Pre-proposal Assessment of Reliability for Spacecraft Docking with Limited Information

Aron Brall CRE, ARES Technical Services

Key Words: Reliability Assessment, Spacecraft Reliability, Developmental Reliability

SUMMARY & CONCLUSIONS

This paper addresses the problem of estimating the reliability of a critical system function as well as its impact on the system reliability when limited information is available. The approach addresses the basic function reliability, and then the impact of multiple attempts to accomplish the function. The dependence of subsequent attempts on prior failure to accomplish the function is also addressed. The autonomous docking of two spacecraft was the specific example that generated the inquiry, and the resultant impact on total reliability generated substantial interest in presenting the results due to the relative insensitivity of overall performance to basic function reliability and moderate degradation given sufficient attempts to try and accomplish the required goal. The application of the methodology allows proper emphasis on the characteristics that can be estimated with some knowledge, and to insulate the integrity of the design from those characteristics that can't be properly estimated with any rational value of uncertainty. The nature of NASA's missions contains a great deal of uncertainty due to the pursuit of new science or operations. This approach can be applied to any function where multiple attempts at success, with or without degradation, are allowed.

1 INTRODUCTION

The NASA Goddard Space Flight Center has established the Integrated Design Center (IDC) to assist project teams, who are the customers of the IDC, with establishing key design parameters for proposed new space flight missions. A description of two of the labs in the IDC was presented in (1). A third lab, the Architecture Design Lab (ADL) has been added to the IDC. The ADL's function is to evaluate various options to accomplish a mission and then down select to a few that are feasible within the mission requirements and available resources and schedule. A key part of this process is determining the probability of mission success (Reliability). The results of these studies are used to prepare proposals for NASA Headquarters to approve the development and launch of the spacecraft and instruments.

2 ACRONYMS

ADL Architecture Design Lab
HST Hubble Space Telescope
IDC Integrated Design Center
I&T Integration and Test
NASA National Aeronautics and Space Administration

3 ARCHITECTURE DEVELOPMENT LABORATORY

The ADL is a logical outgrowth of the IDC's Mission and Instrument Design Labs. The purpose of the ADL is to evaluate a number of potential solutions to accomplish a mission, winnow these down to a manageable set of alternatives, then evaluate the alternatives to determine which are the most suitable to accomplish the mission. The evaluation addresses all of the key parameters to accomplish the mission including mass, cost, schedule, technological risks (ability to design and build the hardware required and operate in space) and reliability. Ideally, one or two of the evaluated configurations would then be subject to a more detailed modeling in the Mission Design Lab for Spacecraft and Mission Operations, and the Instrument Design Lab if any specialized instruments had to be developed as well. The ADL Operational Methodology is the following:

- **Generate a Trade Tree that covers the complete study trade space**
  - List every possibly reasonable and conceivably viable option; examine and leverage off of previous studies on the subject; explore all available applicable material, known solutions, general knowledge. Do not reinvent the wheel! Conduct brainstorming sessions, add all creative and novel solutions as practical.
- **Explore the Trade Space**
  - Examine, evaluate, and disposition, every option on the Trade Tree one by one without exception; categorize and document the disposition rationale for every option
    - **Category 1 Options:** These options are confirmed realistic, feasible and viable; will be taken through the complete evaluation process, and placed on the Final Comparison Charts; conduct in-depth engineering and programmatic analyses, as applicable, and generate parametric sizing / design; Generate Ps numbers; generate Mission Lifecycle Cost in a uniform manner.
    - **Category 2 Options:** Considered as potentially feasible until more in-depth calculations or analyses prove otherwise
      - Conduct assessments and some analyses as required to disposition these; one possible outcome is the

promotion to Category 1; Disposition rationale is typically added as an Appendix to the Trade Tree.

- **Category 3 Options:** Obviously unattractive, unfeasible, or absurd
  - Expert judgment and/or engineering assessment is sufficient to disposition these. Unanimous study team plus customer lead concurrence is required; a note with disposition rationale is added to the Trade Tree.

- **Compile Summary Charts**

4 THE MISSION – DOCKING WITH AND DISPOSING OF THE HUBBLE SPACE TELESCOPE AT END OF LIFE

To develop the necessary mission scenarios to be evaluated, the ADL Operational Methodology was applied. A trade tree of 5 mission elements was created: HST operational state, disposal location, capture method, disposal method, main propulsion system. 27 architectures were considered and dispositioned with the 3 category rationale. After mapping the trade tree, 9 Category 1 architectures + uncontrolled re-entry were developed and assessed for risk and cost.

The ADL derived assumptions for Architecture Options were:

- HST's natural orbit degradation will cause its uncontrolled reentry not earlier than ~2025
- Action is required when HST reaches 500 km altitude; uncontrolled reentry predicted 6 to 24 months later
- HST Disposal is the primary mission

The considered architectures are for HST disposal via

- Controlled reentry into Pacific Ocean
- Boost to 1200 km disposal orbit
- Boost to 2000 km disposal orbit (in accordance with international agreement)

The Baseline Docking hardware would be the HST Soft Capture Mechanism (SCM)

- Based on the ISS Low Impact Docking System (LIDS) for all architectures
- Active side never designed; requires customized, flight design/development/hardware for HST-LIDS
- Assume autonomous rendezvous and docking package proposed for another mission

To summarize, the proposed mission investigated in the ADL was to dispose of the Hubble Space Telescope (HST) at the end of its life in the next decade by plunging it into the ocean by controlled reentry; lifting it to a significantly higher orbit; or extending HST's mission by 10 years before plunging in the ocean or lifting to a higher orbit. Without any action, the HST's orbit would decay and result in an uncontrolled reentry with associated possibility of human injury. This disposal mission involves launching a disposal module that has to rendezvous with the HST, dock to a ring that was attached during one of the HST repair missions, and either lift HST to a higher orbit for disposal, lift HST to a higher orbit for continued operations, or plunge HST into the ocean.

5 THE PROBLEM – DETERMINING THE PROBABILITY OF A SUCCESSFUL DOCKING MANEUVER

In evaluating the HST Disposal Mission Reliability four phases were identified for the mission – Launch; Rendezvous with HST; Dock with HST; Disposal of HST. The key factor was determined to be the reliability of successfully docking with the HST. This was going to be an autonomous action, and differentiating from the other stages, there was also very little data available to use for determination of the probability of successful docking. There was anecdotal information that various team members estimated as "very likely" to "difficult" to accomplish (read as 90+% to 50% probability of success). This limited information with substantial uncertainty created a problem that had to be resolved. The only known factor was that there was sufficient fuel for four attempts at docking.

The short duration of the disposal mission (~ 2 weeks) produced a very high reliability for the spacecraft hardware and further emphasized the sensitivity of the mission to the docking reliability.

6 ANALYSIS OF THE PROBLEM

The essence of the problem is that the reliability of the docking process is unknown – it cannot be modeled until actual detailed system design (hardware, software, and process) has been developed and a predicted estimate was required so that a proposal could be prepared for approval by NASA Headquarters.

Although the reliability of the hardware could be estimated, the reliability of the software including the algorithms and the interface of sensor data with processing functions and the actuators and mechanisms required for docking could not be predicted with any reasonable range of accuracy. In fact, if the failure of the software is in the interface where the software controls the docking hardware, a first docking attempt failure due to this failure would preclude any subsequent successful docking attempt. The specific process selected to be enacted with the hardware and software will impact the docking reliability through sequencing of functions that accomplish the docking maneuver. Additionally, the dependence of subsequent docking attempts on the failure of prior attempts was unknown. Some misses where damage is done to the docking mechanisms might greatly reduce the reliability of or preclude the ability to successfully dock on a subsequent attempt. The early stage of the design at this point precludes a usable reliability estimation of the docking hardware and software, let alone a trade space to evaluate alternative approaches. Instead of predicting a reliability value, the necessary initial reliability and freedom from dependence had to be determined. This information would set requirements for accomplishing the docking and provide some assurance that the methods chosen would comply with the requirements.

The problem becomes a set of possibilities (expressed as probability of success per attempt) for initial probability of docking success and a second set of possibilities for

dependence of subsequent docking attempts on prior attempts (expressed as degradation of probability of success of subsequent attempts). This approach contains the problem, and in the analysis will provide a range of possible solutions to the problem. It should be noted that all of the learning of the docking process has to be developed prior to launch since the docking occurs within one week of launch. A significant part of the learning necessary to design the hardware, software and docking methodology would result from the simulation of the process. This would include computer simulations, mechanical model simulations, and possibly ground based simulation using an exact replica of the docking mechanism and control system.

7 RECOMMENDED APPROACH

Even with a successful launch and deployment, and no hardware failures, a failure of the docking maneuver would cause the Mission to fail. The approach taken was to develop a matrix of possible docking reliabilities based on the initial docking reliability and adjusted for dependence of subsequent docking attempts. A defined constraint of the mission at this design stage was that the design was being calculated and implemented with sufficient fuel for a maximum of four docking attempts. The initial estimate assumed the reliability for each docking attempt would be 90% and each attempt would be independent of any other attempt yielding a 99.99% probability of docking success for the maximum of 4 attempts. This assumption is dependent on addressing all risks before commitment to a design, detailed simulation of the docking maneuver and thorough Integration and Test (I&T) to address potential infant mortality. Impact docking reliability induced an assessment for a range of initial reliabilities down to 70%, and degradations as high as 50% for each subsequent attempt.

A table detailing the results for 90%, 80%, and 70% Docking attempt Reliability with no residual dependency as well as residual dependencies up to 50% is provided in Table 1. If the probability of docking success (Total Docking Reliability) falls below 99%, docking becomes the key driver for Mission Reliability and Risk of Human Casualty. A probability for Total Docking Reliability under 95% was considered to be unacceptable.

The Total Docking Reliability is a simple calculation of 1 – the product of the failure probabilities (1 – Reliability) of the four attempts:

$$R_{TD} = 1 - ((1 - R_{1A})(1 - R_{2A})(1 - R_{3A})(1 - R_{4A}) \quad (1)$$

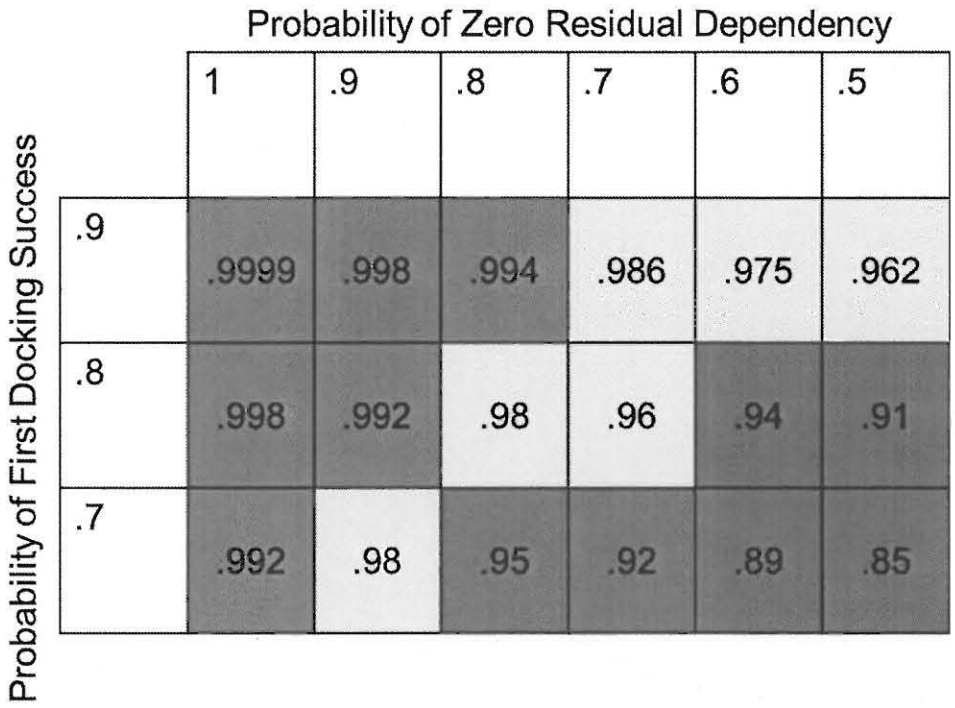
Docking Attempt Reliability	0.9	0.9	0.9	0.9	0.9	0.9	0.8	0.8	0.8	0.8	0.8	0.8	0.7	0.7	0.7	0.7	0.7	0.7
Probability of Zero Residual Dependence	1	0.9	0.8	0.7	0.6	0.5	1	0.9	0.8	0.7	0.6	0.5	1	0.9	0.8	0.7	0.6	0.5
Reliability of 1st Attempt	0.9	0.9	0.9	0.9	0.9	0.9	0.8	0.8	0.8	0.8	0.8	0.8	0.7	0.7	0.7	0.7	0.7	0.7
Reliability of 2nd Attempt	0.9	0.81	0.72	0.63	0.54	0.45	0.8	0.72	0.64	0.56	0.48	0.4	0.7	0.63	0.56	0.49	0.42	0.35
Reliability of 3rd Attempt	0.9	0.73	0.58	0.44	0.32	0.23	0.8	0.65	0.51	0.39	0.29	0.2	0.7	0.57	0.45	0.34	0.25	0.18
Reliability of 4th Attempt	0.9	0.66	0.46	0.309	0.19	0.11	0.8	0.58	0.41	0.27	0.17	0.1	0.7	0.51	0.36	0.24	0.15	0.088
Total Docking Reliability	0.9999	0.998	0.994	0.986	0.975	0.962	0.998	0.992	0.98	0.96	0.94	0.91	0.992	0.98	0.95	0.92	0.89	0.85

Table 1 Determination of Docking Reliability

Developing an understanding of how variation in these assumptions would impact the Total Docking Reliability generated the need for this table. Using the table, it is apparent that if the Reliability of the initial docking attempt is even as poor as 0.7, an acceptable docking reliability can be achieved with modest degradation (less than 10% degradation) of subsequent attempts. If the degradation is expected to be larger, then a higher initial reliability will be required. It is interesting to note that a high initial reliability, even with serious degradation of 50% per attempt, still yields a Total Docking Reliability over 0.96. On the other hand, even though an initial reliability of 0.7 will yield a Total Docking Reliability of 0.992 with no degradation, moderate degradation of 20% gives a Total Docking Reliability of 0.95

which is for all intents and purposes unacceptable since it produces a calculation with an unacceptable probability for possible human injury upon reentry into the atmosphere. To clearly present this information for all the possibilities, a color coded matrix was developed and is shown in Figure 1. As can be seen in the figure, the absolute limits for a fully acceptable docking reliability is >0.7 for initial probability of successful docking, and 20% (1-0.8) for residual dependency on subsequent attempts. Again note that both of these limits could not happen on the same design, or an unacceptable result would occur. Considering the type of mission being considered and the lack of prior experience with this type of maneuver, the ability to estimate the likelihood of degradation with an acceptable degree of uncertainty is not very strong. It therefore becomes fairly obvious that our effort should be biased towards assuring as high a reliability as is practicable within cost constraints for the initial docking attempt, again with a reasonable level of uncertainty.

Figure 1 – Color Coded Total Docking Reliability



REFERENCES

1. A. Brall, "Pre-proposal Assessment of Reliability for Spacecraft and Instruments". Proceedings Annual Reliability and Maintainability Symposium January 26-29, 2012

BIOGRAPHY

Aron Brall
ARES Technical Services
NASA Goddard Space Flight Center
Code 322, Building 6
Greenbelt, Maryland 20771 USA

e-mail: aron.brall-1@nasa.gov

Aron Brall is Reliability Subject Matter Expert at NASA Goddard Space Flight Center for ARES Technical Services. Previously he was Reliability Service Area Lead at NASA Goddard Space Flight Center for ManTech International; and Vice President of Quality during 14 years at Landis Grinding Systems, a UNOVA Company. Prior to that he worked 12 years for Amecom Division of Litton Systems as a Systems Effectiveness Project Engineer. Out of 45 years professional experience, 38 have been in Reliability and Product Assurance. He received a BS in Electrical Engineering in 1967 from Columbia University School of Engineering and Applied Science, NY, NY, and an MBA in 1987 from Sellinger School of Business at Loyola University, Baltimore, MD. He is General Chair of RAMS® 2013 and has been a member of the RAMS® Management Committee since 1999. He is a senior member of ASQ, a Life Senior member of IEEE, and a member of the SRE and SAE. He is an ASQ Certified Reliability Engineer. He is a contributing member of the committees that prepared both editions of SAE M-110, Reliability and Maintainability Guideline for Manufacturing Machinery and Equipment.