Dealing with Uncertainty in Systems Engineering

Jet Propulsion Laboratory

Systems Engineering Advancement Seminar

24 August 2006

Mark A. Powell

Stevens Institute of Technology

Without Uncertainty, There would be No SE

- **Clearly, If**
  - **We *Fully Understand* the *Problem***
  - **We *Fully Understand* the *Solution***
  - **The *Solution* is *Feasible* within *all* the *System Constraints***
    - **We Just Build it and Solve the Problem**
    - ***We don't need Systems Engineering!***
- **Never Been There, Never Done That - Have You?**

But, What is Uncertainty?

- **First, What do Engineers, Specifically Systems Engineers, Really Do?**
  - **In Analysis and Design, *Model* *Abstractions of a System* to *Solve* the *Abstractions of the Problem***
  - **In Integration and Test, *Model* Uncertain Observed Data from the System that was Actually Built to Verify that it Actually has a good Chance to Solve the Problem**
- **Uncertainty is *Epistemological*, not *Ontological***
  - **We Want to Determine What is Knowable**
  - **We can *Never* Truly Know Reality**

Types of SE Uncertainty

- ***Unknown Future Event***
  - **Will Definitely Occur, Outcome Uncertain**
  - **Occurrence Uncertain, Outcome Uncertain**
- ***Unknown Existing State*, not directly Observable**
  - **Measurement Uncertainties**
  - **Precision Limitations**
- ***Deterministic Event or State***
  - **Uncertain States of Nature, Initial Conditions, Parameters**
  - **Outcome Uncertain**
  - **Uncertain Model**
- ***Known and Knowable Item*, but Unknown to Us**
- ***Physical Randomness in Nature***
  - **Heisenberg Uncertainty Principle**
  - **Quantum Mechanics**
  - **Radioactive Decay**
  - **Statistical Mechanics**

Modeling Uncertainty

- **We Always model Uncertainty as *Randomness* Using *Probability* and *Probability Models***
  - **Randomness is a *Metaphor* for Our Personal Uncertainty**
  - **Very *Reasonable***
- **Probability and Probability Models Based on *Axioms of Rational and Coherent Behavior***
- ***Very Good* for Systems Engineering!**

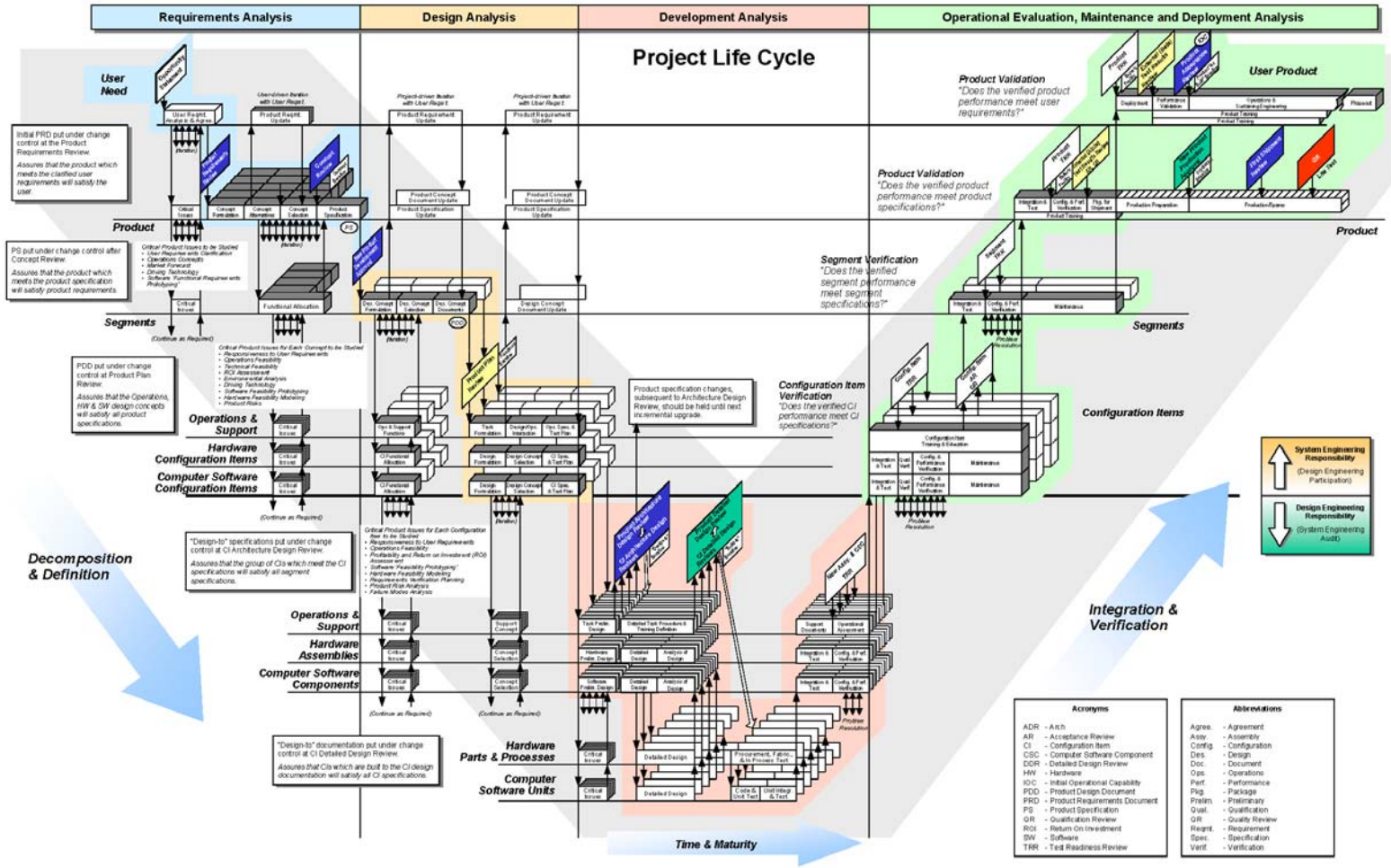
SAIC Science Applications International Corporation
From Science to Solutions™

Where Uncertainty Appears in SE

- **Much *Bigger Role* for *Systems Engineers* than Most Realize**
  - **Requirements**
  - **Functional Analysis and Decomposition (Allocation)**
  - **Design**
  - **Integration of Engineering Specialties**
  - **Quality Assurance**
  - **Integration and Test**
  - **Risk Management, PRA**
  - ***Decision Making***
- **Usually Perceived as *Very Difficult*, or else Glossed Over as *Very Simple***
- **A Primary Function of SE is to *Reduce* the Uncertainty (or *Risk*) about the System Satisfying the Need to some Acceptable Level**

SAIC Science Applications International Corporation
From Science to Solutions™

The Project Life Cycle



SE Decision Making

- **Systems Engineers Make Decisions with Uncertainty in *Every* Facet of the Project Lifecycle**
  - **Verification and QA – Obvious**
  - **Acceptable Risk in Probabilistic Requirements**
  - **Allocation of Performance and Risk**
  - **Design and Other Decisions**
  - **Risk Management**
- ***Good Decision Making* Makes *Good SE***

Suppose …

- **You could Make an SE Decision *without Making any Assumptions*?**
- **You could *Fuse* together every scrap of data and information about the Decision to Reduce your Uncertainty?**
- **You could be *Sure About the Risk* of each Alternative Producing the Desired Outcome of the Decision?**

Would that Help with those Important SE Decisions?

The Premise

- **SE Decisions are *Always* Based on Risk Assessments**
  - **SE Decisions select an Alternative (or Action) to Produce a *Desired Outcome***
  - **The Decision Maker selects an Alternative based on *only* one thing:**
    How Sure they can be, considering the available data, information, and their best judgment, that the Alternative will Produce the Desired Outcome
  - **A *Risk Assessment* tells the Decision Maker the Level of Assurance (How sure they can be) for the Risk of an Alternative producing the Desired Outcome**
- ***Better Risk Assessments Produce Better Project Decisions***

If you know your Risk for each Alternative, Decisions are Smart and Easy

Better Risk Assessments

- ***Qualitative* Risk Assessments**
  - **Decision Maker *Mentally* Integrates and Fuses a variety of Data and Personal Judgments to produce *a Qualitative Measure of Assurance* the Alternative will produce the Desired Outcome**
  - **This *Mental Fusion* Usually requires *Many Assumptions***
  - **For Many SE Decisions, Qualitative Risk Assessments are Sufficient**
- **A *Quantitative* Risk Assessment is a *Statistical Inference***
  - ***Mathematically* Integrates and *Fuses All* Data, Information, and Judgments, producing a *Probability Distribution* for the *Risk* of the Alternative Producing the Desired Outcome**
  - **A *Numerical Value* for Assurance of Risk Can be Computed from the Risk Probability Distribution**
  - ***Important* SE Decisions *Need* Quantitative Risk Assessments**

Using the Same Data, Quantitative Risk Assessments Always Produce Better Decisions

Problems with Quantitative Risk Assessments

- ***Difficult* to Perform**
- **Time *Consuming***
- ***Expensive***
- **Sometimes, they Still Require *Assumptions***
- **Mathematically *Intense***
- **Statisticians Usually *do not Know Enough about the Problem* to provide a Usable Result**
- **Usually *Forced by the Math* to Ignore or Overlook Important and Relevant Data or Information**
- **Sometimes, *Impossible* to Obtain a Usable Result**

Now, The Good News

- **You do *NOT* Have to Be a PhD Statistician to Do a Quantitative Risk Assessment**
- ***New* Numerical Methods Make Quantitative Risk Assessments *Quick, Easy, and Inexpensive***
  - **With just a *little* Programming, you can solve Important Decisions Right at Your Desk in Just a Few Hours**
  - **Knowing about these Methods, you can *Direct* a Quantitative Risk Assessment by Support Staff doing a little Programming in Just a Few Hours**

You can Make Much Better SE Decisions, Now!

Using Probability to Deal with Uncertainty in SE

SAIC Science Applications International Corporation
From Science to Solutions™

Probability Theory on Just One Slide

- **The Axioms: $0 \leq P(A|H) \leq 1$; $P(A|A,H) = 1$;**
  $P(A|H) + P(\sim A|H) = 1$;
  $P(A,B|H) = P(B|H)*P(A|B,H) = P(A|H)*P(B|A,H)$
- **OR Operation: $P(A \text{ OR } B|H) = P(A|H) + P(B|H) - P(A,B|H)$**
- **Mutually Exclusivity:**
  - **For *Mutually Exclusive* Propositions B and C:**
    $P(B,C|H) = 0$; $P(B \text{ OR } C|H) = P(B|H) + P(C|H)$
  - **If $A_1, A_2, A_3, \ldots, A_N$ comprise the set of *N Exhaustive*, *Mutually Exclusive* Outcomes for Proposition A, then**

$$P(A_1 \text{ OR } A_2 \text{ OR } \ldots \text{ OR } A_N \mid H) = \sum_{i=1}^{N} P(A_i \mid H) = 1$$

- **Independence: If A and B are *Independent***
  - **$P(A,B|H) = P(A|H)P(B|H)$**
  - **$P(A \text{ OR } B|H) = P(A|H) + P(B|H) - P(A|H)P(B|H)$**
- **Marginalization: For Propositions A, B, and C**
  $P(B|H) = P(B, \text{any A}, \text{any C}|H)$
  $= P(B|\text{any A}, \text{any C}, H)P(\text{any A}|\text{any C}, H)P(\text{any C}|H)$

Uses of Probability in SE

- **Probabilistic Requirements**
- **Performance Allocation in Functional Analysis and Decomposition**
- **Integration**
- **Verification**

Probabilistic Requirements

- **Many Requirements are *Normally* Stated Probabilistically, but not so Obviously**
  - **The *"illities"*, by definition, e.g.**
    - **Reliability – Probability of Survival during Mission**
    - **Availability – Probability of Readiness for Mission**
    - **Maintainability – Probability can be Repaired in Time**
    - **Safety – Probability of No Injury or Death**
    - **Logistics – Probability Part is There for Repair**
  - **Quality Assurance Requirements – Verification**
  - **Some Performance Requirements – Inherently**
- **By Probabilistically, we mean *in terms of a Probability of Achieving the Performance***
- **Many Requirements that should be Stated Probabilistically are *NOT***

Example of a Probabilistic Requirement

- **Known, Common Scenarios Exist where Many Absolutely Stated Performance Requirements cannot be Satisfied**
- **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 can Make Mission Impossible**
    - **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.

Verification

- **Verification Requirements Establish the *Minimum Acceptable Risk* that the Delivered System will not Perform as needed**
- **Example: Reliability Requirement and Test for a Vehicle**
  - **Performance Requirement: *The vehicle shall have 95% reliability at 100,000 miles.***
  - **Verification Requirement: *Vehicle reliability shall be verified by Test. The test shall demonstrate 90% assurance that the vehicle will have 95% reliability at 100,000 miles.***
  - **Test: Drive two vehicles 107,000 miles**
  - **If none fail (the data), have 90% *Assurance* (or Probability) that Design achieved 95% Reliability at 100,000 miles**
  - **Accept 10% Risk in Design**
  - **(INCOSE IS2004 Paper – Contact me if you want it)**

Using Statistics in SE to Reduce Uncertainty

Reducing Uncertainty

- **We Reduce Uncertainty in SE by using *Observations* and *Data* from a System as it is being Developed and Built**
- **We Use *Statistics* to Process the Observations/Data to *Infer* a Reduced Uncertainty based on *Probability Models***
- **Properly Performed in SE, Statistics can Provide a High Level of *Assurance* that a System will Perform Properly**
- **Verification is the Process to use Statistics to Reduce Uncertainty or *Risk***
- ***Risk Assessments* are used to Reduce Uncertainty to Make SE Decisions**

Verification Method Considerations

- ***Inspection* and *Demonstration* - Insufficient and Inappropriate Methods for Verifying Probabilistic Requirements**
- ***Analysis* and *Test***
  - **Methods require *Prior Uncertainty* and *Data***
  - **In Integration Stages, Data may be *Test Results* from Earlier Tests or Analyses**
  - ***QA Requirements* for these Verification Methods may be *Quite Complex***

Use of Statistics in SE

- **Statistics is the Process used to Reduce Uncertainty *Quantitatively***
- **Classical Statistics *Does NOT Work Well* for SE**
  - ***Overconservative* – SE cannot afford**
  - **Requires *Many* Data – SE rarely Gets a lot of data**
  - **Can *Only* Use Actual Event Data – SE's have Other Data**
    - **Censored Data – Event has not happened**
    - **Expert Opinion**
    - **Surrogate or Analog Data**
- **SE's Need to Use *All Available Data* to Reduce Uncertainty as Much as Possible**
- **SE's Need to Use *Bayesian Statistics***

The Foundation: Bayes' Law

- **Bayes Published in 1763**
- **Laplace Republished in 1812**
- **Jeffreys Republished again in 1939**
- **Analytical Derivation from Axiom 4**
  - **P(A,B|H) = P(A|B,H)P(B|H) = P(B|A,H)P(A|H)**
  - **Now consider only the *Rightmost* Equality**
    P(A|B,H)P(B|H) = P(B|A,H)P(A|H)
  - **P(A|B,H) = P(B|A,H)P(A|H)/P(B|H)**
- ***That's it!***
- **The *Basis* for all of Decision Theory and Analysis**

Interpretation of Bayes' Law

- ***Bayes' Law*: P(B|A,H) = P(A|B,H)P(B|H)/P(A|H)**
  - **If B is a Proposition, and A is Data, we get P(B|Data,H) = P(Data|B,H)P(B|H)/P(Data|H)**
  - **Now, P(Data|H) is just a *Constant Marginal* Probability, and *unimportant*, so we can ignore it and say P(B|Data,H) $\propto$ P(Data|B,H)P(B|H)**
- **The *Interpretation***
  - **P(B|H) is called the *Prior* - the Marginal Probability (Uncertainty) on the Proposition *before* getting the Data**
  - **P(Data|B,H) is called the *Likelihood* - the Probability of Getting the Data Given the Proposition**
  - **P(B|Data,H) is called the *Posterior* - the Probability (Uncertainty) on the Proposition *after* the Probability of Getting the Data Given the Proposition is Compounded with the *Prior***
- ***Works for Probability Density Functions Also!***
- ***Can Fuse Any and All Data Types!***

Problems with Bayesian Statistics

- **Ever Wonder why You were not Taught Bayesian Statistics in Engineering?**
- **For Real World Problems**
  - **Bayesian Solutions are Usually *Analytically Intractable***
  - **Numerical Solutions are Usually Impossible using *Ordinary* Monte Carlo Methods**
- **Up Until the mid-1990's, Impractical and Usually Impossible to Use by SE or Engineering**

The Solution

- **Markov Chain Monte Carlo**
  - **Developed in *Europe* in 1990's mainly for Risk and Decisions in Biostatistics and Bio-medical Research**
  - **More General Numerical Method than Ordinary Monte Carlo, but Produces Same Results**
  - **Works for Analytically Intractable Bayesian Statistics Solutions (like we get in the *Real World of SE*)**
  - ***Simple* Algorithm (M-H): Generates *Multivariate Correlated Random Samples* for use in Ordinary Monte Carlo Calculations (No Need to ignore Conditionality)**
- **Recently Applied to SE Problems**
  - **INCOSE IS02 Paper (Maintenance Interval)**
  - **INCOSE IS04 Paper (Optimal Cost Verification)**

The Metropolis-Hastings MCMC Algorithm

- **To Start, formulate the Posterior density *pd(Θ|data)*, and select a proposal step size *dΘ***
- **Start with any legal value: $\Theta_i = \Theta_1$**
- **Repeat Loop to get new samples**
  - **Propose a new sample: $\Theta_{i+1} = \Theta_i + \Delta\Theta$,**
    where $\Delta\Theta \sim U(-d\Theta, d\Theta)$
  - **Calculate the ratio of Posterior densities:**
    $\alpha = pd(\Theta_{i+1}|data) / pd(\Theta_i|data)$
  - **Obtain a sample *u* from a uniform distribution: *u~U(0,1)***
  - **If $u<\alpha$, then accept the proposed sample as Θ_{i+1},**
    else set the new sample to the previous one: $\Theta_{i+1} = \Theta_i$

How to Avoid Making Assumptions

- **Cannot Completely Avoid Assumptions**
  - **Can Avoid *Overconservative* Assumptions**
  - **Can Avoid *Questionable* Assumptions**
- **The Key: Use *Non-informative* or *Reference* Prior Models**
  - **Model Uncertainty when you Are *Ignorant* about the Uncertainty**
  - **Provide *Realistic* Worst Case Scenarios**
  - ***Derivable* with the Same Solutions Using Three Independent Methods**
  - **Very Simple Functions, Generally Inverses and the Constant 1**
  - **Bernardo and Smith, Excellent Reference**

Sometimes, MCMC Needs Outrageous Assumptions

- **For Many Real World SE Decisions, Posteriors Using non-Event Data will Not produce a *Stable* Markov Chain**
- **M-H Algorithm will not Work**
- **Solution: Use *Pseudo-Ignorance* Priors**
  - **Limit Range to Some *Outrageous* Value (10 times larger than realistic) for Scale and Shape Parameters**
  - **Effective Truncation of Inverses**
  - **Stabilizes the Markov Chain, Good Sampling**

Example: Space Shuttle Cargo Transfer Bag Test

- **Cargo Transfer Bags (CTB) to be Carried on Shuttle to Space Station**
- **Required Zipper Cycle Life – 2,000 Cycles**
- **If CTB Zipper Fails During Launch or Descent, Loose Object could Penetrate the Hull (Rare Event with Extreme Consequences)**
- **Performed a Single Test**
  - **One CTB Only**
  - **8,000 Successful Zipper Cycles**
- **Relevant Question**

How Sure can we be from the Test Result that the TRUE Risk of CTB Zipper failure by 2,000 Cycles is below some Acceptable Level?

Synopsis for the CTB Test

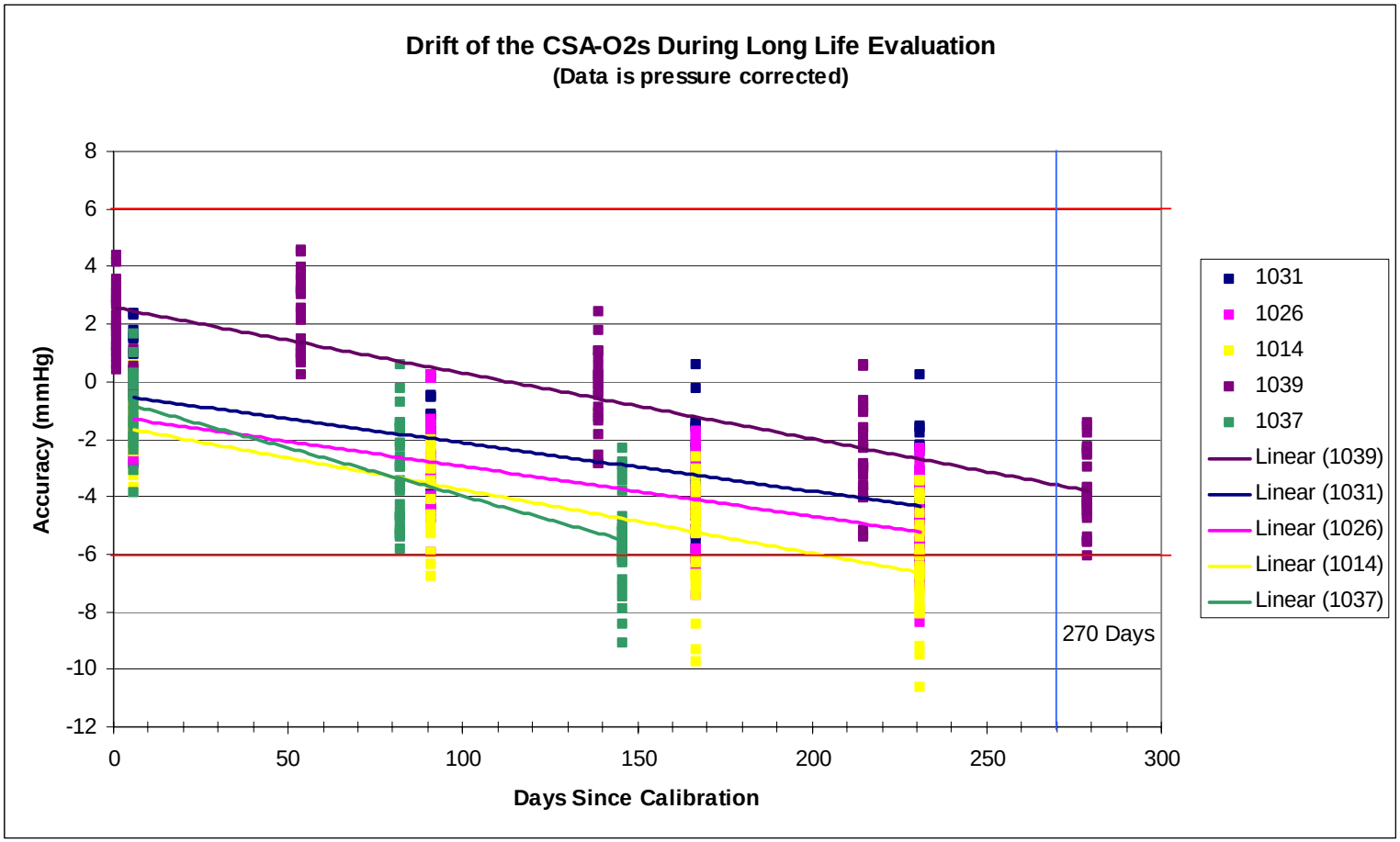
- **Test Datum:**
  Successful 8K Cycles without a Failure on One CTB Zipper
- **Assumptions (*outrageous*):**
  - **Zipper Cycling Cannot Improve Reliability of the CTB Zipper**
  - **At Least 62.4% of CTB failures will occur before 30,000 Cycles**
- **No Stated Minimum Acceptable Risk – So Parameterize**

Risk of CTB Zipper Failure by 2K Cycles (R_{2K})	Assurance Provided by Test Results P(True $R_{2K} < R_{2K}$)
1%	75%
5%	88%
10%	94%
20%	98%

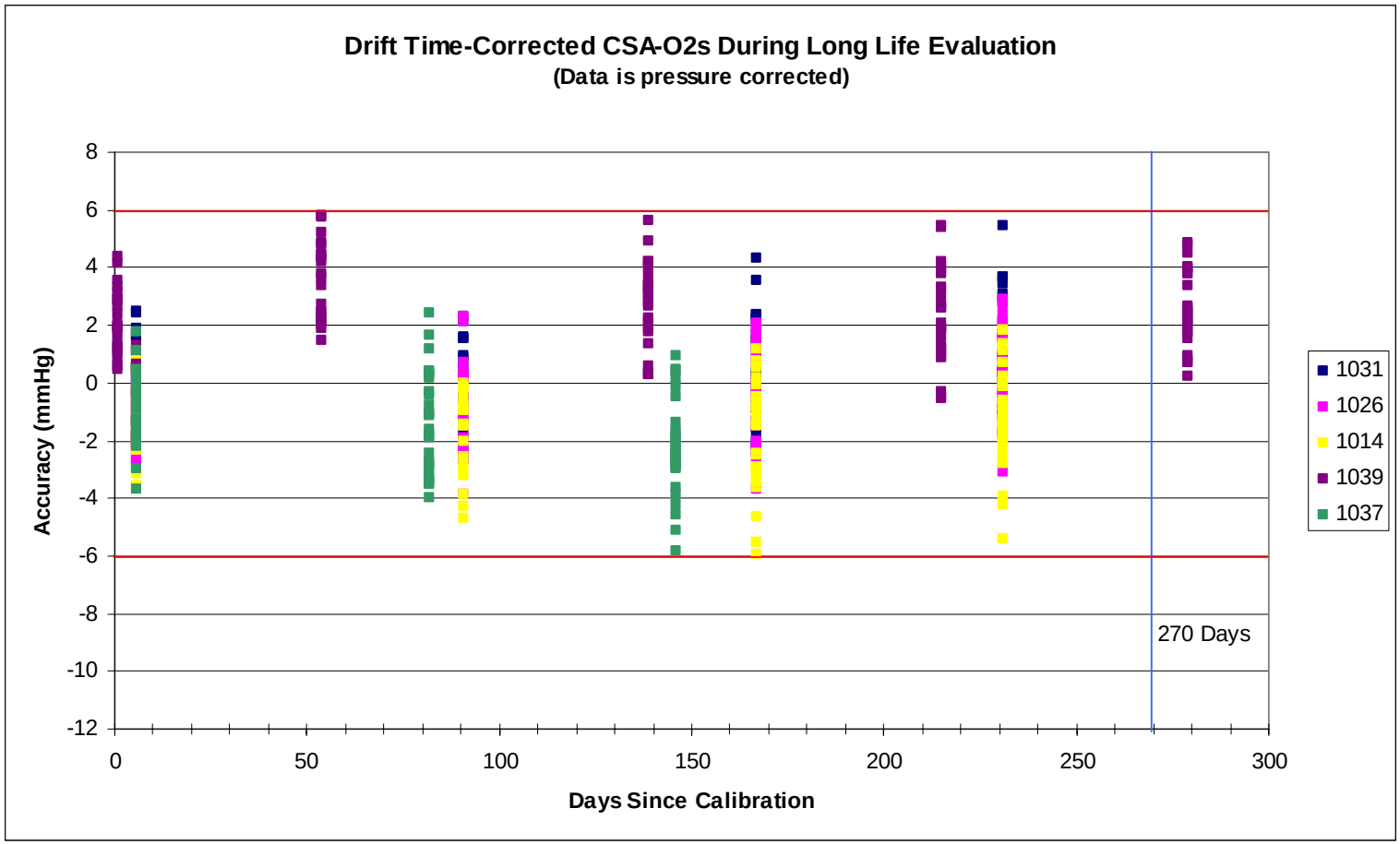
Example: ISS O2 Sensor Drift

- **Problem: Space Station Oxygen Sensor Measurement Accuracy is Observed to drift with Time**
  - **If the Measured O_2 is in Error by more than ±6mmHG within 270 days since Calibration, it could *Kill* an Astronaut**
  - **Already Compensating for Pressure Variations in Measurement Accuracy (Successful)**
- **Proposed Solution Options:**
  - **Test for Drift rates and Compensate for Drift; *OR,***
  - **Redesign O_2 Sensor and Ship Up to ISS**
- **Questions:**
  - **What is the *Existing* Risk of Sensor Accuracy Drift Beyond Acceptable Limits?**
  - **What is the Risk *After* the Proposed Drift Compensation?**

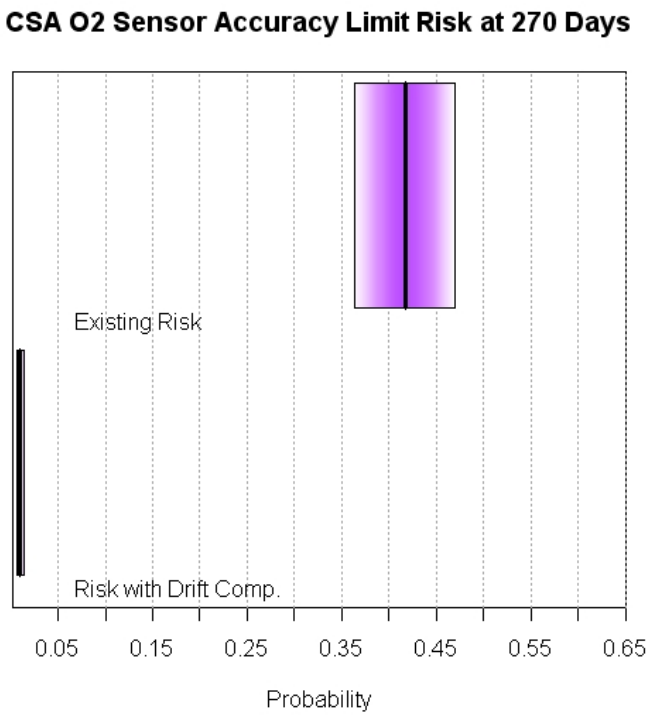
O2 Sensor Test Data

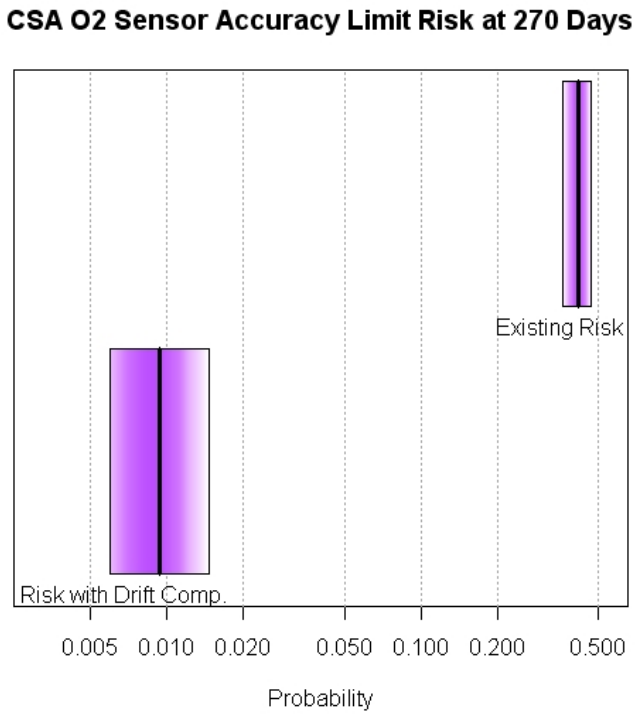


Drift Corrected O2 Sensor Data



Before and After Drift Correction Risk Results





Linear Scale **Logarithmic Scale**

O2 Sensor PRA Summary

- **Without Drift Compensation, Risk of Exceeding Accuracy Limits at 270 Days is 36-46% (with 90% Certainty)**
- **With Drift Compensation, 95% Sure Risk of Exceeding Accuracy Limits at 270 Days is < 1.5%**
- **Additional O2 Level Compensation could Reduce Risk Further**
- **Achieved Stable Markov Chain – *No Outrageous Assumptions Needed***

Example: RSR Loose Screw PRA

- **Problem: Screws Holding Locker Door in Place in Shuttle Bay are Too Short**
  - **If Door Looses Integrity, or Falls off, Something could Penetrate the Shuttle Hull during Launch or Descent**
  - **What is The Risk of having a Loose Screw, that could then Lead to a Risk of Losing a Door**
- **Decision:**
  - **Replace and Retighten All Screws, *OR***
  - **Delay Flight**

Risk of Panel Door Loss

- **Complex Risk Question**
  - **Loss of any Latch or Hinge Plate on Door will cause Loss of Door Integrity**
  - **Loss of a Latch or Hinge Plate requires Loss of One or More Screws**
  - **How many lost screws, in what patterns for Latch or Hinge Plate will Cause Loss of Door?**
  - **The Answer Defines Failure Modes**
- **Potential Failure Modes**
  - **Any One to Six Screws Lost in a Latch or Hinge Plate Causes Door Integrity Loss - *Conservative***
  - **Specific Pattern of One to Six Screws Lost in a Latch or Hinge Plate Causes Door Integrity Loss – *Realistic* Engineering, and Less Conservative**

The Probability Equations for Risk of Panel Door Loss

- **The Complete Probability Equations are usually Neglected, Usually a Mistake**
- **The Probability Statements for this Risk**
  - **P(loss of any door)**
    = 1-(1-P(loss of single panel door))^(# of single panel doors)
    *** (1-P(loss of double panel door))^(# of double panel doors))**
    *** (1-P(loss of triple panel door))^(# of triple panel doors))**
  - **P(loss of door)**
    = P(loss of any Latch OR loss of any Hinge Plate on the door)
    = 1-(1-P(loss of latch))^(# of latches and hinge plates on door)
  - **P(loss of latch) = P(loss of Hinge Plate)**
    = P(M screws lost of Pattern of 6) – the failure mode

$$= \sum_{j=0}^{6} \left[\mathbf{P}(\mathbf{M\ Lost} \mid j\ \mathbf{Loose})\mathbf{P}(j\ \mathbf{Loose}) + \mathbf{P}(\mathbf{M\ Lost} \mid 6-j\ \mathbf{Tight})\mathbf{P}(6-j\ \mathbf{Tight}) \right]$$

Predicted Risk of RSR Panel Door Failure

- **Consider All Conservative Failure Modes (1 to 6 screws may be needed to Retain Each Latch and Each Hinge Plate)**
- **Worst Case – Specific Screw Patterns will Reduce Risk**
- **Table of Predicted Risks for Failure due to Lost Screws**

Failure Mode Definition (# Lost Screws in Pattern of 6)	P(Loss Single Door|Data)	P(Loss Double Door|Data)	P(Loss Triple Door|Data)	P(Loss Any Door|Data)
1 or more	1.91%	3.78%	5.62%	29.34%
2 or more	2.35e-2%	4.69e-2%	7.04e-2%	0.422%
3 or more	2.57e-4%	5.14e-4%	7.71e-4	4.63e-3%
4 or more	2.23e-6%	4.47e-6%	6.70e-6%	4.02e-5%
5 or more	1.34e-8%	2.68e-8%	4.02e-8%	2.41e-7%
6	4.11e-11%	8.23e-11%	1.23e-10%	7.41e-10%

Synopsis

- **Uncertainty is *Prevalent* Throughout Systems Engineering**
- **By Properly Using Probability and Statistics, Uncertainty can *Now* be Handled Very Effectively by an SE**
- **New Methods (*MCMC*, *Reference Priors*, and *Pseudo-Ignorance Priors*) are Available to SE's to Allow Good Statistics**
  - **Better Reduction of Risk and Uncertainty**
  - **Better SE Decisions**
  - ***Better SE!***

Naked Proselytization

- **SE Courses Available at Stevens Institute of Technology via the Web**
  - **SYS601: *Probability and Statistics for Systems Engineers* – Spring Semesters**
  - **SYS660: *Decision and Risk Analysis for Complex Systems* – Fall and Summer Semesters (starting 5 September 2006)**
- **http://webcampus.stevens.edu/**
- **Full Day Tutorial at EUSEC 2006: *Dealing with Uncertainty in Systems Engineering***

Contact Information

- **e-mail**
  - mark.a.powell@saic.com
  - mark.a.powell@nasa.com
  - mpowell@stevens.edu
  - attwater@aol.com
- **Snail Mail**

  P.O. Box 57702
  Webster, TX 77598-7702
- **Telephone**
  - **281-336-3402 (SAIC)**
  - **281-792-7575 (NASA)**
  - **208-521-2941 (Cell)**