A RISK EVALUATION APPROACH FOR SAFETY IN AEROSPACE PRELIMINARY DESIGN

Joseph R. Fragola
Science Applications International Corporation
265 Sunrise Highway, Suite 22
Rockville Centre, NY 11570
516-764-5218/764-5286
fragola@prodigy.net

Blake F. Putney
Science Applications International Corporation
4920 El Camino Real
Los Altos, CA 94022
650-960-5948/960-5965
blake.putney@saic.com

ABSTRACT

The preliminary design phase of any program is key to its eventual successful development. The more advanced a design the more this tends to be true. For this reason the preliminary design phase is particularly important in the design of aerospace systems. Errors in preliminary design tend to be fundamental and tend to cause programs to be abandoned, or to be changed fundamentally, and at great cost later in the design development.

In the past aerospace system designers have used the tools of systems engineering to enable the development of designs which were more likely to be functionally adequate. However to do so has meant the application significant resources to the review and investigation of proposed design alternatives. This labor intensive process can no longer be afforded in the current design environment. The realization has led to the development of an approach that attempts to focus the tools of systems engineering on the risk drivers in the design. One of the most important factors in the development of successful designs is adequately addressing the safety and reliability risk. All too often these important features of the developed design are left to afterthoughts as the design gives sway to the more traditional performance focus. Thus even when a successful functional design is forthcoming significant resources are often required to reduce its reliability and safety risk to an acceptable level.

In the USA NASA has clearly indicated, in the aftermath of the Challenger accident and more recent Mars Mission failures, that safety and reliability risks taken to enhance performance are no longer acceptable. Further, NASA has advanced policies, goals, and requirements which are extremely challenging in the risk area. The question is how can these goals be met in a developed design, and more importantly in the near term, how can NASA select design alternatives at the preliminary design stage which are more likely to meet these challenging reliability and safety risk requirements within schedule and cost constraints?

The issue is extremely challenging and confounding to NASA and its supporting contractors. However the recent completion and broad based circulation of the integrated shuttle risk assessment throughout NASA has indicated a potentially feasible approach to address this issue. This approach, which will be discussed in this paper, builds upon the experience base of the integrated shuttle risk assessment and its recent expansions and applications to the evaluation of newly proposed launcher designs. The approach used the shuttle developed PRA models and associated data sets as functional analogs for new launcher functions. The concept being that the functions of any launcher would be characterized by the associated models developed for those functions on the shuttle. Once this functional decomposition and reconstruction has been accomplished a proposed new design is compared on a function by function basis and specific design enhancements that have significant promise of reducing the functional risk over the shuttle are highlighted. The potential for enhancement is then be incorporated into those functions by suitable modification of the shuttle models and or the associated quantification data sets representing those design features addressed by the new design. The level of risk reduction potential is then estimated by those component failure modes and mechanisms identified for the shuttle function and eliminated in the new design. In addition heritage data that would support the claims of risk reduction for those failure modes and mechanisms that remain albeit at a reduced level of risk are applied.

While this “lego block” functional comparison approach would not suffice to allow for adequate absolute estimates of potential risk it is felt that it has been shown to be sufficient to allow NASA to investigate the risk relative risk reduction potential of proposed alternative designs. This paper presents an implementation of this approach and its application to

the evaluation of shuttle upgrades and selected 2nd generation launcher designs. The evaluation not only addresses the potential safety and mission risk reduction potential of the proposed designs but also the risk of their development.

Background

NASA Ames Research Center has initiated a project, supporting the 2nd Generation Reusable Launch Vehicle (RLV) Program, to develop an advanced suite of conceptual design tools. The tools will be developed within an object-oriented framework to enable integrated multi-disciplinary, multi-fidelity analysis. The new integrated process as well as the individual "plug and play" tools will be inserted into the Reusable Space Transportation System (RSTS) conceptual analysis environment. In order to meet the program requirements for vehicle and crew safety, new analysis capabilities are being developed and integrated within this framework to provide an assessment of risk of failure of given concepts.

In the past aerospace system designers have used the tools of systems engineering to enable the development of designs that were more likely to be functionally adequate. However to do so has meant the application significant resources to the review and investigation of proposed design alternatives, as can be seen in Figure - 1[1] and the consideration of risk and safety impacts is considered afterwards, perhaps after key aspects of the design are frozen. Because of the comprehensive, but unfocused, nature of the traditional systems engineering process much of the expended effort may be wasted on portions of the design that are not key performance discriminators.

Applications of risk analysis are emerging to provide managers a means of focusing programs on key performance drivers, be they cost, safety, or reliability. Lack of focus can result in considerable difficulties when trying to meet risk goals for a program, and can lead to considerable re-work causing overruns or program cancellation if risk drivers are inadequately considered.

Since risk analysis has typically been performed on detailed design for verification purposes, it has been performed at the component level, typically with Fault Trees and has been viewed as very expensive. In the past designers have hesitated to perform risk analysis on design concepts due to lack of design specifics to allow for analysis with fault trees and component level data. The Risk Oriented Optimization Tool (ROPOT) discussed in this paper was developed to determine if a risk analysis developed from the risk drivers of the shuttle could provide useful program insights management for a conceptual design.

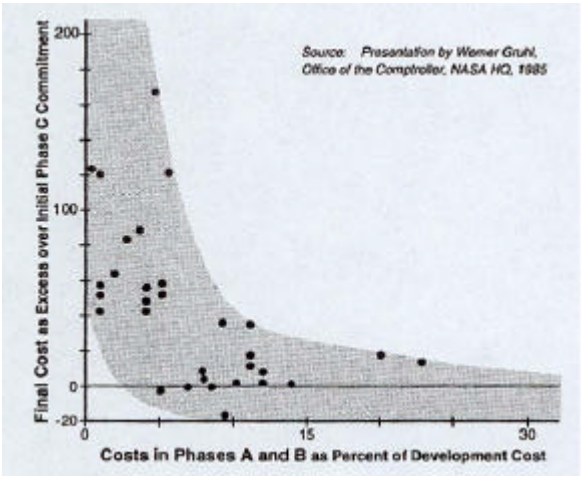

Figure 1. Potential Overruns when Phase A and B are Underfunded.

In the case of the 2nd Generation RLV, cost and safety are primary performance drivers, specific risk goals for the program have been established, and significant development risks may be associated with the achievement of both safety risk and cost goals. The focus the project reported here was the development of a risk/safety tool to support the preliminary design phase of the program, and to provide a basis for understanding the safety benefits of new technology, plumbing the design space for attractive design alternatives, and understanding the development risk trades that are inherent to the maturation of the program.

ROPOT Description

The objective of the project was to provide an integrated safety analysis capability for the RSTS environment. Initially as a separate capability but with the longer-term goal of seamless integration with multi-disciplinary performance analysis tools. The combination of these tools will allow the designer to visualize not only the functionality of the design being reviewed under nominal conditions but also the robustness of the design against probabilistically credible failure events. The scope of this task includes the development of a prototypical tool that allows for the evaluation of safety and reliability metrics (specifically Loss of Crew, and Loss of Vehicle) for the space shuttle, the space shuttle upgraded designs, and new RLV (Bimese) designs based upon space shuttle heritage. The tool was developed to interface with analogous physical design tools (e.g. geometric and finite element structural), phenomenological tools (e.g. Computational Fluid Dynamics tools addressing the Aerodynamic and Aerothermodynamic environment), and economic assessment tools (e.g. Net Present Value and Real Options Valuation of alternatives), so as to seamlessly fit into the set of tools envisioned to support the efforts of the NASA Inter-Center Systems Analysis Team (ISAT). A prototype tool was developed in Microsoft Excel.

Although the prototype version of the tool was developed for launchers, its modular nature allows it to be applied to many different technologies.

The Risk Model

The issue of ensuring enhanced reliability and safety in the next generation of launchers is extremely challenging and confounding to NASA and its supporting contractors. However the recent completion and broad based circulation of the integrated shuttle risk assessment throughout NASA[2] indicated to the SAIC team a potentially feasible approach to address this issue. This approach builds upon the experience base of the integrated shuttle risk assessment and its recent expansions and applications to the evaluation of newly proposed launcher designs.

The Shuttle PRA was first evaluated to highlight elements of the shuttle design identified as drivers. Once this was completed, a new structure was developed in a hierarchical fashion. In this hierarchy the depths to which an element was represented was indicative of its risk contribution, and details necessary to capture future conceptual design alternatives. For example, as can be seen from the resulting hierarchy represented in Figure 2 a Shuttle Based risk model is applicable to the Bimese with minimal changes. This implies that the shuttle and its PRA have the potential, if properly structured, to be representative of a more general class of launchers at least for the LOC and LOV end states.

Whether or not this potential could be actualized depends, of course, on the extent of modification of the risk model necessary to allow the shuttle model to be used as a surrogate for a proposed new launcher. These modifications would be expected to take, and did take, two forms: 1) a modification of the frequency of failure of the same basic events in the proposed new design, and 2) the elimination or addition of elements and their failure contribution.

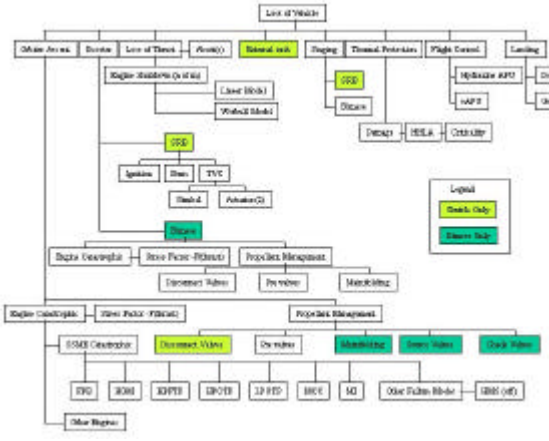

Figure 2. Loss of Vehicle Model Structure

It is expected that the design process of the 2nd Generation RLV will generate many different design alternatives in attempting to meet its cost and safety goals. The risk model will support risk calculations to evaluate the benefit of investments in all aspects of the design. During the evaluation of multiple alternatives it was discovered that the concept of developmental difficulty could provide useful insights to a decision maker. "Difficulty" represents the risk of failing to complete the development process on time to meet the program schedule. Specifically the benefits provided by the promised improved performance or reduced cost of developmental designs must be "discounted", in the economic sense of the term, by the probability that it will be developed and deployed according to the required deployment date. The more creative the design, the scantier its heritage, and the earlier the phase of its development, the riskier the development.

The quantitative approach employed here to evaluate the developmental risk and thereby the difficulty of development has been generated by SAIC over the past several years[3],[4]. The approach is based upon the systematic evolution of the TRL meter shown in Figure 3 is discussed in the above references and is also heuristically derived from experience.

Log normal distributions are used as a basis for calculating the probability that a specific design element will be successfully deployed at a desired time (achievability). Here the product of the achievability of each developmental element is the overall achievability of the program. The program difficulty at the desired time is the complement of the overall achievability. It should be noted that the concept of difficulty could be applied to all performance measures of a developmental system, not just safety.

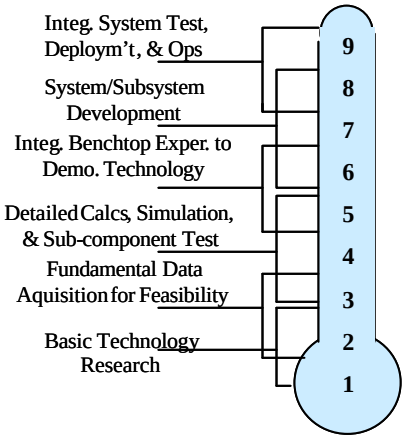

Figure 3. TRL Barometer Risk Insights

A key aspect of applying results of risk assessments is an understanding of how key system elements contribute to risk, and how changes in their reliability change risk. This information provides to user with an intuition about how the risk surface behaves. In this sense the key elements can be viewed as multiple dimensions in the risk space.

The Importance Measure approach is used in traditional risk assessment and it is useful when applied to an existing system. In this case it is not generally feasible to change multiple elements, and large improvements in the system design are difficult to achieve. However, in the early design phases of a system, all system elements are open to improvement, and can be improved in combination with others. This reduces the usefulness of Importance Measures. For example if the Main Engine is identified as contributing 30% to the risk, an improvement program may be put into place to increase engine reliability as much as possible. However, as the engine is improved, other risk contributors may become more important. Continued investment in improving the engine (generally with diminishing returns) will not bring as much benefit as efforts to improve the new dominant risk contributors. This process of switching efforts between elements to achieve an optimal solution generates what is termed a risk "trajectory" through the risk space defined by the set of all achievable values of the risk elements.

A path between the existing or baseline design to an alternative design solution is the risk trajectory. The process of examining various risk trajectories, and understanding how the risk contributors change along the trajectory provides the user without intuition of how risk behaves in the design regime. This information can then be used to sculpt an optimal design/operational solution.

As an example of the usefulness of the risk trajectory concept consider Figure 4 shows how the LOV probability improved as the engine improves holding other design elements constant.

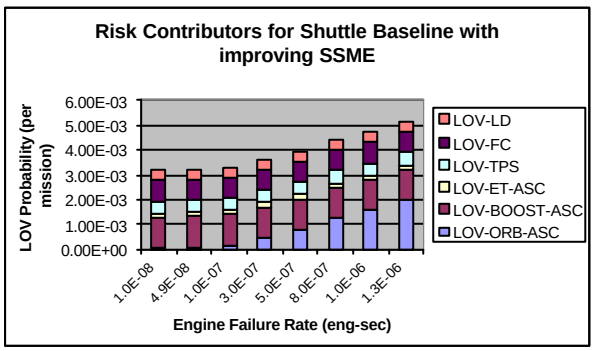

Figure 4. Shuttle Risk Improvement from SSME Improvement

The Figure demonstrates how the LOV probability reduction flattens out as the engine failure rate approaches 3.0 E-7. In this case, improving the engine alone beyond the 3.0 E-7 range will have small relative safety benefit.

Figure 5 below illustrates the same effect for the Bimese configuration.

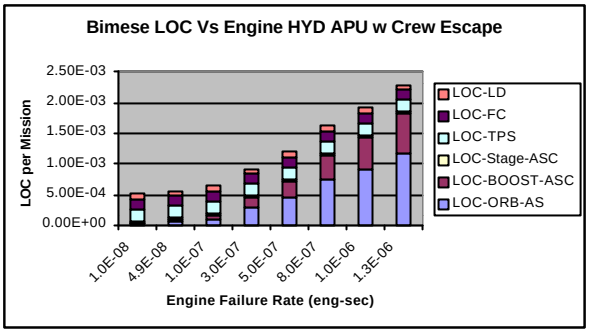

Figure 5. Illustration of the Effect of Improvement of Engine Reliability on Risk

In the Bimese case the LOC probability improvement rolls off at 1E-7, showing risk reduction value for a factor of three greater reduction in engine risk. This is primarily due to the fact that the same Engine is included in both the Orbiter and the Booster designs.

The risk surface can be further examined by varying other parameters that contribute to risk. The example given in Figure 6 shows how Shuttle risk improves with reliability improvements in the SRB (.3,.5,.7 improvement factors), and the replacement of the Hydrazine powered flight controls with an electric APU (EAPU). This figure illustrates how multiple improvements can be viewed as constituting a trajectory over the risk surface.

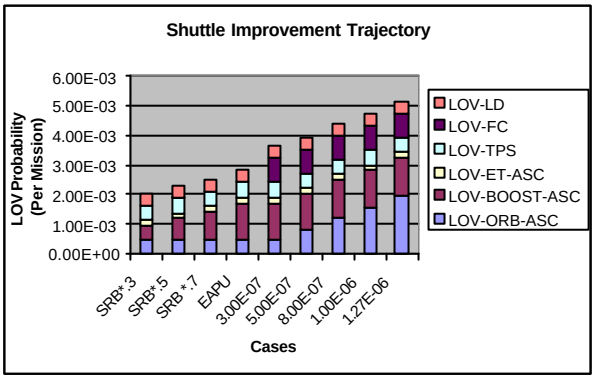

Figure 6. Shuttle Improvement Trajectory Design Trades

Examining how risk changes with design alternatives is useful, but it does not provide the whole story. Risk reduction is not free. Each potential change involves development and operational costs, and difficulty in deploying a new system. Design choices made to improve a system to reduce risk must take into account the development required. To account for alternatives at varying stages of maturity the concept of "difficulty" is introduced. Eventually difficulty can be an input to cost models and the actual economic value of design alternatives can be assessed. Difficulty can be added as another axis in the risk space.

Once the risk space is developed, it can be visualized in various ways. It can be viewed as a carpet plot or from

above as a scatter plot. In this latter case each possible solution has a Risk and Difficulty. Inclusion of uncertainties will create vertical uncertainty error bars around each point and indicate where there is potential overlap between alternatives. Each solution can then be examined to investigate the risk drivers for that particular design alternative.

In evaluating the merit of various design solutions the decision-maker is aided by better understanding how a particular solution compares to the fundamental system goals. For 2nd Gen the fundamental goals are 1,000 dollars per pound to orbit, and LOC risk of less than 1 in 10,000 missions. Therefore plots relating a design to cost and risk are appropriate. As mentioned above a key input for the economic calculations is the development schedule. Here difficulty plays a key role. An example of the usefulness of the difficulty concept is provided below.

A risk space was generated for Loss of Crew (LOC), and Loss of Vehicle (LOV). The model generated a risk probability, and a difficulty for 150 design alternatives. In this example it was assumed that system needed to be deployed in 5 years. The resulting scatter plot in Figure 7 shows the results.

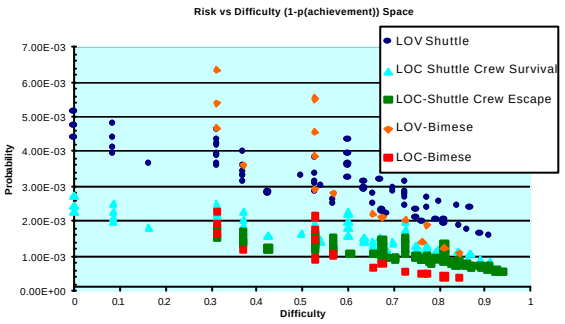

Figure 7. Risk Difficulty Space Quantified at 5 Years

The difficulty factor was based on the assumption of a deployment date of 5 years hence. The resulting plot indicated that there is a wide variation in the difficulty in achieving the lowest risk, and that there are some relatively easy solutions that gain most of the risk reduction benefits. Future displays of this information will allow the user to select a point and display the underlying variables, and generate line segments illustrating how risk and difficulty change by changing design alternatives. A chart of this type could be provided to program managers to help them view the difficulty in achieving the Risk goal. Incidentally, this approach and chart format can be used for any quantitative design goal.

Figure 8 Illustrates the risk surface quantified with a development time of 7 years. As can be seen in the figure, by extending the development time for the vehicle, the program manager reduces the difficulty of developing alternatives, and a number of additional low difficulty design alternatives become attractive.

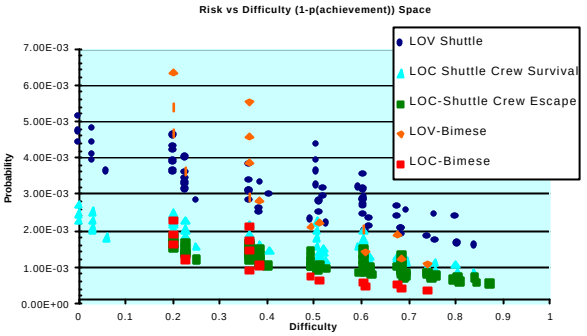

Figure 8. Risk Difficulty Space Quantified at 7 Years

A Summary of Insights

As a result of the study the following insights were gained:

1) The development of a risk-based design tool to aid in programmatic design decision-making is feasible.

2) A simplified "Lego Block" model of the shuttle can be developed from the PRA

3) The lego block model can be extended to alternative vehicles by experienced experts within reasonable time and resource constraints

4) Risk Surfaces and Multiple Dimension Visualizations provide powerful illustrations of the trade space

5) This modeling concept is a viable basis for development of risk tools for future programs

References

[1] Shishko, R. et.al., "NASA Systems Engineering Handbook", SP-6105, June 1995, NASA/JPL, Pasadena, CA.

[2] Fragola, J. R., et al., Probabilistic Risk Assessment of the Space Shuttle: A Study of the Potential of Losing the Vehicle During Nominal Operations, Volume I Final Report, SAIC/NY95-02-25, 28 February 1995.

[3] Fragola, J.R. and Maggio, G., "Application of Probabilistic Program Planning to an Advanced Radiographic Hydrodynamics Facility", ESA Risk Management Workshop, 30 March – 2 April 1998, ESA/ESTEC, Noordwijk, The Netherlands.

[4] Fragola, J.R., "A Heritage Approach to Risk Based Design", Presented at the International Mechanical Engineering Conference and Exposition/ASME/SERAD, November 5-10, 2000, Walt Disney World Dolphin, Orlando, Florida.