．

信頼性のガイドライン(要求事項)の主要項目はつぎのようなものである．メーカーはこの項目につきプロジェクト特有の問題を検討し tailoring してプログラム計画書を作成するのである．

(i) 総則：適用範囲・このプロジェクトにおけるほかの要求事項との関連・信頼性プログラム文書・用語・引用文書．

(ii) 信頼性プログラムマネジメント：組織・信頼性プログラム計画書・信頼性プログラム管理・信頼性進捗報告・信頼性訓練・供給業者の管理・支給品質貸与品の管理．

(iii) 信頼性工学：設計仕様書・信頼度予測・FMECA・システムの保全性，および人間エラーの予防・設計審査プログラム・不具合／故障報告および修正・設計手法の標準化・部品・デバイスおよび材料プログラム．

(iv) 試験および信頼性評価：信頼性評価計画・試験・信頼性推定・射場における「最終確認審査」のための信頼性インプット・信頼性評価プログラム審査．

4.3 設計段階

(1) 基本設計要求仕様書にもとづいて，ハードウエア製作のために必要な設計を行なう．

(2) 主要作業内容

a．基本設計を実施し，この結果をもとに詳細設計仕様書を決定する．

b．これにもとづき詳細設計を行なう．

c．これと並行してモック・アップ，技術モデルの製作評価などを行ない，また，主要コンポーネントおよびサブシステムの機能試験・環境試験を実施する．

d．上記 b および c の結果を入れて製作要求仕様書を決定する．

(3) 信頼性関連作業

前段階で設定した信頼性プログラム計画にしたがって，設計仕様書の作成，信頼度配分・予測・FMECAの実施，部品材料プログラムの設定および実施，試験プログラムの計画などがあるが，これらのしめくくりとして「基本設計審査」および「詳細設計審査」を実施して，つぎの段階に進むことが確認される．

4.4 製作・試験段階

(1) 目的

前段階で作成した設計にもとづいてハードウエ

© 日本オペレーションズ・リサーチ学会．無断複写・複製・転載を禁ず．

アを製作する.

(2) 主要作業内容

a. 人工衛星およびロケットについてはプロトタイプ・フライト・モデルの製作，地上設備については，その製作および設置ならびにこれらを用いたサブシステム，システムの機能試験，環境試験の実施・評価を行なう.

b. 必要に応じ設計変更改修を行なう.

(3) 信頼性関連作業

製造プロセスに関する品質保証と密接な関係で進められるが，設計段階で識別された single failure point などの critical な品目（信頼性管理品目）の管理，部品や材料のトレーサビリティの確保，不具合／故障の解析，取得したデータからの予測や FMECA の見とおしが重点となる. プロトタイプに対する認定試験を経てフライト・モデルのサブシステムおよび総合システム試験が行なわれる. 認定試験完了時にコンフィギレーションの確認が行なわれるが，これを FACI(First Article Configuration Inspection)と言う.

この段階で行なう審査は，前の詳細設計審査のあとをうけて，「認定試験後審査」と「納入前審査」が製造工場内で行なわれ，それまでのデータから総合的に判断して最終的に契約品目が契約上の要求条件を満足し，実用しうるもので，受入可能であることが確認される.

これらの契約品目ごとの納入前審査が終わったあと，ロケット，人工衛星，地上設備，追跡管制システム，打ち上げ運用の各プロジェクトごとに，各主要システムが規定された要求条件を満足し，関連するシステム間のインターフェイスも適切で運用可能であることを確認するため,「プロジェクト開発完了審査」が行なわれ，各プロジェクトごとにこの段階が終了する.

4.5 打ち上げ，追跡管制および評価段階

(1) 目的

打ち上げおよび追跡管制を行ない，その結果を検討評価する.

(2) 主要作業内容

a. 衛星およびロケットの射場への輸送・受入検査を行なう.

b. 打ち上げ前の全システムの機能確認を行なう.

c. 打ち上げおよび軌道上衛星機能試験追跡管制の実施を行なう.

d. cの結果の解析と評価を行なう.

(3) 信頼性関連作業

ロケット・人工衛星は射場に送り出す前に完全なものでなければならない. したがって，これまでのそれぞれの段階でつくり込まれた信頼性の確認を行なってきたわけであり，“ship and shoot”が基本的な考え方となっているが，実用衛星打ち上げ用のNロケットは重量90ton，全長30mを超えるものであり，中に多くの精密な搭載機器を含んでいるので，分解して輸送し，射場で受入れ試験後，組み立て作業に移ることになる. また，地上の電波設備との整合試験はロケット・人工衛星ともに必要な事項で，打ち上げのカウント・ダウンに入るまでの整備期間に数ヵ月を要する. ロケットに含まれる部品は，複合部品のレベルで勘定しても10万点を超えるものであり，整備期間中に偶発故障・劣化故障・人為故障なども発生するが，台風，落雷などの自然現象に対処しなければならない. 一方スケジュールは非常に厳しく，この間の品質保証は時々刻々の変化に対応できる visibility の高いもので，かつ，タイムリーな決断ができるものでなければならない.

この段階のはじめにシステム全体に対し「打ち上げ移行前審査」が行なわれ，各プロジェクト開発成果の総合確認が行なわれ，プロジェクト間のインター・フェイスなどについて審査し，全体システムとして運用可能であり，射場整備作業に移行できることが確認される. ついで，射場における「予備試験完了後審査」ののち,「射場における最終確認審査」が整備期間中約3回にわかれて行なわれる. 最終回において各主要システムの射場

© 日本オペレーションズ・リサーチ学会. 無断複写・複製・転載を禁ず.

整備作業が規定どおり完了し，打ち上げうる状態にあることが確認され，その翌日からカウント・ダウンに入ることになる．整備期間中の信頼性活動は，信頼性管理品目の現状の把握，履歴記録の維持，不具合／故障に対する調査・解析・修正処置，各審査への参加と指摘事項のフォロー・アップなどである．また品質保証活動としては，計測管理・技術文書管理・材料部品管理・清浄管理・特殊工程管理・非打ち上げ品目管理・不具合管理などが総合的に行なわれる．

人工衛星が軌道に投入され，追跡および初期運用がはじめられたあとは，人工衛星のハウスキーピングデータや運用データから信頼性解析を行ない，部品・コンポーネントの信頼性データを収集する．また，「飛行後審査」を行なって，打ち上げ結果の評価およびそれにもとづくプログラム，プロジェクト成果の評価を行ない，次回打ち上げまでのアクション・アイテム，つぎのプログラム／プロジェクトに対するアクション・アイテムを確認する．

おわりに

この稿をまとめるにあたり，ロケット・人工衛星・地上設備などの概要，また，種々の信頼性手法の例示などの下書きを割愛することにした．これは，紙面の都合であるが，長期にわたる信頼性プログラムの骨格やその背後にある考え方を伝えるほうが，断片的なお話をするより重要と感じたからである．このような記述では，いわゆる生野菜の新鮮さは失なわれるかもしれないが，わが国の信頼性に関するアプローチでもっとも特色のある面について述べたつもりである．

また，ここではまったく触れなかったが，それぞれのプロジェクトの段階ごとの信頼性管理とは別に，たとえば高信頼性部品の開発，信頼性技術の研究，職員の信頼性教育やモーティベーションのような恒常的一般的な問題もあるが，これらは多く議論されているし，今後も報告の機会を別の場で得られると思う．

よく，信頼性管理は技術者・科学者の意欲を削ぐものであるとか，信頼性管理は金がかかるとか，否定的な意見を聞くことがあるが，要するに信頼性管理は risk control であるので，信頼性管理の努力により，将来の risk が軽減でき，その見返えりがあると考えられる方法を自ら定めて実行すべきもので，システムの有効性を高めるものであるとの多くの人の理解を得て実行が可能となり，効果も得られるものと思われる．この小文がお役に立てば幸いである．

参考文献

1) “信頼性・保全性シンポジウム報文集 I～VI” 日科技連．1971～1976.

2) 市田，後川 “宇宙開発における信頼性技術” 信学誌 Vol. 59 No. 4 (p. 433) (昭51－4).

3) 市田 “人工衛星とロケットシステムの信頼性設計” 計測自動制御学会シンポジウム資料 (昭和51-1-27).

いちだ・たかし 1920年生 三菱電機 電子計画部製品保証専門部長

専門：製品保証(product integrity)

1945年早稲田大学理工学部卒，電波研究所にて周波数標準の維持・改善，三菱電機にて品質管理・システム設計・信頼性等に従事，宇宙開発事業団信頼性・安全管理部長を経て現在に至る．電子通信学会・品質管理学会・OR学会会員．

メッシュ・データ特集号の原稿募集

来年の1月～3月ごろに，メッシュ・データの特集号を企画しています．つきましては，この特集号にご執筆くださる方を広く募集します．

アブストラクト(長さ，形式など自由)を8月末日までに，編集長宛てにお送りください．ご執筆をお願いすることがきまった場合，その原稿締切は11月末になるかと思います．なお，他薦も大いに歓迎いたしますので，編集長宛てに適切な執筆者をご推薦くださるようお願いいたします．

© 日本オペレーションズ・リサーチ学会．無断複写・複製・転載を禁ず．