

View Through the Door of the SOFIA Project

Michael V. Frank • Safety Factor Associates, Inc. • Encinitas

Key Words: Aircraft, Reliability, Lessons learned, FMECA, Design for reliability, Robust Design

SUMMARY & CONCLUSIONS

The National Aeronautics and Space Administration (NASA) and Deutsches Zentrum Für Luft- und Raumfahrt (DLR) e.V. are working together to create a Stratospheric Observatory for Infrared Astronomy (SOFIA). One of the key elements of the modification of the Boeing 747-SP aircraft to be used is a new door system. It protects the 2.5 meter infrared telescope during flight by covering the aircraft cavity within which the telescope resides and it follows the telescopes motion to provided an unvignetted view of the sky while reducing turbulence inside the cavity. This paper describes the value added by a productive interaction of reliability engineering with the integrated product design team at NASA Ames Research Center that was responsible for design of this “cavity door” system; It points out key reliability improvement strategies applied to the cavity door system and offers a few principles to guide interaction of reliability engineers with a design team. It is shown, for example, that significant assistance to improve reliability is achievable with a thorough and detailed understanding of the system’s intent and an organized approach to how it might fail to carry-out its intent.

1. INTRODUCTION

The intent of this paper is to describe the positive interaction involving the practical use of reliability engineering principles. This is exemplified by the author’s experience working with the SOFIA project’s cavity door design team at NASA Ames Research Center. The purpose of the SOFIA project is to design and construct a 2.5 meter reflecting telescope that will fly within a specially modified Boeing 747-SP aircraft. The DLR is primarily responsible for the telescope and NASA is primarily responsible for the aircraft and operating facilities. The aircraft will be based at NASA’s Ames Research Center at Moffett Federal Airfield near Mountain View, California, and it is expected to begin flying in the year 2001. Figure 1 shows the general concept.

Aircraft are particularly well-suited for infrared astronomy. Because much infrared radiation is absorbed by atmospheric water vapor, ground-based observations are limited to certain wavelength bands. Satellite-based telescopes, while able to observe all infrared bands, are relatively expensive and short-lived. When carried to 41,000 feet and above, airborne telescopes are above 99% of the atmospheric water vapor and thus have virtually unrestricted access to infrared wavelengths. The cost of operating and the ease of maintenance and upgrade of an airborne telescope is lower than that of orbiting spacecraft. In addition, repairs can



Figure 1. SOFIA Concept

be made, and instruments and other technologies can be easily upgraded.

A Boeing 747-SP aircraft will be modified by moving the pressure boundary forward in order to create an aft cavity large enough to accommodate the 20,000 kg telescope. During its mission, the aft cavity and telescope will be exposed to the environment at 41,000 feet (13,226 meters) via a large opening cut into the left side of the aircraft aft of the wing. In order to protect the telescope, minimize the impact of the opening on the aircraft’s flight characteristics, and ease take-off and landing, a cavity door system is being designed at NASA Ames Research Center.

2. OVERVIEW OF THE CAVITY DOOR SYSTEM

An overview of the door system is shown in Figure 2. The cavity door system has three objectives:

- Close the opening when the telescope is not in use in order to reduce the impact of flight transients and decrease telescope degradation by contaminants and moisture, particularly during take-off and landing.
- Seal the opening when the door is closed in order to decrease thermal transients and water vapor ingress. Before take-off, the temperature in the cavity will be artificially and slowly reduced to -50°C , via introduction of cold nitrogen gas to minimize the thermal shock of sudden exposure it to this temperature at altitude. During landings the cavity temperature will be allowed to slowly rise.
- Decrease the turbulent flow of air around the telescope when it is in use. This is obviously important in that the telescope must meet stringent motion requirements relative to the target sources (e.g., stars).

As illustrated in Figure 2, the cavity door system will achieve these objectives using two doors, an upper rigid panel assembly (URP) and a flex aero skirt assembly (FAS), with an imbedded shear layer control ramp (SLC). The FAS is bolted directly to the SLC. Forward of the cavity is a fairing

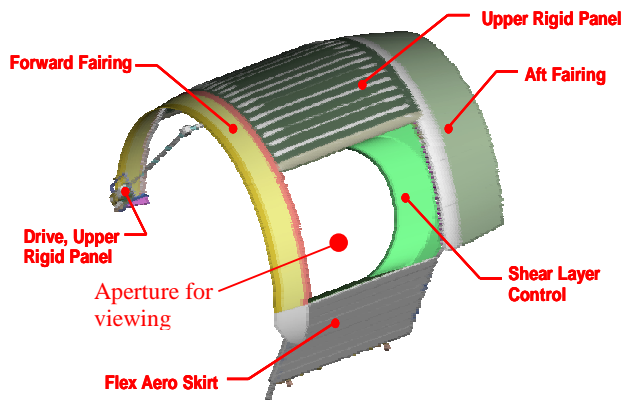


Fig. 2 Cavity Door Concept

to lift the airstream away from the fuselage skin. The shear layer control ramp captures the stream before it can penetrate too far into the cavity and again lifts it to the aft fairing. The outer skin of the URP is the same radius from the aircraft centerline as the fairings. The FAS is an inner, paneled, flexible door which is at the same radius as the original aircraft fuselage.

The summary block diagram of Figure 3 shows that the system is made up of two doors with associated servo-motors, transmissions, a door seal system, the fairings, the shear layer control ramp, and door controller subsystem. The easiest visualization analogy of the URP is a stiff but curved garage door. The analogy of the FAS is more like a common garage door with hinged panels that allow it to move on curved tracks. Each door subsystem includes the door structure, tracks built into the aircraft fuselage or fairings, roller assemblies attached to the doors, and a DC electric motor with integrated brake. Motive force is transmitted to a rack mounted on each door via shafts, gear box and a pinion gear. Each motor is powered using a DC power supply and servo-amplifier.

The motion of both doors is synchronized by servo-controllers commanded by a VersaModule Eurocard (VME) board cavity control system. The doors in turn are synchronized to the motion of the telescope such that the telescope remains approximately centered within the gap, called an aperture, between the two doors. Using the roller assemblies, the doors will move along tracks. During operation of the telescope, the motion of both doors will be circumferential around the fuselage. The aperture is driven from 20° to 60° elevation above the aircraft left horizon to provide the telescope with unvignetted view while minimizing the opening.

High availability of the door is important to the overall goal of the mission which is to achieve approximately 1000 successful hours of astronomy per year during 160 flights. Door failure to open would prevent any science from being conducted during a flight. Door failure in any position during active observations using the telescope would vignette the view. Door failure in the open position also places the telescope itself in a less than ideal environment exposing it to unwanted moisture, contamination and thermal stresses.

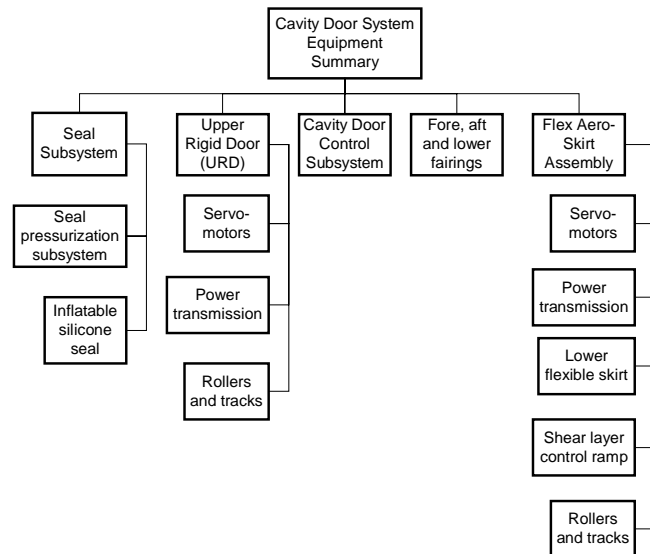


Fig. 3 Cavity Door System Simplified Block Diagram
3. ROLE OF A RELIABILITY ENGINEER

I was introduced to this project at an early stage of design of the cavity door system so that reliability improvement strategies could be implemented with relative ease. My role was not just to perform reliability analysis but to apply practical principles of reliability to improve the cavity door system design. The intent of this paper is to describe the interaction with the design team, to point out key reliability improvement strategies applied to the cavity door system, and to offer a few principles to guide interaction of reliability engineers with a design team. The specifics of the analyses performed are briefly summarized below. However, rather than go over the details of the reliability analyses, this paper emphasizes the key insights into the reliability of the system.

The design team has been very receptive to the results of the iterative reliability analyses as the design has progressed and to the reliability improvement suggestions that emerged from the analyses. A failure mode effects and criticality analysis (FMECA) as specified by MIL-STD-1629A was required by project specifications (Ref. 2). The overall reliability, as expressed in a variety of ways (e.g., mean time between failures (MTBF)), was also developed to compare with its design-to top-down allocation. Criticality was assessed using failure rates developed from a variety of data sources (Refs. 3 – 11) as well as a limited amount of data directly from component manufacturers. Because this is a predictive analysis for a unique overall application and environment, there would obviously be uncertainty in any prediction. Therefore, the likely range of applicable failure rates were developed as probability distributions, although only point estimate representations are presented in this paper.

One of the interesting aspects of working on this project was the juxtaposition of mechanical, relatively low technology hardware such as rollers, bearings, motors and transmissions, with digital control system technology. The design team is particularly adept at melding computer simulations, structural calculations, and subsystem tests to assure that this juxtaposition is done seamlessly.

Two rounds of analyses were conducted. The first was during the preliminary design process and the second was during the months leading up to the critical design review. The details of these analyses are not as important as the insights into the strengths and weaknesses of the design thereby obtained and the subsequent discussions with the design team. I met four times with the design team as a whole to present and discuss these insights. For their part, the team very carefully reviewed the work and modified the designs to compensate for the weaknesses.

4. ROUND 1: INSIGHTS ABOUT THE PRELIMINARY DESIGN

To begin the interaction, we scheduled a meeting so that the designers could explain the design intent in detail. Before the meeting, I studied a large package of drawings and stress calculations. I was, therefore, able to ask questions of clarification and make comments about the design. While designers are concerned with how to get the design to work, the orientation of this analyst is to think in terms of “what would happen if”.

Figure 3 shows a simplified equipment hierarchy noting the major equipment groups. The depth and detail of the FMECA followed the development of the design. Therefore, this round was not as detailed as the next round. The FMECA was reviewed by the designers to determine if the interpretation of their design was accurate. We then met to go over the FMECA in detail at which time the discussion revolved around what I considered to be the major insights derived from performing the FMECA. In deriving major insights, the criticality analysis was used to screen out very low probability failure modes.

The preliminary FMECA predicted that there would be several system failures per year (an MTBF less than 100 hours¹) with the original design as I had received it. The system failures were driven by the following design and operational aspects:

- Two brushless DC motor and drive trains, one for the upper rigid panel and one for the flex aero skirt, provide power to move the URP and FAS on rollers. The combination of contamination, icing, and moisture ingress within the rollers and tracks would add to the required motor torque and might cause large, unanticipated peak motor current requirements. Furthermore, differential thermal expansion among the airframe/fairings, tracks and panels would add to this torque. In addition, the motor for the flex aero skirt is in an unpressurized aircraft compartment exposed to large temperature extremes (-70°C to 40°C).
- Each motor requires a servo-amplifier which is not as reliable as the motor itself.

¹ Please note that all MTBF values quoted in this paper are mechanical and electrical equipment only. Human errors, software errors, and failure of structural members were not in the quantitative reliability estimates.

- The stress analyses revealed the potential for large local thrust stresses (along the roller axis of rotation) on the roller bearings as well as scuffing associated with fore-aft door vibration and small top to bottom door deformations. This, coupled with some of the environmental and thermal expansion factors noted above, would cause a dramatic increase in bearing failure rates. Although the designers had thought of lubricants that would withstand the required temperature variations, it was not clear that the bearing cage material was correctly specified for these conditions.
- The door contains an inflatable silicone/nomex seal that seals the interface between the upper rigid panel and the airframe. The seal is inflated when the door is closed on the ground and deflated before the door is opened. As indicated in Figure 4, the fill solenoid valve does not fail in the operational position (open) to assure a pressurized seal. It fails closed instead. Another problem is that a human error during fill operations on the ground could leave the pressurization hand valve open. These hand valves are not accessible during flight. Therefore, when the exhaust solenoid valve is opened to open the door for scientific observations, the pressure supply bottle will drain and the seal could not be re-established after observations are completed.
- Other reliability concerns involved interference with rollers by loose bracket bolts, and tearing or erosion of the inflatable seal.
- Although not a reliability concern because of low probability, failure of either the brakes or power transmission could allow the upper rigid panel to “runaway” into the lower fairing damaging the air frame. Because damage to the airframe is a flight safety issue, this kind of event must be mitigated.
- Similarly, a gap between the bottom of the upper rigid panel and the top of the shear layer control ramp (bolted to the flex aero skirt) is an untested flight configuration. Therefore, it is to be avoided. This was not a system reliability concern because other failures would have to occur before the configuration would be such that the latch was needed.

We discussed several reliability improvement strategies at the meeting. These were:

1. Place the flex aero skirt motor inside of an insulated compartment to mitigate the temperature extremes associated with exposure to the high altitude environment.
2. Provide for ‘graceful degradation’ of the motor by specifying a torque requirement far in excess of nominal that would accommodate roller failures.
3. Provide for graceful degradation of rollers by compensating for thrust loads, door vibrations, icing, and crud/contaminant build-up.
4. Motor should be provided with a thermal overload trip that can be reset from the control panel. Furthermore, to preserve the motors, controller logic should include a motor trip if the door fails to move x inches in y seconds (i.e., rate trip or time-out trip).

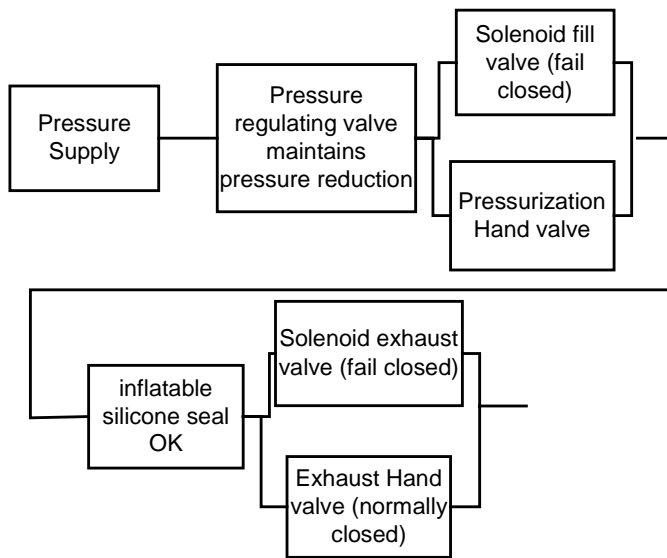


Fig.4 Preliminary Seal Pressurization Subsystem

5. Specify sealed bearings to minimize water ingress. Water ingress degrades the effectiveness of the lubricant and increases internal corrosion and wear.
6. Make sure that the roller bearing cage is specified for a material that does not become brittle in a low temperature environment and does not become too soft at the high end of the temperature environment. Typically, a type of brass is used for this kind of application.
7. Control logic should be made fail-safe such that failure of the flex door or its motor automatically triggers closure of the upper rigid door.
8. Limit switches to shut off power to the motor should be provided at the ends of motion. This was suggested to address the concern of a fault in the logic or other spurious control failure that might attempt to drive the doors beyond the end of the tracks. This is a variation on the “runaway” door scenario.
9. Use locked (e.g., wired) bolts, and redesign roller brackets to minimize the number of bolts that can interfere with roller motion.
10. Require frequent inspections of the silicone/nomex seal.
11. Develop a passive, rubberized hard stop instead of the active upper rigid panel latch mechanism.

To give the design team a perspective on the effectiveness of these measures, I modified the FMECA to account for these suggestions. The overall MTBF of the system increased from an original estimate of under 100 hours to 1500 hours, or a failure approximately once every 1.5 years of operation. This was greater than the allocated reliability requirement.

5. ROUND 2: RELIABILITY INSIGHTS AFTER RE-DESIGN

Because of project difficulties having nothing to do with reliability, my next interaction with the design team was about one year later as which time the design was a great deal more detailed. The control system and logic were specified and several structural and mechanical modifications had been

made. The seal pressurization system had been completely redesigned. The original FMECA was used by the control system engineers to help in placing instrumentation in the seal pressurization subsystem and in developing diagnostic warnings and alarms for the door control system. They found that the alarms, warnings and trips could be designed to include all the failure modes provided by the FMECA.

How had the designers actually responded to the list of important system failures and reliability improvement strategies? What is the reliability of the current system and where might the reliability and availability be further improved?

To answer the first question, the following design improvements, important to reliability, were made:

1. The flex aero skirt motor is now in a thermal compartment.
2. The design is now now for forgiving (or robust) because the specified peak motor torque is far higher than that expected in normal operation. The design team estimated that the doors would be able to close with one or two failed (i.e., frozen) rollers.
3. It has the quality of graceful degradation with respect to the increased friction offered by the natural aging of rollers and bearings.
4. As indicated in Figure 5, pressure and flow instrumentation are placed in the seal pressurization subsystem such that identified failure modes would be detected and diagnosed. The fill solenoid valve is now correctly designed to fail in the open position and the pressurization hand valve is in series and normally open.
5. Both thermal protection and door motion time-out protection were provided as well as numerous other alarms that would indicate abnormal behavior.
6. A hard stop was substituted for the upper rigid panel catch latch.
7. The track and rollers were redesigned such that axial rollers (with axis perpendicular to the rollers that support the door) were added to take up the thrust loads. The roller brackets were redesigned to allow for differential fore-aft motion between the aircraft fuselage and flex aero skirt. The bearing cage material was verified to be adequate.
8. The power transmission system has a breakaway clutch that slips if it experiences a torque higher than the motor can deliver but lower than the failure stress of the shaft. However, end-of-motion limit switches, snubbers, and capture latches were provided so that the runaway door scenario is no longer a flight safety issue.
9. The roller bracket assemblies and the tracks are fastened with locked bolts. However, the number of bolts that might interfere with motion was not appreciably reduced.
10. A manual closure mechanism was added so that the upper rigid panel could be closed upon loss of power.
11. Bearings were specified to handle much greater stresses and a much more aggressive duty cycle than is required. As a result, the potential for premature bearing failures have been reduced and are not a driver for unreliability. However, the bearings are not of the sealed variety and, therefore, still subject to degradation from moisture ingress.

In summary, nearly all of the suggested reliability improvement strategies were implemented. To answer the second question above, the FMECA was updated to include the new design features in addition to the far more detailed list

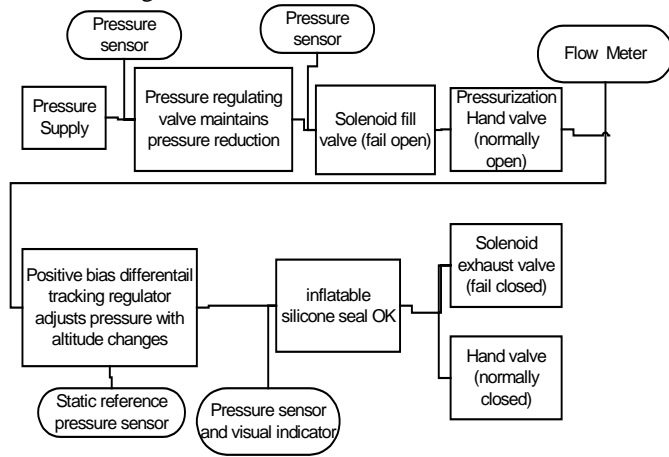


Fig. 5 Redesigned Pressurization Subsystem

of components that was available. This was also reviewed and discussed in detail. A new system MTBF was calculated to be 1890 hours, or approximately two years of operation, which is well above the specified allocation for this system. Table 1 shows a summary distribution of the MTBF by major equipment groups. Note that the group with lowest reliability is the door motion instrumentation and control and electrical power equipment. This is because the VME processor based control system and the electrical system are single string. The least reliable components are predicted to be servo-amplifiers and their power supply units, power distribution units, and the ethernet communications. If these were made redundant, the MTBF would nearly double to about 3500 hours or approximately 3.5 years of operation. As a minimum, these components should be line- replaceable units and have spares in stock to improve availability of the cavity door system.

| Major Equipment Group | MTBF(hours of operation) |
|---|--------------------------|
| Upper rigid panel mechanical assembly | 24,000 |
| Flex aero skirt/shear layer control mechanical assembly | 24,000 |
| Seal subsystem | 11,000 |
| Door Motion Instrumentation, Control and Electrical | 3,000 |
| Processors and Controllers | 6,000 |
| Electrical power | 7,000 |

Table 1. Summary of MTBF after Design Changes

Continued operation of the cavity door system during a flight of the SOFIA aircraft is critical to the successful conduct of astronomy. Failure to close the upper rigid panel would introduce effects on the telescope that would increase the downtime of the SOFIA observatory. Failure to open would mean a wasted flight. With limitations on space and weight, the key to in-flight reliability is graceful degradation of equipment and subsystems. This was achieved by de-rating the motors and roller bearings and by providing redundancy among the rollers. Availability is increased by a well thought out set of instrumentation and control logic for diagnosis of failures. Neither of these are achievable without a thorough and detailed understanding of how the system is supposed to perform its required functions and how it might fail to do this.

Interaction between the designers and the reliability analyst was an important contributor to the design evolution. The FMECA, for example, was used to develop the set of instrumentation for failure diagnosis. Of particular importance, however, was the face to face interaction of the reliability engineer with the design team. Not only did this facilitate the elucidation of general reliability concepts and specific reliability suggestions, but the meetings served as a catalyst of ideas for an overall better performing system. Therefore, important pointers for reliability engineers are:

- Know the system as well as or better than the designers. This takes a background not only in reliability technology but also in the engineering technologies that are involved in developing the system.
- Find out how the system might fail, and screen the failure modes by probabilities in order to present only the credible failure modes.
- Trust your analysis. However, the insights from your analysis, not the analysis itself, should be clearly communicated and discussed with the design team. Managers and designers are not as interested in how you performed your study as they are in the help you can give having done it.

When thinking about reliability improvement strategies, the following were good guiding principles for this application:

- Design for graceful degradation to combat incipient or partial failures, or system aging. (This concept is sometimes called fault tolerance or forgiveness and includes notions that essentially provide a margin of safety to the expected/intended operation.)
- Safeguards and reliability improvement features should be passive whenever possible.
- Redundancy must be judiciously applied in situations of weight and space constraints. All failure modes must be evaluated before adding redundancy. For example, adding redundancy where leakage is an important failure mode exacerbates the problem. Redundancy can also

introduce failure modes and its benefits are limited by common cause failures.

- When thinking about failure modes, do not limit thinking to “fails to operate”. A set of generic failure modes is: fails when needed, fails when not needed, operates when not needed, operates incorrectly when needed, operates incorrectly when not needed, and fails to maintain its own integrity. There are many other generic guides to thinking about failure modes (e.g., ref. 12).
- Avoid unnecessary components. Avoid "asking wouldn't it be nice if...". Balance the introduction of any component by asking how it can fail and what harm it can cause.
- A design should consider the potential for human error. It often is an important contributor to system unreliability or unavailability.
- The ultimate safeguard for critical failures should not be software, whenever achievable. The safeguard should be hardwired or mechanical.
- Materials and components should be specified to withstand reasonable variations beyond the expected environment.

None of these are new and these guidelines are by no means exhaustive. However, I found that writing these down was useful to guide communication with the design team.

REFERENCES

1. E. E. Becklin, “Stratospheric Observatory for Infrared Astronomy (SOFIA),” Proceedings of the ESA Symposium "The Far Infrared And Submillimetre Universe" 15-17 April 1997, Grenoble, France, ESA SP-401 (August 1997) pp. 201-206
2. Military Standard Procedures for Performing a Failure Mode Effects and Criticality Analysis, MIL-STD-1629A, Notice 2, Washington DC, November 29, 1984.
3. W. Denson, G. Chandler, W. Crowell, A. Clark, P. Jaworski, “Nonelectronic Parts Reliability Data 1995,” NPRD-95, Reliability Analysis Center, Rome, New York, 1995.
4. W. Denson, W. Crowell, P. Jaworski, D. Mahar, “Failure Mode/Mechanism Distributions 1997,” FMD-97, Reliability Analysis Center, Rome, New York, 1997.
5. “IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data For Nuclear-Power Generating Station,” IEEE-Std-500, Institute of Electrical and Electronics Engineers, New York, 1984.
6. B.S. Dhillon, *Mechanical Reliability: Theory, Models and Applications*, American Institute of Aeronautics and Astronautics, Washington DC, 1988.

7. D. I. Gertman and H. S. Blackman, *Human Reliability and Safety Analysis Data Handbook*, John Wiley and Sons, New York, 1994.
8. Support Systems Technology Company, “Handbook of Reliability Procedures for Mechanical
9. Equipment,” sponsored by the Office of Naval Technology, 1998.
10. S. Morris, B. Dudley, J. Caroli, P. MacDiarmid, D. Nicholls, A. Coppola. N. Criscimagna. J. Farrell, et.al., “Reliability Toolkit: Commercial Practices Edition,” Reliability Analysis Center, Rome, New York, 1993.
11. “Reliability Prediction Procedure for Electronic Equipment,” TR-332, Issue 6, Telcordia Technologies, December 1997.
12. R. Ellis Knowlton, “A Manual of Hazard & Operability Studies: The Creative Identification of Deviations and Disturbances,” Chemetics International, 1992.

BIOGRAPHY

Michael V. Frank, P.E., Ph.D., CPCM
Safety Factor Associates, Inc.
1410 Vanessa Circle, Suite 16
Encinitas, CA 92024 USA

Internet (e-mail): mfainc@pacbell.net

Dr Michael V. Frank is founder and President of Safety Factor Associates, Inc. For the last three decades he has emphasized the risk management, safety and reliability technologies in the aerospace, nuclear and defense industries. He specializes in the assessment and management of all risks associated with engineered systems and the decision-making that accompanies risk management. A significant feature of his work is the explicit, quantitative analysis of uncertainties within a risk and decision-making framework. Dr. Frank's educational background emphasized engineering, particularly with respect to the fundamentals of heat transfer, fluid flow, materials, and nuclear energy. He has over 70 technical publications in journals and proceedings, and has made hundreds of presentations across the U.S. (including the White House) in the area of risk assessment and management. Recent projects include risk assessments of the Ulysses, Mars Pathfinder and Cassini missions, the Space Shuttle, the International Space Station, nuclear power plant fire and earthquake studies, and wind tunnels, to name a few. He has consulted for the Interagency Nuclear Safety Review Panel which reports to the Executive Office of the President. He is a Professional Engineer, a Certified HAZOP Leader, a member of the Probabilistic Safety and Management technical program committee, and a Certified Professional Consultant to Management. Dr. Frank is listed in Who's Who in America and Who's Who in Science and Engineering.