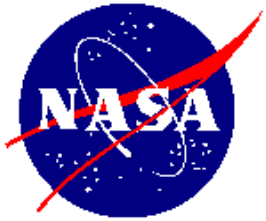




# Risk Management Tools

**Langley Research Center  
May 2, 2000**

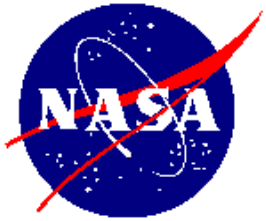
**Michael A. Greenfield  
Deputy Associate Administrator  
Office of Safety and Mission Assurance**



## Recent Reviews Focusing on NASA Failures

---

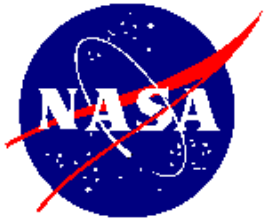
- **Mars Climate Orbiter Mishap Investigation (MCO)**
  - **Chair: Art Stephenson/MSFC**
- **NASA FBC (Faster, Better, Cheaper) Task (FBC)**
  - **Chair: Tony Spears**
- **Shuttle Independent Assessment (SIA)**
  - **Chair: Dr. Henry McDonald**
- **Mars Program Independent Assessment (MPIA)**
  - **Chair: Tom Young**



## Recommendations: Risk Management Deficiencies

---

- Overall there are about 175 recommendations
- Most addressed issues applicable throughout the Agency, at all Centers and all Projects!
- Findings were grouped into 4 large areas: People, Process, Process Execution, Advanced Tools and Techniques
- Risk and Risk Management issues represent a continuing theme
  - Weakness in Risk Identification and Analysis
  - Poor Risk Mitigation and Tracking
  - Lack of strong Systems Engineering
  - Limited application of Risk Assessment tools
- NASA has formed an Integrated Action Team (NIAT) to develop suitable plans to correct the deficiencies
- Briefing to NASA Chief Engineer on June 15.



## Outline

---

- **Continuous Risk Management Process**
- **NASA Risk Management Requirements**
- **Fault Tree Analysis (FTA)**
- **Failure Mode And Effect Analysis (FMEA)**
- **Probabilistic Risk Assessment (PRA)**



# Continuous Risk Management Process

---

- **Risk management is a continuous process which:**
  - Identifies risk
  - Analyzes risk and its impact, and prioritizes risk
  - Develops and implements risk mitigation or acceptance
  - Tracks risks and risk mitigation implementation plans
  - Assures risk information is communicated to all project/program levels
- **Risk management planning**
  - Developed during the program/project formulation phase
  - Included in the program/project plans
  - Executed/maintained during the implementation phase
- **Risk management responsibility**
  - Program/project manager has the overall responsibility for the Implementation of risk management, ensuring an integrated, coherent risk management approach throughout the project



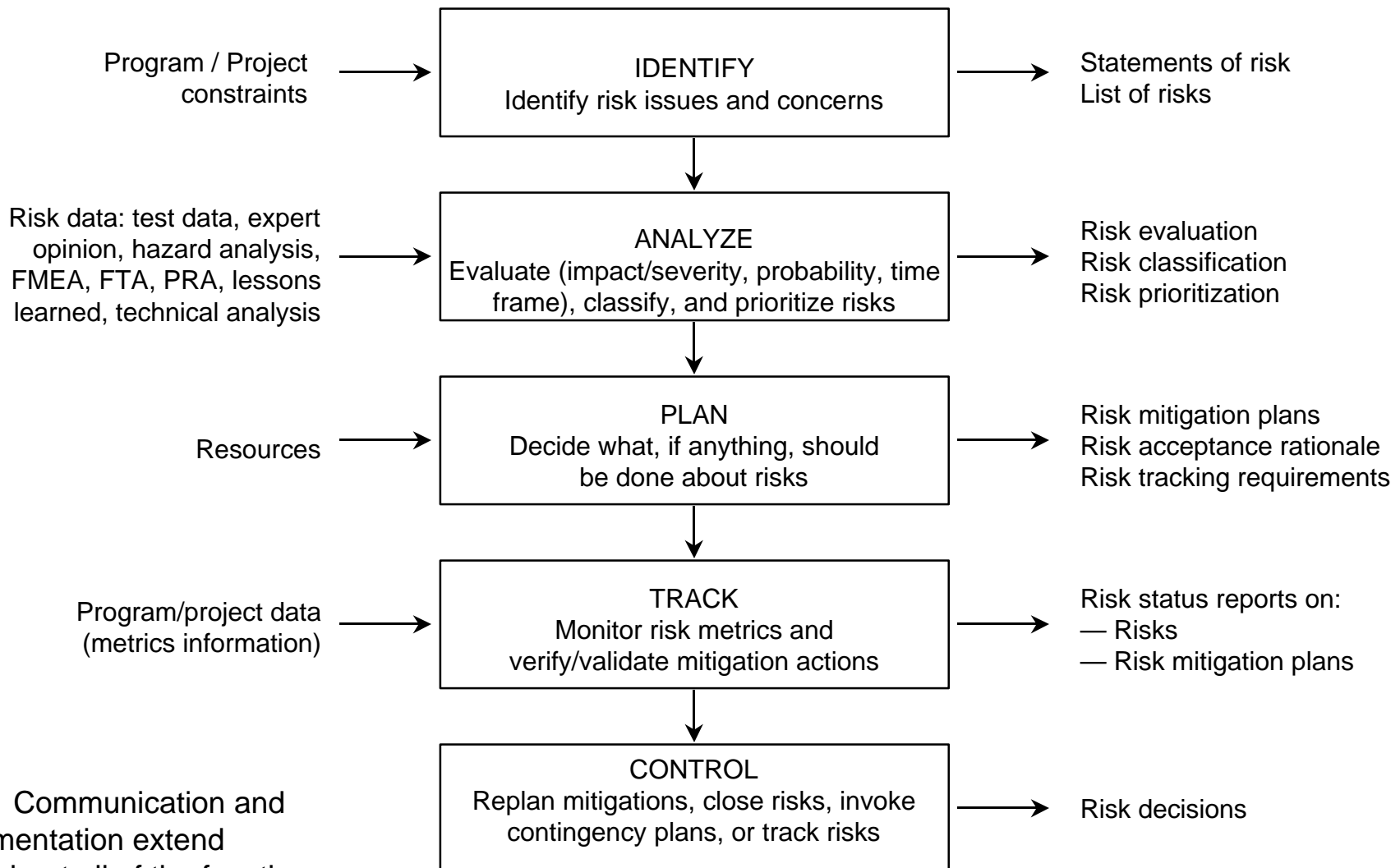
# NASA Risk Management Requirements

---

- **NPG 7120.5, NASA Program and Project Management Processes and Requirements**
  - The program or project manager shall apply risk management principles as a decision-making tool which enables programmatic and technical success
  - Program and project decisions shall be made on the basis of an orderly risk management effort
  - Risk management includes identification, assessment, mitigation, and disposition of risk throughout the PAPAC (Provide Aerospace Products And Capabilities) process
- **NPG 8705.x (draft), Risk Management Procedures and Guidelines**
  - Provides additional information for applying risk management as required by NPG 7120.5



# Risk Management Process





# NASA Risk Management Requirements

---

- **NPG 8715.3, NASA Safety Manual**
  - Purpose of risk assessment is to identify and evaluate risks to support decision-making regarding actions to ensure safety and mission assurance
  - Risk assessment analyses should use the simplest methods that adequately characterize the probability and severity of undesired events
  - Qualitative methods that characterize hazards and failure modes and effects should be used first
  - Quantitative methods are to be used when qualitative methods do not provide an adequate understanding of failures, consequences, and events
  - System safety analysis must include early interaction with project engineering, integration, and operations functions to ensure all hazards are identified
  - The hazard assessment process is a principle factor in the understanding and management of technical risk
  - As part of the responsibility for overall risk management, the program/project manager must ensure that system safety analyses, appropriate to the program/project complexity, have been conducted

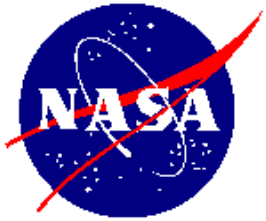




# NASA Risk Management Requirements

---

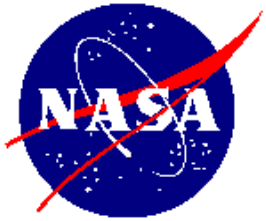
- **NSTS 22206, instructions for preparation of FMEA and CIL [for Space Shuttle]**
  - System and performance requirements are defined
  - Analysis assumptions and groundrules are specified
  - Block diagrams (functional or reliability) are developed
  - Analysis worksheets which include identification of every failure mode are developed (the effects documented address the worst case.)
  - Corrective actions and design improvements are evaluated and recommended
  - Analysis is summarized in report form
- **SSP 30234, instructions for preparation of FMEA and CIL [for Space Station]**
  - FMEA process, requirements, rules, reporting requirements are described
  - CIL process, requirements, rules, reporting requirements are described
  - Ground support equipment FMEA and CIL processes, requirements, approvals, and databases are described



## Risk Management Tools

---

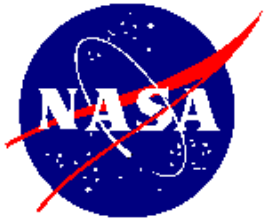
- NASA has been traditionally using one Risk Assessment and Risk Management (RA/RM) tool for some time:  
*Failure Modes and Effects Analysis (FMEA)*
- NASA has also selectively used another important RA/RM tool:  
*Fault Tree Analysis (FTA)*
- Additionally, NASA has been broadening its repertoire of RA/RM tools and has begun to systematically use a more comprehensive set of tools collectively called  
*Probabilistic Risk Assessment (PRA)*
- PRA is a systematic, logical, and comprehensive discipline that uses tools like FMEA, FTA, Event Tree Analysis (ETA), Event Sequence Diagrams (ESD), Master Logic Diagrams (MLD), Reliability Block Diagrams (RBD), etc., to quantify risk.



# Risk Management Tools

---

**An Introduction (to whet your appetite)**



## Design/Develop a Car for the Interstate 64 Commute

---

- **Start with requirements analysis**
  - **Must be safe**
  - **Must provide seating for two persons to allow HOV option**
  - **High price of fuel dictates need for high gas mileage**
  - ***High reliability to protect against being stranded***
  - **And of course must be stylish**
  
- **Apply a disciplined risk management process to uncover risks and develop risk mitigation strategies across the product lifecycle**



# Fault Tree Analysis

---

- **Background**
  - **FTA is a deductive analytical technique of reliability and safety analyses and generally is used for complex dynamic systems**
  - **FTA provides an objective basis for analysis and justification for changes and additions**
  - **First developed by Bell Telephone in 1961 then modified by Boeing for wide uses**

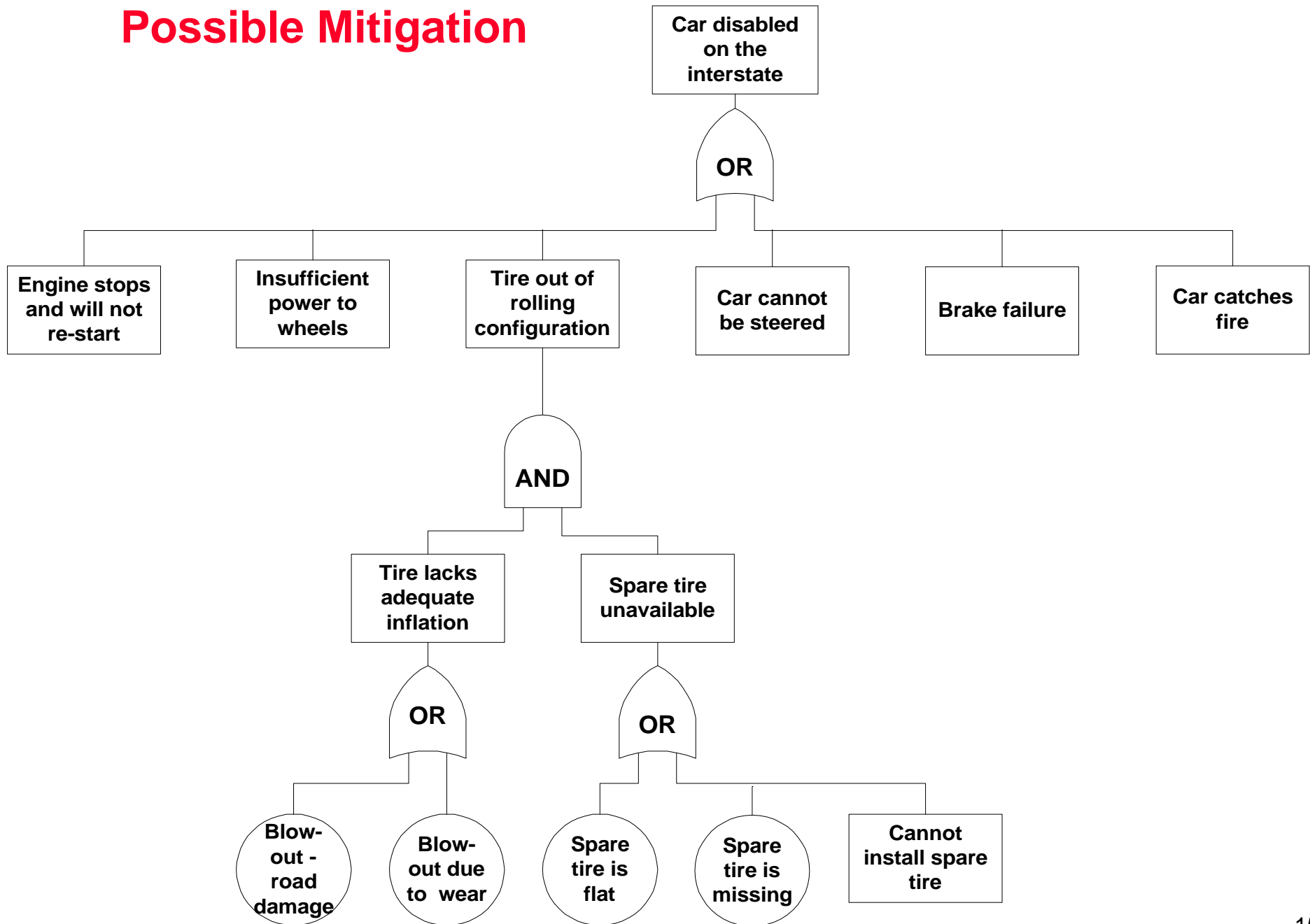


# Fault Tree Analysis

---

- **Concept**
  - A model that logically and graphically represents the various combinations of possible events, both faulty and normal, occurring in a system that leads to the top undesired event, e.g., electrical fire in heater box.
  - FTA uses a tree to show the cause-and-effect relationships between a single, undesired event (failure) and the various contributing causes
  - The tree shows the logical branches from a single failure at the top of the tree to the root cause(s) at the bottom of the tree
  - Standard logic symbols connect the branches of the tree. For example, “gates” permit or inhibit the passage of fault logic up the tree through the “events.”
  - Fault tree does not necessarily contain all possible failure modes of the components of the system. Fault tree contains only those failure modes whose existence contribute to the existence of the top event.

# FTA Provides a Top-Down View to Identify Risks and Possible Mitigation





## Failure Mode and Effect Analysis

---

- **FMEA is an inductive engineering technique used at the component level to define, identify, and eliminate known and/or potential failures, problems, and errors from the system, design, process, and/or service before they reach the customer. (Also see MIL-STD-1629)**
- **FMEA is an early warning or preventative technique that is methodical**
  - **Systematic method of examining all ways which a failure can occur**
  - **For each failure, an estimate is made of:**
    - **Effect on total system**
    - **Occurrence**
    - **Severity**
    - **Detection**
  - **Bottoms-up analysis based on historical or inferential data at component level**
- **FMEA will identify corrections required to prevent failures**





## Failure Mode and Effect Analysis

---

- **Example**

**“For want of a nail, the shoe was lost;  
For want of a shoe, the horse was lost;  
For want of a horse, the rider was lost;  
For want of a rider, the battle was lost;  
For want of a battle, the kingdom was lost!”**

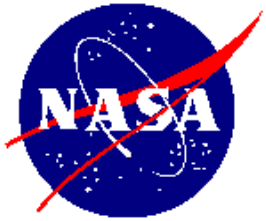
**How would you control the loss of a nail?  
Is there more you can do?**

# FMECA- A Bottoms-Up View to Design, Manufacture, Operations

## Tire FMECA with Reevaluation of Risks

Part Name/ Part Number	Potential Failure Modes	Causes (failure mechanism)	Effects	Risk Priority Rating				Recommended Corrective Action	Improved Rating			
				Sev*	Freq	Det	RPN		Sev*	Freq	Det	RPN
Cord	Fiber separation	1. Weak precursor material	Ply failure	4	3	8	96	Incoming inspection	4	1	8	3
		2. Handling damage	Ply failure	4	3	8	96	Increase process controls during mfg	4	2	2	16
		3. Cumulative fatigue	Ply failure	4	2	8	64	Monitor tire life	4	2	2	16
Ply	Delamination	1. Dirt or grease	Loss of side wall integrity	7	3	8	168	Toluene wipe down during layup	7	1	1	7
		2. Twisted plies	Loss of side wall integrity	7	2	6	84	Automatic ply alignment	7	1	1	7
		3. Poor bond pressure	Loss of side wall integrity	7	2	8	144	Redundant tensioning system	7	1	1	7
Carcass	Disintegration	1. Poor tire alignment	Vehicle loss	9	2	9	162	Planned periodic maintenance	9	1	1	9
		2. Tire hits curb	Vehicle loss	9	2	9	162	Driver training	9	1	1	9

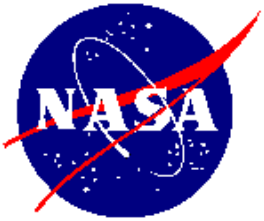
\*Severity ratings 8 to 10 request special effort in design improvement regardless of RPN rating



# Probabilistic Risk Assessment

---

- What is PRA?
  - It is an analysis of the probability (or frequency) of occurrence of a consequence of interest, and the magnitude of that consequence, including assessment and display of uncertainties
  - It is an engineering process, based on comprehensive systems analysis with analytical support, repeated periodically as the design matures and new data become available
  - It is a means to express quantitatively *our state of knowledge* about the risk of failure
  - It does not guess failure rates, or otherwise create data



# Probabilistic Risk Assessment

---

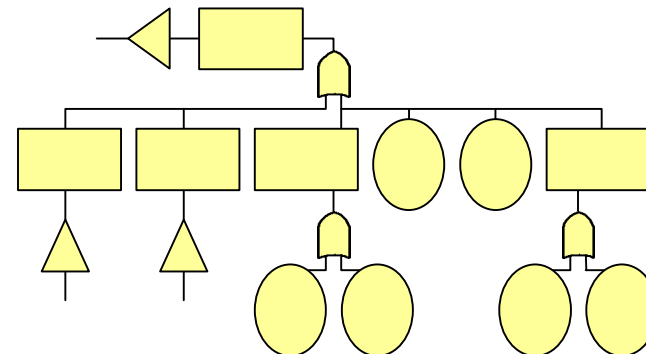
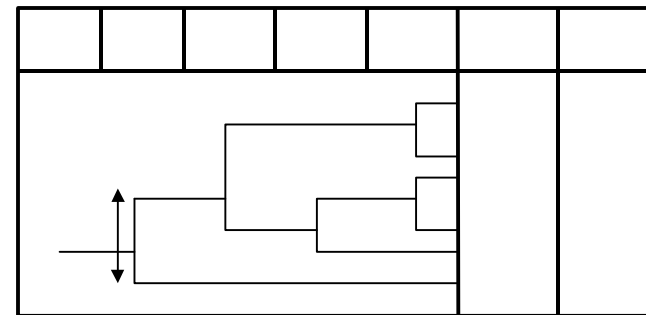
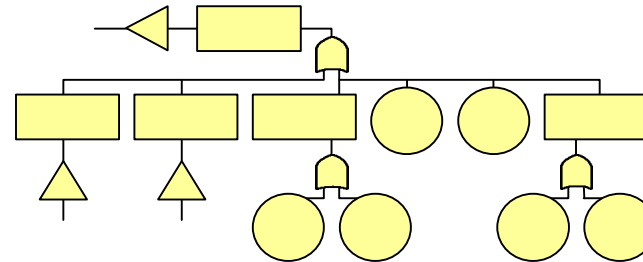
→ What is PRA used for in NASA programs?

- For strategic decision support; e.g., What is the probability of successfully assembling the multi-billion dollar International Space Station?
- For systems under development, to guide trade-offs between safety, reliability, cost, performance, and other tradable resources
- For mature systems, to support decision-making on risk acceptability, and (when risk is considered to be too high) on choices among options for risk reduction; e.g., Space Shuttle upgrades
- To track risk levels:
  - Throughout the life cycle
  - To measure effectiveness of risk reduction options



# Probabilistic Risk Assessment Helps Prioritize Risk Scenarios

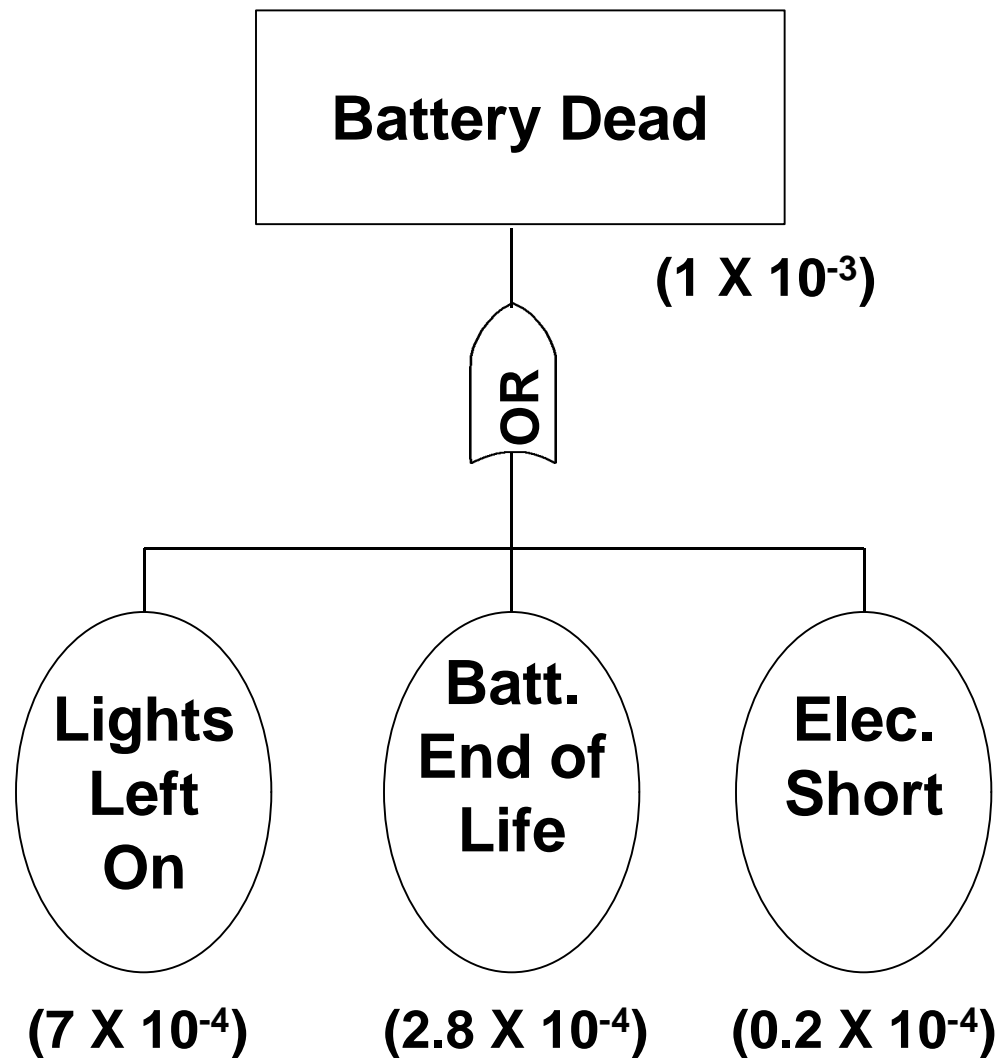
- **Master Logic Diagrams**
  - To identify initiating events
- **Event Trees or Event Sequence Diagram**
  - To construct accident scenarios from initiating events to end states
- **Fault Trees**
  - To quantify initiating and mitigating events



## PRA Supports Design Decisions

	Ordinary tire stays inflated	Changing tools are OK	Spare tire is OK	END STATES (S=success; F=failure)
Tire rolls over road hazard	0.05			S=0.05
	0.95			S=0.40
		0.8	0.6 0.4	F=0.30
		0.2		F=0.19
				<b>S=52%</b> <b>F=48%</b>
	Run-flat Tire Stays Inflated	Changing tools are OK	Spare tire is OK	
Tire rolls over road hazard	0.9			S=0.90
	0.1			S=0.05
		0.8	0.6 0.4	F=0.03
		0.2		F=0.02
				<b>S=96.5%</b> <b>F=3.5%</b>

## Another Risk - A Dead Battery



# PRA Can Provide Quantitative Values for Failure and Facilitate Ranking of Risk Drivers

	Jumper Cables Available	Donor Batt. OK	Batt. Terminals OK	
Batt. Dead (1 X 10 <sup>-3</sup> )*	0.1	0.5	0.8	Can recover (4 X 10 <sup>-5</sup> )
			0.2	Stuck (1 X 10 <sup>-5</sup> )
		0.5		Stuck (5 X 10 <sup>-5</sup> )
	0.9			Stuck (90 X 10 <sup>-5</sup> )

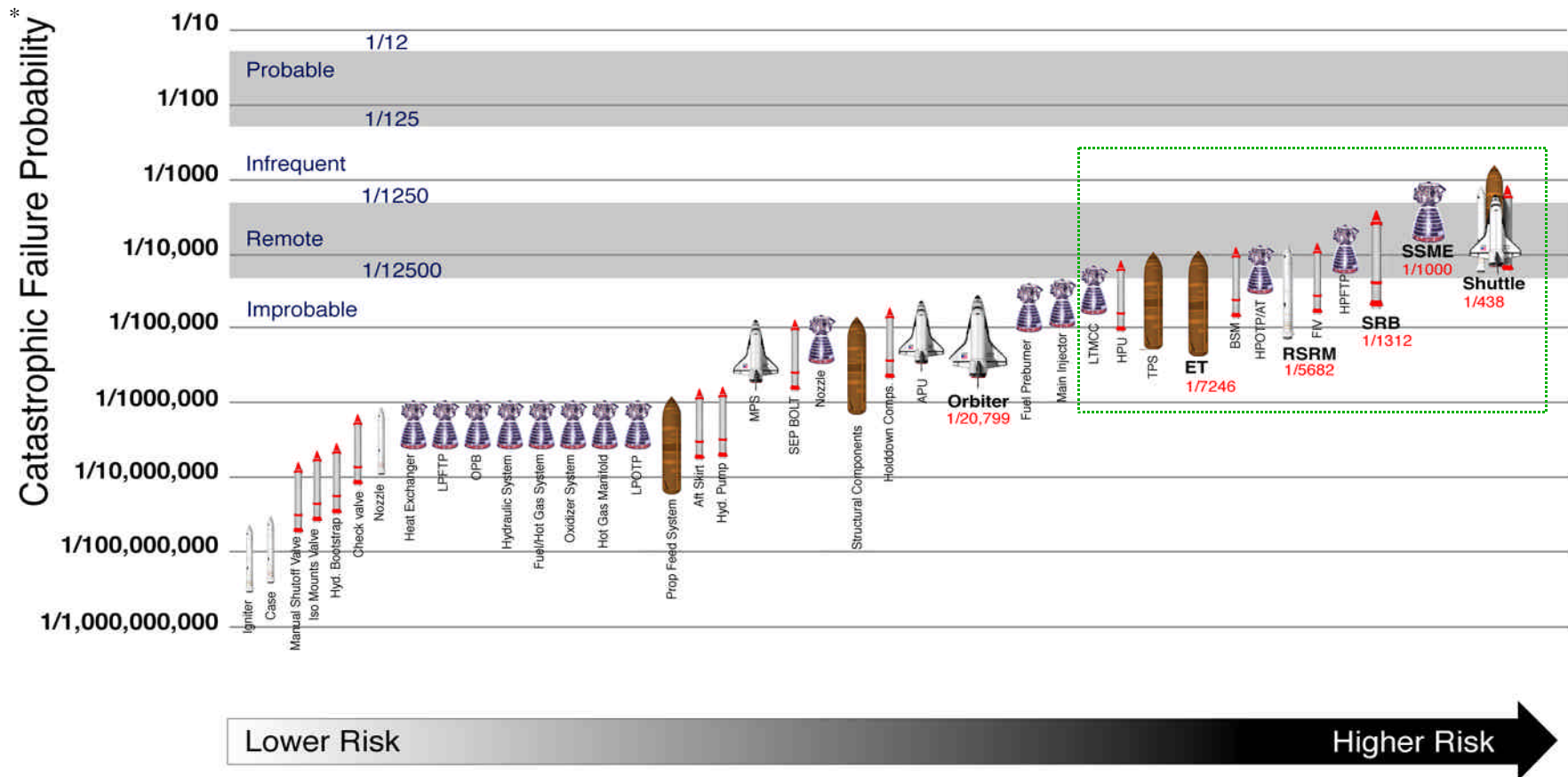
\* Probabilities expressed in terms of a single automobile use.





# Space Shuttle Program Development Office

## Block IIA Configuration - Ascent



\* Based on 1998 QRAS

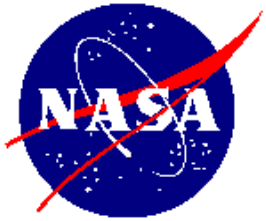


# Space Shuttle Program Development Office

## Reliability Sensitivities Analysis - Space Shuttle Ascent

Shuttle Element	Current Reliability **		What ifs ?		
	Element	Shuttle	Element Risk is Cut in 1/2		Element Reliability is Perfect
			Element	Shuttle	Shuttle
SSME	1.0x10-03* 1/1000	1/438	5.0x10-4 1/2000	→ 1/560	1/779
SRB	7.6x10-04 1/1312		3.8x10-4 1/2624	→ 1/525	1/657
RSRM	1.8x10-04 1/5682		8.8x10-5 1/11,364	→ 1/455	1/474
ET	1.4x10-04 1/7246		6.5x10-5 1/4,492	→ 1/451	1/466
Orbiter	4.8x10-05 1/20,619		2.4x10-5 1/41,238	→ 1/441	1/447

\* Based on SSME Block IIA Configuration  
 \*\* Based on 1998 QRAS



## The SMA Community is Ready to Help

---

- Risk Management tools and techniques continues to be a major thrust within OSMA
- We have enhanced our ability to support Quantitative Risk Assessment
- A recognized expert, Dr. Michael Stamatelatos, has joined our staff to support this effort (202-358-1668)
- Contact Bert Garrido, LaRC SMA Director, X4-3361 or Dr. Peter Rutledge (202-358-0579) or Michael to help you in tool application