Managing the Risk of Command File Errors

Leila Meshkat & Larry Bryant
Jet Propulsion Laboratory
California Institute of Technology

Outline

- Executive Summary
- Introduction
- Background
- Modeling
  - Probabilistic Risk Assessment
  - Bayesian Belief Networks
- Future Directions
- Acknowledgement
- References

Executive Summary

- A command file error (CFE), is a 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 endeavor.
- JPL has managed to reduce CFE's using standard risk management techniques and is currently augmenting this work by including quantitative risk modeling techniques.
- This presentation provides a report on these efforts.

Introduction

- There has been much effort directed at reducing CFE's 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.
- More recently, we are using 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.

Background (1)

- In an effort to identify and classify command errors. Initially, four categories were used to classify the errors. These were:
  - 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)
  - 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)
  - 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)
  - Unexpected results in instrument or instrument related behavior as a result of Science Team command file(s) errors (Non-interactive Commands)

Background (2)

- 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:
  - an error in a command file that was sent to the spacecraft;
  - an error in the approval, processing, or uplinking of a command file that was sent to the spacecraft;
  - 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).

Modeling

- There are two main bodies of work involved in the stochastic modeling endeavor:
  1. Models pertaining to the command generation process, and,
  2. Models of all the causes of commanding errors and their relative contributions.

Probabilistic Risk Assessment (PRA) Models

- These models consider the sequence of activities involved in generating commands.
- PRA models are built for each of the key command generation functions.
- Reliability of human tasks are assessed by matching to the data in Human Reliability databanks from the Nuclear Industry..

PRA models

- Generic Command Generation Process, adopted from Bezjak and Waggoner

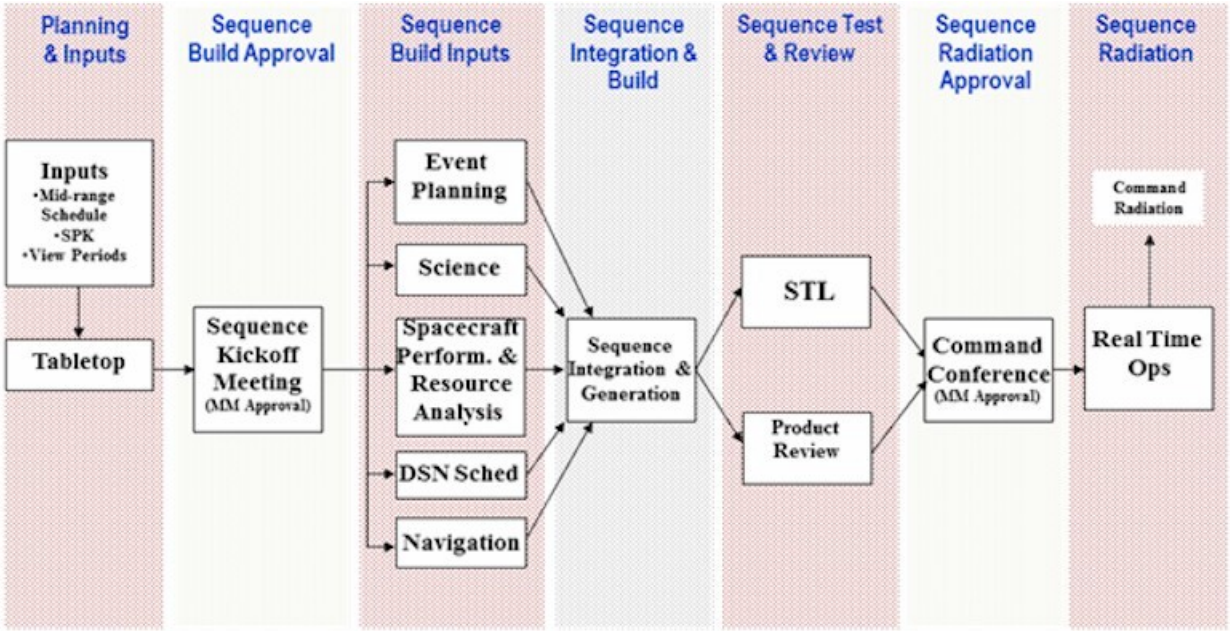


Figure 1. Generic Command Generation Process

Sequence Diagram for Sample Command Generation Function

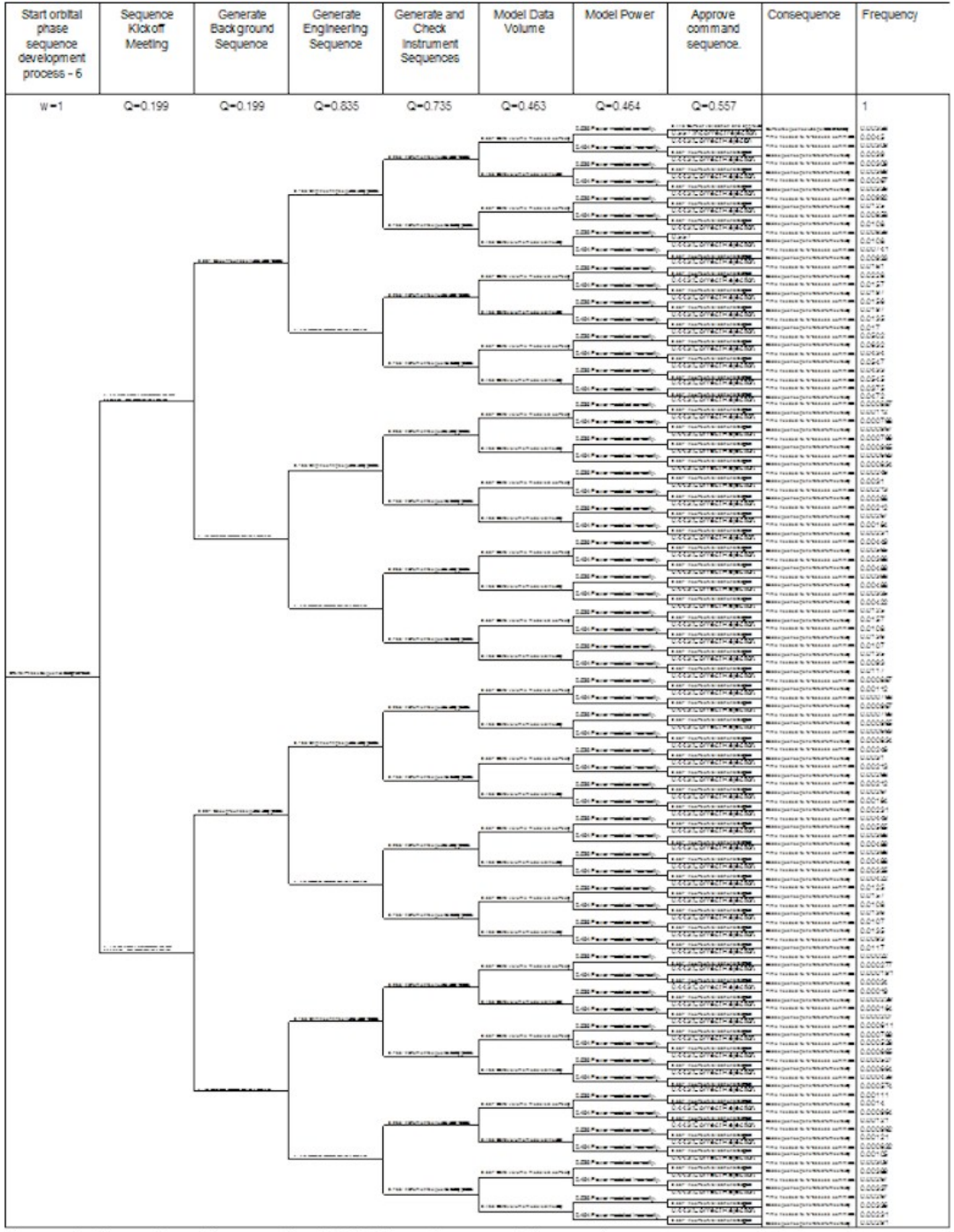
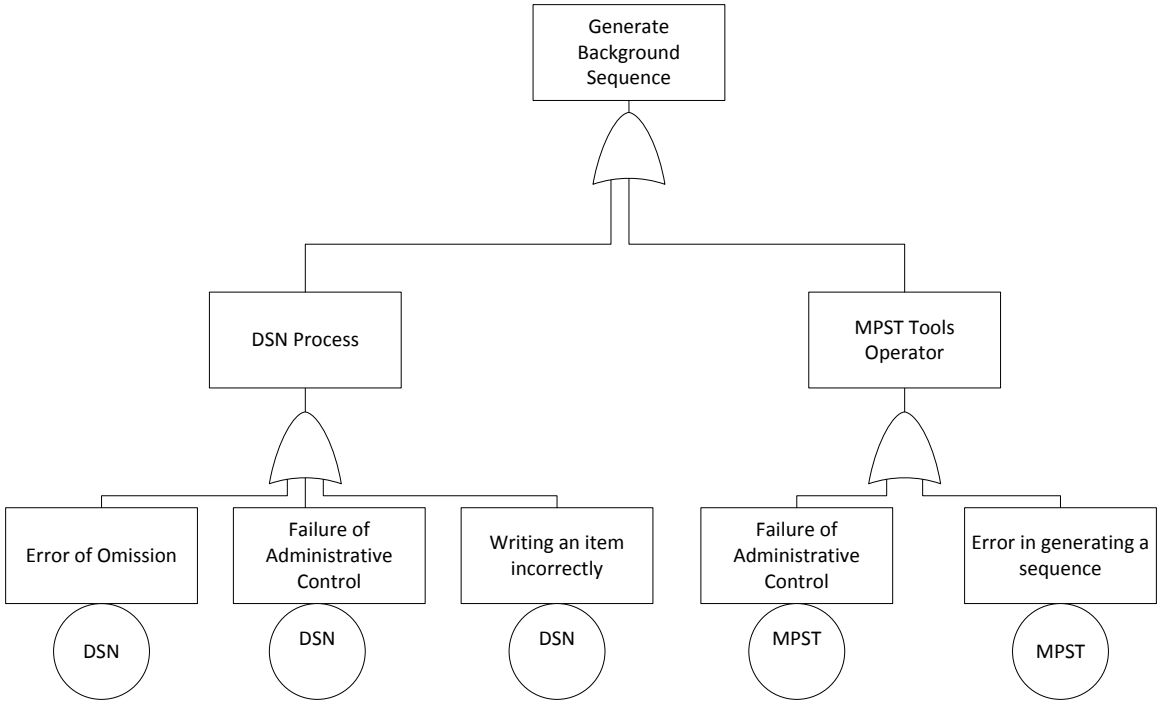


Figure 2. Event Tree Diagram for Orbit Phase Command Generation

PRA models: Fault Tree



Bayesian Belief Network Models

- Broadly, we consider that CFEs are caused either due to slips or mistakes.
- 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

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)
			Fidelity (Hi, Low)
		Software Simulations (Adequate, Inadequate)	**User - Friendly**(True, False)
			Maintained(True, False)
			Set Up(Adequate, Inadequate)
			Up to Date (Adequate, Inadequate)
			Fidelity(Hi, Low)
	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

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

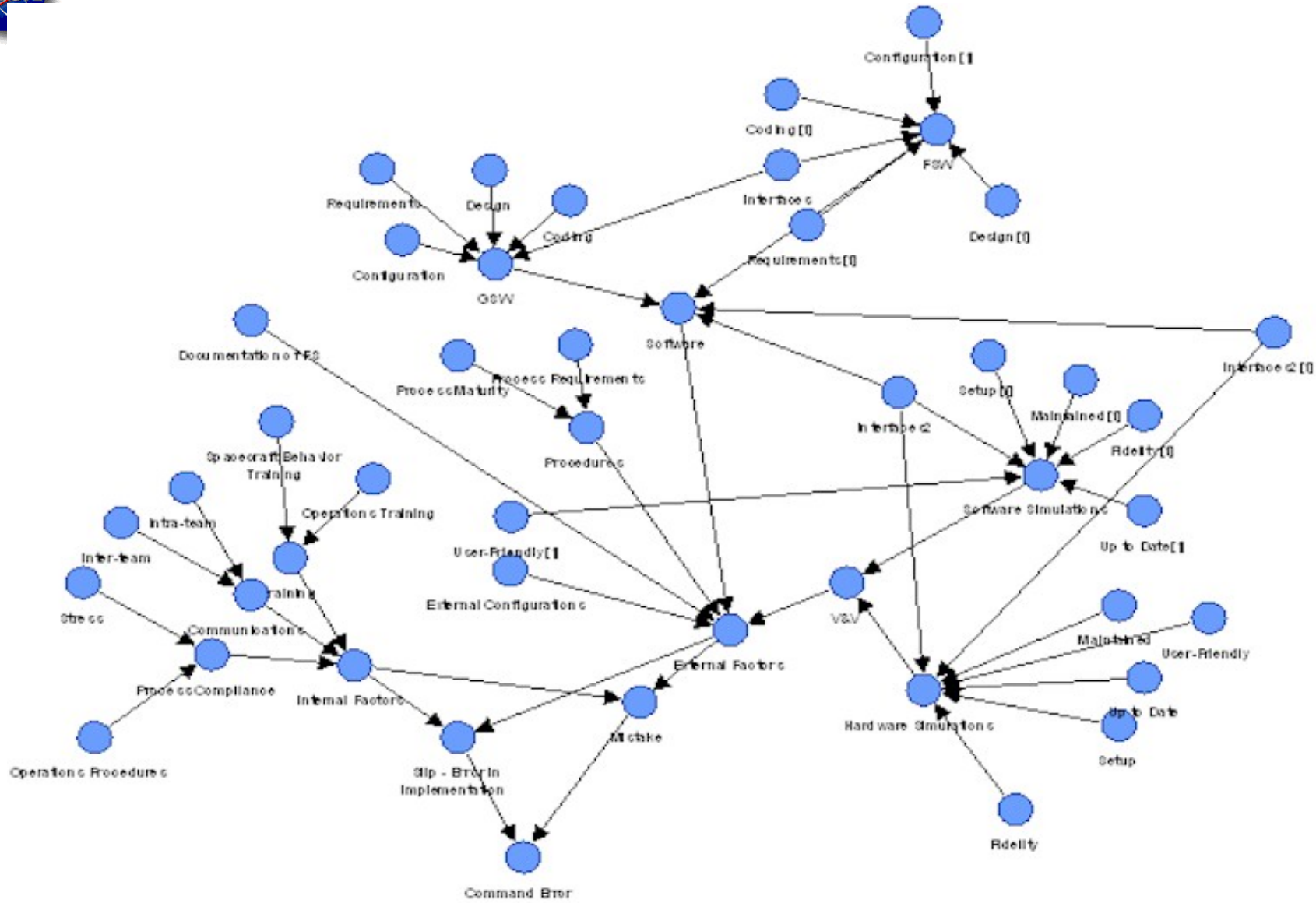
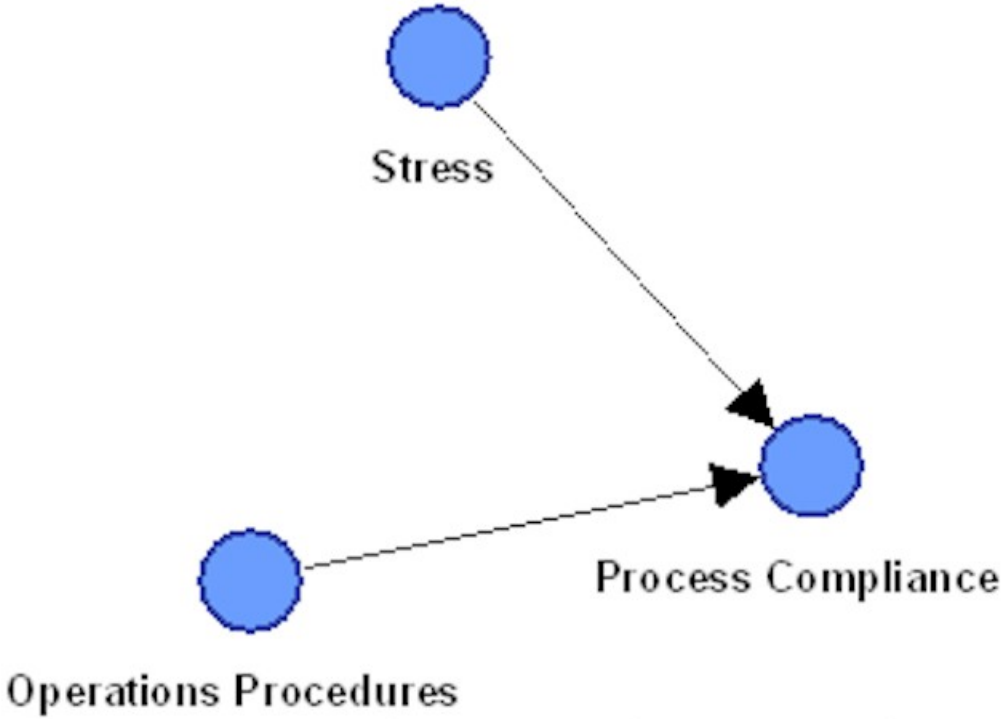


Figure 4. Overall BBN representing Command File Errors

FSW Config(Adequate, Inadequate)	How likely is it that the configuration for the post-launch flight software is adequate?
Coding(Adequate, Inadequate)	how likely is it that the coding for the post-launch flight software is adequate?
Design(Adequate, Inadequate)	how likely is it that the design of the post-launch flight sofware is adequate?
Requirements(Complete, Incomplete)	how likely is it that the requirements specification for the post-launch flight software is adequate/complete? Or on a scale of 1-100, what is the level of completeness.
GSW Config(Adequate, Inadequate)	How likely is it that the configuration for the GSW is adequate?
Coding(Adequate, Inadequate)	How likely is it that the coding for the GSW is adequate?
Design(Adequate, Inadequate)	How likely is it that the design of the GSW is adequate?
Requirements(Complete, Incomplete)	How likely is it that the requirements for the GSW are complete? Or on a scale of 1-100, what is the level of completeness of the GSW requirements? 100 is when they are complete.

Table 3. Sample Questions used to elicit subject matter expertise



Operations Procedures	Stress	Adequate	Inadequate
Adequate	Low	100.000	0.000
	Medium	98.000	2.000
	High	95.000	5.000
Inadequate	Low	99.000	1.000
	Medium	97.000	3.000
	High	90.000	10.000

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

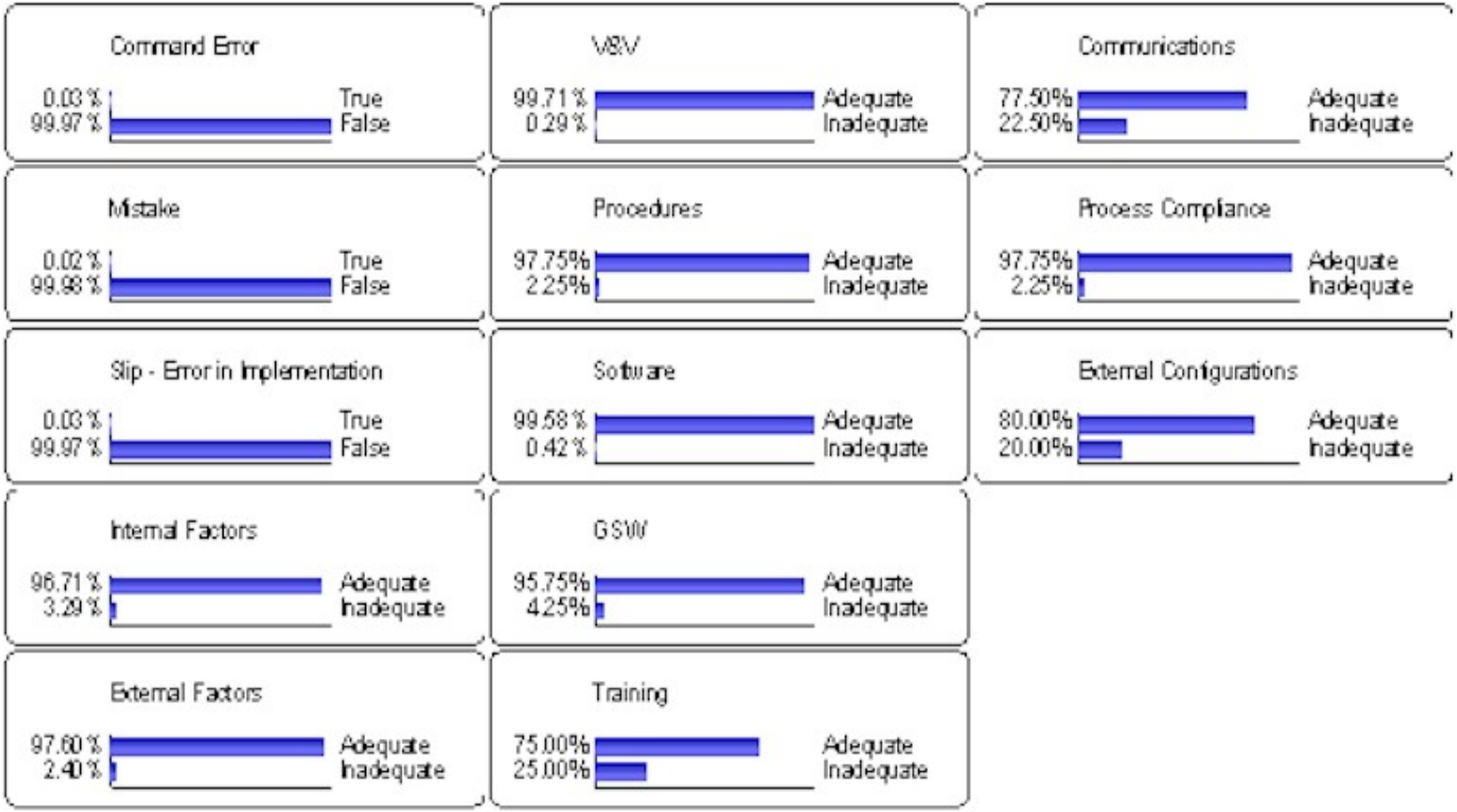


Figure 6. Probability distributions for the end nodes of the BBN based on an average estimate for JPL Missions

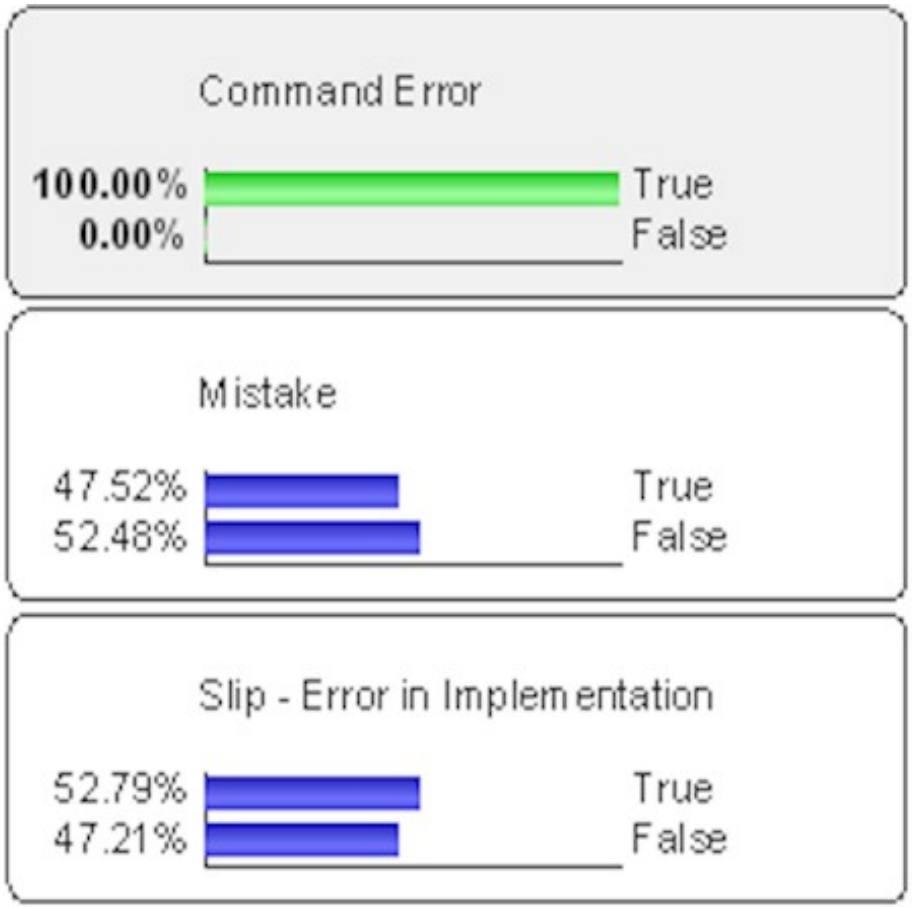


Figure 7. Depiction of probability distribution of slip and mistakes when a command file error has occured

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
Internal Factors Inadequate	High Stress	30.30%
	Inadequate Communications	31.70%
	Inadequate Training	17.20%

	Causes	Probability
External Factors Inadequate	Inadequate Procedures	43.60%
	Inadequate Software	20.90%
	Inadequate V&V	8.39%

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

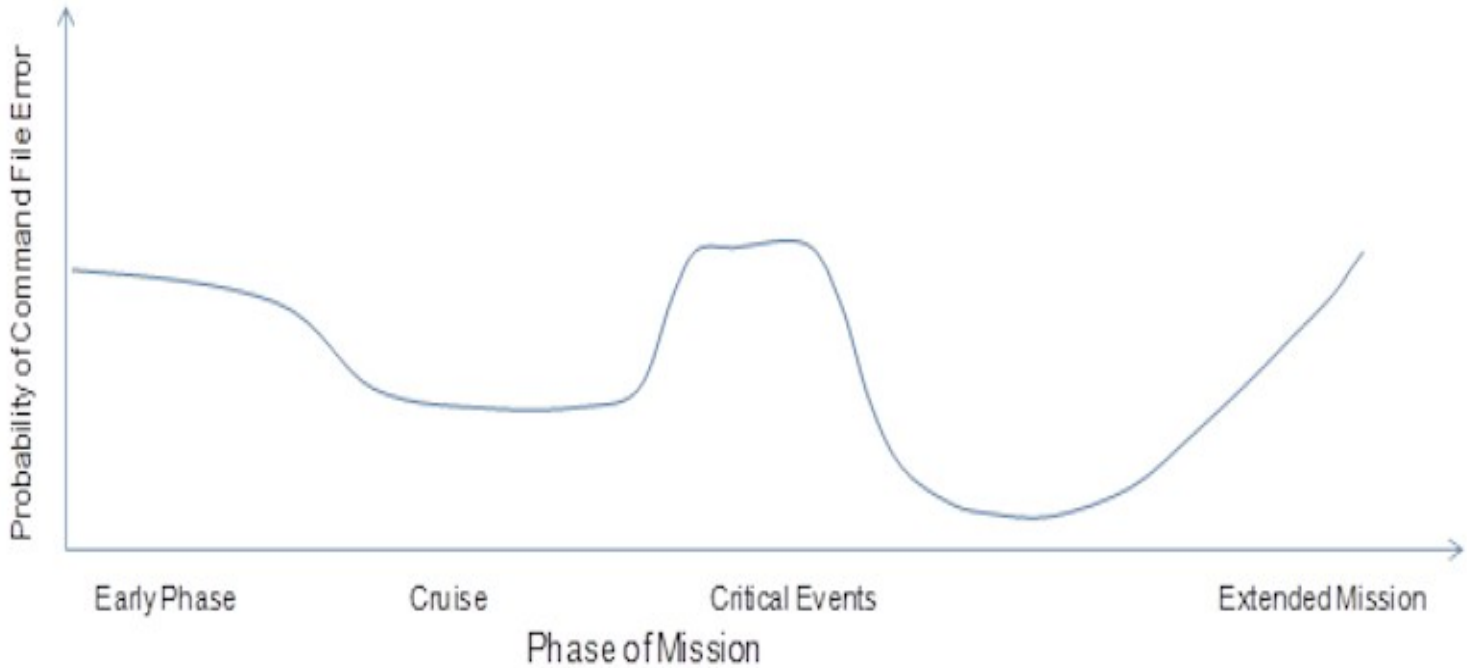


Figure 9. Trend curve for the probability of command file error during various mission phases

Conclusions & 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.
- Extending the model usage and determining their value to each project is a primary direction we plan to continue with in this effort.
- The objective 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 that provided inputs to the models 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.

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

- David I. Gertman, Harold S. Blackman, " Human Reliability & Safety Analysis Handbook", John Wiley & Sons, Inc. 1993.
- Anthony Spurgin, " HRA Concepts and Applications", Series of workshops given at Tsinghua University, Beijing, China May 10th through 12th , 2005
- Grant Faris, " Proposed Institutional Command File Error Definition, Categories, and Metrics". 3 April 2008.
- Michael Jones, “Juno Project Functional Description Document”.
- 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.
- 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.
- Grant Faris, January 2010, “Mars Program Office Command File Errors”
- 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
- L. Meshkat, J. B. Dugan, G. Faris, “Command Error Modeling”, International Symposium for Software Reliability Engineering, November 2011
- L. Meshkat, “A Systems Modeling Approach for Risk Analysis for risk management of command file errors.” , Space Operations Workshop at JPL, April 2012
- G. B. Faris, L. W. Bryant “Improving Operations: Metrics to Results”.
- Kelly Bezjak and Bruce Waggoner, “Mission Operations Flight School”, 2010.
- H. Kwong-Fu, C. Scott, R. Smith, G. Chin, “ Command File Error Metrics Working Group Analysis & Results”, 2008.