https://ntrs.nasa.gov/search.jsp?R=20190001306 2020-05-09T22:24:55+00:00Z

Valuing Rigor in the Risk Management Process

Robin L. Dillon
Georgetown University
Washington, DC 20057
202-687-5398
Rld9@georgetown.edu

Gerald A. Klein, Jr.
NASA Goddard Space Flight Center
Greenbelt, MD 20771
240-684-0954
gerald.a.klein@nasa.gov

Edward W. Rogers
NASA Goddard Space Flight Center
Greenbelt, MD 20771
301 286-4467
ed.rogers@nasa.gov

Christopher J. Scolese
NASA Goddard Space Flight Center
Greenbelt, MD 20771
cscolese@nasa.gov

***Abstract*—NASA, as an organization, takes risk management (RM) seriously, and for most projects, the risk management process is exemplar. There can be challenges, though, with defining RM processes. For example, many different risk analysis methodologies are available, they can be applied with varying degrees of rigor, and they can have different value depending on how projects use them. In particular, risk analysis methodologies vary considerably in the level of quantitative detail, with more probabilistic techniques encouraged in some situations. We discussed these processes and methodologies with ten project managers (PM) at the NASA Goddard Space Flight Center (GSFC). Our intent was not to prove with some level of statistical significance that some are more helpful than others, but rather to obtain a general understanding of how projects are identifying, and thinking, about risks. This paper describes some of the available risk processes and methodologies, and provides some insights about the benefits that can gained from their use. We provide an in-depth discussion of one quantitative methodology, Probabilistic Risk Assessments (PRAs), and conclude with a few insights from observed best practices.**

TABLE OF CONTENTS

1. INTRODUCTION 1
2. THE COMPLEX RELATIONSHIP BETWEEN RISKS AND ESCALATION OF COMMITMENT 2
3. COMMONLY USED RISK PROCESSES AND METHODOLOGIES 3
4. AN ANALYSIS OF THE VALUE OF ANALYSIS 5
5. PROBABILISTIC RISK ASSESSMENT 9
6. BEST PRACTICES 10
ACKNOWLEDGEMENTS 11
REFERENCES 11
BIOGRAPHY 12

1. INTRODUCTION

NASA has developed requirements, procedures, and process guidelines to establish, implement, and manage effective risk management processes [1,2]. The guidelines, however, leave much of the details of the process implementation to individual project managers to determine (e.g., how often risk lists are updated, etc.); a significant aspect of this is that different project managers will approach risk management processes with different degrees of rigor and vigilance. For example, an interesting observation from Dillon, Klein, Rogers, and Scolese [3] is how widely projects vary in their risk management process execution. Variation in project size is a reasonable factor contributing to variation in risk management methodologies and processes; Table 1 illustrates this by showing the number of unique risks documented in the GSFC Flight Projects Directorate (FPD) Cross-Cutting Risk Framework database between July 2015 and July 2017. Focusing on only the Class B projects in Phase D, of which there were seven, the number of risks documented in the two year period for each project were 2, 4, 17, 21, 26, 65, and 121. While there is not a "correct" number of risks for a project to identify (and the authors acknowledge that the identification of risks depends on many specific project factors), the variance between 2 and 121 is certainly worth noting. It certainly appeared to the authors that the degree of rigor applied to the risk management process from project to project was more diverse than anticipated.

Table 1 – Unique Risks Documented in Cross Cutting Risk Framework Database by Project [3]

Project ID	Number of unique risks	Project size and project phase between 7/15- 7/17
1	**21**	**Class B, Phase D**
2	14	Class A, Phases C & D
4	**2**	**Class B, Phase D**
5	77	Class B, Phases B & C
6	**26**	**Class B, Phase D**
7	**17**	**Class B, Phase D**
8	**4**	**Class B, Phase D**
9	47	Class B, Phase N/A
12	6	Class N/A, Phase N/A
13	**121**	**Class B, Phase D**
15	26	Class C, Phase C
16	3	Class N/A, Phase N/A
17	**65**	**Class B, Phase D**
19	33	Class C, Phase D
20	80	Class B, Phase B
21	11	Class B, Phases B & C
22	32	Class C, Phase C
24	3	Class N/A, Phase N/A
25	33	Class C, Phase D
26	44	Class C, Phase C
27	11	Class N/A, Phase N/A

978-1-5386-6854-2/19/$31.00 ©2019 IEEE

It appeared that some project managers find risk management processes extremely valuable, and others find the process less helpful, thus only minimally implementing the process to meet risk process requirements ("check off a box"). Many situations could have occurred to unintentionally reinforce a project manager's negativity toward the risk management process. For example, PMs could have experienced the following on previous projects:

- Low-probability, high-consequence events that were nearly impossible to predict ("Black Swans") and were thus not identified by the risk management process, leaving the impression that the RM process is not an effective method of preventing problems.
- Risk management process investment outweighed the expected return. Some reasons could include:
    - Too bureaucratic or complicated to be efficient or helpful to the project
    - Risk analysis tasks that took too long and thus delayed other project activities.
    - Too many risks were identified, and thus too much noise and busy work attached to the risk management process, resulting in a lack of focus on the most important ("real") risks.

For the undetected, undesirable, events, adopting systematic risk management processes (while not perfect), should reduce the likelihood of such events occurring on future projects. As Paté-Cornell [4, p. 1828] states "Risk analysis is thus an alternative to the 'stuff happens' philosophy – ignoring signals and deciding that accidents are 'normal' events or are too unlikely to be accounted for." But as is emphasized in the NASA risk guidelines [1,2], and in most best practice recommendations for risk management, the amount of effort expended in a RM process should depend on the value of the mission. The more expensive the mission, the more warranted are increased investments in rigorous risk management processes to seek out small probability, high consequence events.

In the second case, where one's experience is with poorly-implemented RM processes, the insights and suggestions described here should help future projects balance the costs of an effective, efficient, risk management process against its benefits.

2. The Complex Relationship between Risks and Escalation of Commitment

Decades of academic research have examined the effect of risks on decision-making behavior. Generally, the conclusion is that the relationship between risks and decision making is complicated by many different contributing factors. For example, some studies [5] find that individuals with past successes will be risk-averse in future decision making (to protect prior gains), and others [6] find decision-makers, with past successes, will take more risks based on confidence from prior successes. We are particularly concerned about the linkages between risks, risk management processes, and escalation of commitment decisions.

The escalation-of-commitment "bias" refers to the tendency of people, in the face of negative consequences, to increase resource commitment, and risk further losses [7,8]. This tendency makes risks, and escalation of commitment, explicitly linked. If projects do not have significant issues arise (i.e., realized risks), they would not need to escalate commitment.

A consistent finding in project management is that, as projects approach their final stages, strong desires for completion (and at NASA, strong needs for project success) affect resource allocation decisions; while at earlier project stages, risks can have a more significant role in influencing resource-allocation decisions [8]. This shifting focus across a project's timeline becomes a challenge for projects, especially for the projects with smaller budgets. Table 2 describes the characteristics of project classes from NPR 8705.4 NASA Procedural Requirements, Appendix D [9]. The implication of deeming a project as a Class C or D, should allow more risk tradeoffs to be made on the project. At earlier stages in the project, when risks are influencing allocation decisions, this may be true, but as projects approach the final life cycle stages, the need for completion, and the strong desire for success, tend to overtake a willingness to take risks. At a recent GSFC Masters Forum, a common concern raised by many was that despite initial risk-based decisions made in the project life cycle, "*on the pad, every project is Class A.*" This effect can easily contribute to inconsistent decisions regarding risk across different project phases, and an unwarranted escalation of commitment in late phases when unanticipated problems arise.

Table 2 – Some Classification Considerations for NASA Class A-D Payloads [9, Appendix B]

	Class A	Class B	Class C	Class D
Agency Priority	High	High	Medium	Low
National significance	Very high	High	Medium	Low to medium
Mission Lifetime	Long > 5 yrs	Medium 2-5 yrs	Short < 2 yrs	Short < 2 yrs
Cost	High	High to medium	Medium to low	Low
Alternative Opportunities for Science Collection/ Reflight	None	Few	Some	Many

Additionally, academic research indicates that if problems were identified in advance by the risk management process, and thus were "expected to occur", this encourages project managers to continue with the project even if it means an escalation of commitment because the project is perceived to

be "on-track" [10]. The implication is that if projects do a sufficient job identifying critical risks, then when problems arise that were linked to identified risks, project managers may be convinced that the project is proceeding well, despite the remaining significant challenges. This is where a minimalist RM process, that identifies risks, but only does a cursory job understanding the implications and mitigation actions for the risks, would be less helpful than a risk management process that fully details, tracks, and effectively mitigates these risks. A minimalist risk process that identifies, but does not thoroughly characterize the risks may reinforce an unjustified escalation of commitment.

We next describe multiple methodologies and processes that can contribute to an effective RM process, and explore the value of different degrees of rigor.

3. COMMONLY USED RISK PROCESSES AND METHODOLOGIES

As part of the GSFC-specific Risk Management Training course at NASA's Goddard Space Flight Center [11], students are instructed on many topics including the NASA Continuous Risk Management (CRM) process steps. The first step in CRM is "Identify the risks", and the students are encouraged to recognize that risks can come from many sources. The other steps are: Analyze, Plan, Track, Control, and Document & Communicate. The course also provides a list of some useful sources for identifying risks. Here are the thirteen areas highlighted in the course as potential sources for identifying risks:

Trade studies – an activity used to identify the preferred technical solution among a set of alternatives. Trade studies should document the decision making process to enable traceability and repeatability. There are numerous techniques that can be applied to conduct a trade study, and like most risk analysis methodologies, trade studies need to be tailored to the specific problem circumstances. Risks associated with project tradeoffs should be identified and entered into the project "risk register."

Safety/Hazard analysis – an activity used to identify hazards that may arise on the project, or be caused by the project; the goal of a safety/hazard analysis is to reduce these risks. The safety/hazard analysis should document the potential negative consequences that could occur while examining the potential causes of such consequences, documenting the hazards and the probability that these hazards could occur. The method of safety/hazard analysis, and reliability analysis, may overlap (e.g., a Failure Mode and Effect Analysis could be used for either purpose).

Independent project reviews – a review involving unbiased, external experts, often conducted at major project milestones, to assess a project's progress and evaluate a team's ability to meet mission objectives. These outside experts often identify new risks for the project during the course of the review.

Technical Peer Reviews – a review involving a team of peers, not directly involved with the project, who have the subject matter expertise pertaining to the topic being reviewed. Risks are often identified in the course of the review, frequently from problems that cannot be resolved during the technical peer review.

Reliability analysis – an activity used to examine ways the project, or system, can fail. For our purposes, we discuss non-probabilistic methodologies separate from probabilistic risk assessments. A common reliability analysis methodology (that may also be used in safety/hazard analyses) is a Failure Mode and Effect Analysis (FMEA). The FMEA is an inductive analysis that systematically details, on a component-by-component basis, all possible failure modes, and identifies their resulting effects on the entire system. Possible single-failure modes of each component in a system are identified and analyzed to determine the effect on surrounding components, as well as the entire system. Most FMEAs also include a component criticality score, and one of the most common methods is to assign a Risk Priority Number (RPN) to the possible failure of a specific component.

Probabilistic Risk Assessment (PRA) – an activity that incorporates a system functional analysis to identify failure modes with estimates of the probabilities of external events and component failures, to quantify failure probability. The probabilistic risk assessment process starts with an identification of sequence initiating events, computation of the probabilities of reaching different final systems states given these initiating events, and the evaluation of the consequences of different degrees of system failure. Common methodologies include Fault Tree/Event Tree modeling and System Simulation (Monte Carlo techniques). The results of a PRA are often represented by a probability distribution of different potential system states (i.e., a risk curve) based on best estimates of the model and parameter values.

Problem Failure Reports – a report documenting non-conformances, failures, or anomalies, that have been detected during inspection or testing. Depending on the impact to the project, the documented condition may be a project risk, or issue.

Monthly status reports (external) – reports from partners, contractors, etc. that provide the current status of the work and the achieved progress during the reporting period. Risk and issues are required content and flow into the project RM process.

Budget Estimates – the budget estimate establishes the cost constraint for the project. As the project is developed, budget challenges will become risks, and budget reserves will bound risk mitigation options.

Schedule Reviews – the project schedule establishes the time constraint for the project. Risks that will delay project progress are identified in routine project schedule reviews and major milestone reviews.

Table 3- Importance of Risk Processes and Methodologies

	Average	Minimum	Maximum
Trade Studies	4.3	3	5
Technical Peer Reviews	4.2	3	5
Risk Brainstorming Sessions	4.1	2	5
Schedule Reviews	4.0	2	5
Meeting Discussions	3.9	2	5
Problem Failure Reports	3.9	3	5
Forward Thinking Mindset	3.9	1	5
Monthly Status Reports	3.8	2	5
Budget Estimates	3.6	2	5
Safety/Hazard Analyses	3.3	1	5
Reliability Analyses	3.1	1	5
Independent Project Reviews	3.0	1	5
Probabilistic Risk Assessments	2.7	1	4

Meeting discussions – during the course of routine project meeting discussions, risks are often identified. These risks should be considered for entry into the project risk register for formal tracking and mitigation.

Forward Thinking mindset – it is important that project leadership has a constant focus on what still needs to happen, and the challenges associated with those pending activities. Since the NASA workforce it typically made up of individuals with a forte of problem-solving, it is often a challenge to get them to focus on *future* problems, rather than the "problem du jour."

Risk Brainstorming sessions – sessions dedicated to identifying risks by answering: 1) what can go wrong, 2) how likely is it, and 3) what are the consequences. These sessions could include a pre-mortem discussion in which a project team imagines that the project has failed, and then works backward to determine what could cause such a failure. These meetings are typically in addition to other RM meetings and are productive while preparing for major milestone reviews.

We discussed these thirteen processes and methodologies with ten project managers at the NASA Goddard Space Flight Center to better understand the degree with which they influenced the project RM process. Our intent was not to prove, with some level of statistical significance, that some processes, or methodologies, are more helpful than others, but rather to obtain a general understanding of how projects are identifying (and thinking about) risks.

The PMs were asked to assess, on a 5-point scale, where 1 = not at all important, and 5 = extremely important, how important each process, or methodology, was for their project's risk-informed decision-making process (on their current project, or a recent project). Table 3 illustrates the average PM's assessment for each process/methodology. As was the case with the variance of risks being recorded by the projects, within our ten project managers, there was significant diversity of opinions (amplified by the fact that our sample involved many different types of projects). Therefore, we also report the minimum, and maximum, scores that each item received.

For the purpose of discussion, we will consider the data with a median split, i.e., any value below the median is placed in the "Less Important" category, and any value above the median is placed in the "More Important" category. The median importance score for the data shown in Table 2 is 3.9. Several observations about the assessments include:

- Trade studies and technical peer reviews are processes to closely identify and manage technical challenges that are occurring on a project, so it makes sense that these methodologies would be a useful source for identifying risks.
- While not every project conducted risk brainstorming activities, those that did, find them to be very useful. Additionally, the NASA Risk Handbook [1, p. 100] recommends brainstorming activities as a common method for identifying risks. Some project managers stated that risk brainstorming consistently occurred every time their Risk Board met, making additional risk brainstorming meetings unnecessary.
- The processes and methodologies that ranked around the median were mostly those that occurred as part of project implementation, such as schedule reviews and meeting discussions. It is interesting to note that our sample of PMs found schedule reviews to be more helpful for identifying risks than cost estimates. This makes sense because technical, and other challenges, result in schedule delays, which increases cost.
- Independent project reviews were ranked less important in identifying risks. A common PM perception is that the value of independent project reviews is in the preparation for the review, i.e., a focus on the overall risk posture, and what risks may be *missing*, rather than the review itself.
- Probabilistic Risk Assessments were clearly identified as less important than other methodologies for identifying risks, and we will discuss in a subsequent section.

While not trying to draw strong conclusions from our small sample of project managers, processes and methodologies that, for the most part, are occurring on the project as a matter of routine, without the explicit purpose to identify risks (e.g., trade studies, schedule review, meeting discussions, and problem failure reports), are important sources for identifying

risks. Additionally, processes and methodologies that facilitate communication, and discussion among the team, and provide input from other organizational units (e.g., brainstorming, reviews, meeting discussions, and monthly status reports), were also highlighted as important for risk identification.

4. AN ANALYSIS OF THE VALUE OF ANALYSIS

In 1968, Matheson explored "The Economic Value of Analysis and Computation" [12]. His basic model considered a decision problem and several analytical procedures that could be used to analyze the problem. The procedures varied in the amount of information each could provide concerning uncertain parameters that affected the decision. He used value of information calculations to determine the economic benefit of each additional type of analysis. For the expected-value (risk neutral) decision maker, the value of information is the difference between the expected value of the outcomes of the best decision alternative with, and without, the additional information gained from the additional analysis after accounting for the costs in obtaining the information. We use this concept to illustrate a method of thinking about the optimal level of risk analysis given the decisions that the risk analysis is going to support. We assume that the decision maker wants to minimize the expected value of the overall risk costs. In what follows, we assume that the decision maker is risk neutral.

Risk analysis methods are evaluated here based on four characteristics:

- the ability to detect potential problems before they occur,
- the capability to support more effective corrective actions, such as mitigating the consequences over and above what would normally occur,
- the costs of the analysis method, of corrective actions, and of undetected problems, and
- the cost savings if earlier detection of problems can occur.

Figure 1 shows an influence diagram that depicts the relationships among the factors needed to quantify the value of different analyses. Circles represent uncertainties, and squares are decisions that are made. The rounded rectangle is the measurable outcome, and in this discussion, is only measured in terms of costs. The uncertainties include:

- the probability that a potential problem (risk) exists during development,
- the likelihood of any evidence, or warning signs, of the potential problem, if it exists,
- the likelihood of detecting the potential problem, conditional on the potential problem existing and any evidence, and
- the possible outcomes of the project, conditional on whether or not, a potential problem exists, it is detected before a problem occurs, and what corrective actions have been taken to prevent the problem from occurring.

For different risk analyses, we assume the probability of detection varies given the amount of evidence, or warning signs.

The decisions in the model are: what risk analysis methods to use, and what mitigating (or corrective actions) to take if a problem is discovered. The value of the analysis is the difference between the expected project costs with the selected analysis, less the expected value of the project without the analysis (or as in the example to be described a more rigorous level of risk analysis versus a less rigorous analysis).

In general, the results of such an analysis will be highly sensitive to the type of problem, the probability of detection of problems given the risk analysis method, and the probability of failure for the system given no detection of the problems. These should be the factors that a project manager considers when planning a risk management process.

The value of a particular risk management process can be estimated by the difference between the expected costs of the outcomes of the best decisions based on the analysis and the expected value of the risk costs for the system that would be constructed otherwise. The identification of the optimal choice of risk analysis methodologies should be based on an incremental analysis of each possible methodology compared to the previous one based on increments of costs, and on increments of the probability of potential problem detection. This implies that one should be willing to spend an incremental cost for risk analysis if the expected benefits from an improved risk detection process justify the additional costs. If project managers are actively mitigating future problems routinely through project risk management, the cost savings should not only offset the risk management costs, but have the potential to provide additional margin for "Black Swans."

Illustration of Approach

Assume that for the development of a project, the manager believes that there is a 10% probability that a significant problem exists that has yet to be detected. The PM is trying to choose the best level of investment in a risk management process. The choices are a minimalist approach, which will add $15,000 to the cost of the project, versus an aggressive approach which will add $100,000 to the cost of the project. The full decision tree for this illustration is divided into Figures 2-4; Figure 2 shows the two choices available for risk management, Figure 3 shows the top branch of the decision tree.

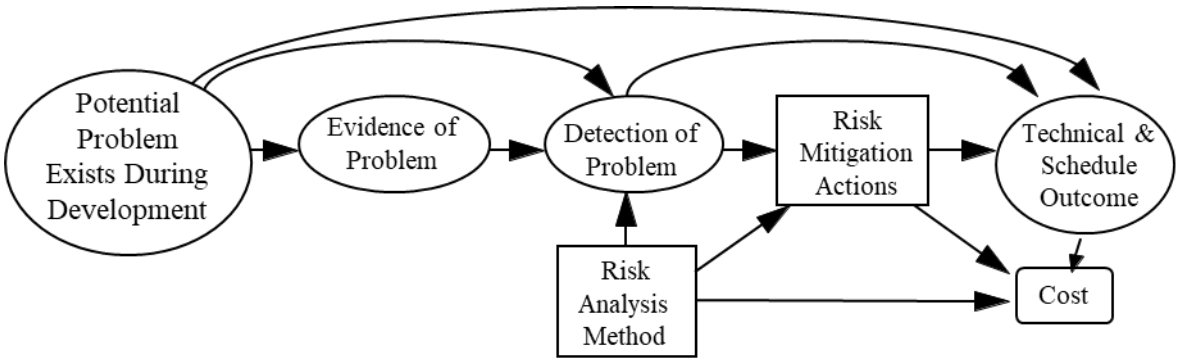


Figure 1- Influence Diagram for Quantifying the Value of Analysis

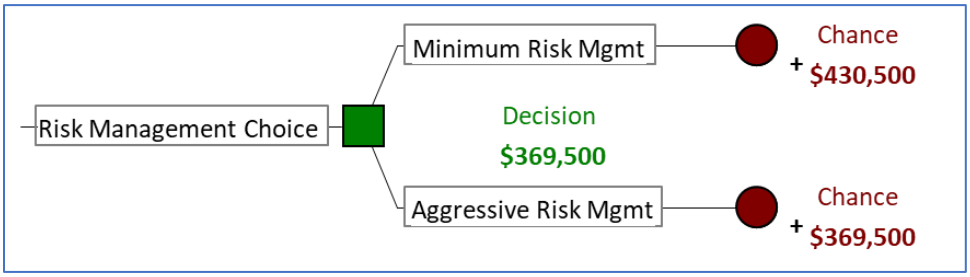


Figure 2 – Illustration of Analysis of Value of Analysis

Table 4- Sensitivity Analysis of Probability of Initial Problem

Probability of Initial Problem	Minimalist Risk Management Approach	Aggressive Risk Management Approach	Value of Enhanced Risk Management Approach
1%	$56,550	$126,950	-$70,400
5%	$222,750	$234,750	-$12,000
10%	$430,500	$369,500	$61,000
20%	$846,000	$639,000	$207,000
30%	$1,261,500	$908,500	$353,000

Given that the choice is the minimalist risk approach, Figure 3 shows the probabilities of (1) warning signals to the problem being available, (2) detecting the problem earlier, or later, given the risk management approach, and (3) project failure given detection and corrective action with, and without, detection. Figure 4 shows the corresponding probabilities for the aggressive risk management approach. In both branches, assume corrective actions cost $500,000 if the problem is found early, and $1,000,000 if the problem is found later. Also assume that if "failure" occurs, the cost to the project is $10,000,000. In the example, the expected cost of the minimalist risk management alternative is $430,500, and the expected cost of the aggressive risk management alternative is $369,500 (see Figure 2), an expected value savings of $61,000 after inclusion of the different costs of the two risk management processes. This difference comes from the fact that for the same initial design, the aggressive risk management process is detecting and correcting the problem more efficiently than the additional costs of the process. Therefore, in this illustration, the decision-maker should choose the more aggressive risk management process, and the expected value of the analysis is a cost savings of $61,000. This savings, however, is highly sensitive to the probabilities and costs assumed in the illustration. For example, Table 4 shows the savings (or lack thereof) if the probability of an initial undetected problem varies between 1% and 30%. For the lesser probabilities, if there are not problems to be found, the more aggressive risk management process does not have value, but as the likelihood of problems increases, the value of the more aggressive process increases.

In summary, a value of analysis calculation can provide important information in deciding the appropriate level of risk analysis, and management, to perform for a project and the approximate resources that should be allocated to the process, or analysis. In deciding on the appropriate level of analysis, the relevant factors include:

- the type of decision
- the data already available
- the level of uncertainty
- the risk attitude of the decision maker
- the costs of the mission and of the proposed analysis

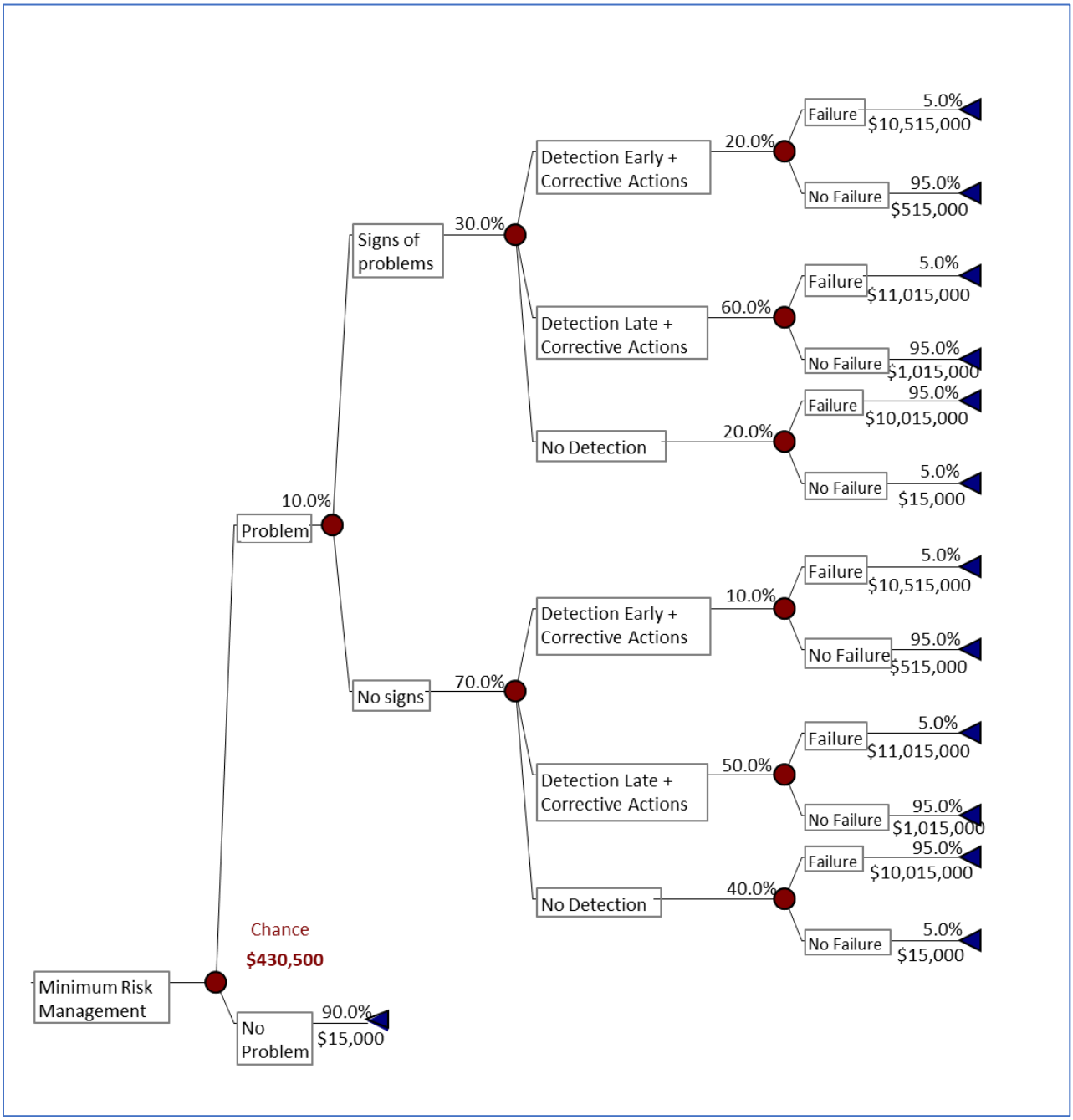


Figure 3- Example: Branch for the Minimum Risk Management Process

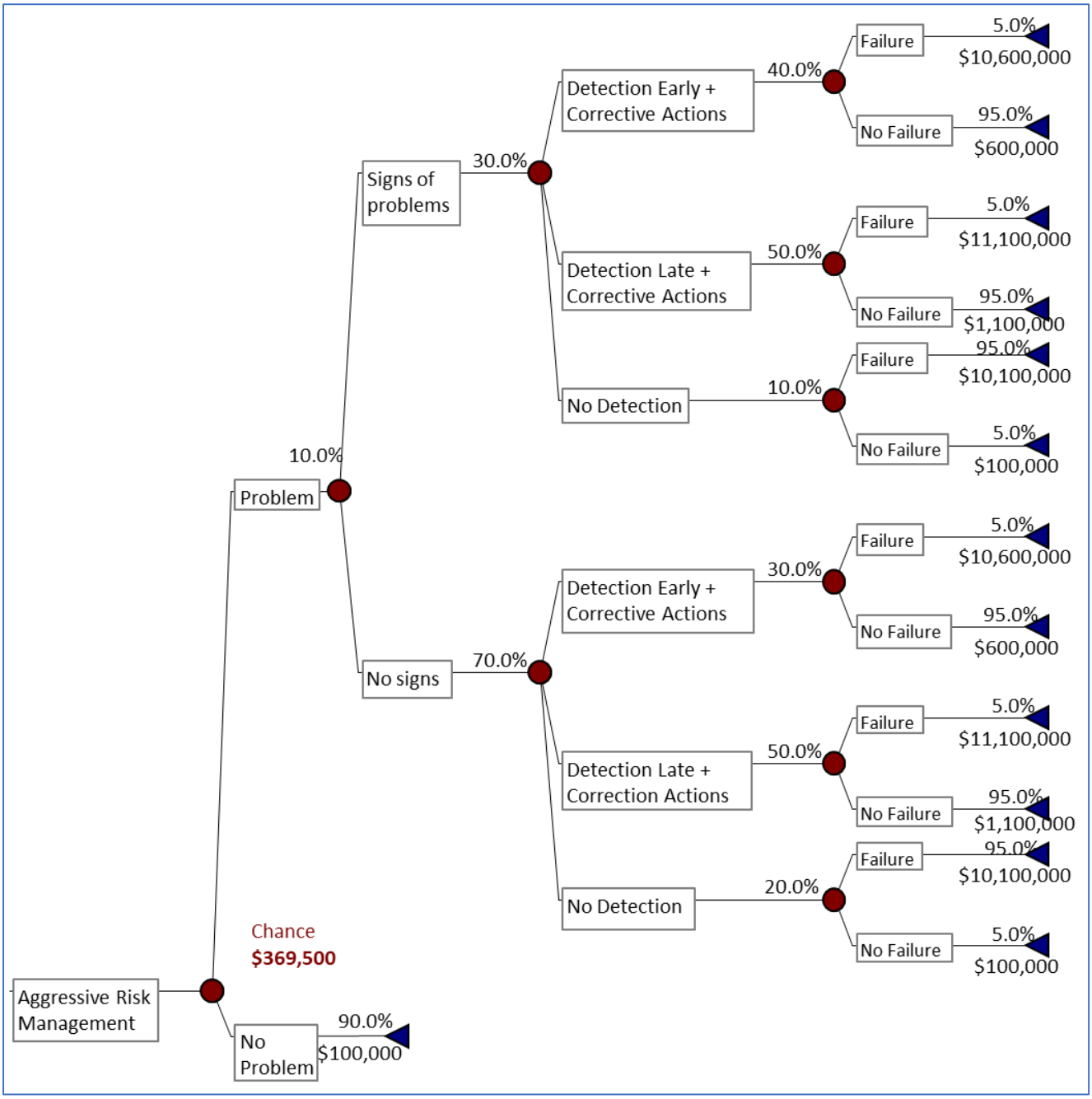


Figure 4 - Example: Branch for the Aggressive Risk Management Process

The illustration described demonstrates the type of thoughts that should be used to consider the value of investing additional resources in a more aggressive risk management process. In reality, the baseline risk in the GSFC project environment is very high, particularly since the technical challenges are routinely extreme. Given the factors to consider, logic dictates that an aggressive approach to risk management should be adopted for all projects, unless otherwise justified.

5. PROBABILISTIC RISK ASSESSMENT

Of the 13 RM processes and methodologies listed in Table 3, generally, the most costly is the PRA; consequently, it is typically only performed on large budget, high-visibility projects. More commonly, less-costly, similar, analyses are performed on projects with smaller budgets, sometimes referred to as "lower-case PRAs" (pra).

Probabilistic risk assessment is a group of techniques that incorporate variability and uncertainty into risk assessments [13, 14, 15]. PRA can be used to support decision risk management by clearly characterizing the impacts of uncertainties on potential decision alternatives.

The alternative to a PRA is a risk assessment with a single point estimate of risk (pra), and usually some brief qualitative descriptions of uncertainty. The PRA on the other hand does not generate a single point estimate, but rather produces a probability distribution of the range of consequences that could occur, providing more information to decision makers [13, 14, 15].

PRA approaches will tend to be more data intensive than non-PRA approaches, and thus will require additional time, financial, and analytic resources to obtain the needed probabilistic input data for each aspect of the risk assessment, and for aggregating the input data into a full characterization of the uncertainty of the system. As more projects incorporate probabilistic designs in risk assessment, and an organization gains more experience, the costs of PRA (relative to other methods) could decline.

We will not repeat the procedures to perform a PRA here, referring the reader to NASA's *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners* [15]. Instead, we will focus on when PRA is most helpful, and what significant challenges remain in the use of PRA.

When is a Probabilistic Risk Analysis Most Helpful

Using the logic outlined in the previous section regarding the value of the analysis, we identify several important system factors that will likely justify the PRA effort. These include:

- If high quality probabilistic input data are obtainable
- If a probabilistic approach to better characterize the uncertainty can be accomplished in a timely manner
- If there is a reasonable probability of major undetected problems, and sophisticated risk modeling are needed to discover these problems
- If the uncertainty in some aspect of project is very high, and decisions are contentious, or have large resource implications, or if there is a belief that additional data collection would likely lead to a different decision
- If there are major gaps in knowledge, or major assumptions being used in the current level of risk assessment that could be improved with more risk modeling (the risk manager must understand the major assumptions being made in any project risk modeling)
- If the criticality order does not coincide with the actual ranking of risk contributions, (e.g., FMEA might be sufficient when all criticality 1 items are strong risk contributors and non-criticality 1 items are not, and therefore when problem detection in these items is the primary goal)

Challenges of Probabilistic Risk Analysis

Even if a probabilistic risk analysis is justified, there will still be challenges. The three most significant are:

- Getting the needed data
- Creating a transparent model
- Communicating the results

As described in [15], there are many sources of the needed data. For example, if there are applicable historical data, it may be straightforward to derive an uncertainty distribution, but the reality is that there will be few instances where there are enough existing applicable, and relevant, historical data. In those cases, data from subject matter experts may be the only option. For example, a critical decision on ICESat-2 needed to be made after the failure of an instrument laser late in the project lifecycle. While the instrument has two lasers, and only one needs to be functioning (i.e., the second is a back-up), once the first one failed during development, it was considered a serious possibility that the second one would do the same. But without substantial past failure data for this unique laser, how likely is something if it is a "serious possibility"? In 1951, Sherman Kent, working with the CIA, interviewed members of the Board of National Estimates and learned that a "serious possibility" could mean anything from 20% to 80% depending on the person being interviewed [16]. Without a good way to technically derive the failure probabilities of the lasers, and because of the consequences if they did fail, the project ultimately assumed that the failure was likely enough to invest extra resources replacing it.

There is value in a probabilistic risk analysis when there are reasonable chances of undetected problems. But consider that undetected problems are commonly at the interface of systems, and PRA models that consider all the multiple possible interdependent component interfaces could become a very complex model, very quickly. PRA models that are *too* complex are less valuable. For example, the National Academy of Sciences criticized a PRA developed by the Department of Homeland Security called the Biological Threat Risk Assessment (BTRA). The National Academy report criticized the BTRA as having "great complexity, which requires many more SME (Subject Matter Expert)

estimates than can be supported by the limited base of knowledge about biological terrorism. It also precludes transparency, adequate sensitivity analysis, and validation" [17].

The third challenge, the dissemination of a statistical distribution, or probability output number, should be considered carefully given the quality, and coverage, of the input data. A PRA model that has been created with probabilistic input data, that was not high quality, could lead the decision maker to a false sense of confidence, or costly, unnecessary "corrective action." One output of a PRA model should be a clear characterization of how confident decision makers should be in their choices, based on the analysis (i.e., how uncertain is the uncertainty?).

Also, research has shown that the ability of decision makers to deal with concepts of probability, and uncertainty, varies. For example, Krupnick et al. [18] concluded that most people have difficulty understanding information on uncertainty with conventional scientific presentation approaches. This study highlighted the need for practical strategies for the communication of PRA results and uncertainty information between risk analysts, decision makers, and other stakeholders.

Finally, PRA models can be problematic, just like any analysis. Poorly performed PRA models could result in worse decisions if the probabilistic data used in quantification have significant errors. For example, if the relative criticality of different scenarios is misstated, then resources could be diverted from the prevention of more likely scenarios, to prevention of less likely ones. If the overall risk is overstated, or understated, this would distort the priorities for different prevention measures. Also, the absolute benefit of any given prevention measure could be in error. All of these issues can misinform the decision maker.

While the optimal level of quantitative analysis should be determined for a specific mission, in general, PRA is needed when decisions need to be made that involve high stakes in a complex situation, as in a high-hazard mission with critical functions being performed by complex systems, and where high quality input data are available. Being able to carefully manage project resources requires good risk models, and allocating project resources to further uncertainties needs to be informed by insight into which uncertainties' resolution offers the greatest benefit.

Parallels to Joint Cost and Schedule Confidence Level Analysis

While the previous section focused on benefits and challenges to PRA, similar benefits and challenges are also generally present in NASA's Joint Cost and Schedule Confidence Level (JCL) analysis. The goal of a JCL is to identify the probability that a given project cost will be equal to, or less than, some defined cost level, and that the schedule will be equal to, or earlier than, a specific date [19]. In order to produce an accurate JCL, analysts must understand where significant project risks exist and be able to model uncertainty using current, and historical, data. These significant risks need to be included as uncertain impacts in the schedule, which, when realized, impact the cost estimates [19]. Similar to PRAs, JCLs have a challenge with data. For example, the NASA guidance for JCL states, "[u]nfortunately, it is rarely the case that data exist to justify all the uncertainty distributions required for JCL analysis" [19, p. 34]. Additionally, even if the challenge of accurately identifying risks with probability distributions is disregarded, it is "nearly impossible to predict the time and budget required to complete many aspects of NASA projects" [19, p. 15].

Similar to PRA, while there are challenges with JCL, in most cases, the benefits of the additional insight are worth the costs. Analysts and projects must invest time and thought in developing credible, and appropriate, models that clearly characterize the uncertainty in the models. Additionally, the models need to be used by decision makers based on the strengths of the model; in particular, its ability to facilitate communication within the project, and with external stakeholders.

6. BEST PRACTICES

In conclusion, we provide a few insights from observed best practices.

1 - A good risk management process should reduce work load if potential problems are avoided, or at least identified early. The resources invested in a rigorous risk management process should pay for themselves by avoiding problems, or at least detecting them earlier in the project life cycle.

As demonstrated in the illustration described in Table 4, an effective risk management process, that can detect potential problems, can have genuine benefits in terms of a reduction in project's expected costs. Additionally, some of these expected benefits may arise from avoiding an inappropriate escalation of commitment as a project nears completion.

2 - The majority of a project's risks do not require complex analysis to identify, and the process will undoubtedly reap benefits from the communication.

Several project managers that we talked with had significant project risks that did not require complex analyses to detect, e.g., working with liquid methane, planning a satellite servicing mission for a more than twenty year old satellite, etc. Even when the risks were significant, and obvious, project managers praised the communication that risk methodologies and processes can provide, as critical for mission success.

3 - An effective risk management process will bolster communication with external partners, especially international partners.

Echoing the previous insight, that risk processes are

important for the communication they facilitate, this was particularly true on a recent mission partnering with the Japanese Space Agency (JAXA). The risk management process provided an opportunity to overcome different cultural approaches to project management that may have existed between the US and Japanese partners. The Japanese partners saw the opportunity to seek more detail on risks appearing at the interfaces.

4 – The best Risk Boards will have psychological safety and accountability.

With hindsight, the environment on failed projects, or missions, are often described as lacking in "psychological safety" [7]. Roberto [7, p. 144] describes psychological safety as "team members do not believe that the group will not rebuke, marginalize, or penalize individuals for speaking up and challenging prevailing opinions". At a project management forum at Marshall Space Flight Center, that two of the authors attended several years ago, there was concern expressed for how the culture on the Space Shuttle Program around 2000-2002 (just prior to the Columbia Accident) was such that anomalies needed to be handled by individuals, and not reported in tracking systems, since reported anomalies could be detrimental to the space shuttle program staying on its launch schedule. Risk Boards must be forums for open communication about potential problems. This will only occur in an environment with strong psychological safety.

Additionally, research has shown that when a person is accountable for his, or her, behavior to a legitimate, reasonably well-informed audience, whose views are unknown, and who is interested in accuracy, he (or she) will engage in more effortful thought and more self-critical, qualified judgments [20, 21]. Thus, accountability in Risk Boards should enhance the communication, problem solving/avoidance, and the application of all relevant information.

5 – *Project Risk Boards would benefit from best practice formal guidance.*

The insights that we gained from our discussions with a small sample of project managers further emphasized the different approaches that projects take when implementing risk management processes (see for example the spread between minimum and maximum importance scores for the various methodologies described in Table 3). We recommend more detailed guidance be developed based on best practices, e.g., for how often Risk Boards should meet, what is a quorum for a risk board, what should happen at a Risk Board, should minutes be kept, etc.

NASA takes risk management very seriously, and for most projects the risk management process is exemplar. Lessons from these stellar projects should be captured and institutionalized for all projects. This paper is just a small step in that process.

ACKNOWLEDGEMENTS

Robin Dillon's time was supported by the National Science Foundation (CMMI 1757350).

REFERENCES

[1] National Aeronautics and Space Administration (2011) *NASA Risk Management Handbook*, NASA/SP-2011-3422, Version 1, November 2011.

[2] Goddard Space Flight Center (2012) *Risk Management, Goddard Procedural Requirements (GPR),* GPR 7120.4D.

[3] RL Dillon, GA Klein Jr, EW Rogers, CJ Scolese (2018) "Improving the Use of Risk Matrices at NASA," *Proceedings of the IEEE Aerospace Conference*, March 2018.

[4] ME Paté-Cornell (2012) "On 'Black Swans' and 'Perfect Storms': Risk Analysis and Management when Statistics are Not Enough," *Risk Analysis*, 32(11):1823-1833.

[5] D Kahnenman, A Tversky (1979) "Prospect theory: An analysis of decision under risk" *Econometrica* 47: 263-291.

[6] RN Osborn, DH Jackson (1988) "Leaders, riverboat gamblers, or purposeful unintended consequences in the management of complex dangerous technologies" *Academy of Management Journal* 31: 924-947.

[7] MA Roberto (2002) "Lessons from Everest: The Interaction of Cognitive Bias, Psychological Safety and System Complexity," California Management Review 45(1), 136-158.

[8] X He, V Mittal (2007) "The effect of decision risk and project stage on escalation of commitment" *Organizational Behavior and Human Decision Processes* 103: 225-237.

[9] NASA (2004) NASA Procedural Requirements, NPR 8705.4, Washington, DC.

[10] BM Staw, J Ross (1987) "Knowing When to Pull the Plug" *Harvard Business Review*, March 1987.

[11] Goddard Space Flight Center (2018) *Presentation: ABCs of Risk Management,* NASA Goddard Space Flight Center Risk Management Training.

[12] JE Matheson (1968) "The Economic Value of Analysis and Computation," *IEEE Transactions on Systems Science and Cybernetics* 4(3), 325-332.

[13] US Environmental Protection Agency (2014) *Risk Assessment Forum White Paper: Probabilistic Risk Assessment Methods and Case Studies,* EPA/100/R-14/004 July 2014.

[14] US Environmental Protection Agency (2014) *Probabilistic Risk Assessment to Inform Decision Making:*

Frequently Asked Questions, EPA/100/R-14/003 July 2014.

[15] National Aeronautics and Space Administration (2011) *Probabilistic Risks Assessment Procedures Guide for NASA Managers and Practitioners*, NASA/SP-2011-3421, Version 2, December 2011.

[16] A Mauboussin and MJ Mauboussin (2018) "If You Say Something Is 'Likely,' How Likely Do People Think It is?" Harvard Business Review, July 3, 2018, accessed at https://hbr.org/2018/07/if-you-say-something-is-likely-how-likely-do-people-think-it-is on September 4, 2018.

[17] National Research Council (2010) *Review of the Department of Homeland Security's Approach to Risk Analysis*, The National Academies Press: Washington DC.

[18] Krupnick, A., R. Morgenstern, M. Batz, P. Nelson, D. Burtraw, J. Shih, and M. McWilliams. 2006. *Not a Sure Thing: Making Regulatory Choices Under Uncertainty.* Washington, D.C.: Resources for the Future.

[19] NASA (2015) NASA Cost Estimating Handbook Version 4.0 Appendix J: Joint Cost and Schedule Confidence Level (JCL) Analysis, Washington DC.

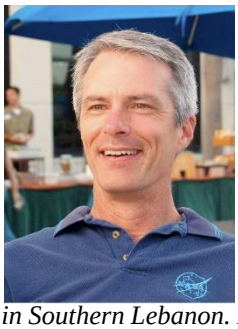
[20] Tetlock, P.E. 1983. Accountability and complexity of thought. *Journal of Personality and Social Psychology*, 45: 74-83.

[21] Lerner, J.S. and Tetlock, P.E. 1999. Accounting for the effects of accountability. *Psychological Bulletin*, 125(2): 255-275.

BIOGRAPHY

Robin L. Dillon *is a Professor in the McDonough School of Business at Georgetown University. Professor Dillon seeks to understand and explain how and why people make the decisions that they do under conditions of uncertainty and risk. This research specifically examines critical decisions that people have made following near-miss events in situations with severe outcomes including hurricane evacuation, terrorism, cybersecurity, and NASA mission management. She has received research funding from the National Science Foundation, NASA, the Department of Defense, and the Department of Homeland Security through USC's National Center for Risk and Economic Analysis for Terrorism Events. She participated as a NASA Summer Faculty Fellow at Goddard Space Flight Center in 2004.*

Gerald (Jerry) A. Klein, Jr*. functions as NASA Goddard Space Flight Center (GSFC) Flight Projects Directorate's Risk Manager and subject matter expert, the Joint Polar Satellite System Program (JPSS) Risk Manager, the Instrument Projects Division risk management discipline lead across their extensive instrument project portfolio, and teaches Center-wide risk management courses. With experience in avionics design and installation in private, commercial, and military aircraft, as well as quality engineering on a U.S. Navy submarine R&D contract and the NEXRAD Doppler weather radar, Mr. Klein transition from the Naval Research Lab to the GSFC was a logical progression. Mr. Klein has contributed to the success of EOSDIS, Landsat 7, WMAP, GOES, SDO, MMS, and JPSS.*



Edward Rogers *is the Chief Knowledge Officer at NASA's Goddard Space Flight Center in Greenbelt Maryland. He received a Ph.D. from Cornell University's School of Industrial and Labor Relations focusing on the role of cooperation in high tech firms. In the early 1980s he performed five years of international relief work in Southern Lebanon. Prior to returning to academic work at Cornell, Dr. Rogers operated a private consulting practice focused on knowledge workers and intelligent enterprise. His research and publications apply game theory models to human behavior in organizations. He has consulted with a number of organizations on building conceptual transparency and leveraging collective knowledge. Before joining NASA he taught strategic management and entrepreneurship at Cornell, Duke and the University of Alabama in Huntsville.*

Christopher J. Scolese *is the director of NASA's Goddard Space Flight Center. Dr. Scolese assumed this post on March 5, 2012. Dr. Scolese was previously NASA's Associate Administrator, the agency's highest-ranking civil servant position. In that position, he was responsible for the oversight and integration of NASA's programmatic and technical efforts to ensure the successful accomplishment of the agency's overall mission. From Jan. 20, 2009, until July 2009, Dr. Scolese served as NASA's acting administrator where he was responsible for leading the development, design and implementation of the nation's civil space program. As such, Dr. Scolese provided overall leadership for NASA's multiple field installations, worked closely with the Executive and Legislative branches to ensure that NASA was supporting appropriate national policy, and led an international*

collaboration in carrying out high-profile space missions including the Space Shuttle, the International Space Station, the Hubble Space Telescope, and a multitude of other scientific and technological efforts.

Previously, Dr. Scolese served as NASA's Chief Engineer, the Deputy Director of the Goddard Space Flight Center, and the Deputy Associate Administrator in the Office of Space Science at NASA Headquarters. Dr. Scolese also served as the Earth Observing System (EOS) Program Manager and the Deputy Director of Flight Programs and Projects for Earth Science at Goddard. While there, he also served as the EOS Terra Project Manager. Prior to his 1987 appointment at Goddard, his experience included work in industry and government. Dr. Scolese is the recipient of several honors including the Presidential Rank Award of Meritorious Executive, the NASA Distinguished Leadership Medal; Goddard Outstanding Leadership, two NASA Outstanding Leadership Medals and the American Institute of Aeronautics and Astronautics (AIAA) National Capital Section Young Engineer/Scientist of the Year award.