# An Ultra Reliability for Project for NASA [1,2]

Andrew A. Shapiro
California Institute of Technology, Jet Propulsion Laboratory
4800 Oak Grove Drive
Pasadena, CA 91109
818 393-7311
aashapiro@jpl.nasa.gov

*Abstract*—NASA has embarked on a new program designed to improve the reliability of NASA systems. In this context, the goal for ultra reliability is to ultimately improve the systems by an order of magnitude. The approach outlined in this presentation involves five steps: 1. Divide NASA systems into seven sectors; 2, Establish sector champions and representatives from each NASA center; 3. Develop a challenge list for each sector using a team of NASA experts in each area with the sector champion facilitating the effort; 4, Develop mitigation strategies for each of the sectors' challenge lists and rank their importance by holding a workshop with area experts from government (NASA and non-NASA), universities and industry; 5, develop a set of tasks for each sector in order of importance for improving the reliability of NASA systems. Several NASA-wide workshops have been held, identifying issues for reliability improvement and providing mitigation strategies for these issues. Results from these workshops will be presented.

TABLE OF CONTENTS

1. INTRODUCTION ..... 1
2. STRATEGY ..... 2
3. PROJECT SECTORS ..... 3
4. WORKSHOPS ..... 5
5. WORKSHOP RESULTS ..... 6
6. COOPERATION OUTSIDE NASA ..... 11
7. CONCLUSION ..... 11
ACKNOWLEDGMENTS ..... 12
REFERENCES ..... 12
BIOGRAPHY ..... 12

## 1. INTRODUCTION

The objective of the Ultra Reliability task is to increase the reliability of all aspects of NASA missions by an order of magnitude.

The general strategy is to divide NASA systems into seven major sectors, develop a list of issues that are critical in limiting the reliability in each sector and determine mitigation strategies for each. The list of mitigation strategies will form the basis of a set of tasks to be executed with the aim of improvement of the reliability of NASA systems.

This NASA-wide effort involves representatives and participation from all NASA centers as well as addresses different ultra-reliability needs in different various NASA enterprises, leverages the wide variety of expertise across all of the agency and helps to develop an agency - wide infrastructure.

Definitions

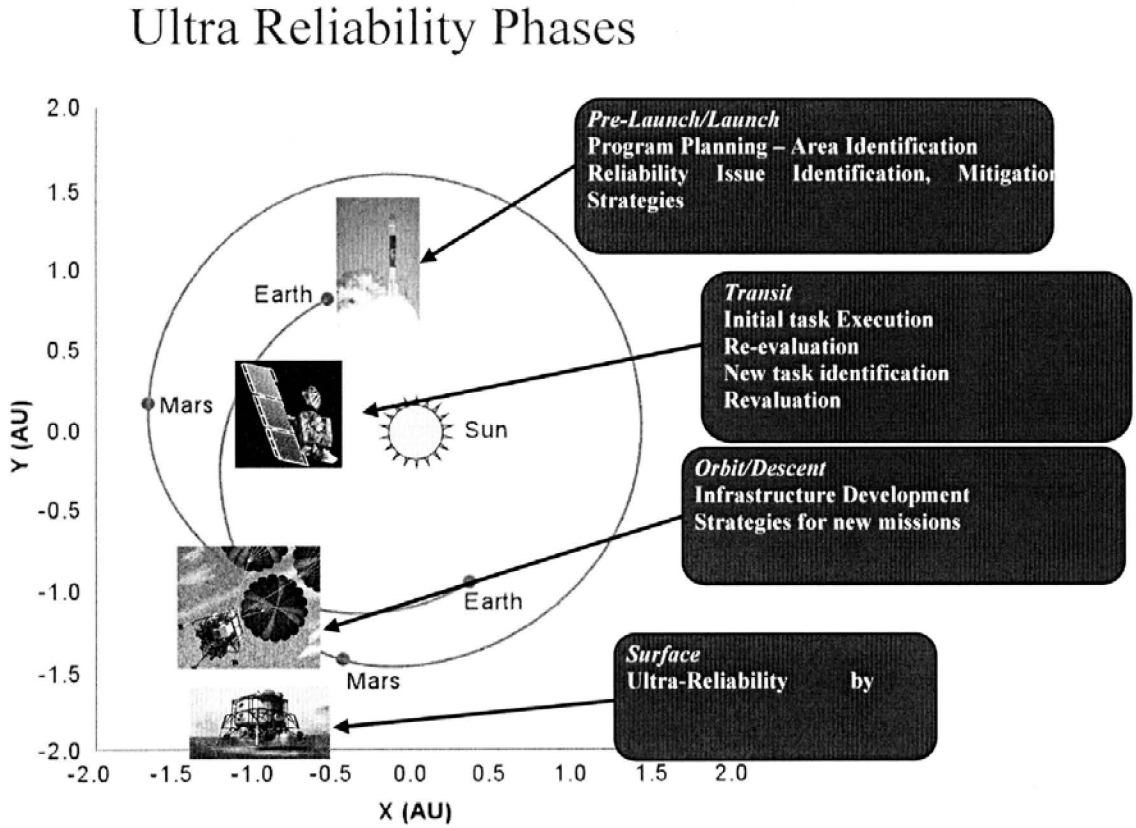
The initial NASA workshop in May 2002[1] determined the following working definitions. This was motivated by the close link between long-life and ultra reliability.

Ultra-reliability:
Given a specific time frame – reliability one order of magnitude more than current standard
Long Life:
Missions with a design lifetime of 20 years or more

To clarify with an example, launch vehicles typically have an operational lifetime of a few minutes, a fairly short life. However, the goal of the Ultra Reliability program is to increase the reliability of these systems by an order of magnitude.

[1] 0-7803-8155-6/05/$17.00© 2005 IEEE
[2] IEEEAC paper #1001, Version 0, Updated October 10, 2004

## 2. STRATEGY




The overall strategy for this project was to use a methodology similar to one developed on the Failure Defect Detection and Prevention[2] program sponsored by Dr. Michael Greenfield (and currently managed by Mr. Patrick Martin) out of the NASA Headquarters S&MA office starting in about 1998. This strategy involves listing specific objectives, in this case increasing reliability by an order of magnitude, listing specific barriers to achieving those objectives, and then tabulating mitigation strategies to address each of the barriers. Next, software, developed by NASA on the above mentioned program, can be used to score the various mitigation strategies to help rank their effectiveness against multiple barriers. Finally, from this listing of mitigation strategies, a series of tasks will be developed and executed to attack the barriers to achieving the program objective. The barriers and mitigation strategies are developed by a team of NASA, Government, university, industry and NGO participants to give. The lists were developed by a series of workshops. Several of them were in-person and two were virtual.

A few additional hurdles must be overcome in order for this strategy to be successful. One of these is to make sure that these tasks do not overlap with each other and to make sure that these tasks do not significantly overlap with existing efforts, particularly at NASA or DOD.

The approach for this program involves five steps:

1. Divide NASA systems into seven areas;
2. Establish areas champions and representatives from each NASA center;
3. Develop a reliability issue list for each area using a team of NASA experts in each area with the sector champion facilitating the effort;
4. Develop mitigation strategies for each of the areas' issues lists and ranking their importance by holding a workshop or with a working group of area experts from government (NASA and non-NASA), universities and industry;
5. Develop a set of tasks for each area in order of importance for improving the reliability of NASA systems.

Because a careful culling of these lists of mitigations is required, a two pronged approach is being taken for task selection. First, for near-term tasks, team members from the different NASA centers have been requested to propose small tasks taken from the top ranks of these lists, modulated by their residing experts in the field. Second, the task lists presented in this plan will be reviewed in detail over the next six months to identify overlaps. When overlaps are identified, the Ultra-Reliability program will work in cooperation with the existing programs that are executing these tasks and take advantage of the results from their

NASA and DOD partners. The selection of tasks for the Ultra-Reliability program will then proceed to the next ranked task on the list until an appropriate task is found.

The particular Ultra Reliability Areas identified for the purposes of this task were based on the results of the Ultra Reliability workshop held in May of 2002[1]. Parsing of NASA components for Ultra Reliability is difficult. No single parsing satisfies all work objectives. The specific area parsing may be altered as the project progresses. Five of the seven areas were explicitly mentioned in the 2002 workshop. Two additional areas were determined by review of the workshop notes and observing trends that went across all or most of the areas.

These two additional areas were infrastructure development and cross-cutting technologies. Essentially every team, from the 2002 workshop, identified needs in these two areas. Because these are far reaching and potentially quite costly areas to conquer (infrastructure improvements could run in the billions of dollars), they will be delayed until this program is more mature. There are several things that this program can do immediately, however, to help in these areas as well. This program can be used to highlight specific gaps and needs in both infrastructure and cross-cutting technologies so that NASA may use this information for efforts from other programs. In addition, this program can identify available infrastructure, such as test beds and analysis tools, and facilitate their use by other centers through the program. If one center needs to use a test bed for reliability testing that resides at another center, it is the intention of this program to help enable the activity.

Because of the relatively small budget for this program, immediate tasks will be funded for NASA centers only. As the budget for this program grows, it is intended to entertain proposals from outside NASA, both independent and partnering.

## 3. Project Sectors

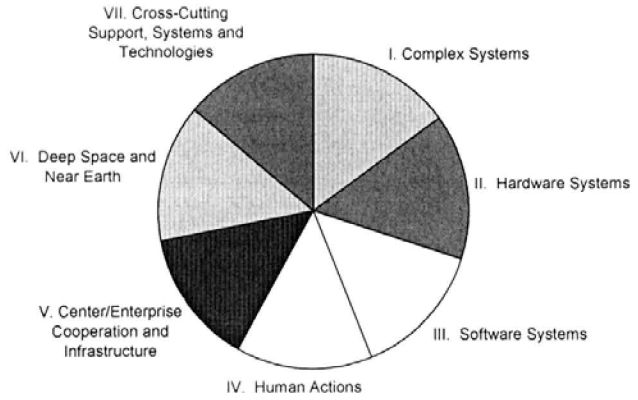
The program has been divided into seven primary sectors with some of these being sub-divided further. The seven sectors are:

- Engineering for Complex Systems
- Hardware Systems, including:
  - Launch Vehicles
  - Aircraft and Aerospace Vehicles (Aeronautics)
  - Manned Spacecraft
- Software
- Humane Actions
- Center/Enterprise Cooperation and Infrastructure
- Deep Space and Near Earth Long Life Missions
- Cross-Cutting Support, Systems and Technologies

As stated earlier, because of the magnitude of items five and seven, they will be postponed. Additionally, NASA has a significant multi-year existing effort in the area of Complex Systems. The Ultra Reliability program has already been and will continue to coordinate activities, but not entertain proposals in this area at this time. It should be noted that the reliability barriers lists generated by the Ultra Reliability workshops have already been shared with the people working Complex Systems. The issues raised are being built into their current generation of risk models.

Tasks will be reviewed quarterly using earned value metrics for cost and schedule in terms of performance of stated activities. The entire plan will be reviewed and updated on an annual basis. The ultimate goal, in addition to increasing the reliability of NASA systems, is to change the culture of NASA design to include ultra reliability as part of the systems design strategy and eventually to achieve ultra reliability by design. The remaining four areas will be the significant focus for the FY05 program.

**Ultra Reliability Components**



*Hardware*

Hardware involves a variety of large systems (and subsystems) including (but not limited to):

Aircraft and Aerospace Vehicles (Aeronautics)
Launch Vehicles
Manned Spacecraft

The first of these areas is being addressed by a virtual team jointly led by GRC and LaRC. The results of their efforts will be shown in the Workshop 5 section.

Launch Vehicles and Manned Spacecraft were covered in Workshops 3 and 4 respectively. The focus of these efforts is on key reliability items that will enhance the reliability of each of these types of systems. Some of these key items include design qualification and validation processes, a detailed risk assessment for the changing risk in launch vehicle failure for all candidate exploration launch vehicles, and the development of an integrated approach to create a NASA systems engineering architecture.

*Software*

The study of software reliability is the least mature of the reliability fields. Experts do not seem to agree on the best strategies, practices or execution of reliability methods in software. As software is becoming a more and more significant part of the system complexity and cost, this area should have an increasing importance. The work in software, again a virtual Workshop, has synchronized their tasks with the significant computing efforts at JPL, ARC, JSC, SSC and the IV&V center. Representatives from each of these organizations are coordinating their activities to avoid overlap.

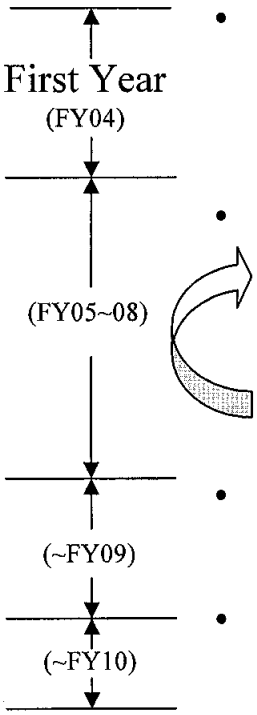
*Human Actions*

The activity in Human Actions is being led by KSC. The actions of humans both in space and on the ground as they interact with various systems (most of them complex) are important factors in the reliability of systems. Ultra reliability methods must account for the interactions of humans with the systems under consideration.

Their effort is being coordinated with an intramural task sponsored by the Exploration Office. The focus of some of the Human Actions proposed tasks are, to modify top level documents to include Human Factors in the requirements, in design and implementation of entire systems including both hardware and software, and design of better human to machine interfaces to minimize confusion or physical difficulties in operation of all systems.

*Long-Life Deep Space and Earth Orbiting Missions*

The 2003-2004 activity for Ultra-Reliability, led by JPL (and now including GSFC) was focused on long life missions, that is missions with durations of longer than 20 years. These tasks, as a result, are slightly ahead of the rest of the Ultra-Reliability program. The focus has been on the analysis of data for several JPL long life missions. A paper was published by Hoffman, Green and Garrett[3] entitled "Assessment Of In-Flight Anomalies Of Long Life Outer Planet Missions" as part of this effort and is attached as an appendix to this report. Additional studies were performed by Thompson[4] and will be published as "Space Systems Failure Analysis," in the near future. The area of Long Life missions was used as a front-running task to try out various techniques used for the Ultra Reliability program. Workshop 1, held at JPL in May 2004, was an outstanding success in terms of participation and in terms of the resulting barriers and mitigations list. The results of this workshop may be found in the following sections.




- Planning
  - *Area Identification*
  - *Reliability issue Identification*
  - *Mitigation and Task Identification*
- Execution of reliability assessment /improvement tasks
  - *Initial Task Start*
  - *Re-Evaluation*
  - *New Initial Tasks*
  - *Re-Evaluation*
- Infrastructure Development
- Strategies for New Missions

**Products**

Key reliability issue identification
Reliability assessment
Mitigation approaches and techniques

Execution plan for NASA-wide strategy for Ultra Reliability

Necessary to accomplish 10X improvement

Ultra Reliability by Design (increased by 10X)

## 4. WORKSHOPS

Four workshops were held in FY04. The first was hosted by Dr. Henry Garrett at JPL on the topic of long-life missions. The remaining three were held at JSC hosted by Mark Valentine. Below are the summaries by Dr. Garrett and Mr. Valentine.

*Long-Life Missions*[5]

On 23-24 June 2004, JPL hosted a one and a half day workshop on Long Life Risk Mitigation (LLRM). Approximately 40 scientists and engineers from a broad spectrum of commercial, NASA, and DoD organizations attended and took part in workshop study groups. Wednesday afternoon, as part of the NASA Code Q sponsored Ultra-Reliability/Long Life Program, the LLRM workshop provided demonstrations of ultra-reliability and long life mitigation products JPL and GSFC are currently researching and developing for Code Q. Presentations included the Space Systems Failure Database, the Assessment of In-flight Anomalies of Long Life Outer Planet Missions Study, GSFC data base efforts in Ultra-reliability, and the JPL DDP Ultra Reliability computer tool (all presentations are available on the Workshop CD). In conjunction with these research tools, on Thursday the Workshop identified the major risks to long life to be addressed by Code Q in next year's mitigation phase of the LLRM program. The main goal of this activity was to recommend potential thrusts and strategies to be pursued in future investigations for increasing the reliability of long life missions. Emphasis was placed on specific tasks Code Q could address and on potential partnerships with other NASA Codes. To summarize, the attendees received demonstrations of the Long Life mission assessment tools being developed as well as took part in the planning for next year's LLRM effort.

The specific goals of the Workshop were to:

1) Review and update the Long Life Risk lists for:
   - Space Environments
   - Human Interfaces, Structures, and Operations
   - Power and Propulsion
2) Identify the top five critical risks in each area
3) Determine potential mitigation methodologies or processes to lower mission risk in each area
4) Develop a plan (cost and schedule) for Code Q to achieve to meet the next level in Long Life or Ultra-Reliability

The introduction of the workshop was followed by presentations on specific JPL and GSFC Ultra-reliability tasks. Presentations included "Space Systems Failure Analysis" by S. Thompson, "Assessment Of In-Flight Anomalies Of Long Life Outer Planet Missions", by Mr. A. Hoffman, N. Green, and H. Garrett[3] and a discussion of the JPL DDP Tool[2], by M. Feather, S. Cornford, and A. Shapiro. Demonstrations of the DDP tool were available.

R. Beaman and M. Rousch also covered the on-going efforts at GSFC to identify ultra-reliability/long-life concerns and their risk management tool/data base.

On the second day, workshop participants were divided up into the three areas listed previously and asked to follow the following steps to meet the Workshop goals:

STEP 1: For each Risk Area (e.g., Power/Propulsion), review the previously complied Risk list and correct or update the list.
STEP 2: Using updated Risk list, identify approximately five "top" risks for what you consider to be the key "Long-Life" mission scenarios.
STEP 3: For each Risk, identify the Mitigation for the risk that we can effectively address over the next decade.
STEP 4: Layout a simple timeline/resource plan starting in FY05 for developing the Mitigation list.

Details of the working groups' results are available on the Ultra-Reliability website[6].

*Summary of Workshops 2-4, Ultra Reliability Risk Mitigation for Launch Vehicles, Manned Spacecraft and Human Factors[7]*

On July 20th-23rd, 2004, a workshop was held at the NASA Johnson Space Center with the intent to identify research opportunities and needs that would facilitate reliability improvement of space systems. This workshop included representatives from each of the NASA research centers, the Army and private industry. The workshop's primary purpose was to identify, explore and prioritize research opportunities seen to have the greatest potential for improving space related systems reliability. Several presentations, concerning the topic of reliability, were also included during the conference. This workshop focused on the areas of: launch vehicles, crewed spacecraft, and human factors, with subtopics in each area.

On the first day, Robert Kuper spoke on the U.S. Army, ultra reliability program, "US Army Transformation Reliability Improvement Program, ATRIP". Mr. Kuper discussed the Army program history, successes and lessons learned, and how some of these may apply to a NASA program. James Wetherbee of JSC, spoke on "NASA Safety Cultural Improvements". Specifically, Mr. Wetherbee discussed corporate culture and psychological impediments to having an effective safety culture and the characteristics common to organizations recognized as being "highly reliable". David Wadsworth and Anil Varma spoke on a planned reliability/maintenance program at GE designed to provide constant revenue to GE by providing timely cost effective planned maintenance to GE products. Customers see a better bottom line by having their GE equipment available a greater portion of the time and having maintenance occur during planned down times rather than having unexpected costly breakdowns.

The second day of the conference, the morning was devoted to human factors issues. Jack Knight spoke on Mission Control, workshop members then broke into several groups to identify human action related risks. Reconvening before lunch, David Witwer, a Continental Airlines pilot and a member of the MER, (Mission Evaluation Room for Shuttle missions) spoke on human factors relating to communication and social convention. After reconvening, Suzanne Thompson of JPL spoke on a launch vehicle failure database that is in development. The group then reconvened in small groups to finish on the topic of human factors and start the topic of launch vehicles. Later in the afternoon the findings of the human factors teams were presented and the group adjourned.
In the morning, Joe Levine of SAIC, retired from NASA, spoke on the history of reliability at NASA from Mercury to Shuttle. The rest of the morning was devoted to finalizing and documenting risks relating to launch vehicles. The afternoon was started by Jeff George of Exploration at JSC, speaking on some of the possibilities and the considerations of future human exploration. This served as an opener to the afternoon session beginning the topic of crewed vehicles. This topic was completed the morning of the next day after Chris Ramsay discussed "Software Safety Standard Update, STD 8719-13B".

Results of the conference and copies of most presentations may be found at the Ultra-Reliability website.[6]

## 5. WORKSHOP RESULTS

*Top reliability issues and mitigations, a summary of key workshop findings*

*Long-Life Missions*

A summary of the four main recommendations of the working groups (not necessarily in rank order) is given below.. Note that these are only intended as an overview—see the Ultra Reliability website[6] for complete details.

1. Lack of adequate models and testing procedures for the spacecraft environment and for long term failure mechanisms

Recommendations: The Office of Safety and Mission Assurance (OSMA) should take the lead in working with Science Office, the Office of Space Exploration, and the

Office of Engineering to evaluate the overall status of environmental and failure models to identify shortfalls, particularly in the models' accuracy. Support should be given to developing consistent agency-wide modeling and testing procedures with emphasis on synergistic testing capability.

2. Need to update orbital debris and meteoroid effects on long life space systems with particular concern for how to manage loss of spacecraft control for planetary protection requirements.

Recommendations: OSMA should work with the Science Office and Office of Space Exploration, actively encourage updating of the debris/meteoroid models and the detection technologies associated with them. The development of unique shielding and redundancy methodologies to avoid catastrophic failures should be developed to support planetary protection requirements (both nuclear and biological).

3. Concerns for the long term "health" of the mission teams and the physical infrastructure necessary to control and manage missions greater than ~10 years.

Recommendations: OSMA should take the lead in identifying and addressing the growing issues with the maintenance of long life missions. Specific areas would be the identification of strategies for identifying and maintaining trained personnel and skills, infrastructure, software, and ground support systems.

4. Continuing lack of adequate understanding of the physics of failure (particularly for mechanisms).

Recommendations: OSMA should continue to develop and encourage failure analysis programs, failure modes and effects analysis (FMEA) correlation studies, and failure analysis tools (see #1). Failure data bases should be expanded and made widely available for study. Missions to specifically study failure mechanisms and mitigations should be flown (in conjunction with the Offices of Space Exploration and Science).

*Launch Vehicles*

Launch vehicles were defined as vehicles/components used for transportation from ground to orbit. The teams were evaluating issues for ultra reliability, reliability one order of magnitude better than current standard.

The Launch Vehicle team was divided into 3 subteams

- Team 1 - Requirements, Modeling, and Analysis
- Team 2 - Primary Systems
- Team 3 - Secondary and Support Systems

The following is a summary of the team Findings

1. *Issue* -Requirements.
*Risk* -Lack of complete and comprehensive, but meaningful, system design requirements
*Mitigations*- Developing quantitative reliability requirements early in the contract definition phase in Statement of Work, establishing a method to measure and enforce the requirement. There has to be upfront system engineering of the integration of technology for design, manufacturing, and testing.

2. *Issue* - S&MA Staffing
*Risk* - Reliability engineers are being diluted over too many projects and activities.
*Mitigation* - Reliability engineers efforts/assignments should be more focused. [not stated but an obvious solution - increased staffing]

3. *Issue* -Part Quality
*Risk* - There is a lack of requirements for the deliberate selection of high quality parts.
*Mitigation* - Develop a selection/screening plan for parts to verify that each can withstand the uses for which they are intended. Consider derating and degradation effects on reliability.

4. *Issue* Testing / Validation
*Risk* - Insufficient design qualification and validation processes [Analysis, Testing].
*Mitigation* - Need to establish testing plans/requirements to support ultra reliability goals.

5. *Issue* - Analysis Tools / Processes
*Risk* - Lack of standard/integrated process/tools for validation of Safety, Reliability and Quality assurance requirements.
*Mitigation* - Need to develop/select reliability models/tools that give designers immediate feedback and provide design verification/validation at all stages of development

6. *Issue* - Data
*Risk* - Lack of sufficient, consistent, and accurate data
*Mitigation* - Instrumentation to detect all known failure modes, stronger contractor data delivery (and access) requirements

7. *Issue* - Provide a high-sigma design process
*Risk* - Lack of uncertainty management process - Dependence on traditional max. design conditions and safety factors
*Mitigation* - Use probabilistic design with real world variability

8. *Issue* - Risk Management
*Risk* - Lack of comprehensive risk management.
*Mitigation* - Design to avoid failure, making risk metrics more important than performance metrics

9. *Issue* - Thermal Issues
*Risk* -Thermal Risks related to Launch Vehicles include operating in extreme environments both self created and pre-existing.
*Mitigation* - A better understanding and tracking of the thermal environment for launch vehicles is needed.

*Human Factors*

The main concern with human errors was inadequate implementation/integration of human factors principles of design. Human factors need to be included in engineering and operational plans and procedures. Standard methods need to be developed to consider effects of human factors on manufacturing, operation, and maintenance of the system. The following are the top three Ultra Reliability human factors topics, listed by risks and mitigations.

1. *Risk* - Training
(Policy, Requirements, Communication and People)
Management
- Bottleneck in middle management
- Feedback not directly to maintainer

Communication
- Lack of information sharing
  - Fear/Lack of confidence

Given that displays may project incorrect information, too much information or not properly summarize information; then there is the concern that during a situation which requires fast decision responses, the operator may not properly respond or have a suboptimal response.

Training Management, Given that individual training and personnel development may be inadequate or un-optimized, then there is the concern that the individual may not be adequately qualified for the his/her assigned tasks. This includes, frequency of training, Poor training/verifying certification/understanding, poor students records management, the training not being tailored to the student the right individual being selected for the task areas and the possible inability of the individual to apply the information.

Miscommunication: Given that there may be inability to properly communicate during emergency situations, then there is the concern that proper information may not be communicated to decision makers. This problem may include inability to communicate due to panic, and lack of confidence to ask for help/information and the perception that input may be ignored anyway.

Given that situation awareness may be compromised due to inconsistent information channels, information sources/rationale are not clearly indicated and time pressure factors; then there is the concern that decisions may be suboptimal.

*Mitigations*
Some mitigations are:
- Capture tribal knowledge into process plans, procedures.
- Develop strong mentoring program.
- Determine feedback system for LL into process, etc.
- Develop metrics to relate Reliability to HF
- Boost GSE importance for next design, next mission.
- Delete caste system.
- Develop a cross training program.
- Training on communication and teamwork
- Scheduling for joint tasks, joint recreation, "alone time"
- Crew design: Crew selection /assembly
- Habitability of space in which crew lives and works

Lack of training scenarios with all level of decision makers in how to handle ST and LT failure scenarios and anomalies. Needs bottom up communication and specific support channels to allow information to be passed to middle and upper management in a sufficient fidelity to allow correct decisions to be made.

Support NASA Assurance Technology Center to expand personal training management to include training requirements, retraining requirements, certification and recertification, integrated systems simulation, etc. [1a] Support ATC to provide training profiles. [2] Support detailed profiling of personnel who are successful in functioning in the given environment and the application of this profiling to new hires. [3] In a similar manner analyze the successful team dynamics which are required to operate a specific decision support system.

With respect to Emergency Operations (specifically decision making process information channels), experience training through emergency scenario training is needed. Predefine information sources, rules and rationale for rules.

Additional mitigations include
[1] Human factors analysis for control panels, etc. will fit all sizes of personnel.
[2] Checklist, manuals.
[3] Visual displays standardized.
[4] Top-down requirements for displays.
[5] Increase awareness building procedures for human factors engineering.
[6] Required work instructions and agency level support
[7] Related center level procedures.
[8] Advance display algorithms that increase system knowledge and provide solutions to anomalies as they occur and as a function decision making/information timing needs.

2. *Risk* - Human Health & Safety (Exploration)

- Radiation Microgravity
- Nutrition/Water

- Physical Fitness
- "Mental fitness"
- Crew psychosocial health

*Mitigation* - Radiation Shielding, Medical training, Exercise countermeasures, Autonomous medical care technologies, Spare parts, maintenance schedules.

3. *Risk* - Systems Engineering (Implementation of Design)

- Inadequate safeguards, Accessibility Issues, Lack of data of HF Reliability, Flight Integration, Lack of Understanding of Human Cognition, Test Methods/ Simulation Models, Determination of correct variables in UR
- GSE feedback to designer is lacking. Ground Support needs better interaction with mission (Flight OPS). There need to be demonstrated process studies and accounting for ground OPS planning shortfalls.
- Awkward Lifts (unplanned and inadequate lifting and handling equipment) are also an issue. Repetitive lifting and handling issues. Continuous leaks in pressurized systems. GSE issues (need to provide configuration control and compatibility with flight hardware).
- Lack of maintainability requirements: knowledge, anthropometry, ergonomics, fatigue, situation awareness, decision making, workload/task management and team communication need to be considered.

- Automation, displays and controls, usability and trust are also risks.

In long duration flight command decisions, crew does not have sufficient expertise to make the correct decision. There are fewer people contributing to the decision than when mission control made command decisions. Mission controller knowledge and experience must be captured and contained on board. Type I (critical/emergency), II (time is available to get ground support), and III (restoration is needed – delay is needed) decisions are different. The crew cannot be prepared for every contingency: not foreseen, foreseen but not enough time to train ahead of time

Given that there may be multiple factors that cause the inability to make decisions; then there is the concern that incorrect or damaging decisions may be made. These factors may include [1] real knowledge of systems, [2] the wrong person making the decision, [3] written policy verses emergency responses, decision strategy and information structures being incompatible and the reliability of data sources.

*Mitigations* -

- Establish quantitative maintainability requirement. (e.g. PIT-STOP engineering). Develop a design for maintainability. Develop a design for Reliability (e.g. process flow for HF).
- Develop a program to study human factors in reliability issues (data collection critical). Develop a sound reliability and maintainability statistics (RAMS) program to understand failure mechanisms and drivers, including tool methodologies. Remove as much as possible humans (include more robotics). Develop diagnostic and prognostic health management systems.

- Human-centered design requirements, processes, tools, methods. Training for decision making strategies, situation awareness strategies, contingencies is needed. Just-in-time Training for knowledge, skills, learning also needs to be included as well as consideration for automation, display and control design and usability as part of conceptual design

Additional mitigations include:
- Good automation/display design
- Work schedules for routine tasks
- Shift schedules, detailed work schedules with sufficient slack
- Self-paced instead of machine-paced work
- Flexible requirements for tasks, cross-training/redundancy, training
- Crew design (size, selection, assembly)
- Job design, constraints among international partners.

*Manned Space Vehicles*

*Crew Related Systems:*

1. *Risk* - If human factors, medical requirements, and new processes are not in place for long-duration exploration, then crew well being and safety may be compromised.
*To mitigate this risk:* Human factors must be included early in the design process as requirements: Modify top level documents to include Human factors in the requirements; Update the current documents for Human factors and make them into requirements with a required periodic revision process.

2. *Risk* - There is a risk that the interface between human and machines will be a cause for unrecoverable errors. Interfaces between humans and machines that could fall into this risk category include confusion by commonality or complexity of displays, controls that are difficult to rapidly understand especially in time critical operations, controls that are not designed to accommodate crew anthrometry or ergonomic constraints. Interfaces that require repetitive motion or high force exertions also pose similar risks to both the crew and the systems as a whole.
*To mitigate this risk:* Human factors must be included early in the design process, and tested at every phase of the project; Educate Safety and Engineering personnel on the importance and necessity of including Human Factors in design and implementation of entire systems including both

hardware and software; Better human to machine interfaces need to be designed to minimized confusion or physical difficulties in operation of all systems; Human factors needs to be included in system safety reviews of all hardware and software projects.

3. *Risk* - If communication with ground support is inadequate, hardware downtime and problem solving may be extended.
*To mitigate this risk:* Human-human (ground-flight, ground-ground) human-machine, and machine-machine communication systems should be optimized; Interpersonal communication should be optimized by training and in-situ practice; Human to machine communication should be addressed through interfaces that include attention to clarity and commonality; Short range communication devices should be provided to crew (e.g. ISS personnel) beyond those included in EVA apparatus; Continued development of communication hardware needs to be stressed.

4. If there is extended space flight, a variety of illnesses and injuries may occur. If there are exposures to radiation during extended space flight, there may be adverse health effects. If there are exposures to micro gravity during extended space flight, there may be adverse health effects. In-flight noise may also adversely affect crew operations.
*To mitigate these risks:* To provide medical care independent of Earth-based resources, an autonomous medical care system will be required; Design adequate shielding for extended and interplanetary flight. Early warning systems on board to detect radiation exposures; Design a method to impose artificial gravity; Design hearing protection systems and design sound reduction systems into crew habitat.

5. *Risk* - If there are extended or extensive EVAs, there can be increased health risks.
*To mitigate this risk:* Minimize the risk of Decompression Syndrome and prebreathe overheads for performing Extra Vehicular Activities from the Crew Exploration Vehicle and lunar habitat to avoid acute and chronic physiological changes from long-term exposure to reduced levels of partial pressure oxygen; Design EVA suit for better protection against environmental threats.

*Manned Space Vehicles*

*Systems/Structures Related:*

1. *Risk* - Launch vehicle reliability is a serious risk to mission success for large infrastructure missions.
*To mitigate this risk:* Conduct a detailed risk assessment for the changing risk in launch vehicle failure for all candidate exploration launch vehicles, existing and proposed, from pre-launch to orbit insertion. This calculation of changing risk should be to the highest resolution possible (i.e. minute-to-minute, or even second-to-second.

2. *Risk* - There is a risk of requiring high performance propulsion systems due to increased mass margin restrictions in the launch vehicle structure. Launch vehicles are typically over-designed with excessive safety margins.
*To mitigate this risk:* Options for Reducing Structural Mass for Exploration Missions: Maximizing the mass available for science and systems will require that the structural mass of spacecraft, vehicles, and habitats be reduced as much as possible. A multi-center steering group should be formed to coordinate the development of structural technologies for exploration programs.

3. *Risk* - The level of modularity vs. the size of the launch vehicle vs. the ability to replace a payload after a launch failure.
*To mitigate this risk:* Trade studies need to be done to assess the optimum strategy for launching mission infrastructure.

4. The risk of failing to detect the onset of cascading or catastrophic failures during long duration missions.
*To mitigate this risk:* Systems to Predict Failure. Investigate the greater usage of Failure Prediction capabilities to provide insight into impending spacecraft malfunctions.
5. Many of the missions will be long-term and remote and will very likely have numerous system failure and maintenance issues. T*o mitigate this risk:* In Space Repair and Maintenance. : In-space repair and maintenance of the Crew Exploration Vehicle (CEV) systems, and those of subsequent elements of Project Constellation, should consider a supportability concept, a set of design and operational requirements, and key technologies.

5a. Due to the extended communication times for deep-space missions; the crew may not have the proper information or knowledge to make a proper decision in an emergency.
*To mitigate this risk:* Investigate how and what knowledge to capture for the crew or vehicle and get it into a form where the crew or vehicle can act upon an emergency situation.

*Manned Space Vehicles*

*Management/Integration Related:*

1. *Risk* - NASA does not have adequate top down systems engineering (engineering management/program management, etc.) in place to manage large programs. NASA has already paid a premium price for the lessons learned by not having systems engineering environments and architecture on its large projects and programs. *To mitigate this risk:* It is the recommendation that NASA pursue the development of the integrated approach to create a NASA systems engineering architecture in which contractors can support the creation of tools and systems. NASA should review the best practices of other similar organizations, i.e.

large program management. Identify effective management structures, applicable commercial software, management training. Special attention given to integration of complex systems designed to interact with humans.

2. *Risk* - Poorly defined testing processes with respect to overall development approach. There needs to be a NASA minimum set of testing standards requiring a bottoms up system testing.
*To mitigate this risk:* 1. review what NASA has, 2. define where we need to be. 3. Write the standards.

3. *Risk* - There is a lack of formal way to propagate technological advances between programs.
*To mitigate this risk:* This needs study, for example: How to get separately contracted projects to coordinate shared technology development.

4. *Risk* - For long duration missions, maintainability and sustainability are essential.
*To mitigate this risk:* Involvement of Operations in the Design Process- Research integration of operations, human factors and probabilistic expertise with design expertise.

5. *Risk* - Current NASA systems do not adequately capture operational data. This hampers trending, failure prediction and proper systems management, integration, operations and resource management.
*To mitigate this risk:* A system wide (to component level) data capture system must be in place at the start of phase c design of any new program. Capturing design and operational data of susbsystem, components, etc.

It is clear that the risks and mitigations from the workshops are far-reaching. Considerable effort is still required to consolidate these risks and mitigations. The current plan is to generate tasks related to the risks and mitigations outlined and to start to work the issues.

## 6. Cooperation Outside NASA

As part of the ultra-reliability effort, a significant thrust will be to work with outside partners, including contractors, universities, government agencies (including the military) to keep abreast of the latest developments in high and ultra reliability and to find synergies that will benefit both organizations. The initial foray in this direction is with three organizations.

1. US Army, with Robert Kuper, Executive for Reliability, US Army, RDECOM, QESA – The US Army has a significant effort in Ultra Reliability and is more than two years into its transformation process. Mr. Kuper is very interested in working with NASA on synergistic issues.
2. General Electric, with Dr. Anil Varma. GE has achieved ultra-reliability in several significant areas including reliability improvements of jet engines and locomotives by an order of magnitude. GE is currently working with the NASA ultra reliability program to explore opportunities to use their technologies.
3. Florida International University, Professor Marc Resnick. Professor Resnick was a visiting fellow at KSC and is working with the NASA ultra reliability program on an Ultra Reliability Roadmap.
4. Papers at Relevant Conferences. This year, Phil Napala, Dr. Henry Garrett and Dr. Andrew Shapiro hosted a panel discussion on Ultra-Reliability at the Reliability and Maintainablity Symposium (RAMS) conference sponsored by IEEE. Additionally, a paper was given at the 5th International Symposium on Environmental Testing for Space Programs by Mr. Alan Hoffman (JPL). Another was submitted by Dr. Ed Zampino (GRC) and Mr. Mike Packard (GRC) to the RAMS conference for next year. Dr. Andrew Shapiro had an abstract accepted for a paper on Ultra Reliability at NASA at the IEEE aerospace conference and also presented on the same topic at the NASA Assurance Technology Symposium in Cleveland sponsored by S&MA.

## 7. Conclusion

This program is NASA-wide:

- to address different ultra-reliability needs in different NASA Enterprises
- to leverage the wide variety of expertise across all of NASA
- to develop a NASA-wide ultra-reliability infrastructure
- to leverage overlapping issues
- to take advantage of related on-going NASA tasks.

There is a lead center for each major area, but many centers are participating and should be funded in each area. One metric is for leveraging of internal OSMA research. Earned value and schedule metrics will be used for tracking of tasks. The development of reliability assessment is a key for success. Intelligent consistent use of existing NASA methods and an opportunity to develop novel ways of assessing reliability will both be used.

A pathway for a strategic plan for increasing the reliability of NASA missions' one order of magnitude has been defined.

A short term plan has been defined, and NASA is moving forward:

- Area leaders have be identified
- Reliability issue lists have been developed in each area
- Reliability workshops have held
- Issue and mitigation lists have been generated in each appropriate area.

## ACKNOWLEDGMENTS

The research described in this paper was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

This plan is the accumulation of substantial work by a large number of individuals. The Ultra-Reliability team consists of representatives from each center who have agreed to champion the program and be the focal point for their center. A number of individuals from NASA, government agencies (including the military), universities, industry and non-governmental organizations also contributed significantly to this effort. Most of their names may be found on the Ultra-Reliability PBMA website: http://ultrareliability-workshop-pbma-kms.intranets.com/login.asp

| | | Center | Area(s) |
|---|---|---|---|
| Marcus | Murbach | ARC | Software / Human Factors |
| Eddie | Zavala | DFRC | Aero |
| Robert | Loomis | DFRC | Reliability Methods |
| Edward | Zampino | GRC | Aero / Manned Space Vehicles |
| Lydia | Lee | GSFC | Earth Orbiting |
| Bob | Beaman | GSFC | Earth Orbiting |
| Phil | Napala | HQ | Headquarters |
| Hank | Garrett | JPL | Earth Orbiting |
| Andrew | Shapiro | JPL | Program Manager |
| Jan | Railsback | JSC | Manned Missions |
| Mark | Valentine | JSC | Manned Missions |
| Natesan | Jambulingam | KSC | Reliability Methods |
| Gena | Humphrey | KSC | Human Factors |
| Duane | Pettit | LaRC | Aero |
| Prince | Kalia | MSFC | Launch Vehicels |
| Mike | Rewis | SSC | Launch Vehicels |


## REFERENCES

[1] P. Napala, "Ultra-Reliability Workshop Report," *Office of Safety and Mission Assurance, NASA Headquarters*, Pasadena, CA, May 2002

[2] M. S. Feather, K.A. Hicks, K.R. Johnson and S.L. Cornford; "Software Support for Improving Technology Infusion," Proceedings of the 1st International Conference on Space Mission Challenges for Information Technology; Pasadena, California, July 2003, pp. 359-367; JPL Publication 03-13A, Jet Propulsion Laboratory, California Institute of Technology.

[3] A. Hoffman, N. Green and H. Garrett, "Assessment of In-Flight Anomalies of Long Life Outer Planet Missions,"

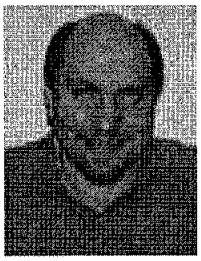
[4] S. Thompson, "Space Systems Failure Analysis," presented at "Ultra Reliability Workshop on Launch Vehicles," Houston, TX, July 2004.

[5] H. Garrett, "Summary of Ultra Reliability Workshop on Long-Life Risk Mitigations", Pasadena, CA, June 2004.

[6] Ultra-Reliability website: http://ultrareliability-workshop-pbma-kms.internets.com/default.asp?link=

[7] M. Valentine, "Summary of three Ultra Reliability Workshops," Houston, TX, July 2004.

## BIOGRAPHY



**Andrew A. Shapiro** has been working in microelectronic interconnects for twenty years. He has worked as a member of the technical staff at Rockwell International and Hughes Aircraft, where he was responsible for the packaging of a number of phased array radars and ran their high density interconnect line. He was a Principal Scientist at Newport Communications/Broadcom, where made the first commercial polymer 10GHz Si packages, and he has designed and packaged 10 and 40GHz optoelectronic modules. He has also been Project Manager at California Institute of Technology's Jet Propulsion Laboratory and is currently a Principal Engineer in the Electronic Packaging and Fabrication Section (349) at JPL where he is implementing new electronic, RF and optical technologies onto space missions. He earned his BS in chemical engineering at U.C. Berkeley, his MS in Materials Science at UCLA and his Ph.D. in Materials Science at U.C. Irvine. He is on several national committees including NEMI optoelectronics roadmap, ECTC optoelectronics and, IMAPS education. Dr. Shapiro is also currently Assistant Adjunct Professor in Materials Science and Engineering at U.C. Irvine and is performing research in environmentally friendly manufacturing of electronics and optical and high frequency packaging.