Space Shuttle Probabilistic Risk Assessment
スペース・シャトルの確率論的リスク評価

Joseph R. Fragola
Advanced Technology Division, Science Applications International Corporation
New York, NY USA

概要

スペース・シャトル・システムの確率論的リスク評価（PRA）が最近になってようやく完了した。この1年間に及ぶ努力はシャトルに対しリスク技術を7年間適用したひとつの成果を示すものである。このシャトルの運用リスクの評価に用いた基本的な方法はシナリオベースであり、また、シャトルシステム設計の防御的かつ緩和的特徴によって抑止されたり方向が変えられたりするような想定される開始事象の潜在的進歩を定量的に評価することから成っている。さらに、その方法はミッション・リスクの“生きた”モデルをNASAに提供するべく将来のシャトル飛行および試験のデータを現行ベースで組み込むことを許すところの統計的更新手続きを含むものである。そのリスク評価データベースはすべてのシャトル飛行関連の経過、即ち、実際の飛行中の不具合や異常と同様に飛行不具合の前兆となるものと試験時の異常をも含んでいる。本論文は研究結果又は遭遇した困難への考察と組み込まれた解決策を示すものである。さらにシャトルシステムの意思決定に向けての本研究の応用についても触れるであろう。

1.0 序言

定量的リスク評価は新しいものではない。このルーツは少なくとも17世紀にまで戻るもので、この時代には安全通行頻度と死亡統計が集められ、解析されて、輸送および生命保険産業の基礎をなしていた。しかし、古代に溯る定性的リスク評価に比べればつい最近のことである[1]。さらに、その開発の後でさえも、PRAは、「事実上無制限の同一条件の下での観察のシーケンス」[2]が存在する保険業界等のたった二、三の分野に限られていた。この制約は狭義の確率の定義が論拠とした「…は同じ事象が繰り返し出現するもの、又は同時に非常に多数の同一の要素が関係するものにのみ適用できる[2]」に基づいている。この狭い見解からは重要な意思決定課題である「戦争で勝利する確率というようなものは同じような事象が何度も繰り返されるわけではないので我々の理論が出る幕はない。」[2]ということになる。

上記の視点は「主観確率」の概念を本質的に排斥したもので今世紀の中頃まで支配的

な理論的統計的視点であった。事実、今日まで続く頻度屋対ベイジアンの論争の根として残っている。今世紀の初めまでこの論争は非常に過熱したもので公開の戦争のようなものであった。一方はケインズ[3]や、何人かの論理屋や、物理学者に特に擁護された主観主義者達であり、他方は統計屋の大部分を代表する頻度主義者達である。ラムゼイ[4]は2者が主として語義論的であると仮定することによって相違の橋渡しを試みた。しかし、デフェネッチ[5]が確率の定義を明確にして、帰納的理由付けの概念のために合理的な基礎を提供する「交換性」の概念を導入するまで、重大な理論的問題が残っていた。最近の研究成果[6]、[7]はこの代替的確率的視点と意思決定者によって支配的に直面する型の仮説との間の関係に光をあてた。特に、定量的予測において明確に不確かさを取り扱う重要な役割が、次に示すように、明確に識別された。

「定量的予測は常にある程度の不確かさ内の予測であるに違いない。；この程度とは色々な場合で異なっているだろうが、何らかの役に立つものであるべき一つの決まりとして、それ｛定量的予測｝はその程度を明確に述べなければならない。」[6]

このように、一つの予測は常に異なった量の変動に対する相対確率の言明であり、より容易く経験から学ぶ常識的考えと適合するものである。何故なら、新しい観察が行われたり、新証拠が伝えられた時に確信の度合いが変わるという概念というものを予測は許しているからである。

2.0 NASAにおける初期の適用

定量的リスク評価の理論的基礎はNASAの誕生に、そしてアポロ計画の始まり時に間に合いしっかり築かれた。しかるに、NASAは、初期において関心を持った証拠があるにも拘わらず、プログラム途中で定量的リスクアプローチを避けてしまった。事実、月プログラムをケネデイが発表した後数ヶ月にしてNASAの設立者たちは議論の末、アポロミッションには定量的な数値目標を持つべきであるとの結論に達し、ミッション遂行に対しては百分の一のリスクを許容し、乗組員の安全については千分の一のリスクを許容することを決めた。彼らは、故障の目標を設定するだけでは不十分であり、むしろ、「潜在的故障とそれらのリスクの識別が成功する設計つまりミッションの成功に本質的である」[8]ことを理解した。さらにNASAマネジャー達は「リスクが決定測定の基礎的な共通分母である」[8]ということも知った。この初期の理由付が、すべてのアポロ要素に対する定量的リスク・モデルの開発を導いた。この開発はプログラムの進行と共に進められ、1960年代の半ばまでにモデルやモデル化の試みは少なくともアポロ司令およびサービスモジュール、[9]ルナモジュール、[10]そしてサターンⅤロケット[11]について存在した。

これらのツールが利用でき、定量的にリスクを扱う必要性の認識があったにもかかわらず、NASAはプログラムが進行するにつれて定量的に扱うことを疎んじ、結局5項目の要素に基づいて意思決定を行うことに退却してしまった。

（1） 最後の設計審査の後組み込まれたすべての重要な装置改修、およびすべての未承認事項に対し予想される修正内容、の審査。
（2） それ自体の故障が生命の喪失やロケットの失敗につながるいかなるシステム要素（単一故障点）の認定状況の識別および決定。
（3） すべてのロケットおよび特別システム試験結果の審査。
（4） すべての重要な故障およびその後の修正措置の審査。
（5） 未解決問題、修正措置の計画、および完了予定日の審査。

単一故障点の識別は専ら故障モードおよび影響解析（FMEA）の性能によって成し遂げられた。そのような解析を通じて、系のおのおのの構成要素が潜在的にどのような故障モードをもっており、その故障の結果がどのサブシステムに影響し、それがどのシステムにおよび、ロケットからミッションそして乗組員にどのように影響するかが審査された。このボトムアップ解析は個々の構成要素がミッションをどの程度リスクのあるものにするか識別するために意図されたものである。その解析は既存の設計内で組み込まれうる潜在的なアプローチをも指示したし、あるいは別の方法としてその故障モードを除去するか、頻度を減じて許容できるほどにリスクを低減するものをも示した。このようにFMEAはリスク解析の予期される姿として示された。取り除くことも緩和されることもできない単一故障は何故そのようなままなのかの理由付けとともに設計を通じて集められ、これら全ての識別された単一点故障(SPF)リストが重要品目表（CIL）にまとめられた。このリストはその品目が開発、製造、組み立て、試験において特別な配慮を受けることを促した。FMEAとこれに関連したCILは先述の意思決定5要素の重要な決定物であったから、そのプロセス全体がしばしばFMEA/CILプロセスと呼ばれた。

3.0 FMEA/CILプロセス

FMEA/CILプロセスはそれ故に静的に定性的で、ボトムアップ・アプローチで単一の独立要素の故障が引き起こす乗組員の喪失、ロケットの故障、ミッション失敗のリスクを評価し減じるための適応させられた方法であった。そのアプローチは信頼に足る（アポロの成功に基づいた）衛星やロケットを製造することに目覚しい成功を収める方法であることを確かに証明した一方で、その特徴的姿のおのおのがいくつかの欠点をもたらした。このプロセスの欠点に対する突っ込んだ議論はここでは出来ないがその問題点の

要約をリストにするとつぎのようなものになろう。

- 自然な確率を求める近道がないこと。
- リスクに焦点が合っていないこと。
- 関連故障や共通故障によるインパクトを無視した単一独立故障を指示していること。
- ヒューマンおよびソフトウエアのエラーを組み込む事が困難なこと。
- 動的な状態を扱うことが困難なこと。
- 不確かさを識別して取り扱うシステマチックなやり方がないこと。
- 試験資源に関してかなりの財政的コストがかかること。

FMEA/CILプロセスの欠点があるのと定量的リスク評価を得るという当初のNASAの意図とがあって、何故NASAは定量的評価を止め、多くの問題を含むことが判っていながら定性的アプローチをしっかりと擁護しょうとするのかを聞くことは論理的である。それに答えることはもち論すこしばかり推測的であるが著者の経験と利用可能な歴史的証拠が一つの可能な答えを支持する。その証拠とは次のようなものである。(1) FMEA/CILプロセスの欠点の多くはアポロ時代を通じて存在した環境下ではそれほど重要でなかったこと、(2) 重要なものでもその時点でとにかくも利用できる定量的アプローチが適切に処理されなかったこと、(3) 現存定量的モデルから得られる予測が全く受入られないものであり、実際のミッション中に「負うべき」リスクの予想として不正確であったことである。このことは、試験プログラム費が豊富であったこともあって、プログラムの成功のレベルが高いと一般に認識されていること、そしてアポロ13号乗組員の帰還（一つの共通原因故障であったにもかかわらず）はすべてNASA内でFMEA/CILプロセスが制度化されてしまっているかのように見えた。この思想が深く染み込ませられたので、1970年代の10年と80年代初期を通じてのアポロに続くシャトルの開発時代にNASAは定量的リスク解析を、厳しく試験予算が制限され、むしろ、重要な開発上の問題が潜在的な必要性を支持していた時でさえ、採用しなかった。

4.0 シャトルの定量的リスク評価

歴史的なNASAのPRAに対する嫌悪はロジャース委員会[12]（特に根気の良いリチャード・ファインマン教授[13]）が定量的な方法を勧告したことによって少し緩和された。この勧告によって、チャレンジャーの事故から現行のシャトルの間に一連の定量的評価の研究が進んだ。これら研究の結果は（別に報告されている[14]）宇宙飛行局次長に感銘を与え、シャトルのメインエンジン点火時点から着陸時の首輪接地までの全てのミッション・フェーズを通じてのスペース・シャトルのリスクの包括的な調査を着手させた。加えて、この研究はあるケースについてはリスク要因を個々のコンポーネントにまで調

べることでリスクに重要な領域においてより深く立ち入るものでもあった。その研究はシャトルの設計と試験プログラムに特有な面があるが、その再使用性によりもたらされる特有な考察と同様に信頼に足るものとする試みにおいて、NASAの経験だけでなく契約者の経験も出来るだけ広範囲に利用するものでもあった。結局、このフェースで達成されるべき仕事の最も重要な特色はNASAにミッション・リスクの“生きた”モデルを残したことであった。この生きたモデルとシャトル・プログラムのリスク管理｛risk management｝に対する現在及び潜在的な将来の適用性について次節で議論される。

5.0 リスク管理とシャトルの生きたリスク・モデル

定量的リスク評価がNASAの宇宙プログラムに再導入されつつあったころ、リスク評価の技術は進歩し続けた。コンピュータ・ハードウエアの進歩と、より新しくより早い数値化アルゴリズムは数値化にかかる時間を数日から一夜にそして数時間にまで減じた。加えて、初期に利用可能であった粗末なワークステーションは追加データプリプロセッサーと事後解析を含む統合パーケージとなった。事象の木｛event trees｝は自動的にすべての適切な故障の木｛fault trees｝にリンクされ、データベースのデータが基本事象集合の故障の木に自動的にリンクされ得た。これまでの故障の木を描く退屈な仕事とさらにもっと退屈なそれらに対する変更のコンフィギュレーション管理の仕事がいまや自動的に組み込まれる。解析者は速記を非常に早い図的方法を事象の木と故障の木を作成するのに使え、これらの隠れた基本的な図形モデルが自動的に美しい出力のツリーを生成するのである。ポストスクリプト型のレーザープリンタの出現により、その仕事はより簡単にそしてコードは標準の出力形式で自動ページ付けと一つの木から他への自動入出力転送を組み込む利点を持っている。すばやい数値化における助けとして独立な下位事象のグループからモジュール事象を自動的に生成するためのルーチンもまた自動的に利用可能である。現在、最新世代のラップトップPCで核プラントのレベルＩPRA（即ち、イニシエータを追跡する一つが炉中心の損傷の兆候まで）が今や数十分から1時間で数値化出来る。

PRAモデルが運用の意思決定に動的に用いられることをこれらの進歩が許してきた。継続的なリスク評価は潜在的で重要なリスク影響を早期に悪化傾向を探知することを許し、それゆえにマネージメントが前もって干渉するのを許すのである。この方法でPRAはプラントの“生きた兆候”を継続的にモニタしそれらの影響の項で質問するという意味で“生きて”いるものである。

スペース・シャトルに対して最近完了したリスク評価は同様な形で行われてきている。全モデルがPCやラップトップ上で組み込まれている。もし、ゲート確率が欲しくなけ

れば数値化は10分の速さで出来るし、そうでなくても20分である。不確かさ伝達解析に基づく一つのモンテカルロ法でおのおのの重要なシーケンスに5000個のサンプルを使っても15分以内で完了する。加えて、潜在的な悪化傾向を探知するため現行のプログラマチックなデータが定期的に入力され、最近の設計変更がリスク低減の潜在性で評価され、提案された設計変更がリスク低減のコスト効果で評価される。

6.0 緊縮予算環境でのリスク制御〔Risk Control〕にシャトルPRAの使用

如何にPRAが現行のシャトルの課題に用いられ得るかの例は別途[14]報告されている。しかし、多分もっと重要なもう一つ別のシャトルPRAの使用は予算がかなり減じられた時の運用リスクの管理にある。このゼロベースのリスク管理の概念は、ある一つの機能を実行するために実際に必要なステップに運用ステップを減じるという単純な原理を適用することから始まる。シャトルに対して本質的なステップは次の飛行を打ち上げることが出来るために絶対的に必要なものである。生き残ったステップは次の飛行を打ち上げることが出来るために絶対的に必要なものである。生き残ったステップはより以上のステップ減少へのリストラクチャの可能性があるとみなされる。一旦、最小セットにまで減じられたら、残っているステップは試験や点検は含まないし、飛行後調査もないし、維持活動もないし、ペイロードの積み込み以外にはないはずである。これがゼロベースである。ゼロベース打ち上げプロセス・ステップの集合は審査され、シャトルのミッション・リスクへの貢献度についてランク付けがなされる。この方法で、関連プロセスの保証を止めることの結果によるリスクの差分が評価され得る。この評価が完成した時に、保証活動のステップが時系列的に文書化されたミッション・リスク・シナリオ、関連リスクの緩和、必要な関連実施費用の識別又は除去の有効さに関して評価される。それから保証ステップが現行の許容飛行リスクに一致する推定リスク目標に達するまで、ミッション・リスクを識別することや除去、又はリスクの緩和とそれらを実行するために必要な第一線の作業工程に加えられる。すべての追加の保証活動は頻度減少やリスク除去の候補としてプログラム・マネージメントの審査に供せられるものとして識別される。一連のリスクベースのプロセス指示器がその時点で設立され得て、測定可能なプロセス・パラメタに基づき、いかなるプロセス・リスク増をも識別し、直接マネージメントに注意を払うべく、指示すべく追跡され得る。最後に、“生きた”プロセス・リスク管理が設定される。このプログラムは体系的に飛行経験を蓄積することを許し、残存する地上作業の保証ステップによってもたらされる保証を増加させる。こうして飛行経験を蓄積することにより、頻度を減少させ除去に繋がるものとなる。

そのようなプロセス・リスク管理のシステムは、一つの背景としてシャトルPRAを用いて、シャトル運用コスト対安全リスクのジレンマに対して直接的援助を提供する。こ

の方法でシャトルプロセスを管理することはこれらの保証作業がもっとも費用効果の高いものに留める。そしてシャトルの運用経験が秩序あるやり方でプロセス・ステップ保証に置き換えられ、将来の厳しい緊縮予算環境においてさえリスクの増大なしにシャトル飛行の頻度を保つことを許すかもしれない。それはシャトル運用が利益動機で運用する民間契約者へ移されても（ますますそのようになると見られるので）[15]現在のシャトル安全水準が妥協されないという保証をNASAに与えることにもなるかもしれない。

7.0 謝辞

著者はこの論文の基礎となったいくつかの作業の支援をして頂いたNASA JSCのデービッド・ホイットル氏とNASA HQのブライアン・オコーナ氏に感謝したい。また、元NASA HQで今はヒュートロン社のベンジャミン・ブッチバインダー氏の開拓者努力を認識したい。SAICのギャスペア・マギオ氏は本文で引用したシャトルPRAの性能に対する貢献が認識されるものであり、最後にSAICのダレル・ワルトン氏とエリン・コリン女史の原稿準備の支援に対し特別に感謝するものである。

8.0 参考文献

[1] Fragola, J.R., "Reliability and Risk Analysis Data Base Development, An Historical Perspective", submitted to *Reliability Engineering and System Safety*, special issue on Reliability Data Bases, Elsvier – North Holland, Amsterdam, The Netherlands.

[2] Von Mises, R., *Probability, Statistics, and Truth*, Dover, New York, 1957.

[3] Keynes, J.M., *A Treatise on Probability*, Macmillian, London, 1921, (Reprinted Harper Torch Books, New York 1962)

[4] Ramsey, F.P. "Truth and Probability", originally included in *The Foundation of Mathematics and Other Logical Essays*, (R.B. Braithwaite, ed.), The Humanities Press, New York, 1950 Reprinted in *Studies in Subjective Probability*, Kyburg, H.E. and Smokler, H.E. eds. Krieger, Huntington, New York, 1980.

[5] DeFinetti, B., *The Theory of Probability*, Vol. I, John Wiley and Sons, New York, NY, 1974.

[6] Jeffreys, H., *Theory of Probability*, Third Edition, Oxford University Press, New York, 1961.

[7] Antona, E., Fragola, J., and Galvagni, R., "Risk Based Decision Analysis in Design", Fourth SRA Europe Conference Proceedings, Rome, Italy, October 1993.

[8] Catto, R.E. Jr. and Wheadon, W.C., "The Impact of Failure Data on Management of a Launch Operations Reliability Program", *Annals of Assurance Sciences*, 8th Reliability and Maintainability Conference Proceedings, 7-9 July 1969, Gordon & Breach, New York, 1969. LCN64-22868

[9] McKnight, C.W. et al, "Automatic Reliability Mathematical Model", North American Aviation, Inc., Downey, CA, NA66-838, 1966.

[10] Weisburg, S.A. and Schmidt, J.H., "Computer Technique for Estimating System Reliability", Proceedings 1966 Annual Symposium on Reliability, pp. 87-97.

[11] _____, "Saturn V Reliability Analysis Model Summary", SA-502, MSFC Drawing No. 10M30570, August 1967, NASA/MSFC, Huntsville, AL.

[12] Rogers, W. et al., "Report of the Presidential Commission on the Space Shuttle Challenger Accident", Washington DC, 1986 (see especially II-F, "Personal Observations of Reliability of Shuttle", Feynman, R.)

[13] Feynman, R., "Personal Observation of Reliability of the Shuttle", Appendix IIF in Rogers et al Ibid.

[14] Fragola, J.R., "Space Shuttle Program Risk Management", Proceedings of the 1996 Reliability Availability, Maintainability Symposium (RAMS), Las Vegas, NV, January 1996.

[15] Lannotta, B., "Firms Double-Team Shuttle Management Issue", *Space News*, August 7-13, 1995, pg. 3.