A Systems Approach to Reliability Enhancement

Leila Meshkat
Jet Propulsion Laboratory
California Institute of Technology

© 2013 California Institute of Technology.
Government sponsorship acknowledged

Outline

- Overview
- Reliability Analysis for the project lifecycle
  - Conceptual Design
    - TeamX Case Study
  - Development & Implementation
    - Mars Orbiters Case Study
  - Operations
    - Anomaly Investigation Case Study
    - Managing the Risk of Command File Errors
- Summary & Conclusions

Overview

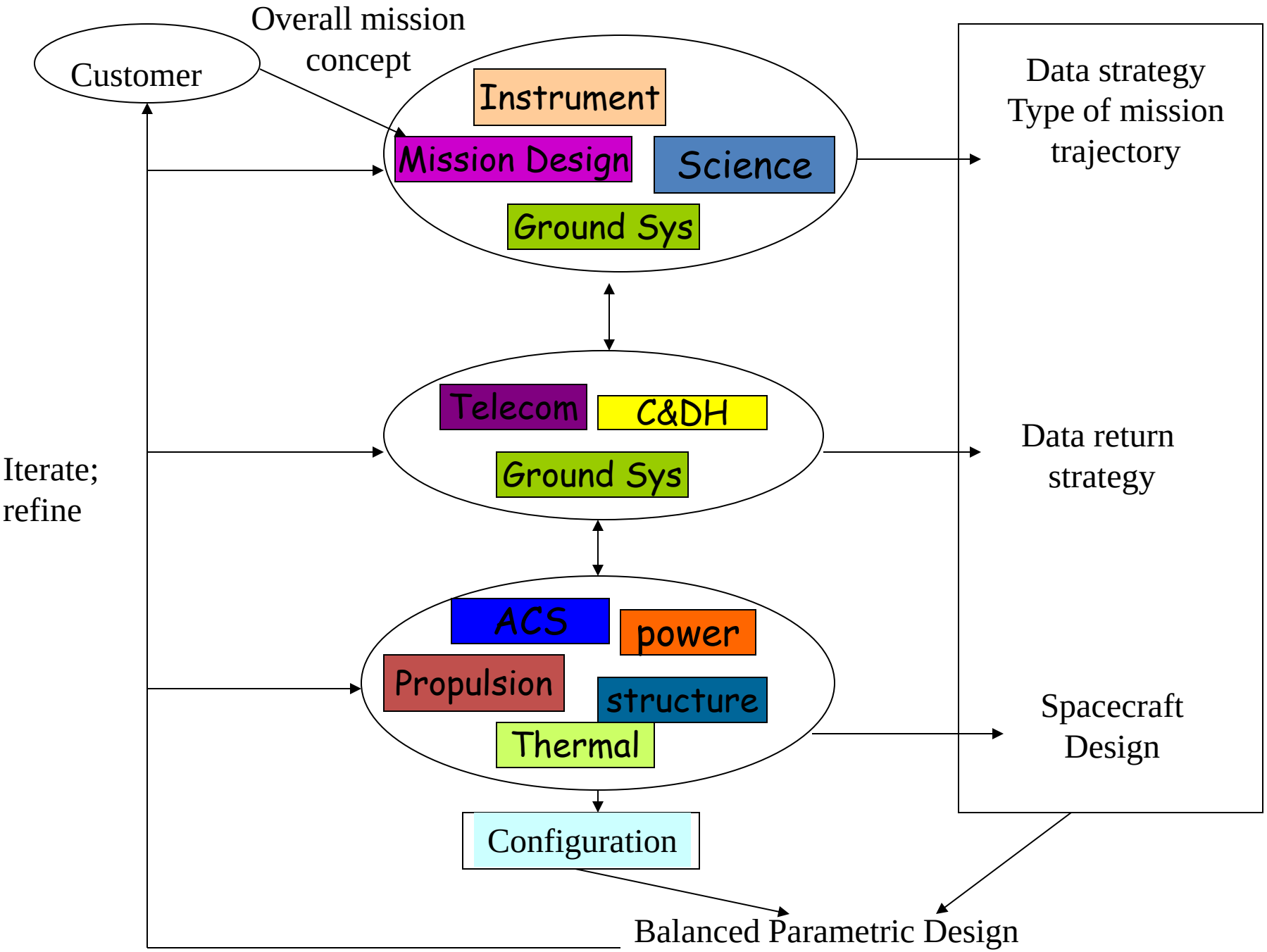
- Reliability and Risk are measures of performance of a system and should be considered within the context of the system design, development and operational lifecycle.

- Engineering projects typically have several major phases:
  - Concept Development & Design
  - Detailed Design & Implementation
  - Operations

- This talk provides example reliability analyses conducted by the author for each of these phases of the lifecycle in the context of spacecraft design, development and operations and concludes with a vision for a systemic approach for reliability enhancement.

Conceptual Concurrent Design Context

- JPL's Advanced Design Team or TeamX
  - Produces Conceptual Space Mission Designs.
  - Mainly for the purpose of Feasibility Studies.
  - Duration of study is typically one to two weeks.
  - Final report includes equipment lists, mass and power budgets, system and subsystem description, and projected mission cost estimate.


Customer
Overall mission concept
Instrument
Mission Design
Science
Ground Sys
Telecom
C&DH
Ground Sys
ACS
power
Propulsion
structure
Thermal
Configuration
Data strategy
Type of mission trajectory
Data return strategy
Spacecraft Design
Iterate; refine
Balanced Parametric Design

Risk Assessment/ Risk Chair Creation & Infusion

STEP ONE:	STEP TWO	STEP THREE	STEP FOUR
•Define Risk Terminology; •Define software requirements	•Design Architecture for Software tool •Initiate Process of “risk training” within team	•Develop prototype tool. •Train team members to use tool and refine tool using team feedback. •Determine role of risk chair/ approach for risk communication within team.	•Use tool concurrently during design. •Build standard risk item libraries to make consistent assessments across missions. •Refine tool •Add additional features; •Towards Probabilistic Risk Assessment in Conceptual Design

Risk & Rationale Assessment Program (RAP)

- Distributed software that enables communication between designers.
- User can initiate a “New Risk” or assess a risk already on their screen.
- Features include:
  - Risk statement- likelihood, impact, type of risk.
  - Mitigation- residual likelihood & impact.
  - Details – any additional explanation.
  - Objective that the risk effects.
  - Affected Roles
- System allows user to enter as little or as much information as they want.
- It can automatically generate reports for any combination of roles.
  - Report includes fever chart, overview table, and all details

Risk & Rationale Assessment Program (RAP)

New Risk… Update RAP View Chart Report…

Study: Test

Role: Risk

	Risk Element		Impact	Likelihood	Mitigation		Impact	Likelihood	Details
	Other pe								
	Can't get mph.								
	short sch								
	I might e informati								
	test								
	Second t								
	People d								
M	short schedule		3	3					
L	RAP & RAP interactions		1	1					

Risk Scoring

Risk: Other people sending you junk

Objective: Mission Success

Mitigation: none

Description:

Status: Open

OK Cancel

Likelihood 1 2 3 4 5

Impact 1 2 3 4 5

	Informational Risks		Impact	Likelihood	Mitigation		Impact	Likelihood	Details
L	Second test (Systems)		2	2					

Risk Analysis Sheet1

Experiments with Probabilistic Risk Assessment in TeamX

- Case study for Mars Aero-capture Mission Design:
  - Used the TeamX sessions to generate data needed for conducting PRA
    - Data related to expert opinions about events, risk items, and mitigations was collected through RAP.
    - Design information, and system schematics was included in the subsystem write-ups.
    - Used information for building PRA models with several different tools.
      - These tools include DDP, QRAS and Galileo ASSAP
      - Each tool served a different purpose
    - Developed algorithm for combining different PRA tools and approaches.

Reliability Analysis for other phases – Mars Orbiters

- Development, Implementation and Operations Phases of Mars Orbiters:
  - Determine type of analysis required for each orbiter.
    - Determine major failure drivers for each case.
      - For orbiters that are not yet in orbit:
        - » Determine the events leading to orbit.
        - » Determine the probability of success/failure of each event.
        - » Aggregate this with the reliability analysis of the spacecraft using system schematics information.
      - For orbiters that are in orbit:
        - » Determine the current state of the spacecraft.
        - » Obtain the latest consumable information for life-limiting components, including the fuel.
        - » Conduct a reliability analysis of the spacecraft using system schematics information.
  - Build appropriate reliability models.
  - Obtain the reliability of each orbiter over time using these models.
  - Iterate as more information is obtained/accumulated.

Integrated Approach – Mars Orbiters

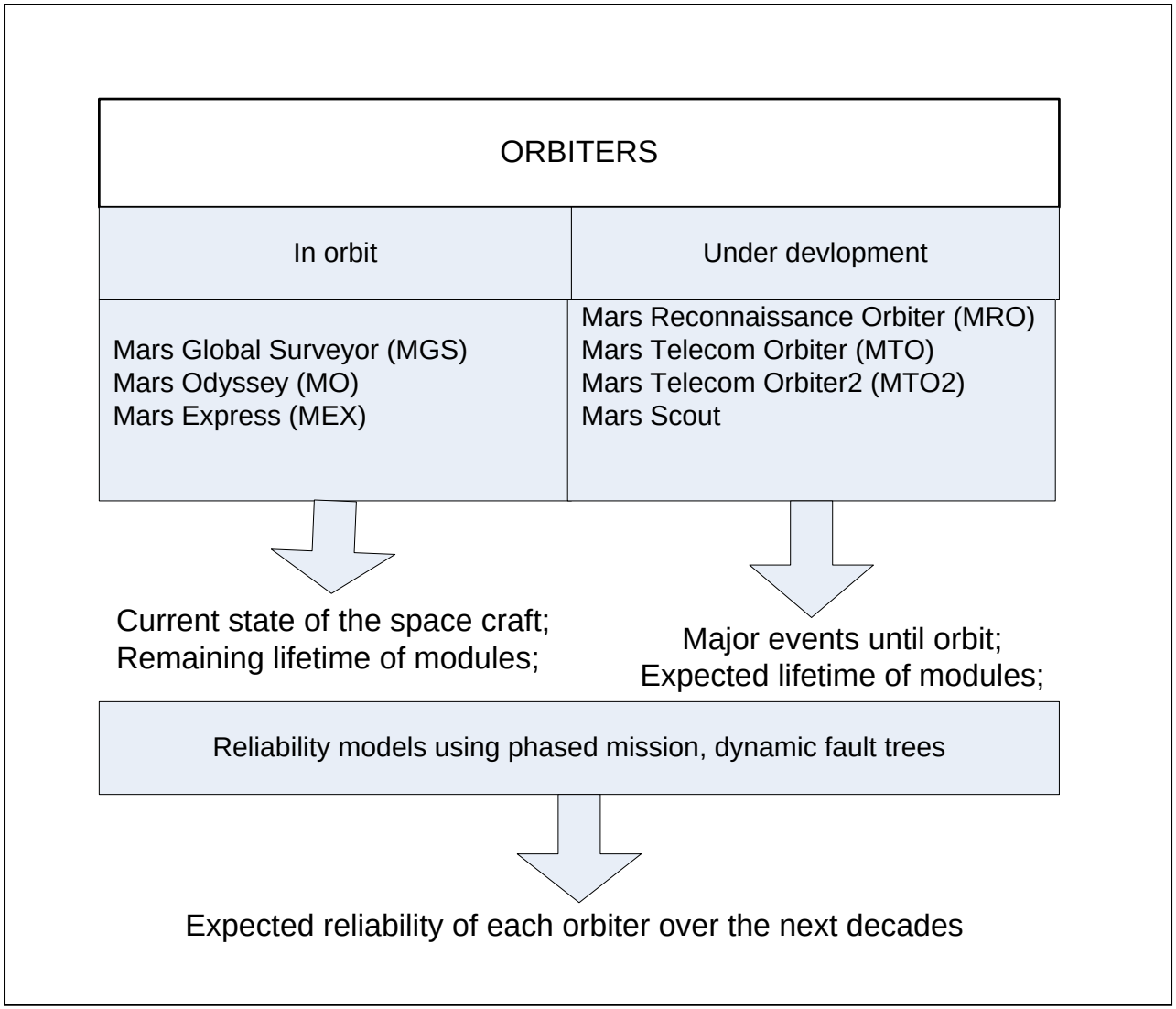


Figure 1: Reliability analysis process for the Mars Orbiters

* Some of these orbiters were planned to be launched at the time this study was conducted.

Data Sources – Mars Orbiters

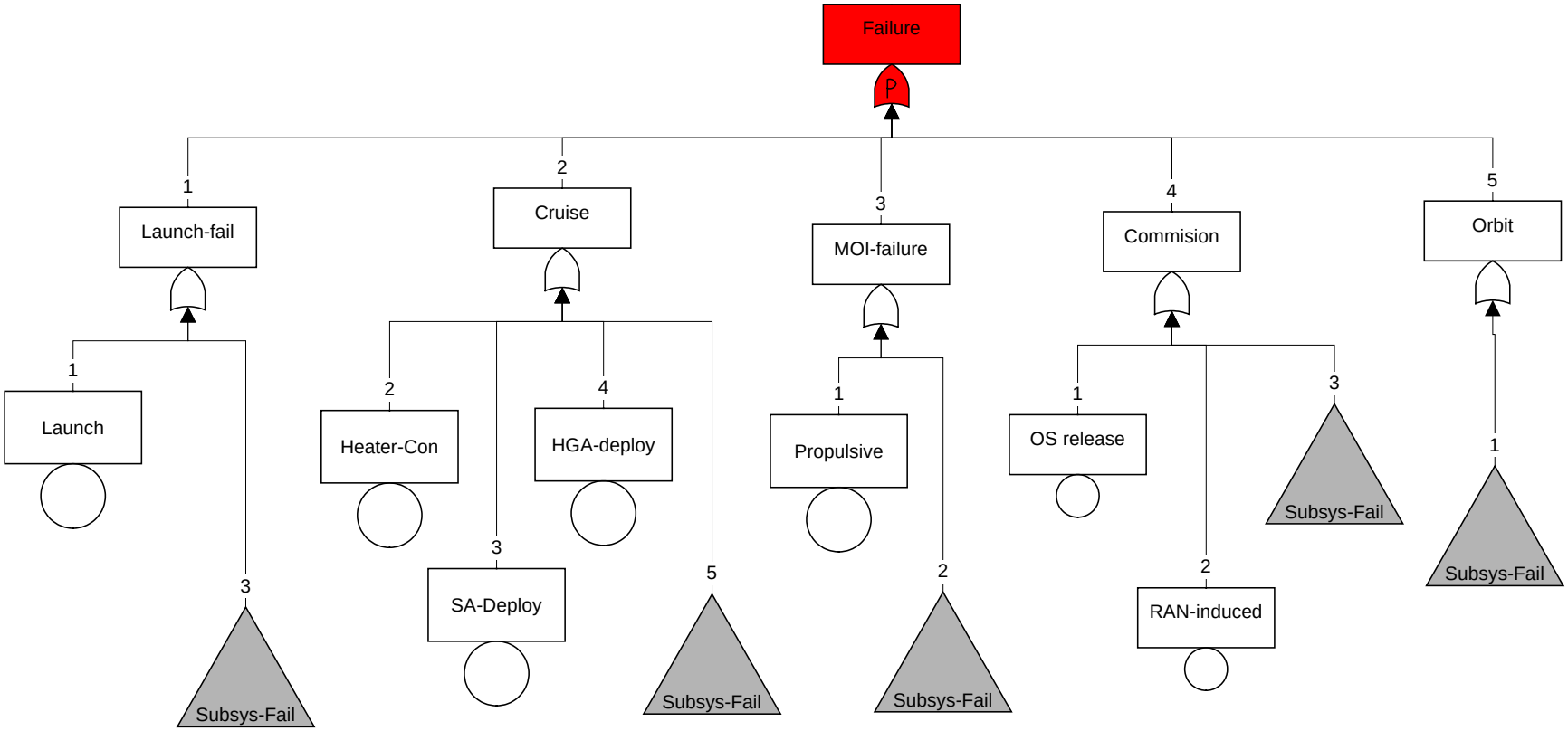
- System Schematics of the Mars Odyssey and Mars Reconnaissance Orbiters.
- The conceptual design information from the Mars Telecommunications Orbiter obtained from TeamX.
- Failure information of components:
  - Remaining lifetime and thermal duty cycles of the Odyssey System Components.
  - Engineering estimates & expert opinions.
  - Exponential distribution
- Fuel Expenditures:
  - Function of the expected fuel consumption per unit time.
    - Steady state burn rate,
    - Fuel consumption rate for planned targeting maneuvers.
    - Fuel usage for anomalies.
  - Aggregated information ➔ P(running out of fuel at time t.)
  - Weibull distribution.

Modeling Approach: Critical Events – Mars Orbiters

	Orbiters			
	MRO	MTO	MTO-2	Mars Scout
Major Events				
Launch	x	x	x	x
Antenna Deployment	x	x	x	x
Heater Configuration	x	x	x	x
Solar Array Deployment	x	x	x	x
Propulsive Capture		x	x	x
Aerobraking	x			
Orbiting Sample Release		x		
Rendezvous & Autonomous Navigation Experiment		x		

* These orbiters were planned to be launched at the time this study was conducted.

Modeling Approach: Sample Dynamic Fault Tree – Mars Orbiters



PRA during Spacecraft Operations – Anomaly Investigations

- During operations, goal is to maximize the utility of the space mission.
  - This goal is often achieved by maximizing the lifetime of the mission and utilizing the spacecraft to achieve the desired objectives, which can be science measurements, relay, or technology demonstrations.
- QRA models can help support the decisions by addressing:
  - What are currently the most likely failure paths in the system based on the latest information available?
  - What component do we expect to fail next?
  - How sensitive is the system reliability, key risk drivers, and failure behaviour of the system to:
    - The failure of each component.
    - Possible environmental effects due to changes in the trajectory and/or orbit.
    - Possible common cause failures.
    - Failure propagations due to software commands.
    - Anomaly resolution activities (such as resetting the system).
  - How do our assumptions about the system behavior affect the reliability and sensitivity metrics of the system.

Problem Addressed- Anomaly Investigations

- To determine the effect of anomalies on the remaining lifetime and failure scenarios of the spacecraft for the Mars Odyssey (ODY), and Mars Reconnaissance (MRO) Orbiters.

- Following questions were addressed during the post-anomaly risk analysis:
  - What are the updated failure paths for the system?
  - How can we utilize the information obtained from the failure of the components that have caused the anomalies to better understand the failure characteristics of other similar components in the system?
  - Are there any common causes of failure? In other words, could the causes of the anomalies also propagate throughout the system and cause other failures in the system?

Case Study 1: MRO – Anomaly Investigations

- Following anomalies had occurred:
  - An anomaly had occurred in a waveguide transfer switch (WTS) reducing the number of possible paths for routing the redundant X-band Traveling Wave Tube Amplifiers (TWTA's) to the antennas.
  - The Ka-band exciter of the A-side Small Deep Space Transponder (SDST) had failed; while this was mainly a technology demo, it also provided some redundancy as an independent high rate downlink option.
  - A side swap had occurred in the Command and Data Handling system from side A to side B.

Case Study 2: ODY- Anomaly Investigations

- The B side of the High Energy Power Supply (HEPS) unexpectedly shut down.
  - It provides power to the B-side hardware.
  - It had been a hot spare for the A side.
  - ODY has limited cross-strapping between sides.
  - Components on A-side have been degraded more since they have been in use all these years.
  - Some components (including IMU and UHF) on A-side have limited remaining lifetime.

Post-anomaly Risk Modeling

- The main objective was to determine how these anomalies affect the remaining lifetime, and the various failure scenarios of the system.
- New information had been generated over the course of time.
  - information about the failure behaviour of the individual system components and,
  - information about the failure paths in the system.
- In order to have a better understanding of how the anomalies affect the failure paths of the system it was important to increase the fidelity of the models associated with the subsystems that were most affected by the anomalies.

Operations Phase: Managing the Risk of Command File Errors

- 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.

Command File Error 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

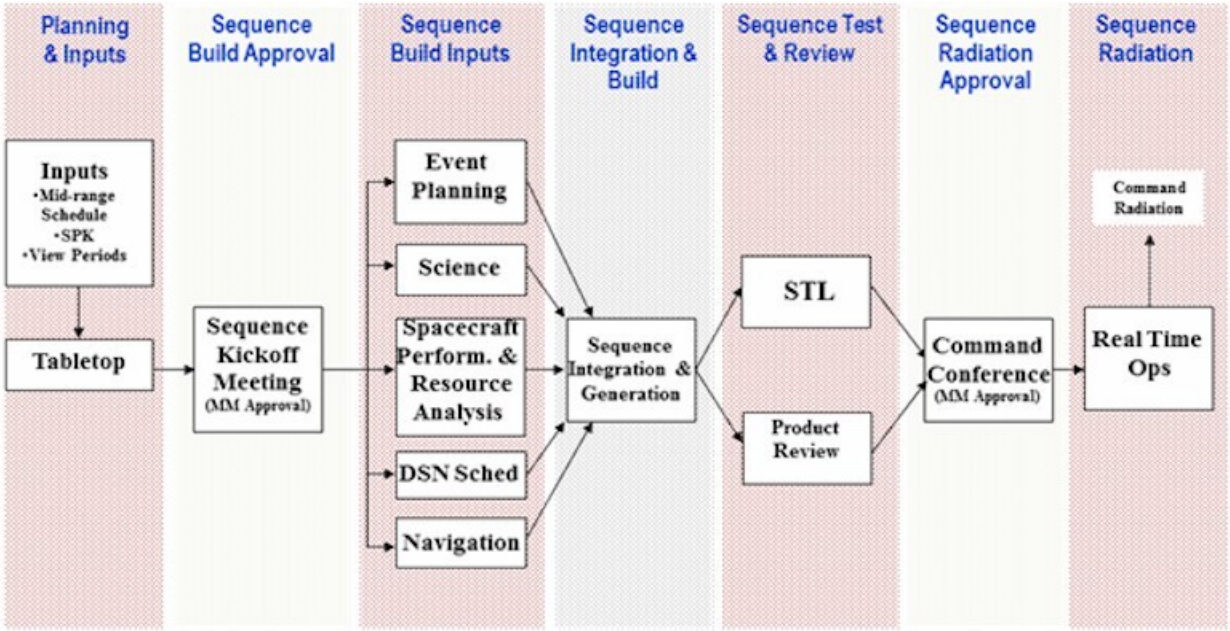


Figure 1. Generic Command Generation Process

Sequence Diagram for Sample Command Generation Function

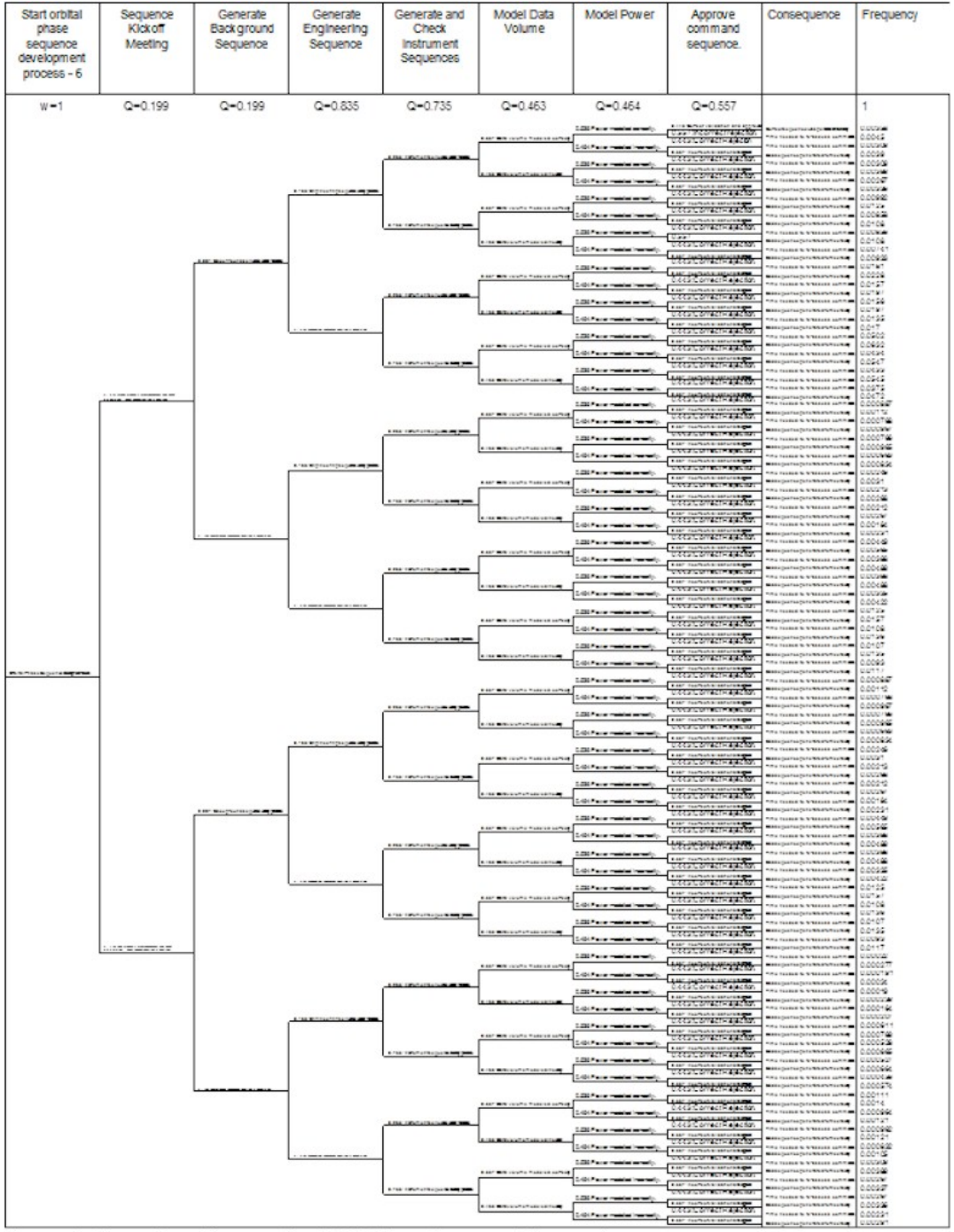
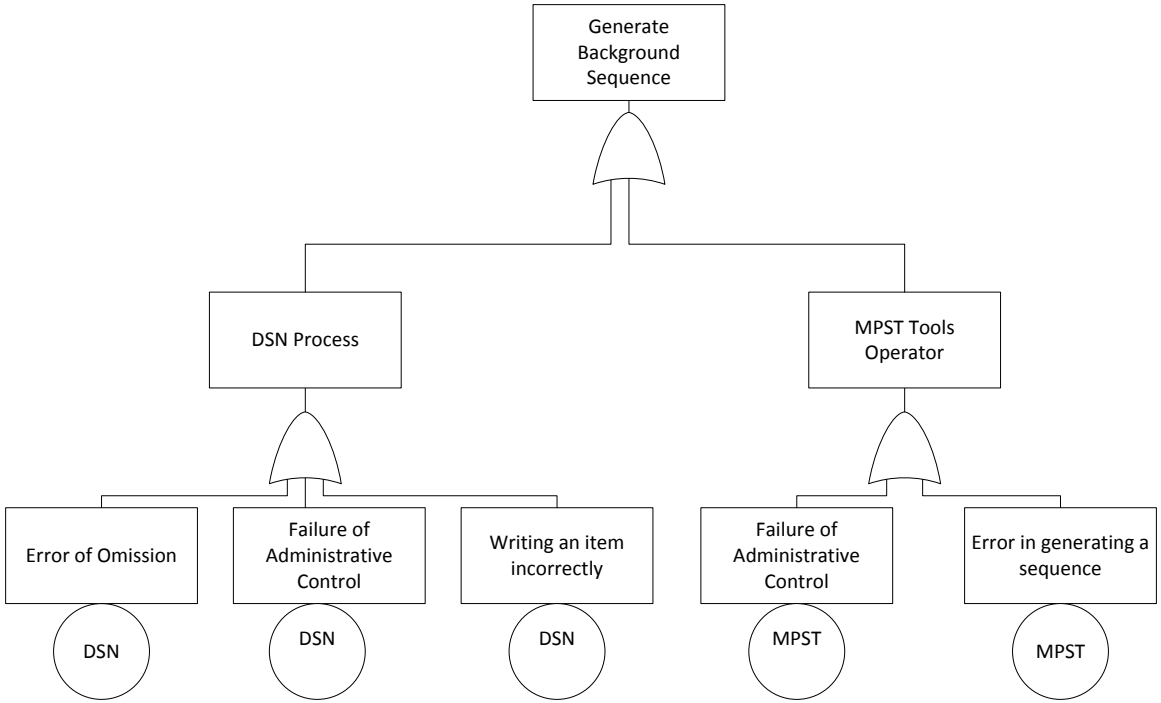


Figure 2. Event Tree Diagram for Orbit Phase Command Generation

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

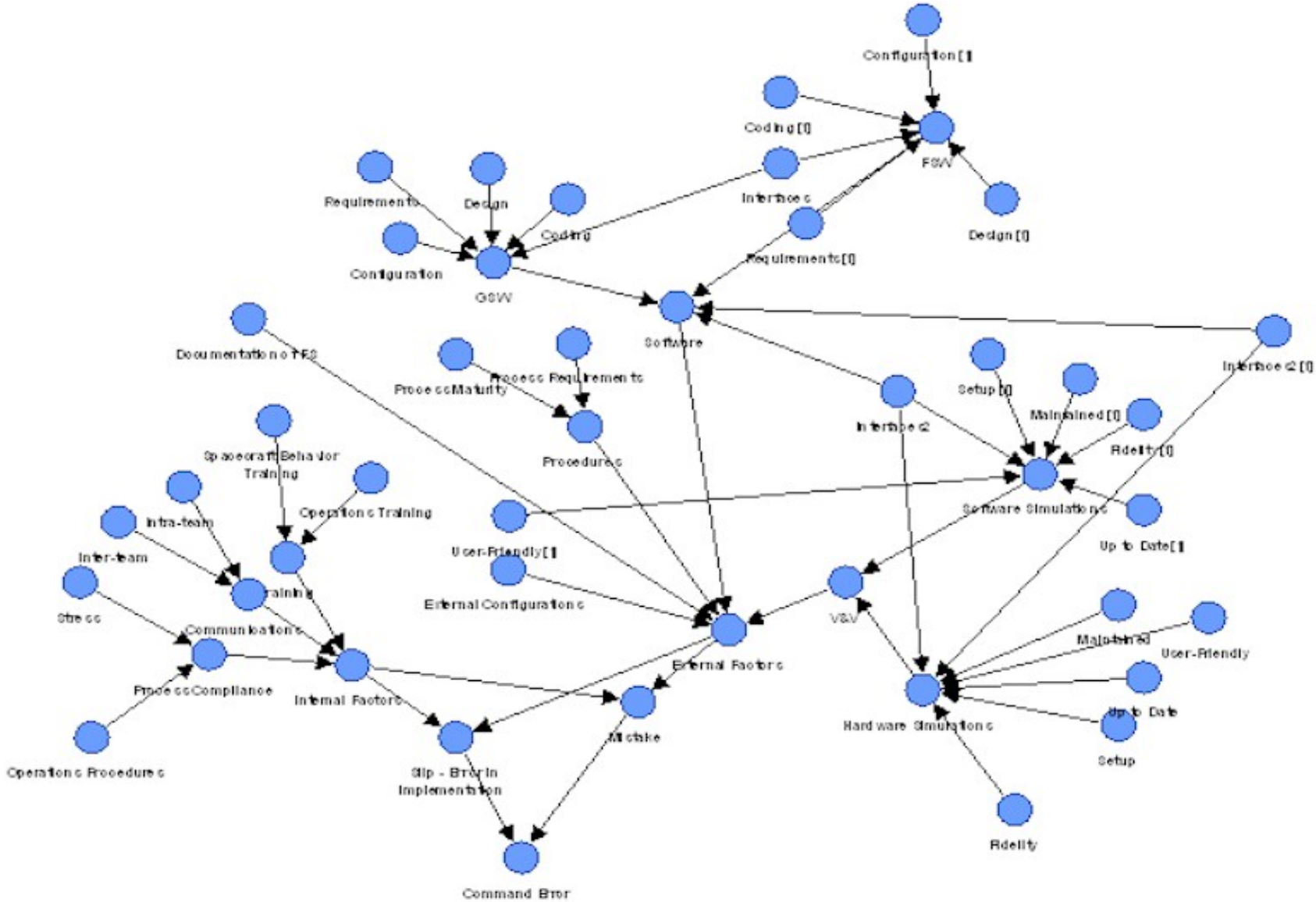


Figure 4. Overall BBN representing Command File Errors

Summary & Conclusions

- Several pieces of work, spanning multiple phases of the spacecraft design, development and operations phases were presented.
- Connecting these pieces together and continuously updating and maintaining models would provide much greater insight during the lifecycle of a project.
- The end to end systems approach would include the addition of subtle behaviors of real time embedded systems and the connection of hardware, software and human/operational error models.

References

- L. Meshkat & L. Bryant, “Managing the Risk of Command File Errors”, AIAA Aerospace Sciences Meeting, January 2013.
- L. Meshkat, “Probabilistic Risk Assessment for Decision Making during Spacecraft Operations”, Reliability and Maintainability Symposium, January 2009.
- L. Meshkat , A.Girerd , C. Edwards, “An Integrated Approach for the Probabilistic Risk Assessment of the Mars Relay Network “Reliability & Maintainability Symposium” January 2006.
- L. Meshkat, “Probabilistic Risk Assessment for Concurrent, Conceptual Design of Space Missions” AIAA conference –September 2005.