Decisions Under Risk
– Mathematics in Action –

Tim C. Adams, ASQ CRE
NASA Kennedy Space Center
Engineering Directorate
Tim.Adams@NASA.gov

American Mathematical Association of Two-Year Colleges
44th Annual Conference
November 15, 2018 (revised)
Presentation Objectives

♦ Demonstrate the benefit of Mathematics in the work place.
  – “Where is this stuff ever used?”
  – “Did it really help?”

♦ Provide real examples (questions) where the NASA program/project manager was faced with making a decision involving technical risk with uncertainty.

♦ Provide insights on how a Reliability-Risk Engineer responded to these questions (problems).

♦ Observe when the probabilistic method (as opposed to deterministic method) was and was not used.
Thinking Styles and Belief Systems

♦ **Big Q vs. Little q**
  - Qualitative (expert opinion) vs. quantitative (mathematical analysis)
  - Determinism (certain) vs. Probabilism (uncertain)

♦ **Uncertainty** does not imply no knowledge, but it does imply the exact outcome is not completely predictable. Most observable phenomena contain a certain amount of uncertainty.

♦ “Basically, an **anti-empirical system** states that things may look like X, but in reality they are Y. Between us and **reality** is a screen of ideology.”

  “God and Mankind: Comparative Religions,” Robert Oden (former Professor and Chair, Department of Religion, Dartmouth College), The Great Courses, Lecture 2, 1998
“Don’t bring me a perfect answer after launch.”

A NASA Johnson Space Center Manager’s directive to his safety and mission assurance engineers

– Use the probabilistic method when necessary.

In engineering assurance, there are four types of uncertainty.

1. Aleatory Uncertainty or Observed Randomness
2. Parameter (Statistical) Uncertainty
3. Model Uncertainty
4. Completeness Uncertainty

The last three types are called epistemic uncertainty, the state of knowledge and deals with non-observable quantities.
## Engineering Assurance (Specialty Engineering)*

<table>
<thead>
<tr>
<th>Safety: Freedom from accident and loss</th>
<th>Usability: Human interfaces</th>
<th>Supportability and Serviceability: Service throughout the planned life cycle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reliability: Likelihood of having an uptime (failure-free) state for a stated duration or load</td>
<td>Maintainability: Likelihood of returning to an uptime state during maintenance or repair</td>
<td>Availability: Likelihood a repairable item has an uptime state; $f (R, M) = A$</td>
</tr>
<tr>
<td>Producibility: Ease and economy of producing or manufacturing</td>
<td>Affordability: Total cost of ownership and not only system acquisition cost</td>
<td>Disposability: Disassembly and disposal (environmental stewardship)</td>
</tr>
</tbody>
</table>

*Engineering assurance* (as opposed to design engineering and engineering management) identifies and addresses issues and hazards early (i.e., during design, not during operation).
Risk as a Concept

- Risk is potential loss or potential gain.
- Thus, risk is the uncertain deviation (delta) in the execution of a management plan.
- Reference: ISO 31000.
- When limited to potential loss:
  - Risk is a qualitative or quantitative estimate of the potential loss occurring due to natural or human activities.

Risk as an Operation

- Both potential loss and gain:
  Actual results = Planned results +/- Risk
- Only potential loss:
  - Scenario x: What can go wrong?
  - Likelihood for x: What is the probability it will happen?
  - Consequence for x: What is the impact if it did happen?
  - Risk measure for x = (Likelihood) * (Consequence). This assumes consequence can be and wants to be measured.
Good Decision = Good Information * Enough Processing Time

- “To a great extent, the successes or failures that a person experiences in life depend on the decisions that he or she makes.
- The person who managed the ill-fated the space shuttle Challenger mission is no longer working for NASA.
- The person who designed the top-selling Mustang became the president of Ford.
- Why and how did these people make their respective decisions?”

Five Ways: Deciding about Risk

1. Accept (retain, engage, fight).
2. Avoid (run, flight).
3. Hold (freeze; get information to later select one of the other four).
4. Mitigate (change something to reduce the risk; countermeasure).
5. Transfer (share the risk).

Quantitative Analysis for Management, 6th Ed, Render & Stair
Systems Thinking and Measuring Performance

- **System**: A collection of different elements that together produce results not obtainable by the elements alone.
- **Metric**: The comparison of the current state to the desired state.
- **System Metrics**: Effectiveness, efficiency, and appeal (E-e-a).

```
Start → Goal → Desired State → Metric
Work Process → Current State

Not OK → Decision
Not Sure → Risk Analysis

OK
```
Details: (Reliability + Safety) ⊂ Risk ⊂ Good Decision

- **Reliability** is the likelihood an item will perform its intended function for a specified period of time (or number of demands or load) with no failure under stated conditions.

- The measure for “not reliable” combined with the measure for “not safe” make a **risk** (potential loss) measure or point in a matrix.

- Understanding and prioritizing risk helps managers and engineers to make “**risk-informed**” decisions.
When reliability ($R$) is probability of success (uptime state) and Unreliability ($U$) is probability of failure (downtime state), then:

- $R + U = 1$. Thus, $U = 1 - R$.
- $U$ is the likelihood axis in a risk matrix.

Reliability is...

For a stated mission time (duration as time or cycles) or stress (load):

Under stated conditions (environment).

1. Reliability ($R$) does not address or model Maintainability ($M$). $M$ is the item’s design in regards to the need for, ease to perform, and amount of downtime for maintenance, repairs, and replacements. Availability ($A$) addresses and models both $R$ and $M$. $A$ is a math function of $R$ and $M$.

2. A description of intended function includes the boundaries of the item and the definitions of success and failure.

3. Types of input data used in RMA analyses:
   - Time to failure with no maintenance or repair by failure mode. This data type models Reliability.
   - Time to failure with time to return service. This data type being a pattern of uptimes with corresponding downtimes models Availability.
   - Stress-Strength (Load-Capacity) Interference. This data type models failures caused by variation.

4. Time to failure (or uptime) data is typically stated in hours or as number of successes (demands or cycles) out of a number of attempts (trials). The latter is known as success-failure or pass-fail data.

5. Other reliability analysis techniques used to design reliability systematically include Worst Case, Sneak, Durability, Thermal, and Electromagnetic Analyses. Use testing to verify the results of the analysis.
Details: Data Types used in Reliability Analyses

- The **item under study** for a reliability analysis can be hardware, software, orgware (humans, human processes), or any combination.

- Quantitative reliability typically encounters **three types of data**:
  1. **Time-based (clock) data**
     - Continuous
     - **Weibull** (uptime), **Log-normal** (downtime).
  2. **Event-based (demand) data**
     - Discrete
     - **Binomial** (x or more), **Poisson** (x or less).
  3. **Stress (load) and strength (capacity) data**
     - For example, use **normal** distribution’s mean and standard deviation of the item’s stress and item’s strength to calculate the **probability of failure**, the overlap in the distributions’ tails.
     - **Note**: A safety factor does not characterize the item’s uncertainty in stress and strength.

This area corresponds to the **probability of failure** due to variation **uncertainty** in stress and strength.
**Tutorial: System Reliability (via RBDA*)**

1 - Given

a. **System Description:** System X must satisfy requirements A and B. B is dependent on the success of A. B has two independent elements, denoted B1 and B2. At least one of the two B elements must be successful. The diagram that follows is the block diagram for System X’s two requirements.

![System X Diagram]

b. **Data (3 types):** (1) The table provides the point estimate values (not the probability distributions) for the likelihood of success (reliability) for each *requirement* based on experience. (2) If needed, assume the likelihood of the *initiating event* that triggers the need for System X equals one. (3) The quantity or measure for failure *consequence* at this time will be a placeholder since it is unknown.

c. **Problem Statement:** What is the likelihood System X will successfully perform its intended function?

<table>
<thead>
<tr>
<th>Event</th>
<th>Reliability</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>90%</td>
</tr>
<tr>
<td>B1</td>
<td>80%</td>
</tr>
<tr>
<td>B2</td>
<td>70%</td>
</tr>
</tbody>
</table>

*RBDA* = Reliability Block Diagram Analysis. The reliability of each item (block) are required inputs to perform a RBDA.
2 - Analysis

d. **Outcome Statement:** If $S$ denotes success and $S'$ denotes the complement of success (failure), and there is no degraded mission state (partial success), then $S = A$ and ($B_1$ or $B_2$ given $A$).

e. **Event Tree Method:** Events $A$, $B_1$, and $B_2$ generate eight ($2^3$) possible scenarios. Scenarios need to be assessed for applicability. As given, since $B$ is dependent on $A$, then $P(B_i|A') = P(A'|B_i) = 0$. Thus, $P(A'$ and $B_i) = 0$. Therefore, events $A'$ and $B_i$ as are mutually exclusive (i.e., if $A'$ occurs, then $B_i$ cannot, and conversely). Also, since it is given events $B_1$ and $B_2$ are independent, then $P(B_1$ and $B_2) = P(B_1)*P(B_2)$.

<table>
<thead>
<tr>
<th>Scenarios</th>
<th>Scenario Likelihoods</th>
<th>Outcomes (End States)</th>
<th>Outcome Likelihoods</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$A'$</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$B_1$</td>
<td>1*.9*.8*.7 = 0.504</td>
<td>Success</td>
<td></td>
</tr>
<tr>
<td>$B_1'$</td>
<td>1*.9*.8*.3 = 0.216</td>
<td>Success</td>
<td></td>
</tr>
<tr>
<td>$B_2$</td>
<td>1*.9*.2*.7 = 0.126</td>
<td>Success</td>
<td></td>
</tr>
<tr>
<td>$B_2'$</td>
<td>1*.9*.2*.3 = 0.054</td>
<td>Failure</td>
<td></td>
</tr>
<tr>
<td>Sum of Scenario Likelihoods</td>
<td>1.000</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Sum of Scenario Likelihoods</th>
<th>1.000</th>
<th>1.000</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Success</td>
<td>0.846</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failure</td>
<td>0.154</td>
</tr>
</tbody>
</table>

f. **Formula Method:**

\[
P(\text{System X Success}) = P(A \text{ and } [B_1 \text{ or } B_2]) = P(A)*[1-(1-P(B_1)*(1-P(B_2)) = (0.9)*[1-(1-0.8)*(1-0.7)] = (0.9)*[1-(0.2)*(0.3)] = (0.9)*[0.94] = 0.846.\]

\[
P(\text{System X Failure}) = 1-P(\text{System Success}) = 1-0.846 = 0.154. \text{ System X's Risk} = (0.154)*\text{Consequence}.\]
Example #1: The Problem

◆ A recent system failure caused major embarrassment as well as much expense. Should this system be upgraded or replaced with new technology?

◆ If upgraded, identify the system elements causing the trouble and determine the minimum required reliability to complete missions over the life of the program.
Example #1: This problem occurred with a Space Shuttle Orbiter’s Fuel Cell

A fuel cell on a Space Shuttle Orbiter caused a minimum duration flight (MDF) during STS-83. In addition to the MDF, a previous launch delay and numerous maintenance actions during “vehicle turnaround” made this subsystem a serious candidate for improvement.
A detailed reliability and maintenance (R&M) analysis and assessment report on all fuel cell line replaceable units (LRUs) from the STS-26 to STS-85 time period was completed.

This R&M assessment was instrumental in the decision to change regulator material in all fuel cell LRUs for $12M instead of replacing with a new design estimated at $50M.
Example #2: The Problem

During a final review of a system prior to shipment, questionable test data appears on one of the system’s components.

Assuming all other system elements are believed to perform as expected, what is the risk in shipping as is?

In particular, what is the likelihood the system will not work (i.e., perform to meet its minimum requirements)?
Example #2: This problem occurred with the International Space Station’s Gyroscopes as a payload

STS-118 Canadian Space Agency Astronaut and Mission Specialist Dafydd “Dave” Williams is attached to an Adjustable Portable Foot Restraint on the end of the Space Station Remote Manipulator System Canadarm 2 as it transports the new Control Moment Gyroscope (CMG) to the External Stowage Platform 2 for temporary stowage.
Example #2: System Configuration for ISS Gyros

CMG, the system

Gyro, a subsystem

Sensor, a component

Input

Output
Example #2: Reliability in Action

- Vendor test data generated a concern with the expected reliability of the Hall resolvers (sensors). These sensors are used on the Control Moment Gyros (CMGs), a Space Shuttle payload planned for Space Station’s Flight 3A.

- A **reliability analysis** presented to the Space Station Control Board (SSCB) showed there was a 4-6% chance of not having a minimum CMG. A minimum CMG is at least 1 of 2 sensors working in each gyro and at least 2 of the 4 gyros working for 5, 7, or 9 thermal cycles.

- The **uncertainty** in the thermal-cycle count was because the sensor heaters on the Space Station would not be operational until after the sensors experienced an estimated number of thermal cycles.

- The **consequence** of not having a minimum CMG meant that 6 metric tons of propellant for a reboost would have to be consumed at a cost of $100 million.

- The **decision** was made to ship the CMGs as planned--which proved to satisfy the mission requirements both for the short and long terms.
Example #3: The Problem

- The test director wants to know: Can testing stop after receiving no failures in 360 tests on a life-critical item?

- In particular, does this testing certify that the item is safe?
Example #3: This problem pertained to the Astronaut’s Extravehicular Mobility Unit

Extravehicular Mobility Unit (EMU) is an independent system that provides environmental protection, mobility, life support, and communications for a Space Shuttle or International Space Station (ISS) crew member to perform extra-vehicular activity (EVA) in earth orbit.
Example #3: In particular, interpret test data

- The White Sands Test Facility (WSTF) conducted 360 tests to determine if ignition would occur during the presence of a small quantity of hydrocarbon oil in 100% oxygen under adiabatic compression, the compression heating of oxygen.

- None of the WSTF tests produced ignition. These tests were in response to a hydrocarbon-oil contaminate found in the Life Support System (PLSS) used in the Extravehicular Mobility Unit (EMU).
Example #3: This problem made the news!
Example #3: Reliability in Action (but limited)

♦ **Method 1** used **Classical Test Statistics** to determine the maximum failure probability with a high degree of statistical confidence. This failure probability did not meet the program’s failure-probability goal. Thus, *more testing required* if only this type of analysis (little q) was used for decision making.

♦ **Method 2** used **Ancillary Data** (i.e., similar test data) to identify a boundary for ignition and no ignition. This method was *not sufficient for decision making* since heat loss was not addressed.
Example #3: Reliability in Action (but limited)

- **Method 3** used the **Arrhenius Reaction Rate Model**. This model (pseudo-big Q) adjusted the failure probability found in the first method since all WSTF testing was done under stressed conditions (higher pressure). *The failure-probability goal was surpassed under certain assumptions.*

- **Method 4** used **Combustion Physics** (Semenov equations) to address the heat loss not addressed in Method 2. It was found that the reaction rate was not fast enough to cause ignition in the PLSS. Thus qualitatively (big Q), the *failure-probability goal was believed (decided) to be satisfied.*
Example #4: Obstacles for not having “zero defects”

- **Classical reasons** why failures occur:

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Overstressed</strong>: Applied stress exceeded the strength. Events external to design limits.</td>
<td><strong>Sneaks</strong>: The system does not work properly even though every element (part, process) does.</td>
</tr>
<tr>
<td><strong>Variation</strong>: Stress and strength are not fixed. Variation causes one to interfere with the other.</td>
<td><strong>Errors</strong>: Incorrect specifications, design, software coding, assembly, test, use, or maintenance.</td>
</tr>
<tr>
<td><strong>Wearout</strong>: Fatigue. An item is strong at the start of its life and becomes weaker with age.</td>
<td><strong>Other</strong>:</td>
</tr>
</tbody>
</table>

- Knowing the **potential causes** of failures (defects, anomalies, loss of an item’s intended function) is fundamental to preventing them.
- There are different **perceptions** on what kinds of events might be classified as failures. Burning O-rings on the Space Shuttle boosters were not failures until …
- An organization’s reliability effort during design, development, production, operation, and service should address **anticipated causes** of failure as well as take in account the **uncertainty** involved.
Example #4: Reliability for zero failures (discrete data)

- Time-based data and event-based data are the data types most common in determining a measure for reliability.

- **Time-based data** is the item’s exposure time or run time (e.g., hours) from birth (new item) to death (failed item). **Event-based data** counts the number of failures incurred in the total number of trials or tests (n) placed on the item.

- Both classical and Bayesian statistics have methods to measure reliability when no failures occur. What follows is a method from classical statistics for event-based data.

- **For event-based data** (pass-fail data, Bernoulli trials) has no failures, the table provides the required number of consecutive successes (n) to demonstrate reliability at the level equal to the left side of a specified confidence interval. With failures, use the **Clopper-Pearson interval method**. Without failures, the Clopper-Pearson interval reduces to \( n = \ln(1 - \text{confidence})/\ln(R_L) \).

- **Example**: An item performed 300 times with 300 successful outcomes (no failures). As per the table, the demonstrated lower-bound reliability for this process is a little better than 0.99 with a 95% statistical confidence. Thus, the upper-bound failure probability is < 1%.

<table>
<thead>
<tr>
<th>Lower-Bound Reliability</th>
<th>Statistical Confidence</th>
<th>Exact Count</th>
<th>Rule of Thumb for Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.9</td>
<td>90%</td>
<td>22</td>
<td>2.30 x 10^9s</td>
</tr>
<tr>
<td>0.99</td>
<td>90%</td>
<td>229</td>
<td></td>
</tr>
<tr>
<td>0.999</td>
<td>90%</td>
<td>2301</td>
<td></td>
</tr>
<tr>
<td>0.9999</td>
<td>90%</td>
<td>23025</td>
<td></td>
</tr>
<tr>
<td>0.99999</td>
<td>90%</td>
<td>230257</td>
<td></td>
</tr>
<tr>
<td>0.999999</td>
<td>90%</td>
<td>2302584</td>
<td></td>
</tr>
<tr>
<td>0.9</td>
<td>95%</td>
<td>28</td>
<td>3.00 x 10^9s</td>
</tr>
<tr>
<td>0.99</td>
<td>95%</td>
<td>2994</td>
<td></td>
</tr>
<tr>
<td>0.999</td>
<td>95%</td>
<td>29956</td>
<td></td>
</tr>
<tr>
<td>0.9999</td>
<td>95%</td>
<td>299572</td>
<td></td>
</tr>
<tr>
<td>0.99999</td>
<td>95%</td>
<td>2995731</td>
<td></td>
</tr>
<tr>
<td>0.9</td>
<td>97.5%</td>
<td>35</td>
<td>3.69 x 10^9s</td>
</tr>
<tr>
<td>0.99</td>
<td>97.5%</td>
<td>367</td>
<td></td>
</tr>
<tr>
<td>0.999</td>
<td>97.5%</td>
<td>3687</td>
<td></td>
</tr>
<tr>
<td>0.9999</td>
<td>97.5%</td>
<td>36887</td>
<td></td>
</tr>
<tr>
<td>0.99999</td>
<td>97.5%</td>
<td>368886</td>
<td></td>
</tr>
<tr>
<td>0.999999</td>
<td>97.5%</td>
<td>3688878</td>
<td></td>
</tr>
<tr>
<td>0.9</td>
<td>99%</td>
<td>44</td>
<td>4.60 x 10^9s</td>
</tr>
<tr>
<td>0.99</td>
<td>99%</td>
<td>458</td>
<td></td>
</tr>
<tr>
<td>0.999</td>
<td>99%</td>
<td>4603</td>
<td></td>
</tr>
<tr>
<td>0.9999</td>
<td>99%</td>
<td>46049</td>
<td></td>
</tr>
<tr>
<td>0.99999</td>
<td>99%</td>
<td>460515</td>
<td></td>
</tr>
<tr>
<td>0.999999</td>
<td>99%</td>
<td>4605168</td>
<td></td>
</tr>
</tbody>
</table>
Example #5: What is the trend for these discrete events?

That is, for each chart, is the trend increasing, decreasing, or constant?
Example #5: Determine the trend without graphing

- All graphs on the previous page use the same data!
- To test for a trend without graphing, use the Laplace Test (U), a test statistic.
- As a discrete event, 1600, the first event in the third histogram, could mean:
  - From a problem reporting database, the number of days from 01/01/09 (the start date of the trend period under study) to 05/20/13 (date of first event for item xyz).
  - From a machine-hour meter, the number of hours a machine (e.g., server) has operated from the time it was new and restarted after each upgrade or refurbishment.
- The Laplace Test applied to the four absolute times (1600, 2400, 2800, and 3000) and 3800 as the selected length of the observed period, make U, the test statistic, is +1.00 (< 0 is decreasing trend, 0 is no trend, >0 is increasing trend).
- Formally: Since $U = +1.00$, then $z = 1.00$ in a normal distribution table indicates the area to the left of $z$ is 0.8413. When a statistical hypothesis is based on a one-tailed test and it is decided to reject the null hypothesis ($H_0$: data has no trend) with ~84% confidence, the research hypothesis ($H_a$: data has trend, up since $z > 0$) is assumed true. The probability this decision is the wrong (Type I error) is ~16%. This type of error is denoted $\alpha$ and is called producer’s risk.
Example #5: This “dashboard” reports 182 trends as a score for 26 systems

```
<table>
<thead>
<tr>
<th>Trigger Rating Criteria</th>
<th>Trend Score</th>
<th>UA Trend Score (Date Sets 1-3 Only)</th>
<th>Failure Critically Measure</th>
<th>Average Age of Open Pending Case</th>
<th>Problem Count Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red (Most Unsolved)</td>
<td>≥ 1.65</td>
<td>≥ 0.25, if trend score ≥ 1.65</td>
<td>≥ 0.25</td>
<td>≥ 24 Months</td>
<td></td>
</tr>
<tr>
<td>Yellow (Undesired)</td>
<td>0.0 to 1.65</td>
<td>−1.00 to 0.00</td>
<td>0.33 to 1.65, if trend score exists</td>
<td>12 to 24 Months</td>
<td></td>
</tr>
</tbody>
</table>
```

```
| Tim.Adams@NASA.gov |
```

```
30
```
Example #5: Characterizing risk in previous report as a matrix
Example #6: Based on this test data, what is the probability of success when the stress ratio is 80% and mission time is 150 days?

Legend: Blue = Time of failure; Red = No failure since test stopped
Example #6: Use accelerated-life tests since test conditions vary

- It can be shown that $Ps = \exp[- (t / \theta)^\beta]$, the complement of the Weibull’s cumulative distribution function, satisfactorily models the life data sets for each of the six stress levels (s). $Ps = \text{probability of success}$ (as a point estimate; not interval estimate for uncertainty), $t = \text{mission time starting at zero}$, $\theta = \text{scale parameter}$, and $\beta = \text{shape parameter}$.

- **Step 1**: Use the "median-rank-Y-on-X-regression" method at each stress level to determine the Weibull parameters $\theta$ and $\beta$ at each stress level.

- In good accelerated-life tests, $\beta$ remains relatively constant at each stress level to assure the correct failure mode. For these data sets, $\bar{\beta} \approx 0.245$.

- **Step 2**: Use the six ordered pairs $(s, \theta)$ to determine the functional relationship between the $s$ and $\theta$ (see next page). For this data, $\theta^* = \exp[-126.176s+121.563]$ days. $\theta^* = 9.0387E+08$ days when $s = 80\%$.

- **Answer**: $Ps = 0.9784$ using $\theta^*$ at $s = 80\%$, $t = 150$ days, and $\bar{\beta} = 0.245$. Probability of failure, $Pf$, is $1 – Ps = 0.0216 \approx 2 \text{ out of } 100$. 

Tim.Adams@NASA.gov
**Step 2:** Determine the relationship between $s$ and $\theta$

\[ \ln(\theta) = -126.18s + 124.74 \text{ (hours)} \]

$R^2 = 0.8569$
Example #7: Parameter (statistical) uncertainty

* Design Objective: Make a survivability metric* with associated uncertainty for personnel working in the Vehicle Assembly Building (VAB) to assemble and checkout a spacecraft. This metric will combine or join two likelihoods (probabilities), namely,

1. The likelihood of occurrence and

2. The likelihood of impact to personnel

… for various hazards occurring over time, at different locations, and during different vehicle build phases.

* To provide a metric, the VAB survivability probability for each identified hazard was compared to the complement or one minus the accident rate for aerospace workers.
The survivability measure (not metric) for each hazardous scenario, at each phase, at each zone, and at each time mark was called the Probability of Survival, \( P(S) \), where:

\[
P(S) = 1 - \{ P(E) \times [1 - P(S|E)] \}.
\]

- \( P(E) \), Scenario Likelihood, is the probability of the hazardous scenario occurring at any or all zones at any phase.
- \( P(S|E) \), Survival Level, is the probability of survival given the hazardous event occurred in zone \( x \) and phase \( y \). Survival Level ranges from 0% (death) to 100% (survival).
- The formulas for Aggregate Survival Level and Composite Scenarios, a group of scenarios, are not described here.
Example #7: Input uncertainty makes output uncertainty

- If the Excel formula is: \( 1 - \{ P_E * [ 1 - P_{S|E}] \} = P_S \),

- Then the Palisade @RISK add-in tool uses the Excel formula to make:

\[
1 - \{ \* [ 1 - \] \} =
\]
When the Excel equation has at least one data input that is (or should be) a probability distribution, then the probabilistic simulation* software such as Palisade’s @RISK can be used. This software performs the following tasks:

- Defines probability distributions for each uncertain input, the blue-shaded graphs.
- Deterministically solves the equation numerous times (iterations) until a specified level of convergence is obtained or a fixed number of iterations were completed (e.g., 10,000 times).
- Collects the 10,000 answers.
- Organizes the probabilistic output (answers) into a histogram, the red-shaded graphs.
- Converts the histogram into a probability distribution to make the area under the curve = 1.00.

*Note: Frequently, the words “Monte Carlo” are used to mean probabilistic simulation. Actually, Monte Carlo is a type of sampling method for simulation and not the only type. A common and often a preferred type of sampling method is the Latin Hypercube sampling method. Thus, to be informative, the analyst should state the type of sampling method the software used to perform the probabilistic simulation.
General strategy: Thinking and producing analytically

- **COP**: Non-linear process that builds a traceable solution.
  - **Concept**: talk  What concepts and data map to the desired outcome?
  - **Operation**: do  What method make the concepts and data operational?
  - **Product**: produce  Do the Cs and Os build, explain, and defend the P?


- Expertise in the **O** task (e.g., mechanics, computation) is necessary but not sufficient to answer questions that are new to the assigned analyst.

- Thus, the manager of the analytical project can use COP as a template to inquire and distinguish between unproductive activity and productive tasks that lead to results. Productive tasks include: (1) “Work smarter” by researching lessons learned and (2) Use the Test-Analyze-And-Fix (TAAF) process to learn and produce iteratively.
Practice COP with the customer before the “due date”

- With analytical-type work, there are advantages when the analyst is able to communicate with the decision maker while the analytical work is in the design (conceptual) and build (operational) phases.

- “…only 40% of projects suggested by quantitative analysts were ever implemented. But 70% of the quantitative projects initiated by users, and fully 98% of projects suggested by top managers, were implemented.”

  Barry Render & Ralph M. Stair Jr., Quantitative Analysis for Management, 6th edition

- And because … see next page.
Besides increasing the likelihood the analysis will be used, concurrent work reduces surprises and provides empathy for the decision maker.

Don’t Throw The Technical Report Over The Fence

When Necessary, Use Tutorials To Prepare The Decision Maker Before The Formal Technical Meeting

1 Review = Decision maker(s) react positively, understand technical content as needed, and accept or reject the findings, conclusions, and recommendations.

2 Ideally, tutorials are informal two-way discussions between the analyst and the decision maker (customer, manager) about the hope, business need, design, and development of the analysis.
Analyst Mantras

◆ “Success comes in cans, not in cannots!”
   Joel H. Weldon, motivational speaker

◆ “Think about your thinking.”
   The 7 Levels of Change, Rolf Smith

◆ “Do you think if you torture the data long enough it will confess to you?”
   Dr. Harold V. Huenke, Professor of Mathematics, University of Oklahoma.
   
   Update: Mark Hulbert’s Sept 26, 2006 Market Watch stated, “If you torture the data long enough, you can get it to say just about anything.”

◆ “Somebody is going to have to suffer, either the reader or the writer.”
   Tom Murawski, national leader in writing improvement, The Murawski Group Inc

◆ “A perfect world is when ‘big Q’ (qualitative view) and ‘little q’ (quantitative view) agree--or at least understand why not to agree!”
   Author