Journal of Space Safety Engineering 000 (2018) 1–14

Contents lists available at ScienceDirect

Journal of Space Safety Engineering

journal homepage: www.elsevier.com/locate/jsse

Analyzing spaceflight residual risk acceptance decisions before launch

David M. Lengyel[a,*], Thomas A. Mazzuchi[b]

[a] The George Washington University, Former NASA Risk and Knowledge Management Officer for the Human Exploration and Operations Mission Directorate, NASA Headquarters, United States
[b] Professor and Department Chair, School of Engineering Management and Systems Engineering, The George Washington University, United States

ARTICLE INFO

Article history:
Received 9 August 2017
Revised 6 November 2017
Accepted 21 November 2017
Available online xxx

Keywords:
Residual
Risk
Acceptance
Decision
Multi-attribute preference model

ABSTRACT

This paper will examine the typical decision process that National Aeronautics and Space Administration (NASA) project management team members utilize to rank and then accept residual risks before the launch of a spacecraft. Interviews of two flight project management teams at NASA's Goddard Space Flight Center (GSFC) were conducted to understand the structuring of these decisions. Decision attribute preferences were elicited using a lottery technique and a multi-attribute preference model (MAPM) was constructed. MAPM model ranking was consistent with the actual project management team residual risk ranking as well as the ranking determined by the project's risk scoring scheme. While we found differing risk acceptance behaviors among project team members, the MAPM model generally agreed with the team's actual ranking decisions. However, the MAPM model showed incongruences between the risk scoring scheme ranking and model outputs in the moderate risk region as compared to the GSFC risk scorecard, which may point to a potential area of disagreement between project management team members when moderate risks must be accepted before flight.

1. Introduction

Residual risk ranking and acceptance decisions are made within the context of a project's Continuous Risk Management (CRM) process. Today, CRM is utilized across many industries as well as U.S. Government agencies to identify and manage risks [8,9,20]. Within this process, key decisions are made such as risk ranking and prioritization, risk-handling strategies, the amount of programmed or reserve resources to be applied for mitigation activities, and eventually the closure or acceptance of residual risks before the product or process is deployed. The outcome of residual risk acceptance decisions can be harmful if made incorrectly. In the space industry, as well as others, if the residual level of risk is improperly characterized or understood, technical requirements or mission objectives may not be met if the risk is realized and in some cases catastrophic consequences may result. The purpose of this research is to examine the characteristics of residual risk acceptance and ranking decisions made before launch by senior project team members. In an effort to enhance understanding of the decision framework, Multi-Attribute Preference Model (MAPM), in combination with the project risk scoring scheme (also referred to as risk matrix or probability-impact diagram), will be used to further understand this framework. Two NASA flight projects were used as representative case studies and while the dataset for this field study is limited, the eventual goal is to be able to apply this research across multiple space flight projects. For the current effort, the Magnetospheric Multiscale Mission (MMS) and Discover (DSCOVR) Projects, both in-house development efforts at the Goddard Space Flight Center in Greenbelt, Maryland, USA, were used to pilot the research methodology and data analysis. How are residual risk ranking and acceptance decisions structured at the project management team level? Additionally, how multi-attribute preference modeling contributes to explaining residual risk ranking and risk acceptance behaviors of the team and the performance of the risk scoring matrix will also be explored.

1.1. Motivation

The primary motivation for this research was to try to make implicit risk ranking decisions, residual risk acceptance decisions, and risk acceptance behavior of project management team members explicit, discoverable, and useful for researchers as well as practitioners. The secondary motivation was to examine the performance of risk scoring matrices as a risk ranking and decision support tool vis-à-vis the factors noted above and how their use and construction might be improved. The tertiary motivation was

* Corresponding author.
E-mail addresses: dmlengyel@icloud.com (D.M. Lengyel), mazzu@gwu.edu (T.A. Mazzuchi).

https://doi.org/10.1016/j.jsse.2017.11.004
2468-8967/

to determine the efficacy of using MAPM to model residual risk ranking and acceptance decisions.

1.2. Continuous Risk Management (CRM) at NASA

NASA flight projects are required to perform CRM (NPR 8000.4, 2014). Implementation, including risk scoring schemes, may be tailored across projects but the basic procedures have been routinized over the last 20+ years. The CRM process consists of identifying, analyzing, planning, tracking and controlling risks—communication and documentation are integral to the framework and apply to all of the steps [9]. NASA utilizes the classic five by five (5×5) matrix in which risks are assessed for likelihood and consequences. The latter include cost, schedule, technical and safety attributes. The 5×5 matrix is sometimes referred to as the probability-impact diagram, or PID, and is used in conjunction with the project's risk scoring scheme to plot risks. Location on the PID indicates the risk likelihood and consequence as well as general risk level (low-green, moderate-yellow or high-red). Most of the risks accepted before launch of GSFC projects will generally be in either the low (green) or lower moderate (yellow) region of the PID.

The risk scoring matrix, for both the MMS and DSCOVR projects, was adopted in full from the GSFC risk requirements document [12] and is shown in Fig. 1 below. Note the quantitative boundaries for the respective ordinal scores of one through five for likelihood as well as the linguistic, or qualitative, definitions for the consequences of safety, technical, schedule and cost.

A nuance of the GSFC risk scoring process is that risks are first categorized as cost/schedule, technical or safety. They are then scored for consequence and likelihood for that specific category. Early in the project most of the risks are cost/schedule related. Some of these risks however may be reclassified later in the project (e.g. after system integration and test) and therefore rescored if the technical component becomes the driver.

As a NASA flight project moves from design, development, test and evaluation (DDT&E) phases, risks are identified and those warranting attention are mitigated to acceptable levels. In general, a fraction of the risks identified cannot be closed out before launch and management must decide to accept the residual risk remaining. In many cases the mitigation plans have been exhausted and short of delaying launch or cancelling the project, there is nothing that can be done to mitigate them further—even risks, which may negatively impact, mission objectives. NASA guidance requires that key stakeholders of a flight project, i.e. senior NASA center and headquarters management, the principal investigator(s), and the science community involved, must buy into the residual risk being accepted.

2. Related literature

The proposed research requires a review and integration of two research paths acceptable risk and decision theory. The research gap will be discussed within the context of these integrated paths.

2.1. Acceptable risk

NASA defines acceptable risk as:

> "The risk that is understood and agreed to by the program or project, Governing Program Management Council (GPMC), Mission Directorate, and other customer(s) such that no further specific mitigating action is required. (Some mitigating actions might have already occurred) [28]."

During the course of any program or project, risks are identified and a handling strategy is determined to watch, research, transfer, mitigate, or accept risks. Generally speaking, high and moderate-level risks are mitigated to a lower, or acceptable, level at which point a decision is taken to close or accept the risks. Normally, at that point, the perceived residual risk level as defined by the remaining open risks is believed to be well-defined and acceptable to key stakeholders. These open (referred to at this point as "residual risks") are then ranked and presented to key stakeholders for acceptance. This process is supported by the realization that there is a tradeoff between the remaining risks and the cost and schedule to further mitigate those risks [25,29,21,35].

It has been noted that risk tolerance of managers making the decision to accept risk can be inconsistent especially as it applies to acceptance criteria [11]. Several authors caution that the interpretation of risk acceptance criteria as decision support aids should be used as benchmarks rather than rigid rules [15]. In the safety domain, arguments have been made for ranking of risks according to the expected value of losses or other utility functions to account for risk aversion [29]. Cox notes that, "the information in a risk matrix represents a mixture of factual (probability and consequence) information about the risk and (usually unstated) psychological information about the risk attitude of the person or people performing the risk categorization (2009)."

Comparing the acceptability of residual risks requires a comparison of their attributes. This can be accomplished qualitatively or quantitatively or using a combination of both techniques. Deciding on acceptability of risks involves first determining the significance of the risk, which is dependent on risk criteria. Thus, establishing risk acceptance criteria is in fact an exercise in determining how safe is safe enough. In their 2013 annual report, NASA's Aerospace Safety Advisory Panel noted that:

> "There are several definitions of risk management in aerospace acquisition, but at its most basic level, safety risk management has three primary elements: (1) risk identification and characterization, (2) risk minimization, and (3) determination of when the remaining risk is low enough to be acceptable."

In the space flight domain, understanding residual risk for the first flight of any system is aided by system safety tools/processes such as probabilistic risk analysis (PRA), hazard analysis, failure modes and effects analysis and fault trees. However, due to the fact that almost all verification modalities are subject to some error and the reliability of newer systems/sub-systems is based on predictions, the success or failure of a vehicle's first flight or a spacecraft's commissioning on orbit is an event with several unknowns. In a recent update to their risk management policy document, NASA states,

> "When a decision is made to accept a risk, the manager shall ensure that each acceptance is clearly documented in their organizational unit's risk database (list), including the rationale for acceptance, the assumptions and conditions (including programmatic constraints) on which the acceptance is based, and the applicable risk acceptance criteria [27]."

2.2. Decision theory

Risk-informed decision-making has been extensively studied for decades. Several competing theories and models exist to explain attributes of the decision-makers behavior. Many of these models, such as Multi-Attribute Utility Theory [5,17] and Analytic Hierarchy Process [32]—are normative and some, such as Cumulative Prospect Theory (CPT), are descriptive [16]. Decision trees have been utilized [13,30] to better visualize and communicate risk acceptance decisions.

A decision taken to accept risks, particularly risks designated as top project risks, implies that project management and key