Reliability and Cost/Benefit

Abstract

Probabilistic Risk Assessment (PRA): A Practical and Cost Effective Approach

Lydia Lam Lee

Antonino J. Ingegneri

Melody Djam

Probabilistic Risk Assessment (PRA): A Practical and Cost Effective Approach

The Lunar Reconnaissance Orbiter (LRO) is the first mission of the Robotic Lunar Exploration Program (RLEP), a space exploration venture to the Moon, Mars and beyond. The LRO mission includes spacecraft developed by NASA Goddard Space Flight Center (GSFC) and seven instruments built by GSFC, Russia, and contractors across the nation. LRO is defined as a measurement mission, not a science mission. It emphasizes the overall objectives of obtaining data to facilitate returning mankind safely to the Moon in preparation for an eventual manned mission to Mars. As the first mission in response to the President's commitment of the journey of exploring the solar system and beyond: returning to the Moon in the next decade, then venturing further into the solar system, ultimately sending humans to Mars and beyond, LRO has high-visibility to the public but limited resources and a tight schedule.

This paper demonstrates how NASA's Lunar Reconnaissance Orbiter Mission project office incorporated reliability analyses in assessing risks and performing design tradeoffs to ensure mission success. Risk assessment is performed using NASA Procedural Requirements (NPR) 8705.5 - Probabilistic Risk Assessment (PRA) Procedures for NASA Programs and Projects to formulate probabilistic risk assessment (PRA). As required, a limited scope PRA is being performed for the LRO project. The PRA is used to optimize the mission design within mandated budget, manpower, and schedule constraints.

The technique that LRO project office uses to perform PRA relies on the application of a component failure database to quantify the potential mission success risks. To ensure mission success in an efficient manner, low cost and tight schedule, the traditional reliability analyses, such as reliability predictions, Failure Modes and Effects Analysis (FMEA), and Fault Tree Analysis (FTA), are used to perform PRA for the large system of LRO with more than 14,000 piece parts and over 120 purchased or contractor built components.

However, a comprehensive PRA database for spacecraft missions that provides the requisite probability distribution functions for major elements and assemblies is not available for risk assessment purpose, as acknowledged by the Director of Safety and Assurance Requirement Division, NASA Headquarters. As a result, MIL-HDBK-217F Reliability Prediction of Electronic Equipment, heritage data, and best practices were utilized to establish and maintain consistent methods for estimating and evaluating the LRO system reliability. The handbook provided the guidance to prepare a failure database for piece parts and components as applicable. The prediction analysis, with understanding of its limitations, was performed to identify the design weak links by ranking the failure factors and focusing on the failure distribution of each of the components rather the resulting number of the system reliability. By using the existing

methods and standards as well as heritage data, a failure database was accomplished within cost and schedule.

Concurrently, Failure Modes and Effects Analysis (FMEA) was performed to identify the critical items that might cause loss or degradation of the mission. A Critical Items List (CIL) was formed as the results from the FMEA. The failure data obtained from reliability predictions, together with the reliability drivers, were then incorporated into the CIL and used as inputs of the PRA process using Quantitative Risk Assessment Software (QRAS) provided by NASA Headquarters.

QRAS is a comprehensive Windows-based software tool for conducting PRA. QRAS is put in place to model the system failure logic in the form of Event Sequence Diagrams (ESD) and Fault Trees. The LRO PRA analyzes full mission success criteria as well as all scenarios of minimum mission success. Those scenarios are addressed by 10 mission phases with the requirements of a certain number of components and instruments need to work to satisfy the identified criteria. System risk levels are then quantified using Headquarters provided software.

The LRO project office has ensured mission success with a tight schedule by utilizing the existing standards, traditional and innovative methods, together with a no-cost to the project tool (QRAS). The analyses are performed to formulate the probability of the failure for each of the components of the system. PRA then integrates these analytical techniques and results to assess the potential for failure and to help find ways to reduce the mission risks.

The future plan of NASA GSFC is to develop a PRA database using the available on-orbit failure data across the Agency. By then PRA will be more accurate and meaningful to all space projects. Within the NASA community, the approach described above has shown the most efficient way to assess mission risks at the present time.