Development and Verification of Probabilistic Requirements

Mark A. Powell

Stevens Institute of Technology

20 June 2006

First, What is a Probabilistic Requirement?

- **Simply, a Statement of a Required Probability for Performance, e.g.,**
  - **Reliability – Probability of Survival until Time Specified**
  - **Availability – Probability that Item Ready when Needed**
  - **Maintainability – Probability that Repair Completed in Time**
  - **Safety – Probability of Loss of Life or System**
  - **Logistics – Probability of Repair Parts Availability for Repair**
  - **Navigation or Tracking Accuracy – Probability of Achieving Stated Accuracy**
  - **Requirements with Tolerances – Probability of Manufacturing Exactness**
- **By Probabilistically, we mean in terms of a *Probability* of Achieving the Performance**

A Statement of Required Performance with a Statement of Acceptable Risk

Some Requirements should Be Probabilistic

- **Known, Common Scenarios Exist where Many Performance Requirements *cannot* be Satisfied due to Random Events**
- **Example: Original International Space Station Microgravity Mission Requirement**

The ISS Program shall provide 180 days of microgravity per year in periods of no less than 30 days.

  - **Known Random Events which would Happen**
    - **Debris Avoidance Maneuvers**
    - **Unscheduled Maintenance Requiring Use of Attitude Jets**
  - **Corrected Requirement:**

The ISS Program shall provide a 70% probability of achieving 180 days of microgravity per year in periods of no less than 30 days.

Probabilistic Mission Requirements Examples

- **Space Station Microgravity Mission Requirement**

The ISS Program shall provide a 70% probability of achieving 180 days of microgravity per year in periods of no less than 30 days.

- **Space Defense Operations Center**

SPADOC Block 4B shall detect 99.995% of CONUS bound ICBMs.

- **Global Positioning System**

The Precise Positioning Service shall provide a 15m SEP absolute position accuracy.

How to Write Probabilistic Requirements

- **Probabilistic Requirements should *Always* be Stated in terms of Some *Probability Level* that the Performance Level will be Achieved or Met**
  - ***Never* State in Terms of a Probability Model**
  - ***Never* State in Terms of Moments (Means and Variances)**
  - ***Never* State in Terms of "3 Sigma" (3*sqrt(Variance))**
  - ***Never* State with "Confidence" Levels**
    - **Intent Belongs in the Verification Requirements**
    - **"Confidence" Term means something different to a Statistician – *NOT what you want!***
- **For Most "illities" Requirements, the Definition is in terms of a Probability**

Multivariate Accuracy Specifications

- **Recall from Verification Training the Joint STARS Targeting Performance Requirement - in Terms of a *CEP***

  ***JSTARS Shall Direct and Deliver Ballistic Bombs with 100m CEP Accuracy.* (100m Value Made Up)**
- **What is a *CEP*?**
  - **Circle of Equivalent Probability or Circular Error Probable**
  - **A two dimensional circle containing 50% of the probability, usually specified as a *Radius* or r_{CEP}**
  - **The *Integral* of some bivariate Probability Model over the Specified Circle that evaluates to 0.5**
- ***SEP* - three dimensional Analog of the *CEP*, 50% Sphere**
- **Not Necessary to use *50^{th} Quantile* (not a CEP or SEP then), e.g., 99.865% (mean + 3 sigma for a Gaussian Model)**
- **Do NOT Specify as: *"The CA shall provide 100 meter accuracy (3 sigma)."* What does this Mean?**

Verification for Probabilistic Requirements

- **Verification Requirements for Probabilistic Requirements are *Always* Statistically Based**
  - **Recall, Verification Requirements establish the *Acceptable Risk* that the Requirement is not Satisfied with a Success**
  - **Must State a *Required Probability* for Performance Requirement being Satisfied**
  - **Must State *How* that Verification Required Probability is to be Obtained**
  - ***NEVER* use Confidence Intervals**
- **For Probabilistic Requirements, You must Verify by either**
  - **Test: Requires Data and a Statistical Inference, or**
  - **Analysis: Requires Monte Carlo Simulations (or PRA) and Statistical Inferences**

Verification Requirements for Test and Analysis

- **Verification Requirements for Probabilistic Requirements are *Always* Statistically Based**
  - **Should State a *Required Probability* for Performance Requirement being Satisfied – the *Success Criterion***
  - **Should State *How* this Required Probability is to be Obtained**
  - **May State *Data Limitations* to be Observed for Successful Test**
- **For CARD Level, *Do not Expect any Test Methods* for Probabilistic Requirements**
  - **CARD documents Requirements for Entire Constellation Architecture**
  - **Statistical Test of Entire CA Almost Always too Expensive**
  - **If Test is Chosen, Review Section 3 Requirement for Appropriate Level of Design Detail**

A Good Constellation Example

- ***The Risk of Loss of Crew (LOC) during a Lunar Sortie shall not be greater than 1 in 100 (TBR).***
  - **Frequency Statement (1 in 100) can be Confusing to Managers**
  - **But, Okay as stated for Provider Interpretations**
- **Verification Requirements**

  Risk of LOC shall be verified by Analysis. The Analysis shall be conducted in conformance with CxP 77001. The Verification shall be successful when the analysis shows that there is a TBD Probability that LOC for a Lunar Sortie is not greater than 1 in 100.

Synopsis

- ***Always*** **State Probabilistic Requirements in Terms of a *Probability*, *Never* in Terms of *Means* and *Variances* (or any other Moments)**
- **Do not Include Acceptable Verification Risks in the Probabilistic Requirement – Do not Use "Confidence Intervals"**
- **Be Aware of Probabilistic *Definitions* of "illities" for Writing Requirements**
- **Consider the Verification Method with some Serious Thought (Must be Analysis or Test)**
- **Going Back Much Later to Change an Absolutely Stated Performance Requirement that should have been Stated Probabilistically can be Difficult**

Contact Information

- **Mark Powell, SAIC**
  - **E-mail: attwater@aol.com, mpowell@stevens.edu, mark.a.powell@nasa.gov**
  - **Cell: 208-521-2941**
- **Call or e-mail if You need some Help developing Probabilistic Requirements or Verification Requirements**

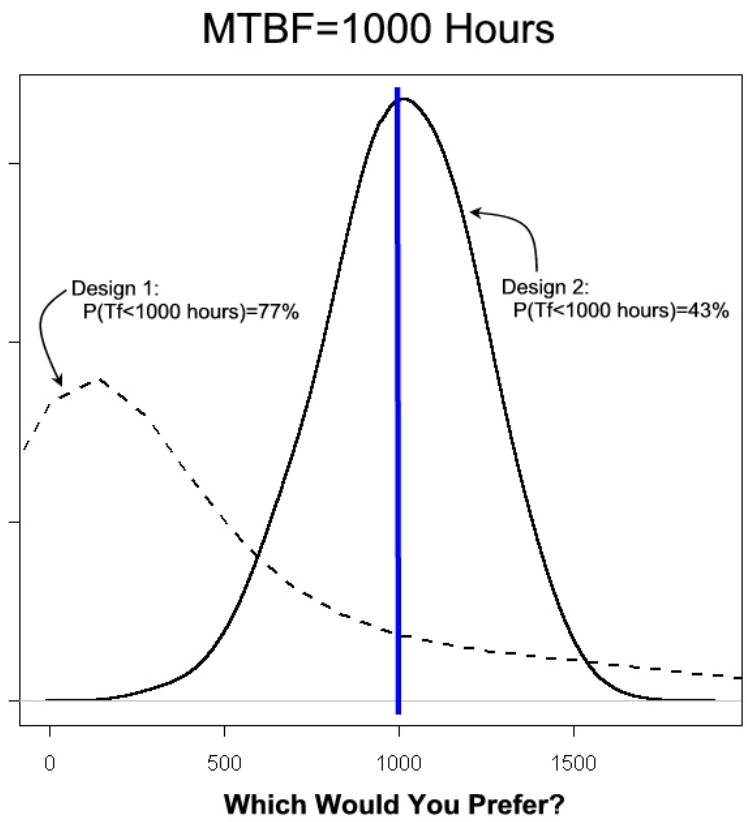
Backup Charts

Beware of "Confidence"

- **To the *Statistician***
  - **Given that the Null Hypothesis is *really True***
  - **Using Stats *Recipes*, Can compute an Interval about the Null Hypothesis for the given Number of Data to be Observed at a "Significance" level α**
  - ***If you could repeat your Experiment a near infinite number of times*, each time obtaining the same number of data and computing the Estimator, then your Estimator should fall inside the Interval you computed with a frequency of 1- α**
  - **Suppose your Estimator Falls inside the Confidence Interval** *Is the Null Hypothesis True, or did you just get a bad set of Data for one of the Other Hypotheses that are really True?*
  - **Suppose your Estimator Falls Outside the Confidence Interval** *Is the Null Hypothesis False, or did you just get a bad set of Data for one of the Other Hypotheses that are really False?*
- **To the *Decision Maker*, "Confidence" is the Probability that the Requirement is Satisfied with Verification Success**

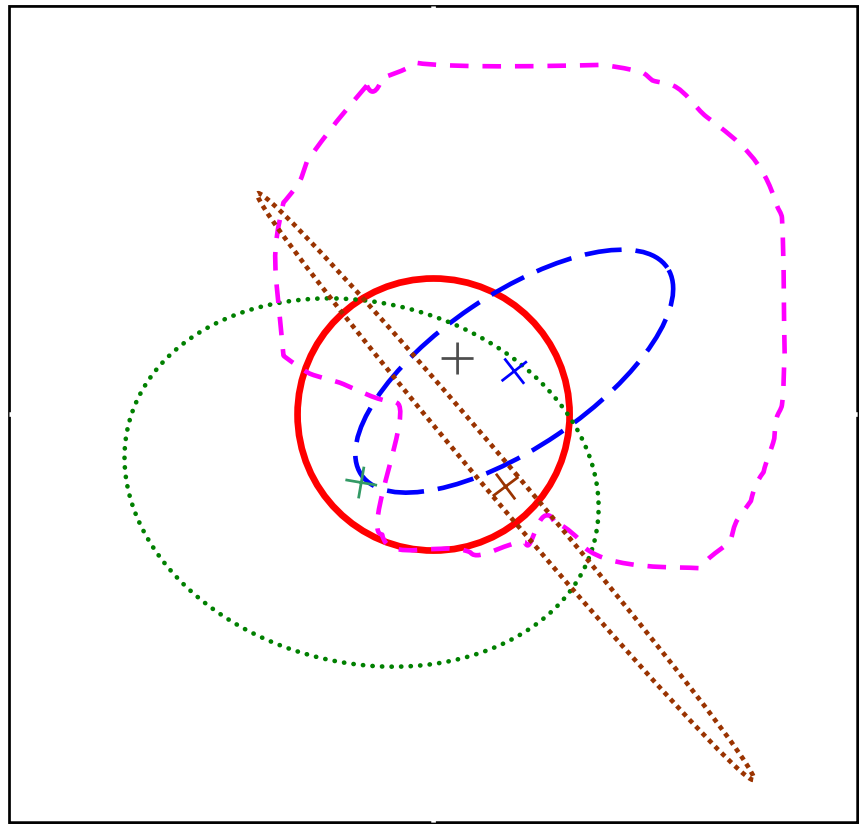
Problems Specifying Using Means

- ***Never*** **Use Means to Specify Probabilistic Requirements (including MTBF, MTTF, MTTR)**
- **Means can be at *Any* Probability Level (0% to 100%)**
  - **MTBF specified to be 1000 hours**
  - **Two Designs satisfy this Requirement**
  - **What is probability that failure will occur before 1000 hours if Requirement is met?**



Some CEP Examples

- **Specifying by CEP or Equivalent Provides Design Freedom**
  - **No Restrictions on *Mean* Locations for errors**
  - **No Restriction on *Orientation* of Contours**
  - **No Restriction on *Shapes* of Contours**
- **Contours in Figure at 1σ Levels about Peaks (+)**
- **Requirement is Satisfied if Red Circle contains 50% probability, regardless of error distributions**



Test Attributes

- **Specify the *Measure* for the Test**
- **Specify the *Initial Conditions* and All other Important *Assumptions***
- **Describe the *Experiment*, e.g.,**
  - **Minimum Numbers of Samples**
  - **Minimum Numbers of Test Items**
  - **What can be Simulated, and Simulation Assumptions**
  - **Specify what *System HW/SW* will be Used**
- **Specify *Success Criterion* in terms of the Measure**

An Auto Industry Test Example

3.2.x.y The vehicle shall have 95% reliability at 100,000 miles.

4.2.x.y Vehicle reliability shall be verified by Test.

---- The test shall use accelerated life testing procedures in accordance with TSP 432-1.

---- The test shall use at least 3 prototype vehicles.

---- The test shall use as data simulated mileage at failure and total simulated mileage for prototype vehicles that do not fail by the end of the test.

---- The test shall statistically process the data to calculate the probability that the vehicle provides 95% reliability at 100,000 miles.

---- The test shall succeed if the probability that the vehicle provides 95% reliability at 100,000 miles exceeds 90%.

The Method

The IC's and Assumptions

System HW/SW

Specific Directions

The Measure

Success Criterion

Analysis Attributes

- **Almost the Same as Test**
  - **Specify the *Measure* for the Analysis**
  - **Specify the *Initial Conditions*, All other *Assumptions*, and Sources of *Equations***
  - **If a *Simulation*, Specify the Extent of the Simulation**
    - **How many *Repetitions* (think Monte Carlo)**
    - **Extent and Range of *Simulated Environmental Conditions* to be Considered**
  - **Specify if *System HW/SW* will be Used**
  - **Specify *Success Criterion* in terms of the Measure**

An Auto Industry Analysis Example

3.2.x.y The vehicle shall have 95% reliability at 100,000 miles.

4.2.x.y Vehicle reliability shall be verified by Analysis.

---- The analysis shall simulate accelerated life testing procedures, environmental conditions, and maintenance in accordance with TSP 543-2.

---- The analysis shall use 100 simulated vehicles and simulate driving for 200,000 miles.

---- The analysis shall use as data simulated mileage at failure and 200,000 miles for simulated vehicles that do not fail.

---- The analysis shall statistically process the simulated data to calculate the probability that the vehicle provides 95% reliability at 100,000 miles.

---- The verification shall succeed if the probability that the vehicle provides 95% reliability at 100,000 miles exceeds 90%.

The Method

The IC's and Assumptions

Simulated HW/SW

Specific Directions

The Measure

Success Criterion