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

Prepared by

Roger L. Boyer, MS, CRE

Chief, Risk & Reliability Analysis Branch

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

Prepared for

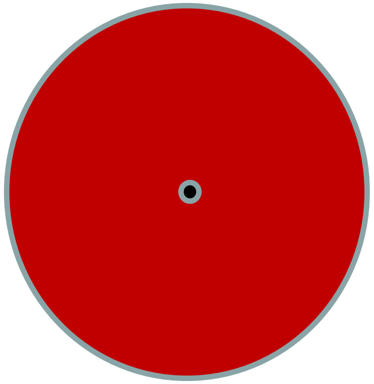
National Academy of Science
Ad Hoc Study Committee for Undersea Bolts

March 22, 2017

Pop Quiz:
Using different views in analysis

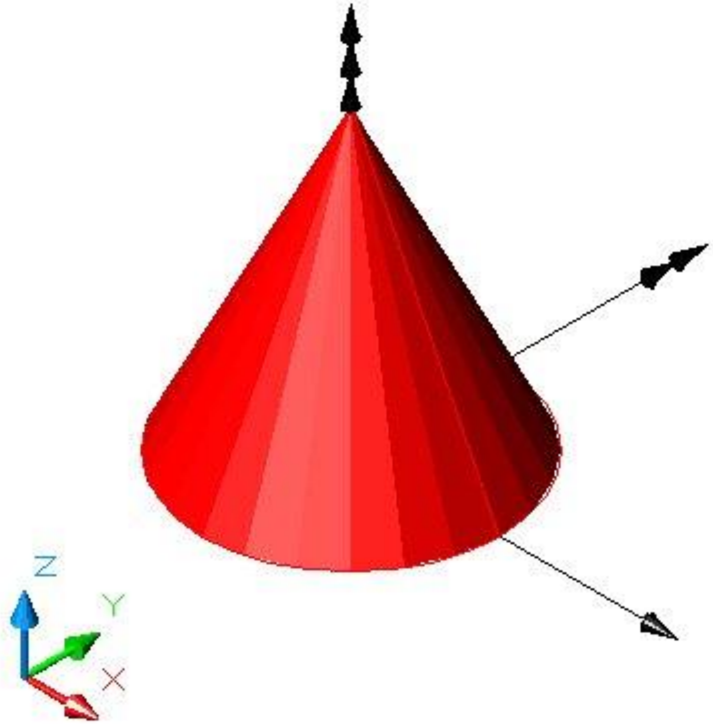
JSC S&MA Analysis Branch

What does this look like?

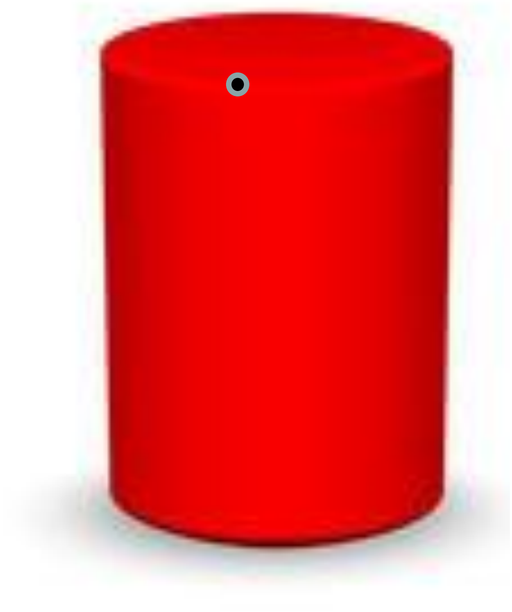


A circle with a dot in the center?
A sphere with a hole through the center?

It could be this…



Or it could be this…



A single view can mislead you…

Conclusion

As designers, you have an arsenal of tools, techniques, and personnel available to you.

Given your available budget and time, we must be smart and efficient in how and what we do. That’s where you can make a difference.

Questions?

Introduction

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

- It's been used successfully in several industries, such as commercial nuclear power, aerospace, transportation, chemical, and medical.

- 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.

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, 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.

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. Risk assessments can evaluate the impact of system changes and help avoid compromises in quality or reliability while increasing productivity.

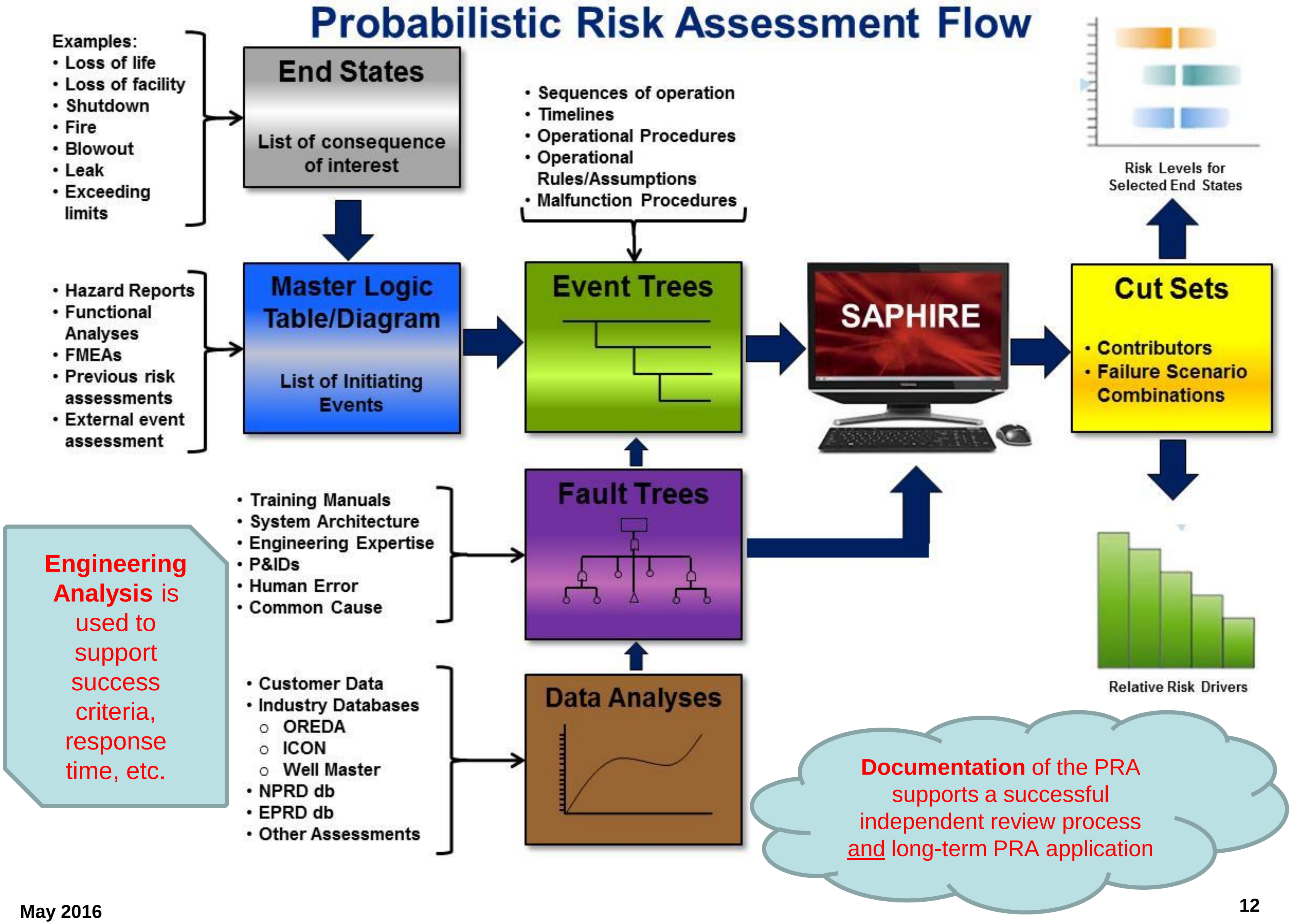
INCIDENT RESPONSE

In the event of unexpected downtime or an accident, our team can assess the cause of the failure and 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.

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

- Hazard Reports
- Functional Analyses
- FMEAs
- Previous risk assessments
- External event assessment

Master Logic Table/Diagram

List of Initiating Events

- Sequences of operation
- Timelines
- Operational Procedures
- Operational Rules/Assumptions
- Malfunction Procedures

Event Trees

SAPHIRE

Cut Sets

- Contributors
- Failure Scenario Combinations

Risk Levels for Selected End States

Relative Risk Drivers

- Training Manuals
- System Architecture
- Engineering Expertise
- P&IDs
- Human Error
- Common Cause

Fault Trees

- Customer Data
- Industry Databases
  - OREDA
  - ICON
  - Well Master
- NPRD db
- EPRD db
- Other Assessments

Data Analyses

Engineering Analysis is used to support success criteria, response time, etc.

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 and PRA analysts. The key to success is multi-way communication between the PRA analysts, domain experts, and management.
- A majority of PRA analysts 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 data analysts 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 and 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

Oil & Gas Examples

- **Facility Level Risk Assessment**
  - Deepwater Drilling Operation
  - Shallow Water Drilling Operation
  - Subsea Oil Production
  - Rigs and Platforms

- **System Level Risk Assessment**
  - Generic Blowout Preventer (BOP)
  - Dynamic Positioning System (DPS)
  - Mud Systems

- **Focused risk trade studies between current and proposed process/design. For example:**
  - to 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

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 need answered.

- **PRA (with the help of deterministic analyses) identifies and ranks the risk contributors, the FMEA analysts and Reliability Engineers can help solve the problem by focusing on the top risk drivers.**

Backup Charts

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 sixties (most notably on the Apollo Program) but then abandoned it and reduced quantitative risk assessment**
- **Nuclear power industry picked up the technology in early seventies and created WASH-1400 (Reactor Safety Study) in mid seventies.**
  - This is considered the first modern PRA
  - Was shelved until 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" based approach that is heavily dependent on PRA.

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, overpressurization, 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**

Common Cause Modeling

(More details and examples on this later)

- **All large PRAs of complex and redundant machines must include "common cause" effects to be complete and accurate**
- **Common Cause are those conditions that defeat the benefits of redundancy**
  - Not "single point failures"
  - Similar to "generic cause"
- **There are three recognized ways to perform common cause modeling:**
  - The Beta Model
  - The Multiple Greek Letter Model
  - The Alpha Model
- **We use an iterative approach to modeling common cause first the Beta Model approach is used and if it shows up as a risk driver a Multiple Greek Letter Model is used**
- **Generic data from NUREG/CR-5485 for the majority of the events since there are few cases where there is enough Shuttle data to develop Shuttle specific values**
  - RCS Thrusters and ECO sensors are examples of cases where Shuttle specific data is used to calculate the common cause parameters

Notional PRA Examples

JSC S&MA Analysis Branch

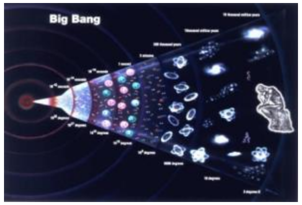
First the Math

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)

Time Perspective

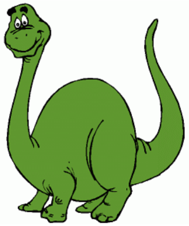


1.2 x 10^{14} hours ago

~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

Uncertainty Distribution

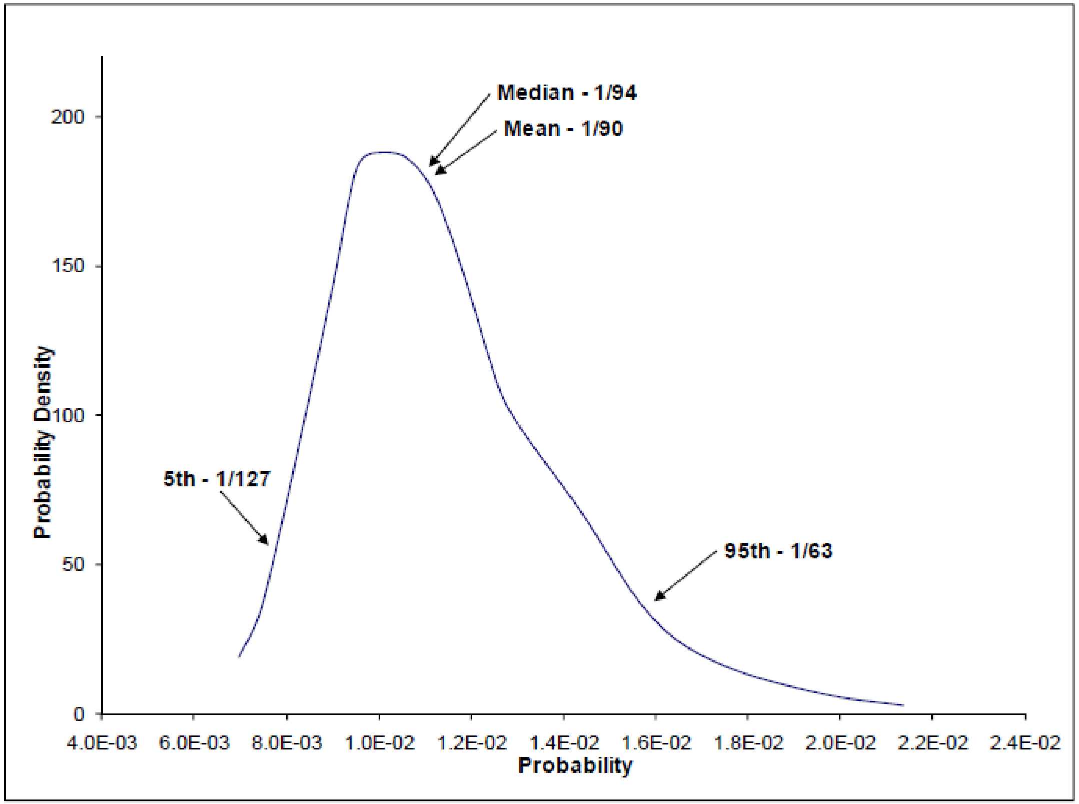
- This distribution is a representation of the uncertainty associated with a PRA's results
- The median is also referred to as the 50th percentile

Mean – 1.1E-02 (1:90)

Median – 1.1E-02 (1:94)

5th percentile – 7.9E-03 (1:127)

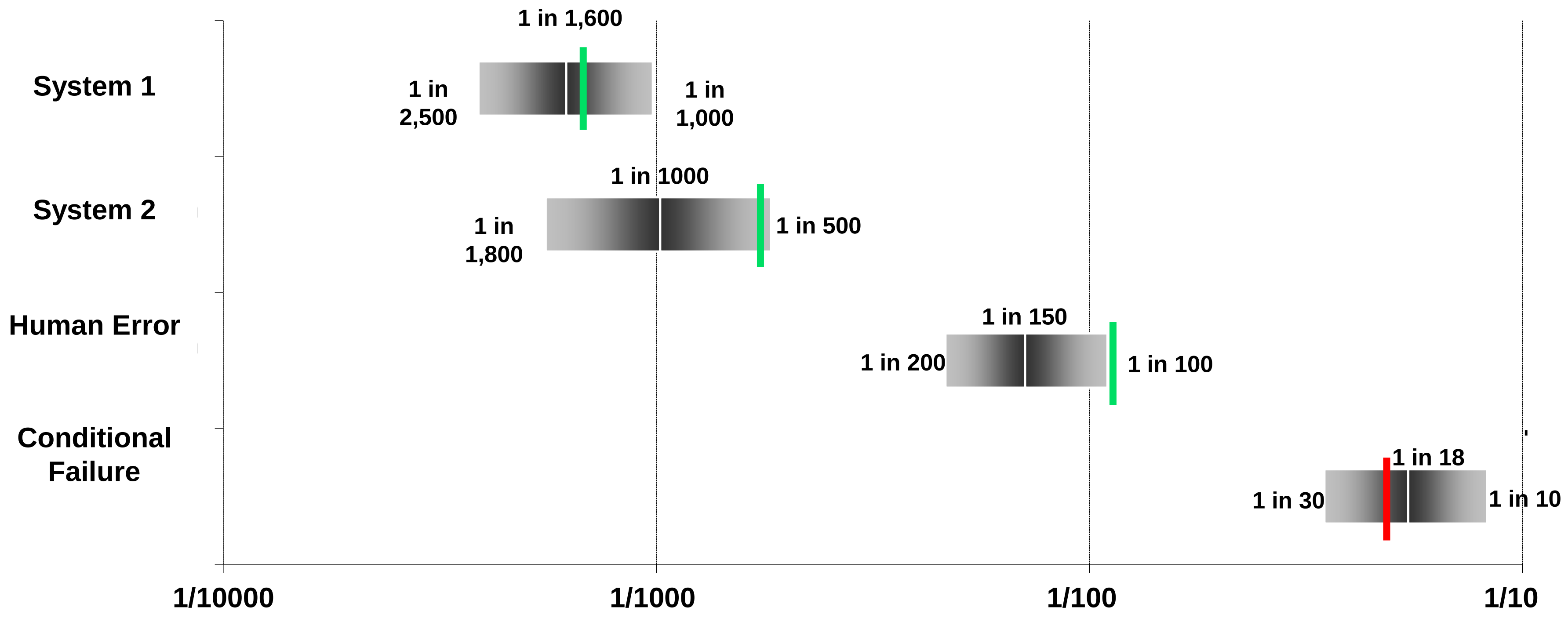
95th percentile – 1.6E-02 (1:63)



- 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.

Showing Uncertainty wrt Requirements

Notional

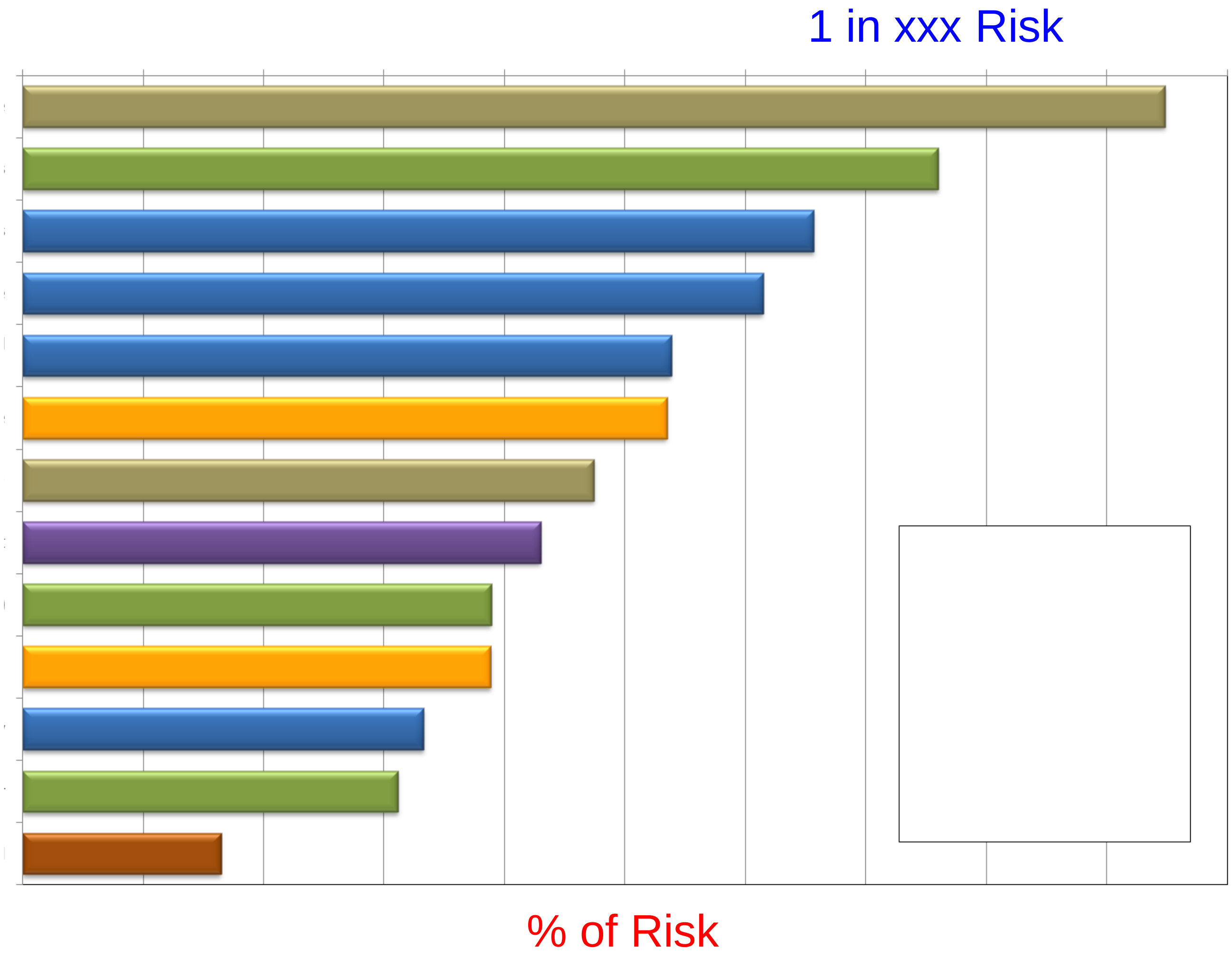


Green Bar shows Requirement Value is met
Red Bar shows Requirement Value is not met

Notional Risk Drivers via Pareto

(Top 80% of Calculated Risk)

A Pareto chart like this can be made for each project, rig, platform, etc.



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 company can live with either due to loss of life or for environmental or economic reasons
- To support Risk-Informed Decision Making (RIDM) throughout a project's life cycle from "formulation to implementation" or "concept to decommissioning"

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 a drilling rig is on a different scale than just the Blowout Preventer (BOP). However, understanding the need for a BOP can be important in its design and operation.

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.**

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.