

Managing the Risk of Command File Errors

Leila Meshkat¹ and Larry W. Bryant²
Jet Propulsion Laboratory/California Institute of Technology
Pasadena, CA 91109

Command File Error (CFE), as defined by the Jet Propulsion Laboratory's (JPL) Mission Operations Assurance (MOA) is, regardless of the consequence on the spacecraft, either: an error in a command file sent to the spacecraft, an error in the process for developing and delivering a command file to the spacecraft, or the omission of a command file that should have been sent to the spacecraft. The risk consequence of a CFE can be mission ending and thus a concern to space exploration projects during their mission operations. A CFE during space mission operations is often the symptom of some kind of imbalance or inadequacy within the system that comprises the hardware & software used for command generation and the human experts involved in this endeavour. As we move into an era of enhanced collaboration with other NASA centers and commercial partners, these systems become more and more complex and hence it is all the more important to formally model and analyze CFEs in order to manage the risk of CFEs. Here we will provide a summary of the ongoing efforts at JPL in this area and also explain some more recent developments in the area of developing quantitative models for the purpose of managing CFE's.

I. Introduction

There has been much effort directed at reducing command file related errors at JPL over the last decade. These efforts have included the identification, classification, tracking, recording and root cause determination of these errors for all flight projects. The effort described in this paper is a recent endeavour to use the existing knowledge and body of work within the institution to develop compact, executable stochastic models that are re-usable and can be tweaked for the purposes of sensitivity analysis for the effectiveness of error reduction measures.

In the background section below, the on going effort at JPL over the last decade is explained. In the modeling section, the overall development of the model and some of the analyses conducted with it to date are explained. We conclude by synthesizing the results obtained to date and describing the expected future directions for this endeavour.

II. Background

Ask 100 members of the space operations community how they define a command error, and you will end up with 100 different definitions. While many will have similarities, each will have its own subtle nuance that reflects the individuals experience and perception of what an error in the command process is. Some individuals will focus exclusively on the real time transmission of commands and consider errors when the wrong command is sent or when sent at the wrong time. Others will have a broader view that includes errors within a command, such as an incorrect sign (+ instead of -, and so forth) or other "typo" or errant entry as part of the command composition. While the general perception may be similar, the small differences lead to lengthy discussion when trying to gather statistics on whether a command error has occurred or not. For an operations organization to gather and analyze statistics consistently for command related errors, a documented definition that is easily understood and agreed to is essential.

¹Senior Engineer, Systems and Software Engineering, 318K - Reasoning, Modeling & Simulation, 4800 Oak Grove Drive, MS 144-208, Non-Member.

² Mission Operations Assurance Manager for MRO, MER, and Juno, 5150-Mission Assurance Management Office, 4800 Oak Grove Drive, MS 264-767, Senior.

With the potential to disastrously terminate a mission, command errors within projects at the Jet Propulsion Laboratory (JPL) are a major concern. In an effort to understand and reduce command errors, the Mission Operations Assurance (MOA) team within JPL's Office of Safety and Mission Success (OSMS) began working with the operations teams at JPL and at systems contractors to identify and classify command errors. Initially, four categories were used to classify the errors. These were

- 1) An error directly related to the ACE and/or RTO operation while on-console processing a Command File for Radiation via the DSN. (Real-time command error)
- 2) An error that can be traced directly to an uplink process that wasn't followed correctly or that should have been caught in that process. (Command development process error)
- 3) An unexpected result on-board the spacecraft directly related to a command file or files. The appropriate uplink process was followed and adhered to as well as possible. (Unexpected result)
- 4) Unexpected results in instrument or instrument related behavior as a result of Science Team command file(s) errors (Non-interactive Commands)

Clearly these cover the complete spectrum of the uplink process and include both science and engineering sides of a flight project. None the less, there were difficulties in using these as the definition of a command error. For example, a category 1 error would include the attempted transmission of a command without the uplink being enabled at the deep space antenna. If this were not time critical and the uplink was subsequently enabled and the command re-transmitted, some might not consider that this was a command error, after all, no harm, no foul. Consequently some events might not be captured in the statistics if they had no deleterious effect, yet they might point to a potential future problem and should indeed be captured. Considering a category 2 type error we would include an incorrect or missing sign on a number because the values were transmitted via phone, even though the procedure calls for a written interchange. In many instances this would be a minor annoyance, but if we are defining a burn direction for a critical maneuver, clearly the consequence could be catastrophic. An example of a category 3 type error might result from a less than perfectly understood operational environment. The conditions on the surface of Mars have contributed to a number of such errors as a result of models that are imprecise. Lack of understanding of vehicle tilt angle can result in a failed attempt to send a signal to Earth when Earth was above the Mars horizon because the vehicle deck had sufficient tilt to block the signal. For category 4 commands, the initial thought was to include a category that was beyond the control of the engineering side of the project, which would be non-interactive commands submitted by an instrument, that in theory affected only the instrument. The outcome would be an instrument issue but the error could in fact be looked at as a category 2 or 3 within the instrument team. An example might be the selection of an incorrect filter for a camera due to a typographic error or lack of thorough checking during the review process. One common thread in these is that an underlying inference that some one individual is at fault. While this may be the case, it is not conducive to gathering complete data and analyzing the data for an improved approach without teams responding defensively. Because of this, the MOA at JPL team undertook to develop a definition for command errors that would reduce the attribution and be applicable equally to all elements of a project's flight team.

After substantial discussion, the decision was to use the term "Command File Error" defined as one of the following, regardless of the effect on the spacecraft:

- 1) an error in a command file that was sent to the spacecraft;
- 2) an error in the approval, processing, or uplinking of a command file that was sent to the spacecraft;
- 3) the omission of a command file that should have been sent to the spacecraft.

This definition has been instantiated in JPL's institutional Anomaly Resolution Standard. Collection of statistics is now implemented through a new module of the Incident, Surprise, Anomaly (ISA) report as part of JPL's Problem Reporting System (PRS). When an issue arises that is attributed to a Command File Error (CFE), the issue is documented in an ISA and the CFE section of the ISA must be completed prior to close out of the ISA report. This section provides for the collection of a variety of information regarding the CFE. The type of command file, whether interactive or non-interactive is identified as well as the phase of the command process where the initial error occurred. A description of the error is required as are brief descriptions of Proximate, Contributing, and Root cause. While data collected in the past has permitted tracking of error rates, this new data captured in PRS provides more insight into the nature and causes of errors. With this insight, it is now possible to develop a model of the cause and effect interactions associated with CFEs. This model in turn can provide us with a tool to evaluate potential scenarios which may be appropriate to reduce both the quantity and the severity of CFEs. The development and initial applications of this model is the focus of the remainder of this paper.

III. Modeling

The modeling activities conducted in order to reduce CFEs have been two-fold. On one hand, the command generation processes for a sample space mission [4] were generalized and Probabilistic Risk Assessment (PRA) models were built for each of them. On the other hand, all the various root causes of CFEs (not just the processes) were elicited from Subject Matter Experts(SMEs) as well as the existing body of work explained in the background section, and Bayesian Belief Network (BBN) models were built for their analysis. In this section, we describe each of these modeling efforts separately.

A. Probabilistic Risk Assessment Models

The goal of the PRA models is to provide a formalism for the main processes involved during command generation and enable trade studies and design analysis for the purpose of risk reduction. As it turns out, the key higher level functions or processes that are conducted during a command generation process are fairly generic for different types of missions[8]. Furthermore, as the key activities conducted during these functions are broken down into their lowest level or atomic level activities, it becomes possible to draw a correspondence between them and the activities for which there exist failure rates in human reliability data banks from the nuclear industry [1]. Therefore, these models enable quantitative risk assessment for the command generation processes.

Figure 1, which has been adopted from Bezjak and Waggoner [12] demonstrates a generic command generation process. The process starts with the planning & inputs. The inputs are reviewed in a tabletop session and may include the mid-range schedule, view periods, or the SPK (Spacecraft & Planet Kernel) file, which represents a common format for a standard navigation product containing ephemeris data. Then there is typically a kickoff meeting where the Mission Manager (MM) approves the initiation for the building of the sequences. The Sequence build inputs are then generated by the various teams. This task includes the event planning, science, spacecraft performance and analysis, Deep Space Network (DSN) scheduling, and navigation activities. These sequences are then integrated and tested in the Spacecraft Test Laboratory (STL) and reviewed by the flight team. At this point, a command conference occurs in which the command products are reviewed and approved by the Mission Manager before the final command product is radiated to the spacecraft.

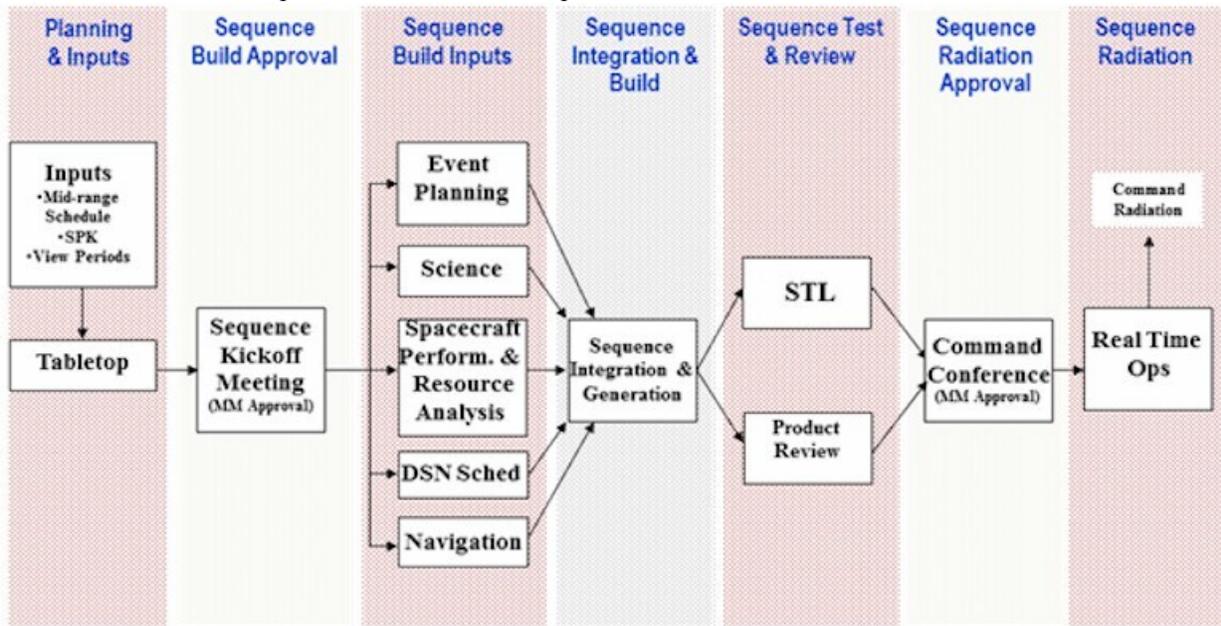


Figure 1. Generic Command Generation Process

The first level PRA model corresponding to a specific command generation process during the orbit phase, for the Juno mission [4] is represented in figure 2. Even though the various branches of this logic tree are not readily legible, the intent of including this diagram is to demonstrate all the possible combination of events that can occur. Each of the main activities that occur during this sequence generation correspond with an event in the event tree diagram. For instance, the kickoff, generating background sequence, generating engineering sequences, generating

The failure modes in each of these is further broken down to atomic level elements which correspond to failure data available in the Nuclear Industry Human Reliability data banks [1, 2].

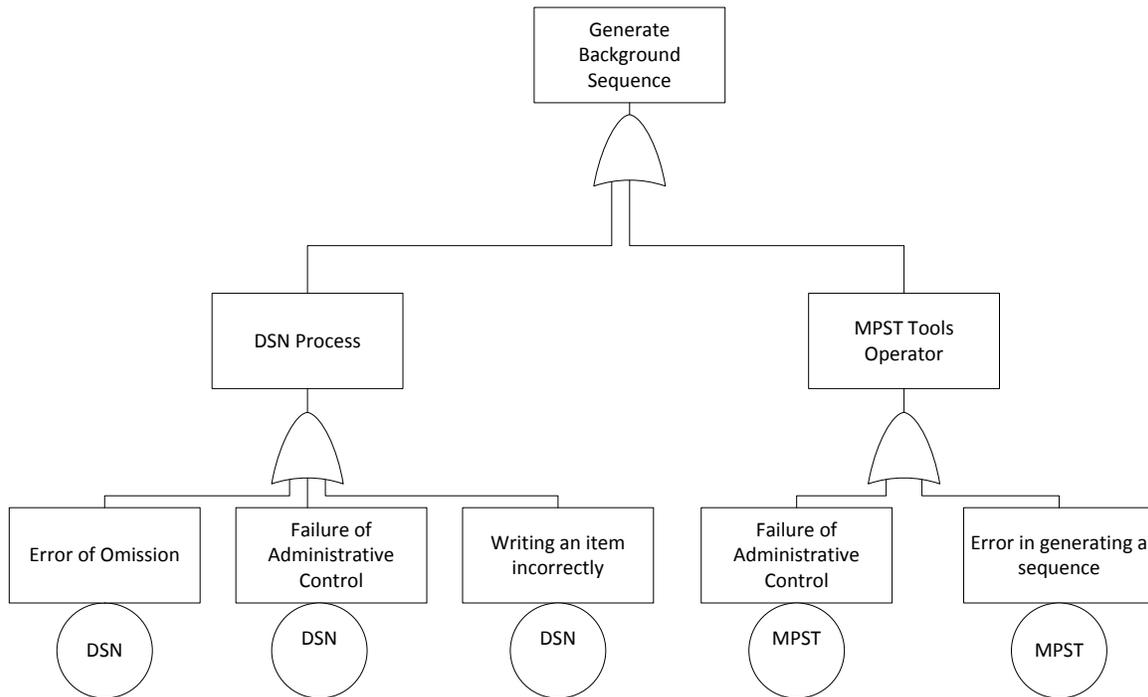


Figure 3: Generate Background Sequence Fault Tree

There is a fault tree corresponding to each of the events in the event tree. The possible end states of the event tree and the corresponding probabilities associated with each of them are determined by aggregating the probabilities of the corresponding fault trees for each of the events based on the logical combinations for each end result of the tree.

B. Bayesian Belief Network Models

Tables 1 and 2 show a classification of CFEs. Broadly, we consider that CFEs are caused either due to slips or mistakes [1,2]. A slip occurs when the operators intended course of action is correct but the implementation is not. A mistake occurs when the operators intended course of action is incorrect. Both slips and mistakes can be due to internal or external factors. Internal factors have to do with the cognitive abilities of the operator and external factors all the external tools, processes, models, hardware or software that has an effect on the understanding the operator has of the state of the spacecraft and the best course of action associated with it.

Both the external and internal factors affect slips and mistakes but their effect is not identical. Internal factors have a larger effect on slips and external factors a larger effect on mistakes. We broadly classify the external factors into Verification & Validation (V&V) activities, flight team external configurations, flight system documentation, procedures, software and interfaces. The V&V activities, in turn, can be carried out by testbeds or simulations. The flight team external configurations relate to collaborator teams outside of JPL. The flight system documentation is especially important when a spacecraft is built by a contractor and operated in house. Procedures are decomposed into two elements: process maturity and process requirements. The idea is that any inadequacy in the procedures is due to either the lack of maturity of the process or the incompleteness of the requirements.

External Factors (Adequate, Inadequate)	FS Document		
	Verification & Validation (Adequate, Inadequate)	Hardware Testbeds (Adequate, Inadequate)	User - Friendly (True, False)
			Maintained(True, False)
			Set Up (Adequate, Inadequate)
			Up to Date (Adequate, Inadequate)
		Software Simulations (Adequate, Inadequate)	Fidelity (Hi, Low)
			User - Friendly(True, False)
			Maintained(True, False)
			Set Up(Adequate, Inadequate)
	Flight Team External Configurations (Adequate, Inadequate)		
	Procedures	Process Requirements (Complete, Incomplete)	
		Process Maturity (Adequate, Inadequate)	
	Software (Adequate, Inadequate)	Post-launch FSW (Adequate, Inadequate)	FSW Config(Adequate, Inadequate)
			Coding(Adequate, Inadequate)
			Design(Adequate, Inadequate)
			Requirements(Complete, Incomplete)
		GSW (Adequate, Inadequate)	GSW Config(Adequate, Inadequate)
			Coding(Adequate, Inadequate)
			Design(Adequate, Inadequate)
Requirements(Complete, Incomplete)			
Interfaces	GSW/FSW		
	SW/SW Simulations		
	SW/HW Simulations		

Table 1. Classification of Command File Errors - External Factors

The internal factors include elements such as communications, process compliance, training, situational awareness, operator morale and operator alertness/complacency. Process compliance itself is classified into stress and operations procedures. The idea here is that the level of stress and the quality of the operations procedures are the factors that affect process compliance. The BBN associated with the classification tree is shown in figure 4.

Internal Factors (Adequate, Inadequate)	Communications (Adequate, Inadequate)	Intra-team (Adequate, Inadequate)
		Inter-team (Adequate, Inadequate)
	Process Compliance (Adequate, Inadequate)	Stress (Hi, Med, Low)
		Operations Procedures (Adequate, Inadequate)
	Training	Operations Training (adequate, inadequate)
		Spacecraft behavior training (adequate, inadequate)

Table 2. Classification of Command file Errors - Internal Factors

Nodes in a Bayesian network represent conditions; arcs represent influences. In order to explain the underpinnings of this model, we zoom in on selective nodes and describe them.

1. *Process Compliance*

A node with input arcs has an associated conditional probability table (CPT). A CPT defines the probability of the target node state in terms of the combinations of the states of the input nodes. Consider the “Process Compliance” node in the subnet in Figure 5. The probability of process compliance depends on the level of stress and the adequacy of the operations procedures. The Stress node is defined to represent three states: low, medium and high. The Operations Procedures have two states, adequate and inadequate. The CPT for process compliance indicates the probabilities associated with it being adequate for various combination of states for the operations procedures and the stress levels. For instance, if the stress is low and the operations procedures are adequate, there’s a 100% chance that the process compliance is also adequate.

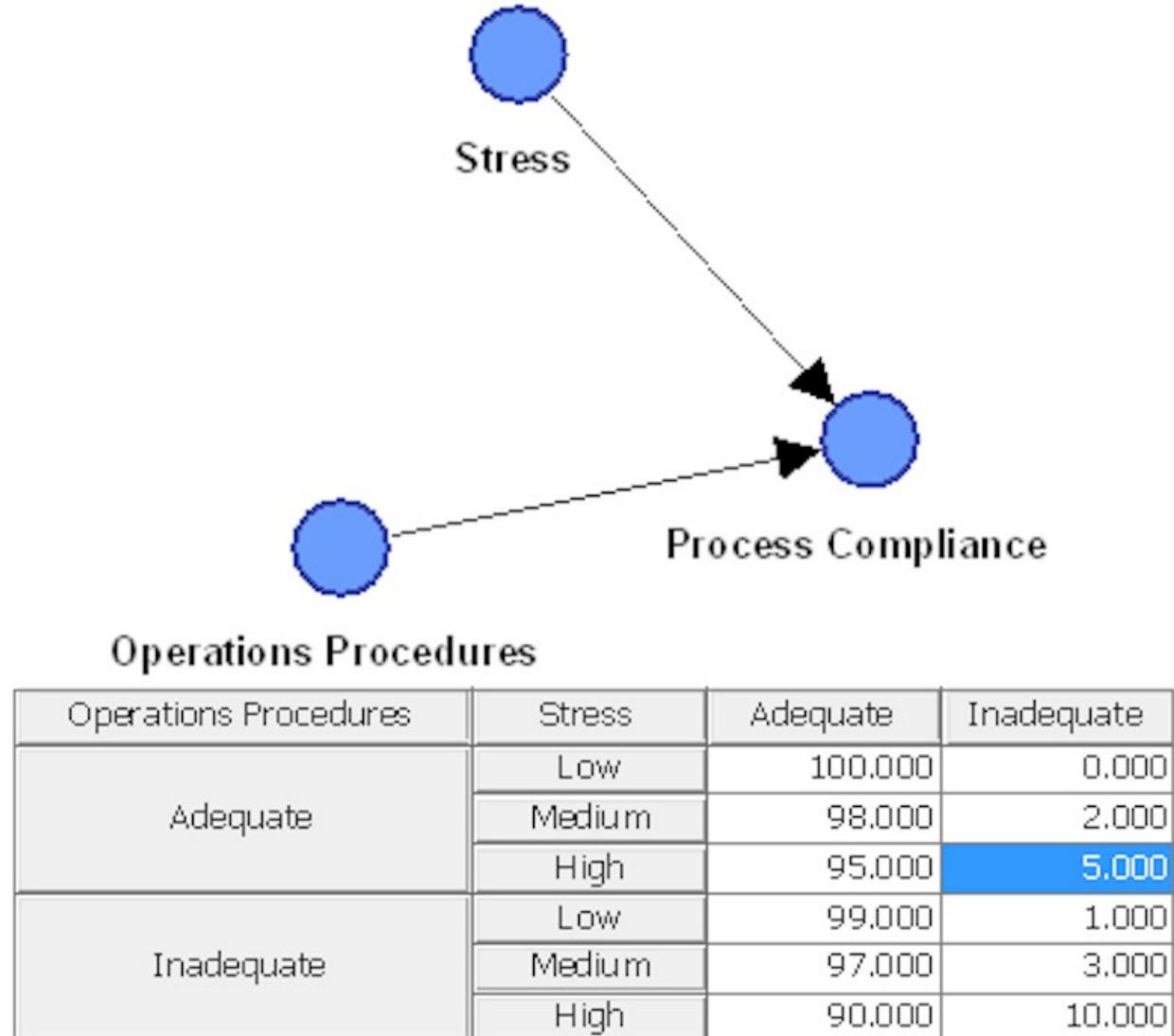


Figure 5. Sub-tree associated with "Process Compliance" and its conditional probability table (CPT)

The probabilities associated with the CPTs were reverse engineered based on the error rates that have been observed at JPL[11, 13].

The probability distributions for the end nodes are calculated based on the data obtained from the SME’s for the root node probability distributions and the CPT’s. A summary of these probabilities for the average JPL mission is shown in figure 6.

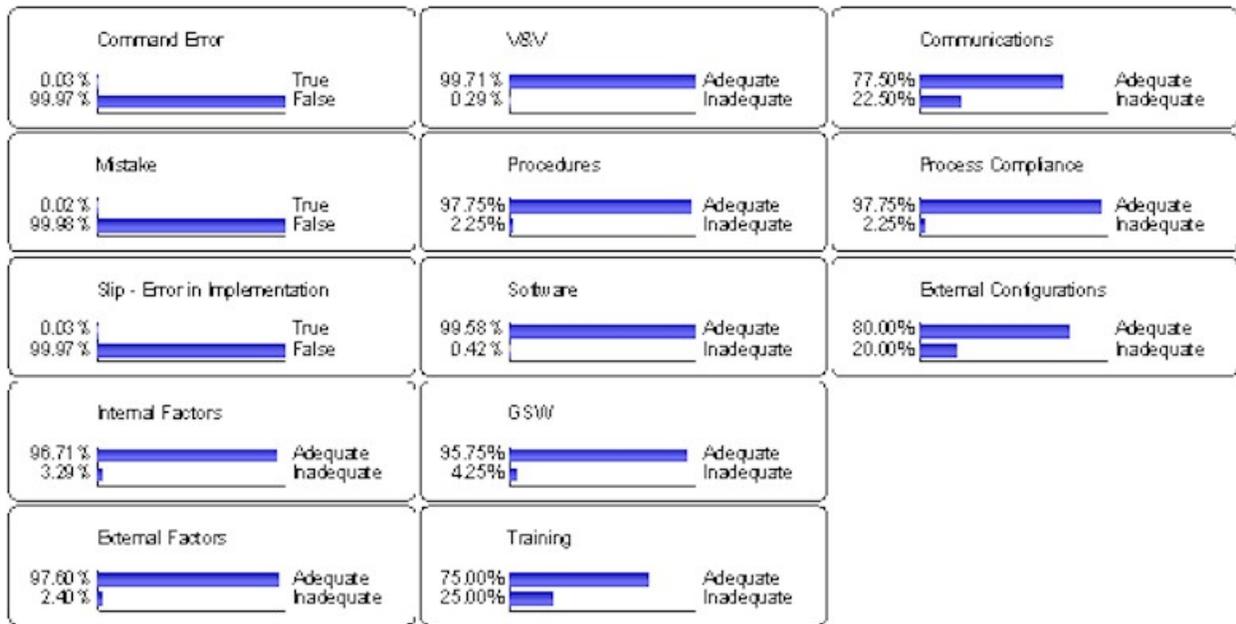


Figure 6. Probability distributions for the end nodes of the BBN based on an average estimate for JPL Missions

IV. Probabilistic Root Cause Analysis

Using the BBN model, we can conduct various types of analysis. By having a variety of analysis to conduct, it provides a range of areas for projects to examine to identify potential focus areas that would prove fruitful to concentrate on in reducing the risk of CFEs. One of them is a probabilistic root cause analysis. For instance, if in fact a command file error has occurred, we see in Figure 7, there is a 47.52% chance that it has been due to a mistake and a 52.79% chance that it has been due to a slip.

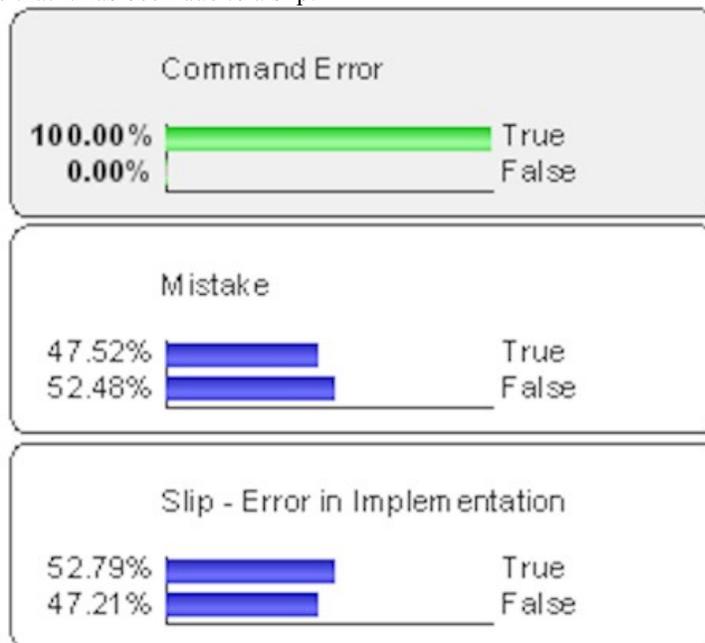


Figure 7. Depiction of probability distribution of slip and mistakes when a command file error has occurred

Slip Occurred?	Mistake Occurred?	Internal Factors Inadequate	External Factors Inadequate
Yes	Yes	39.89%	55.28%
Yes	No	25.83%	71.82%
No	Yes	57.60%	39.80%
No	No	3.26%	2.38%

	Causes	Probability		Causes	Probability
Internal Factors Inadequate	High Stress	30.30%	External Factors Inadequate	Inadequate Procedures	43.60%
	Inadequate Communications	31.70%		Inadequate Software	20.90%
	Inadequate Training	17.20%		Inadequate V&V	8.39%

Figure 8. Tables that demonstrate the probabilistic root cause analysis example

Figure 8 includes a set of tables that trace back the occurrence of slips and mistakes to root level events. Figure 9 shows the trends associated with the probability of command file errors during the various phases of missions.

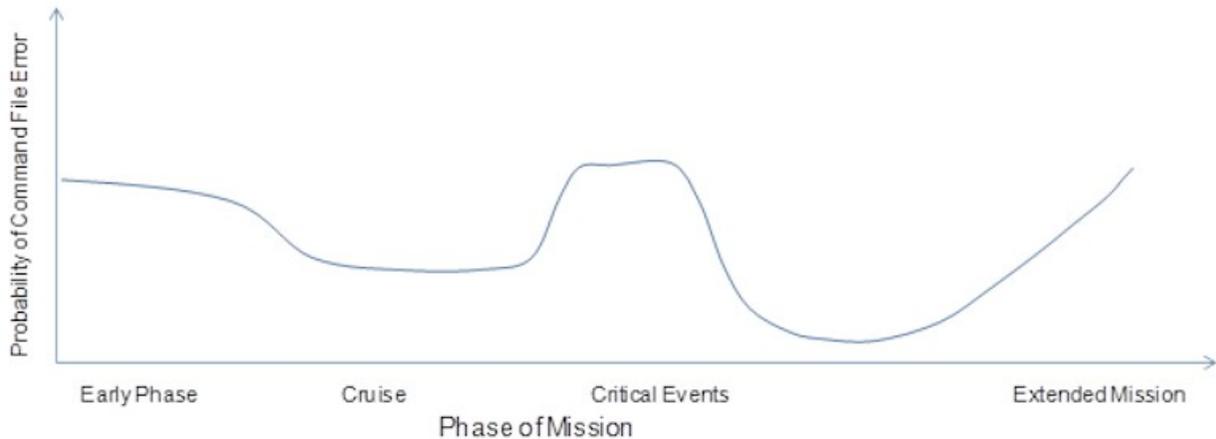


Figure 9. Trend curve for the probability of command file error during various mission phases

V. Summary & Future Directions

A structured approach for analyzing the risk of CFEs was presented in this paper. This approach begins by delineating the different types and causes of CFEs based on the body of knowledge and experience in this area at JPL over the course of the last thirteen years. Then PRA and BBN models were created to provide a modeling approach for analysis and quantification of CFE risk.

The models that were developed are now ready for use within each of the projects to enable them to more fully assess and manage the risk of CFEs. The intent of the authors is to work individually with each of the projects that provided the input data to develop case studies of operational scenarios and associated CFE risk for each. We will address questions that are posed to the projects during reviews to provide them more insight into the modeling process and explore their options for making use of these tools and improve the CFE risk posture on their project. This will most likely require us to add depth and detail associated with each project in a customized manner for that

project. The objective of this work is to assist each project in identifying the elements of the command generation process which have the most potential for cost effectively providing an opportunity to reduce the risk of CFEs. Several projects included in this work have developed process improvement changes to reduce their vulnerability to CFEs. However, even with years of experience, it is difficult at best to take all the contributing factors for CFEs into consideration at once. The models developed here can do that and thus have the potential to identify new areas for improvement that were inadvertently missed in discussions and reviews to date. Extending the model usage and determining their value to each project is a primary direction we plan to continue with in this effort.

Acknowledgements

The work reported in this paper was performed at the Jet Propulsion Laboratory, California Institute of Technology under a contract with NASA.

The authors gratefully acknowledge the contribution and inputs of the following Subject Matter Experts: Luis Morales, Reid Thomas, Bruce Waggoner, Timothy Weise, Robert Nelson, Chuck Scott and Ed Hirst, as well as inputs from Grant Faris and Kyle Martin.

References

1. David I. Gertman, Harold S. Blackman, " Human Reliability & Safety Analysis Handbook", John Wiley & Sons, Inc. 1993.
2. Anthony Spurgin, " HRA Concepts and Applications", Series of workshops given at Tsinghua University, Beijing, China May 10th through 12th , 2005
3. Grant Faris, " Proposed Institutional Command File Error Definition, Categories, and Metrics". 3 April 2008.
4. Michael Jones, "Juno Project Functional Description Document".
5. Shamas P. Smith and Michael D. Harrison, " Blending Descriptive and Numeric Analysis in Human Reliability Design". The Dependability Interdisciplinary Research Collaboration, Department of Computer Science, The University of York, United Kingdom.
6. P. Trucco, E. Cagno & O. Grande, " A Bayesian Belief Network Approach for Integrating Human and Organizational Factors in Risk Analysis: A Case Study for the Maritime Industry.
7. Grant Faris, January 2010, "Mars Program Office Command File Errors"
8. L. Meshkat, S. Grenander and K. Evenson, "Reliability Analysis and Standardization of the Spacecraft Command Generation Process", International Symposium for Software Reliability Engineering, November 2011
9. L. Meshkat, J. B. Dugan, G. Faris, "Command Error Modeling", International Symposium for Software Reliability Engineering, November 2011
10. L. Meshkat, "A Systems Modeling Approach for Risk Analysis for risk management of command file errors.", Space Operations Workshop at JPL, April 2012
11. G. B. Faris, L. W. Bryant "Improving Operations: Metrics to Results".
12. Kelly Bezjak and Bruce Waggoner, "Mission Operations Flight School", 2010.
13. H. Kwong-Fu, C. Scott, R. Smith, G. Chin, " Command File Error Metrics Working Group Analysis & Results", 2008.