Risk Analysis, Vol. 9, No. 1, 1989

Guest Editorial

Risk Assessment Practices in the Space Industry: The Move Toward Quantification

B. John Garrick[1]

INTRODUCTION

The National Aeronautics and Space Administration (NASA) and the defense industry had the momentum in the 1950s in the development and application of probability-based techniques for analyzing system safety and reliability of space and defense systems. The defense industry employed fault tree methods in the design and deployment of the minuteman missile system and utilized reliability modeling extensively in other programs such as the C-5A cargo airplane. When NASA commenced the Apollo program to eventually land a man on the moon, they too were involved in the use of probability-based methods to address questions of safety, reliability, and risk. Then, something happened that changed NASA's whole approach, especially to risk and safety analysis.

The time is remembered as about 1960, and the event was a bad experience with a probability calculation on the likelihood of successfully getting a man to the moon and back. The calculation was very pessimistic and embarrassing to NASA officials and soured them on the utility of probability calculations. From that point forward, NASA chose not to do probability, that is, quantitative risk and safety analysis, on their space systems. Rather, they adopted a qualitative approach utilizing failure mode and effects analysis (FMEA) as the principal building block for their risk analysis program.

The Space Shuttle Challenger accident raised the whole issue again of NASA's approach to risk assessment. NASA has come under some criticism from the public, the Congress, and the risk assessment professionals. It is the purpose of this paper to review some of the events surrounding this issue, to discuss alternative approaches to risk management, and to observe the current trend in the space industry.

[1] Pickard, Lowe and Garrick Inc., 2260 University Drive, Newport Beach, California 92660.

NASA'S APPROACH TO RISK AND SAFETY ANALYSIS

Exhaustive design reviews, detailed analyses, and extensive acceptance and qualification testing are elements that are characteristic of the space vehicle development process. To facilitate this process, NASA relies on qualitative FMEA and hazard analysis (HA) as the backbone of their risk and safety analysis process.

FMEAs are hardware oriented and consist of assuming individual component failure modes and assessing worst case effects.[1] FMEAs are performed on all space transportation system (STS) flight hardware as well as ground support equipment, which interfaces with flight hardware at the launch sites to identify hardware items that are critical to the performance and safety of the vehicle and the mission and to identify items that do not meet design requirements. Theoretically, all component failure modes are identified through the FMEA "bottom-up" process, in which a single component failure and its effect on a particular subsystem, subsystem interface, and overall flight system is determined. The process of conducting the FMEA includes the following:

- Defining the system and its performance requirements.
- Specifying the assumptions and ground rules to be used in the analysis.
- Developing block diagrams or other simple models of the system.
- Devising an analysis worksheet and completing it for every identified failure mode. Effects documented on the worksheet address the worst case.
- Recommending and evaluating corrective actions and design improvements.

0272-4332/89/0300-0001$06.00/1

From the FMEA failure mode and "worst case" effect identification, a critical items list (CIL) is constructed. This list summarizes single point failures and failures of redundant elements that do not meet certain design or redundancy fail-operational/fail-safe requirements. For example, before the shuttle can fly, critical items with these failure modes must be subjected to design improvements or to corrective action to meet redundancy requirements. If corrective actions are not feasible, a waiver request must be submitted to NASA management to present the rationale for retaining such an item. Types of data included in this "retention rationale" are design, test, inspection, failure history, and operational experience. An approved waiver must support the decision to accept the risk represented by the critical item and ensure that maintenance, test, or inspection procedures will minimize the potential for the failure to occur. Rejected critical items are fixed.

CILs are ranked qualitatively by consequence importance as Criticality 1, 1R, 2, 2R, or 3, as shown in Table I.[1] In contrast to the FMEA/CIL process of identifying particular failure modes and effects, the HA process consists of identifying undesired events, hazardous conditions, or accident scenarios and systematically identifying hazard causes, effects, and recommended corrective actions. HA utilizes the failure modes and associated data developed in the FMEA process. In addition, the HA "top down" approach goes beyond the hardware and addresses software requirements, coding errors, environmental impacts on operations, crew errors, and procedural anomalies for each of the accident scenarios. The HA used by NASA evolves during the conceptual, design, testing, and operational phases of space vehicle development leading to four primary types of hazards analyses. In addition, fault tree analysis, sneak analysis, software analysis, and mission safety assessments supplement the four primary types of hazards analyses. Details of these analyses can be found in Ref. 2.

Table I. Criticality Ranking

Criticality category	Potential effect of failure
1	Loss of life or vehicle
1R	Redundant hardware element failure that could cause loss of life or vehicle
2	Loss of mission
2R	Redundant hardware element failure that could cause loss of mission
3	All others

Each of the four primary types of hazard analyses performs the same function of hazard identification. Analyses differ depending on the stage of vehicle development. Each type of HA report documents each hazard condition, hazard cause, hazard effect, hazard level (e.g., catastrophic or critical), safety requirements (those measures for preventing a hazardous condition), and hazard control (documentation of the methods to eliminate, control, or accept hazards). A hazard is said to be "eliminated" when its source has been removed. A "controlled hazard" is one that has been effectively controlled by a design change, the addition of safety or warning devices, procedural changes, or operational constraints. Any hazard that cannot feasibly be eliminated or controlled by these means is termed an "accepted risk."

NASA's HA technique represents a very good start toward a risk assessment process that addresses the concerns of the critics. These concerns, as discussed in the next section, center around the absence of an integrated and quantitative approach to risk assessment resulting in the inability to put safety issues into perspective. HA contains in it some of the ideas of the scenario-based approach to risk assessment.[(3)2]

HA, in principle at least, addresses both scenarios and consequences, only falling short of being quantitative by not responding to the likelihood question. As we shall see, however, there are some completeness deficiencies in the HA approach to structuring the scenarios.

The point is that NASA's HA technique is the most attractive of all their methods for being logically extended to embrace the ideas of quantitative risk assessment. In fact, NASA is examining this possibility by conducting a study[(4)] on how HA may be enhanced to better address the issue of quantification and common cause and multiple failures. The enhancements for HA to make this transition appear to be as follows:

- The need to structure scenarios in a more detailed and systematic way to achieve improved scenario completeness, especially with respect to a more

[2] The scenario-based approach to risk assessment starts with defining risk as the answer to three basic questions: (1) What can go wrong? (2) What is the likelihood? and (3) What are the consequences? The "what can go wrong" question is answered by a structured set of scenarios that is so defined as to represent all the threat possibilities of the system being assessed. Depending on the complexity of the system involved, a complete set of scenarios may number in the thousands or even millions. Of course, as noted in Ref. 3, when we refer to scenarios, we are really referring to classes or categories of scenarios rather than to scenarios involving pieces, parts, and microevents. Generally, it is a manageable number of scenarios that dominate the risk.

detailed linking of initiating failures to the final, undesired damage state.

- The need to assess the likelihood of the scenarios; i.e., the frequencies of the scenarios should be quantified rather than simply tagged as "unlikely," "likely," or "highly probable", as is currently done in an HA.
- The need to collect, organize, and process all the evidence and experience relevant to the scenario frequency so that the lessons and conclusions can be drawn in an orderly fashion for all to see.

Having addressed a possible response to the critics, let us now back up and review more specifically what the critics are saying.

REVIEW OF NASA'S RISK MANAGEMENT PROCESS

As a result of the Challenger accident on January 28, 1986, a presidential commission, the Rogers Commission, was established to review circumstances surrounding the accident and to develop recommendations for corrective actions that would return the space shuttle program to operating status. Among the recommendations of the Rogers Commission[5] was to further review NASA's safety and hazard analysis process. As a result and at the request of Dr. James C. Fletcher, NASA's Administrator, the National Academy of Sciences, through the National Research Council, organized a Committee on Shuttle Criticality Review and Hazard Analysis Audit.[6][3] In addition, the House of Representatives Committee on Science and Technology conducted a comprehensive investigation into the cause of the accident.[7] From a risk management perspective, the reports of these three committees describe NASA's current risk management practices and present recommended actions to NASA to ensure the reliability and safety of future missions.

One perceived weakness of NASA's current risk management process is that all Criticality 1 and 1R items are formally treated equally even though many differ substantially from each other in terms of the probability of failure or malperformance and in terms of the potential for the worst-case effects postulated in the FMEA. As a result, NASA cannot efficiently allocate its resources to correct those items that are most important for mission success.

[3] The author served on this committee from its inception until February 19, 1987.

The Congressional Report stated:

> The Committee finds the FMEA to be an appropriate method for identifying the Critical 1 and 1R elements of the NSTS; however, not all elements so identified pose an equal threat. Without some means of estimating the probability of failure of the various elements, it is not clear how NASA can focus its attention and resources as effectively as possible on the most critical systems.[4]

The Congressional Report summarizes the weakness of the current NASA risk and safety program: "Top NASA managers lack a clear understanding of risk management." When asked what risk management meant, Fletcher stated in the report

> Well, risk management is a pretty generic term. Risk management is decided in headquarters in terms of what are the chances of an overall failure of a system under a given set of circumstances. When you get down to the flight team, the launch crew in those last several hours or couple of days, risk management is an entirely different thing. They have to look at the factors that have come up just before launch and assess whether this is a risk we want to take. This is a judgment question; you can't make calculations at this point.

What this seems to boil down to is NASA questioning whether or not quantitative methods of risk assessment have a role to play in launch decision making, especially "just before launch." To be sure Fletcher is correct in that the decision to launch is a judgment question; that is exactly why quantitative information is so valuable and necessary—it provides the decision maker with the best information from which a decision can be made! Best because, at least in the sense used here, the information is cast in a form to convey the analysts' confidence in the results. The quantitative language of confidence, or conversely of uncertainty, is probability—at least the concept of probability advocated here. For example, did the launch team of the Challenger have quantitative statements of confidence on such issues as solid rocket booster joint integrity as a function of such phenomena as outside temperature? Certainly, the technical knowledge of the launch team would have been greatly enhanced had they been able to study on the spot a probability versus temperature curve as is shown in Fig. 1. To be able to see in black and white just how the experts think the probability increases with decreasing outside temperature would have been a very valuable piece of evidence in the decision-making process. The outcome may have been the same, but the decision basis would certainly have been more scientifically founded and more easily defended. With respect to launch deci-

[4] It should be noted that in the meantime NASA has come forward with schemes for prioritizing criticality items. While none of the schemes involve a direct use of quantitative risk assessment (QRA), they do move in the direction of making "likelihood" judgments.

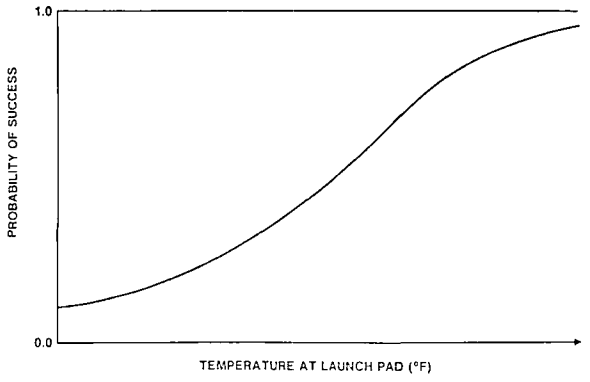

Fig. 1.

sions, the congressional committee review recommended that NASA establish rigorous procedures for identifying and documenting launch constraints. This recommendation was made based on findings that

> There is no clear understanding or agreement among the various levels of NASA management as to what constitutes a launch constraint or the process for imposing and waiving constraints. Launch constraints were often waived after developing a rationale for accepting the problem rather than correcting the problem; moreover, this rationale was not always based on sound engineering or scientific principles.

The "waiver" process mentioned in this recommendation is found throughout the risk management process of NASA. As discussed earlier, waivers are used, along with retention rationale, to reject or accept risks associated with inadequate designs, hazardous conditions, etc. Prior to the launch of the Discovery space shuttle on September 29, 1988, NASA reviewed over 4,600 Criticality 1/1R items, of which more than 2,100 were waived by the Program Requirements Control Board. Many of these items have waivers permitting flight of critical items. Both the congressional and National Research Council (NRC) reports made similar conclusions with respect to NASA's overall waiver process as it is used for risk management. The NRC committee stated

> The Committee views the NASA CIL waiver decision-making process as being subjective with little in the way of formal and consistent criteria for approval or rejection of waivers. Waiver decisions appear to be driven almost exclusively by the design-based FMEA/CIL retention rationale rather than being based on an integrated assessment of ALL inputs to risk management. The retention rationales appear biased toward proving that the design is "safe," sometimes ignoring significant evidence to the contrary.

From these and similar findings regarding the subjectivity of NASA's risk management process, the NRC committee strongly recommended that formal risk management procedures, including prioritization of Criticality 1 and 1R items, be adopted by NASA and that QRA be used as the primary basis for retention or rejection of hazards and critical items. The NRC committee stated, "Criticality 1 and 1R items should be assigned priorities based on the probability of occurrence." In response to committee suggestions NASA stated

> An effort is underway to assess the utility of probabilistic risk assessment in the NSTS FMEA/CIL process. Activities have been initiated to engage two independent firms with expertise in probabilistic risk assessment to perform detailed reviews of the orbiter auxiliary power unit and the shuttle main propulsion pressurization system.

Both of these pilot probabilistic risk assessment (PRA) studies were completed about December 1987. One of the studies involved Pickard, Lowe and Garrick, Inc. (PLG), and is briefly discussed in the next section.

SPACE SHUTTLE PROOF-OF-CONCEPT APU/HPU PROBABILISTIC RISK ASSESSMENT

The space shuttle orbiter auxiliary power units (APUs)[5] were one of the subsystems selected by NASA for pilot testing the PRA concept. The APU provides shaft power to the hydraulic pump critical to such orbiter functions as flight control surfaces, main engine gimbaling, and landing gear deployment. The APUs (there are three redundant units, two of which are generally required to operate) are one of some 26 subsystems that make up the orbiter.

The PRA of the APU was performed by a team of McDonnell Douglas Astronautics Company (MDAC) and PLG personnel.[8] The processes and methodologies used to perform the study were based upon the PRA techniques discussed in detail in Refs. 3 and 8.

Highlights of the steps taken in the PRA were as follows:

- A careful scoping of the problem to be clear on the purpose of the PRA, which was first and foremost to demonstrate the PRA concept while carrying out a limited amount of technology transfer to NASA. A secondary purpose was to give perspective to the role of the APUs and HPUs in terms of their contribution to the risk of delaying or scrubbing the launch or damaging or losing the space shuttle following launch.
- A detailed review of APU operating modes, failure modes, failure rates, crew interactions, sys-

[5] The solid rocket booster hydraulic power units (HPUs) were also included in this analysis but are not discussed here.

tem interactions, operating profiles, testing, maintenance, design changes, refurbishment activities, and environmental conditions.

- The development of initiating failure categories, definition of damage states, and the structuring of scenarios to be assigned to damage states.
- A quantification of the frequency of occurrence of scenarios, specific events, and different damage states varying from scrubbing the launch to losing the space vehicle.
- Importance ranking, by frequency and consequence, of scenarios contributing to risk as a function of the individual mission phases (ascent, orbit, entry, etc.) and for the entire mission.

The APU and the chance of loss of vehicle (LOV) caused by APU mishaps were calculated to be driven by leakage of hydrazine fuel. The dominant scenario was hydrazine fuel leakage downstream of fuel isolation valves and into the aft compartment during orbit or entry leading to failure of two APUs or flight critical equipment. This single scenario category represents over 39% of the LOV risk due to APU failures.

It turns out that the NASA techniques of FMEA and HA identified hydrazine leaks as important matters of safety. Therefore, in terms of initiating failures (such as fuel leaks) and possible consequences that may occur (such as loss of vehicle), the PRA offered nothing new. However, with respect to the question of the likelihood of a specific consequence and the details and frequencies of the scenarios important to APU failure and possible LOV, only the PRA was able to provide these important results. In the APU pilot study, another important result came out of the PRA that was not extractable from the FMEA and HA analyses, and that is an identification and quantification of the contribution of common cause and multiple failures to risk.[6]

For example, a substantial fraction of the APU/LOV risk, approximately 27%, involved a common cause hydrazine leak from at least two APUs simultaneously (two of three APUs are needed to have high confidence in a successful entry). The leakage location was identified as downstream of the fuel isolation valve and into the aft compartment where the APUs are located. The leaks are envisioned to occur during orbit or entry.

A key point is that for important contributors to risk the PRA identified failure modes at a finer level of detail than the comparable FMEAs. For example, the APU PRA identified hydrazine leakage from a fuel pump as the third highest risk-ranked failure mode. The FMEA, however, identified fuel pump failure as an all-encompassing failure mode with no importance ranking. For items that were calculated to be relatively unimportant to risk, the PRA sometimes identified failure modes at a coarser level of detail than the FMEAs. This was the case, for example, in describing heater failure modes.

The MDAC/PLG PRA analysis had characteristics not typical of most modern PRAs. First, the study was a phased analysis; the system that was analyzed changed operating modes depending on the mission phase (ascent, orbit, entry, etc.) and the system external environment also changed with mission phase. Second, unlike many PRAs, the study found that a substantial data base existed with respect to components and systems. Based on what had been heard about the lack of data at NASA, this was a pleasant surprise and needs a brief explanation.

Insufficient data is the most common reason given for not wanting to do a PRA. There are two important points to be made here. The first is that PRA is not dependent on the availability of so-called "statistical quality data." In fact, it should be said that the more limited the data, the more important it is to quantify the risk. The key thought here relates to what is meant by quantification. Briefly, what is meant is a statement as scientifically based as is practical of the confidence that the analyst has in the parameter chosen to convey risk (such as the frequency of LOV, or scrubbing a mission, etc.). The format often utilized[3] is the "probability of frequency" idea; that is, the frequency of occurrence of an event or scenario, or specific failure is embedded in a probability distribution as a means of communicating confidence. A narrow curve conveys high confidence while a wide or broad curve conveys low confidence when utilizing appropriate scales. Thus, a systematic, deliberate, and technically based indication of confidence is the true manifestation of quantification. Of course, the greater the lack of confidence, the more important it is to know about it. Quantification in the sense of expressing an analyst's state of knowledge is therefore always possible.

The second point has to do with proper use of data. Data from different sources have to be evaluated and logically combined. No relevant data should be ignored. In this regard, careful consideration must be given to success data—as the best situation of all is where no failures occur. The data methods must accommodate a proper consideration of all evidence of system failure or success including the implications on data of specific

[6] A common cause failure involves a cause, such as a material flaw in a component common to otherwise redundant systems that can result in multiple failures. Another form of a common cause failure would be an event such as a fire or an external force that could initiate multiple failures.

fixes. The use of Bayes' theorem[9] as the fundamental rule for the treatment of data is one approach that has been successfully applied in many PRAs including the one performed on the APU.

NASA's large "success" data base and smaller failure data base combine to provide the space program with a data base more extensive and complete than the data bases characteristic of PRAs performed in other industries such as the nuclear power or chemical process industries.

In general, the MDAC/PLG study indicated that PRA could be very useful as input to NASA's risk management process. The weakness of the current qualitative analysis techniques used by NASA is that they do not account for the ordering of failures with respect to importance to risk. The FMEA and HA approaches that NASA currently uses do not account for cascading and multiple failures. The APU PRA found that cascading and multiple failures were the most important contributors to risk—far greater than would be expected if the APUs were failing as independent and redundant systems. Redundancy effectiveness is limited in the APUs because the highest-ranking contributor to risk was calculated to be leakage-induced hydrazine damage; more APUs simply mean more leakage sources. While redundancy is a recognized safety improvement technique in many instances, it does not increase safety against all failure modes. The PRA clearly identified this problem and supported the result with shuttle data and sound engineering judgment.

NASA'S CURRENT RISK MANAGEMENT GOALS

Difficulties in implementing comprehensive and quantitative approaches to risk management are believed to be more institutional or cultural than they are technical. While it is clear from examples, especially in the nuclear industry, that quantitative risk management is a viable, technical discipline, NASA has been hesitant to move toward quantification quickly. Nevertheless, progress toward a comprehensive risk management program has been made.

On February 3, 1988, Fletcher released NASA's Risk Management Policy for Manned Flight Programs.[10] Essentially, this policy reinforced NASA's commitment to the qualitative FMEA and HA techniques by stating, "It is expected that qualitative risk assessments will be appropriate for most elements of NASA programs." Fortunately, the policy did open the door for future QRAs: "development of quantitative risk assessment methodology and associated data base requirements for application to future manned flight systems is a NASA objective." However, with respect to current NASA programs, quantitative risk management is treated as an option that may or may not be included depending on "subjective ratings of the frequencies and severities of mishaps that potentially can arise from hazards."

NASA's progress in reassessing its risk management program and openly considering the implementation of quantitative risk management is a positive sign. All members of NASA and the PRA community have the same goal—to provide the United States with a safe and reliable space program. Hopefully, through the NASA documents following NMI 8070.4, a PRA-based risk assessment methodology will become a viable element of NASA's risk management program.

SUMMARY AND CONCLUSION

Safety has always been a prime consideration in the design, manufacturing, and operation of all types of aerospace systems. Few industries have been as sensitive to the need to design safety into their systems as has the aerospace industry. The only other industry that has a similar consciousness level for risk and safety is probably nuclear power. These happen to be the two industries that have contributed the most to making risk and safety analysis an applied science.

In the 1950s and early 1960s, the aerospace and defense industry had the lead in the technology of systems safety analysis. The initiative was then taken over by the nuclear industry, which was under great pressure to demonstrate to the public the safety of nuclear power plants. Just when NASA decided not to utilize probabilistic assessments as a major element of their safety assurance activities, the nuclear industry saw such techniques as perhaps the answer to how to give perspective to the risk of nuclear power. Thus, beginning in about 1966, most of the advances in probabilistic risk assessment, or as some prefer, quantitative risk assessment, were coming from the nuclear safety field. Today, NASA, also under some public pressure, especially since the Challenger accident, is taking another look at their approach to risk and safety analysis, including a look at the advances that have been made in the use of quantitative risk assessment.

It is clear that even after backing off from the extensive use of probabilistic methods beginning in the early 1960s, NASA and the rest of the aerospace industry did not back off from emphasizing safety in the design and operation of their aerospace systems. In fact,

they continued to push what they labeled as the assurance sciences—reliability, maintainability, safety, availability, quality control/assurance, etc. It might even be observed that the assurance sciences became so involved and expansive in scope that it was difficult to see how they all interconnected. It is believed that this is, in fact, the kernel of the problem; namely, that the assurance sciences lost their connectivity to each other in relation to the overall matter of risk management and control. It is also believed that the key technology for providing this integration and for interpreting the results is the technology of contemporary quantitative risk assessment.

NASA is taking steps to upgrade their overall approach to risk management. Among the actions being taken is to experiment with different risk and safety analysis techniques, including quantitative risk assessment. They have not yet committed to quantitative methods, but they have opened the door and are moving in the right direction.

ACKNOWLEDGMENTS

The author wishes to acknowledge the assistance of Stan Kaplan, Brian A. Fagan, and Michael V. Frank of Pickard, Lowe and Garrick, Inc., for providing source material and a review of the paper.

REFERENCES

1. National Aeronautics and Space Administration, "Instructions for Preparation of Failure Modes and Effects Analysis (FMEA) and Critical Items List (CIL)," NSTS 22206, October 10, 1986.
2. National Aeronautics and Space Administration, "Instructions for Preparation of Hazard Analysis, Preliminary," NSTS 22254, December 1986.
3. S. Kaplan and B. John Garrick, "On the Quantitative Definition of Risk," *Risk Analysis*, **1**, 11–27 (1981).
4. M. V. Frank, S. Kaplan, and B. J. Garrick, "Enhanced Hazard Analysis for Space Systems," prepared for Vitro Corporation, PLG-0665. (This work is sponsored by NASA and is expected to be published in December 1988.)
5. Presidential Commission on the Space Shuttle Challenger Accident, "Report to the President," Appendix D, June 6, 1986.
6. National Research Council, Aeronautics and Space Engineering Board, Committee on Shuttle Criticality Review and Hazard Analysis Audit, "Post-Challenger Evaluation of Space Shuttle Risk Assessment and Management," January 1988.
7. Committee on Science and Technology, U.S. House of Representatives, "Investigation of the Challenger Accident," Ninety-Ninth Congress, October 29, 1986.
8. McDonnell Douglas Astronautics Company, Engineering Services, "Shuttle Probabilistic Risk Assessment Proof-of-Concept Study," Working Paper No. 1.0-WP-VA88004-1, December 18, 1987.
9. S. Kaplan, "On a Two-Stage Bayesian Procedure for Determining Failure Rates from Experiential Data," PLG-0191, *IEEE Transactions on Power Apparatus and Systems*, **PAS-102**, No. 1, (1983).
10. National Aeronautics and Space Administration, "Risk Management Policy for Manned Flight Programs," Management Instruction, NMI 8070.4, February 3, 1988.