Introduction To Risk Assessment Concepts, Tools, and Techniques

(This tutorial is designed to provide an introductory level overview of risk assessment tools and techniques)

Fayssal M. Safie, Ph.D.
Reliability and Maintainability Engineering Technical Fellow
MSFC/QD01

RAM 8 Training Summit, Huntsville, AL
November 3rd, 2015

Agenda

- **Introductory Material**
  - Definitions
  - Probability Basics
- **Risk Assessment Tools and Techniques**
  - Risk Matrix
  - Probabilistic Risk Assessment (PRA)
  - Fault Tree Analysis (FTA)
  - Event Sequence Diagram (ESD)
  - Event Tree Analysis (ETA)
  - Bayesian Analysis
- **Risk Assessment Related Tools and Techniques**
  - Hazard Analysis, Failure Modes and Effects Analysis/Critical Items List (FMEA/CIL), Reliability Predictions, Reliability Demonstration, and Ishikawa Chart (Cause and Effect Diagram)
- **References**
- **Concluding Remarks**

Introductory Material – Definitions

Reliability Engineering

- **Reliability engineering** is a design function that involves the application of engineering principles to the design and processing of products, both hardware and software, for the purpose of meeting product reliability requirements or goals.
- **Reliability as a figure of merit** is the probability that an item will perform its intended function for a specified mission profile.

Safety

- Safety
  - Safety is the freedom from those hazards that can cause death, injury, or illness in humans or adversely affect the environment.
- System Safety (NASA/SP-2010-580, NASA System Safety Handbook)
  - System safety is the application of engineering and management principles, criteria, and techniques to optimize safety and reduce risks within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle.
  - System safety to safety is as system engineering to engineering.

Risk Assessment

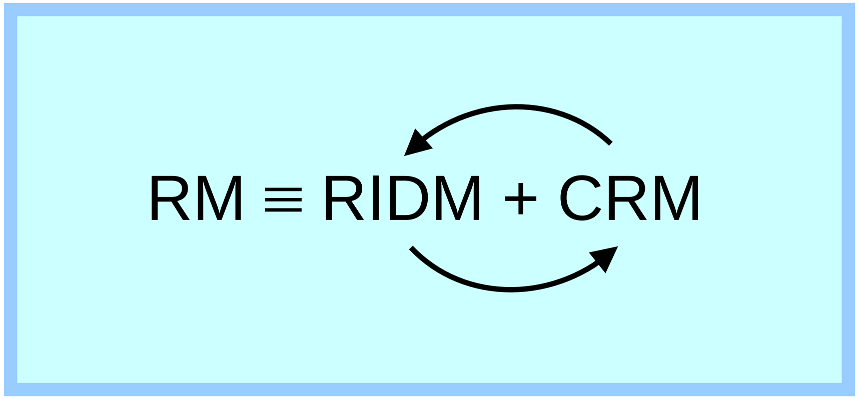
- **Risk assessment** is the process of determining the magnitude and consequences of risk.
- Risk is the uncertainty regarding the future outcome of an undertaking of some kind, e.g., a decision alternative, a project, a launch, etc.
- In the context of mission execution, risk is the expression of the potential for shortfalls related to any one or more of the mission execution domains (i. e. Safety, Technical performance, Cost, and Schedule).
- Risk is defined as a set of triplets:
  - The scenario leading to a shortfall with respect to one or more Performance Measures (e.g., scenarios leading to injury, fatality, destruction of key assets; scenarios leading to exceedance of mass limits; scenarios leading to cost overruns; scenarios leading to schedule slippage)
  - The likelihood of the scenario (Quantitative/Qualitative).
  - The consequences (severity) of the performance degradation that would result if the scenario was to occur.

Risk Management

- In general, risk management is the systematic and iterative optimization of the project resources according to a risk management policy.
  - The risk management process consists of:
    - Defining a risk management policy
    - Identification and assessment of risks
    - Determining risk mitigation and control
    - Monitoring, communication, and acceptance of risks.

Risk Management

- NPR 8000.4A, NASA Risk Management Procedural Requirements, involves two complementary processes:
  - ○ Risk-informed Decision Making (RIDM)
    - To risk-inform direction-setting decisions (alternative selection).
    - To risk-inform the development of credible performance requirements as part of the overall systems engineering process.
  - ○ Continuous Risk Management (CRM)
    - To manage risk associated with the implementation of baseline performance requirements.



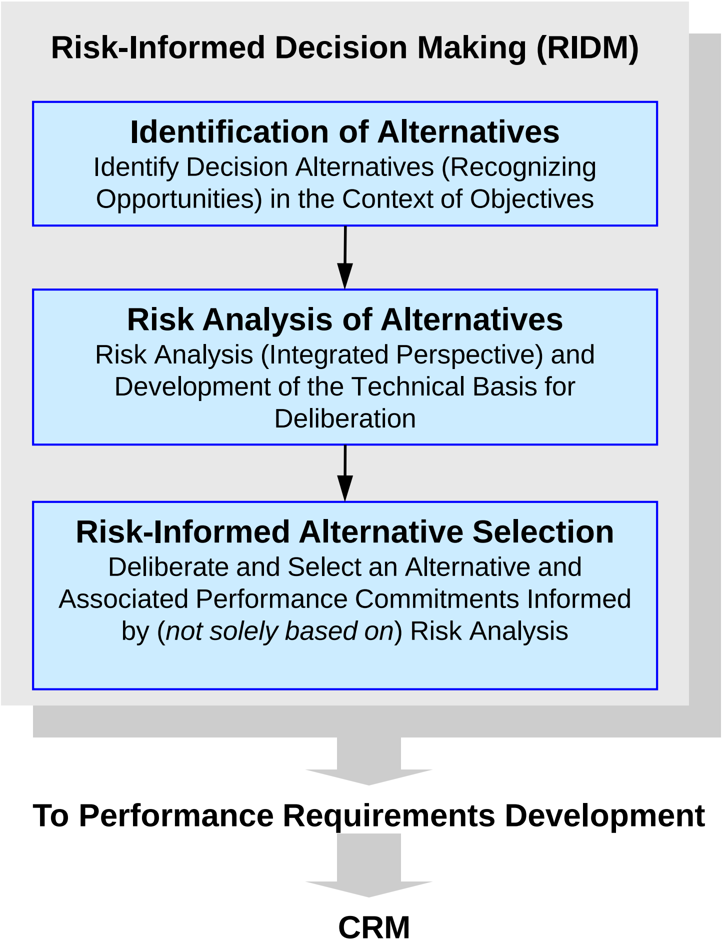
RM ≡ RIDM + CRM

The RIDM Process

- Identification of decision alternatives (*decision context*) and considering a sufficient number and diversity of Performance Measures.

- *Risk analysis* of decision alternatives (uncertainty analysis of performance associated with the alternative).

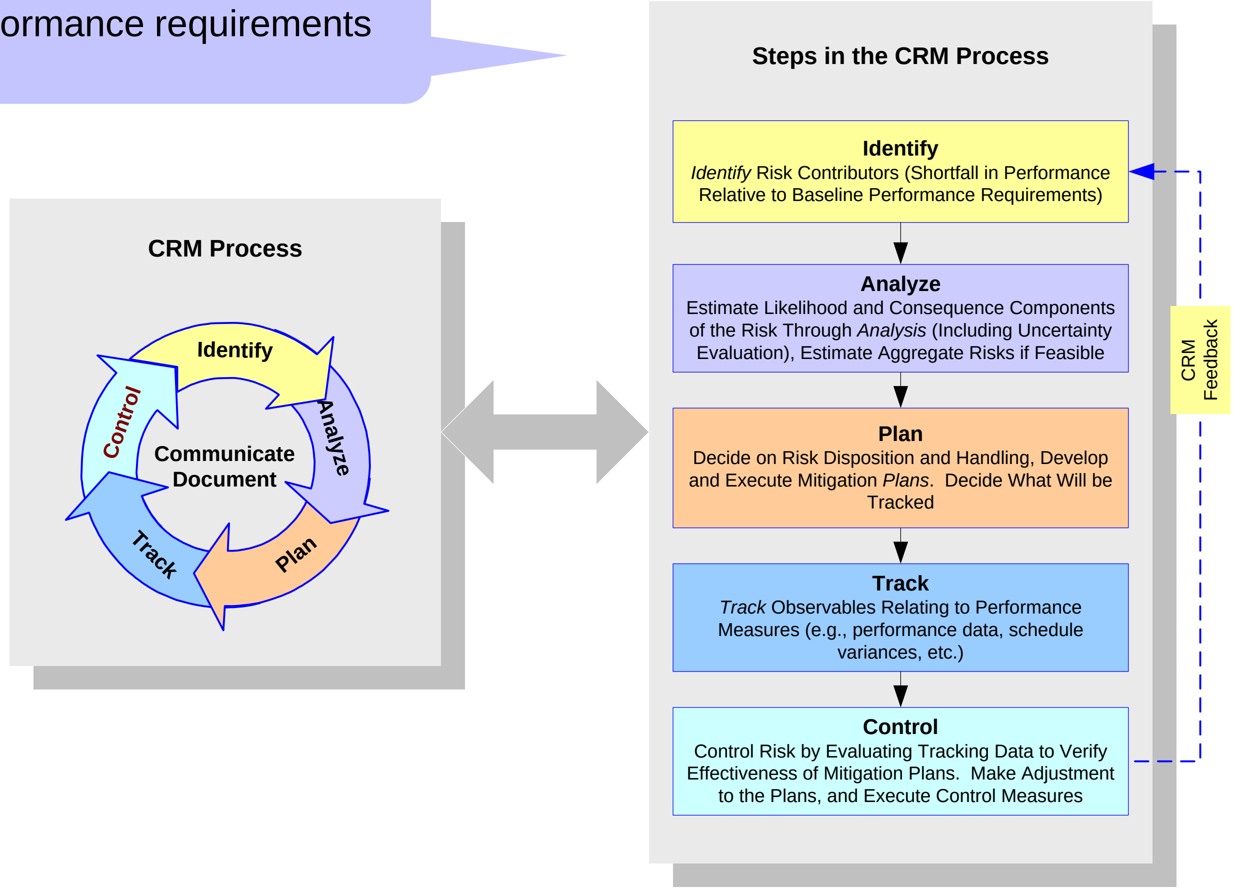
- *Deliberation and Selection* of a decision alternative *informed by* (not solely based on) Risk Analysis Results.



Risk-Informed Decision Making (RIDM)
Identification of Alternatives
Identify Decision Alternatives (Recognizing Opportunities) in the Context of Objectives
Risk Analysis of Alternatives
Risk Analysis (Integrated Perspective) and Development of the Technical Basis for Deliberation
Risk-Informed Alternative Selection
Deliberate and Select an Alternative and Associated Performance Commitments Informed by (*not solely based on*) Risk Analysis
To Performance Requirements Development
CRM

The Continuous Risk Management (CRM) Process

CRM is conducted in the context of performance requirements



Steps in the CRM Process

Identify
Identify Risk Contributors (Shortfall in Performance Relative to Baseline Performance Requirements)

Analyze
Estimate Likelihood and Consequence Components of the Risk Through *Analysis* (Including Uncertainty Evaluation), Estimate Aggregate Risks if Feasible

Plan
Decide on Risk Disposition and Handling, Develop and Execute Mitigation *Plans*. Decide What Will be Tracked

Track
Track Observables Relating to Performance Measures (e.g., performance data, schedule variances, etc.)

Control
Control Risk by Evaluating Tracking Data to Verify Effectiveness of Mitigation Plans. Make Adjustment to the Plans, and Execute Control Measures

Introductory Material - Probability Basics

Probability

- The probability of an event A is a quantity that satisfies the following axioms (Kolmogorov, 1933):

  $0 \leq Pr(A) \leq 1$

  $Pr(\text{certain event}) = 1$

- Imagine a large number (n) of repetitions of the "experiment" in which A is a possible outcome.
- If A occurs k times, then its relative frequency is: k/n.
- It is postulated that:
  lim k/n when $n \rightarrow \infty$ is Pr(A).
- In terms of Bayesian statistics, probability is defined as "Degree of Belief"

Probability Basic Rules

- The sum of the probabilities that an event will occur plus the probability that an event will not occur is equal to 1.

$$P(A) + P(\text{not } A) = 1$$

Example: The probability of rolling an even or an odd number on a fair die is 1.

Probability Basic Rules

- If two events can’t occur at the same time, they are called mutually exclusive events. The probability of either one event or the other event happening is equal to the sum of the probabilities of the individual events.

$$P(X \text{ or } Y) = P(X)+P(Y)$$

Probability Basic Rules

- If two events can happen at the same time, the probability of either event happening is equal to the sum of the probabilities of the individual events minus the probability of both events occurring simultaneously.

$$P(X \text{ or } Y) = P(X) + P(Y) – P(X \text{ and } Y)$$

  - If the two events are independent, the probability of both events occurring is equal to:

$$P(X \text{ and } Y) = P(X) * P(Y)$$

  - If the two events are dependent, the probability of both events happening consecutively is equal to:

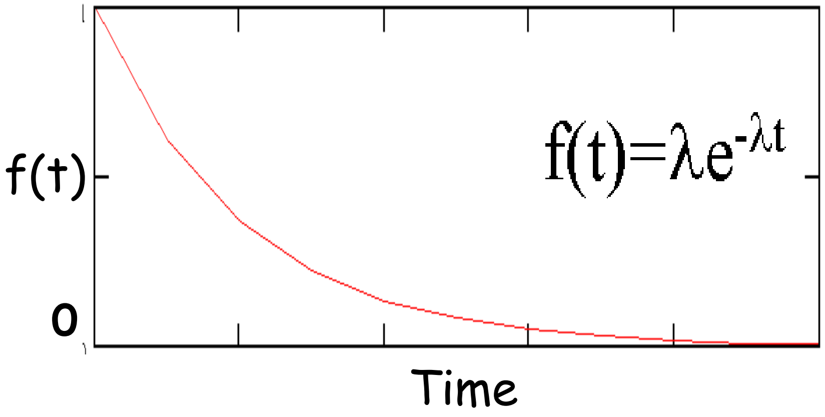
$$P(X \text{ and } Y) = P(X) * P(Y/X)$$

Where P(Y/X) is the conditional probability of Y given that X has already occurred.

Probability Related Functions (Using Exponential for Illustration)

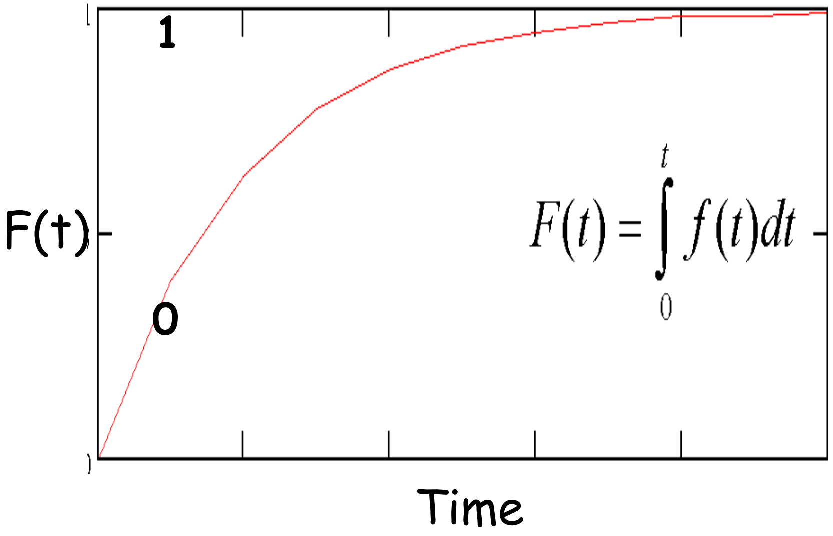
Probability Density Function, f(t)

- It describes where failures occur over time.
- The area under curve is always = 1.



Cumulative Density Function, F(t)

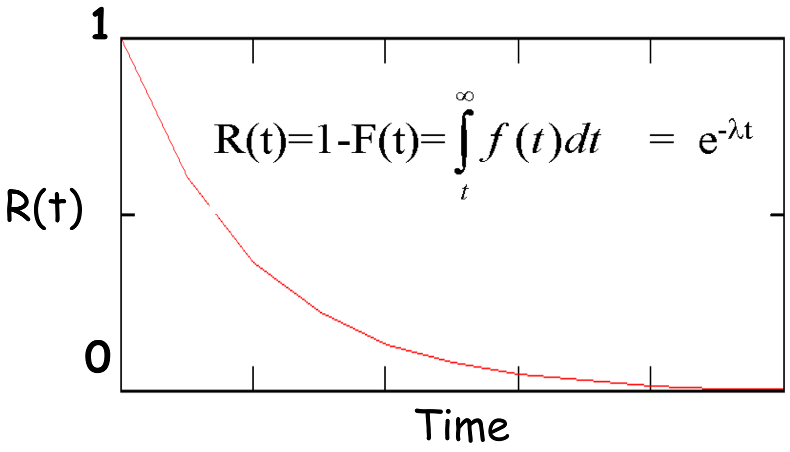
- It displays the percentage of the population that has failed at some specific time “t”.
- It ranges between 0 and 1 and equals the area under the f(t) curve up to time “t”.



Probability Related Functions (Using Exponential for Illustration)

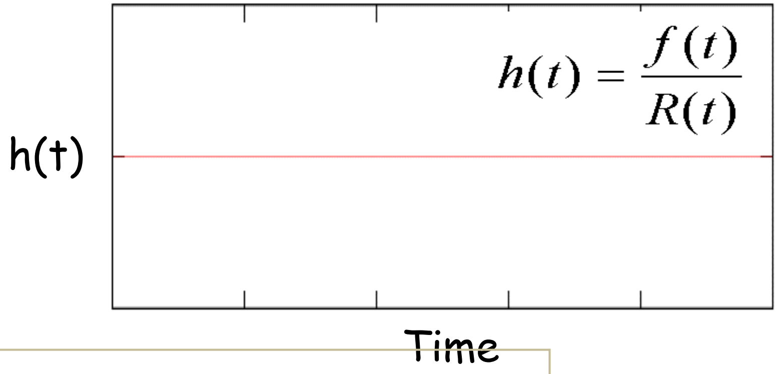
Reliability Function, R(t)

- For a given t, it represents the percentage that has survived to that point.
- Is always between 0 and 1.
- R(t)=1-F(t)



Hazard Function

- h(t) is the instantaneous failure rate at time t.
- h(t)=f(t)/(1-F(t))



Other general relationships

$$R(t) = e^{-\int_{-\infty}^{t} h(t)dt} \qquad MTTF = \int_0^\infty R(t)dt$$

Risk Assessment Tools and Techniques

The Risk Matrix

- Purpose:
  - Sort through a large amount of risks and determine which are most important.
  - Separate out which risks should be dealt with first (the vital few risks) when allocating resources.
- Description:
  - Involves partitioning risks or groups of risks and ranking risks or sets of risks based upon a criterion or set of criteria.
  - Ranking should yield the project's "Primary Risks."
  - NPR 8000.4, Agency Risk Management Procedural Requirements, defines a Primary Risk as those undesirable events (risks) having both high probability and high impact/severity.
  - Characterization of a Primary Risk as "Acceptable" shall be supported by rationale, with concurrence of the Governing Program Management Council (GPMC), that all reasonable mitigation options within cost, schedule, and technical constraints have been instituted.

Standardized Agency 5x5 Risk Matrix

LIKELIHOOD		1 Very Low	2 Low	3 Moderate	4 High	5 Very High
Very Likely	5	🟩	🟨	🟥	🟥	🟥
High	4	🟩	🟨	🟨	🟥	🟥
Moderate	3	🟩	🟨	🟨	🟨	🟥
Low	2	🟩	🟩	🟩	🟨	🟨
Very Low	1	🟩	🟩	🟩	🟩	🟨

CONSEQUENCES

Criticality

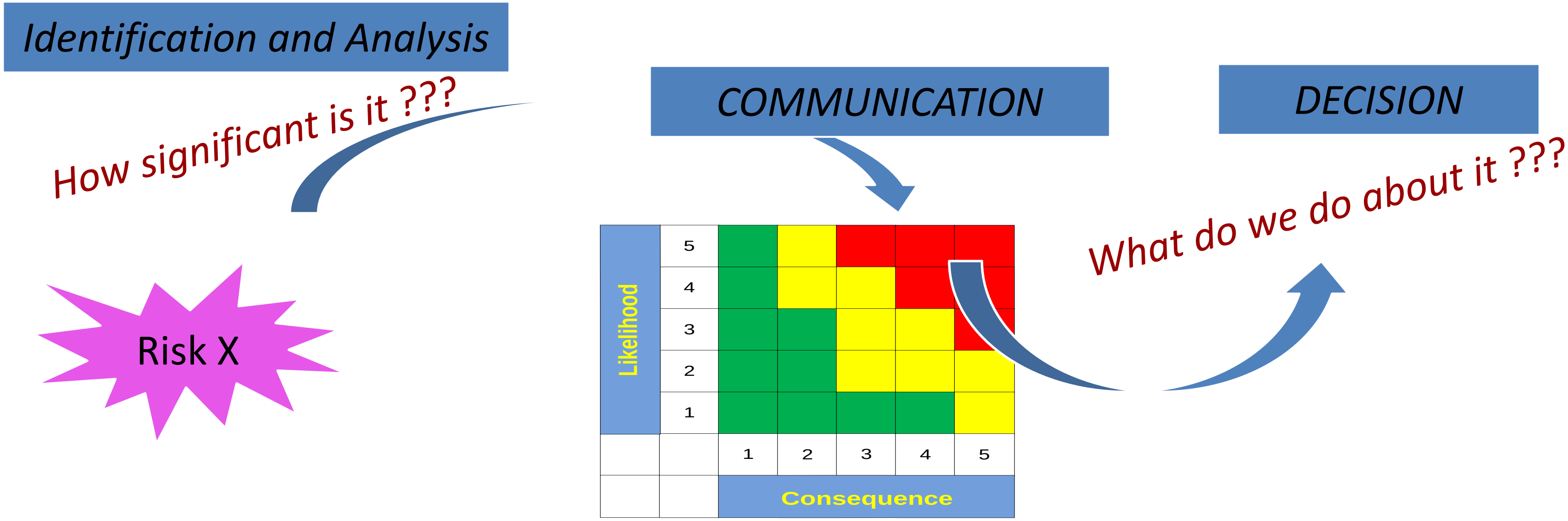
🟥 High	Primary Risks
🟨 Med	
🟩 Low	

NOTE: Specific criteria for each of the Likelihood and Consequence categories are to be defined by each Enterprise or Program. Criteria may be different for manned missions, expendable launch vehicle missions, robotic missions, etc.

Risk Matrix is a Communication Tool

Risk communication:

- Risk communication is the data exchange on risks necessary for decision making on a project.
- Risk communication is supported by project reporting lines.
- The type of decision determines the contents and format of risk data addressed to the decision-maker.



Identification and Analysis

COMMUNICATION

DECISION

Likelihood						
	5	🟩	🟨	🟥	🟥	🟥
	4	🟩	🟨	🟨	🟥	🟥
	3	🟩	🟩	🟨	🟨	🟥
	2	🟩	🟩	🟨	🟨	🟨
	1	🟩	🟩	🟩	🟩	🟨
		1	2	3	4	5
		Consequence				

Risk Matrix

- Advantages
  - The risk matrix is a risk assessment communication tool.
  - The risk matrix provides a useful guide for prudent engineering.
  - The risk matrix provides a standard tool of treating the relationship between severity and probability in assessing risk for a given hazard.
  - Assessing risk subjectively avoids unknowingly accepting intolerable and senseless risk, allows operating decisions to be made, and improves resource distribution for mitigation of loss resources.
- Limitations
  - The risk assessment matrix does not assist the analyst in identifying hazards. It can only be used if hazards are already identified and analyzed.
  - The risk assessment matrix is dominated by subjective information.

Probabilistic Risk Assessment (PRA)

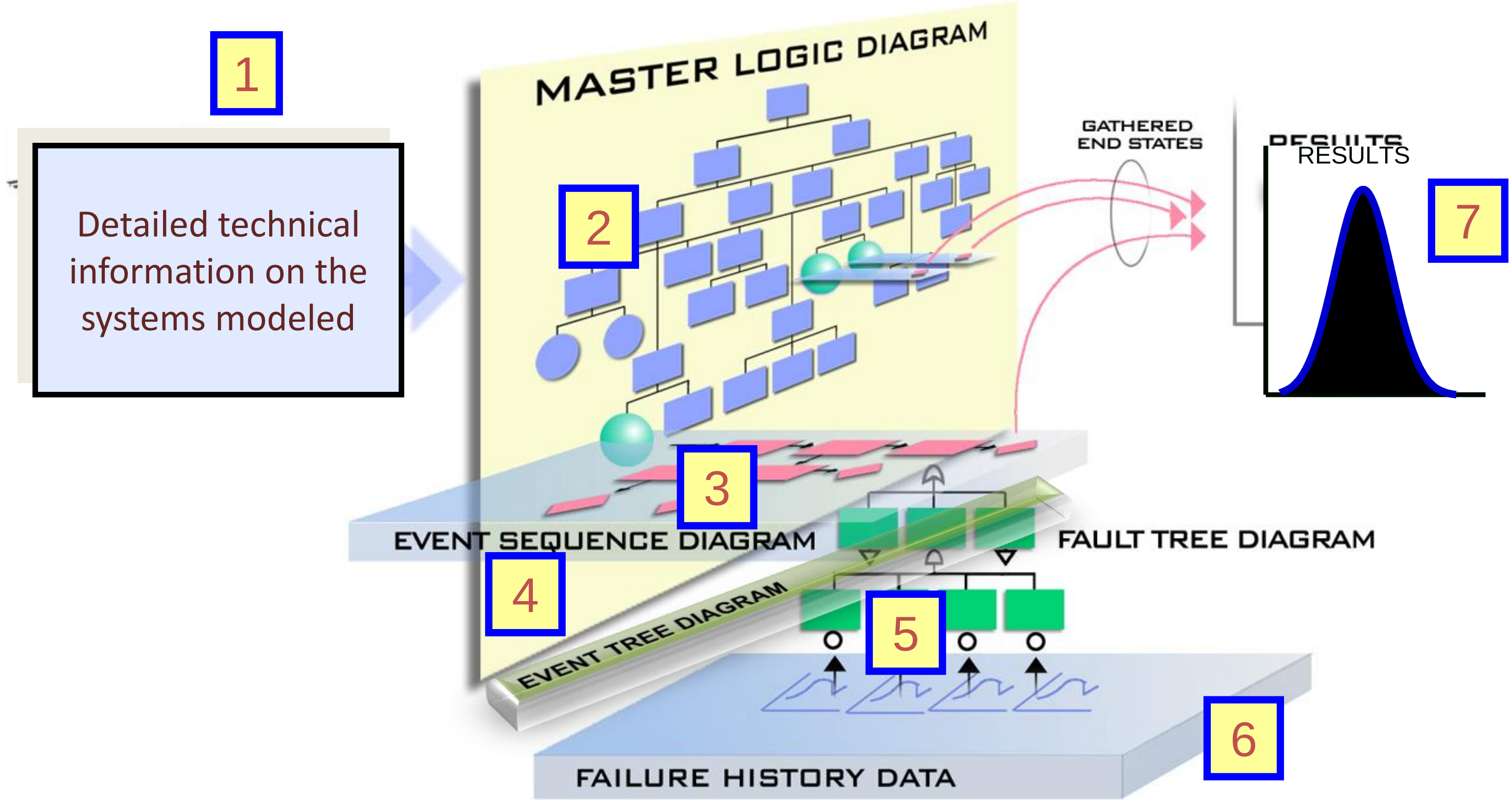
- Probabilistic risk assessment is the systematic process of analyzing a system, a process, or an activity to answer three basic questions:
  - What can go wrong that would lead to loss or degraded performance (i.e., scenarios involving undesired consequences of interest)?
  - How likely is it (probabilities)?
  - What is the severity of the degradation (consequences)?
- PRA is the task of generating the triplet set:

$$R \equiv \text{RISK} \equiv \{S_i, P_i, C_i\}$$

Scenario	Likelihood (Probability)	Consequence
S_1 S_2 S_3 . . . S_N	p_1 p_2 p_3 . . . p_N	C_1 C_2 C_3 . . . C_N

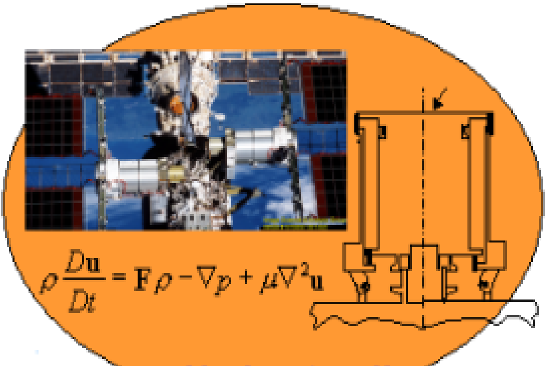
- **Probabilistic risk assessment is a formal method to derive and quantify this set in an *integrated* manner.**
- **This provides a framework to prioritize risks, identify risk contributors, and quantify cumulative (aggregate) risk and associated uncertainties.**

Probabilistic Risk Assessment (PRA)
The PRA Process

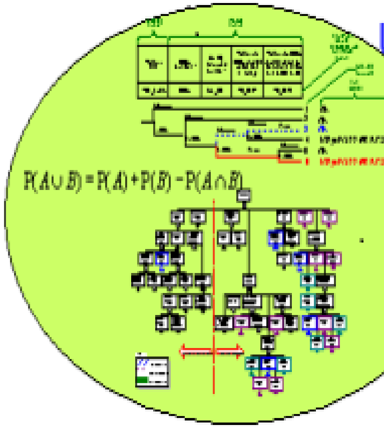


Detailed technical information on the systems modeled

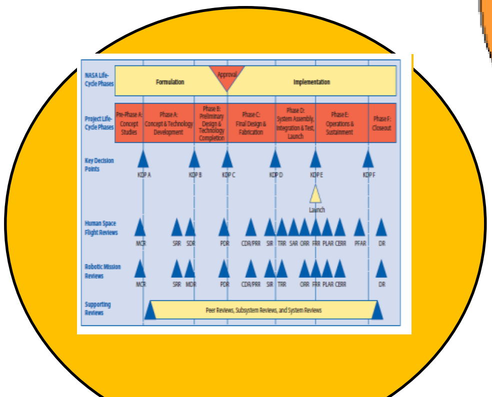
Probabilistic Risk Assessment (PRA) The Skills Needed



Understanding Engineering Science

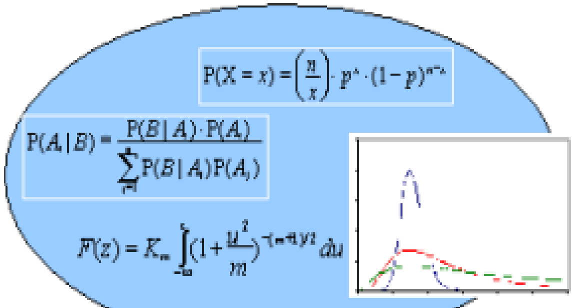


Understanding the Art and Science of Logical Structures



NASA Life-Cycle Phases
Formulation
Approval
Implementation
Project Life-Cycle Phases
Pre-Phase A: Concept Studies
Phase A: Concept & Technology Development
Phase B: Preliminary Design & Technology Completion
Phase C: Final Design & Fabrication
Phase D: System Assembly, Integration & Test, Launch
Phase E: Operations & Sustainment
Phase F: Closeout
Key Decision Points
KDP A
KDP B
KDP C
KDP D
KDP E
KDP F
Launch
Human Space Flight Reviews
MCR
SRR
SDR
PDR
CDR/PRR
SIR
TRR
SAR
ORR
FRR
PLAR
CERR
PFAR
DR
Robotic Mission Reviews
MCR
SRR
MDR
PDR
CDR/PRR
SIR
TRR
ORR
FRR
PLAR
CERR
DR
Supporting Reviews
Peer Reviews, Subsystem Reviews, and System Reviews

Understanding Systems Engineering



$P(X = x) = \binom{n}{x} \cdot p^x \cdot (1-p)^{n-x}$
$P(A_i | B) = \frac{P(B | A_i) \cdot P(A_i)}{\sum_{j=1}^{n} P(B | A_j) P(A_j)}$
$F(z) = K_m \int_{-\infty}^{z} (1 + \frac{u^2}{m})^{-(m+1)/2} du$

Understanding Probability and Statistics

Probabilistic Risk Assessment (PRA)

- **Advantages**
  - Imposes logic structure on risk assessment.
  - Evaluates risk at various system levels including system interactions.
  - Handles multiple failures and common causes.
  - Provides more insight into the various system failure modes and the effects of human/process interaction.
  - Supports sensitivity analysis.
  - Provides a tool to combine both qualitative and quantitative risk analysis.
  - Can be useful in evaluating risk reduction, risk ranking, identifying areas that require further attention, and identifying system scenarios that have major impact on system risk.
  - PRA is a good source of data for sanity check of the likelihood input data of the risk matrix.

Probabilistic Risk Assessment (PRA)

- **Limitations**
  - Could be very expensive.
  - PRA faces a level of skepticism with respect to basic sources of quantification, basic failures/events modeled, basic quantification methods, completeness in covering all significant scenarios, quantification of uncertainty, etc.
  - It is very difficult to account for design margins, maturity, manufacturing capabilities and uncertainties, unexpected failure modes, unexpected common-cause failures, dependency, etc.

Fault Tree Analysis (FTA)

FTA is "An analytical technique, whereby an undesired state of the system is specified, and the system is then analyzed in the context of its environment and operation to find all credible ways in which the undesired event can occur."

Fault Tree Handbook, NUREG-0492, 1981

Fault Tree Analysis (FTA)

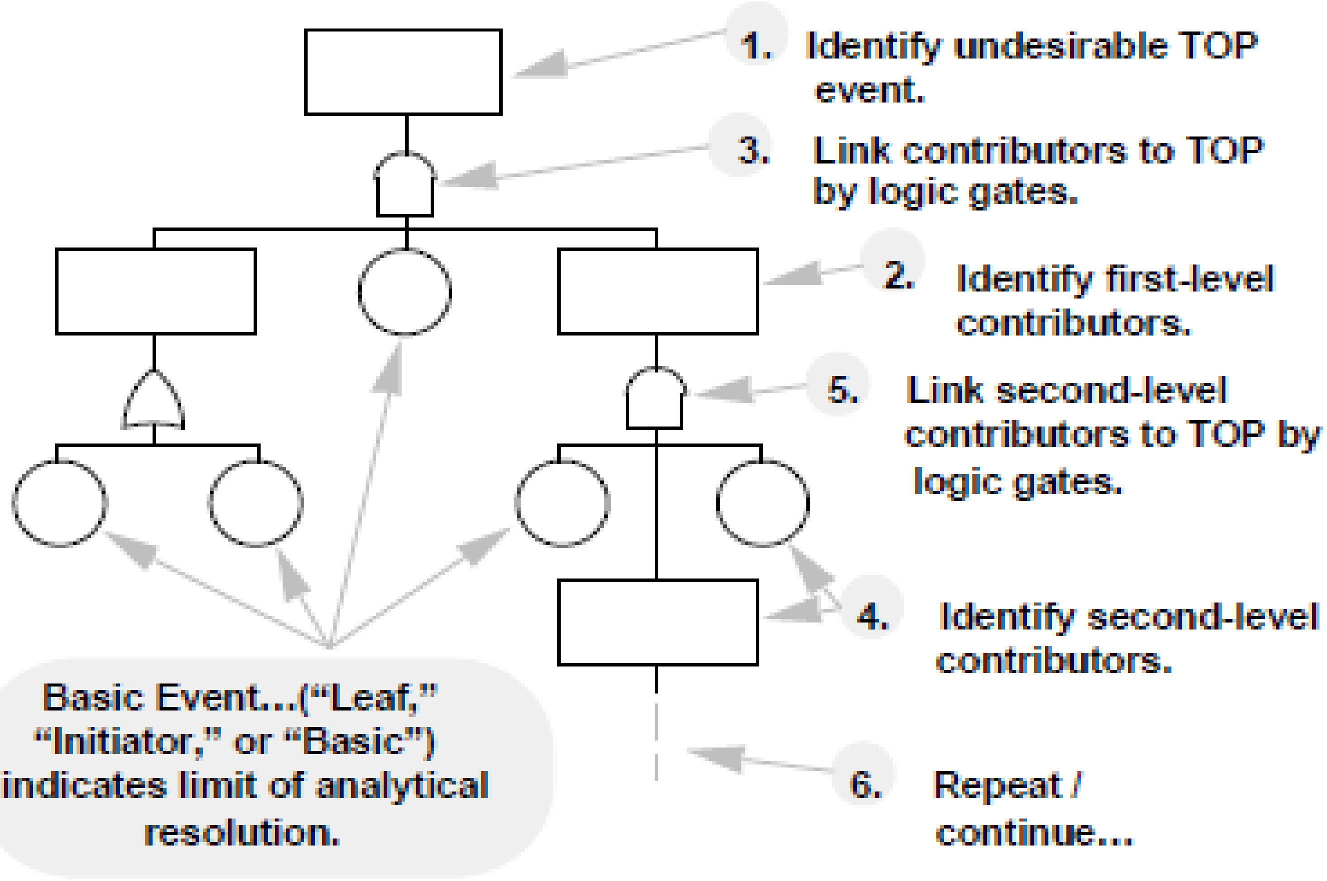
- A fault tree analysis (FTA) is a top-down symbolic logic model generated in the failure domain.
- This model traces the failure pathways from a predetermined, undesirable condition or event, called the TOP event, of a system to the failures or faults (fault tree initiators) that could act as causal agents.
- An FTA can be carried out either quantitatively or qualitatively.
- A quantitative FTA includes generating a fault tree (symbolic logic model), entering failure probabilities for each fault tree initiator, propagating failure probabilities to determine the TOP event failure probability, and determining cut sets that lead to the TOP event.
- A cut set is any group of initiators that will, if they all occur, cause the TOP event to occur.
- A minimal cut is a least group of initiators that will, if they all occur, cause the TOP event to occur.
- FTAs are frequently used in the context of a larger model that analyzes a combination of events, each of which might be a top event of a separate fault tree.

Fault Tree Analysis (FTA)

- An FTA process involves the following steps:
  - Identify the objective for the FTA
  - Define the scope of the FTA
  - Define ground rules for the FTA
  - Define the resolution of the FTA
  - Define the top event of the FT
  - Construct the FT
  - Evaluate the FT
  - Interpret and present the results

Fault Tree Analysis (FTA)

Basic Fault Tree Logic



1. Identify undesirable TOP event.

3. Link contributors to TOP by logic gates.

2. Identify first-level contributors.

5. Link second-level contributors to TOP by logic gates.

4. Identify second-level contributors.

6. Repeat / continue…

Basic Event…("Leaf," "Initiator," or "Basic") indicates limit of analytical resolution.

Fault Tree Analysis (FTA)

- **Advantages**
  - Enables assessment of probabilities of combined faults/failures within a complex system.
  - Single-point failures can be identified and assessed.
  - System vulnerability and low-payoff countermeasures are identified, thereby guiding deployment of resources for improved control of risk.
  - Can be used to reconfigure a system to reduce vulnerability.
  - Can be used in problem investigation.

Fault Tree Analysis (FTA)

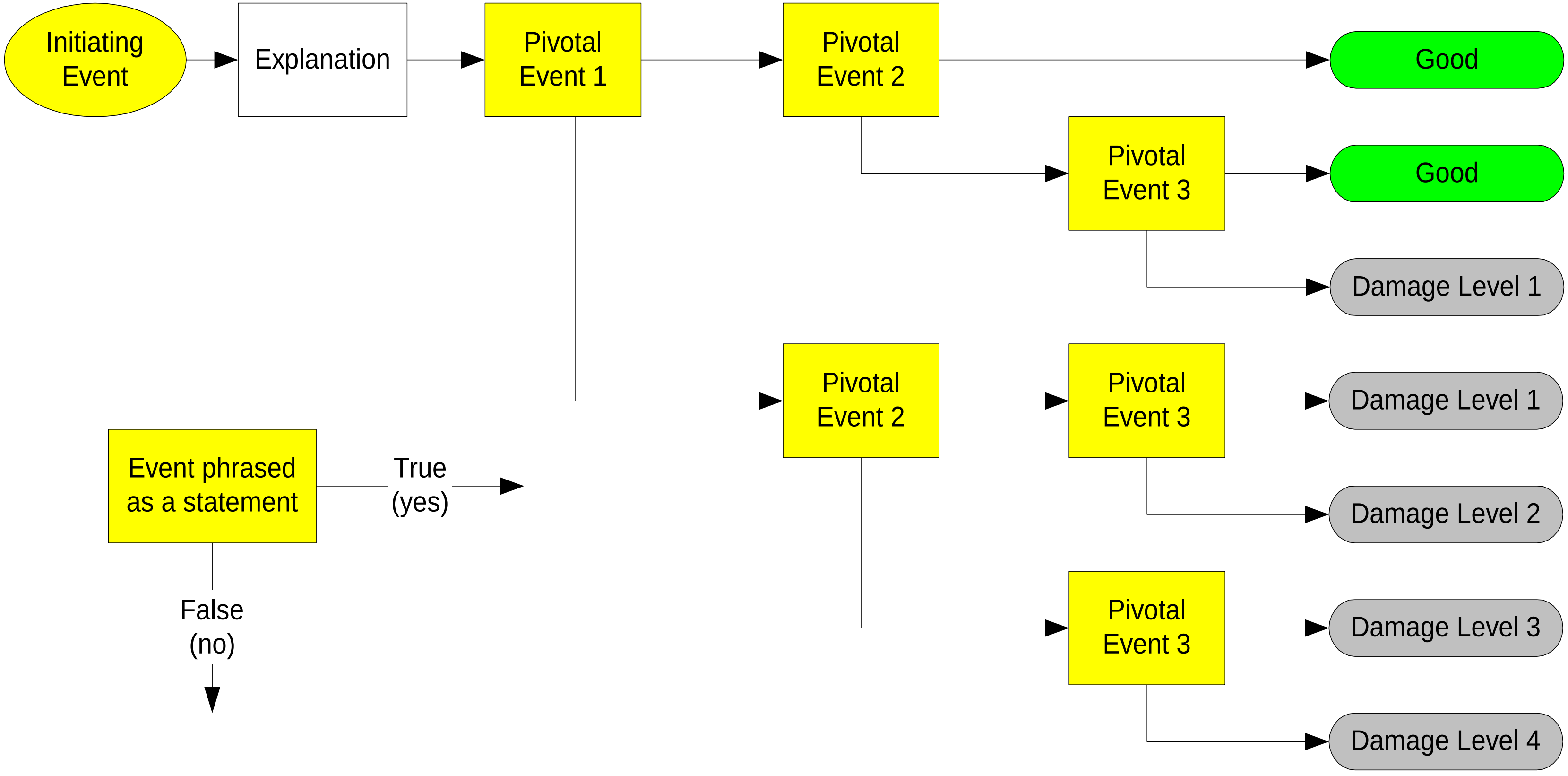
- **Limitations**
  - Addresses only one undesirable condition or event that must be foreseen by the analyst. Thus, several or many FTAs may be needed for a particular system.
  - The generation of an accurate quantitative FTA may require significant time and resources. Caution must be taken not to “over work” determining probabilities or evaluating the system (i.e., limit the size of the tree).
  - A fault tree is not accurate unless all significant contributors of faults or failures are anticipated.

Event Sequence Diagram (ESD)

- An ESD is essentially a flow chart with paths leading to different end states. Each path through the chart is a scenario.
- The method uses forward logic.
- Its primary use is supporting probabilistic risk assessments.
- An ESD is developed for each initiating event category in the PRA Master Logic Diagram.
- The input to an ESD is a defined initial state or “initiating event,” the “pivotal events,” and the end states of the scenarios of concern.

Event Sequence Diagram (ESD)

ESD Logic



F. Safie

Event Sequence Diagram (ESD)

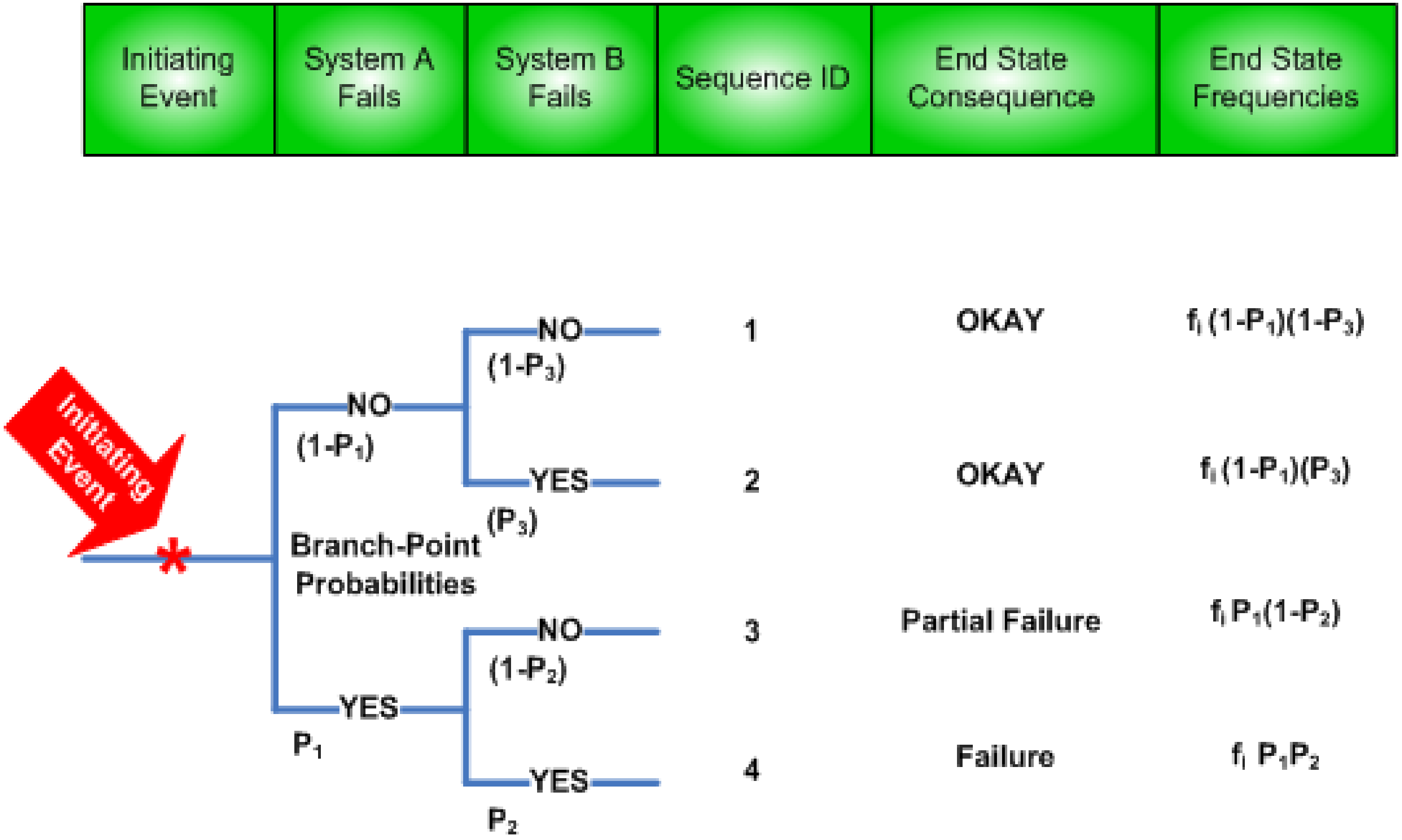
- **Advantages**
  - ESD is useful for identifying accident scenarios.
  - Most engineers find ESDs intuitive and easy to understand.
  - Used for communication between PRA analysts and the engineering community.
- **Limitations**
  - Developing ESDs requires strong engineering knowledge and background in logic flows.
  - An ESD is qualitative in nature.

Event Tree Analysis (ETA)

- ETA is a forward binary logic modeling technique used to determine the propagation paths (sequence of events) to a set of final states resulting from a given initial state or condition.
- In technical risk assessment, the initial state, or “initiating event,” is generally a hazard or failure, the intermediate events are potential propagation paths, and the final states are either conditions of loss (degradation, damage, destruction, death) or successful loss mitigation.
- Event tree analysis is generally applicable for almost any type of risk assessment application, but used most effectively to model accidents where multiple safeguards are in place as protective features.
- ETA is a primary tool of Probabilistic Risk Assessment.

Event Tree Analysis (ETA)

ETA Logic



Initiating Event	System A Fails	System B Fails	Sequence ID	End State Consequence	End State Frequencies
	NO $(1-P_1)$	NO $(1-P_3)$	1	OKAY	$f_i\,(1-P_1)(1-P_3)$
		YES (P_3)	2	OKAY	$f_i\,(1-P_1)(P_3)$
	YES P_1	NO $(1-P_2)$	3	Partial Failure	$f_i\,P_1(1-P_2)$
		YES P_2	4	Failure	$f_i\,P_1P_2$

Event Tree Analysis (ETA)

- **Advantages**
  - Provides a clear order of events from the initial to end states.
  - Allows discrete time sequencing within failure scenarios.
  - Accounts for complexities of design mitigations (safety features, etc.).
- **Limitations**
  - Can become exceedingly complex and require simplification.
  - Separate trees required for each initiating event.
    - Difficult to represent interactions among events
    - Difficult to consider effects of multiple initiating events
  - Requires ability to define a set of initiating events that will produce all important accident sequences.
  - Very resource intensive if applied to every hazard or failure in a design.

Bayesian Analysis

Bayesian Inference

- In probability and statistics, Bayes' theorem (alternatively Bayes' law or Bayes' rule) relates current to prior belief. It also relates current to prior evidence.
- With the Bayesian interpretation of probability, the theorem expresses how a subjective degree of belief should rationally change to account for evidence. This is Bayesian inference, which is fundamental to Bayesian statistics.
- **Bayesian inference is a method of statistical inference in which Bayes' Rule is used to update the probability for a hypothesis as evidence is acquired**.

Bayesian Analysis

Why Bayesian?

- Bayesian approach is a viable approach, especially when data is scarce and models are complex.
  - It is not limited to observed data.
  - It allows wide variety of evidence to play role in inference.
  - It allows uncertainty to be characterized and propagated through risk model.
  - Modern Bayesian formulation exploits computer power and simulation and avoids past computer limitations and approximations.

Bayesian Analysis

Bayesian vs Classical Statistic

- Classical statistics tries to make inference on the unknown parameters via sampling failure times and establishing confidence intervals for parameters and eventually life length distribution percentiles (A and B allowable).
- In the Bayesian approach, probability is a quantification of degree of belief.
- Bayesian statistics uses the notion that uncertainty about the parameters can be expressed via probability distributions called prior distributions.
- The prior distribution is key to a successful Bayesian analysis.
- The construction of the prior distribution depends on careful quantification of sound expert judgment for the problem at hand.
- This process requires the use of domain experts for defensible implementation.

Bayesian Analysis

The Bayesian Process

- **The general Bayesian procedure is:**
  - Begin with a probability model for the process of interest.
  - Specify a prior distribution for parameter(s) in this model, quantifying uncertainty, i.e., quantifying degree of belief about the possible parameter values.
  - Observe data.
  - Obtain the posterior (i.e., updated) distribution for the parameter(s) of interest.
  - Check validity of model.

Bayesian Analysis

- **Advantages**
  - Provides a way to explicitly introduce assumptions regarding prior knowledge or ignorance.
  - Can bring the engineering judgment applied in the prior out in the open.
  - If the prior information is encouraging, less new testing may be needed to confirm a desired MTBF at a given confidence.
- **Limitations**
  - Prior information may not be accurate, generating misleading conclusions.
  - Customers may not accept validity of prior data or engineering judgments.
  - There is no one "correct way" of inputting prior information (choice of prior) and different approaches can give different results.

Risk Assessment Related Tools and Techniques

- Risk Assessment Related tools and Techniques
  - Hazard Analysis
  - Failure Modes and Effects Analysis/Critical Items List (FMEA/CIL)
  - Reliability Predictions
  - Reliability Demonstration
  - Ishikawa Chart (Cause and Effect Diagram)

References

1. NASA Risk-Informed Decision Making Handbook, NASA/SP-2010-576 Version 1.0 April 2010
2. NASA Risk Management Handbook NASA/SP-2011-3422 Version 1.1, October 2011
3. SLS Booster S&MA Hazard Report Cause Counts/Classification, Hemkin 10/31/13
4. Bayesian Inference for NASA Probabilistic Risk and Reliability Analysis, NASA/SP – 2009-569
5. Fault Tree Handbook, NUREG-0492, 1981
6. Systems Engineering "Toolbox" for Design-Oriented Engineers, NASA Reference Publications 1358
7. Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, NASA/SP-2011-3421
8. NASA's Third Workshop for Probabilistic Risk Assessment Methods (PRAM-9) for Managers and Practitioners, March 23-25, 2010 (PRAM9)
9. NASA Systems Engineering Handbook, NASA/SP-2007-6105 Rev1
10. NASA's Risk Management Approach, Workshop on Risk Assessment and Safety Decision Making Under Uncertainty, September 21-22, 2010 Homayoon Dezfuli, Ph.D.
11. Safety Basics, John Livingston, MSFC SMA
12. NASA System Safety Handbook, NASA/SP-2010-580, Version 1.0, November 2011
13. OSMA safety courses for STEP training program maintained by NASA Safety Center (NSC)

Concluding Remarks

- The tools and techniques discussed here represent just a selected set of a bigger list that the risk assessment community use.
- The application of these tools and techniques depends on the objective of the risk assessment and the applicability of the tool or technique to the situation.
- Caution should be exercised when model selection within a tool/technique could significantly affect the overall results and conclusions. Sensitivity analysis is one option to explore the impact of model selection on the results.