Aramco

DEEP SPACE DEEP OCEAN

Aramco Technology and
Operational Excellence Forum

Probabilistic Risk Assessment (PRA)

How to quantify and understand risk

Presented by: Mike Stewart NASA/JSC

Short History of PRA

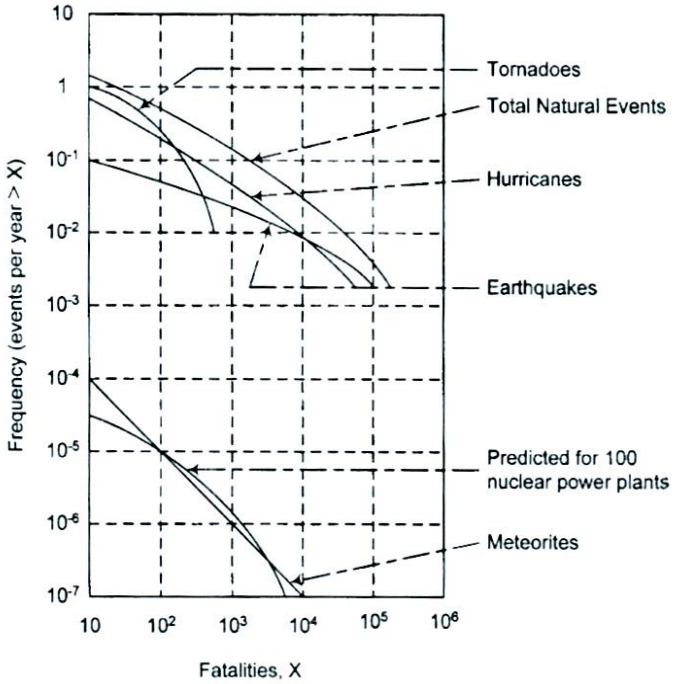
- In late fifties / early sixties Boeing and Bell Labs developed Fault Trees to evaluate launch systems for nuclear weapons
- NASA experimented with Fault Trees and some early attempts to do Probabilistic Risk Assessment (PRA) in sixties (most notably on the Apollo Program) but then abandoned / reduced 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.
  - **Since the implementation of PRA in the Nuclear industry the Capacity Factor has gone from ~50% to over 90% and risk and costs have gone down.**

Some PRA basics

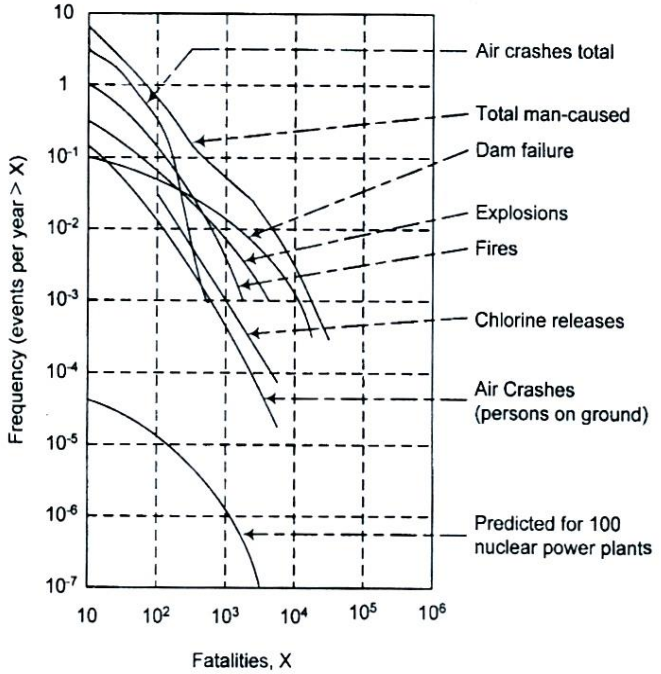
Risk = Frequency x Consequences

How to Compare Risks

Examples from the WASH 1400 Study

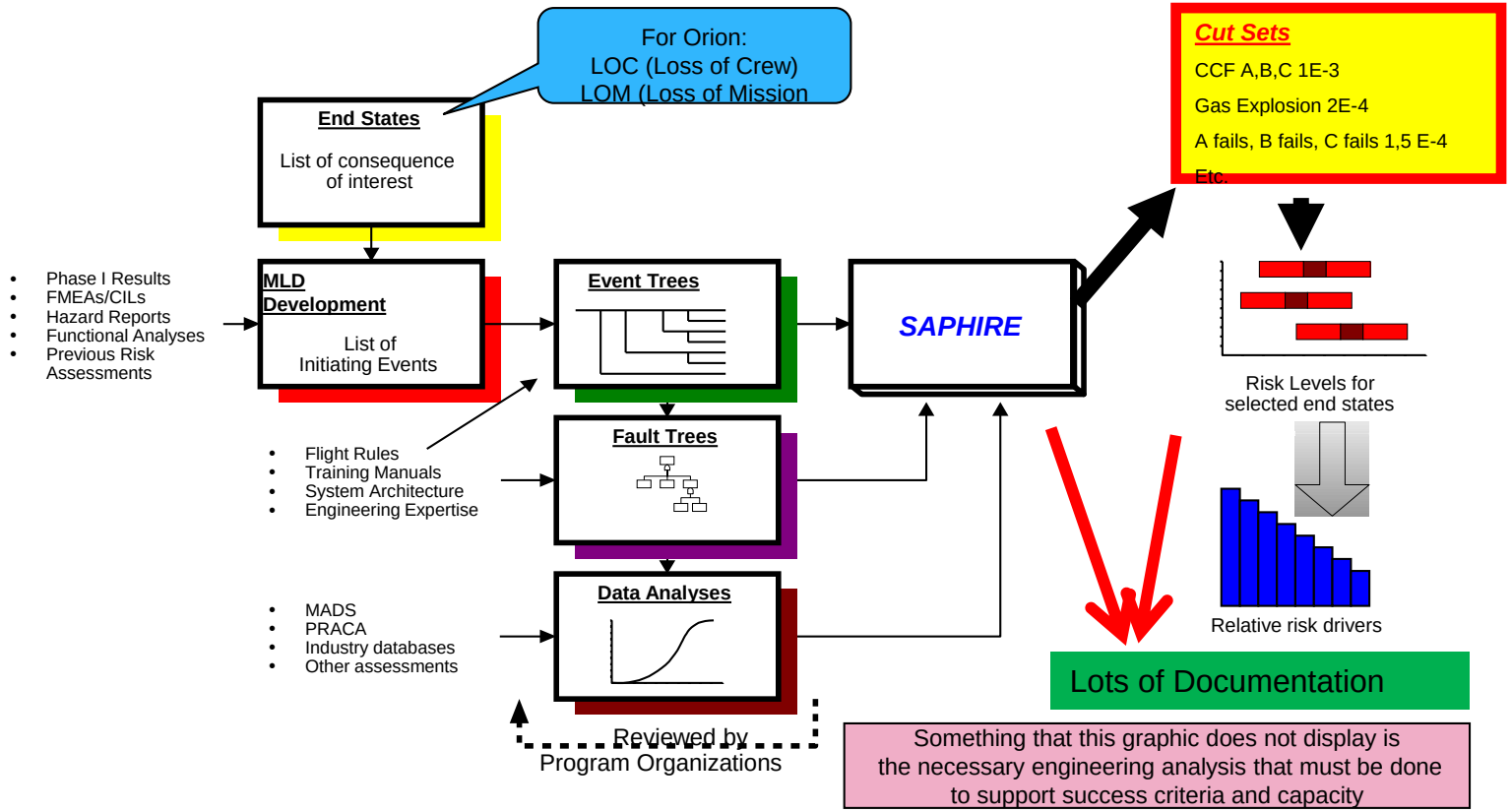


Natural Disasters



Man Made Disasters

The Big Picture



Why Do PRA Models?

- What does a PRA tell you?
  - In a large percentage of cases, the PRA tells you, or confirms for you, what you thought you already knew
    - What it also does in these cases is document in a meaningful way **why** you thought this was true
    - PRAs systematically connect design, logic, operations, Human interaction and external influences for all aspects of large complex machines/processes to detect dependencies and effects that the human mind just could not track and grasp on its own
  - In a small percentage of cases, the PRA results show something significant that you didn't know
    - In these cases you may have a false sense of understanding and in fact the PRA has pointed out something that has been overlooked **or:**
    - Your gut feel is correct and there is a problem with the way something is modeled in a PRA
  - Is the event of concern as low as you thought and are the consequences what you thought?

Why Do PRA Models? (continued)

- PRAs are used to model and quantify rare events
  - If we had 100,000 space stations operating for 40 years each with a catastrophic failure of 500 of them we could do pretty standard statistics to estimate the probability of catastrophic failure of a space station
  - However we have only one space station and it has had minimal experience and no catastrophic failures. Therefore there will rarely be any statistically significant data since it is in rare event territory.
  - They take into account external events
    - Micro-meteoroid and orbital debris (MMOD)
    - Fire, etc.
  - They take into account Human Error and Common Cause
  - They link functional dependency of systems and operations
  - They perform uncertainty analysis
  - Again**, is the event of concern as low as you thought and are the consequences what you thought?**
    - **Prior to the Challenger disaster management at NASA had estimates that such an incident would be 1 in a million to 1 in 100,000 flights.**
    - **When the Shuttle PRA was completed it showed that the Shuttle was more like 1 in 100 to 1 in 50 flights. First flight was more like 1 in 12 flights.**
    - **How about Macondo?**

Why Do PRA Models? (continued)

- Conventional Reliability Studies quantify but do not take into account Human Error and common cause or external events
- FMEAs are inductive logic and are usually not quantified and when they are they are not done in an integrated fashion
  - Bottom up not carried out to end state of concern
- Hazard reports identify potential to cause injury or damage to hardware, or environment.
  - Hazards are not quantified or integrated with each other or with the FMEA/CILs
    - Can be qualitatively evaluated
  - Controls are identified but not quantitatively evaluated
  - Hazards can only be ranked qualitatively

PRA Comparison With Other Methods

	FMEA/CIL	Hazard Analysis	PRA
Generate component failure probability/failure rate	✓		✓
Evaluate external events (MMOD, fire)		✓	✓
Identify causes	✓	✓	✓
Identify end effects	✓	✓	✓
Failure propagation logic			✓
Identify mitigation actions		✓	✓
Effectiveness of mitigations			✓
Ranking of event significance			✓
Relationships between events			✓
Comparison of dissimilar events			✓
Detailed description of events	✓	✓	✓
Details on reference documents		✓	✓
Cross-reference events	✓	✓	✓
Sensitivity study to evaluate event significance			✓
Integrated “overview”			✓
Evaluate human error		✓	✓
Evaluate common cause events			✓
Calculate uncertainty			✓

What do We do With PRA?

- Objectives – establish, **once and for all**, what is the Risk, by quantifying the likelihood and the consequences
  - Identify & evaluate risks to program/project goals to management
  - Support informed decision making with quantifiable data – not just a gut feel
  - Synchronize with other program/project processes and activities in engineering, quality-safety-mission assurance, Operations
- Products
  - Risk models
  - Probability distribution functions for end states, events, and accident scenarios
  - Operational trades and sensitivity analyses ("what if" studies)
- Types of Analysis
  - Run the Complete Model – Common End States (LOC) and Drivers
  - Focused PRA Trade – Part of model, or special model developed specific issue

Perspective

4×10^{13} hours ago

$2 \times 10^{12} – 7 \times 10^{11}$ hours ago

4×10^{8} hours ago

2.1×10^{6} hours ago

6.3×10^{5} hours ago

3.9×10^{5} hours ago

The Columbia accident (2003) occurred 1×10^{5} hours ago
A year ago was 8.76×10^{3} hours ago