



Command Process Modeling & Risk Analysis

August 2011

NASA Software Assurance Symposium

Washington, DC

Principal Investigator: Leila Meshkat

Jet Propulsion Laboratory, California Institute of Technology

Copyright © 2011 California Institute of Technology. Government sponsorship acknowledged

Outline

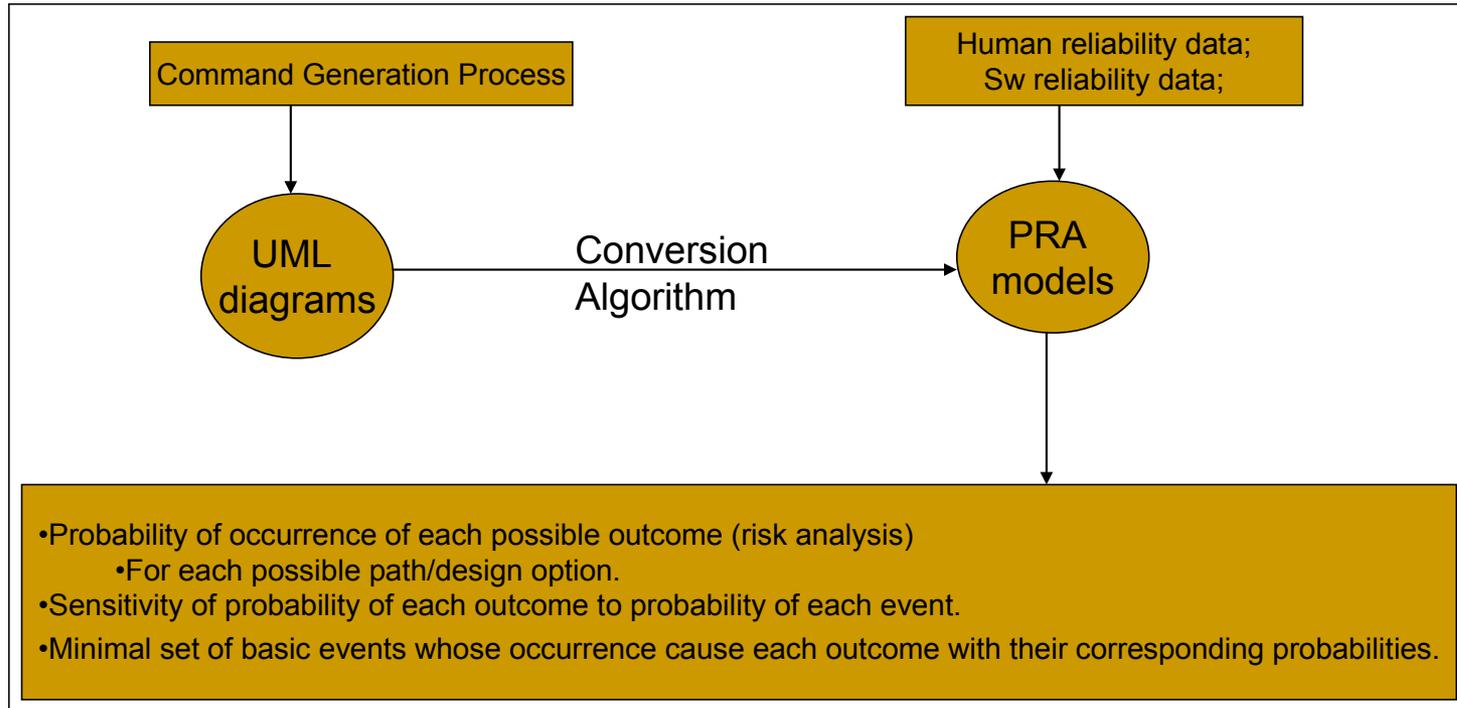
- ▶ Background
 - Research Goals
 - Approach
- ▶ Executive Summary
- ▶ Bayesian Belief Network
- ▶ Periodic Table
- ▶ Functional Analysis
- ▶ Risk Analysis
- ▶ Summary & Conclusions
- ▶ Acknowledgements

Background

Research Goals

- ▶ The goal of this research effort is to develop a suite of techniques and corresponding tools that enable the thorough analysis and informed design of a robust operations process. This suite will provide a decision support methodology for conducting trade studies during the development of operations processes as well as guidance for improving existing processes and mitigating perceived errors.

Background Approach

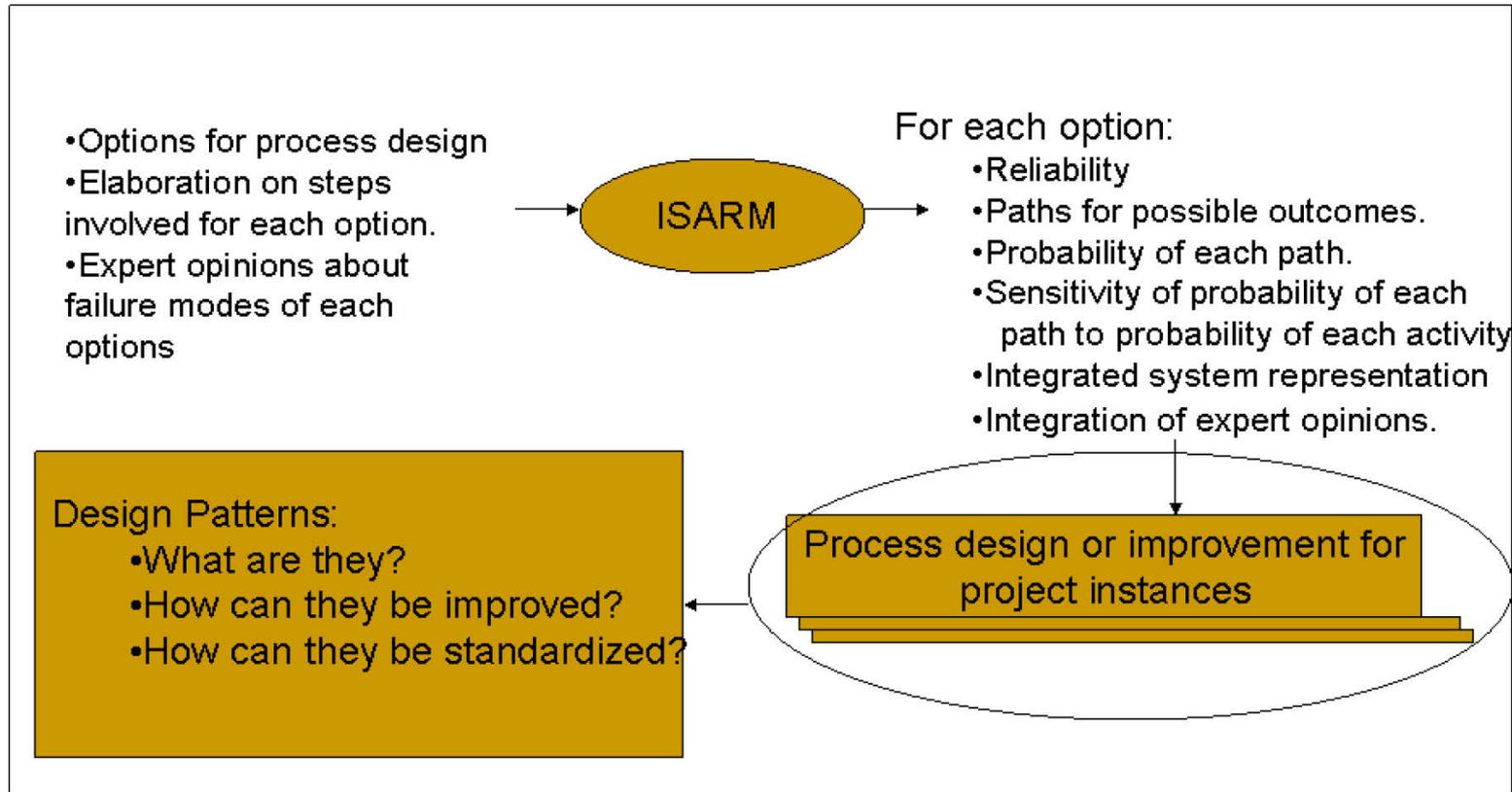


Periodic Table: Atoms → Molecules → Composite Material → Mission Characteristics

PRA Models: Composite Material → Molecules → Atoms

Background

Approach – Expected Results



Periodic Table: Menu of Composite Material to pick from during design phase.
Each menu item comes with a preliminary design and risk model

Executive Summary

➤ Broadening the Problem Definition

- But why are there commanding errors across JPL missions?
 - What is the role of command process modeling in reducing them?
 - Create an optimization model that looks at the options for reducing the likelihood of each root cause, and the cost and benefit of each option or set of options.
- Periodic Table for Standardizing Command and Control Functions for Space Missions
 - Include full range of missions.
 - The key “Molecules” and “Atoms” that are common to a broad range of missions have been extracted and specified.
 - Analysis
 - Simulation Analysis
 - ProModel (Business Process Modeling Network)
 - Probabilistic Risk Analysis
 - Fault Tree +.

Bayesian Belief Network Models

▶ Current Context

- Reviewed JPL Incident & Anomaly Reports
- Collaborated with a working group which has been studying commanding errors for several years.
- Developed a Bayesian Belief Network of the commanding errors, and their causes.
 - Data for executing this model is based on expert opinions combined with historical data (within JPL) and human reliability data (across the nuclear industry).
- Iterated upon the model with several key experts across JPL and solidified basic assumptions.
- Identified the role of Command Process Modeling in the big scheme of commanding errors.
- **Buy-In at the JPL Institutional Level.**

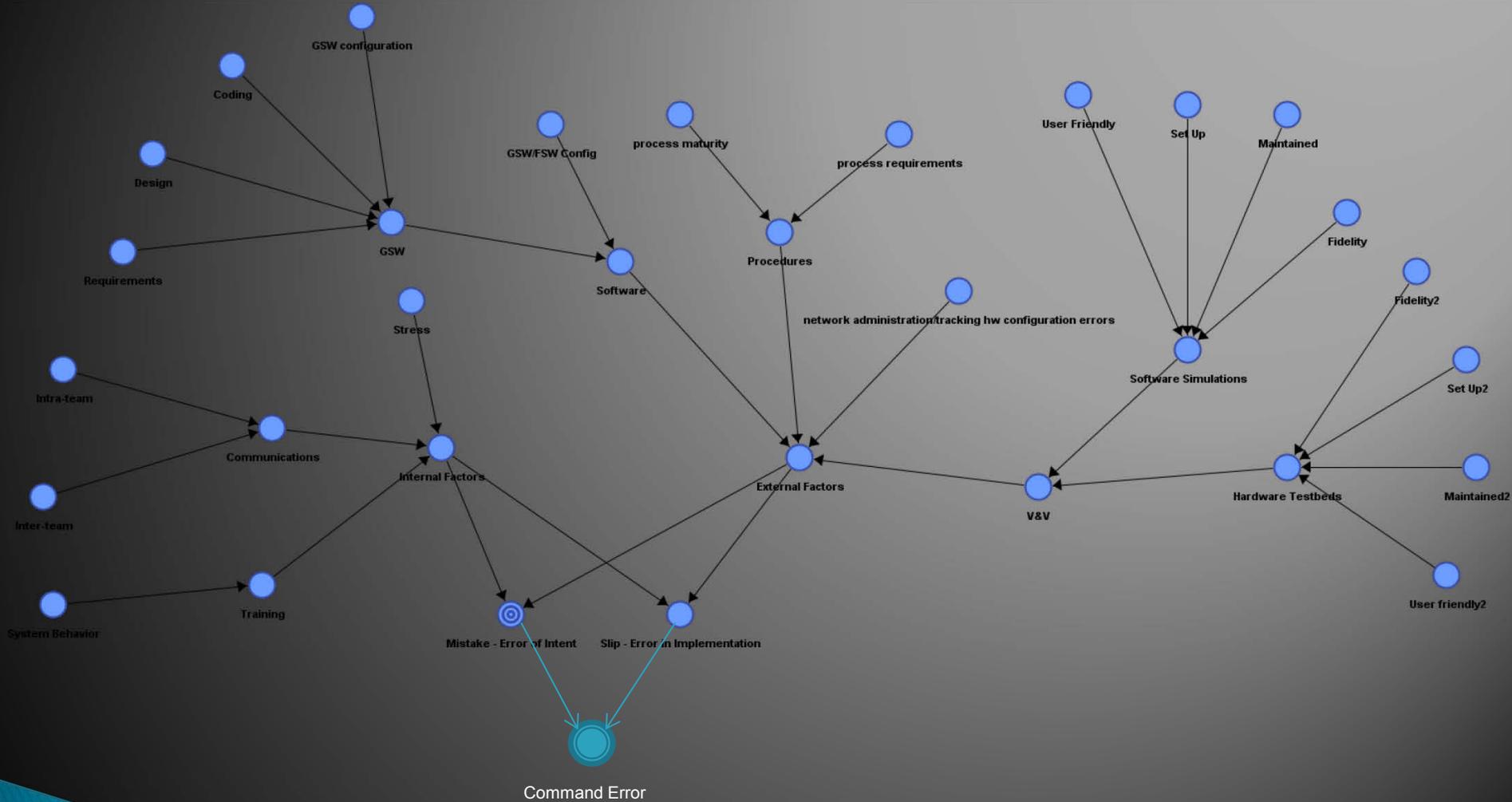
Problem Formulation

BBN Modeling for Commanding Errors

▶ Definitions:

- There are two general types of errors:
 - Errors of intent or “mistakes”
 - Errors in implementing the intent or “slip”.
- Factors that determine whether or not an error occurs can be classified into:
 - External Factors : Factors that are external to the human operators and indirectly affect them.
 - Adequacy of Models and Simulations, Test-beds and Prototypes, Procedures, Auto-checkers, Configuration Management., GSW/FSW Interactions.
 - Internal Factors: Factors that effect the cognitive abilities of the human operators directly.
 - Level of stress and adequacy of training.

Bayesian Belief Network Model



Periodic Table

- ▶ Examined the breadth of space missions and their associated command and control structure
- ▶ Identified eight main molecules:
 - Collect goals or objectives
 - Generate state requests or commands
 - Generate Sequences
 - Validate Sequence
 - Transmit Sequence
 - Execute Sequence
 - Analyze results
 - Make corrections
- ▶ Atomic decomposition of each molecule specified.
- ▶ Currently being mapped to existing data.

Functional Analysis

- The Object Management Group, which is a sub-group of the International Council on Systems Engineering, recommends using BPMN notation for business process modeling.
- UML models of key functions are under transition to BPMN models.
- Simulation Analysis underway.
 - Models are executable.
 - Provides metrics such as time to complete simulation.

Risk Analysis

- ▶ Probabilistic Risk Analysis for same functions are also being built.
 - Models are executable.
 - Data from human reliability handbooks are being used for running these models.
 - Models provide the possible end states for each function, and it's associated probability.
 - Models results can readily be transferred to other tools for performance analysis as appropriate.

Summary & Conclusions

- ▶ Commanding Errors may be caused by a variety of root causes.
- ▶ It's important to understand the relative significance of each of these causes for making institutional investment decisions.
- ▶ One of these causes is the lack of standardized processes and procedures for command and control.
- ▶ We mitigate this problem by building periodic tables and models corresponding to key functions within it.
- ▶ These models include simulation analysis and probabilistic risk assessment models.

Acknowledgements

- ▶ The work was sponsored by the NASA Office of Safety and Mission Assurance under the Software Assurance Research Program. This activity is managed locally at JPL through the Assurance and Technology Program Office.
- ▶ Team Members include:
 - Professor Joanne Bechta Dugan (BBN Modeling – UVA)
 - Ken Evensen (PRA Modeling – JPL)
 - Sven Grenander (Periodic Table – JPL).
- ▶ Many thanks to Allen Nikora and Lisa Montgomery for their feedback and review of technical content of task as it has evolved.