Probabilistic Risk Assessment (PRA): Analytical Process for Recognizing Design and Operational Risks

Prepared by

Roger L. Boyer, CRE

Chief, Risk & Reliability Analysis Branch

NASA Johnson Space Center
Safety & Mission Assurance (S&MA)

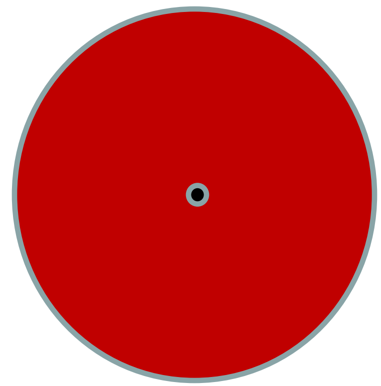
Prepared for

BSEE PRA Industry Day

March 1, 2018

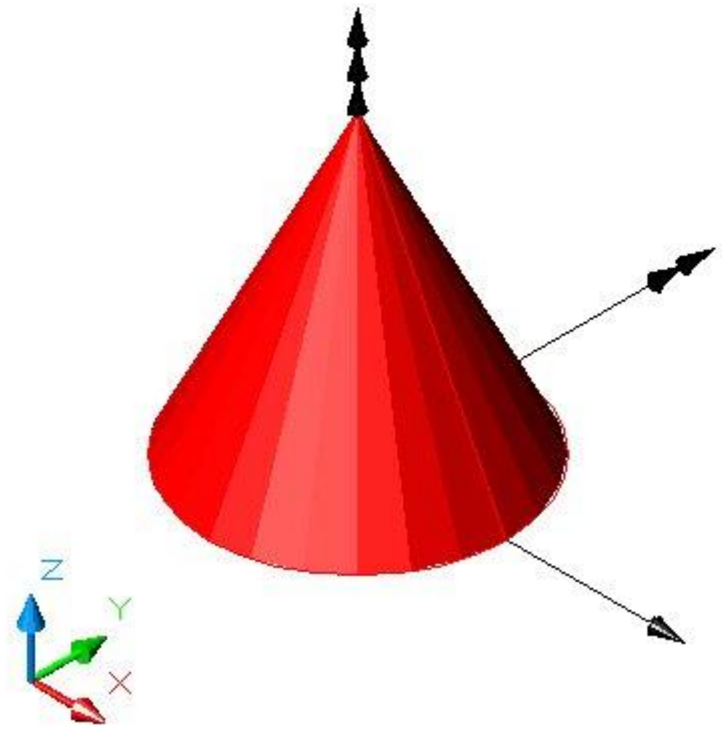
Pop Quiz:
Using different views in analysis

What does this look like?



A circle with a dot in the center?
A sphere with a hole through the center?

It could be this…



Or it could be this…

A single view can mislead you…

Conclusion

Probabilistic Risk Assessment (PRA) is a tool to help you assess the risk by looking at systems and operations in a different view both quantitatively and qualitatively.

Given our available budget <u>and</u> time, we must be smart <u>and</u> efficient in how and what we do. That's where PRA can make a difference.

Introduction

Introduction

- **Probabilistic Risk Assessment (PRA) is one of the tools in NASA's Safety & Mission Assurance (S&MA) toolbox. It's also referred to as Probabilistic Safety Assessment (PSA). PRA/PSA provides both depth and width in evaluating systems, vehicles, vessels, facilities, and missions.**

- **NASA continues to get budgets with high expectations from the public. S&MA must continue to do its job with less, thus we have to be smarter and more efficient.**

- **PRA has been used successfully in several industries, such as commercial nuclear power, aerospace, chemical, transportation, oil & gas, and medical.**

- **The Johnson Space Center (JSC) is actively supporting the Bureau of Safety and Environmental Enforcement (BSEE) and several Oil & Gas companies with respect to PRA in addition to its traditional human space programs.**

What is PRA?

- **PRA is a comprehensive, structured, and disciplined approach to identifying and analyzing risk in engineered systems and/or processes. It attempts to quantify rare event probabilities of failures. It attempts to take into account all possible events or influences that could reasonably affect the system or process being studied. It is inherently and philosophically a Bayesian methodology. In general, PRA is a process that seeks answers to three basic questions:**
  - ✓ **What kinds of events or scenarios can occur (i.e., what can go wrong)?**
  - ✓ **What are the likelihoods and associated uncertainties of the events or scenarios?**
  - ✓ **What consequences could result from these events or scenarios (e.g., Loss of Crew/Life, Loss of Mission, Loss of Hydrocarbon Containment, Reactor Core Damage Frequency)?**
- **There are other definitions and questions that it can help answer.**
- **The models are developed in "failure space". This is usually different from how designers think (e.g. success space).**
- **PRAs are often characterized by (but not limited to) event tree models, fault tree models, and simulation models.**

Oil & Gas Examples

- **Facility Level Risk Assessment**
  - Deepwater Drilling Operation
  - Shallow Water Drilling Operation
  - Subsea Oil Production
  - Rigs and Platforms
- **System Level Risk Assessment**
  - Blowout Preventer (BOP)
  - Dynamic Positioning System (DPS)
  - Mud Systems
- **Focused risk trade studies between current and proposed process/design. For example:**
  - Evaluate the proposed requirement for additional subsea accumulator bottles in the Well Control Rule for a five year time frame vs. the existing system in API STD-53.
  - Comparing different BOP ram drivers and sealing.
  - Evaluating operational work arounds given an initiating event, such as bolt failure.

When can PRA be Performed?

NEW DEVELOPMENTS
The ideal time to conduct a PRA is at the beginning of the design process to incorporate the necessary safety and risk avoidance measures throughout the development phase at minimal cost.

EXISTING SYSTEMS
PRA can be applied to existing systems to identify and prioritize risks associated with operations. PRAs can evaluate the impact of system changes and help avoid compromises in quality or reliability while increasing productivity.

INCIDENT RESPONSE
In the event of unexpected downtime or an accident, a good PRA team can assess the cause of the failure <u>and</u> develop appropriate mitigation plans to minimize the probability of comparable events in the future.

In a nutshell, PRA can be applied from concept to decommissioning during the life cycle, including design and operations.

Some Background

- **In late fifties / early sixties Boeing and Bell Labs developed Fault Trees to evaluate launch systems for nuclear weapons and early approaches to human reliability analysis began.**

- **NASA experimented with Fault Trees and some early attempts to do Probabilistic Risk Assessment (PRA) in the sixties (most notably on the Apollo Program). The estimated risk was believed to be too high, so it was abandoned and quantitative risk assessment was off the table until post-Challenger.**

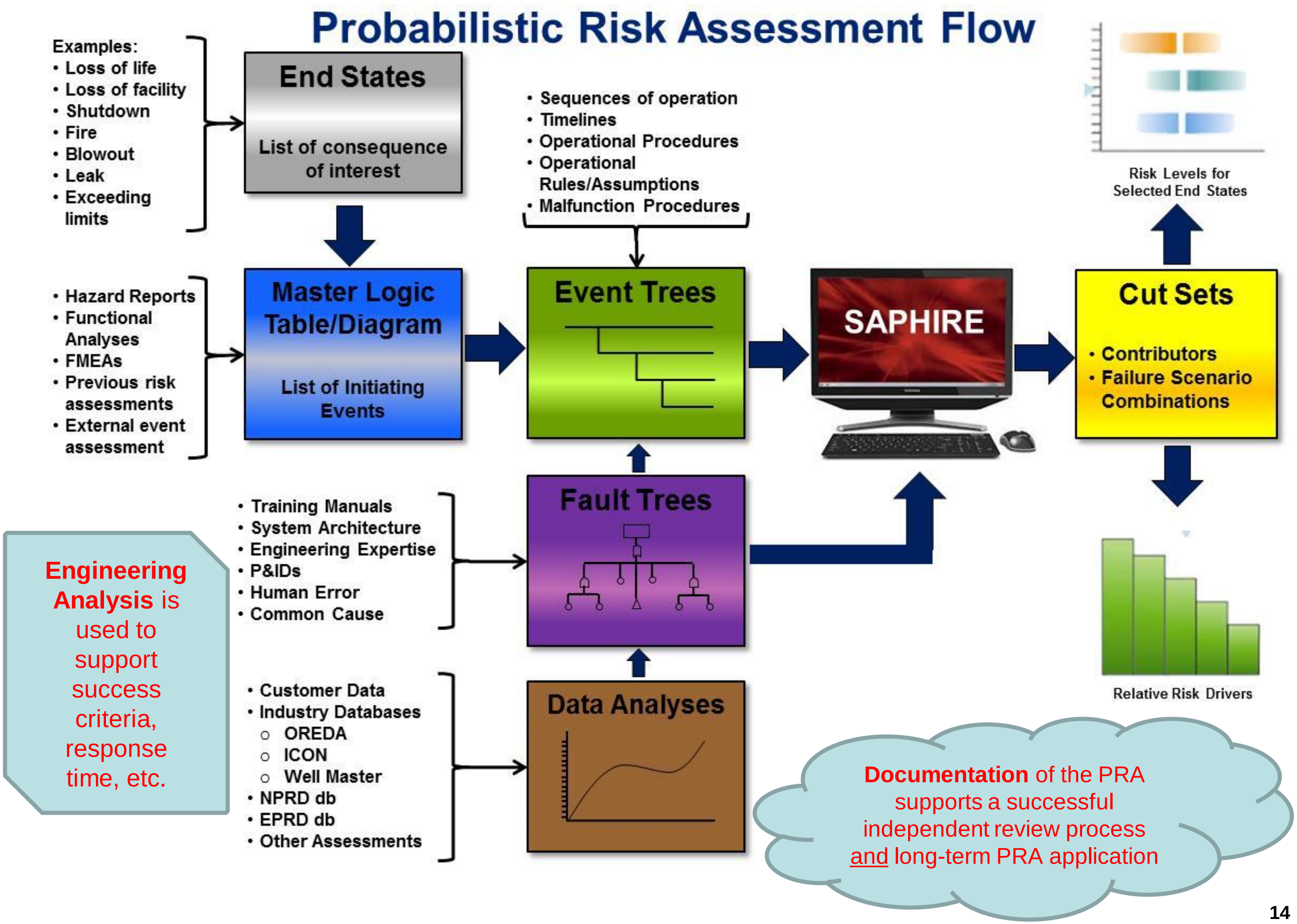
- **Nuclear power industry picked up the technology in early seventies and created WASH-1400 (Reactor Safety Study) in the mid seventies.**
  - This is considered the first modern PRA.
  - Was shelved until the Three Mile Island (TMI) incident happened in 1979. It was determined that the WASH-1400 study gave insights to the incident that could not be easily gained by any other means.

- **PRA is now practiced by all commercial nuclear plants in the United States and a large amount of data, methodology, and documentation for PRA technology has been developed by the industry and the Nuclear Regulatory Commission (NRC).**
  - All new Nuclear Plants must license their plants based on PRA as well as "Defense In Depth" concepts.
  - The NRC practices its oversight responsibility of the commercial nuclear industry using a "Risk-informed" approach that is heavily dependent on PRA.
  - SAPHIRE (Systems Analysis Programs for Hands-on Integrated Reliability Evaluations) is a PRA software tool developed by the Idaho National Lab for the U.S. NRC and also used by NASA and some oil companies now.

JSC S&MA Analysis Branch

PRA Overview

PRA Process


Probabilistic Risk Assessment Flow
Examples:
• Loss of life
• Loss of facility
• Shutdown
• Fire
• Blowout
• Leak
• Exceeding limits
End States
List of consequence of interest
• Sequences of operation
• Timelines
• Operational Procedures
• Operational Rules/Assumptions
• Malfunction Procedures
Risk Levels for Selected End States
• Hazard Reports
• Functional Analyses
• FMEAs
• Previous risk assessments
• External event assessment
Master Logic Table/Diagram
List of Initiating Events
Event Trees
SAPHIRE
Cut Sets
• Contributors
• Failure Scenario Combinations
• Training Manuals
• System Architecture
• Engineering Expertise
• P&IDs
• Human Error
• Common Cause
Fault Trees
Relative Risk Drivers
Engineering Analysis is used to support success criteria, response time, etc.
• Customer Data
• Industry Databases
o OREDA
o ICON
o Well Master
• NPRD db
• EPRD db
• Other Assessments
Data Analyses
Documentation of the PRA supports a successful independent review process and long-term PRA application

The PRA Team

- **A PRA system analysis team includes both system domain experts <u>and</u> PRA analysts. The key to success is <u>multi-way communication</u> between the PRA analysts, domain experts, and management.**
- **A majority of <u>PRA analysts</u> have engineering degrees with operations and/or design backgrounds in order to understand how systems work and fail. This is essential in developing the failure logic of the vehicle or facility.**
- **Good <u>data analysts</u> understand how to take the available data to generate probabilities and their associated uncertainty for the basic events that the modelers can use or need.**
- **Building or developing a PRA involves:**
  - understanding its purpose <u>and</u> the appropriate modeling techniques,
  - designing how it will serve that purpose,
  - populating it with the desired failure logic and probabilities, and
  - trouble shooting it (nothing works the first time)

The PRA Team

JSC S&MA Analysis Branch

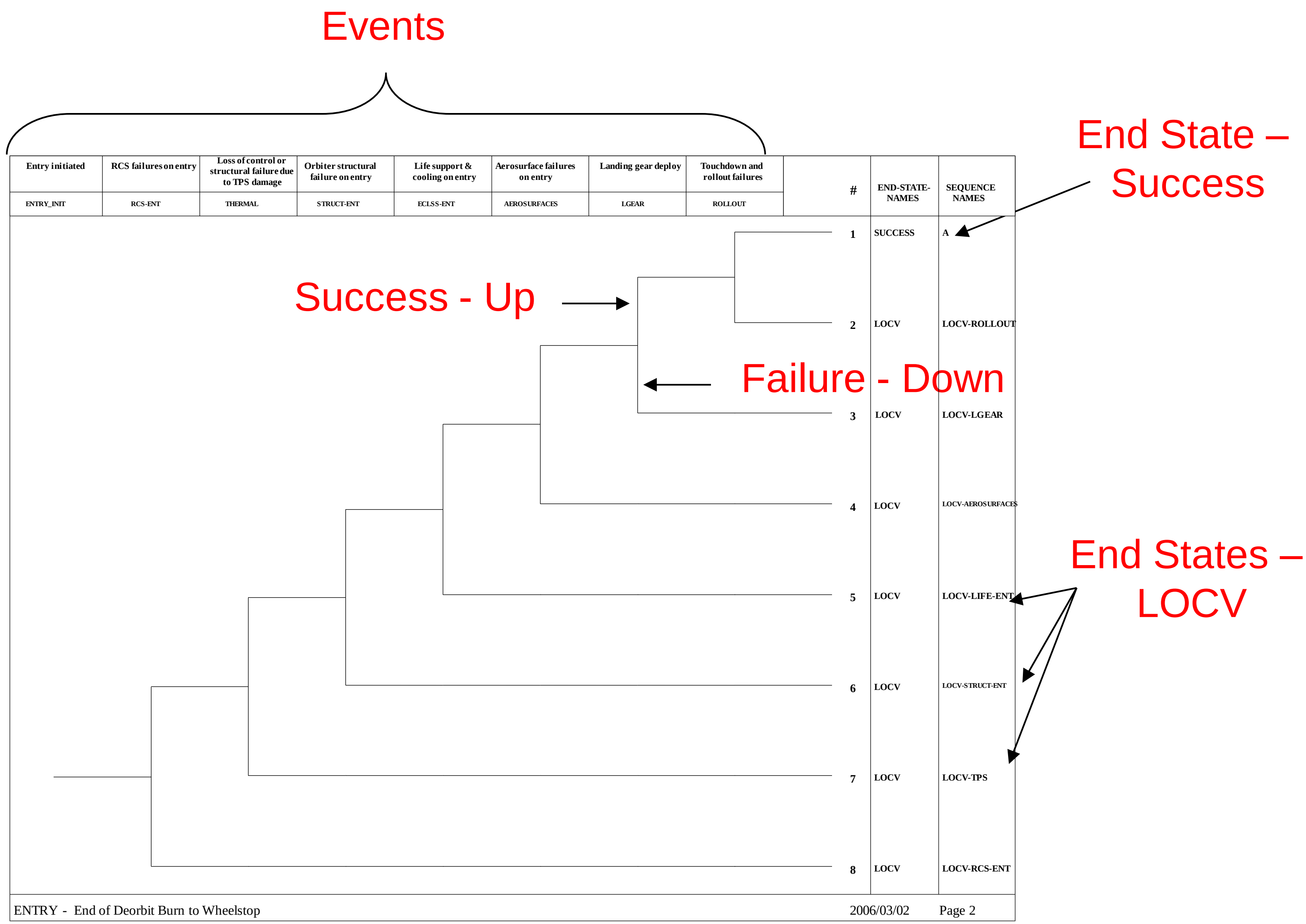
PRA Development Process

Failure Logic

Event Tree Analysis

- **Event trees are the tools that model the overall mission or operation starting with an initiating event, such as a well kick, and ending with successful well closure or not.**
- **The event trees are timelines of critical events that occur during a mission with branch points that generally represent a successful event or a failure during the event.**
  - A failed branch in an event tree is the start of a scenario that may end directly in a loss of hydrocarbon event, or it may have mitigations associated with it such as remote operated vehicles (ROVs).
  - Each branch of the event tree is followed in a deductive fashion to its end state.
- **Multiple event trees are used in order to model a complete mission, and the event trees are linked together to get the appropriate potential event sequences.**
  - An example of a Shuttle event tree is shown on the following page.
- **The results of the event tree analysis is a list of ranked "cutsets" or failure scenarios for the entire mission that can be categorized by phase, element, system, etc.**

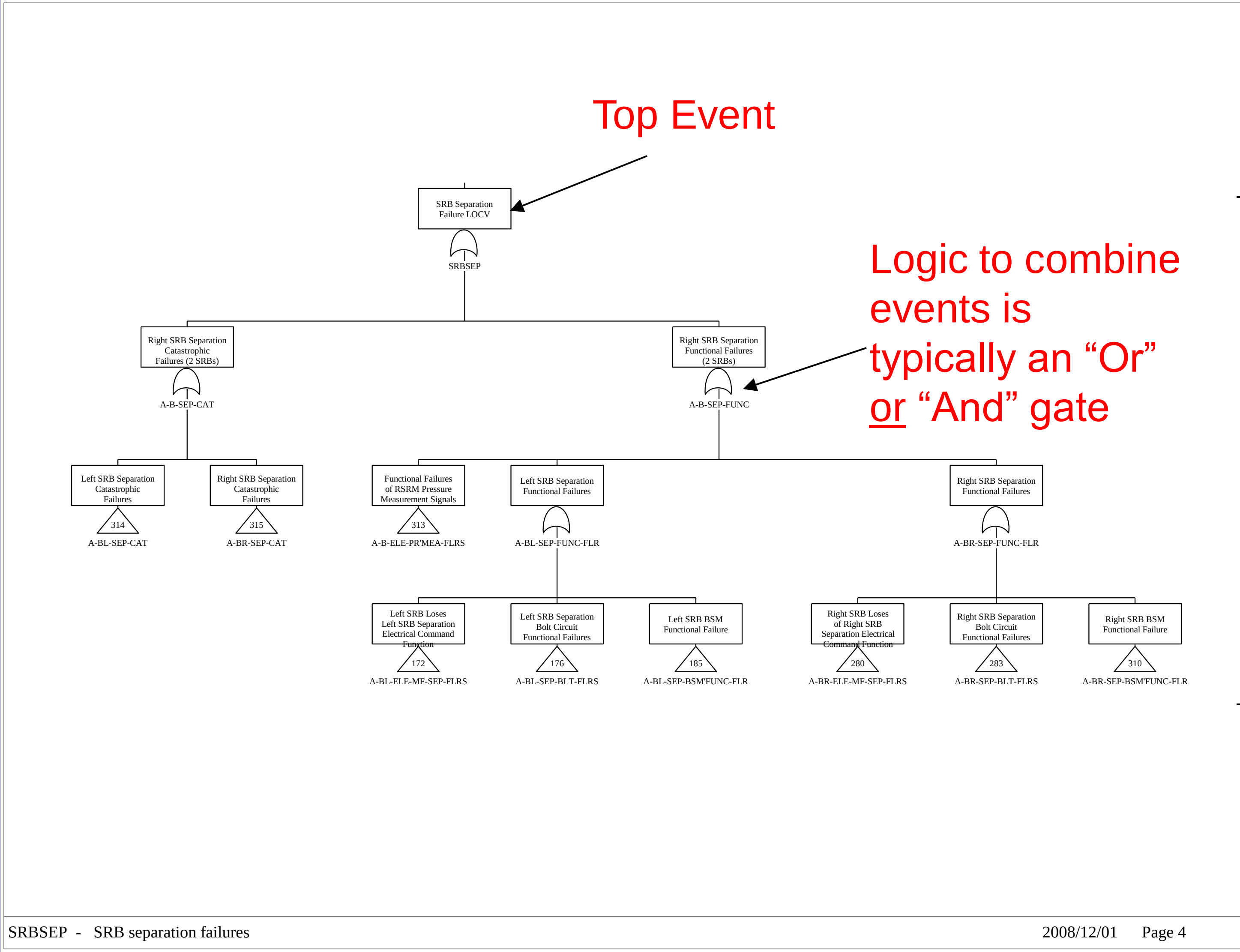
Example Event Tree



Fault Tree Analysis

- **Fault trees are the tools that model the individual events in the event trees.**
  - Typically failure of a system or function
- **The fault trees are developed in a deductive fashion, starting with a top event and developing logic that will result in the top event occurring**
- **Many systems are used in multiple mission phases, e.g. power, so fault trees must account for partial losses in multiple phases resulting in a total loss of the system or function.**
- **Recovery actions may be included in the logic of the fault tree, that require both a failure to occur and a failure to recover.**
- **Fault tree logic is developed downward to a level compatible with existing data.**
- **Each fault tree produces "cutsets" or failure scenarios for that top event. The fault trees are input into the event trees to develop overall integrated mission level results.**

Example Fault Tree Analysis

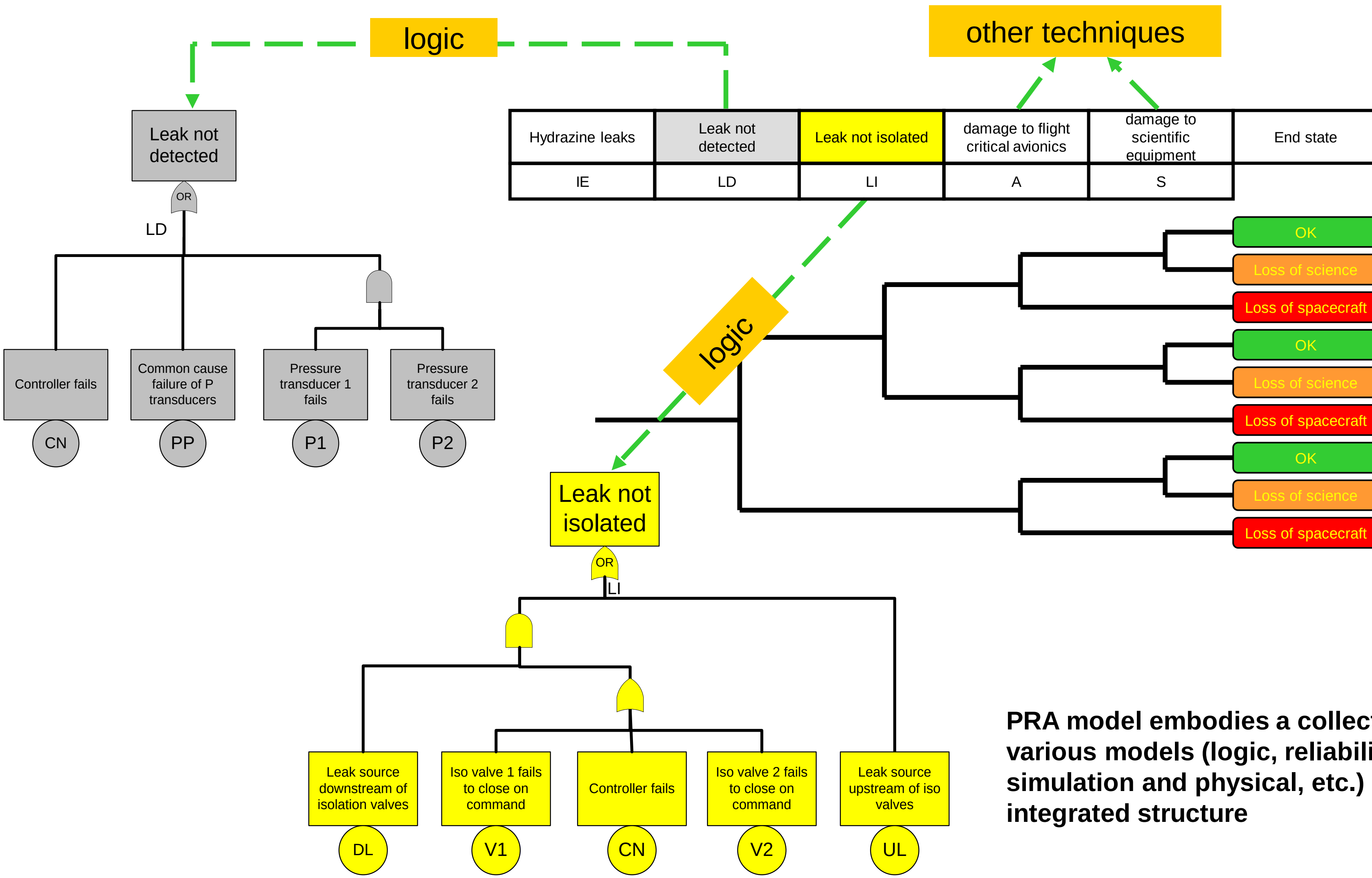


Top Event

Logic to combine events is typically an “Or” <u>or</u> “And” gate

Logic proceeds to lower levels as data permits

Fault Trees Are Attached to the Event Tree



PRA model embodies a collection of various models (logic, reliability, simulation and physical, etc.) in an integrated structure

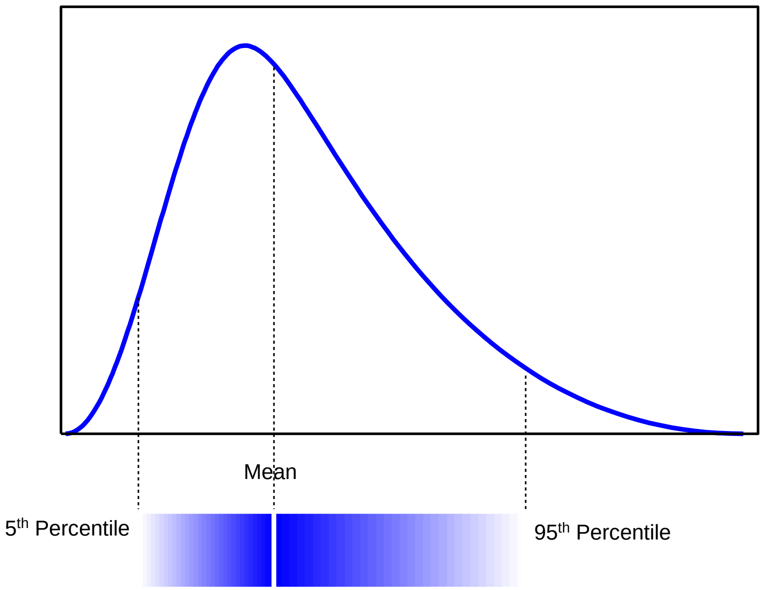
Data Analysis

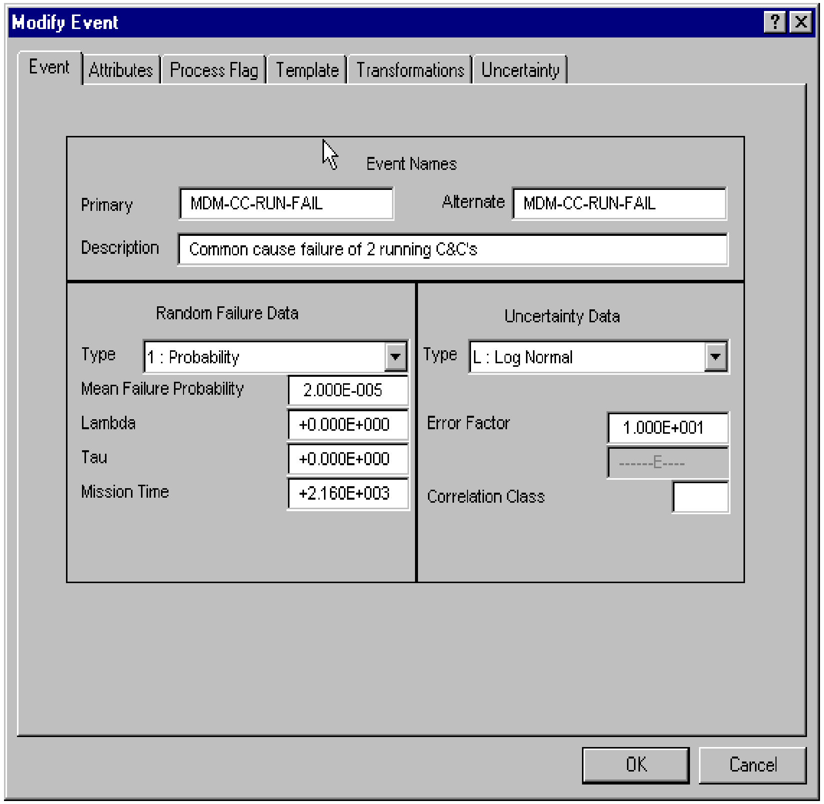
<u>or</u>

Basic Event Development

Basic Event Input

- **For each Basic Event**
  - probability of failure
  - probability distribution
  - 5th and 95th percentiles





SAPHIRE Screenshot

Types of Data that Exist in the Models

- **Functional – A functional failure event is generally defined as failure of a component type, such as a valve or pump, to perform its intended function. Functional failures are specified by a component type (e.g., motor pump) and by a failure mode for the component type (e.g., fails to start). Functional failures are generally defined at the major component level such as Line Replaceable Unit (LRU) or Shop Replaceable Unit (SRU). Functional failures typically fall into two categories, time-based and demand-based. Bayesian update as Shuttle specific data becomes available.**

- **Phenomenological – Phenomenological events include non-functional events that are not solely based on equipment performance but on complex interactions between systems and their environment or other external factors or events. Phenomenological events can cover a broad range of failure scenarios, including leaks of flammable/explosive fluids, engine burn through, over pressurization, ascent debris, structural failure, and other similar situations.**

- **Human – Three types of human errors are generally included in fault trees: pre-initiating event, initiating event (or human-induced initiators), and post-initiating event interactions.**

- **Common Cause – Common Cause Failures (CCFs) are multiple failures of similar components within a system that occur within a specified period of time due to a shared cause.**

- **Conditional – A probability that is conditional upon another event, i.e. given that an event has already happened what is the probability that successive events will fail**

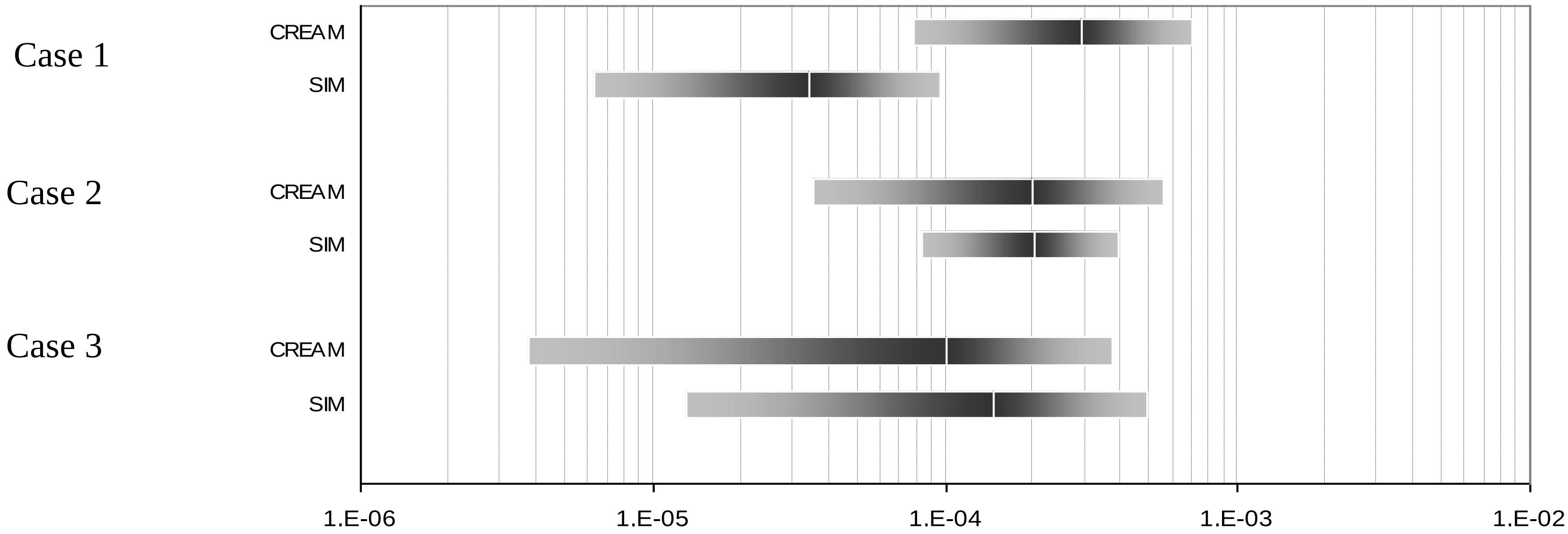
Functional Data Sources

- NASA's PRACA databases are sources for Shuttle specific failure data
- Contractor/vendor data, when available
- OREDA. Offshore and Onshore Reliability Data 6th Edition. 2015.
- SINTEF Reliability Data for Safety Instrumented System, 2013 Edition.
- Non-electric Part Reliability Database (NPRD) is a generic data source for run time failure data for mechanical components
- Electric Parts Reliability Data (EPRD) is a generic data source for run time failure data for electrical components
- Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR) is a generic data source for on demand failures
- Expert Opinion
- Miscellaneous references

Human Reliabilty Analysis (HRA)

- **HRA is a method used to describe, qualitatively and quantitatively, the occurrence of human failures in the operation of complex machines that affect availability and reliability.**
- **Modeling human actions with their corresponding failure in a PRA provides a more complete picture of the risk and risk contributions.**
- **A high quality HRA can provide valuable information on potential areas for improvement, including training, procedural and equipment design.**
- **Screening analysis is performed on the bulk of the human errors with a detailed analysis only performed on the significant contributors.**

Comparison of HRA Results to Training Data



For available data, CREAM compared well with simulator data

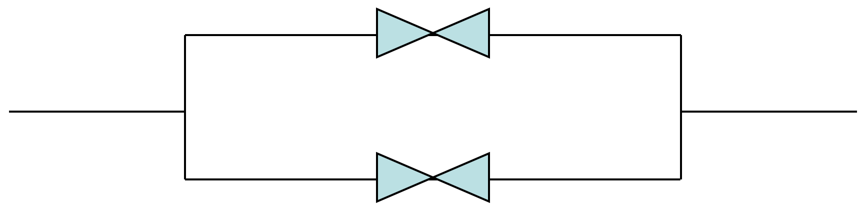
- **– Added to credibility of the analysis**

Common Cause Definition

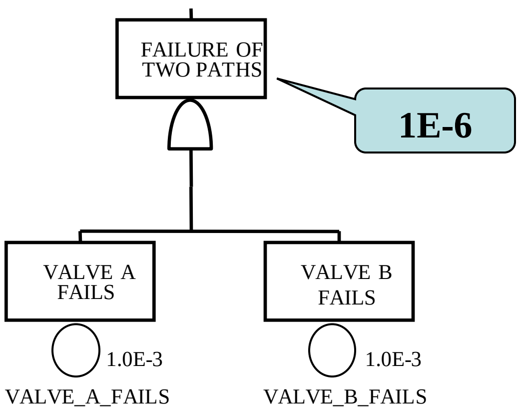
- **In PRA, Common Cause Failures (CCFs) are failures of two or more components, subsystems, or structures due to a single specific event which bypassed or invalidated redundancy or independence at the same time, or in a relatively short interval like within a single mission**
  - May be the result of a design error, installation error, or maintenance error, or due to some adverse common environment
  - Sometimes called a generic failure.
- **Common Cause, as used in PRA, is <u>not</u> a single failure that takes out multiple components such as a common power supply to computers or common fluid header to multiple pumps.**
  - Single point failures, such as these, are modeled explicitly in a PRA

Common Cause Modeling (2)

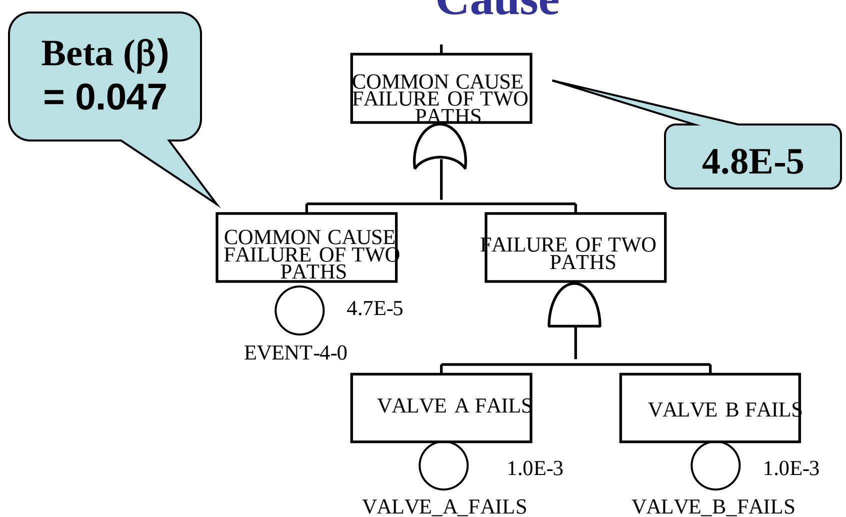
A system consisting of two trains:



Without Considering Common Cause



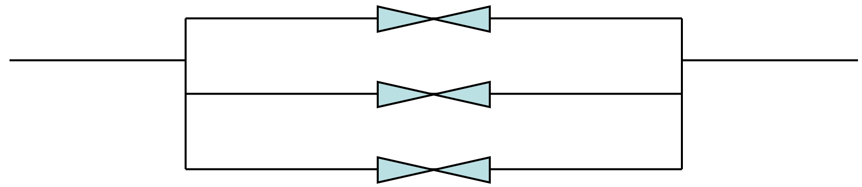
Considering Common Cause



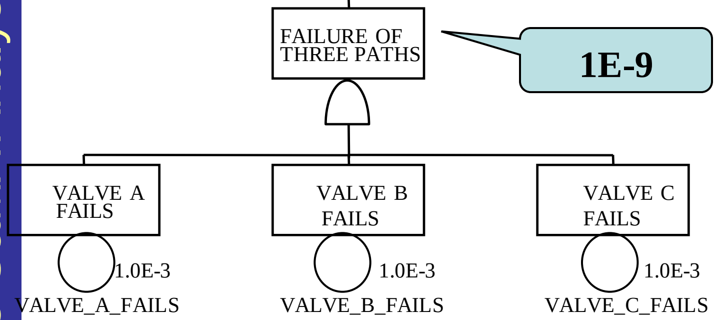
Results in a ~ 4.7E-05 Underestimate of Risk Which is 48 Times the Risk Without Considering Common Cause

Common Cause Modeling (3)

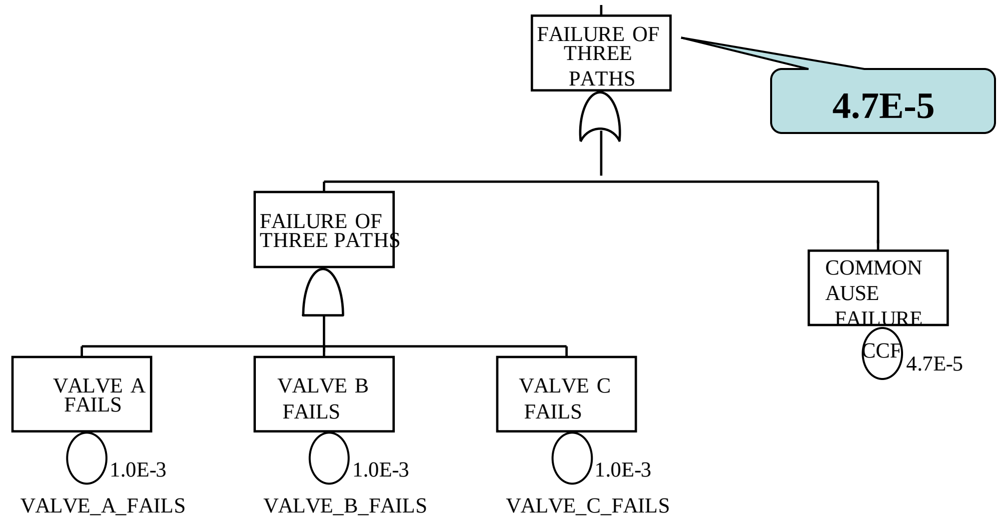
A system consisting of three trains:



Without Considering Common Cause



Considering Common Cause (Beta Model)



Results in a ~ 4.7E-05 Underestimate of Risk Which is 47,000 Times the Risk Without Considering Common Cause

Note: Using a MGL Model Would Reduce Result to 2.6E-05

Conditional Probability

- **Given that an event has already happened what is the probability that successive events will fail.**
  - Example: Given a blown tire in the time interval between main gear touch down and nose gear touch down what is the probability that the Orbiter crashes (i.e. strut fails or crew looses control of vehicle).

- **Conditional probabilities are typically relatively large (e.g. values like 0.1 to 0.9) and are usually derived from expert opinion or direct experience.**

Keep in Mind

Unknown and Underappreciated Risks

- **Risk model completeness** has long been recognized as a challenge for simulated methods of risk analysis such as PRA as traditionally practiced.

- These **methods are generally effective** at identifying system failures that result from combinations of component failures that propagate through the system due to the functional dependencies of the system that are represented in the risk model.

- However, they are typically <u>ineffective</u> at identifying system failures that result from **unknown or underappreciated (UU)** risks, frequently involving complex intra- and inter-system interactions that may have little to do with the intentionally engineered functional relationships of the system.

Unknown and Underappreciated Risks (Cont'd)

- Earlier in 2009, the NASA Advisory Council noted the following set of contributory factors:
  - Inadequate definitions prior to agency budget decision and to external commitments
  - optimistic cost estimates/estimating errors
  - inability to execute initial schedule baseline
  - Inadequate risk assessments
  - higher technical complexity of projects than anticipated
  - changes in scope (design/content)
  - Inadequate assessment of impacts of schedule changes on cost
  - annual funding instability
  - eroding in-housetechnicalexpertise
  - poor tracking of contractor requirements against plans
  - Reserve position adequacy
  - lack of probabilistic estimating
  - "go as you can afford" approach
  - lack of formal document for recording key technical, schedule, and programmatic assumptions.

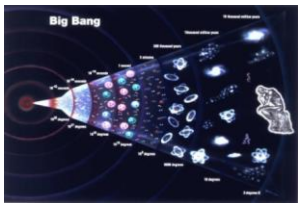
Examples of Results

JSC S&MA Analysis Branch

First, the Math

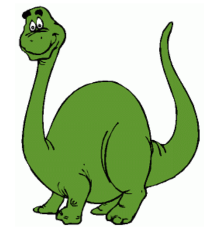
1.0E-02 = 0.01	➔ 1:100	(Probable)	➔ ~Shuttle Mission Risk
1.0E-06 = 0.000001	➔ 1:1,000,000	(Improbable)	➔ having 20 coins simulaneously landing on tails
1.0E-12 = 0.000000000001	➔ 1:1,000,000,000,000	(ridiculous)	➔ Built by Dinosaurs?

Time Perspective



1.2 x 10^{14} hours ago
~14 billion years ago

4 x 10^{13} hours ago
~4.5 billion years ago



2 x 10^{12} – 7 x 10^{11} hours ago
~228 – 80 million years ago

4 x 10^{8} hours ago
~46,000 years ago

2.1 x 10^{6} hours ago
~240 years ago

6.3 x 10^{5} hours ago
~72 years ago

PRA Top Risk Contributors / Scenarios

Notional

Rank	%age of Total	Cumulative Total	Point Estimate Probability (1:n)	Failure Scenario Description	Related Hazard Reports	Program Action / Status (Open/Accepted SIRMA risks)	Previous Iteration (For Comparison) Rank	Previous Iteration (For Comparison) Probability
1	30	30	3.3E-03 (1:300)	Debris strikes vehicle on orbit leading to LOC on orbit or entry	HA-007	(IRMA 2530, numerous child risks) Optimizing vehicle mission flight attitude profile to reduce risk. Inspection, repair, and crew rescue capabilities are applicable through late inspection. *A xx" discernment or use for late inspection could reduce the risk*.	1	3.3E-03 (1:300)
2	15	45	1.5E-03 (1:670)	Rocket Engine catastrophic failure	Numerous	(IRMA concern 2723) SSME-induced catastrophic failure is still a top contributor in this iteration. Iteration x takes credit for the system upgrade which mitigates catastrophic failure . No other major improvements are planned.	2	1.5E-03 (1:670)
3	10	55	1.1E-03 (1:940)	Ascent debris strikes vehicle leading to LOC on orbit or entry	HA-009 HA-007 Numerous Others	(IRMA Ascent Debris Risks 2679, 2681, 2682) Additional design and processing plans either under evaluation or have been implemented for further improvement. Inspection, repair, and crew rescue capabilities provide significant benefits. *Mission data will continue to be reviewed to monitor for further improvement.*	3	1.1E-03 (1:940)
4	5	60	8.2E-04 (1:1200)	Crew error during entry	HA-21 HA-079 HA-192 HA-217	(IRMA 4068) Concurrence with the community that current training level is sufficient. No significant upgrade activities planned. *No significant additional PRA development planned.*	4	8.2E-04 (1:1200)
5	5	65	6.5E-04 (1:1500)	System 1 catastrophic failure	Numerous	(No Program Risk Assigned) No significant upgrade activities planned. *No significant additional PRA development planned.*	5	6.5E-04 (1:1500)
6	2	67	2.3E-04 (1:4400)	System 2 catastrophic failure during ascent	HA-059	(No Program Risk Assigned) No significant upgrade activities planned. *System 2 is a developing field, and therefore continued effort will be spent evaluating this risk.*	New	2.3E-04 (1:4400)

Uncertainty Distribution

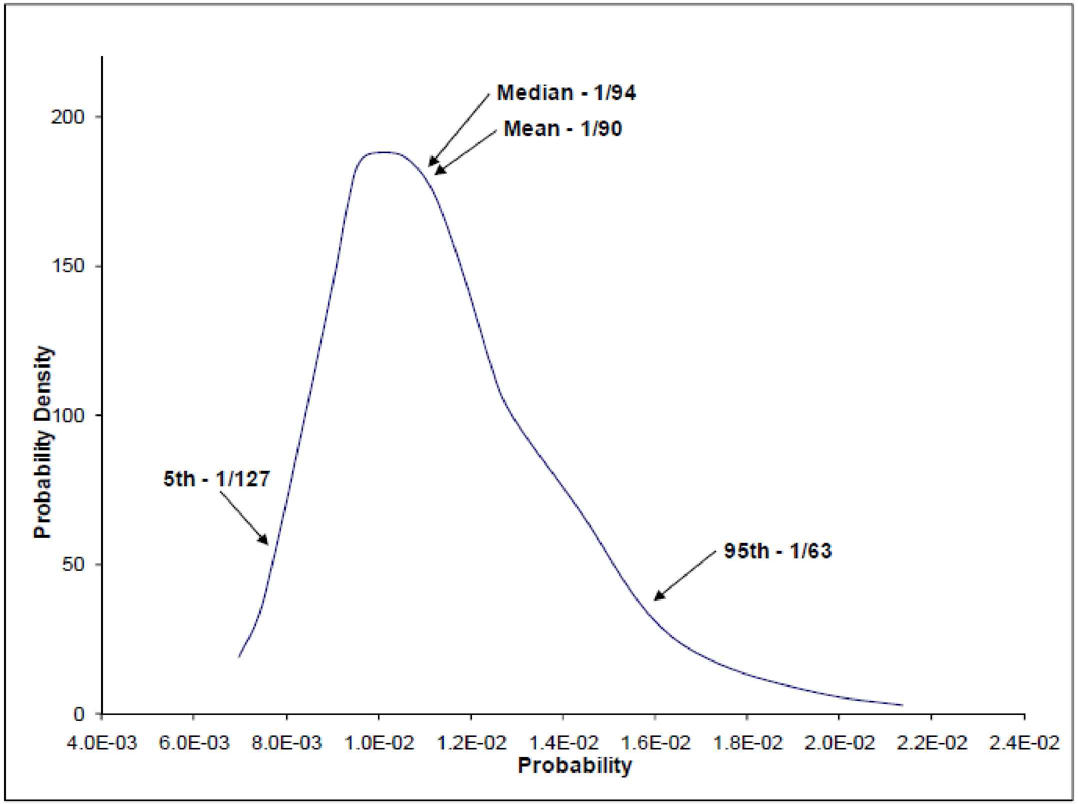
- This distribution is a representation of the uncertainty associated with a PRA's results
- The median is also referred to as the 50th percentile

Mean – 1.1E-02 (1:90)

Median – 1.1E-02 (1:95)

5th percentile – 7.7E-03 (1:130)

95th percentile – 1.7E-02 (1:60)



- The 5th and 95th percentile are common points on a distribution to show the range that 90% of the estimated risk lies between.
- The mean is a common measure of risk that accounts for uncertainty or this distribution, thus the value or metric used to verify LOC requirements.

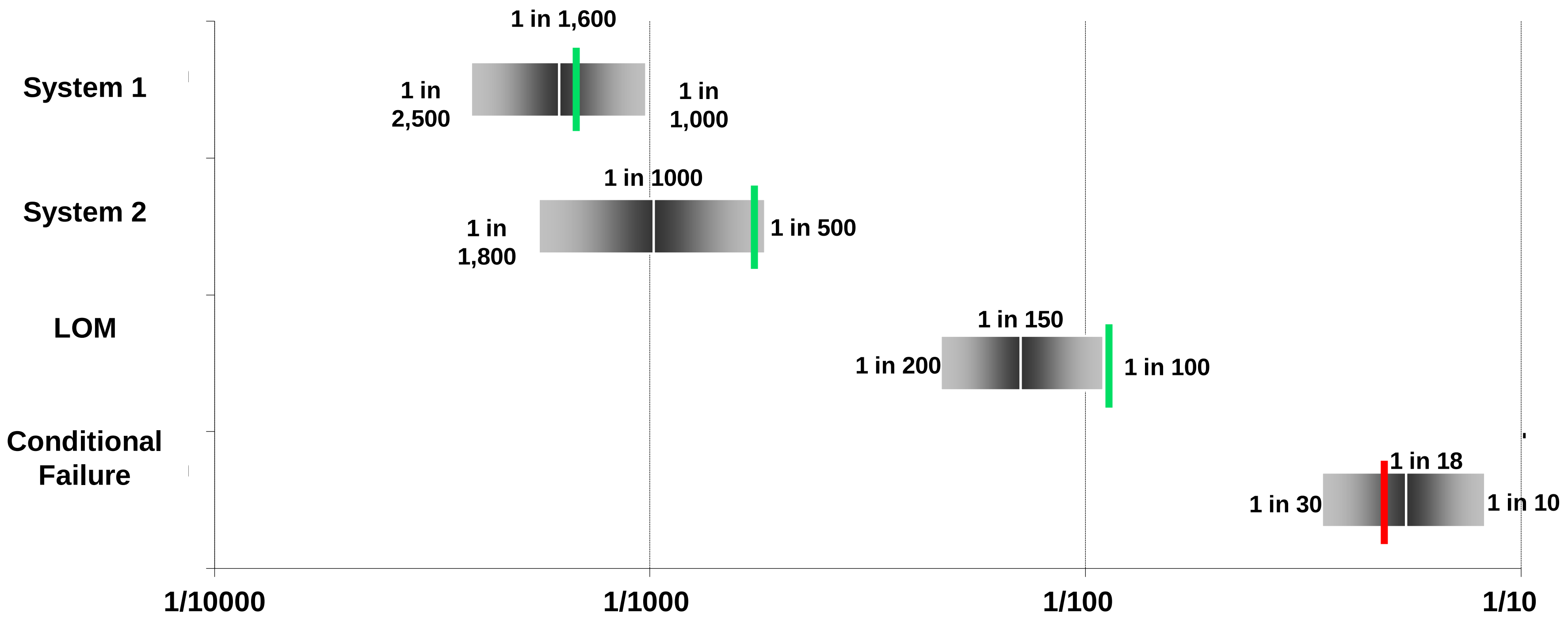
Estimated Risk vs Requirements/Goals

Notional

Mission		Current LOC/LOM Requirements (Mean Values)	Notional PRA Results (Estimates)		
			5th Percentile	Mean	95th Percentile
Mission	System 1 LOC	1 in 1,400 (R-16, CV0978)	1 in 2,500	1 in 1,600	1 in 1,000
		7.14E-04	3.88E-04	6.12E-04	9.81E-04
	System 2 LOC	1 in 550 (R-16, SLS.16)	1 in 1,800	1 in 1000	1 in 540
		1.82E-03	5.55E-04	1.00E-03	1.84E-03
	LOM	1 in 85 (I.MPCV-SLS.3132)	1 in 210	1 in 140	1 in 90
		1.18E-02	4.65E-03	7.14E-03	1.10E-02
	Conditional Failure	1 in 20 (CA5913)	1 in 29	1 in 18	1 in 12
		5.00E-02	3.49E-02	5.55E-02	8.28E-02

Showing Uncertainty wrt Requirements

Notional

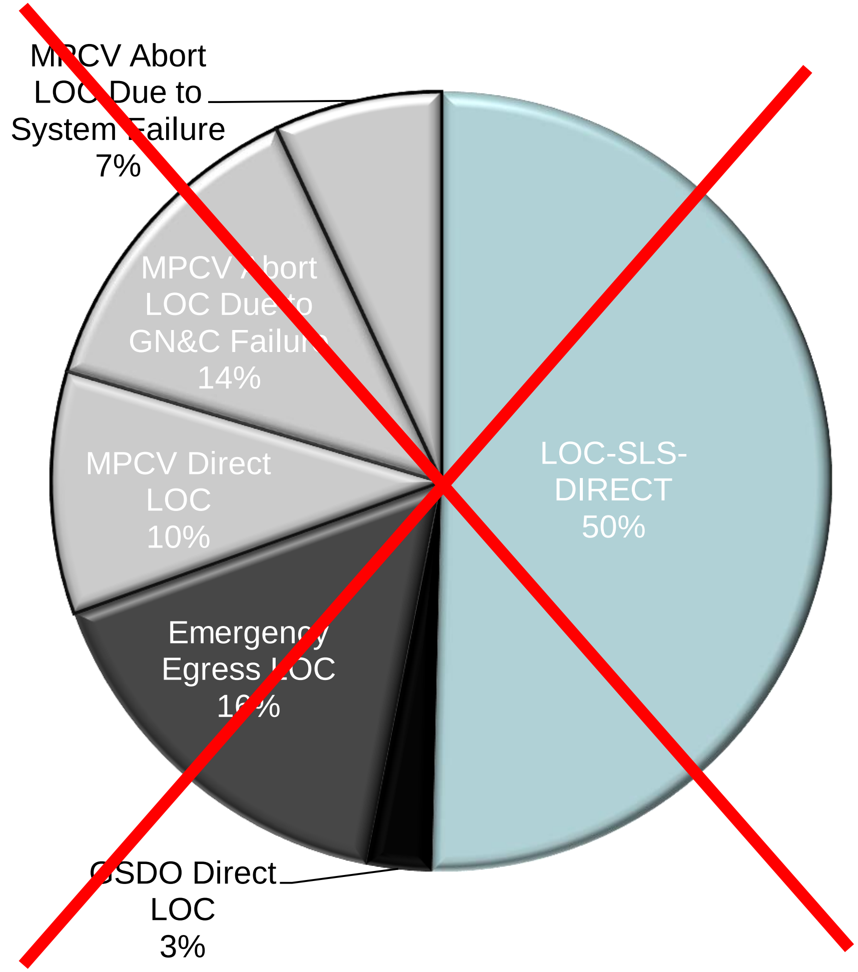


Green Bar shows Requirement Value is met
Red Bar shows Requirement Value is not met

What Not to Do

No Pie Charts,

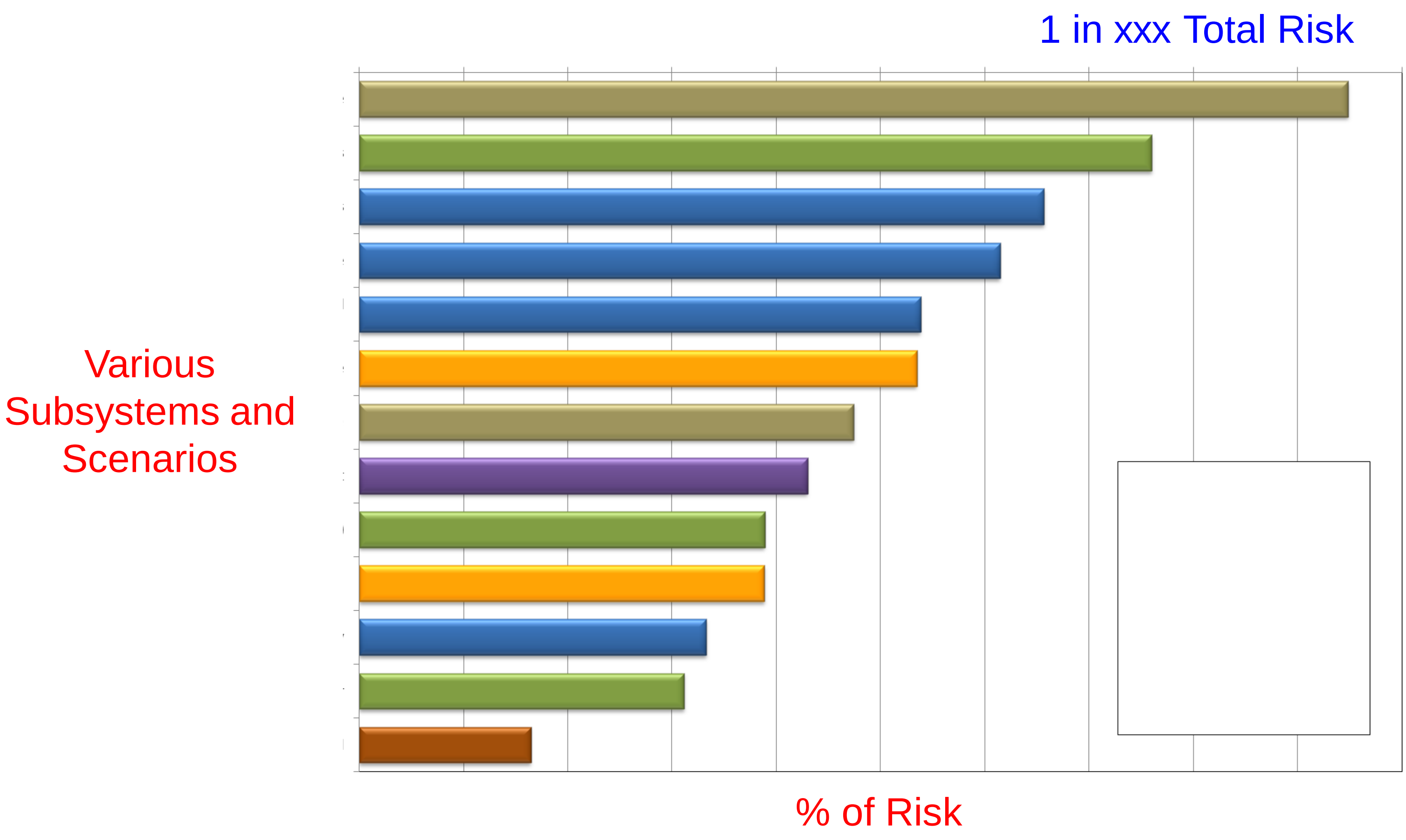
They assume completeness <u>and</u> we know that we don't know it all.



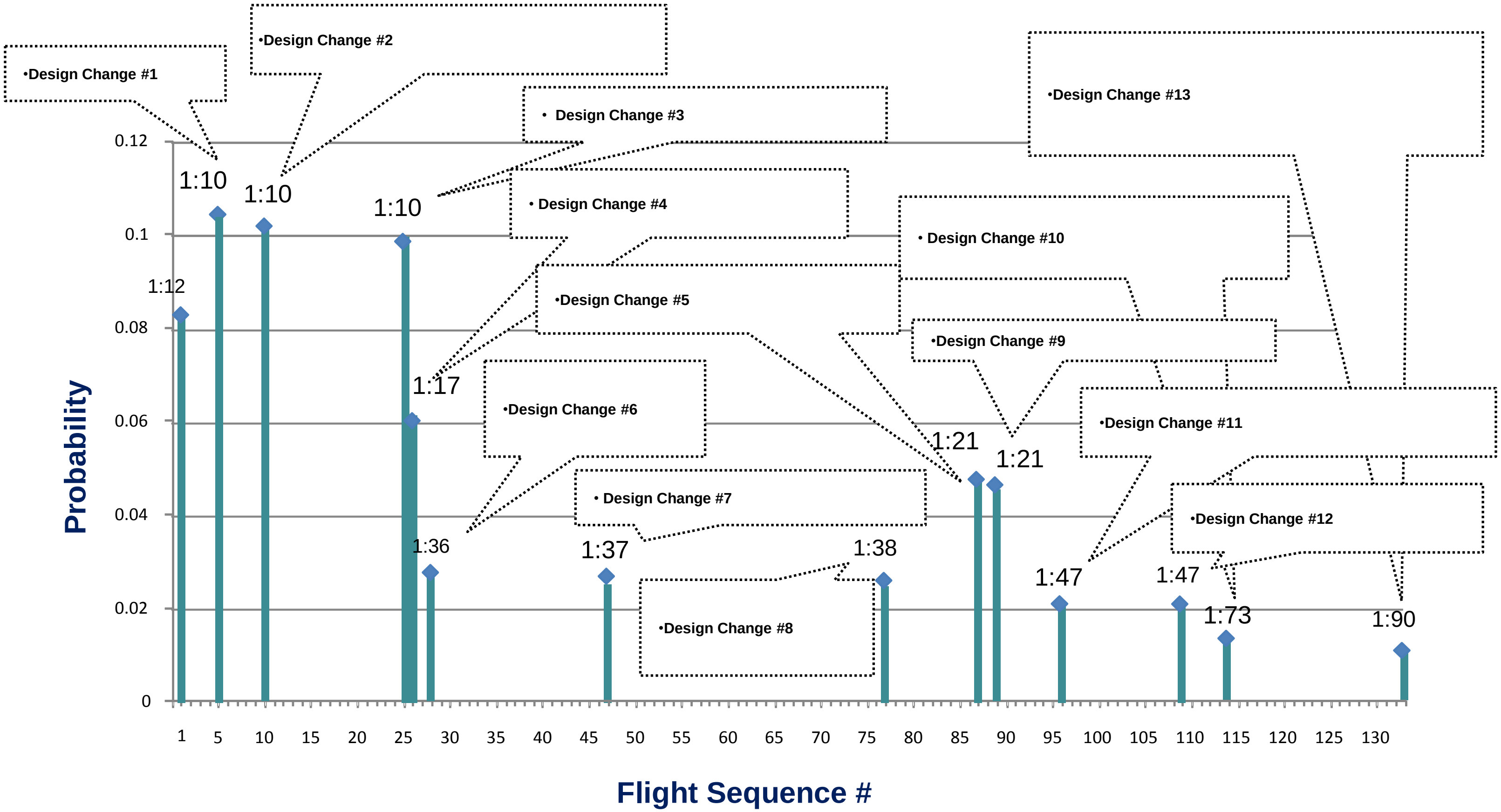
JSC S&MA Analysis Branch

Notional Risk Drivers via Pareto
(e.g. Top 80% of Calculated Risk)

A Pareto chart like this can be made for each project, mission phase, etc.



Risk Regression Example



This chart shows how calculated risk changed following design and ops changes over a 30 year program by peeling back the "onion" (starting at the end and undoing changes). Note that risk doesn't decrease according to a nice exponential curve, but only after something fails <u>and</u> it gets "fixed".

Today's "Take Aways"

- "Essentially, all models are wrong, but some are useful."
- PRA is a tool that has been demonstrated in multiple industries to help identify and rank risk drivers (e.g. HRA vs Training Risk)
- PRA is <u>not</u> just a math model, but an integrated assessment of the system. It is, or should be, based on engineering analysis, operational input, human health & performance (as applicable), historical evidence when available, …., thus needs management support across disciplines and programs to make it work.
- Statistics address large amounts of data / experience. PRAs address events that hopefully never happen, thus are probabilistic.

In Closing

- **There is much more to know about PRA than what you've seen today. This presentation was to give you insight in order to ask the right questions when you are trying to decide:**
    - whether you need a PRA or not,
    - is it being performed properly and by qualified analysts,
    - is it answering the question(s) you <u>need</u> answered.

- **PRA (with the help of deterministic analyses) identifies <u>and</u> ranks the risk contributors, the Failure Mode & Effect Analysis (FMEA) analysts and Reliability Engineers can help solve the problem by focusing on the top risk drivers.**

- **Call me if you have questions at (281) 483-6070 or e-mail me at Roger.L.Boyer@nasa.gov**

Questions?

Backup Charts

JSC S&MA Analysis Branch

Absolute vs Relative Risk?

- **You may have heard, "Don't believe the absolute risk estimate, just the relative ranking".**
- **Each event in a PRA is assessed to having a probability of failure (since the PRA is performed in "failure space").**
  - these failures are combined via the failure logic which is used to determine how they are combined and the resulting scenarios.
  - the failure probabilities of each event are used to establish the probability of each scenario thus ranks the scenarios as well as being added to produce the overall risk.
  - If different approaches and methods are used (which sometimes are needed in full scope PRAs), then the absolutes can be challenged and so may their rankings. This is where experienced PRA analysts earn their pay to help minimize the difference.
- **As a result, some decision makers or risk takers want to know the overall risk, while others want to know how to reduce it by working on the top risk drivers first.**

When Should You Do a PRA?

- As early in the design process as you can in order to affect the design and corresponding risk with minimal cost impact (i.e. to support Risk Informed Design (RID))
- When the risk of losing the project is greater than the agency can live with either due to it being crewed <u>or</u> for financial reasons
- To support Risk Informed Decision Making (RIDM) throughout the program life cycle from “formulation to implementation” or “concept to closeout”
- Flying Nuclear Payloads in support of Presidential Order

How much does a PRA cost?

- **As you can also ask, "How much will it cost to <u>not</u> do a PRA?"**
- **The cost of a PRA is a function of the level of detail desired as well as the size/complexity of the item being assessed and the mission life cycle**
  - You should only model to the level of detail that you have data and no further. You may identify that significant risk exists at a sublevel, then your PRA is telling you that you need to study that level further. It may not be a PRA, but a reliability assessment at that time.
  - Modeling the ISS and Space Shuttle is on a different scale than an Earth communications satellite. However, deep space probes and Mars landers can be quite complex due to their mission duration and operational phases.