



A Europa Clipper, Integrated Model-Centric Engineering (IMCE), and Safety and Mission Assurance (SMA) partnership

# Model-based Probabilistic Risk Assessments (PRA)

## MBSE Symposium

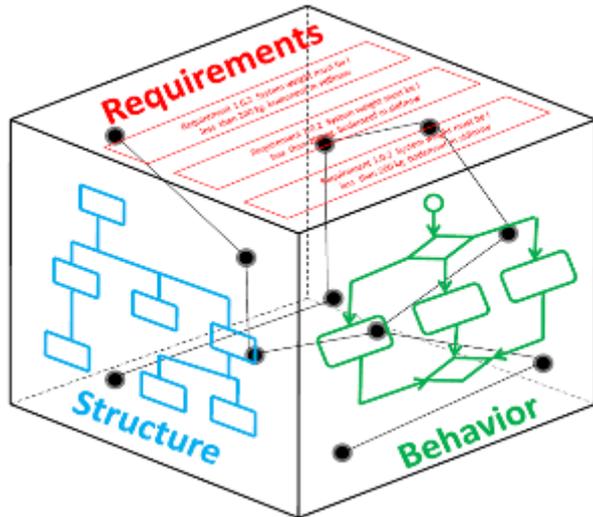
Kelli McCoy, Chet Everline, Josh Bendig

January 24, 2019



**Jet Propulsion Laboratory**  
California Institute of Technology

# What is MRAP? Mission Risk Assessment



System Model



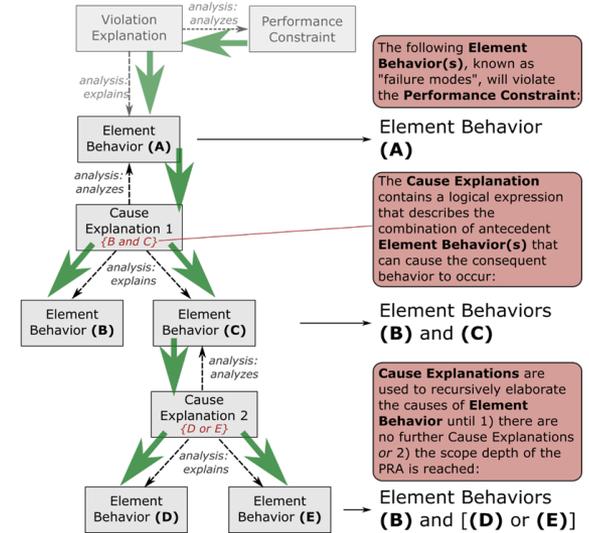
**Violation Explanations** explain how certain **Element Behavior** violates the **Performance Constraint** being analyzed.

**Element Behavior** that violates a **Performance Constraint** is considered a "failure mode".

**Cause Explanations** analyze **Element Behavior(s)** and explain why other **Element Behavior(s)** may cause it.

**Element Behavior** that is not analyzed by a **Cause Explanation** has no identified causes, which classifies it as "basic behavior" (i.e. Element Behavior B).

The PRA methodology recursively traverses through **Cause Explanations** to locate basic **Element Behaviors**. The occurrence of a basic behavior is considered a basic event.



IMCE PRA scripts

The following **Element Behavior(s)**, known as "failure modes", will violate the **Performance Constraint**:

**Element Behavior (A)**

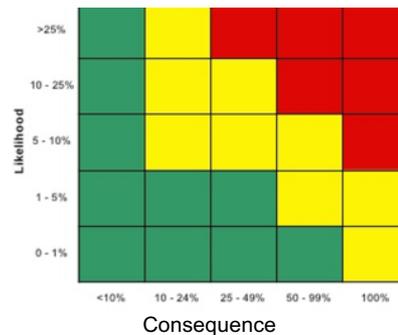
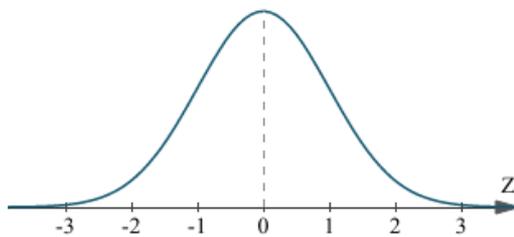
The **Cause Explanation** contains a logical expression that describes the combination of antecedent **Element Behavior(s)** that can cause the consequent behavior to occur:

**Element Behaviors (B) and (C)**

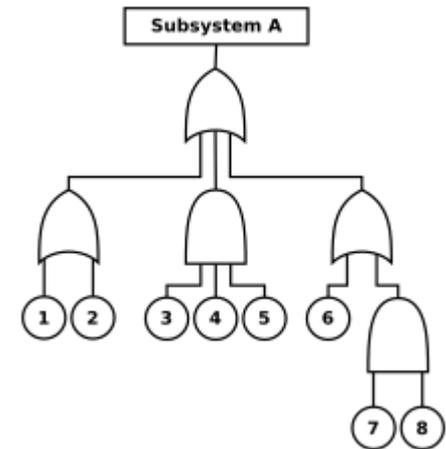
**Cause Explanations** are used to recursively elaborate the causes of **Element Behavior** until 1) there are no further **Cause Explanations** or 2) the scope depth of the PRA is reached:

**Element Behaviors (B) and [(D) or (E)]**

Europa's MBSE infrastructure + IMCE's PRA script development = unique opportunity to pursue a novel approach to performing PRAs



Probabilistic Risk Assessment

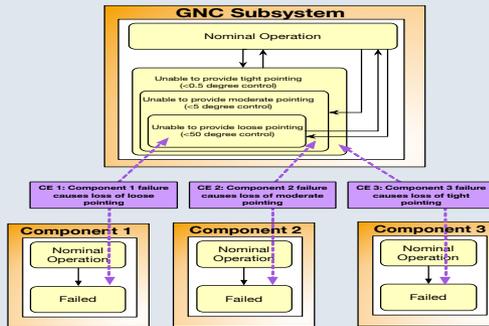


# MBSE PRA Process

Develop foundational capability to perform Probabilistic Risk Assessments (PRAs) from a System Model



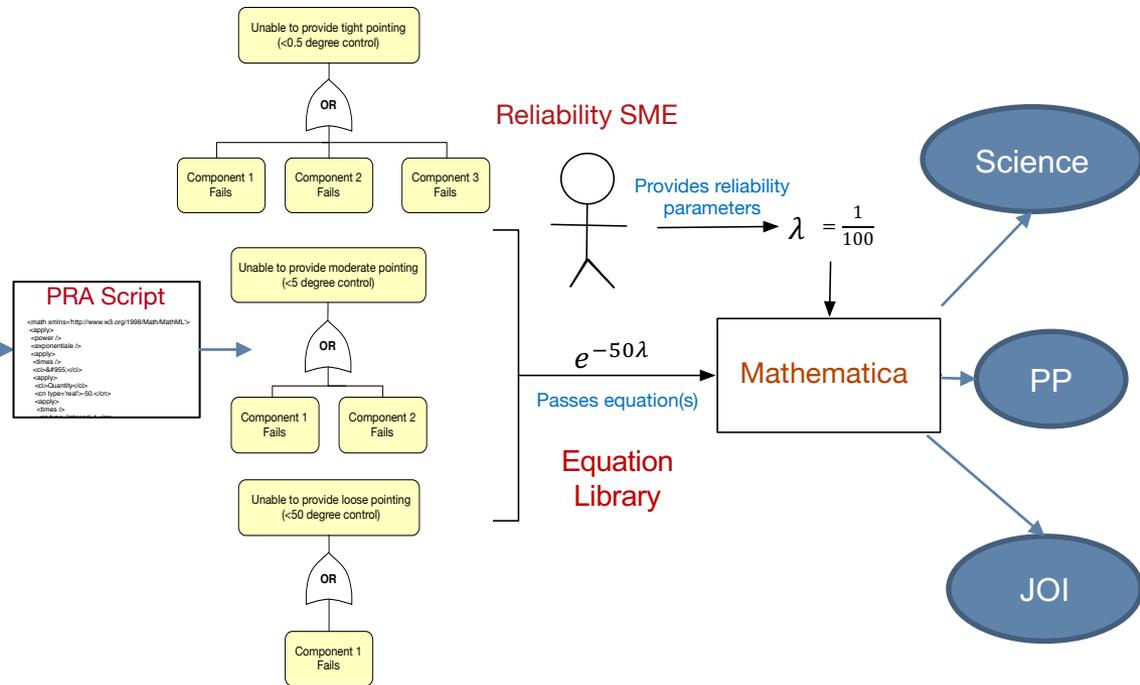
Design Capture Model: causal dependencies, state machine



Box-level modeling now in place

Time Management System: operational

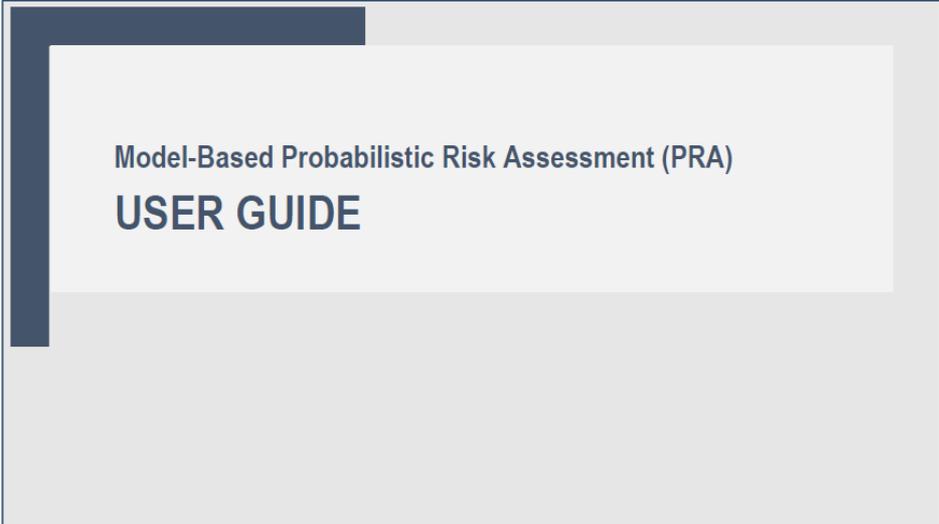
SCET	2024-355T00:00:00	2024-356T00:00:00	2024-357T00:00:00	2024-358T00:00:00	2024-2024-
MissionSubPhase	2024-12-20 00:00:00	2024-12-21 00:00:00	2024-12-22 00:00:00	2024-12-23 00:00:00	Jupiter_Orbit_Ca
GNCMode		EARTH1		INERTIAL	DE
Inertia_Measurement			On_Full_Power		
Inertia_Measurement			On_Full_Power		



The use of a single source of truth ensures a consistent foundation across all PRAs.

# MRAP Documentation

---

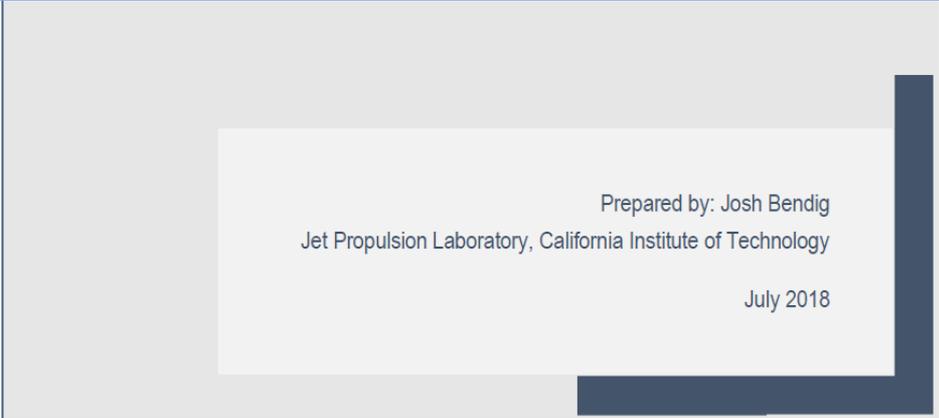


Model-Based Probabilistic Risk Assessment (PRA)  
**USER GUIDE**

Documentation was developed to help other missions implement a similar process

*Additional Public references:*

1. Schreiner, S., et al. "Towards a methodology and tooling for Model-Based Probabilistic Risk Assessment (PRA)." AIAA Space 2016.
2. Castet, J. F., et al., "Fault Management Ontology and Modeling Patterns." AIAA Space 2016. Long Beach, CA, 2016.
3. Castet, J. F., et al. "Ontology and Modeling Patterns for State-Based Behavior Representation," Infotech @ Aerospace, AIAA SciTech, Kissimmee, Florida, 2015.



Prepared by: Josh Bendig  
Jet Propulsion Laboratory, California Institute of Technology

July 2018

# Traditional vs MRAP Approach

## System modeling:

- understanding the system elements to be modeled;
- modeling how failures in these elements (leaf-level events) cause functional failure;
- identifying risk scenarios and modeling their occurrence probability;
- acquiring reliability data.

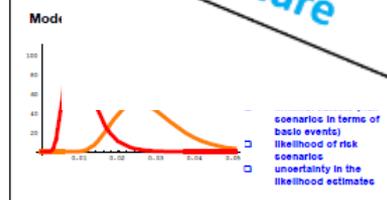
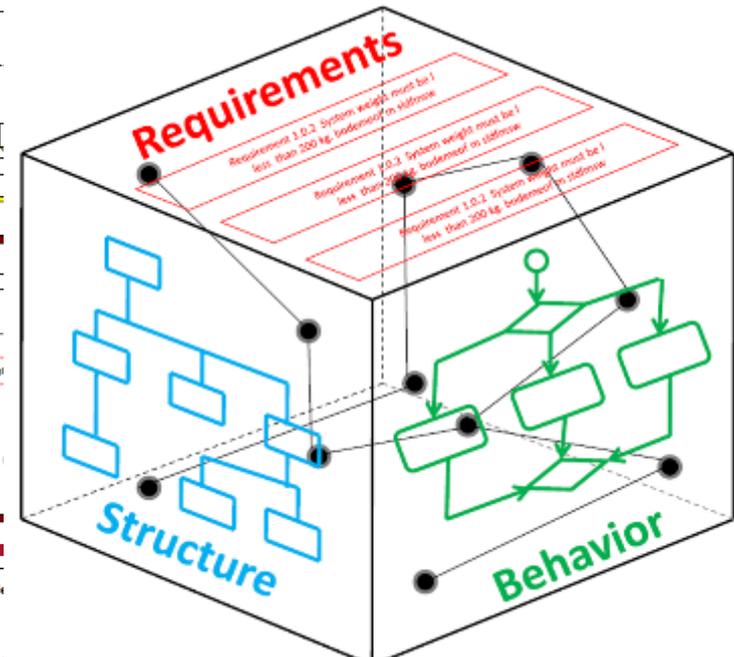
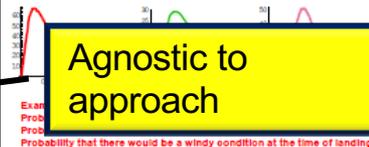
Should already be in the system model.

Added to system model through cause & violation explanations

PRA script and Equation Library

Agnostic to approach

Probabilistic Treatment of Basic Events



- human errors, etc.)
- Insights into how various systems interact
- Tabulation of all the assumptions
- Identification of key parameters that greatly influence the results
- Presenting results of sensitivity studies

Using the MRAP approach, there were roughly 3 PRAs developed (for the Europa Clipper mission) for the cost of 1 PRA, using traditional methods

# **Example Application: Europa Clipper PRAs**

# Europa Clipper PRAs of interest

## Europa System Model/TMS

Hardware  
Requirements  
State transition timelines  
Cause Explanations

PRA  
Scripts

## MRAP

Planetary Protection

Study Outcome:  
Probability of  
Contamination

Performing greater microbial reduction will not improve probability of contamination (increased bioburden reduction decreases reliability)

Science Sensitivity

Study Outcome:  
Probability of Meeting L1  
Science Objectives

A non-driving flyby recovery capability (hours, not min) is needed to preserve science in the presence of expected outages

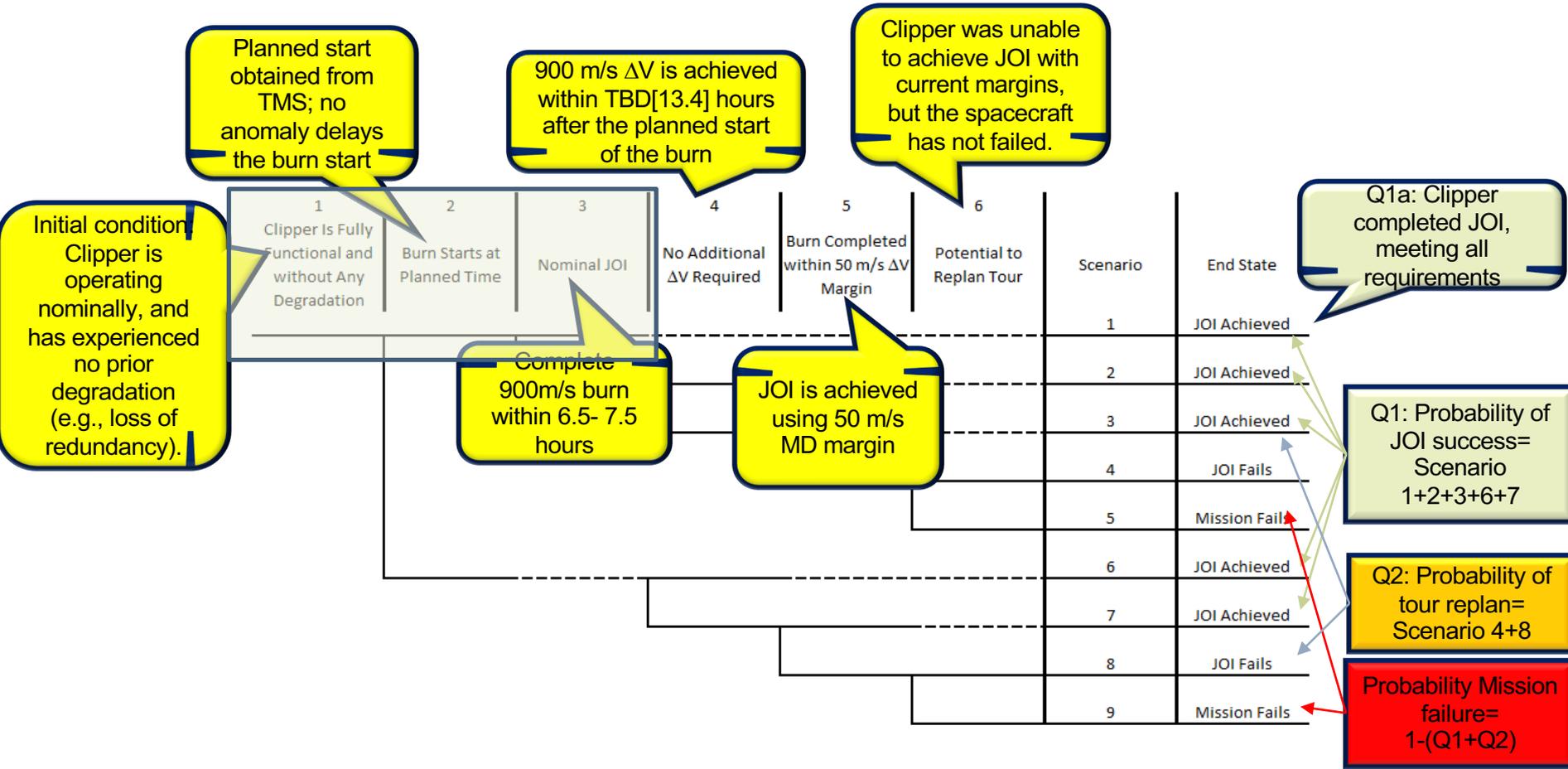
JOI Achievement

Study Outcome:  
Probability of Successful  
JOI

A requirement on the time duration of JOI was unnecessarily confining fault protection recovery strategies during the burn

Notable contribution

# Event Tree Example for JOI



# Question #1a Analysis and Results

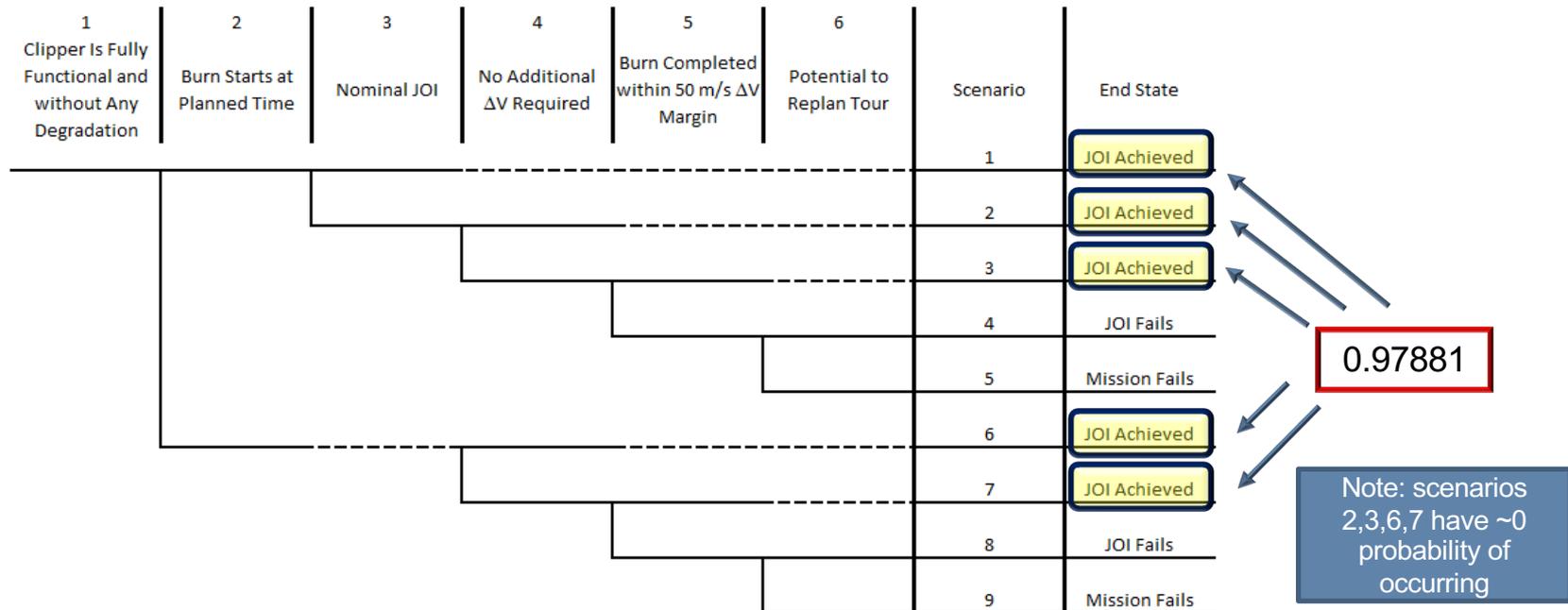
1a. What is the JOI success probability, adhering to all Project RQs (nominal JOI execution)?

1 Clipper Is Fully Functional and without Any Degradation	2 Burn Starts at Planned Time	3 Nominal JOI	4 No Additional $\Delta V$ Required	5 Burn Completed within 50 m/s $\Delta V$ Margin	6 Potential to Replan Tour	Scenario	End State
						1	JOI Achieved
						2	JOI Achieved
						3	JOI Achieved
						4	JOI Fails
						5	Mission Fails
						6	JOI Achieved
						7	JOI Achieved
						8	JOI Fails
						9	Mission Fails

0.97881

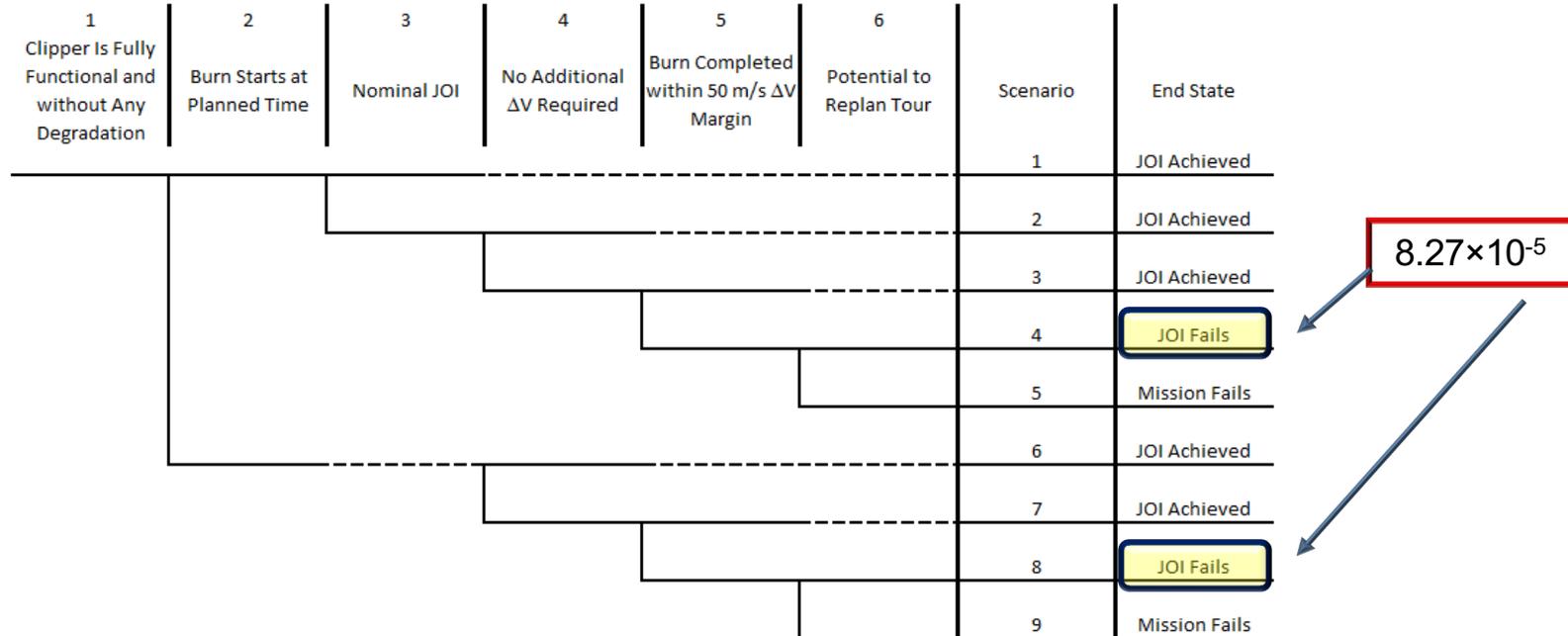
# Question #1 Analysis and Results

## 1. What is the JOI success probability?

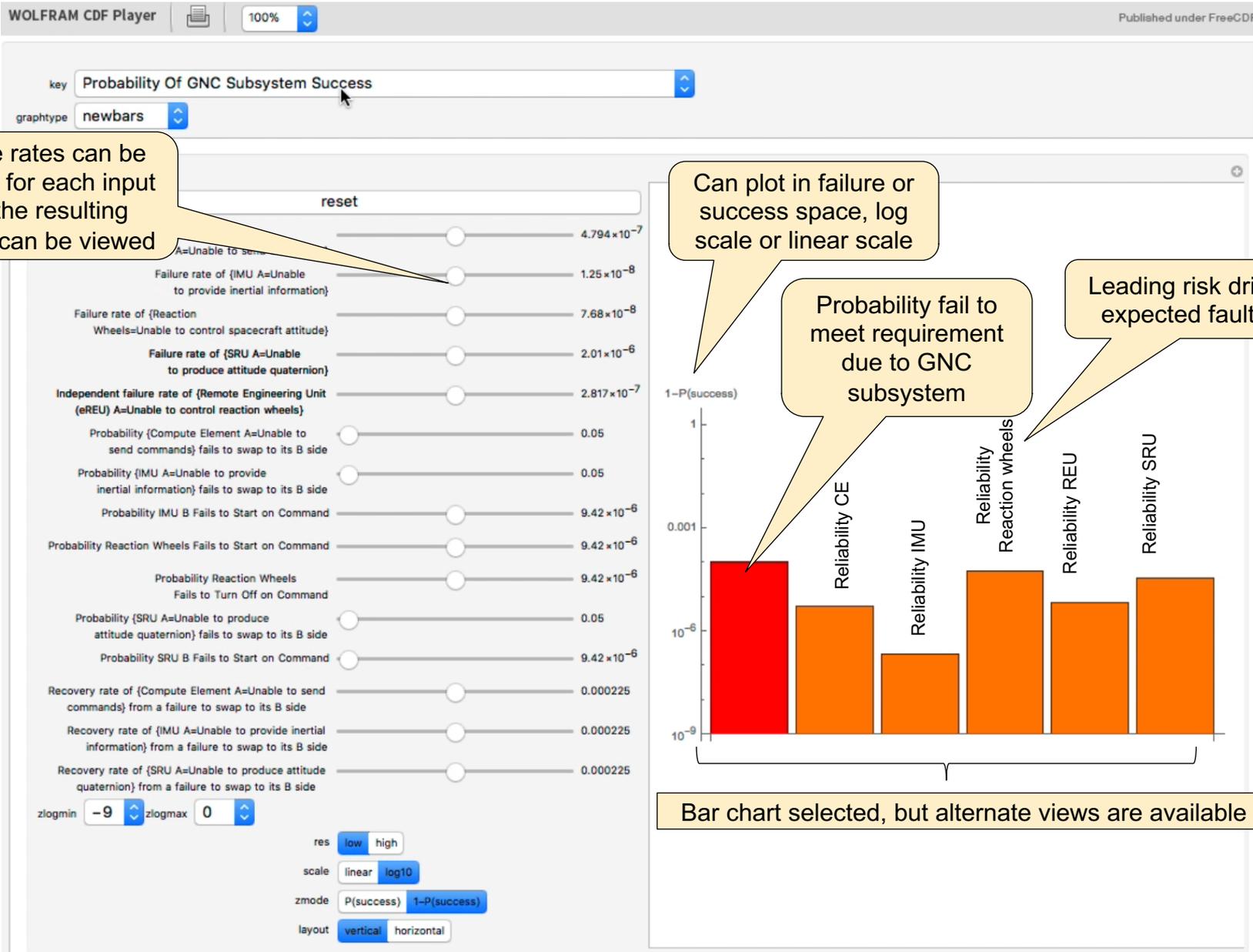


# Question #2 Analysis and Results

2. What is the probability a tour redesign is required (i.e. trajectory margin of 50m/s delta-V is exceeded in JOI)?



# Result Analysis: Assessing Drivers of Unreliability

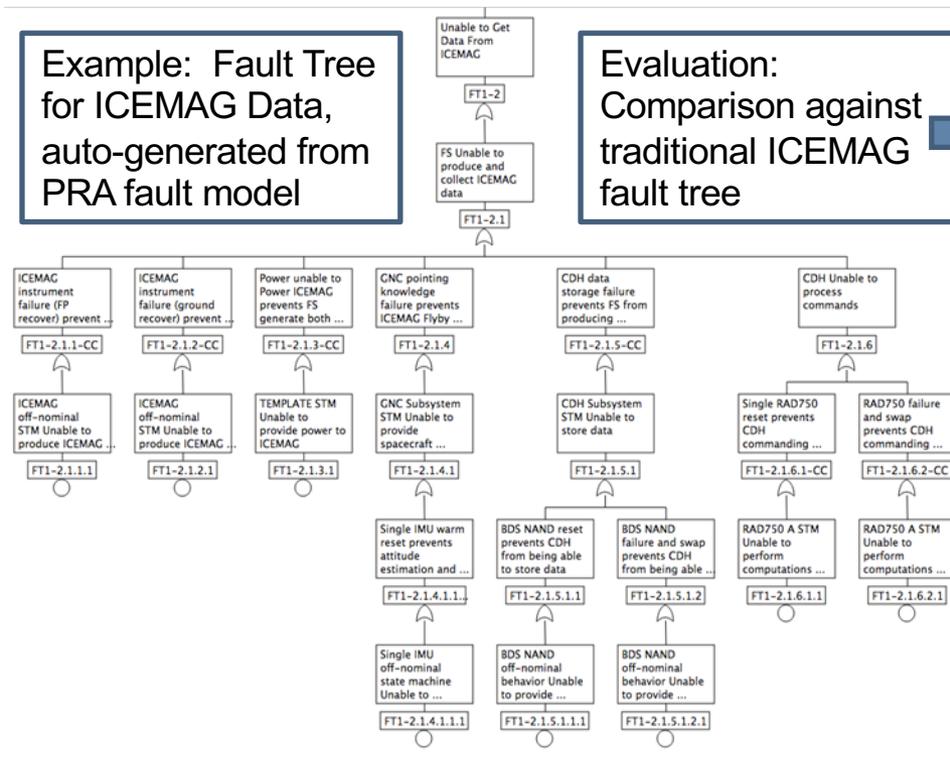


# Visualization and Validation

Graphical visualization tools are used to validate results

Example: Fault Tree for ICEMAG Data, auto-generated from PRA fault model

Evaluation: Comparison against traditional ICEMAG fault tree



Proper FTA Node	Addressed in PRA	PRA Node ID	Notes
Failure to acquire valid data from ICEMAG	Yes	FT1.2	Head node
ICEMAG provides no data	Rolled up	(FT1.2)	Part of head node
ICEMAG is broken	Yes	FT1.2.1.1	Distinct node
Science path is broken or stuck	Rolled up	(FT1.2.1.1)	Part of ICEMAG is broken
Data path is broken or stuck	Rolled up	(FT1.2.1.1)	Part of ICEMAG is broken
ICEMAG is not powered	Covered		Only switch faults are modeled
Spacecraft power fault	Handled in safing		s/c wide power faults are assumed to trigger safing
ICEMAG circuit is not energized	Yes	FT1.2.1.3	Distinct node
ICEMAG command is not executed	Covered		
ICEMAG fails to respond to command	Yes	TX	Transition failure is modeled explicitly
ICEMAG data path is damaged	Rolled up	(FT1.2.1.1)	Part of ICEMAG is broken
ICEMAG is latched	Rolled up	TX	Part of transition failure
CB&DH fails to emit correct command	Covered		
CB&DH causes safing	Handled in safing		
CB&DH is in reset or swap	Yes	FT1.2.1.6.1, FT1.2.1.6.2	double fault etc assumed to trigger safing
CB&DH is otherwise functional but cannot emit commands	Rolled up	(FT1.2.1.6.1, FT1.2.1.6.2)	Distinct nodes
Execution Engine is stuck or in reset	Rolled up	(FT1.2.1.6.1, FT1.2.1.6.2)	"Other" CB&DH fault rate rolled into reset / swap rates
Execution Engine has a bad sequence	Rolled up	(FT1.2.1.6.1, FT1.2.1.6.2)	
Sequence itself is bad	No	(FT1.2.1.6.1, FT1.2.1.6.2)	Command faults should be treated separately
ART sequence is bad	No	(FT1.2.1.6.1, FT1.2.1.6.2)	Probably roll up into command faults when available
ICEMAG provides bad data	Rolled up	(FT1.2)	Part of head node
Science path is broken or stuck	Rolled up	(FT1.2.1.1)	Part of ICEMAG is broken
ICEMAG is cold	Rolled up	(FT1.2.1.1)	Part of ICEMAG is broken
Thrusters are firing	Covered		
Spontaneous firing	Not credible		Assumed unplanned thruster firing can only result from safing
GNC in an RCS mode	Handled in safing		
Electrical power / EMI	Covered		
Spacecraft fails to provide clean power	Rolled up	FT1.2.1.3	Part of ICEMAG circuit is not energized
ICEMAG short	Rolled up	(FT1.2.1.1)	Part of ICEMAG is broken
Propulsion module EMI	No	(FT1.2.1.1)	Very tricky to estimate
Other EMI	No	(FT1.2.1.1)	Very tricky to estimate
ICEMAG sends data at unexpected rate	Rolled up	(FT1.2.1.1)	Part of ICEMAG is broken
ICEMAG command not executed [see above]	Covered		
ICEMAG pointing is unknown	Yes	FT1.2.1.4	Distinct node
GNC data not provided	No		Intercom rolled into CB&DH failures
Intercom broken	No		Intercom rolled into CB&DH failures
GNC unpowered or resetting	No		General GNC failure rolled into CB&DH failures
GNC estimates invalid or missing	Yes	FT1.2.1.4.1	Distinct node
GNC sensors broken	Yes	FT1.2.1.4.1.1	Distinct node
GNC estimator broken	No		Difficult to model - "All Other GNC Fault" node temporarily removed
ICEMAG data not transferred to Spacecraft	Rolled up	(FT1.2)	Focused on BDS story
ICEMAG data path broken	Rolled up	(FT1.2.1.1)	Part of ICEMAG is broken
Intercom broken	No		Intercom rolled into CB&DH failures
BDS failure	Yes	FT1.2.1.5	Distinct node
BDS unable to handle data rate	No		Roll into command failure?
BDS unable to receive any data	Yes	FT1.2.1.5.1	Distinct node
BDS unpowered	No		Roll into command failure?
BDS is full	No		Roll into command failure?
BDS is broken	Covered		
BDS NAND is broken	Yes	FT1.2.1.5.1.1, FT1.2.1.5.1.2	Distinct nodes
BDS Controller is broken	No		Roll into command failure?

Auto-generated vs. Manually Generated fault tree of PRA model

# Summary, Observations, and Lessons Learned

---

- **Every detail of system cannot be modeled**
  - Model things conservatively first; if result favorable, stop!
  - Else, target high-risk areas for detailed exploration
- **Stop at box level unless specific Project question arises driving lower-level modeling**
  - Reliability information often not available at lower levels
- **Use visualization to help validate that the system model is correct**
- **Always iterate modeling, findings, and results with subject matter experts prior to delivery**
- **Always verify MRAP scripts and architecture after each revision.**

# Back-up material

---

# Result Analysis: Assessing Drivers of Unreliability

key Probability Of GNC Subsystem Success

graphtype newbars

Failure rates set to lowest setting

reset

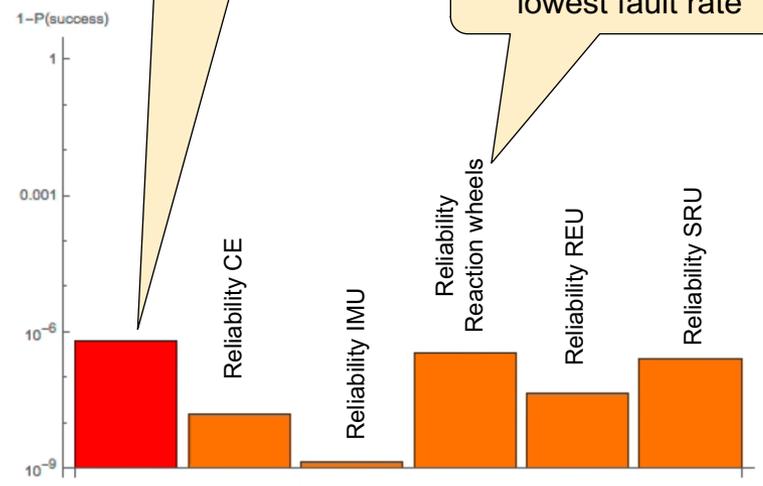
- Failure rate of {Compute Element A=Unable to send commands}  $3.16228 \times 10^{-10}$
- Failure rate of {IMU A=Unable to provide inertial information}  $1. \times 10^{-10}$
- Failure rate of {Reaction Wheels=Unable to control spacecraft attitude}  $5.62341 \times 10^{-8}$
- Failure rate of {SRU A=Unable to produce attitude quaternion}  $1.77828 \times 10^{-9}$
- Independent failure rate of {Remote Engineering Unit (eREU) A=Unable to control reaction wheels}  $1.77828 \times 10^{-9}$
- Probability {Compute Element A=Unable to send commands} fails to swap to its B side 0.05
- Probability {IMU A=Unable to provide inertial information} fails to swap to its B side 0.05
- Probability IMU B Fails to Start on Command  $5.62341 \times 10^{-8}$
- Probability Reaction Wheels Fails to Start on Command  $5.62341 \times 10^{-8}$
- Probability Reaction Wheels Fails to Turn Off on Command  $5.62341 \times 10^{-8}$
- Probability {SRU A=Unable to produce attitude quaternion} fails to swap to its B side 0.05
- Probability SRU B Fails to Start on Command  $9.42 \times 10^{-6}$
- Recovery rate of {Compute Element A=Unable to send commands} from a failure to swap to its B side 0.0316228
- Recovery rate of {IMU A=Unable to provide inertial information} from a failure to swap to its B side 0.0316228
- Recovery rate of {SRU A=Unable to produce attitude quaternion} from a failure to swap to its B side 0.0316228

zlogmin -9 zlogmax 0

res low high  
 scale linear log10  
 zmode P(success) 1-P(success)  
 layout vertical horizontal

Probability fail to meet requirement due to GNC subsystem

Leading risk driver at lowest fault rate



# Result Analysis: Assessing Drivers of Unreliability

WOLFRAM CDF Player



100%

Published under FreeCDF™

key Probability Of GNC Subsystem Success

graphtype newbars

Failure rates set to highest setting

reset

Failure rate of {Compute Element A=Unable to send commands} 0.0000562341

Failure rate of {IMU A=Unable to provide inertial information}  $1.77828 \times 10^{-6}$

Failure rate of {Reaction Wheels=Unable to control spacecraft attitude} 0.00001

Failure rate of {SRU A=Unable to produce attitude quaternion} 0.000316228

Independent failure rate of {Remote Engineering Unit (eREU) A=Unable to control reaction wheels} 0.0000316228

Probability {Compute Element A=Unable to send commands} fails to swap to its B side 0.05

Probability {IMU A=Unable to provide inertial information} fails to swap to its B side 0.05

Probability IMU B Fails to Start on Command  $9.42 \times 10^{-6}$

Probability Reaction Wheels Fails to Start on Command  $9.42 \times 10^{-6}$

Probability Reaction Wheels Fails to Turn Off on Command  $9.42 \times 10^{-6}$

Probability {SRU A=Unable to produce attitude quaternion} fails to swap to its B side 0.05

Probability SRU B Fails to Start on Command  $9.42 \times 10^{-6}$

Recovery rate of {Compute Element A=Unable to send commands} from a failure to swap to its B side 0.000225

Recovery rate of {IMU A=Unable to provide inertial information} from a failure to swap to its B side 0.000225

Recovery rate of {SRU A=Unable to produce attitude quaternion} from a failure to swap to its B side 0.000225

zlogmin -9 zlogmax 0

res low high

scale linear log10

zmode P(success) 1-P(success)

layout vertical horizontal

Probability fail to meet requirement due to GNC subsystem

Leading risk driver at highest fault rate

