Ultra Reliability at NASA

Andrew A. Shapiro[*]
Jet Propulsion Laboratory, California Institute of Technology, Pasadena CA 91009

Ultra reliable systems are critical to NASA particularly as consideration is being given to extended lunar missions and manned missions to Mars. NASA has formulated a program designed to improve the reliability of NASA systems. The long term goal for the NASA ultra reliability is to ultimately improve NASA systems by an order of magnitude. The approach outlined in this presentation involves the steps used in developing a strategic plan to achieve the long term objective of ultra reliability. Consideration is given to: complex systems, hardware (including aircraft, aerospace craft and launch vehicles), software, human interactions, long life missions, infrastructure development, and cross cutting technologies. Several NASA-wide workshops have been held, identifying issues for reliability improvement and providing mitigation strategies for these issues. In addition to representation from all of the NASA centers, experts from government (NASA and non-NASA), universities and industry participated. Highlights of a strategic plan, which is being developed using the results from these workshops, will be presented.

I. Introduction

THIS paper gives a brief history of the Ultra-Reliability program at NASA, an outline of the current thrust of the program and an idea of where the program will be going. As outlined in previous publications[1] the objective of the Ultra-Reliability task is to increase the reliability of all aspects of NASA missions by an order of magnitude. The initial NASA workshop in May 2002[2] determined the following working definitions, motivated by the close link between long-life and ultra-reliability. Ultra-reliability: Given a specific time frame, an increase in reliability by one order of magnitude more than current standard. Long Life missions are those 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.

The general strategy was 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 intended to be executed with the aim of improvement of the reliability of NASA systems. The NASA-wide effort involves representatives and participation from all NASA centers as well as addresses different ultra-reliability needs in various NASA enterprises, leverages the wide variety of expertise across the entire agency and helps to develop an agency-wide infrastructure.

NASA as an agency has changed direction substantially since the inception of the Ultra-Reliability program in 2002. The agency has gone from Faster, Better, Cheaper, to military style procurement, to its current focus on the manned lunar and ultimately the manned Mars missions. As a result, the Ultra-Reliability program has had to be agile and re-focus to meet the agency's requirements. This is true particularly in light of the changes for 2006. In general, Safety and Mission Assurance research budgets have been declining, requiring the program to become more of a NASA-wide program related research coordination effort than a self-funded NASA research effort.

[*] Lead Division Technologist, Enterprise Engineering Division, M/S 103-106, 4800 Oak Grove Drive

II. Background

A. Initial Strategy

The initial strategy, during the formulation of the program, was to use a methodology similar to one developed on the Failure Defect Detection and Prevention[3] program by Dr. Steven Cornford and Dr. Martin Feather and initially sponsored by Dr. Michael Greenfield and subsequently by Patrick Martin out of the NASA Headquarters Safety and Mission Assurance (S&MA) office starting in about 1998. This strategy, shown, 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. From this listing of mitigation strategies, a series of tasks will be developed, ranked and executed to attack the barriers to achieving the program objective. The tasks will be reviewed each year with completed tasks retiring and new tasks from the ranked lists started. As the program matures, infrastructure improvements will be recommended based on acquired information and strategies for new programs will be developed. Finally, if the program is successful, that new programs and systems will be "ultra-reliable" by design. The barriers and mitigation strategies are developed by a team of NASA, Government, university, industry and Non-Government Organization (NGO) participants to give. The lists were developed by a series of workshops. Three of them were in-person and two were virtual.

A few additional hurdles needed to be overcome in order for this strategy to be successful. One of these was to make sure that these tasks do not overlap with each other and the second was to make sure that these tasks do not significantly overlap with existing efforts, particularly at NASA or the Department of Defense (DOD).

The initial approach for this program involves nine 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 (lists) 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;
6. Culling of mitigation lists to reduce overlap;
7. NASA centers propose small tasks from top ranked task lists
8. Review of tasks to clean up and reduce overlap;
9. Select tasks from top down to match program funding level.

A careful culling of these lists of mitigations was required; a two pronged approach was taken for task selection (steps seven and nine). 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 (step seven). Second, the task lists presented in this plan will be reviewed in detail 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 (step eight). 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 (step nine).

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[2]. 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. 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.

B. System Partitioning

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

I. Engineering for Complex Systems
II. Hardware Systems, including:
  a. Launch Vehicles
  b. Aircraft and Aerospace Vehicles (Aeronautics)
  c. Manned Spacecraft
III. Software
IV. Human Actions
V. Center/Enterprise Cooperation and Infrastructure
VI. Deep Space and Near Earth Long Life Missions
VII. Cross-Cutting Support, Systems and Technologies.

As stated earlier, because of the magnitude of items five and seven were postponed. Additionally, NASA had 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. Tasks were intended to 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.

1. *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 Glen Research Center (GRC) and Langley Research Center (LaRC). 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.

2. *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 the Jet Propulsion Laboratory (JPL), Ames Research Center (ARC), Johnson Space Center (JSC), Stennis Space Center (SSC) and the Integration, Validation and Verification (IV&V) center. Representatives from each of these organizations are coordinating their activities to avoid overlap.

3. *Human Actions*

The activity in Human Actions is being led by Kennedy Space Center (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.

4. Long-Life, Deep-Space and Earth-Orbiting Missions

The 2003-2004 activity for Ultra-Reliability, led by JPL, and now including Goddard Space Flight Center (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[4] 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 and presented by Thompson[5] entitled "Space Systems Failure Analysis." The area of long life missions was used as a front-running task to try out various techniques used for the Ultra-Reliability program.

C. Workshops

Four workshops were held in 2004. 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.[6,7]

1. Long Life Missions

On June 23rd-24th 2004, JPL hosted a one and a half day workshop on Long Life Risk Mitigation. 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 S&MA sponsored Ultra-Reliability program, the long life workshop provided demonstrations of ultra-reliability and long life mitigation products JPL and GSFC are currently researching and developing for S&MA. 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 Defect Detection and Prevention (DDP) Ultra-Reliability computer tool. In conjunction with these research tools, the Workshop identified the major risks to long life to be addressed by S&MA in the next year's mitigation phase of the long life 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 S&MA could address and on potential partnerships with other NASA offices. 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 long-life 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 S&MA to achieve to meet the next level in Long Life or Ultra-Reliability

2. Summary of Workshops 2-4, Ultra-Reliability for Launch Vehicles, Manned Spacecraft and Human Factors

On July 20th-23rd, 2004, a workshop series 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. These workshops included representatives from each of the NASA research centers, the Army and private industry. The workshops' 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 series focused on the areas of: launch vehicles, crewed spacecraft, and human factors, with subtopics in each area. Results of the conference and copies of most presentations may be found at the Ultra-Reliability website[8].

The above describes the direction of the Ultra-Reliability program in 2004. Substantial changes in the agency took place during 2005 during which the program continued at a relatively low level. The next section outlines some of the accomplishments during this low level of activity.

III. 2005 Program Highlights

A. Overview

The continuation of the Ultra-Reliability program was successful as follow-on to the NASA-wide planning of 2004. Budget limitations did not allow the execution of the program as planned, instead, with the limited funding available at each center, a surprising amount of progress was made on small tasks. Monthly conference calls were held for team sharing and communication. Meetings were held at most of the NASA centers at least once during 2005 to keep the teams coordinated for the overall Ultra-Reliability program. Additionally, some centers were able to leverage their funding with larger programs. Other centers, including DFRC, GRC, JSC, KSC, and LaRC opted to accumulate their funding for slightly larger tasks in 2006.

B. Summary of NASA Center Work for 2005

1. *Work performed at ARC (Marcus Murbach)*

Dr. Murbach worked on the development of practical flight test-beds that will accelerate the testing/evolution of ultra-reliable sensor-webs, interfaces, and software systems and on the development of an advanced planetary probe for the SCRAMP[9] program. Dr. Murbach was able to leverage the seed money provide by the Ultra-Reliability program to assist him in performing work on optimized re-entry vehicles and provide a plan for improved sensor networks for integrated vehicle health management that will be applicable to NASA's Crew Exploration Vehicle.

2. *Work performed at GSFC (Lydia Lee, Marvin Rousch)*

Ms. Lee and Dr. Rousch progressed significantly with a task is to establish a risk/standard website to provide a structured, disciplined approach for risk identification and provide standards, guidelines, and preferred practices to help guide/support programmatic and design decisions. This work will continue in 2006 along with a coordinated effort with LaRC and GRC for a failure analysis database.

3. *Work performed at JPL (Henry Garrett, Nelson Green, Martin Feather, Allan Nikora)*

Because of the limited funding at the other NASA centers, a portion of the JPL funding intended for workshops and coordination was diverted to work on long life missions. Nelson Green, under the direction of Dr. Henry Garrett researched and wrote several papers on the analysis of anomaly reports for Mars robotic missions, looking at the trends and implications for future Mars missions.[10] Suzanne Maddock (now at LaRC), also under the direction of Dr. Henry Garrett completed a report on probabilistic assessment of the success of previous Lunar missions to the probability of success of future Lunar missions.

Additional work was performed by Dr. Allan Nikora and Dr. Martin Feather, coordinated with the work of Pedro Curiel at SSC, on the linkage of the Automated Risk Manager (ARM) with various software reliability tools. This work will continue in 2006.

4. *Work performed at MSFC (Prince Kalia)*

Prince Kalia leveraged the Ultra-Reliability effort at MSFC to coordinate UR goals with CEV launch vehicle development. This includes preliminary launch vehicle reliability estimates as well as review of shuttle sensors related to the vehicle health. Prince also proposes a general systematic approach to new mission reliability that is in line with the overall goals of the Ultra-Reliability program and is an expected area for the next Ultra-Reliability workshop.

5. *Work performed at SSC (Pedro Curiel)*

Mr. Curiel's work in association with the implementation of ARM, also funded by S&MA was leveraged by the Ultra-Reliability program as part of an effort to link risk management, through software, for a given program across participating NASA centers.[11]

IV. 2006 Program Focus

As a result of the general trend for NASA technical research funding, the Ultra-Reliability program will be taking a different direction for 2006. The program will work on two primary objectives which are still related to the framework outlined in the 2004 strategic plan. These two objectives are:

a) Use the Ultra-Reliability team and resources as a way to link reliability tasks at all of the NASA centers and leverage reliability initiatives for NASA-wide use, and

b) Focus tasks on the five areas of interest listed below:

The five areas that are of primary interests should be directed at support of the major NASA mission direction including the Crew Exploration Vehicle, lunar return program with future utility of mars missions. The five topic areas are:

1. Lunar and Martian mission reliability. A workshop on reliability issues associated with extended lunar and Martian missions will be held in Washington DC. The workshop will have a specific deliverable of a risk management plan to address reliability issues for these missions and a plan outlining coordination of Ultra-Reliability activities.
2. Integrated System Health Management and Predictive Maintenance issues directed at CEV. The concept is to use the tools and methods developed by industrial partners like General Electric to analyze sensor data from the space shuttle. From this analysis, a model will be developed to provide better data, analysis and sensor placement recommendations for CEV.
3. A NASA-wide failure analysis database. Data from various component and system failures (from both flight and test) is not currently captured on a common system. This topic area will emphasize collection of failure analysis data for a unified system that is contributed to and accessible by all NASA centers. An effort will be made to include existing NASA center databases.
4. Software reliability. The efforts on software reliability have been significantly reduced in an age when software is quickly becoming one of the most significant portions of the system both in terms of complexity and criticality. This area is anticipated to be a significant reliability issue for the future targeted programs.
5. Long life missions. Although no specific “long-life” missions (>20 years) have been designated, it is likely that the CEV and additional lunar return and Martian exploration programs will have a long life aspect. Currently the shuttle systems are long-life vehicles and it is anticipated that CEV will be as well. With this extended operation time in mind, particular reliability strategies need to be developed in the early design stages so that the vehicles may be maintained and updated easily. In addition, particular design-for-reliability features will enhance the lifetime and improve the reliability of these vehicles.

If sufficient funding is available, an additional workshop will be held to refine the 2004 strategic plan including the reliability risk lists that were developed. Additional tasks taken from the top of these rank-ordered lists will be supported as funding becomes available.

V. Conclusion

The Ultra-Reliability program has significantly evolved with substantial accomplishments made in 2005 in a diverse number of areas relating to the overall goals of the Ultra-Reliability program including published papers, and numerous reports and presentations. More importantly, 2005 has seen the building of a cooperative link for sharing information and developing a reliability direction for all of NASA, laying the groundwork for a productive effort for 2006.

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[7].

Representative	**Center**	**Area**
Marcus Murbach	ARC	Software / Human Factors
Ed Zavala	DFRC	Aero
Edward Zampino	GRC	Aero / Manned Space Vehicles
Lydia Lee	GSFC	Earth Orbiting
Marvin Roush	GSFC	Earth Orbiting
Phil Napala	HQ	S&MA Sponsor
Henry Garrett	JPL	Earth Orbiting
Andrew Shapiro	JPL	Program Manager
Jan Railsback	JSC	Manned Missions
Henk Rolent	JSC	Manned Missions
Natesan Jambulingam	KSC	Reliability Methods
Gena Humphrey	KSC	Human Factors
DuanePettit	LaRC	Aero
Prince Kalia	MSFC	Launch Vehicles
Mike Rewis	SSC	Launch Vehicles
Pedro Curiel	SSC	Software Tools

References

[1] Shapiro, A. A., “An Ultra-Reliability Project for NASA,” Proceedings, *IEEE Aerospace Conference, Big Sky Montana*, IEEE, March 2005.

[2] Napala, P., “Ultra-Reliability Workshop Report,” Office of Safety and Mission Assurance, NASA, Feb., 2002.

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

[4] Hoffman, A., Green, N., and Garrett, H., “Assessment of In-Flight Anomalies of Long Life Outer Planet Missions,” presented at *5th International Symposium on Environmental Testing for Space Programmes, in the topic of* “*Environmental Test Method: Programmes,* European Space Research and Technology Centre (ESA-ESTEC), Noordwijk, The Netherlands, June 2004.

[5] Thompson, S. “Space Systems Failure Analysis,” presented at *Ultra-Reliability Workshop on Launch Vehicles*, Houston, TX, July 2004.

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

[7] Valentine, M., “Summary of three Ultra-Reliability Workshops,” NASA, Houston, TX, July 2004.

[8] Ultra-Reliability website: http://ultrareliability-workshop-pbma-kms.internets.com/default.asp?link= November 2005.

[9.] Murbach, M., 2. “SCRAMP: The Development of an Advanced Planetary Probe from CFD to Re-Entry Test Flight,” presented at *The Third International Planetary Probe Workshop*, Athens, Greece, July 2005.

[10.] Green, N., Hoffman, A., Garrett, H., “Anomaly Trends for Long Life Robotic Spacecraft,” submitted to Journal of Spacecraft and Rockets, AIAA, October, 2005.

[11.] Curiel, P., Williams, E. R., “Active Risk Manager Implementation,” NASA, Stennis Space Center, July 2005.