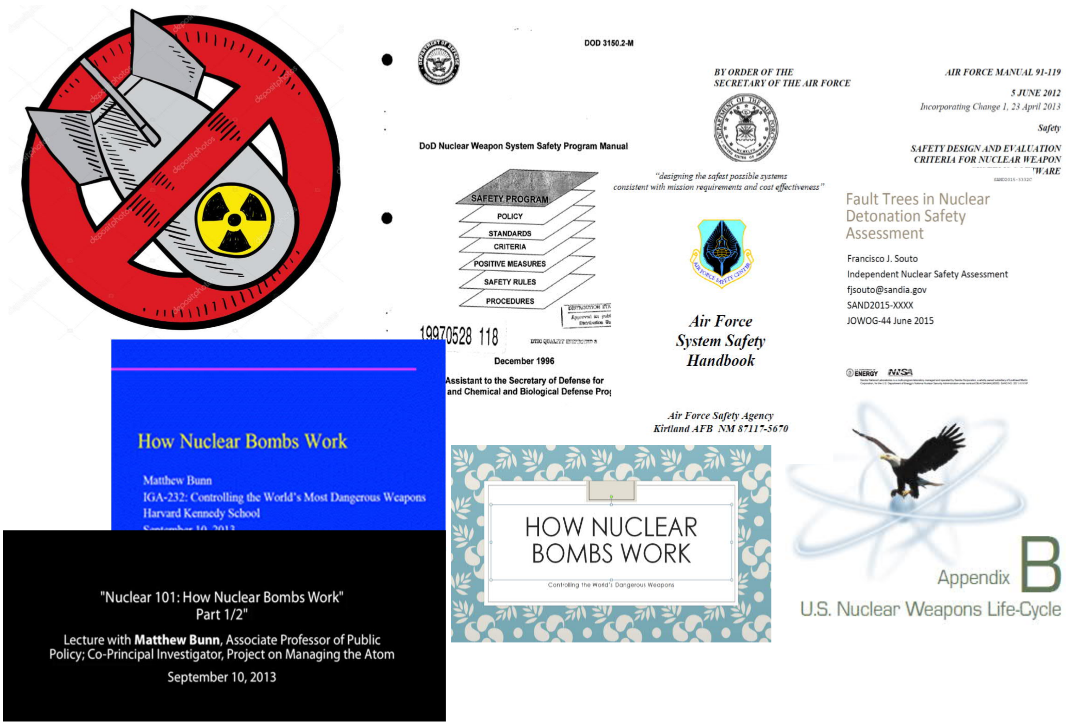
Managing Risk In Complex Engineering Systems

an application in weapon system safety assessment



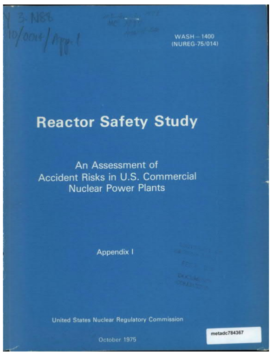
All materials are taken from public domain

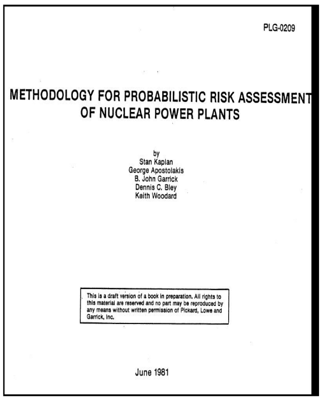
No classified materials are used

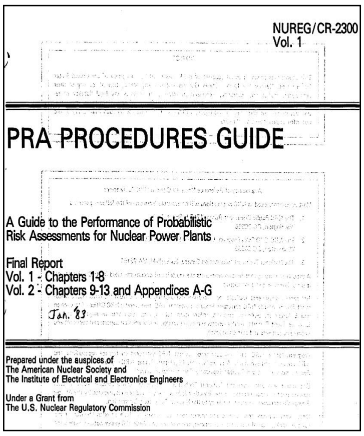
Contents

- Risk assessment 101
- Weapon system safety assessment
- How the system works
- An example – using risk assessment in assuring weapon safety

Risk Assessment 101







Since safety cannot be measured directly, we assess the risk of a system to register the “degree of unsafe”

What is "Risk"?

$$\text{Risk} = \frac{\text{Harm}}{\text{Safeguard}}$$

- There is no such thing as zero risk or zero accident, as long as harm is present – risk is never zero even by increasing safeguard
- Conceptually good but difficult to use in an assessment

Risk = Likelihood x Consequence

- Commonly used in hazard and risk analyses
- Is likelihood a probability or frequency?

Risk assessment is commonly used to prioritise accident contributors or options in cost/risk benefit analyses

Defining Risk – From ISO 31000:2009 Risk Management- Principles and Guidelines on Iimplementation; ISO 73: Risk Management - Vocabulary

- First ISO on risk management, published in Nov 2009

- Risk is defined as the

"effect of uncertainty on objectives, whether positive or negative"

- ...to be applicable and adaptable for "any public, private or community enterprise, association, group or individual"
- In order to have risk, "uncertainty" or "consequence" must be present: Without uncertainty or damage/consequence, there is no risk
- Consequence can be positive or/and negative
- Anybody can guess the extent of damage/consequence but with different levels of uncertainties – subjective?

This sounds good but what does it mean?

Which System will You Use?

- System A: catastrophic failure with a failure value of 1, once every 6 years (MTTF = 6 yrs or failure rate = 0.167/yr)
- System B: same failure value of 1, MTTF= 5 years (or failure rate = 0.2/yr)
- Using Risk = Likelihood x Consequence?

Risk is subjective and situational specific

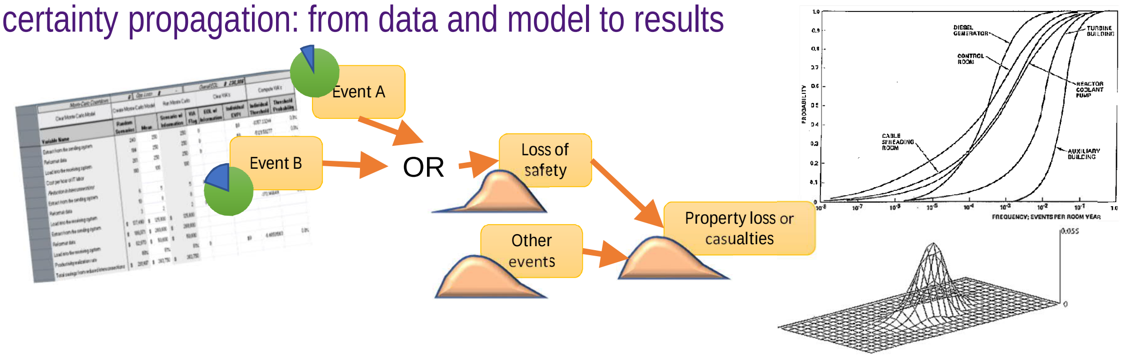
Which System will You Use?

- System A: failure value of 1, MTTF=6 yrs, λ = 0.167/yr
- System B: failure value of 1, MTTF=5 yrs, λ = 0.2/yr
- A and B have same cost, same mission life, say, 8 years
- Using Risk = Likelihood x Consequence?

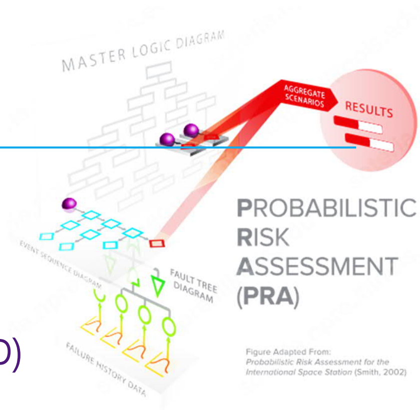
Risk is the effect of uncertainty on objectives,
whether positive or negative

Uncertainties

- Sources/ Types of uncertainties associated with a risk assessment
  - Aleatoric (Stochastic) uncertainties – nature's randomness
  - Epistemic uncertainty – lack of knowledge
    - o Modelling uncertainties
    - o Parameter uncertainties
- Subjective / Bayesian probabilities – probability is used to measure level of personal belief → uncertainties
- Uncertainty propagation: from data and model to results



Measuring Risk



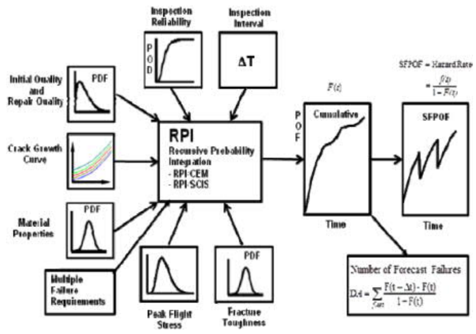
- Qualitative terms to indicate the risk level of hazards
  - Yes/No , Acceptable/ Unacceptable
  - Risk classes; e.g., (High, Medium, Low), (A, B, C, D)
- If You Can't Measure It, You Can't Improve It
  - Quantitative Risk Assessments (QRA) use numerical values to register risks; e.g., 4.3 x 10-6 death/yr
  - In Probabilistic Risk Assessments (PRA), numbers are represented by probabilistic distributions and uncertainties are explicitly addressed
- QRA and PRA are extensively used in risk assessments of complex engineering systems

The numbers in risk assessments are mainly
for risk prioritisation and comparison

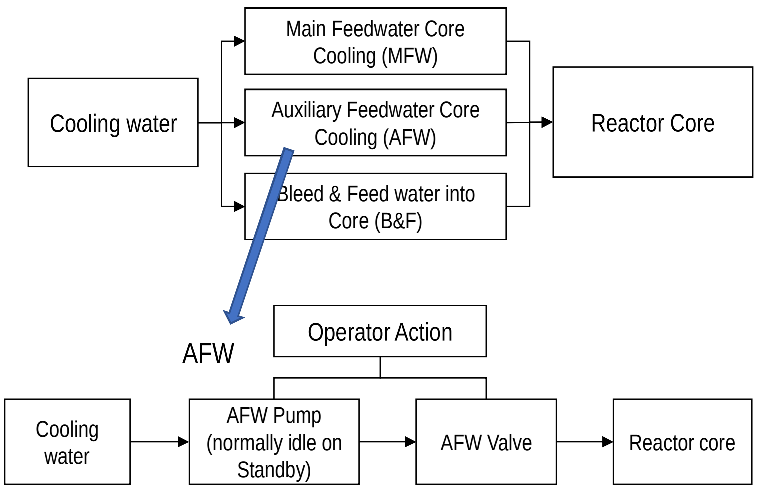
Quantitative Definition of Risk

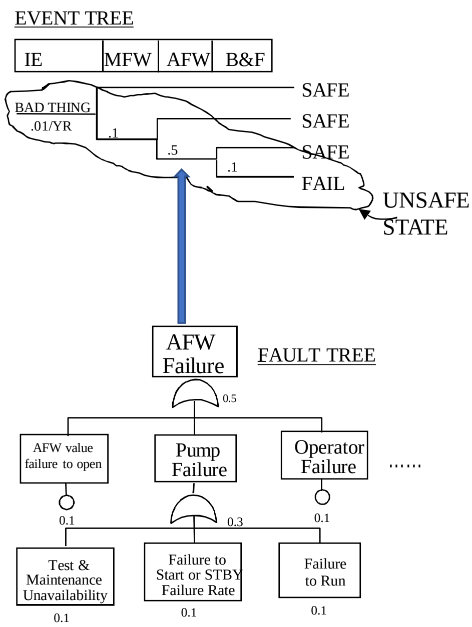
- In general, risk analysis is used to answer:
  - What can go wrong?
  - What are the damage effects?
  - How likely is it that this will happen?
  - What are the uncertainties?
- Thus, risk can be thought to be consisting of :
  - Scenarios or accident sequences
  - Consequence
  - Likelihood / Uncertainties
- Risk = Σ {<s_i, C_i, L_i,>}
- Common tools in a PRA
  - Event tree analysis
  - Fault tree analysis

Scenario	Likelihood	Consequence
s_1	L_1	C_1
s_2	L_2	C_2
s_3	L_3	C_3
.	.	.
.	.	.
.	.	.
.	.	.
.	.	.
s_N	L_N	C_N



1-minute PRA - System Modeling



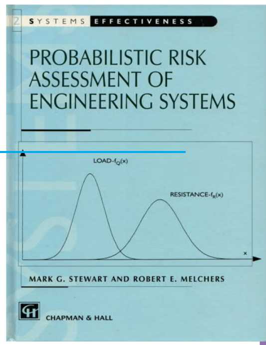


Fail Path Frequency

Bad Thing X MFW X AFW X B&F

.01/YR X .1 X .5 X .1 = $5X10^{-5}$/YR

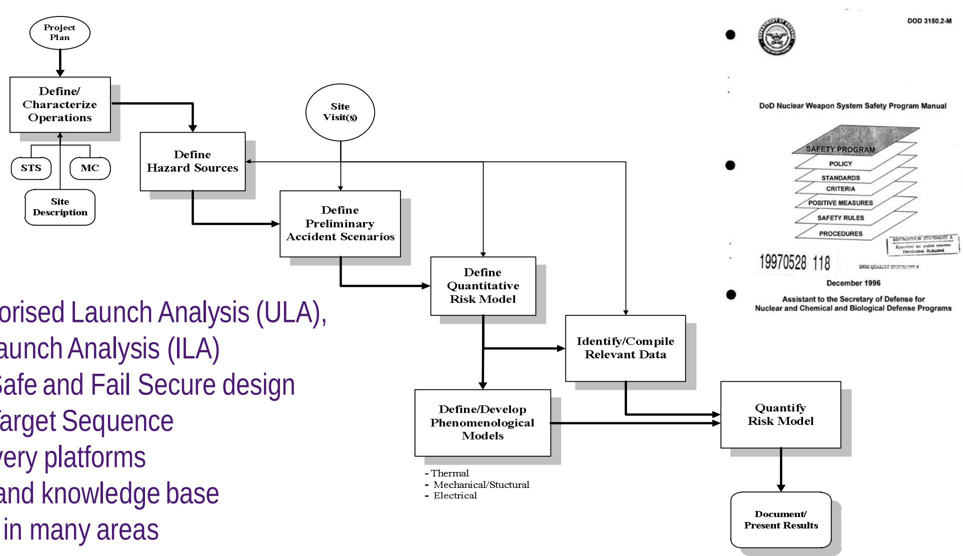
PRA for Engineering Systems



- PRA has been used extensively for high risk systems where failure data are limited
  - Physical and mathematical models
  - System safety analysis, O&SHA, FMECA, HAZAOP, etc.
  - Human action analysis, human error rate
  - Bayesian data update, expert opinion, knowledge modelling
  - External events: Fire, earthquake, flooding, volcano, tsunami, tornado, etc..
- Typical applications are systems with a steady state, e.g., power plants, airplanes, oil platform operations, etc.

How to assess the risk of a weapon that takes on different states and delivery platforms?

Weapon System Safety Assessment



- PRA, Unauthorised Launch Analysis (ULA), inadvertent Launch Analysis (ILA)
- Unique Fail-Safe and Fail Secure design
- Stockpile to Target Sequence
- Different delivery platforms
- Limited data and knowledge base
- Uncertainties in many areas
- Different damage states

Ho, V. S., et al., "The Application of Probabilistic Safety Assessment Techniques in a Nuclear Weapon System Safety Assessment," Probabilistic Safety Assessment and Management Conference III

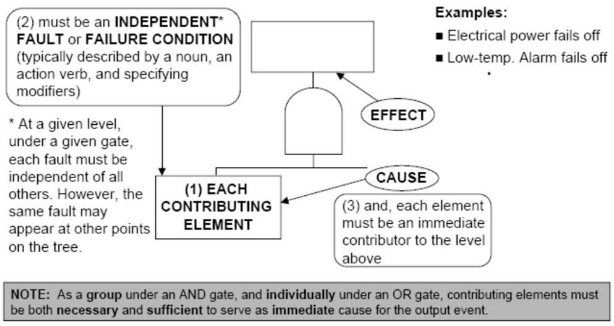
Need to understand Stockpile to Target Sequence

An Example – Using Risk Assessment In Assuring Weapon Safety

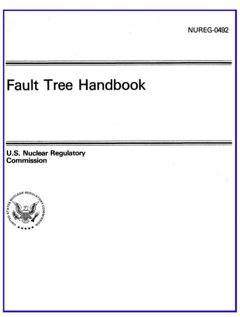
- Consider the design of a LA as a normally open switch that closes when the proper acceleration signals are received
- Once the LA switch is closed, it allows signals from power sources (e.g., batteries) to pass to other components (e.g., capacitors)
- The LA switch can be considered a normal environment safety component (i.e., with a failure probability < 10^{-3} per weapon lifetime)
- From the nuclear safety perspective, the LA switch has to remain open and close exclusively on demand (i.e., when proper acceleration is experienced)

Fault tree analysis is an ideal tool to show compliance with these quantitative probabilistic requirements

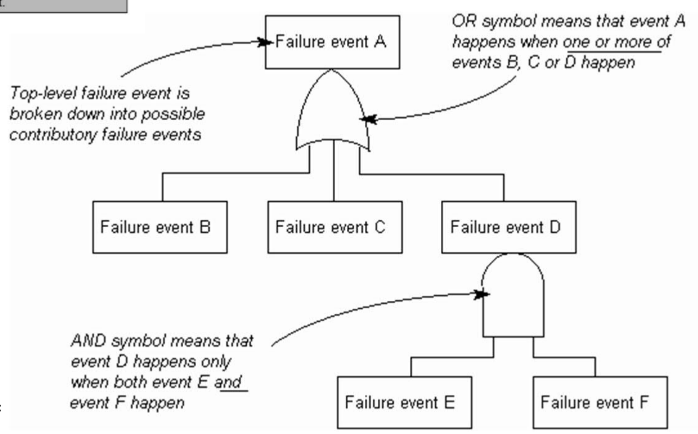
Fault Tree Analysis



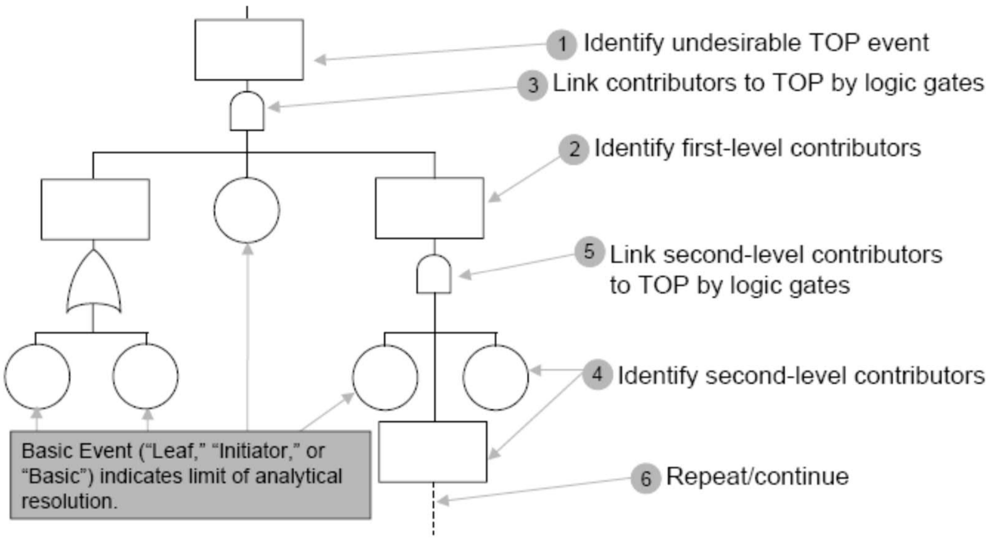
Fault trees use deductive logic



http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0492/sr0492.pdf



Fault Tree Construction



Top Event = LA Switch is closed inadvertently

- Undesirable effect = LA Switch is closed inadvertently
- For nuclear safety, the LA switch has to remain open until receiving the correct signal to close (i.e., correct acceleration). It can fail due to any of the following:
  - G1=LA switch installed in the closed position. The LA switch is tested for normal operation and is left inadvertently in the closed position (e.g., human errors)
  - G2=LA switch malfunctions and inadvertently closes. Many faults can result in closing inadvertently the LA switch (e.g., internal contamination between the normally open contacts)
  - G3=LA switch experiences an unintended launch. The LA switch is designed to close at launch conditions

How to safeguard against G1?

G1=LA switch installed in the closed position

- To mitigate G1 risk, design engineers propose two independent methods to verify that the LA switch is not installed closed (i.e., it is in the open position)

Proposed LA Switch (Open)

Proposed LA Switch (Closed)

- One method is by electrically testing that the contacts in the LA switch are open
- The second method is by radiographically observing that the contacts in the LA switch are open

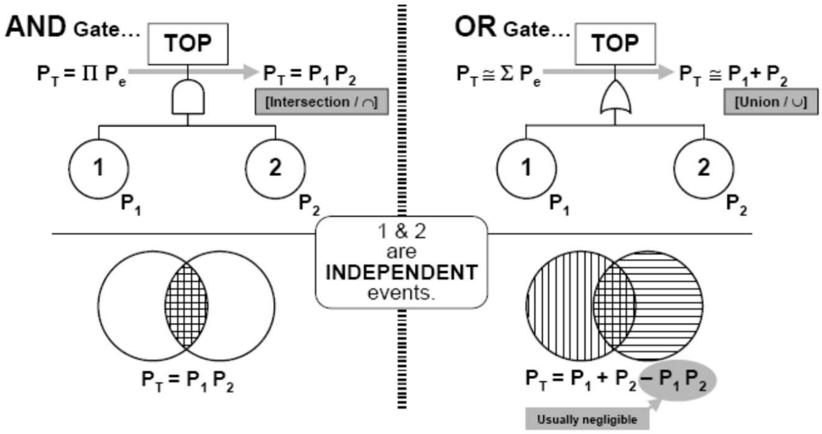
Engineers ended up using both methods

How G1 occurs?

- G1=LA switch installed in the closed position. This failure mode can occur only when both measures failed
  - G4=Reset Monitor (RM) electrical verification fails. The RM contacts should be closed when the LA switch contacts are open
  - G5=Radiographic verification fails. Radiography of the high-density piston should show that the piston is in the proper position for the LA switch contacts to be open

Fault Tree Calculations

- Fault trees are quantified to assess the probability of top events

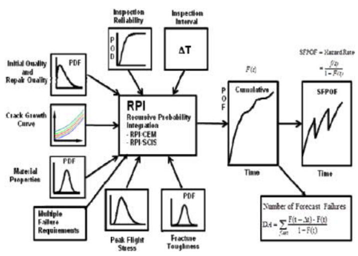


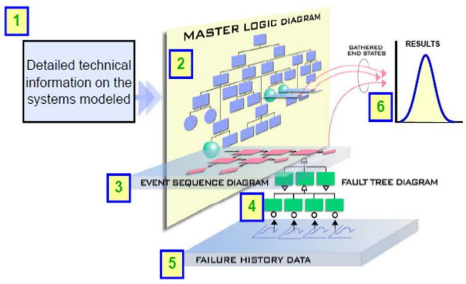
- Design modification would be required if the failure probability of a subsystem or system does not meet the design criteria. This cannot the done unless you can quantify the risk

Where does uncertainty fits in?

Weapon WSSA

- Other risk tools such as event tree analysis, human error analysis, consequence modeling, external event analysis, Bayesian data analysis, security assessment, etc., would be used to build up the overall risk model
- The processes repeat until all reasonably foreseeable failures have been identified and modeled, for all subsystems, systems, key elements of each weapon/mod, for each platform, on each STS….
- Component failure and human error data exist from military and commercial nuclear power plants databases





Summary

- Uncertainties drive risks
- Logical tools model failures and system interactions
- Risk is the effect of uncertainty on objective
- Quantify risk to check design criteria compliance or compare options
- Reduce risk to improve system safety
- Risk assessments are never simple

... Conducted a risk assessment would not make a system safer, but taking reasonably practicable risk control actions would

END

A Scholarship for HK Students Studying Risk Engineering at UCLA

Dr Vincent Ho Scholarship for Risk Management

Thank you for your time