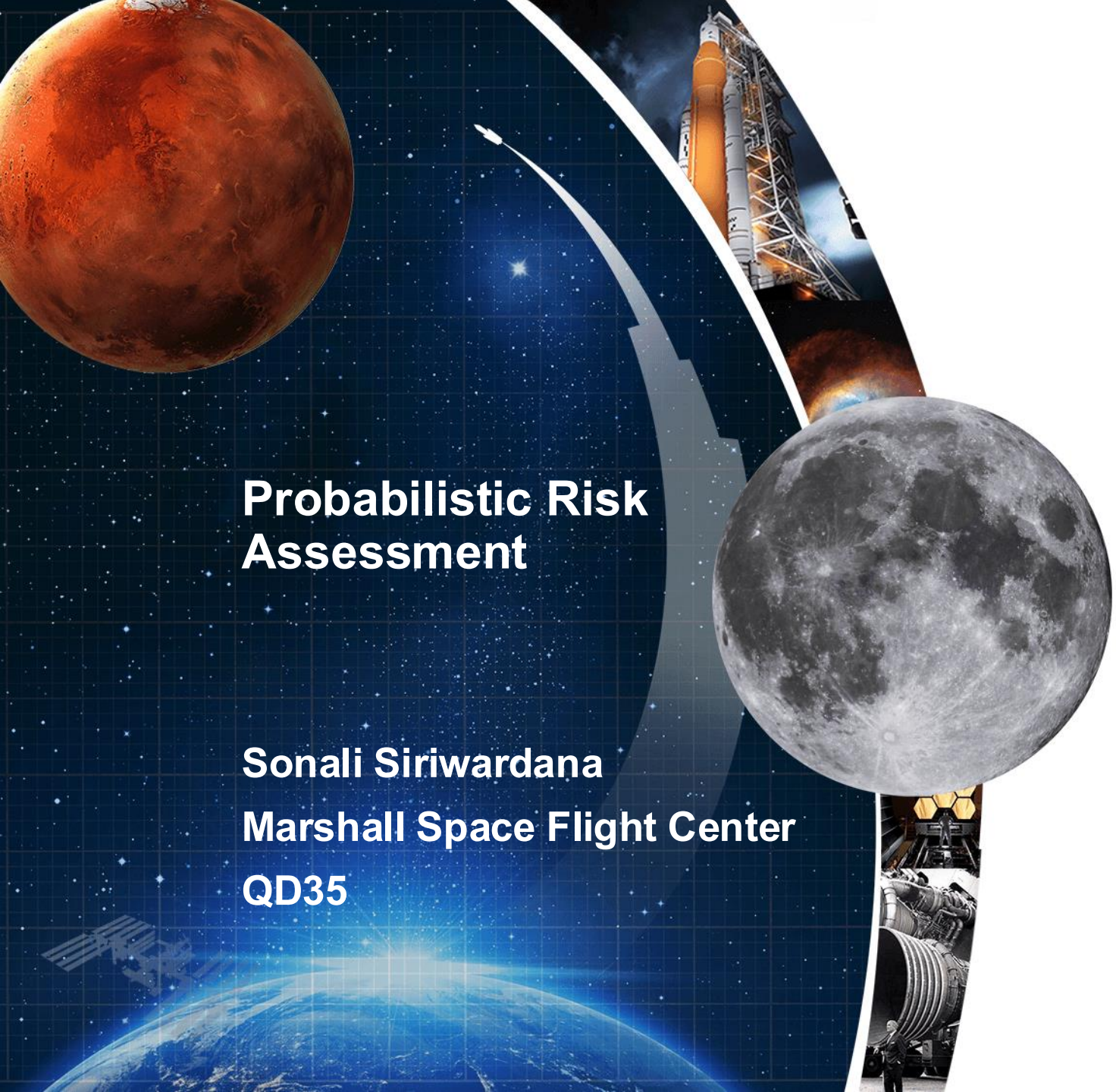


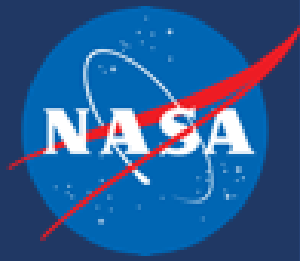
National Aeronautics and Space Administration

Probabilistic Risk Assessment

Sonali Siriwardana
Marshall Space Flight Center
QD35

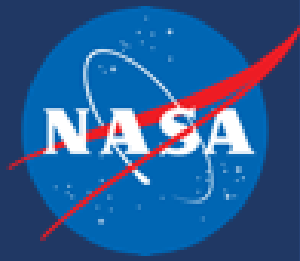
EXPLORE MARSHALL

Intro to Probabilistic Risk Assessment



- When PRA should be Implemented
- Necessary Skill Sets
- Tools
  - Basic Approach
  - Data Sources
  - Fault Tree Analysis
  - System Example
- Trade Studies
- PRA Limitations
- Common Cause Failure

When PRA Should be Implemented



- It is best if PRA is involved in the design process from the beginning. Once budget, schedule, and initial design has been established, a full-up detailed PRA can be implemented
  - During SRR, the reliability assessment serves as the quantitative analysis
  - Carry out PRA at the beginning of each major design phase; it will be more detailed as the program moves through each milestone
- PRA is meant to provide risk-informed inputs for decision-making processes
- When used correctly, PRA can positively impact design changes by pointing out risk drivers early on in the design process, which could potentially lower costs (design changes happen sooner than later) or improve safety
- PRA studies can also be conducted in response to issues, to better understand the integrated risk and consequences of a particular problem, such as
  - Performing sensitivity studies
  - Determining the relative risks due to any design changes.

Necessary Skill Set for PRA

- PRA is a method that is used to evaluate risks associated with a system or process
- Determining and evaluating risk typically answers three questions:
  - What can go wrong? (Failure Event)
  - How likely is it? (Failure Event Probability)
  - What are the associated consequences? (Undesired End State)
- Investigating only those risks involving the end states of interest
- A set of accident scenarios defining the path to the undesired end states
- Historical Data or Engineering Judgment is used to determine the probability of failure events which lead to an undesired end state

What is Risk?

Risk = Likelihood x Consequence

The probability of something happening multiplied by the resulting cost or benefit if it does.

Data Gathering

Types of Data

- Historical
  - Actual component data
  - Similar component data (other industries)
  - Testing

- Prediction
  - Piece Part Method (MIL-HDBK-217 add up the constituent component's reliability)
  - Expert Judgment
  - Engineering Judgment
  - Physics based modeling results

Not all sources are as applicable as one another
Represent that difference through uncertainty

Fault Tree Introduction

Fault tree analysis is a tool used to model credible sets of failures that a system can experience to enter a specified undesirable state.

- Top Down – Undesired end state is specified, then system failures that could lead to this state are determined.
  - In a fault tree the undesired state is often referred to as the “top gate”
- Failures in the fault tree are modeled as “events”
  - These can be component failures, human errors, system configurations, etc.
- “Gates” are used to logically link these events in ways that would lead the system to the undesired state.

Fault Tree Elements – Basic Event

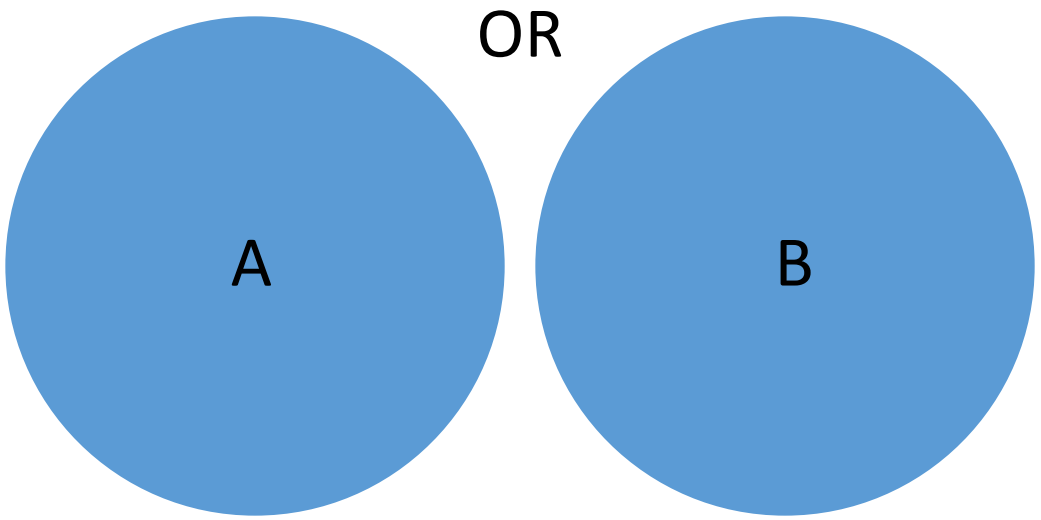
BASIC EVENT – A basic initiating fault requiring no further development

The basic event represents a failure or fault in the system. The value associated with a basic event is usually a probability of failure. Using a Venn diagram, the basic event would be represented by a single circle.

Fault Tree Elements – OR gate

OR – Output fault occurs if at least one of the input faults occurs

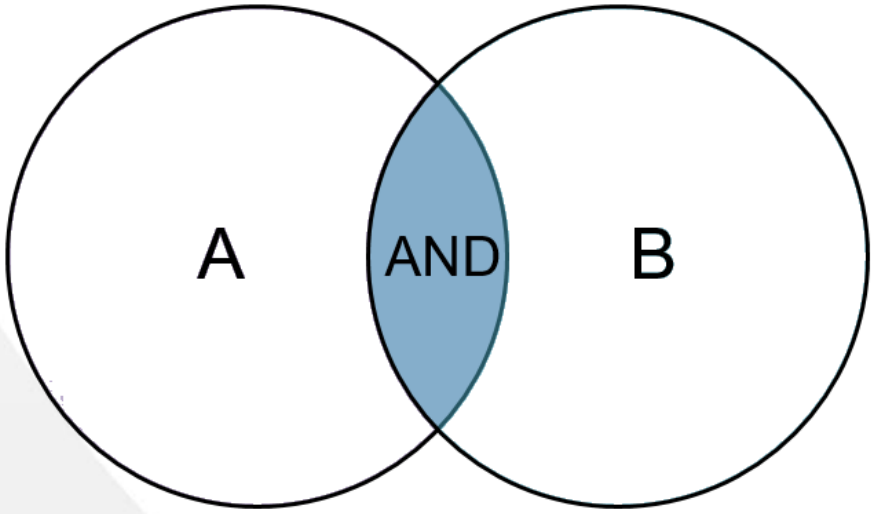
The OR gate represents addition. This gate will output if any input basic event occurs. (e.g. A or B occurs) This is represented in a Venn diagram by the full area.



Fault Tree Elements – AND Gate

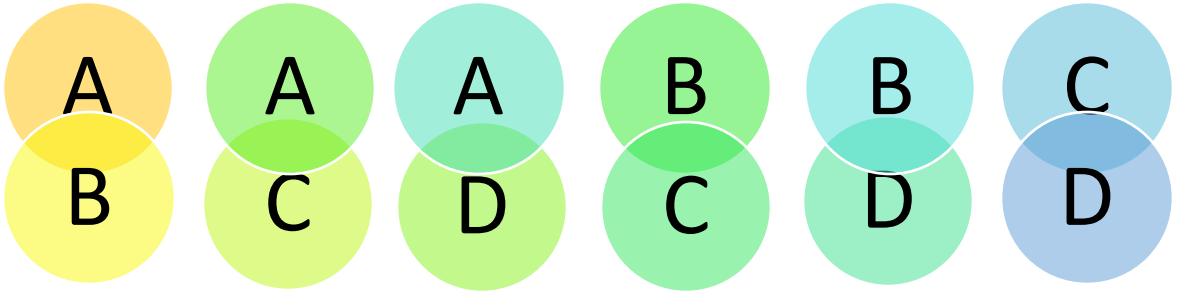
AND – Output fault occurs if all of the input faults occur

The AND gate represents multiplication. It will output if the failure of ALL of its inputs occur. (e.g. A and B occur.) This is represented in a Venn diagram by the overlapping area.

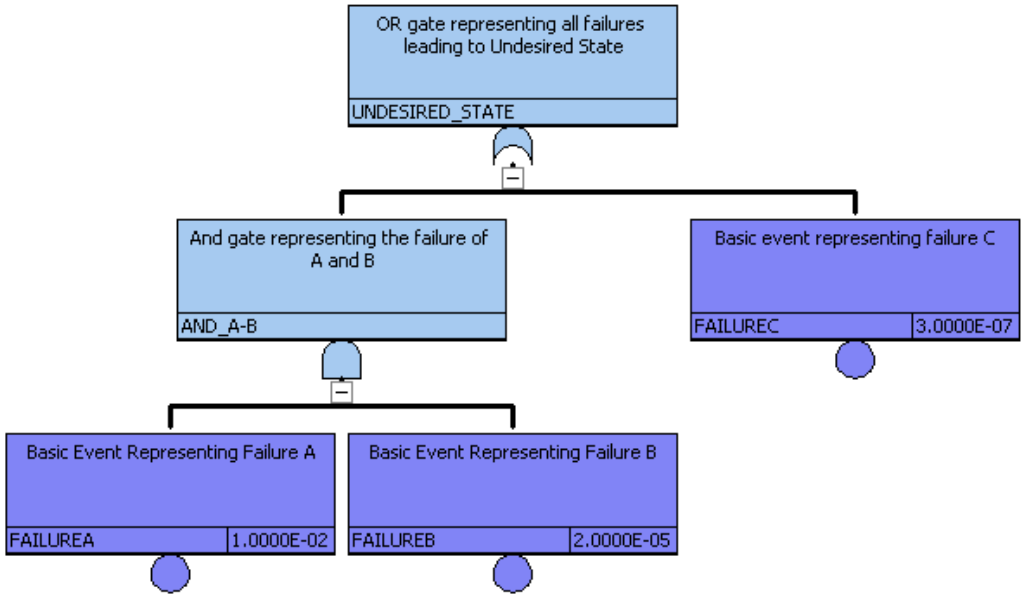


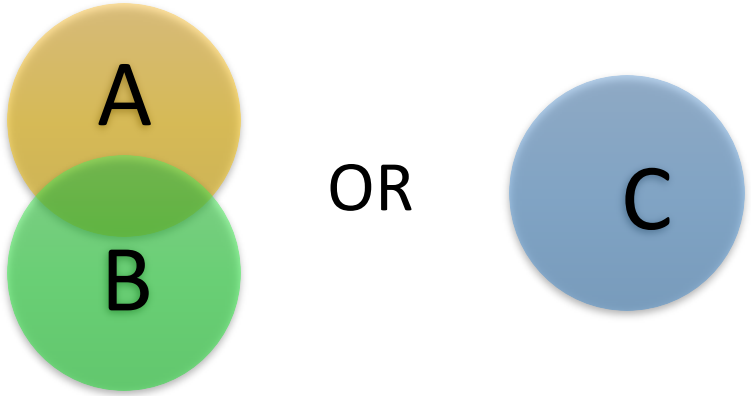
Fault Tree Elements – N of M Gate

The N of M gate is a specialized gate. It evaluates for N of M failures. i.e. if the total number of inputs is four, and we specify N = 2, then the gate will output if any two of the four failures occurs. It is used as shorthand for a series of OR and AND gates. The Venn diagram shows this example.



Fault Tree Elements – Example





Summary of Trade Study

for their risk contribution

- Given the design options PRA will model each option into its model
- The models are then solved, and the risk is presented for each option
- PRA shows the relative risk differences for each option
  - It does not attempt to show any other pro/cons associated with an option. It's simply a tool to allow decision makers to see what risk they will be imparting to the design with each option
    - Data fidelity will affect the results of the risk analysis – analysis limitations should be noted
  - Therefore it should not be assumed that the lowest risk option is what PRA is suggesting, sometimes the benefits of a particular design may lead to the decision to accept that increase in risk
  - In general during a trade study the PRA team does not make a recommendation for any option, but simply presents the risks to decision makers

PRA Limitations

- Relevant historical data is hard to come by for some designs
- This has some historical roots in how data was gathered, but also is due to the nature of the industries relatively infrequent launch rate
- Due to this, uncertainties applied need to be thoroughly explained to prevent misunderstandings in what the PRA is able to accomplish
- Depending on how difficult it is to attain historical data, it can lead to a relatively large error distributions on the risk analysis
- Limitations from the software itself (e.g. SAPHIRE) used to create the PRA model
- Note all assumptions as they can have large impacts on the risk estimate

Common Cause Failure

- Failure of two or more similar components within mission time due to similar cause.
- Defeats redundancy in systems where the redundant system uses similar components.
- Example: Two valves on redundant lines, similar design and manufacture, with the same duty cycle, and same environment. The likelihood of both valves failing is fairly higher than their independent failure rates.

References

- NUREG-0492, Fault Tree Handbook, Nuclear Regulator Commission Jan. 1981
- Reliawiki.com: Same Example Modeled with RBDs or Fault Trees
  - http://reliawiki.com/index.php/Same_Example_Modeled_with_RBDs_or_Fault_Trees
- Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners
  - https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20120001369.pdf
- The Challenger Disaster: A Case of Subjective Engineering
  - https://spectrum.ieee.org/tech-history/heroic-failures/the-space-shuttle-a-case-of-subjective-engineering
- Reliability and Probabilistic Risk Assessment – How They Play Together
  - https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20150002964.pdf
- System Modeling Techniques for PRA P-200, U.S. NRC (2009)
  - https://www.nrc.gov/docs/ML1204/ML12044A155.pdf

Backup

Data Source Uncertainty Heuristic Chart

Source	Category	Source Descrption	Source Application	Source Application Error Factor	Adjusted Environment
Historical	A	Other Launch Vehicle Data (Most Applicable)	Same component	3	Increases the Error Factor
			Like component	4	
	B	Aerospace Data	Same component	5	
			Like component	6	
	C	Other Industry Data	Same component	6	
			Like component	7	
Prediction	D	MIL-HDBK-217F Methods	Same component	8	
			Like component	9	
	E	Non-expert Engineering Judgment (Least Applicable)	Documented Process	10	
			Undocumented Process	15	

Reliability

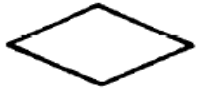
- The probability that a component will perform its intended function for a defined time interval (for a mission time, t).
  - (probability of success)
  - Where R(t) = reliability, Tf = time to failure, t = mission time
  - R(t) = P{Tf > t} , the likelihood that component succeeds past the mission time
  - F(t) = 1 – R(t)

Fault Tree Elements – Event Symbols

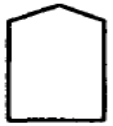
PRIMARY EVENT SYMBOLS

BASIC EVENT — A basic initiating fault requiring no further development

CONDITIONING EVENT — Specific conditions or restrictions that apply to any logic gate (used primarily with PRIORITY AND and INHIBIT gates)



UNDEVELOPED EVENT — An event which is not further developed either because it is of insufficient consequence or because information is unavailable



EXTERNAL EVENT — An event which is normally expected to occur

INTERMEDIATE EVENT SYMBOLS

INTERMEDIATE EVENT — A fault event that occurs because of one or more antecedent causes acting through logic gates

Fault Tree Elements – Gate Symbols

GATE SYMBOLS

AND – Output fault occurs if all of the input faults occur

OR – Output fault occurs if at least one of the input faults occurs

EXCLUSIVE OR – Output fault occurs if exactly one of the input faults occurs

PRIORITY AND – Output fault occurs if all of the input faults occur in a specific sequence (the sequence is represented by a CONDITIONING EVENT drawn to the right of the gate)

INHIBIT – Output fault occurs if the (single) input fault occurs in the presence of an enabling condition (the enabling condition is represented by a CONDITIONING EVENT drawn to the right of the gate)

Fault Tree Elements – Transfer Symbols

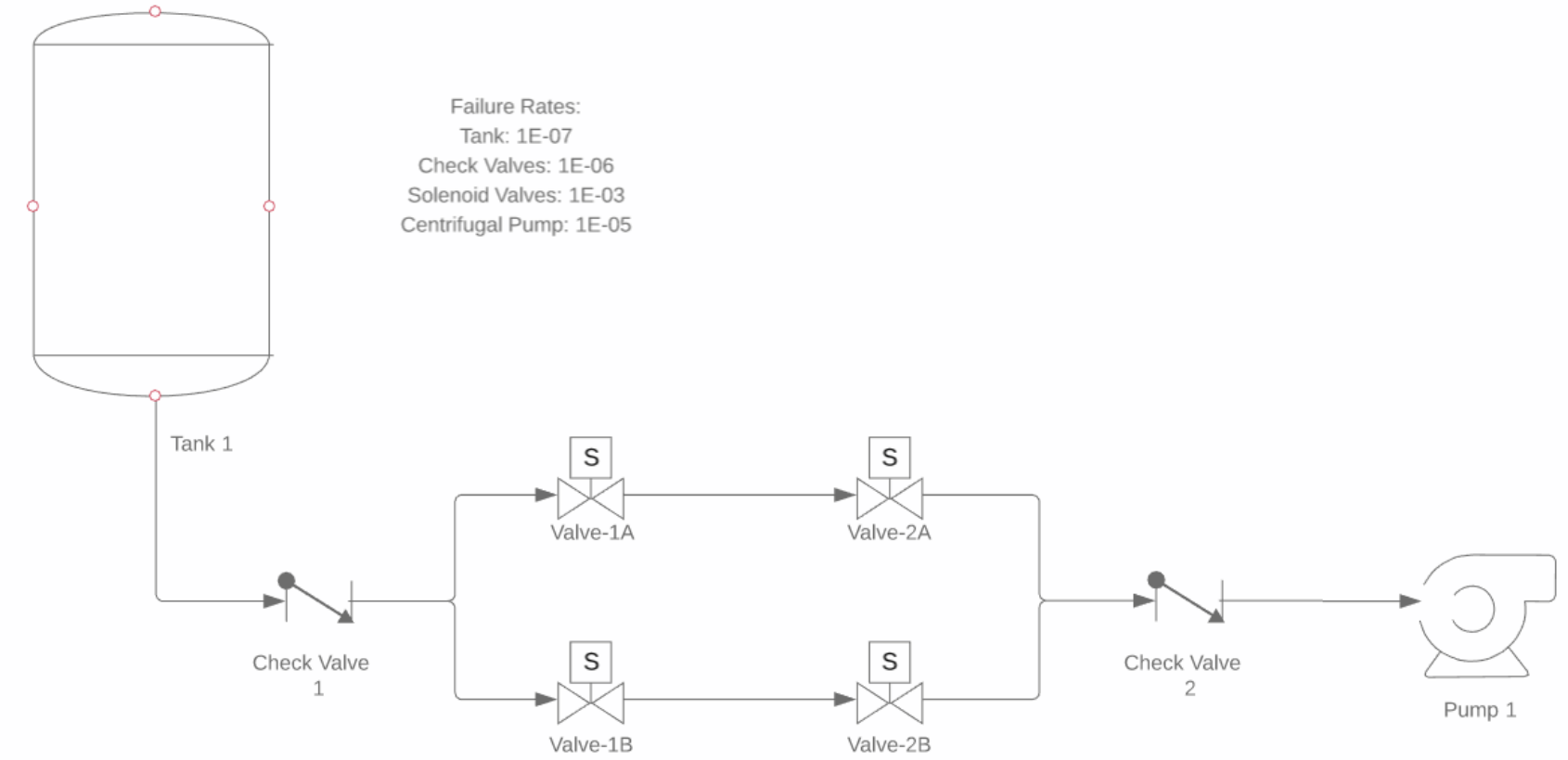
TRANSFER SYMBOLS

TRANSFER IN – Indicates that the tree is developed further at the occurrence of the corresponding TRANSFER OUT (e.g., on another page)

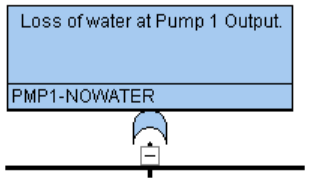
TRANSFER OUT – Indicates that this portion of the tree must be attached at the corresponding TRANSFER IN

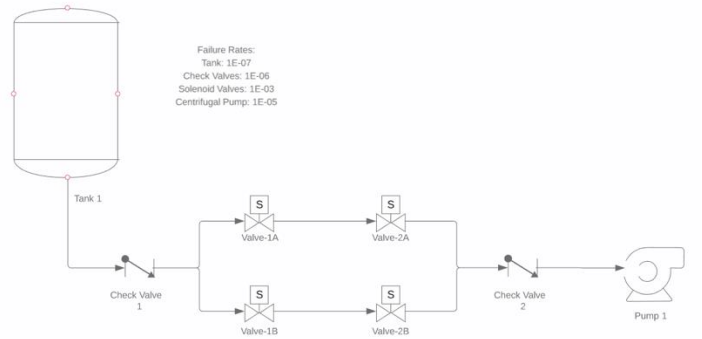
Transfers are simply when one fault tree is developed separately, and then that fault tree logic is ‘dropped in’ to another tree.

Example System



Example System





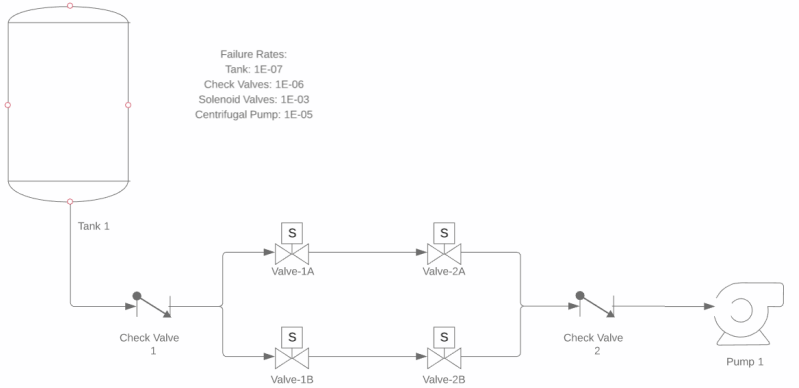
Example System

Cutsets:

Tank 1 – 1E-7
Check Valve 1 – 1E-6
Valve-1a, Valve-1B – 1E-6 (1E-3*1E-3)
Valve-1a, Valve-2B – 1E-6 (1E-3*1E-3)
Valve-2a, Valve-1B – 1E-6 (1E-3*1E-3)
Valve-2a, Valve-2B – 1E-6 (1E-3*1E-3)
Check Valve 2 – 1E-06
Pump 1 – 1E-05

What would the total failure probability be for this system?

1.61E-05



	#	Prob/Freq	Total %	Cut Sets
		1.610E-5	100	Displaying 8 of 8 Cut Sets.
⊞	1	1.000E-5	62.11	PUMP1-FAILS
⊞	2	1.000E-6	6.21	SVALVE-1B,SVALVE-2A
⊞	3	1.000E-6	6.21	SVALVE-1A,SVALVE-1B
⊞	4	1.000E-6	6.21	SVALVE-1A,SVALVE-2B
⊞	5	1.000E-6	6.21	SVALVE-2A,SVALVE-2B
⊞	6	1.000E-6	6.21	CHECK1-STUCKCLOSED
⊞	7	1.000E-6	6.21	CHECK2-STUCKCLOSED
⊞	8	1.000E-7	0.62	TANK-RUPTURE

National Aeronautics and Space Administration

Data Development

By Sonali Siriwardana

Data Sources and Failure Type

- Rate Failures
  - Number of Failures (event counts)
  - Total Operating Time
  - Examples: check valves, sensors

*Number of similar components in use, operating time, design changes, etc. are needed to deduce a failure rate

- Demand Failures – system or component failing to perform its intended function when called upon (or when a demand is placed on it).
  - Example: Firmware

Data: Failure Modes

- Multiple Failure Modes
  - Data sources may include multiple ways in which a component fails
  - Examples:
    - Filter
      - Leakage – external
      - Rupture
      - Failure to filter
      - Reduced flow
      - Excessive pressure drop

Failure Mode	Nominal Fraction
Leakage	0.03
Rupture	0.04
Failure to Filter	0.80
Reduced Flow	0.06
Excessive Pressure Drop	0.07

- Make sure to record what modes are included in the model
- Example calculation for filter failing by rupture:
  - Overall failure rate of filter is 1E-05
  - Filter failing by rupture = overall failure rate * nominal fraction$_{rupture}$ = 1E-05 * 0.04 = 4E-07

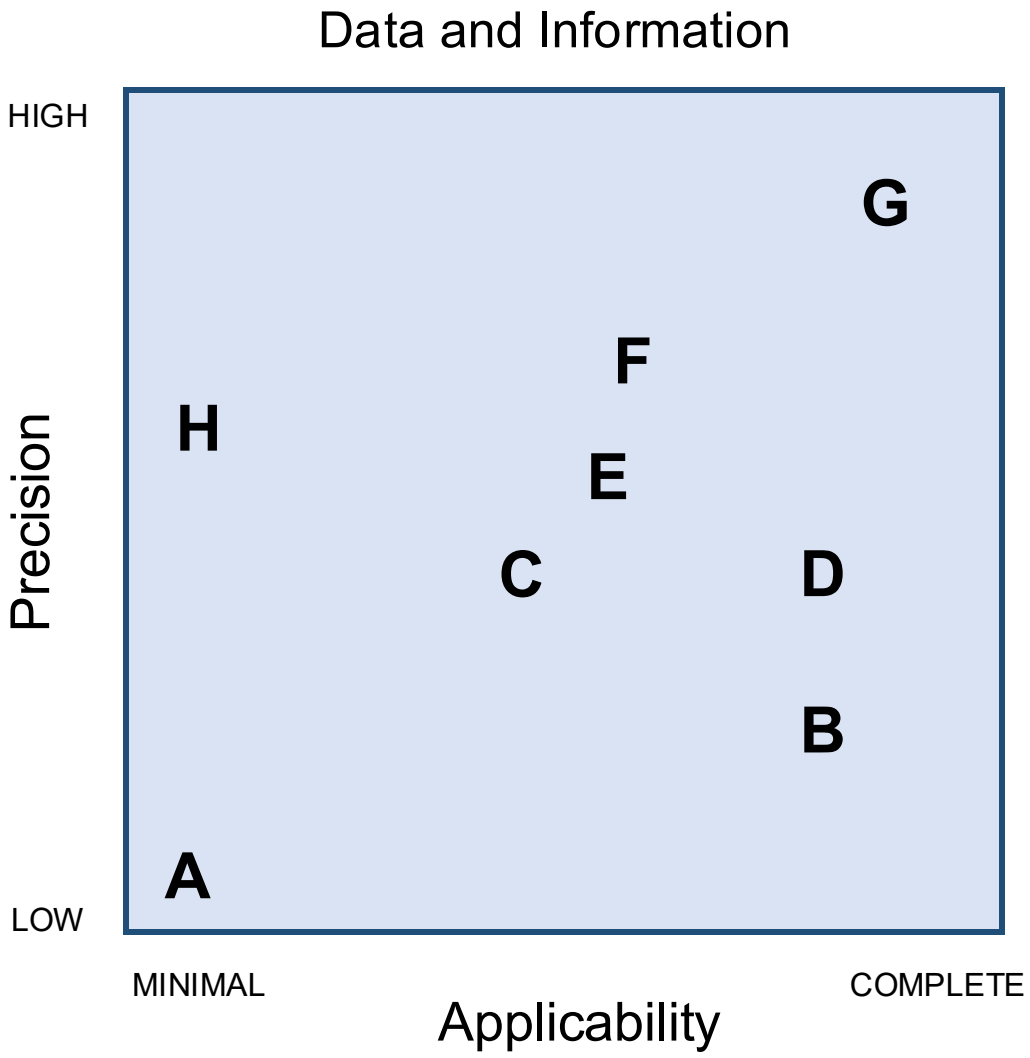
Data Sources

- System-specific data
  - Maintenance logs
  - Test logs
  - Operation records
- Test and operational data (industry databases/manufacturing data)
  - Identical systems and environments
  - Other systems and environments
- Engineering and scientific knowledge
- Expert opinion
- Physics-based modeling

Data Development

- Developing a database of parameter estimates involves
  - Model-data relation
    - Component boundaries
    - Failures modes
    - Failures rates
  - Data collection
    - Failure/success data
    - Data sources
    - Classification of the data
  - Parameter Estimation
    - Statistical methods to develop uncertainty distributions
  - Documentation
    - Assumptions that went into the model
    - Data sources used
    - How uncertainty distributions were estimated

Types of Data and Information



- A: Generic Data for a class of components
- B: Generic data for specific component type
- C: Test data for a new system
- D: Test data for a new component
- E: Expert opinion on an existing component
- F: Test and operational data for a similar component
- G: Test and operational data for actual component
- H: Test and operational data for a dissimilar component

Failure Cause Classification Process (Hardware)

- Functional Failure Mode
  - Particular way the function of the component is affected by the failure even (e.g., fail to start, fail to open)
- Failure Mechanism
  - Physical change (e.g., crack, block) in the component that has resulted in the functional failure mode
- Failure Cause
  - The event or process responsible for the observed physical and functional failure modes

Likelihood Function

- For data generated from counts of failures during operation
  - Poisson Process is the proper likelihood function
- For data generated from the Bernoulli process (counts of failures on system demands)
  - Binomial distribution is the proper likelihood function
- For data in form of expert estimates or values for data sources (e.g., a best estimate based on engineering judgement)
  - Lognormal distribution may be the proper likelihood function

Data Source Uncertainty Heuristic Chart

Source	Category	Source Descrption	Source Application	Source Application Error Factor	Adjusted Environment
Historical	A	Other Launch Vehicle Data (Most Applicable)	Same component	3	Increases the Error Factor
			Like component	4	
	B	Aerospace Data	Same component	5	
			Like component	6	
	C	Other Industry Data	Same component	6	
			Like component	7	
Prediction	D	MIL-HDBK-217F Methods	Same component	8	
			Like component	9	
	E	Non-expert Engineering Judgment (Least Applicable)	Documented Process	10	
			Undocumented Process	15	

Environmental Tables

TABLE 10.3-3: ENVIRONMENTAL CONVERSION FACTORS
(MULTIPLY SERIES MTBF BY)

From Environment	To Environment: G_B	G_F	G_M	N_S	N_U	A_{IC}	A_{IF}	A_{UC}	A_{UF}	A_{RW}	S_F
G_B	X	0.5	0.2	0.3	0.1	0.3	0.2	0.1	0.1	0.1	1.2
G_F	1.9	X	0.4	0.6	0.3	0.6	0.4	0.2	0.1	0.2	2.2
G_M	4.6	2.5	X	1.4	0.7	1.4	0.9	0.6	0.3	0.5	5.4
N_S	3.3	1.8	0.7	X	0.5	1.0	0.7	0.4	0.2	0.3	3.8
N_U	7.2	3.9	1.6	2.2	X	2.2	1.4	0.9	0.5	0.7	8.3
A_{IC}	3.3	1.8	0.7	1.0	0.5	X	0.7	0.4	0.2	0.3	3.9
A_{IF}	5.0	2.7	1.1	1.5	0.7	1.5	X	0.6	0.4	0.5	5.8
A_{UC}	8.2	4.4	1.8	2.5	1.2	2.5	1.6	X	0.6	0.8	9.5
A_{UF}	14.1	7.6	3.1	4.4	2.0	4.2	2.8	1.7	X	1.4	16.4
A_{RW}	10.2	5.5	2.2	3.2	1.4	3.1	2.1	1.3	0.7	X	11.9
S_F	0.9	0.5	0.2	0.3	0.1	0.3	0.2	0.1	0.1	0.1	X

Environmental Factors as Defined in MIL-HDBK-217

G_B - Ground Benign; G_F - Ground Fixed; G_M - Ground Mobile; N_S - Naval Sheltered; N_U - Naval Unsheltered; A_{IC} - Airborne Inhabited Cargo; A_{IF} - Airborne Inhabited Fighter; A_{UC} - Airborne Uninhabited Cargo; A_{UF} - Airborne Uninhabited Fighter; A_{RW} - Airborne Rotary Winged; S_F - Space Flight

CAUTION: Do not apply to MTBCF.

References

- NASA's Ninth Workshop for PRA Methods (2010)
- Probabilistic Risk Assessment, QD35 (2025)

National Aeronautics and Space Administration

Common Cause Failures

By Sonali Siriwardana

Definitions

- Common Cause Failure (CCF): failure or unavailable state of more than one of the same type of component during the mission time and due to the same shared cause.
  - CCF represent the risk of dependent failures of multiple similar components that would defeat the functional redundancy of a system and meet the following four criteria:
    - Two or more components fail or are degraded
    - Failure occurs within a selected period of time such that success of the mission would be uncertain
    - Failures results from a single shared cause
    - Component failure occurs within the established component boundary

Common Cause Failures

- Dependent Failures: P(AB)
  - P(AB) ≠ P(A)*P(B)
  - Often P(AB) is greater than P(A)*P(B)

- Intrinsic vs Extrinsic dependencies
  - Intrinsic (not CCF)
    - Functional status of one component is affected by the functional status of another
    - Stem from system design
    - If failure requirements are modeled at the system level, these dependencies are explicitly accounted for in modeling logic and not considered common cause.
  - Extrinsic (CCF)
    - Not inherent to design of the system; not explicitly modeled
    - May include physical/environmental interactions (including human interactions, e.g., maintenance errors)

Common Cause Failures

- Examples of Extrinsic couplings can be the same
  - Design
  - Hardware
  - Function
  - Installation, maintenance, or operations staff
  - Procedures
  - System/component interfaces
  - Location
  - Environment

Non-staggered vs Staggered Testing

- Non-staggered
  - Components are tested simultaneously
- Staggered
  - Components are tested one at a time at fixed intervals
  - The staggered model results in a lower incidence of common cause depending on how the generic data is interpreted
- The method used needs to stay consistent between the entire system analysis
- When performing trade studies, the method used needs to stay consistent between all alternatives used in the study; otherwise, using the staggered testing for one alternative will result in a low risk estimate relative to the non-staggered alternative.
- For spacecraft, it is generally recommended to use non-staggered testing

Example and Case Type Description for a 2/3 Failure

Type	Failures included in Common Cause Event	Failures of at Least Two Components NOT included in Common Cause Event	Description
All	AB, AC, BC, ABC	--	Any failure of at least two components. Generally, this represents any failure of at least k (or more) components.
Exact	AB, AC, BC	ABC	Any failure of exactly two components, but no more than two. Generally, this represents any failure of *exactly* k components, but no more than k components. i.e. larger group sizes are not included.
Specific	AB, ABC	AC, BC	Any failure of at least two components that includes the failure of two specific components (in this case, A and B). Generally, this represents any failure that includes *at least* k specific components (such as component A and B). This can include group sizes larger than k as long as the specific components are part of the group.
Precise	AB	AC, BC, ABC	Failure of precisely two particular components (in this case, A and B), and no additional failures of similar components. Generally, this represents the failure of k precise components (such as component A and B) and no additional failures.

CCF Global Alpha Factor Derivations

- Probability of a common cause failure of components a, b, and c is equal to a global common cause factor α times the probability of a single component (a) failing

$$P(C_{ABC}) = \alpha\ P(A) \quad (1)$$

- Failure probability for a 2/3 system can be given by P(S):

$$P(S)=P(A)P(B)+P(A)P(C)+P(B)P(C) +P(C_{AB})+P(C_{AC})+P(C_{BC})+P(C_{ABC}) \quad (2)$$

- This can be simplified if you assume probabilities involving similar components are equal:

$$P(A)=P(B)=P(C)=Q_1$$
$$P(C_{AB})=P(C_{AC})=P(C_{BC})=Q_2$$
$$P(C_{ABC})=Q_3 \quad (3)$$

- Use equation 3 to simplify to a Q equation to show the probability of system failure P(S) for a 1/3 system, 2/3 system, and a 3/3 system:

$$P(S_{1/3})=Qs=3(Q_1)+3(Q_2)+(Q_3) \quad (4)$$
$$P(S_{2/3})=Qs=3(Q_1)^2+3(Q_2)+(Q_3) \quad (5)$$
$$P(S_{3/3})=Qs=3(Q_1)^3+(Q_3) \quad (6)$$

CCF Global Alpha Factor Derivations

- The coefficients in front of the Q's in equations 4-6 represent the number of combinations of *i* failures in an overall failure group size *m*.
- These coefficients are defined as x_i^m :
  - *m* is the group size
  - *i* is the number of failures within that group size
  - *k* is the failure requirement (i.e., *k* out of *m* components must fail in order for the system to fail)

$$x_i^m = \binom{m}{i} + \frac{m!}{(m-i)!\,(i)!} \quad (7)$$

- Generalized equation for the failure probability of the system, P(S):
  - When 1<i<k, xi(Qi) is not included since that number of failures does not lead to system failure.
  - The first term, $\boldsymbol{x_1^m(Q_1^m)^k}$, represents the independent risk. This portion of failure risk is explicitly modeled through the use of k/m gates.

$$\mathrm{P}(S) = Qs = x_1^m(Q_1^m)^k + \sum_{i=k}^{m} x_i^m(Q_i^m) \quad (8)$$

where k>1

CCF Global Alpha Factor Assumptions

- Q_i^m = the probability of a common cause basic event involving *i* specific components in a common cause component group size *m*.

- Q_t = total failure frequency of each component due to all independent and common cause events
  - SLS PRA uses the **single component failure rate** for this value
  - This assumes that the single component failure rate (FR) is Q_t. When testing a single component to failure, manufacturers are not parsing out the data to separate independent failures from dependent failures, so the "single" component failure is representing the total failure rate.

- Alpha factor α_i = the fraction of the total frequency of failure events that occur in the system and involve the failure of *i* components due to a common cause.
  - These alpha factors are found in the CCF Parameter Estimates, 2020 Update data tables and are specific for demand/rate-based events and group size *m*.
  - Lack of historic data requires us to use generic data sources such as the Nuclear Regulatory Commission's database

Global Alpha Model Uncertainty Tool (GAMUT)

- Microsoft Visual Basic code embedded into the spreadsheet
- Array of all alpha values from the nuclear industry (CCF Parameter Estimates, 2020 Update)
- Column A: Type of Input
- Column B: Value for the inputs
- Column C: Blank
- Column D: Number of failures
- Column E: System status (if i < k, then status is OK, else status = LOM)
- Variables:
  - i = number of failures. i is defined from 1 to m, it is the number of failures. It is not the failure requirement
  - k = failure requirement (LOM_Minimum is the failure requirement)
  - m = group size
- Column F and G are equations that the code puts into Excel and Excel calculates it based on what it is told. These columns are combinatorial equations.
- Column L is the precise case.

Global Alpha Model Uncertainty Tool (GAMUT)

- Inputs:
  - Group size
  - Failure requirement
  - LOM only
  - Demand or Rate failure
- Output
  - Four cases of Global Alpha Factors: All, Specific, Exact, and Precise

References

- General Info:
  - Probabilistic Risk Assessment, QD35 (2025)
  - Common Cause Failure Modeling Aerospace vs Nuclear, Hatfield/Hark/Britton/Ring
- GAMUT tool:
  - Bruce Reistle, GAMUT (2011)
  - Joseph Osowski, GAMUT (2020 update)
- NUREG calculations/derivations:
  - Guidelines on Modeling Common Cause Failures in Probabilistic Risk Assessment, NUREG/CR-5485 (1998)
  - CCF Parameter Estimations 2020, INL/EXT-21-62940, Rev. 1
    - https://nrcoe.inl.gov/ccf_pe/

National Aeronautics and Space Administration

Uncertainty

By Sonali Siriwardana

SAPHIRE Uncertainty Analysis

- For all basic events, SAPHIRE randomly samples the parameters from their uncertainty distributions and uses these parameter values to calculate the probability.
- Sampling and calculation are repeated several thousand times and uncertainty distribution for the probability of the top tree is found empirically
  - Mean of the distribution is the best estimate of the probability
  - Dispersion quantifies the uncertainty in this probability
- SAPHIRE will calculate the 5^{th}, 50^{th}, mean, and 95^{th} percentile values along with the first four moments
  - Sample mean
  - Sample variance
  - Coefficient of skewness – used for comparison to a normal distribution
  - Coefficient of kurtosis – used for comparison to a normal distribution

SAPHIRE Uncertainty Analysis

- SAPHIRE supports multiple distributions, most of which can be defined with two statistical parameters (although some take more)
  - First parameter – mean failure probability calculated from the data input into the Failure Data section in SAPHIRE's basic event input screen
  - Second parameter – specific to the particular uncertainty distribution

- SLS PRA uses lognormal distribution
  - Parameters are the mean of the lognormal distribution and the upper 95% Error Factor (EF)
  - Occasionally, information will need to be converted into the required input parameters
    - If probability distribution is not known, but median and standard deviation is available, then these two inputs can be converted into the associated mean and EF.

SAPHIRE Correlation

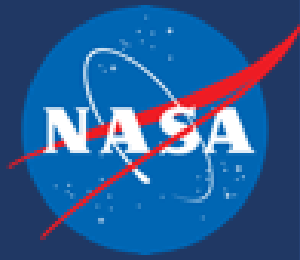
- Correlation between events
  - Used to identify basic events whose failure data are derived from the same data source
  - Described as a “lack of knowledge” dependency that is induced because of the way the data are used
  - Correlated uncertainty distributions must be distinguished from the independence of the basic events
  - User must set up a correlation class labeling scheme for basic events in the database
  - Compound events or identifying a basic event as a “template” may also be used to correlate failure rate basic events
- Inherent limitation of SAPHIRE event correlation
  - Only identical basic events can share a correlation class
    - i.e., if the period of operating time for the components is not identical, then they cannot be put into the same correlation class

Types of Uncertainty

- Monte Carlo sampling
  - Simple Monte Carlo
    - Uses the assigned probability distributions for each failure rate basic event to calculate the probability distribution of the top fault tree
    - Each basic event uncertainty distribution is sampled using a random number generator to select the failure probability of the basic event
  - Latin Hypercube
    - Selects n values from each of the k variables, where n = number of probability areas and k = number of components. Each variable is divided into n nonoverlapping intervals based on equal probabilities for the intervals – equal probability areas
    - The n values obtained for component 1 are randomly paired with the n values of component 2. These n pairs are randomly combined with the n values of component 3, and so on and so forth.
    - Forms an n x k matrix where each row contains specific values for each of the k input variables to be used on the evaluation of the cut sets.

References

- SAPHIRE Version 8: Technical Reference (NUREG/CR-7039, Vol. 2) (2011)
- System Modeling Techniques for PRA P-200, U.S. NRC, INL (2009)
  - https://www.nrc.gov/docs/ML1204/ML12044A155.pdf



BACKUP

SAPHIRE Correlation cont'd

- Example: a cut set with two components, q_1 and q_2
  - If independent, then Q = q_1 * q_2
  - Expected value of Q is given by $E(Q) = E(q_1)E(q_2)$
- If the components are identical and $q_1 = q_2 = q$, then the equations above reduce to
  - $Q = q^2$
  - $E(Q) = E(q^2)$
- Standard identity from Statistics says that
  - $E(q^2) = [E(q)]^2 + var(q) > [E(q)]^2$
- This is why the point estimate and the mean of the uncertainty distribution are not equal in PRAs.

SAPHIRE cont'd

- Aleatory Uncertainty
  - Also known as Stochastic
  - This type of uncertainty cannot be reduced
  - Example: uncertainty in occurrence of time of event (when during the mission will the failure occur if it occurs at all?)
- Epistemic Uncertainty
  - Also known as "State-of-Knowledge"
  - This type of uncertainty can be reduced with further testing/operation
  - Example: uncertainty in the rate of occurrence (component failure rate)

National Aeronautics and Space Administration

PRA Overview

By Sonali Siriwardana

What is PRA?

- Quantification of event probabilities of failures
- PRA process seeks to answer 3 questions:
  1. What kinds of events/scenarios can occur?
  2. What are the likelihoods and associated uncertainties of the events/scenarios?
  3. What consequences can results from the events/scenarios?
- Model are developed in “failures space” (vs. “success space”)
- Multiple tools can be used
  - Excel
  - CAFTA
  - 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 used by NASA.

Decision Context

- PRA can be applied from concept to decommissioning during the life cycle of a project, but is best applied at the beginning of the project life cycle to mitigate risk.
- If a PRA model is used to influence a design, then it should be structured to suit this purpose
- Performance Measures are defined according to decisions being supported
- Identify the performance measures:
  - P(loss of life or injury/illness to the crew)
  - P(loss of mission)
  - P(damage to the habitat)
  - P(crew evacuation)

Fault Trees

- Top-Down scenario-based analysis
- Used to analyze initiating or pivotal events in terms of more detailed causal events
- Breakdown until
  - Data is available for quantification (e.g., component, box level data)
  - Scope of work dictated by requirements'
- Lowest level, called basic event, is largest level of assembly for which data are available

Probability

- Probability
  - $0 < P(A) < 1$
  - For two mutually exclusive events A and B: $P(A \text{ or } B) = P(A) + P(B)$
- Probability of failure represents the likelihood that a system/component will fail
  - Used to assess the risk of a single event or outcome of a system
- Failure rate describes the frequency of failures over a specific time period
  - Used to understand the lifespan and reliability of a component or system
- Independent vs Dependent Failures
  - Independent: failure or unavailable state of a component during the mission time that does not depend on another component's functionality
  - Dependent: failure or unavailable state of more than one of the same type of component during the mission time and due to the same shared cause.
- Initiating Events
  - Identify any failures, or initiating events, that can lead to Loss of Mission/Habitat

End States: Scenario Development

- Now we identify the Loss of Mission/Habitat scenarios that failures will lead to (i.e. Contained tank failures, etc.)
- Examples:
  - Loss of life
  - Loss of facility
  - Shutdown
  - Fire
  - Explosion
  - Leak
  - Exceeding limits

Using PRA to Influence Design

- Assess a system/subsystem based on current and proposed/alternate designs to compare risk profiles
  - Perform trade studies on applicable systems/subsystems to determine most efficient options
  - Assess importance analyses on top tree/overall model to understand dominant contributors and how the risk shifts depending on the failure probability of components of interest
  - Calculate uncertainty to understand the probability distribution for each design
  - Calculate contribution to loss of crew risk estimate
  - Discuss risk mitigation strategies for each design

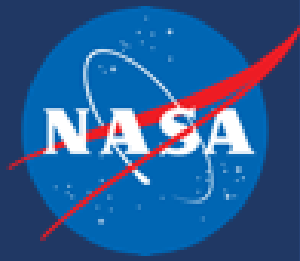
Milestone Reviews

- SRR
  - Risk modeling is consistent with concept studies to characterize mission risk for the habitat
  - Quantify major risk drivers and understand relative risk differences among
  - Development of loss of habitat/loss of mission scenarios
- SDR
  - Refines top-level risk models for preferred configuration of habitat and risk analysis for design and operational concept trade studies
  - Loss of crew assessment is developed in coordination with other disciplines
- PDR
  - Continue to inform design trade studies by analyzing design alternatives for risk impact
  - Development of fault tree probabilistic failure logic used to quantify loss of mission risk using the SAPHIRE tool
  - Baseline MPH PRA report is created
  - Submittal of MPH PRA loss of mission risk estimate to the Cross-Program PRA team (XPRAT)

Milestone Reviews cont'd

- CDR
  - MPH PRA loss of mission and loss of crew modeling and documentation will be developed in parallel and will mirror design maturity
  - Integrated modeling update uses analysis products and data from approved element documents
  - MPH PRA report is updated and provided to the program
  - Assist XPRAT with model integration for entire mission
- DCR
  - PRA helps define operations and process controls to mitigate and control risks
  - Risk data and information is
    - used to support risk assessment objectives and provides quantitative risk information for data package required for human-rating certification
    - Verification of MPH probabilistic requirements for loss of crew and loss of mission
- Beyond DCR (mature flight)
  - Perform vehicle level risk assessments and targeted risk analyses of anomalies and flight constraints
  - Evaluate potential corrective actions for risk impact

Software



- Physical
  - Line count regardless of whether it is a logical operator or not
    - Includes variables, declarations, blocking, etc.
  - More conservative than logical SLOC
- Logical
  - Active lines
  - This is what should be used for the PRA analysis
- Software (SW) is not modeled as a fault tree
  - Not concerned with how SW interacts with itself
  - SW risk that can cause loss of mission is a single point failure
  - SW risk can be evenly distributed as long as all SLOC is accounted for in the analysis
- Most failures result from system entering an operational regime that is unanticipated or poorly understood

Contribution to Loss of Crew Evaluation

- Contribution to loss of crew risk will depend on the crew's ability to evacuate the MPH
- Work with Gateway/Environmental Health Program/Human Landing System

PRA Communication

- Always present the bottom line up front
  - Understand the target audience and cater the results to them (e.g., if presenting to a board, then is the PRA meeting requirements?, etc.)
- When presenting results, format in tables that are easily readable
  - Do not present in Excel spreadsheet
  - Have all assumptions, limitations, and variables defined clearly

References

- SLS-PLAN-064, Space Launch System (SLS) Probabilistic Risk Assessment (PRA) Plan, Revision A (2014)

National Aeronautics and Space Administration

SAPHIRE Overview

By Sonali Siriwardana

Table of Contents

SAPHIRE Overview

- Probabilistically quantify and evaluate hazards
- Capabilities:
  - PC-based fault tree and event tree text editors
  - Cut set generation and quantification
  - Importance measures and uncertainty modules
  - Relational database with cross-refereeing features
  - Common Cause Failure basic event capabilities
- Output of SAPHIRE will provide Loss of Mission or Loss of Crew frequency
  - Identify end state scenarios and their frequencies
  - Basic event sequences that lead to loss of mission/loss of crew
  - Dominant contributors to loss of mission/loss of crew

Fault Trees

- SAPHIRE evaluates fault trees to find system minimal cut sets and the system failure probability
- Represented in a “top-down” fashion
- Gates specify logical combinations of basic events that lead to “top” (end state) event
- Used to identify interrelationships between events
- Creating fault trees:
  - Create a folder in preferred destination to save project
  - Double click *New Fault Tree* in left panel
  - Name Project and select folder to save it in
  - Follow naming convention to create name and add description, hit ok
  - Note: Fault Trees will default to an OR top gate
    - To change this, double click on the fault tree, and select the AND gate option from the dropdown menu.

Basic Events

- Represent a fault (e.g., hardware failure, software failure, adverse condition, etc.)
- Create Basic Events
  - Double click *New basic event* in top left panel
    - Option to check “Template” event if creating similar basic events
  - Fill out the name and description.
  - In the “Failure Model” row, select the type of failure data from the dropdown menu
    - Ex. 1: If selecting “1: Failure Probability”, then enter the corresponding mean failure probability
    - Ex. 2: If selecting “3: Fails to Operate (without repair), then enter lambda and mission time
  - Under “Uncertainty Distribution” select the distribution for the data set
    - Ex.: “Log Normal” and enter the Error Factor (see more on Uncertainty chart)
  - Correlation classes may be specified IF basic events are using data derived from the same data source. If events are correlated, a name for the correlation class may be added. Events in the same class are 100% correlated.
  - Compound Events may also be created for correlating events
    - In the Failure Model dropdown menu, select “C - Compound Events”
    - In the Library dropdown menu, select PLUGUTIL
    - In the Procedure dropdown menu, select MULTIPLY
    - In the Input Parameters dropdown menu, add all applicable basic events

Generating Cut Sets

- Right click the top fault tree in left panel and select “Solve”
  - If there is a cutoff value, enter the global cutoff value, then click the “solve” button
  - The output will total the number of cut sets and total risk estimate
- Click the “Cut Sets” button at the bottom of the display window
  - The results will show each cut set and its consisting basic events, its rank in terms of probability, and percentage of total risk
  - Make sure all cut sets have a probability value above zero
  - Hit “Publish” if a report of the cut sets is needed – can choose in what format the results are published
  - “Slice” will allow dividing the risk up by different categories (by % contribution, a set values, etc.)

Uncertainty

- Monte Carlo
  - A fundamental approach which makes repeated quantifications of the system cut sets using each random variable sampled from the basic event uncertainty distribution.
- Right click top fault tree in left panel and select “View Uncertainty”
  - Set a number of samples (number of samples SAPHIRE takes to develop the distribution)
  - Do not have to select a random seed number
  - Select Monte Carlo
  - A cumulative distribution chart will be displayed

Importance Analysis

- Provides quantitative perspective on dominant contributors and sensitivity of risk to changes in input
  - Importance Analysis tells you how basic events are impacting the model, i.e. risk drivers in the model
- Multiple measures of importance: Fussell-Vesely, Birnbaum, risk reduction worth, risk achievement worth, etc.

- Fussell-Vesely measure
  - Measure overall percent contribution of cut sets containing a basic event of interest to the total risk
  - Calculated by finding the value of cut sets that contain the basic event of interest and dividing by the value of all cut sets representing the total risk
  - $\frac{[R(base) - R(x_i = 0)]}{R(base)}$ OR $\frac{R(x_i = 1)}{R(base)}$

*Where base = total cut sets, R(xi) = cut sets that have xi, and R(xi=0) are all cut sets without xi

Importance Analysis

- Birnbaum
  - Importance measure for the probability of the top event given that event x occurred minus the probability of the top event given that event x did not occur.
  - $R(x_i = 1) – R(x_i = 0)$
- Risk Reduction Worth
  - $\frac{R(base)}{R(x_i = 0)}$
- Risk Achievement Worth
  - $\frac{R(x_i = 1)}{R(base)}$

Importance Analysis

- Provides quantitative perspective on dominant contributors and sensitivity of risk to changes in input
  - Importance Analysis tells you which basic events are impacting the model the most, i.e. risk drivers in the model
- Fussell-Vesely measure
- After solving the top fault tree, to have SAPHIRE assess importance
  - Right click on the fault tree
  - Mouse over “Display”
  - Click Importance
  - Column “FV” or Fussell-Vessely will be the column we are looking at – all basic events falling above the 5E-03 value will be
    - Delete all phase splits/scenario splits/conditional events first since every basic event will get caught
    - Delete all events below the 5E-03 cut off.

Importance Analysis Limitations

- Exclusion of risk from the model
  - Ground Rules and Assumptions/Limitations of the model itself
- Truncation limits affect importance rankings
  - E.g., RAW – you may have many more important events with a cut off at 1E-10 vs 1E-7.

Data Loading

- Mar-D
  - Extracting/Loading
- Extract
  - Under File, select “Load/Extract”
  - Select a folder as a location for the extracted SAPHIRE files
  - Select applicable choices, but must select basic events, fault trees, and project
- Loading
  - Under File, select “Load/Extract”
  - Open the folder for the saved SAPHIRE files and select the .MARD file
  - Hit Process

References

- Idaho National Laboratory SAPHIRE Basics, Smith & Knudsen (2007)
- Idaho National Laboratory, Importance Measures
- SAPHIRE Version 8: Technical Reference (NUREG/CR-7039, Vol. 2) (2011)

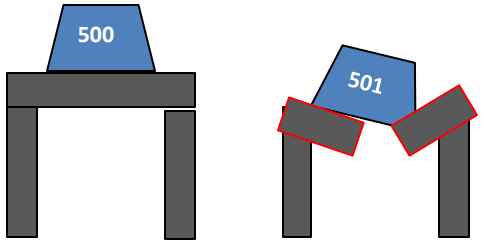
- Special thanks to Quinn Slaugenhoupt for the SAPHIRE 8 tool overview

Structural Probabilistic Risk Assessment (PRA) Training Module

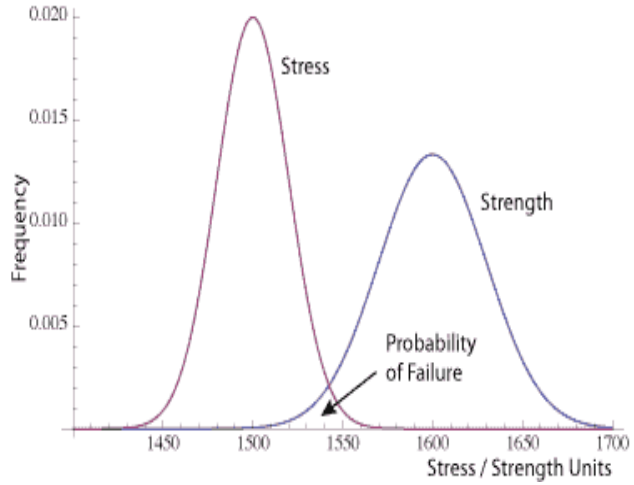
Becky Rea – 2018
Joseph Osowski – 2025 Updates

Structural PRA Strategy Background

- **For any part or component, there exists some load which, when imparted on the component, will cause the component to fail.**
  - Hypothetically, if you knew the exact strength of a part and the exact stresses applied with perfect accuracy, you could also know exactly what load would cause the part to fail.
    - Example: A table is able to withstand a 500N load. Any load greater than 500N is guaranteed to cause failure, and any load less than 500N will not cause failure.



- **In reality, these are not known with absolute accuracy.**
  - There is uncertainty in the underlying properties of the material that the table is made from.
  - There is uncertainty in the strength of the table and the analysis of that strength.
  - There is uncertainty in the load being applied to the table.
  - All these parameters can be represented by uncertainty distributions.



Ref: https://accendoreliability.com/wp-content/uploads/2013/02/stress-strength.png

- **Structural PRA modeling involves:**
  - 1) Describing these uncertainty distributions and
  - 2) Estimating the probability that the stress (burden) applied to the component exceeds the component's strength (capability).

SLS
SPACE LAUNCH SYSTEM

Overview of Key Terminology & Definitions

Factor of Safety, Safety Factor, Margin of Safety, and “Stress Max”

Factor of Safety, Safety Factor, and Margin of Safety

- **Factor of Safety, Safety Factor, and Margin of Safety are key parameters to understand for structural analysis.**
- **Factor of Safety (FoS) : "Part Strength" ÷ "Design Load".**
  - "Part strength" can be rephrased several ways: ultimate strength, part strength, component failure stress, etc.
    - Describes the point at which the component fails.
  - "Design load" can be similarly rephrased: stress of component under design load, stress, design load, etc.
    - Describes the load or stress the part is designed to withstand and operate under.
- **Safety Factor (SF): An additional "survival" factor applied to the design load.**
  - Often a design requirement.
  - From a design standpoint, a component must generally perform its function up to the design load limit. The component must survive up to (SF*Design Load).
- **Margin of Safety (MoS): A measure of how well a part meets the required safety factor.**
  - Margins of Safety are often the output of structural analysis, and **they are the key input to the structural PRA**.
  - Positive MoS: The SF is exceeded.
  - Negative MoS: The SF is not met.
  - Zero MoS: The SF is met exactly.

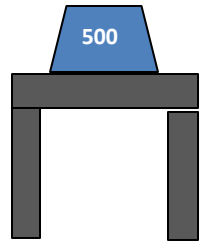
$$\boldsymbol{MoS} = \frac{Part\ Strength}{(Design\ Load) \times SF} - 1 \qquad \boldsymbol{FoS} = \frac{Part\ Strength}{Design\ Load} = SF(MoS + 1)$$

SLS

Factor of Safety, Safety Factor, and Margin of Safety

- **Example: A customer wants a table that is expected to regularly encounter and withstand a load of 500N. The customer also has a 1.4 Safety Factor requirement.**

- **Your engineering department designs a table and then performs a structural analysis of the table design.**
  - The initial structural analysis shows that the table will fail when experiencing a 600N load.
  - The FoS for this design is 600N/500N = 1.2
  - The MoS for this design is $\frac{600N}{(500N)\times 1.4} - 1 = -0.14$
    - Negative MoS; the SF requirement is not being met.



- **Given the negative MoS, the engineering team re-designs the table and then performs another structural assessment.**
  - The updated design and analysis show that the new table will fail when experiencing a 1000N load.
  - The FoS for this design is 1000N/500N = 2.0
  - The MoS for this design is $\frac{1000N}{(500N)\times 1.4} - 1 = 0.43$
  - Engineering reports the 0.43 MoS, showing the SF requirement is met.

$$\boldsymbol{MoS} = \frac{Part\ Strength}{(Design\ Load) \times SF} - 1 \qquad \boldsymbol{FoS} = \frac{Part\ Strength}{Design\ Load} = SF(MoS + 1)$$

Factor of Safety and "Stress Max"

- **Before the stress vs. strength distributions are discussed, it is important to recognize a "hidden" term related to the Factor of Safety.**
- **Recall: The Factor of Safety is defined as: "Part Strength" ÷ "Design Load".**
  - FoS is a **ratio** between the strength of the part and the design load.
- **Given that FoS is a ratio, FoS can also be thought of as the ultimate strength of an "equivalent" part (with the same FoS) when the design load equals 1. We call this "adjusted" design load "Stress Max":**

$$\frac{Factor\ of\ Safety}{1} = \frac{Equivalent\ Part\ Strength}{\boldsymbol{Stress\ Max}} = \frac{(actual)\ Part\ Strength}{(actual)\ Design\ Load}$$

- **The stress vs. strength (or burden vs. capability) analysis relies on the ratio of the "Strength of the Component" to the "Stress of the Components under Design Loads".**
  - The actual strength and stress information is not often reported.
  - Margin of Safety is typically reported instead as it readily shows whether a SF requirement is met.
- **Rather than using the actual "Ultimate Strength of the Component" and "Stress of the Components under Design Loads", the "Factor of Safety" and "Stress max" (Stress Max = 1) are used instead.**
  - Stress Max = 1 is the "hidden" term that arises by relying on the ratio rather than the raw stress/strength.
  - The load and strength distributions are dimensionless.

SLS
SPACE LAUNCH SYSTEM

Estimating the Uncertainty Distributions

Load Distribution, Material Strength Distribution, and overall Component Strength Distribution

Estimating the Load Distribution

- **Three parameters are used to create a lognormal distribution for the "load" (stress, burden, etc.) the components experience:**
  - CV_{load}: the coefficient of variation assumed for the loads that the component is subjected to.
    - Ratio between the standard deviation and mean; describes how 'wide' the distribution is.
    - Generally, CV_{load} is assumed to be 0.2 (describes a healthy amount of uncertainty in the component loading)
  - Z_{max} – The number of transformed normal standard deviations that is assumed between the loads that are used in the analysis (i.e., design loads) and the mean load the part will actually experience. Z-score for Stress Max.
    - Generally, Z_{max} is assumed to be 3 or -3 (implies that the stress analysis is conservative and uses the 99/95 confidence expected load).
  - Stress max – The stress that is expected for the component when applying the design loads.
    - Since we're using Factor of Safety for the strength estimate, "Stress max" = 1
    - If using actual stresses for the strength vs. stress calculation, this value is the expected stress when design loads are applied.
- **Assuming a lognormal distribution, the load distribution parameters (σ_L and μ_L) are described by:**

$$\sigma_L = \sqrt{\ln(CV_{load}^2) + 1} \qquad \mu_L = \ln(Stress\ Max) - Z_{max}\sigma_L$$

Estimating the Component Strength Distribution (1/2)

- **To arrive at the overall strength (capability) distribution, the uncertainty in material strength must first be accounted for.**
- **Three parameters are used to find the component strength mean and standard deviation:**
  - $CV_{strength}$: the coefficient of variation assumed for the material strength.
    - Ratio between the standard deviation and mean; describes how 'wide' the distribution is.
    - Generally, $CV_{strength}$ is assumed to be 0.05
    - Different values can be used depending on the materials used in the components.
    - Typically assume low $CV_{strength}$ values for metals (0.03-0.05, low variation in properties, well understood)
    - Composites, plastics, or newly developed materials may necessitate higher values (0.08-0.15, higher variation & uncertainty).
  - $K_{strength}$ – The number of transformed normal standard deviations between the material strength capability assumed in the analysis and the mean material strength capability. Reflects the conservatism in materials properties used for structural analyses.
    - Generally, $K_{strength}$ is assumed to be 3 (implies that the stress analysis is conservative and uses the 99/95 confidence expected capability).
  - Factor of Safety – The ratio between the part ultimate strength and the design load. Calculated from MoS and SF.
    - A "global" SF value, such as 1.4, is often assumed to find the FoS.
    - If using actual stresses for the strength vs. stress calculation, the actual stress capability of the part would be used rather than the FoS.
- **Assuming a normal distribution of the underlying strength data and no correction for anomalies, the component strength mean and standard deviation (μ_m and σ_m) are described by:**

$$\mu_m = \frac{FoS}{1 - K_{strength} CV_{strength}}$$

$$\sigma_m = CV_{strength} \mu_m$$

Estimating the Component Strength Distribution (2/2)

- **Given the component strength mean and standard deviation, and assuming that the component strength distribution is lognormal, the lognormal distribution is described by parameters:**

$$\mu_s = ln\left(\frac{\mu_m^2}{\sqrt{\mu_m^2 + \sigma_m^2}}\right) \qquad \sigma_s = \sqrt{\ln\left(1 + \frac{\sigma_m^2}{\mu_m^2}\right)}$$

Recall:

$$\mu_L = \ln(Stress\ Max) - Z_{max}\sigma_{load} \qquad \sigma_L = \sqrt{\ln(CV_{load}^2) + 1}$$

- **Failure occurs when the applied load exceeds the strength of the component, i.e., whenever S-L<0**
  - Therefore, the probability of failure of the component is calculated as Pr(S-L<0)
  - Using normal distribution theory, we can transform S-L to a standard normal distribution z ~N(0,1) by subtracting the means and dividing by the standard deviation.
  - The Excel NormsDist function can then be used to easily calculate the probability of failure.

$$Z = \frac{\mu_s - \mu_L}{\sqrt{\sigma_s^2 + \sigma_L^2}} \qquad P(Failure) = 1 - NormsDist(Z)$$

SLS
SPACE LAUNCH SYSTEM

Structural PRA Method Summary

Putting it All Together: SLS Structural PRA Method

Variable	Typical Value/Formula
SF	1.4 (assumed) Often a Design Requirement
MoS	Input from Structural Analyses $MoS = \frac{part\ strength}{(design\ load) \times SF} - 1$
FoS	$FoS = \frac{part\ strength}{design\ load}$ $FoS = SF(MoS + 1)$
Z_{max}	3 (assumed)
StressMax	$Stress\ Max = 1$
CV_{load}	0.2 (assumed)
$K_{strength}$	3 (assumed)
$CV_{strength}$	0.05 (assumed)

- **Estimate Load Distribution parameters:**

$$\mu_L = \ln(Stress\ Max) - Z_{max}\sigma_L \qquad \sigma_L = \sqrt{\ln(CV_{load}^2) + 1}$$

- **Estimate component strength mean and standard deviation:**

$$\mu_m = \frac{FoS}{1 - K_{strength}CV_{strength}} \qquad \sigma_m = CV_{strength}\mu_m$$

- **Estimate Component Strength Distribution parameters:**

$$\mu_s = ln\left(\frac{\mu_m^2}{\sqrt{\mu_m^2 + \sigma_m^2}}\right) \qquad \sigma_s = \sqrt{\ln\left(1 + \frac{\sigma_m^2}{\mu_m^2}\right)}$$

- **Transform to standard normal distribution and calculate P(Failure):**

$$Z = \frac{\mu_s - \mu_L}{\sqrt{\sigma_s^2 + \sigma_L^2}} \qquad P(Failure) = 1 - NormsDist(Z)$$

SLS
SPACE LAUNCH SYSTEM

Putting it All Together: SLS Structural PRA Method

Variable	Description	Value/Formula
SF	Safety Factor. SF is essentially a factor of safety applied to the design limit load, i.e., the load used for analysis. Often a design requirement. From a design standpoint, a component must generally perform its function up to the design load limit. The component must survive up to (SF * Design load).	1.4 (assumed)
MoS	Margin of Safety. Input from structural analyses. MoS is essentially a measure of how well a part meets the required safety factor. A positive MoS means the SF is being exceeded, a negative MoS means the SF is not being met, and a zero MoS means the SF is met exactly.	Input $MoS = \frac{part\ strength}{(design\ load) \times SF} - 1$
FoS	Factor of Safety – Ratio between the part ultimate strength and the design load. Calculated.	$FoS = \frac{part\ strength}{design\ load}$ $FoS = SF(MoS + 1)$
Z_{max}	The number of transformed normal standard deviations that is assumed between the loads that are used in the analysis (i.e., design loads) and the load mean.	3 (assumed)
StressMax	StressMax is the standardized load related to the Factor of Safety ratio. StressMax=1 by convention.	$\frac{FoS}{1} = \frac{FoS}{StressMax} = \frac{strength}{load}$
CV_{load}	Coefficient of variation for the loads the component is subjected to. A measurement of uncertainty of the design loads.	0.2 (assumed)
$K_{strength}$	The number of transformed normal standard deviations between the material stress capability assumed in the analysis and the mean material stress capability. Reflects the conservatism in materials properties used for structural analyses.	3 (assumed)
$CV_{strength}$	Coefficient of variation for the material strength. A measurement of uncertainty of the material strength properties. Typically assume low values for metals (0.03-0.05, low variation in properties, well understood) and higher values for composites, plastics, or newly developed materials (0.08-0.15, higher variation & uncertainty).	0.05 (assumed)

References

- Interrelation between Safety Factors and Reliability, NASA/CR-2001-211309, Elishakoff (2001)
- Panel Failure Example Calculation, Mike Kelly, Bastion Technologies, Inc., MSFC