ABS Consulting

Example Application of RISKMAN®

Prepared by:

Donald Wakefield
ABS Consulting, Inc.
Operational Risk and Performance Consulting Division
300 Commerce Drive Suite 200
Irvine, CA, 92602
Tel: (714) 734-2503
Fax: (714) 734-4282
E-mail: dwakefield@absconsulting.com

In Conjunction with:

GAIN Working Group B, Analytical Methods and Tools

September 2004

Global Aviation Information Network
ENHANCING AVIATION SAFETY THROUGH SHARING

Preface

This example application has been prepared by ABS Consulting, Inc. in conjunction with the Global Aviation Information Network (GAIN) Working Group B (Analytical Methods and Tools) (WGB) as one of a number of such examples of the use of analytical methods and tools described in the "*Guide to Methods & Tools for Airline Flight Safety Analysis*". The intent of these example applications is to illustrate how various tools can be applied within an airline flight safety department, and provide additional information on the use and features of the tool and the value of such analysis. GAIN WG B hopes that these example applications will help increase the awareness of available methods and tools and assist the airlines as they consider which tools to incorporate into their flight safety analysis activities.

Each example application of an analytical method or tool is posted on the GAIN website (*www.GAINweb.org*). Readers are encouraged to check the website periodically for a current list of example applications, as further examples will be added as they become available.

Disclaimers; Non-Endorsement

All data and information in this document are provided "as is," without any expressed or implied warranty of any kind, including as to the accuracy, completeness, currentness, noninfringement, merchantability, or fitness for any purpose.

The views and opinions expressed in this document do not necessarily reflect those of the Global Aviation Information Network or any of its participants, except as expressly indicated.

Reference in this document to any commercial product, process, or service by trade name, trademark, servicemark, manufacturer, or otherwise, does not constitute or imply any endorsement or recommendation by the Global Aviation Information Network or any of its participants of the product, process, or service.

Notice of Right to Copy

RISKMAN®: A General Purpose Tool for Quantitative Risk Analysis

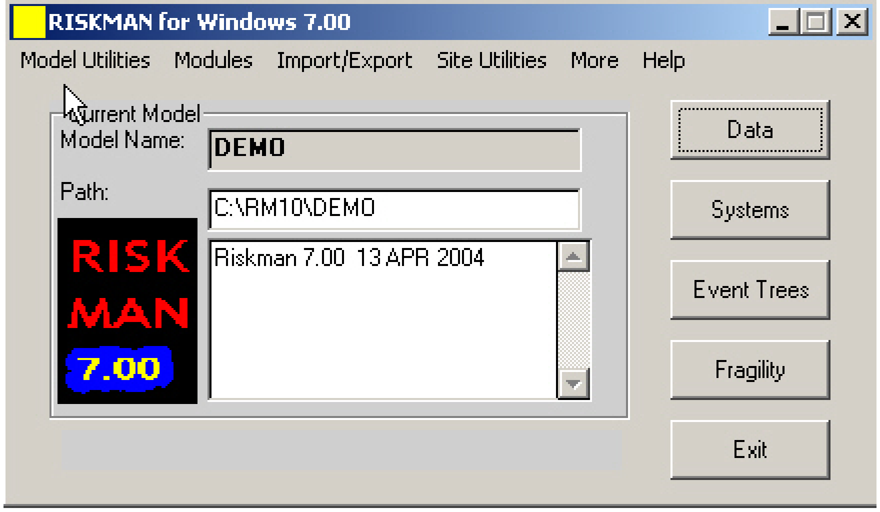
1 Introduction

Quantitative risk analysis can be thought of as the process one goes through to answer three basic questions: (1) What can go wrong? (2) How likely is it? (3) What are the consequences? The answer to the first question is a listing of potential accident sequences, generally described as a sequential combination of events. These sequences are organized into categories and subcategories according to the definitions of the combining events. The answer to the second question is the set of frequencies, or probabilities, of each sequence. The answer to the third question is an estimate of the damage that may occur for each sequence in the list. There may be multiple measures for damage; e.g. dollars lost, passengers injured, etc. The set of answers to these three questions can then be used to measure risk, evaluate proposed changes, and identify major contributors.

1.1 OVERVIEW OF THE TOOL FUNCTIONALITY

The RISKMAN® for Windows software is a general purpose tool to perform quantitative risk analysis, see Figure 1. It has modules to help the analyst identify events and assemble combinations of events into sequences and to calculate the probability of these events and the frequency of the listed sequences. Assessment of the consequences of sequences generally requires tools specialized for the industry being assessed. Instead, RISKMAN® provides a means to categorize the sequences into classes of consequence impacts by assigning each sequence to an end state. Numerical values may be assigned to the severity of these end states so that the relative contribution of sequences to overall risk can be considered.

RISKMAN® consists of four main modules and an entry screen for model utilities. These modules are illustrated and described briefly below.



Current Model

Model Name: DEMO

Path: C:\RM10\DEMO

Riskman 7.00 13 APR 2004

Figure 1 **RISKMAN for Windows 7.0**

The **Data** module is used for developing mean values and full uncertainty distributions for failure rates and related performance model quantification parameters. The often continuous parameter uncertainty distributions are stored and manipulated within RISKMAN® as discrete probability distributions. Use of discrete probability distributions avoids restricting the analysis to distribution types, before and after manipulation, that are a closed analytical form. RISKMAN® has routines to adjust generic data to reflect industry and project-specific experience data using Bayesian techniques. Batch routines for Bayesian updating have been developed and are easy to implement in subsequent calculations when more experience data is collected.

The **System** module accepts as input the data distributions developed in the Data module, and produces system or event failure probabilities that are in turn used in sequence frequency calculations in the Event Tree module. The Systems module employs fault tree graphics to enable the analyst to describe the logical combination of failure events that prevent a system from performing its intended function. The failure event probabilities are entered in equation form in terms of the failure data parameters. Logical reduction tools and point estimate and Monte Carlo uncertainty methods of logical model quantification then assess the system failure probabilities, including uncertainties. Contributors to these system failure probabilities are also provided as output for review. Equipment failure modes may then be ranked according to their importance to the integrated system failure probability. A unique feature within RISKMAN® is the ability to specify common cause failure groups separately from the fault tree and then have these groups automatically added to the fault tree for quantification. A “Red Button” feature is also provided to automate and document system model changes and results for sensitivity studies. Changes to the model can be saved, results created, and then the model reset to base case conditions all using a string of commands saved in a batch file.

The **Event Tree module** allows the analyst to describe sequences of events graphically in the form of event tree diagrams. For each initial event (i.e. initiator) RISKMAN® can solve a linked set of event trees to quantify the frequencies of individual paths through the linked set of event trees. End state frequencies are then obtained by summing the frequencies of all sequences mapped to each end state. Frequency truncation is controlled by the user to examine only the top sequences, or dialed-down for convergence of the results. Key sequences are saved to a sequence database with over 40 publication-quality reports ranging from system importance rankings to end state frequencies. For each sequence or group of sequences, RISKMAN® can display the system success and failed states, human actions, key dependencies, component and basic event importance measures. A key feature is that it can calculate importance measures on all sequences quantified during runtime; i.e. they don’t have to be saved for subsequent processing. This feature means that importance measures can be computed for very low quantification cutoffs. The selected cutoff is only limited by computer runtime and the size of the model.

A **Fragility module** is provided as an alternate means to compute event failure probabilities used in the Event Tree module. Some event failure probabilities can not be computed directly from fault trees. Examples are structural failure probabilities that increase for stronger winds or earthquakes. The Fragility module provides a way to input the results of such evaluations in standard form. RISKMAN® computes the failure probabilities for each component within a specified range of hazard according to the hazard curve information. These component failure probabilities are provided to the Event Tree module for use in sequence frequency estimation.

In addition to the four main modules, RISKMAN® includes important model utility features. These utilities permit multiple models to be created, saved, and deleted. Model parts may also be exported from one machine and imported into another model on the same or a different machine.

1.2 INTRODUCTION TO THE EXAMPLE APPLICATION

Quantitative risk analysis (QRA) can be used as an additional tool to supplement the extensive qualification and testing procedures of the space industry. The strength of QRA is in its ability to look at a whole system from an integrative perspective and in a quantitative, scientific way, consider the consequences, likelihood, and uncertainties. The example presented here is an old one, but still relevant today.

The example application considers a quantitative risk assessment of the space shuttle orbiter auxiliary power units (APUs) powered by hydrazine fuel. Hydrazine is corrosive to some materials, flammable in just 4% oxygen, and will exothermically decompose when in contact with some metal oxides. There are three redundant APUs in the orbiter, two of which are generally required. The APUs provide shaft power to the hydraulic pump that is required for flight control surfaces, main engine gymballing, and landing gear deployment and braking. The example application is summarized in a paper by B. John Garrick for the journal RISK ANALYSIS (November 1988, Risk Assessment Practices in The Space Industry, The Move Toward Quantification).

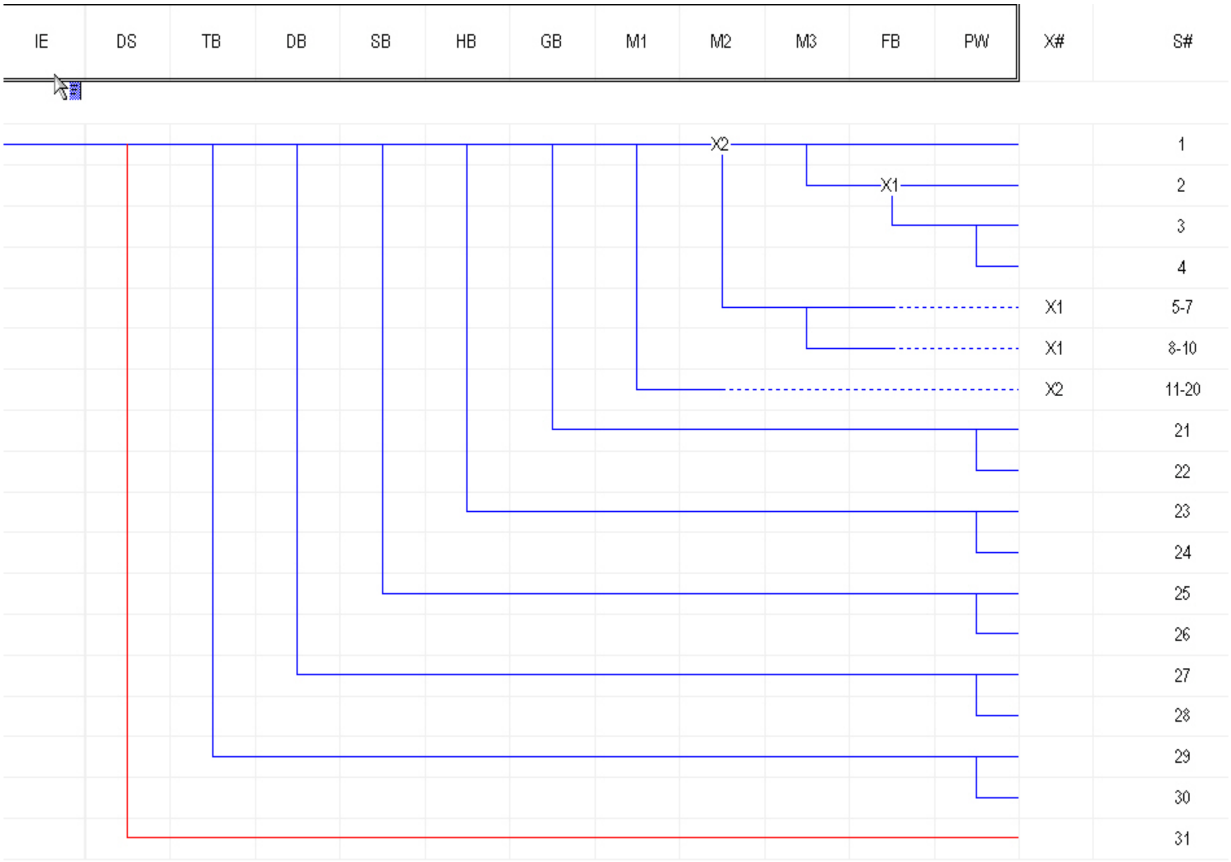
The space shuttle poses a particularly difficult modeling problem because its systems are exposed to a variety of environments, different configurations, and operating modes during a mission. The example application considered the performance of the APUs and their effects on surrounding systems during each phase of the shuttle's mission; i.e. pre-launch, ascent, orbit, descent, and landing.

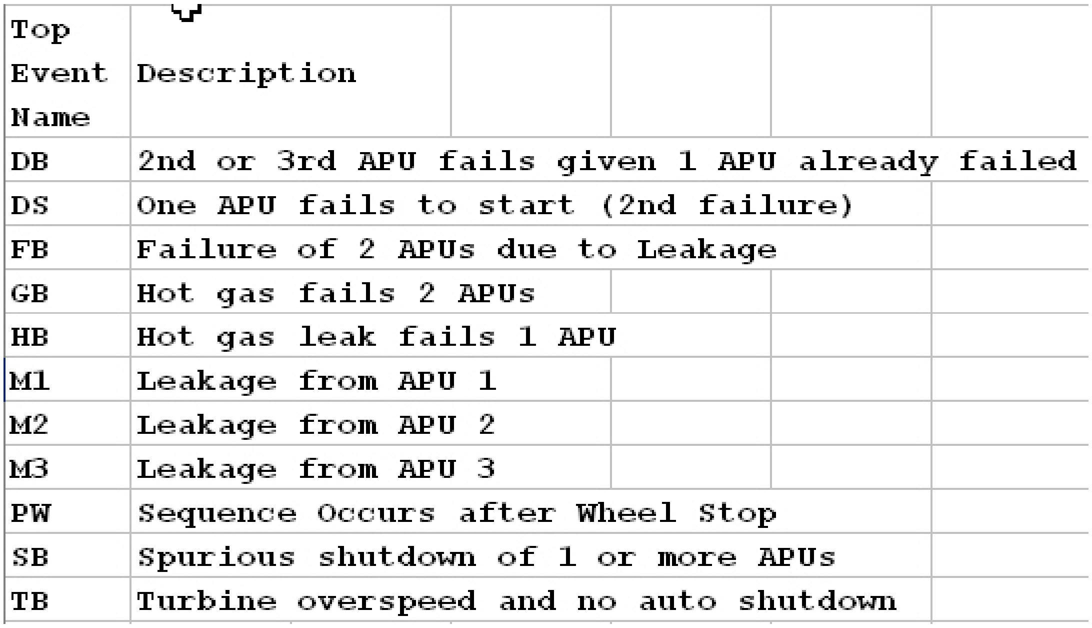
2 Input Data

The RISKMAN® software requires input for each module to be used in the analysis. In this presentation, we focus on the input for three modules, the Event Tree, Systems, and Data modules. Any data preparation and formatting will be required so as to interface with the RISKMAN® software.

For the **Event Tree** module, the events selected to appear as top events in the event trees are developed from information on the phasing of the APU's mission and the interactions of the crew and vehicle design to initial equipment failures. In the example application, this information came from malfunction procedures, flight rules, launch commit criteria, abort criteria, and next planned landing site de-orbit criteria. As an example, an APU was assumed not to be restarted if its initial shutdown was caused by an over-speed condition. Such information is often developed into event sequence diagrams and reviewed before abstracting the logic into event trees. Each of these inputs could affect the role of malfunctions in early phases and of the mission during later phases. The conclusions from engineering studies as to the success criteria (especially for redundant systems like the shuttle APUs) are a key component of specifying the safety function represented by each top event.

For the evaluation of the APUs, two event trees were developed. The first described the pre-launch and ascent phases of the mission. The second event tree described the orbit, descent and landing phases. Sequence end states considered were success, loss of crew, loss of vehicle, and loss of mission; e.g. launch scrub and intact abort. The second event tree, which is then linked to each sequence in the first tree, is shown in Figure 2. The tree structure is followed by the descriptions of the event tree top events.





Top Event Name	Description
DB	2nd or 3rd APU fails given 1 APU already failed
DS	One APU fails to start (2nd failure)
FB	Failure of 2 APUs due to Leakage
GB	Hot gas fails 2 APUs
HB	Hot gas leak fails 1 APU
M1	Leakage from APU 1
M2	Leakage from APU 2
M3	Leakage from APU 3
PW	Sequence Occurs after Wheel Stop
SB	Spurious shutdown of 1 or more APUs
TB	Turbine overspeed and no auto shutdown

Figure 2 **Event Tree Diagrams**

For the **Systems** module, the specification of the event tree top event functions are a key first step. Given the mission to be analyzed, the details of the system design and performance are then used to construct logic models (i.e. fault trees) to determine how the system parts might fail to work in combination to perform the defined safety function. Examples of such failures are hydrazine leaks, spurious shutdowns, and turbine runaways. Such models can be constructed for each phase of the shuttle mission that involves the system. Multiple event tree top events may be used to describe the different phases of the system's mission for each of the three APUs. In Figure 3 below, this fault tree illustrates a portion for the failure mode—turbine wheel runaway.

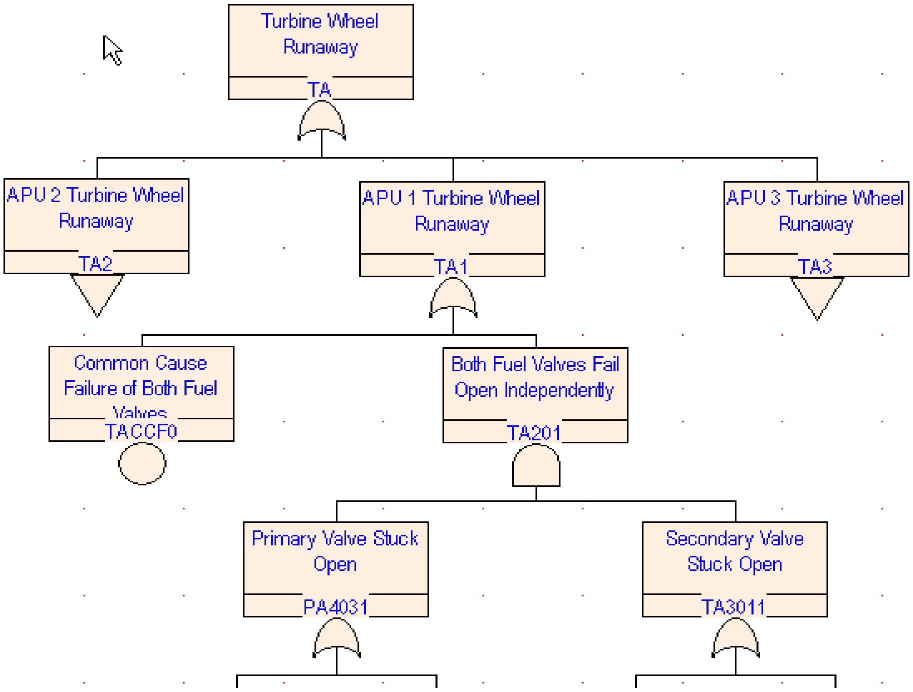
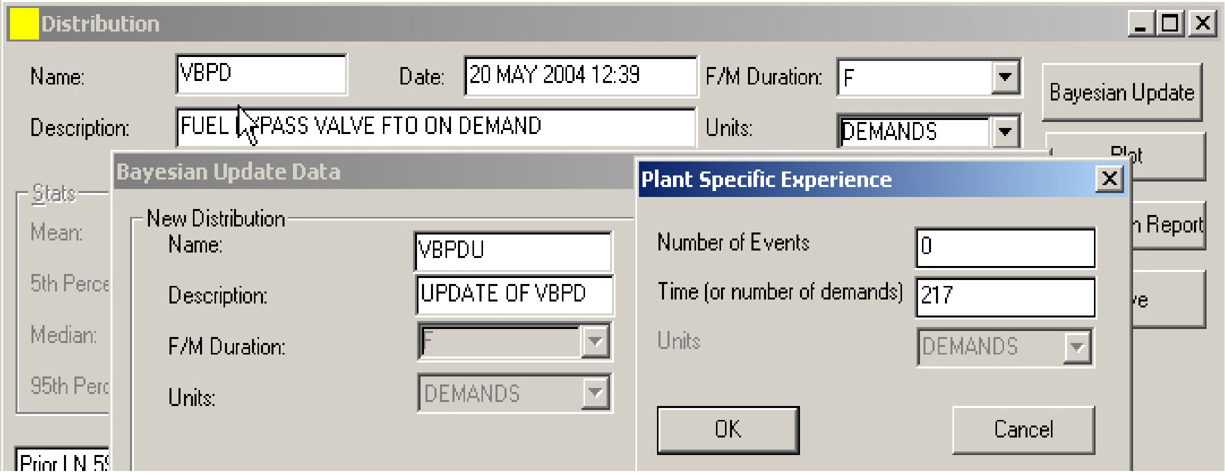

Turbine Wheel Runaway
TA
APU 2 Turbine Wheel Runaway
TA2
APU 1 Turbine Wheel Runaway
TA1
APU 3 Turbine Wheel Runaway
TA3
Common Cause Failure of Both Fuel Valves
TACCF0
Both Fuel Valves Fail Open Independently
TA201
Primary Valve Stuck Open
PA4031
Secondary Valve Stuck Open
TA3011

Figure 3 **Fault Tree Diagram of a Turbine Wheel Runaway**

For the **Data** module, raw sources of information considered in the analysis included actual flight data, shuttle test data, equipment failure mode similarity data from military handbooks, and expert opinion and engineering analysis. The most applicable experience data is chosen for each equipment failure mode, including accounting for subsequent corrective actions. Included in this choice is the availability of success data; i.e. where no failures are reported. The experience of successful operation (e.g. from mission reports) is important evidence to include in the assessment, even if no failures occurred. A sample entry screen from the Data module, used to perform Bayesian updates, is illustrated in Figure 4 for the failure to open mode of a key valve for which there have been no failures in 217 demands.



Name: VBPD
Date: 20 MAY 2004 12:39
F/M Duration: F
Description: FUEL BYPASS VALVE FTO ON DEMAND
Units: DEMANDS

Name: VBPDU
Description: UPDATE OF VBPD
F/M Duration: F
Units: DEMANDS

Number of Events: 0
Time (or number of demands): 217
Units: DEMANDS

Figure 4 **Data Module Entry Screen**

3 Analytical Process

Data Module

The Bayesian approach is capable of combining both engineering judgment about an event frequency and empirical data, such as the actual number of failures observed during operation. The Data module performs such processing after the analyst enters the experience data. In the Bayesian process, as additional experience data is gathered and combined with earlier state of knowledge, the resulting uncertainty distribution for the parameter narrows toward the point estimate of the empirical data. For point estimates, only the mean values of the parameter distributions are used. However, throughout RISKMAN®, the full distributions can be considered when propagating uncertainties.

Systems Module

In the systems module, each graphically entered fault tree is logically reduced to minimal form for evaluation of the top event probabilities. Results from the data parameter analysis are used to perform the top event quantifications. The contributors to the top event probability are numerically ranked and presented to the user for review.

Event Tree Module

The top event probabilities developed in the system analysis are passed to the Event Tree module for quantification of the sequence frequencies. For the space shuttle example, given the start of the mission, RISKMAN® walks each sequence path through the linked set of event trees combining the appropriate branch probabilities at each node to determine the frequency and the appropriate end state for each sequence; e.g. successful mission, or loss of vehicle.

The time required to process each potion of the analysis is dependent on the model size and truncation limits used. The event tree walk usually takes the most time, but for practical applications can often still be completed in less than one minute.

4 Tool's Output

The intermediate results from the Data (e.g. parameter mean values) and System (e.g. top event probabilities) modules are available for reporting. However, the most revealing outputs are from the Event Tree module. The highest frequency sequences to each end state are identified and ranked numerically. The sum of the frequencies of sequences assigned to an end state for each end state is also reported. There are more than 40 reports that can be prepared by the Event Tree module alone. These include importance rankings at the equipment failure mode, branch probability, and by system.

For the space shuttle APU example application, it was shown that the frequency of launch scrub was about a factor of 100 more likely than loss of vehicle. The risk of losing the vehicle during entry or landing dominated the risk posed by operation of the APUs. Among the more interesting reports is a ranking of the sequences involving failure of the APUs and contributing to the loss of vehicle end state as illustrated in Figure 5. Hydrazine leaks in two or more APUs in the same mission account for 25% of the risk. This is consistent with mission experience up to the time of the study. The risks from spatial interactions, failure effects propagating within the sub-system or cascading into other subsystems, and common cause failures pose much greater risks than combinations of independent APU failures.

Rank	**Sequence Description for Sequences Contributing to Loss of Vehicle**	**% Contribution**
1	Hydrazine leak downstream of fuel isolation valves and into aft compartment during orbit or entry resulting in loss of 2 APUs or critical equipment	39
2	Hydrazine leak as above, but from 2 or 3 APUs concurrently	27
3	Hydrazine leak from 1 APU as above with independent failure of 2nd APU	6.4
4	Equipment failure of 2 APUs in orbit, entry or landing (not related to APU start)	5.0
5	Failure to start of 1 APU in orbit, and 2nd APU fails while running	4.0
6	Hydrazine leak into isolation valve solenoid, auto-decomposes, ruptures valve cover, and contents of fuel tank dumped into aft compartment	3.8
7	Turbine comes apart at normal speed during entry; shrapnel and hydrazine effects fail 2nd APU or critical equipment	3.1

Figure 5 **Sequence Ranking Diagram**

5 Application of the Results of the Analysis

The initial quantitative risk assessment of the space shuttle orbiter APU's was a pilot study that demonstrated the utility of QRA for safety decisions. Because of the age of this pilot study, no absolute numerical results are presented here. As more experience data is collected and safety knowledge gained, the results computed today would certainly be different. In addition, changes to reduce the risks may have since been implemented.

Potential changes highlighted by the initial assessment include the introduction of barriers to isolate each APU, improved leak detection procedures during turn around operations, and a fuel isolation valve redesign. Also, engineering calculations to certify that one APU is sufficient through all phases of the mission would greatly alter the risk perception. Such "what if" analyses forms the basis for effective risk management. The quantitative risk model helps the decision maker decide what is important, and what is not important. When properly considered with uncertainties, the results also indicate how well the risk is known. The risk model also provides a systematic way to preserve and enhance the "corporate memory" about system safety.

The pilot study detailed the contribution that the APU system had to scrubbing the launch or to the loss of the shuttle after launch. The identification of hydrazine leaks that may contribute to such failures was nothing new. Failure Modes and Effects Analysis (FMEAs) and Hazards Analysis (HA) had already identified the possibility of hydrazine leaks. The QRA, however, identified the key risk contributors at a finer level of detail than comparable FMEAs. Unimportant risk contributors, on the other hand, may be identified at a coarser level in the QRA. What was new was the ability to quantitatively rank by risk specific component failure modes and the identification of common cause and multiple, or cascading failures to risk. For such an assessment, the sequence-based approach used in QRA is required. Such rankings help decision makers decide where best to improve safety.

The earliest PC version of RISKMAN® was used in the performance of this example application. Following many years of development and refinement, version 7.00 of RISKMAN® for Windows makes the application of such techniques to problems in the aviation field today that much more cost effective and easier to perform.