Statistical Methods Applied to Risk Management at NASA

María de Soria-Santacruz Pich and Chester Everline
Jet Propulsion Laboratory, California Institute of Technology

Space is a harsh place for humans and electronics due to vacuum, extreme temperature ranges, enhanced radiation levels, and the micro-gravity environment. To survive that harsh environment, engineers and managers use statistics to inform their designs and decisions. From the probabilistic definition of the space environments that surround the vehicle, through the estimation of the forces and torques required for attitude control, and even to the higher levels of management to evaluate and control risks, statistics plays a key role in mission success. This article focuses on the latter application, that is, the utility of statistics for assessing and managing project risks. The non-existent or very limited maintainability of the systems operating in orbit as well as the criticality of these systems make risk management not only a necessity but a priority.

Over the years, the space sector has been leading the development of state-of-the art technologies that found many applications in other industries. Back in the 1960s, the aerospace industry was also one of the first adopters of risk and reliability assessment techniques. With the Apollo program, however, NASA found that estimates of the probability of successfully bringing astronauts back to Earth were not encouraging, and this finding was the reason that prevented NASA from further developing quantitative, probabilistic, and systematic risk assessment approaches. Instead, NASA would continue using traditional and qualitative safety assessment analyses for over two decades. In 1988, and motivated by the Challenger accident in 1986, the Slay Committee recommended that Probabilistic Risk Assessment (PRA) be applied to manage risks on the Shuttle program. By that time, the nuclear power industry had been using PRA for many years and it had become a useful and effective tool for risk assessment. It seems like PRA should have been the tool of choice for NASA from its early conception, since it enables risk management of complex technological systems in a comprehensive, systematic, and quantitative fashion to ensure mission and programmatic success. However, it was the Slay Committee that triggered a decade of proof-of-concept applications of PRA, following the nuclear industry's lead. After a long journey, NASA is finally adopting quantitative and probabilistic risk assessment to optimally manage programs and projects and support decision making to improve performance and safety. The discussion in this article is based on one of the most recent efforts in this direction entitled "Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners"[1] that was released with the intent of providing a set of recommended procedures for probabilistic risk assessment applicable to the aerospace industry at different levels.

The main difference between PRA and traditional safety assessment approaches is on the basis for evaluation. Traditional approaches evaluate the likelihood of success with respect to a reference mission (success probability), which can be quantitatively estimated in the case of simple systems. This approach, however, is not based on a quantitative assessment of the risk but simply on the likelihood that a system would perform its function correctly. Moreover, design-based evaluations cannot deal with extreme events that may occur along the mission. The ability to cope with anomalous situations requires a systematic, comprehensive approach based on an evaluation of the risk and capable of identifying failure modes. This is the approach provided by PRA.

The concept of risk in the context of PRA involves a set un undesirable likelihoods and conse-

[1] Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, NASA/SP-2011-3431, Second Edition, December 2011.

In 1988, and motivated by
the Challenger accident in
1986, the Slay Committee
recommended that Proba
Risk Assessment (PRA) be applied to
nage risks on the Shuttle program.

quences, and their characterization normally responds to three questions: What can go wrong?, how likely is it?, and what are the consequences? The answer to these questions correspond to the three main elements of PRA, this is, a set of accident scenarios, their frequencies or likelihoods, and their associated consequences[2]. Uncertainties exist in each of these elements that have to be quantified as an integral part of each step in the analysis and that constitute one of the most important components of PRA. The use of probabilistic or aleatory models is therefore essential in risk analysis to address the variability and randomness of the physical processes; both "natural" or aleatory variability and uncertainty in knowledge of the process (because of unavailable or scattered information) have to be accounted for. Another essential step of PRA is the definition and identification of accident scenarios. A comprehensive set of scenarios is a requirement for analysis completeness but it may be challenging to achieve. Moreover, the development of a comprehensive set of scenarios demands for the involvement of a technically diverse team to ensure that all disciplines have been captured in the analysis. Each scenario contains a set of initiating and pivotal events. Initiating events are a perturbation of the system that requires some kind of response, while pivotal events are the result from successful or failed responses that are relevant to the progression of the scenario. An example of initiating event could be an increased current draw that goes beyond the operational limits of affected electronics components. A pivotal event could be the failure of detecting and mitigating the enhanced current level that could lead to the burn out of critical electronic components and potentially result in loss of the spacecraft. Fault tree analyses are often used to model logical relationships between events with different levels of complexity like system, assembly, and component level failures, and they are also useful to model dependencies and conditionalities between pivotal events. These scenarios, their uncertainties, and consequences are put together to create the risk profile of the system, and they are classified into end states as a function of the severity of the consequences; examples of the latter in the case of NASA programs could be the loss of the crew or mission failure. The probabilities of these

[2] S. Kaplan and B.J. Garrick, "On the Quantitative Definition of Risk," Risk Analysis, 1, 11- 37, 1981.

high-level consequences are quantified with probabilistic figures of merit or performance metrics referred to as “risk metrics”. Uncertainty can play a determining role in the output of the risk metrics. This uncertainty is commonly characterized using Monte Carlo sampling of each one of the basic events that constitute the usually complex risk metric, and the values are next combined to obtain an expression of the risk metric for that sample. Probability distributions can sometimes be easily characterized for areas where data sets are abundant but this may not be the case for many parameters, and so a best guess has to be taken with the expectation that it will be updated in the future as new data become available. Despite the comprehensiveness and the detail of PRA, it is impractical to prove that the risk of a complex system is below a certain expected threshold. For this purpose, PRA assumptions are often substantiated by a set of analyses, tests, and experience-based postulations that form the “Risk-Informed Safety Case”, and there has to be a commitment that specific design, manufacturing, and operational techniques will be followed in accordance with the assumptions that went into the PRA analysis.

Risk management is an essential task in complex projects like NASA missions. Two types of risk can be identified in the context of PRA: performance and individual risks. Performance risks refer to non-compliances of performance requirements that have a direct impact on safety, engineering, cost, and/or schedule. Individual risks differ from performance risks in that they refer to specific issues or departures from the project plan and that have an effect on the overall performance risk. The traditional risk management approach, or “Continuous Risk Management” (CRM), consisted of managing individual risks that appeared over the course of the development of the project. CRM is based on five cyclical concepts that respond to *identifying*, *analyzing*, *planning*, *tracking*, and *controlling* the risks, and that are supported by effective communication and documentation of the process[3]. The concept of performance risk gained momentum in 2008, when NASA revised its risk management approach to also include “Risk-Informed Decision Making” (RIDM)[4] as a complement to CRM. The purpose of RIDM is to inform system engineering decisions by using analyses like PRA to characterize the risk and uncertainty of alternatives and establish performance requirements. RIDM consists of three main steps: (1) identification of decision alternatives within the context of the objectives, (2) risk analysis of each alternative consisting of a characterization of its relevant outcomes and their probability distributions over the performance metrics, and (3) risk-informed alternative selection by the stakeholders. As noted, PRA is especially useful in the risk analysis of alternatives to determine the probability density functions of each outcome with respect to the performance measures. Performance commitments are commonly defined to facilitate the selection phase. These commitments are a set of fixed performance metric values commonly expressed in terms of percentiles that ease the comparison of alternatives. For example, a performance commitment could be the ninety-five percentile in the probability density function of the payload resolution capability. Once an alternative has been selected, systems engineering will use PRA to characterize the risks associated to performance requirements, while individual risks associated with the implementation of the decision will be managed with CRM.

The application of PRA within NASA has seen continuous improvement in the recent years but there are still many areas for development. The accurate characterization of reliability or probability of failure are of extreme relevance to space missions and there is still significant room for improvement as well as ongoing efforts devoted to this area. Similarly, the capabilities of a simulation-based treatment of risk management have been expanding rapidly in the recent years and it is expected that they will enable a more comprehensive understanding of scenarios and characterization of the risks in the future. Following current trends, we should expect an increasing demand for quantitative approaches to risk management at the Agency level in the coming years.

The research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration. Copyright 2016 California Institute of Technology. U.S. Government sponsorship acknowledged.

[3] Carnegie Mellon University Software Engineering Institute. Continuous Risk Management Guidebook, 1996.

[4] NASA Risk-Informed Decision Making Handbook, NASA/SP-2010-576, April 2010.