

# Command Process Modeling & Risk Analysis

PI: Dr. Leila Meshkat

Core team members: Ken Evensen, Sven Grenander, Dr. Joanne Dugan

Collaborators: Grant Faris, Larry Bryant, Luis Morales, Ray Morris

Jet Propulsion Laboratory

California Institute of Technology

©2012 All rights reserved

**OSMA Software Assurance Research Program**

# Outline

- Problem Statement
- Approach
- Current Capability and/or Results
  - BBN Models
  - Standardization
  - PRA Models
  - Juno Anomaly Investigation
- Planned Capability or additional applications
- Technical Solutions Found
- Remaining Technical Challenges

## Objective

Reduce Commanding Errors at JPL and NASA by improving the Command Generation Process

## Approach

- Standardization of Command Generation Process (Periodic Table, Library of Models);
- Systems Analysis of all causes of error using BBN's
- Update to institutional processes.

## Accomplishments

- Framework and approach for standardization;
- Approach and data from human reliability analysis
- Development of libraries
  - Risk models, data applicable, tool and model transformations;
- Publications (ISSRE, ASM, Space Operations)
- Initiated infusion (FPP)
- Anomaly Analysis (MRO, Juno)

## Future Plans

- Extension to Software Reliability Analysis
- Continue Infusion (JPL Processes,)
- Complete tutorial for end to end application
- Establish as an assurance position for projects
- Publications

# Problem Statement

- Develop and Implement a methodology for reducing commanding errors.

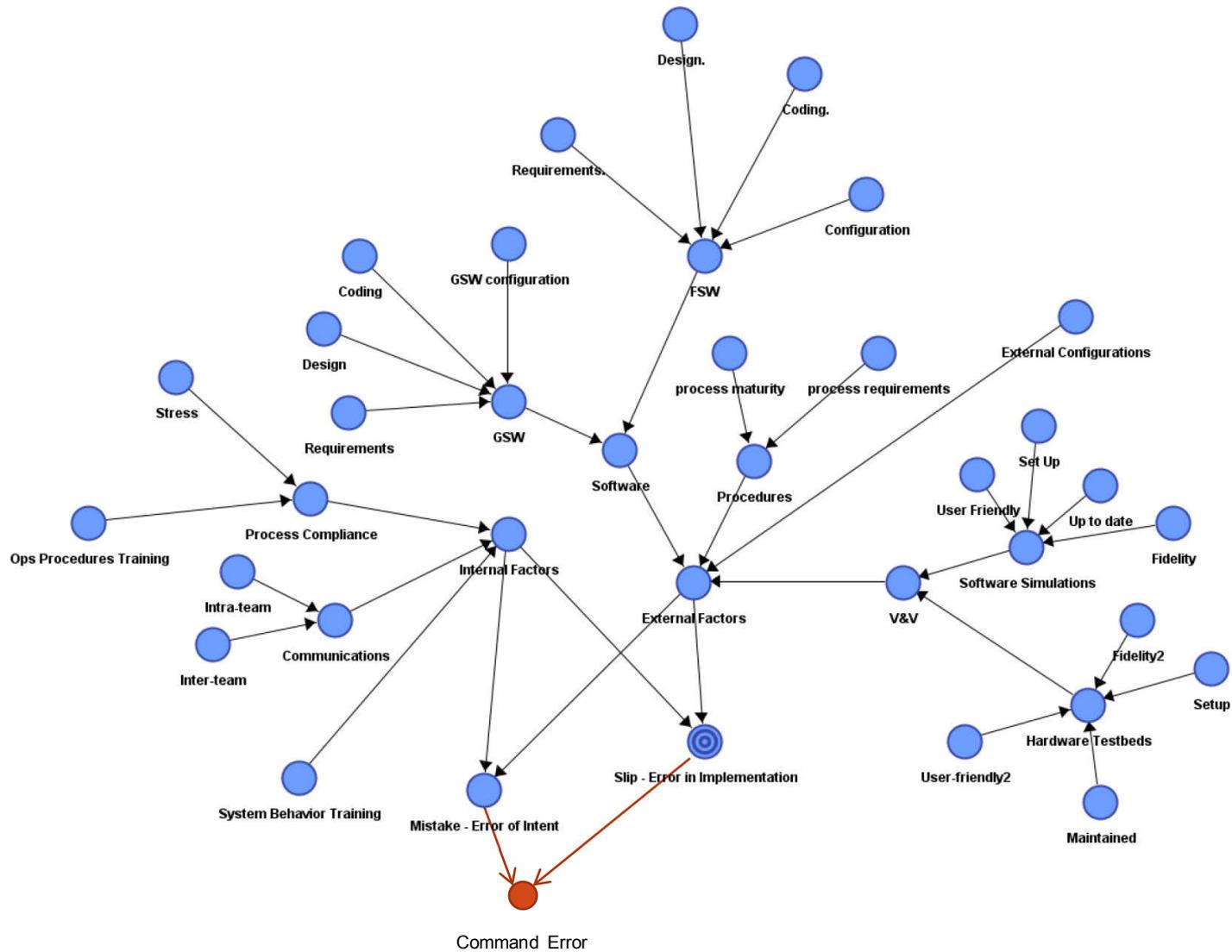
# Why Command Errors?

- Often the symptom of some kind of imbalance or inadequacy
  - within the system that comprises the hardware & software used for command generation and/or
  - the team involved in this endeavor.
- Era of enhanced collaboration with other NASA centers and commercial partners
  - systems become more and more complex
  - it is imperative to formally model and analyze command generation systems in order to manage the risk of command file errors.

# Approach

- Combined Bayesian Belief Network and Probabilistic Risk Assessment Models.
  - BBN model of commanding errors
    - These models take into consideration all the possible causes for commanding errors.
    - They use probabilistic reasoning to determine the relative likelihood of each cause.
    - They are used as an aid to the designer in understanding system sensitivities.
  - Probabilistic Risk Assessment Models of Command Generation Process
    - These models take into consideration the causes of failure during command generation.
    - The human related tasks can fail due to human errors. Probability of these errors are assessed using human reliability data banks from the nuclear industry.
- Standardization of Command Generation Processes

# Sample BBN Model



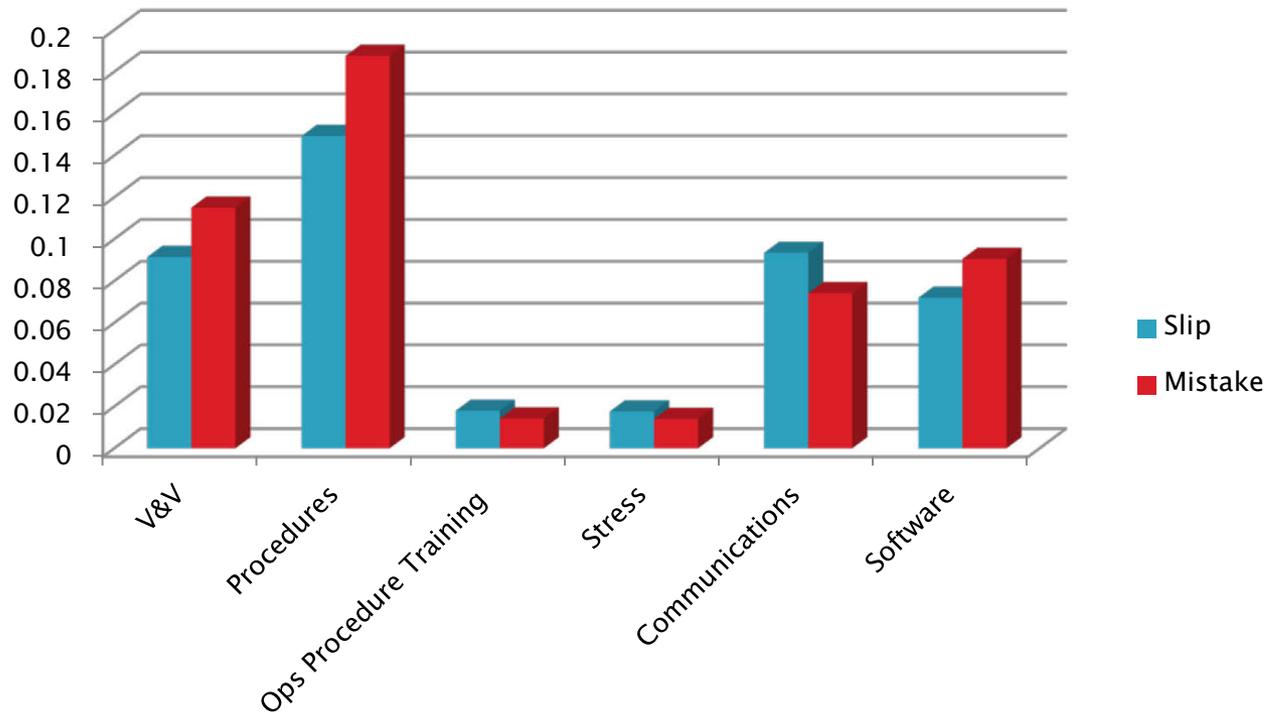
# Sample Sensitivity Analysis

Sensitivity of Probability of Slip to Variable

= Probability (Slip | Variable= Inadequate)-Probability (Slip | Variable=Adequate)

Sensitivity of Probability of Mistake to Variable

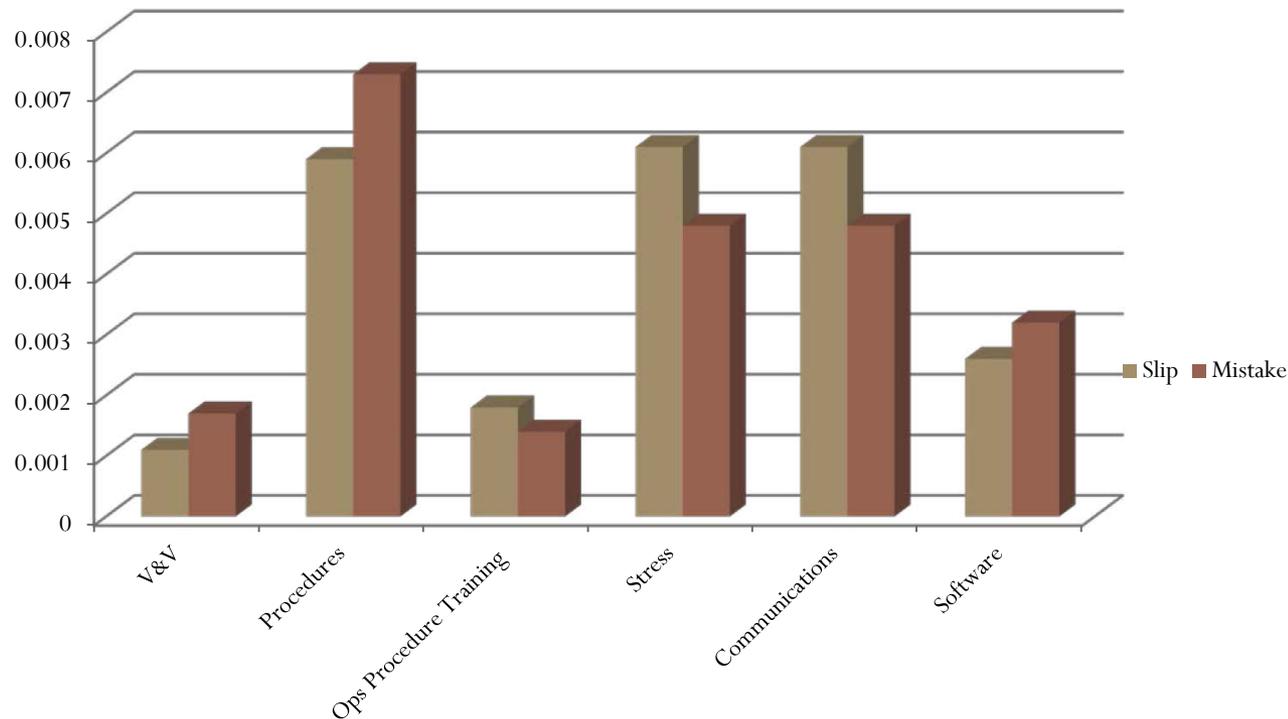
= Probability (Mistake | Variable = Inadequate) – Probability (Mistake | Variable = Adequate)



# Sample Importance Analysis

Improvement Potential Contribution of Variable to Probability of Slip Reduction  
= Probability (Slip| Variable= Baseline)-Probability (Slip | Variable=Adequate)

Improvement Potential Contribution of Variable to Probability of Mistake Reduction  
= Probability (Mistake| Variable = Baseline) – Probability (Mistake| Variable = Adequate)



# Sample Selected Scenarios

<b>Scenario</b>	<b>Probability of Slip Error</b>	<b>Probability of Mistake Error</b>
Baseline Case	4.67%%	4.57%%
Baseline Case + Poor Communications	13.4%%	11.5%%
Baseline + Poor Communications + High Stress	14.6%%	12.4%%
Baseline + Inadequate Procedures	19%%	22.6%%
Baseline + Inadequate Procedures + Inadequate V&V	24.8%	29.9%
Baseline + Inadequate Procedures + Inadequate V&V+ Poor Communications + High Stress	33.7%	36.8%

# Sample Probabilistic Root Cause Analysis

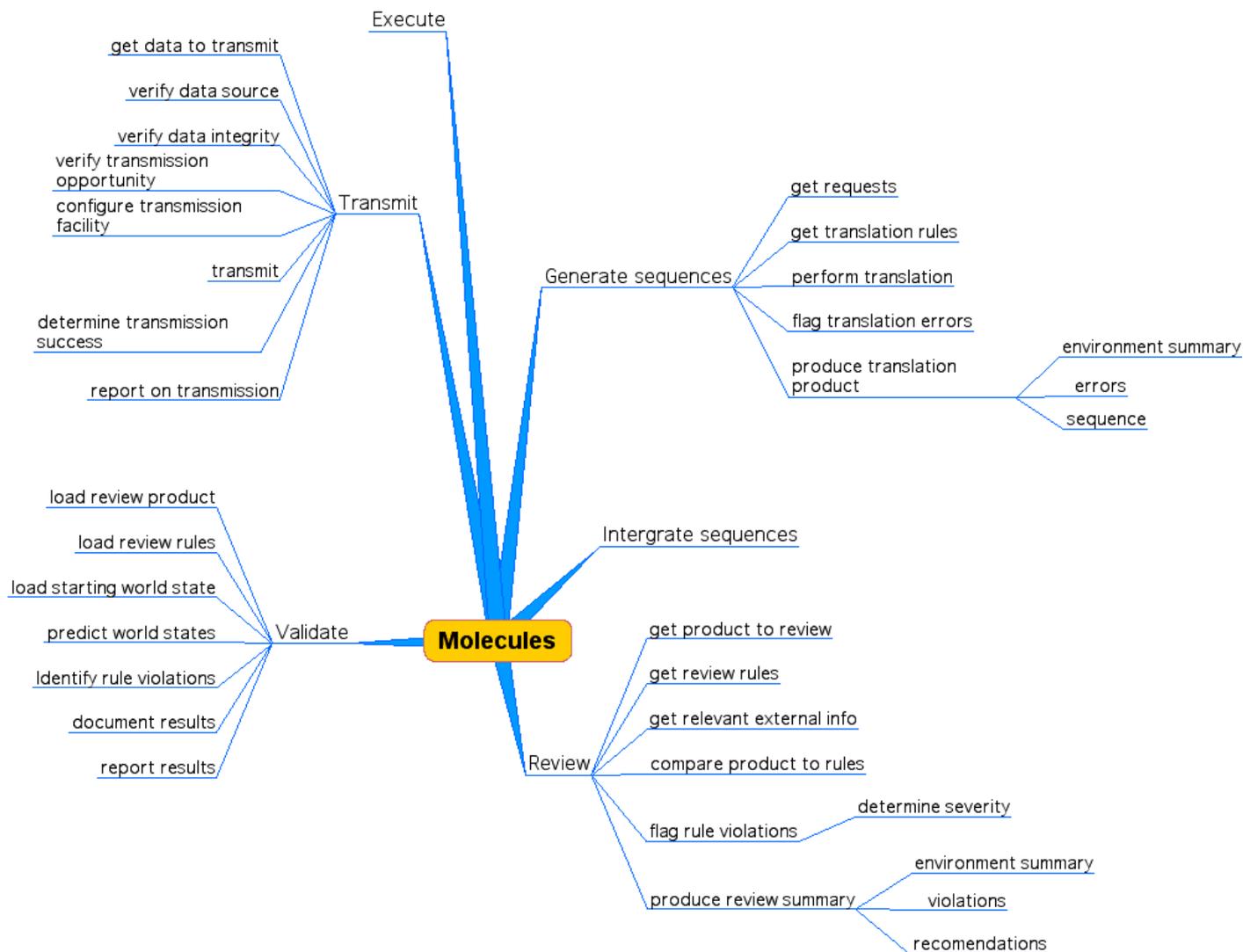
Slip Occurred?	Mistake Occurred?	Internal Factors Inadequate External Factors Inadequate (49.8%)	External Factors Inadequate
Yes	Yes	58.40%	47.30%
Yes	No	45.80%	24.40%
No	Yes	31.80%	62.60%
No	No	98.90%	98.60%

# Sample Probabilistic Root Cause Analysis

	<b>Causes</b>	<b>Probability</b>
<b>Internal Factors Inadequate</b>	High Stress	30.30%
	Inadequate Communications	31.70%
	Inadequate Training	17.20%

	<b>Causes</b>	<b>Probability</b>
<b>External Factors Inadequate</b>	Inadequate Procedures	43.60%
	Inadequate Software	20.90%
	Inadequate V&V	8.39%

# Standardization: Function Decomposition From Project Architectures



Functional breakdown from project documentation study

# Probabilistic Risk Analysis (PRA) for Command Generation

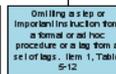
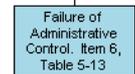
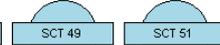
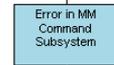
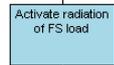
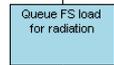
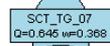
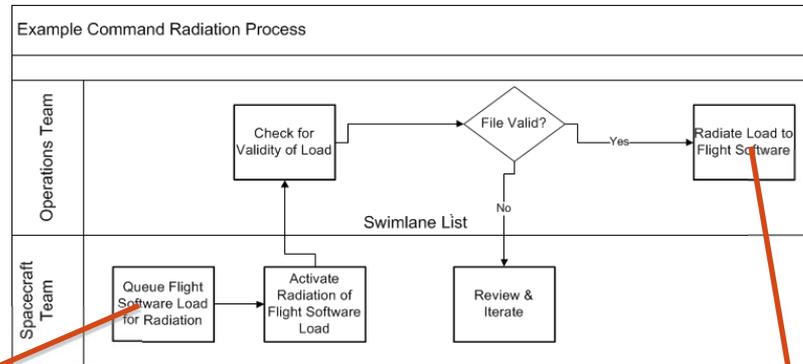
- ▶ The goal is to manage the risks associated with human errors during the command generation process.
- ▶ These models are applicable for:
  - ▶ Risk-based design of Command and Control functions
  - ▶ Mission Assurance of Command and Control functions
- ▶ There are several approaches for Human Reliability Analysis
  - THERP
  - Time Reliability Curves
  - SLIM/FLIM Methodology
  - HEART Approach
  - Cause-Based Decision Tree (CBDT) method
  - Holistic Decision Tree (HDT) Method
- ▶ We use a combined THERP and BPMN approach.
  - Data available is based on the THERP approach.
  - BPMN models facilitate the development of PRA models.

# Probabilistic Risk Analysis

- Probabilistic Risk Analysis (PRA) models for functions identified in the Command and Control standardization effort are built.
  - Models are executable.
  - They provide the possible end states for each function and its associated probability.
  - Data from human reliability handbooks are being used for running these models.
  - Models provide the possible end states for each function, and its associated probability.

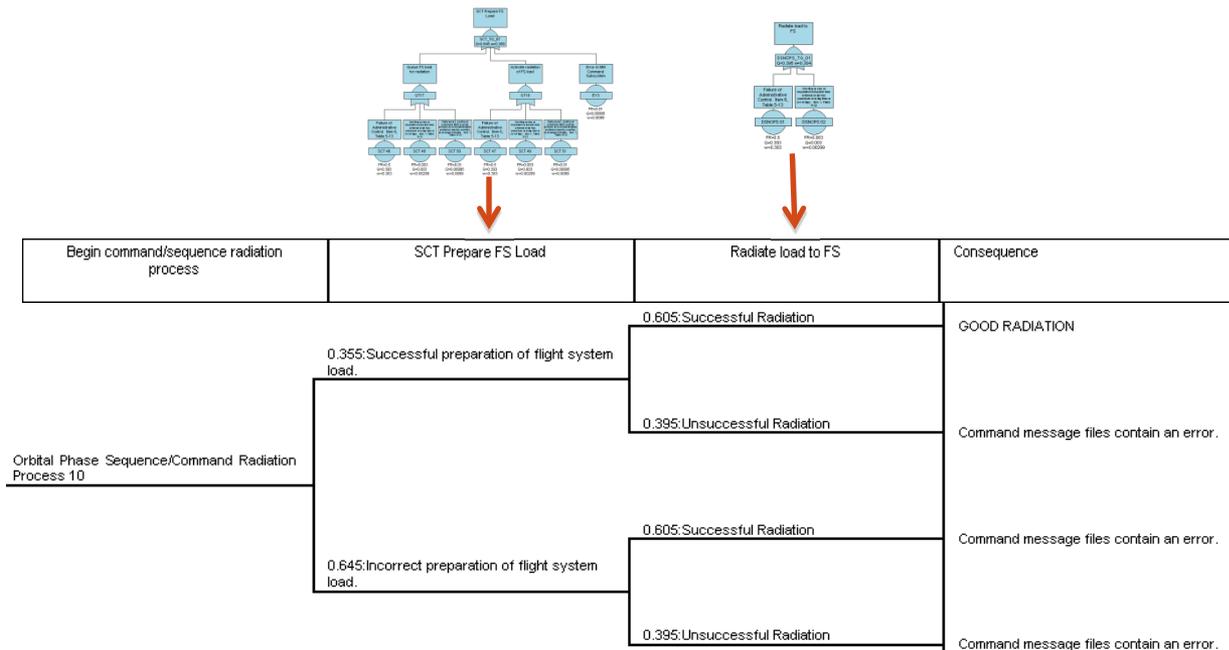
# Probabilistic Risk Assessment: Fault Trees

- Each sub-activity in an activity flow is modeled in a fault tree.
- These activities are further broken down into atomic level tasks that correspond to data in human reliability data banks.



# Probabilistic Risk Assessment: Event Trees

- Top gates from fault tree become successive steps in the event tree
- “Consequences” are used to capture end result of each branch in the event tree with the corresponding probability, and therefore, the output of the modeled activity



# Fault Links

- The correspondence between the “Periodic Table” that is built for standardizing Command and Control (C2) functions and the PRA models that are built for Risk Management is made via the “fault links”
- Each C2 function is the “composite material” built from “molecules” that are combinations of the “atoms” in the table.
- Each function or “composite material”, in turn, corresponds with a BPMN/Event Sequence Diagram.
- Each activity or “molecule” corresponds with a fault tree
- Each basic event in the fault tree corresponds with an “atom”.

# Representation of hypothetical model as Fault Links

Function (Composite Material)	Molecule (Sub-activity)	Atom (Event)	MTTF
Example Command Radiation Process	Begin command/sequence radiation process	Begin command/sequence radiation process	1.0
Example Command Radiation Process	SCT Prepare FS Load	"Failure of Administrative Control. Item 6, Table 5-13"	0.5
Example Command Radiation Process	SCT Prepare FS Load	"Failure of Administrative Control. Item 6, Table 5-13"	0.5
Example Command Radiation Process	SCT Prepare FS Load	"Omitting a step or important instruction from a formal or ad hoc procedure or a tag from a set of tags. Item 1, Table 5-12"	0.0030
Example Command Radiation Process	SCT Prepare FS Load	"Omitting a step or important instruction from a formal or ad hoc procedure or a tag from a set of tags. Item 1, Table 5-12"	0.0030
Example Command Radiation Process	SCT Prepare FS Load	"Carry out a [...] policy or scheduled tasks such as periodic tests or maintenance performed weekly, monthly, or at longer intervals. Item 1, Table 5-13"	0.01
Example Command Radiation Process	SCT Prepare FS Load	"Carry out a [...] policy or scheduled tasks such as periodic tests or maintenance performed weekly, monthly, or at longer intervals. Item 1, Table 5-13"	0.01
Example Command Radiation Process	SCT Prepare FS Load	Error in MM Command Subsystem	0.01
Example Command Radiation Process	Radiate load to FS	"Failure of Administrative Control. Item 6, Table 5-13"	0.5
Example Command Radiation Process	Radiate load to FS	"Omitting a step or important instruction from a formal or ad hoc procedure or a tag from a set of tags. Item 1, Table 5-12"	0.0030

# Use Case – Anomaly Investigation

- Bayesian Belief Network Models:

- For the use case in this study:

- Each anomaly is examined, its' root causes identified in the model and two key scenarios are examined.

- Scenarios where root causes are present.

- Scenario where the root cause eliminated with corrective action is no longer present.

- The probability of commanding error in each case is assessed and compared.

- Probabilistic Risk Assessment Models:

- Probability of error path that led to anomaly is computed, purely with consideration of human error probabilities.

- Note that command generation process errors fall under the category of “Process Compliance” root causes in the BBN model.

- Furthermore, the PRA modeling approach is used to represent and analyze sequence of seemingly unrelated activities that lead to commanding errors.

- That was the case for one of the anomalies.

# Summary of Observations for Use Case

- The anomalies studied were caused due to the following:
  - Inadequate Procedures
    - Process maturity or incomplete process requirements.
  - Lack of Process Compliance.
  - Lack of Understanding of System Behavior/States.
    - Low fidelity of software simulations. (not clearly communicating state of the system.)
  - Inadequate Communication
    - Inter-team or Intra-team communications.
- Most corrective actions address the “Procedures” part of the problem.
  - Although in some instances creating and following clear procedures prevents errors due to lack of understanding system behavior or states of the system, this issue is not addressed directly in the corrective actions.
  - Corrective actions to improve communications or process compliance are not made explicitly.

# Sample PRA Model : Accident Scenario

## Command to Delete Packet Violated Flight Rules

- There was an unexpected data storage overflow
- This resulted in a change in original planned sequences.
- Plans violated flight rules.
- Flight rule violation was not flagged prominently during review/approval portion of the process.
- There is an 0.089 chance of this path occurring.

UNEXPECTED DATA STORAGE OVERFLOW	RE-PLAN SEQUENCE	VALIDATE	APPROVE	Consequence	Frequency
w=1	Q=0.4071	Q=0.3695	Q=0.5923		1
				Command success	0.1524
				Repeat process. delay in sending command	0.2214
				Repeat process. delay in sending command	0.08932
				Repeat process. delay in sending command	0.1297
				Repeat process. delay in sending command	0.1047
				Repeat process. delay in sending command	0.152
				Repeat process. delay in sending command	0.06133
				Command Error	0.08909

# Current Capability and/or Results

- Existing standardized models
  - Periodic table
  - PRA models.
- Existing BBN models
  - Application to several missions
  - Sensitivity analyses
  - Collaboration with key Mission Assurance Management.

# Planned Capability and/or Application

- Extension of BBN models to multiple missions (MRO, MER)
- Synthesis of results for JPL Process improvement.
- Inclusion in JPL Design Principles.

# Technical Solutions Found

- Standardization Approach
- Systems Modeling and Analysis
- Extension to Software Reliability Engineering

# Remaining Technical Challenges

- Completing threads of ongoing work:
  - Tutorial for use of existing data/models/etc.
  - Paper on Software Reliability Engineering
  - Paper for “Managing Command Errors” jointly with Larry Bryant.
- Integrating with other efforts
  - Exploring AADL integration with Michela Munoz Fernandez
  - Exploring Software Reliability Engineering connection with Allen Nikora