Dealing with the Engineering Specialties

Statistical Analysis for Assessing Reliability

AES/ECLSS Reliability Educational Series
NASA JSC, 20 March 2013

Mark Powell

Attwater Consulting

Seminar Outline

Introduction

What are the Engineering Specialties

Why the Engineering Specialties are Challenging

What you can do to deal with the Engineering Specialties

Some Advancements that Help a lot

Summary

Introduction: Your Speaker, Mark Powell

- **Over 40 years' experience in Systems Engineering and Project Management, about 16 years NASA/JSC related**
- **Former Chair, INCOSE Risk Management Working Group**
- **Former Assistant Director for Systems Processes for INCOSE**
- **Session organizer for IEEE Aerospace Conference, *Risk Management and Lessons Learned***
- **Professor, Systems Engineering**
  - **Stevens Institute of Technology**
  - **University of Houston Clear Lake**
  - **University of Idaho**
- **Contact information at the end of the presentation, Contact Welcomed**

Introduction: Where to get the Slides

- **Go to www.attwaterconsulting.com**
  - **Click on "Resources"**
  - **Click on "Tutorials/Seminars"**
- **First presentation, with this Seminar title**
- **In this live presentation, I use slide animations that do not show in the printable slides.**
- **If you follow my presentation using these printable slides, please don't steal my thunder.**

Thanks!

Introduction:

- **Dealing with the Engineering Specialties is Challenging**
- **In this Seminar, I'm**
  - **Not going to tell you what you have to do**
  - **Not going to tell you what you should do**
- **But, I will tell you what you *can* do to be successful in dealing with the Engineering Specialties**

What are the Engineering Specialties?

- **Ancillary, but important parts of every traditional engineering discipline**
  - **Often called the *ilities***
  - **Common to every traditional engineering discipline**
  - **Each is similar if not identical in every discipline**
  - **Similar if not identical methods employed in each *ility***
- **Professional Societies and Certifications Exist for Most Engineering Specialties**

Examples

Reliability, Supportability, Quality, Compatibility, Survivability, Vulnerability, Commonality, Dependability, Accessibility, Availability, Sustainability, Maintainability, Serviceability, Safety, Verifiability, Logistics, Manufacturability, Producibility, Radcon, Controllability, Operability/Human Factors, Risk Management, Etc.

A Commonality

- **This is critical:**

  All ilities address Uncertain Performance

  - **They are all statements of some required probability for performance, *by Definition.***
  - **E. g., Reliability is defined as the probability that a product will survive (not fail) during some specified service life.**
  - **All establish required *Maximum Acceptable Risks.***

Standards Base

- **Some *ilities* requirements may be Best Practices (hard lessons learned) resulting from laws, standards, etc. about how to implement.**
  - **Underwriters Laboratories**
  - **Canadian Standards Association**
  - **OSHA**
- **Always deemed to satisfy some established Maximum Acceptable Risk**
- **May be difficult to find that risk level**

A Reset

- **Most SE's and many specialty engineers are *Unaware* of this Commonality.**
  - **Practice may be reduced to some standards-based process or standard parts**
  - **Failure to recognize this commonality when working on systems not governed by such standards makes it *extremely difficult* to address the engineering specialties properly.**

For the rest of this presentation, we will be focusing on engineering specialties for systems where there are no formal standards for the ilities – i.e., no UL or CSA or OSHA etc.

Definitions to Illustrate

- ***Reliability*** **– the Probability that the item will Survive to (not fail before) a specified Service Life**
- ***Availability*** **– the Probability that the item will be in a condition and state ready to perform its intended function when called upon during a specified service life**
- ***Maintainability*** **– the Probability that a failed item can be repaired and returned to service within some period of time**
- ***Logistics*** **– the Probability that a part needed to repair a failed item can be provided within some period of time**
- ***Safety*** **– the Probability that no harm or injury will occur during some period of time**
- ***Quality*** **– the Probability that an item satisfies its requirements**
- ***Human Factors*** **– the Probability that any human accepted to use the item will be able to operate it as intended**
- **The Rest are all similar *Statements of Probabilities***

Key Points

- **Engineering specialties always concern uncertainty.**
- **We always specify an acceptable amount of uncertainty using probability.**
- **Engineering specialties always cover a specified period of performance.**
- **An engineering specialty requirement always states a maximum acceptable risk.**

Why are the Engineering Specialties so Challenging?

$$P\left(R\left(T\right)\geq R_c\left(T\right)\mid data\right)=1-\int_0^{R_c(T)} pd\left(R\left(T\right)\mid data\right)dR\left(T\right)$$

$$\propto 1-\int_0^{R_c(T)} pd\left(\int_T^{\infty}\left\{\int_0^{\infty}\int_0^{\infty}\left[\left(\frac{\beta}{\eta}\right)\left(\frac{t_f}{\eta}\right)^{\beta-1}e^{-\left(\frac{t_f}{\eta}\right)^{\beta}}\right]\left[\prod_{i=1}^{N}\left(\frac{\beta}{\eta}\right)\left(\frac{t_{f_i}}{\eta}\right)^{\beta-1}e^{-\left(\frac{t_{f_i}}{\eta}\right)^{\beta}}\right]\right.\right.$$

$$\left.\left.*\left[\prod_{j=1}^{M}e^{-\left(\frac{t_{s_j}}{\eta}\right)^{\beta}}\right]\left(\frac{1}{\eta}\right)\left(\frac{1}{\beta}\right)d\eta\,d\beta\right\}dt_f\right)dR\left(T\right)$$

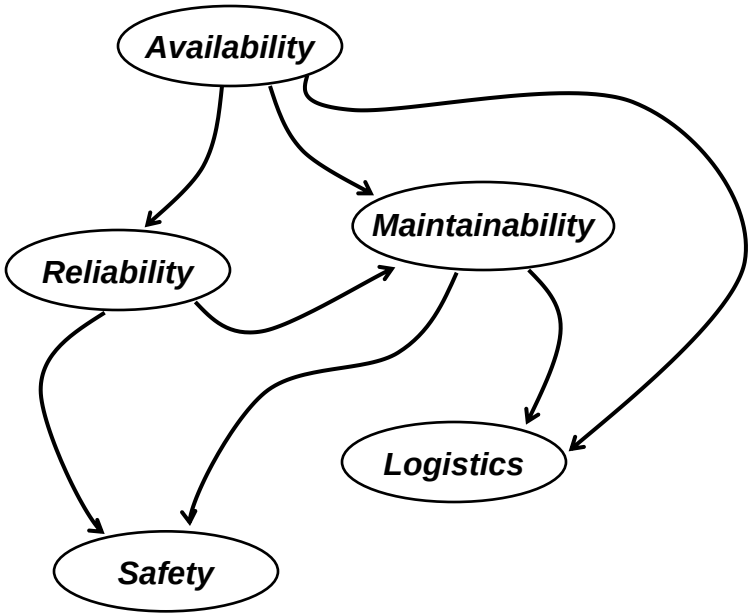
where: $R_c\left(T\right)$ is the critical reliability at service life T, and

data is the set of product failure service lives $\left\{t_{f_1},t_{f_2},\cdots,t_{f_N}\right\}$ and

the set of service lives for products that have not failed $\left\{t_{s_1},t_{s_2},\cdots,t_{s_M}\right\}$

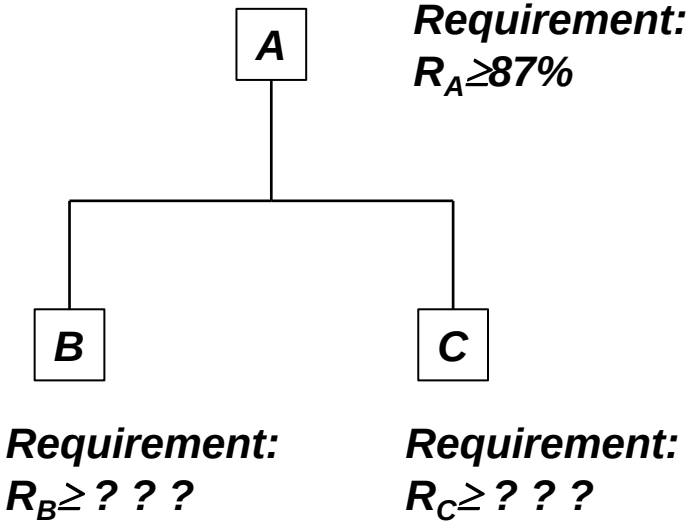
- **Probability and statistics**
  - **Lots of math**
  - **Not well understood**
  - **Humans wired to do P&S poorly**

Interrelated Challenges



- **Many of the specialties are interrelated.**
  - **E.g., RAM and Logistics**
  - **If it's broke, or being maintained, or waiting for a part, it is not available.**
- **Reliability and Safety**

Decomposition and Allocation Challenges



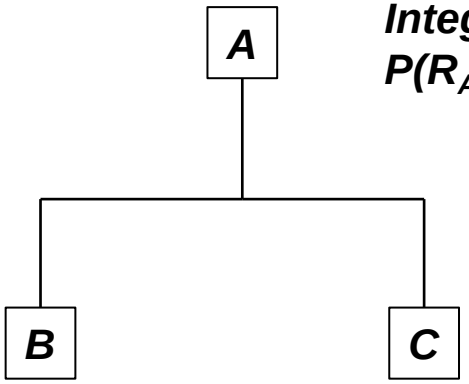
- **In Systems Design, allocation of specialty requirements in decomposition is very complex.**
- **Depends on physical architecture**
- **Depends on logical architecture**

Verification Challenges

- **In Verification of engineering specialty requirements, Test and Analysis methods must be used.**
  - **Requires experiments to obtain data or simulated data**
  - **Requires statistical processing**
- **Verification success always means that the risk that the as-built does not meet the requirement is below a specified maximum acceptable risk.**
- **When verifying engineering specialty requirements, always calculating from the data a *probability that a probability was satisfied by the as-built*.**
- **This disturbs most engineers.**

Integration Challenges

Requirements:
$R_A \geq 87\%$, Verify to 95%
$R_B \geq 95\%$, Verify to 90%
$R_C \geq 90\%$, Verify to 95%



Integration Rollup:
$P(R_A \geq 87\%) \geq ? ? ?$

Verified:
$P(R_B \geq 95\%) \geq 93\%$

Verified:
$P(R_C \geq 90\%) \geq 97\%$

- **In Systems Integration, rollup of verified probabilistic performance is very complex, and math intense.**
- **Depends on physical and logical architectures**
- **Depends on verification results distributions**
- **Equations rarely closed form, complex integrals with integral transforms**

Another Reason: Cousin Requirements

- **Every Functional/Performance requirement will have many Cousins – Engineering Specialty Requirements.**
  - **At the same design generational level**
  - **Derived from parent requirements that are siblings of the functional/performance requirement's parent Requirement**
- **Many cousins directly associated with each functional/performance requirement, and related to each other.**
- **Many cousins directly associated with multiple functional/performance requirements.**
- ***This can be a complex dance to balance!***

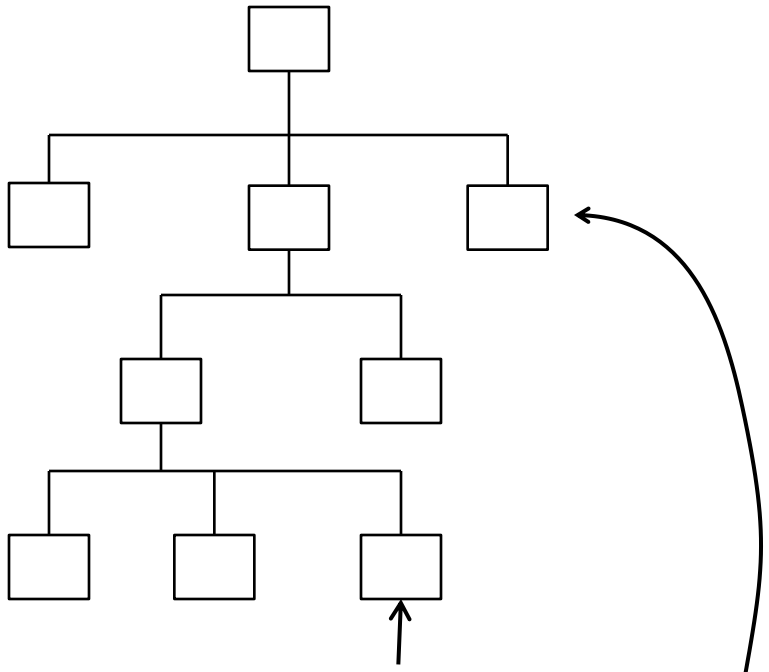
Please don't ask for a transfer to MOD!!!!

- **It is not hopeless at all.**
- **A *modern* P&S refresher might help some.**
- **Some tried and true methods work very well.**
- **Some relatively new methods work wonders to simplify the process.**

How to Deal with the Engineering Specialties

- **General Systems Engineering Advice**
- **Specific Specification Advice**
- **Design/Development Phases Advice**
- **Integration and Verification Phase Advice**

General SE Advice



Don't design this part when you are decomposing this level

- **Exercise Discipline – Finish one design generation before dipping down to a lower level.**
  - **Address all relevant Cousins for every performance requirement.**
  - **Relate in SE tool all relevant Cousins to all performance requirements**
  - **Relate in SE tool all Cousins to all other relevant Cousins.**
  - **Audit to assure all needed relations exist and make sense.**
- **Be prepared to iterate – *a lot*.**

More SE Advice

- **Make some hard decisions**
  - **Consciously establish the maximum acceptable risks for each specialty engineering requirement.**
  - **Achieve a suitable balance of all the related maximum acceptable risks.**
- **Analyze and Audit to assure the balance works.**

Specification Advice

- **State engineering specialty requirements correctly – Make them Probability statements over some period of performance**
  - **Probability statement may be inherent in definitions – e.g., for Reliability**

> ***The Zeus 5000 SUV shall have 95% reliability at 100,000 miles.***

  - ***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 using "Confidence" levels**

Specifying Verifications

- **State engineering specialty verification requirements correctly – Use Test or Analysis methods**
  - **Verification requirements establish the *Maximum Acceptable Risk* that the *ility* requirement is not satisfied in the as-built when successful.**
  - **Verification requirements establish the risk that the verification will fail when the *ility* requirement is actually satisfied in the as-built.**
  - **Must state a *Required Probability* for engineering specialty requirement being satisfied in the as-built**
  - ***NEVER* use confidence intervals or the word *Confidence*.**

Design/Development Advice

- **Excellent Paper**

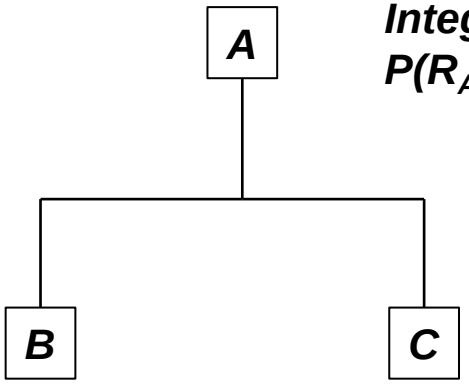
  D. Feng and C. Eyster, "Risk-Based Requirements Management Framework with Applications to Assurance Cases," in *2013 IEEE Aerospace Conf.*, Big Sky, MT, March 2-9, 2013

  Contact me for a copy!

- **Use PRA methods with Monte Carlo to balance engineering specialty requirements**
  - **Tie PRA structures to requirements – Link to your SE Tool database**
  - **When engineering specialty distributions are unknown, *don't make assumptions* – use pre-posterior distributions based on objective models of uncertainty ***

Integration Advice

Requirements:
$R_A \geq 87\%$, Verify to 95%
$R_B \geq 95\%$, Verify to 90%
$R_C \geq 90\%$, Verify to 95%



Integration Rollup:
$P(R_A \geq 87\%) \geq ? ? ?$

Verified:
$P(R_B \geq 95\%) \geq 92\%$

Verified:
$P(R_C \geq 90\%) \geq 97\%$

- **Use PRA methods with Monte Carlo to assure Rollup of verified components *ility* will satisfy verification of subsystem *ility***
- **If not, got a problem to fix**
- **Then verify subsystem requirement**

Advancements that Help

- **Dealing with the Engineering Specialties for systems without ilities standards or standard parts is tough.**
- **PRA methods using Monte Carlo is central.**
- **Markov Chain Monte Carlo can help immensely.**
- **Objective models of uncertainty can help avoid all assumptions**
  - **In general**
  - **In using pre-posterior distributions**

An Aside: Monte Carlo

- **Monte Carlo is nothing more than a numerical method to obtain an approximate solution for a definite integral.**
- **In general, can be used to obtain approximate solutions for integral transforms.**
- **Monte Carlo requires joint samples of the variables in the integrand over the full domain in frequencies proportional over the ranges of the variables.**
- **Ordinary Monte Carlo gets these samples from built-in random number generators. Very Limited.**
- **If the integrand does not have a built-in random sampler, cannot use ordinary Monte Carlo to solve the integral.**

Fairly Recent Advancement: Markov Chain Monte Carlo

- **A *More General* version of Monte Carlo**
  - **MCMC does *not* require recognizable defined sampling models – uses a Markov Chain to sample the integrand**
  - **Will work with analytically intractable integrals**
  - **Can work for *Very High Dimensional Integrals* (up to 20,000 related sources of uncertainty)**
  - ***Very Simple Algorithms* to code, but not amenable to packaging as a commercially available tool – requires manual interactions to tune the Markov chain**
- **Can be used in place of all ordinary Monte Carlo**

A Second not-so-recent Advancement

- **Models of Objective Uncertainty – derivable three ways for every *risk* problem by finding the uncertainty model that:**
  - **Minimizes the Fisher information (Jeffreys, 1930's)**
  - **Maximizes the information entropy (Lindley and Savage, 1960's)**
  - **Or, Maximizes the EVPI (Bernardo and Smith, 1990's)**
- **All three methods produce the same models for the same problem. – *is that ever comforting!!!***
- **You don't have to derive these – available in many sources!**
- **Use instead of assumptions**
  - **Keeps personal values out of the equations**
  - **Avoids compounding personal *risk* averseness and *risk* tolerances**

A Reliability Test: Auto Example

- **Soon to be available Zeus 5000 SUV**
- **Designed for 95% reliability at 100,000 miles**
- **Want to be ≥90% certain with verification success that reliability requirement met**
- **How can we verify that the Zeus 5000 SUV will have 95% reliability at 100,000 miles?**

Classic Problem!!!

That Rascally Zeus 5000

- **We can run a test and collect failure and survivor data for the Zeus 5000.**
- **We want a Quantitative equation we can solve, purely in terms of the data, no assumptions.**

$$P(R(100k) \geq 95\% \mid data) \geq 90\%$$

where

$$P(R(100k) \geq 95\% \mid data) = f(data)$$

The general equation we have to solve:

$$P\left(R(T) \geq R_c(T) \mid data\right) = 1 - \int_0^{R_c(T)} pd\left(R(T) \mid data\right) dR(T)$$

$$\propto 1 - \int_0^{R_c(T)} pd\left(\int_T^{\infty} \left\{ \int_0^{\infty} \int_0^{\infty} \left[\left(\frac{\beta}{\eta}\right)\left(\frac{t_f}{\eta}\right)^{\beta-1} e^{-\left(\frac{t_f}{\eta}\right)^{\beta}} \right] \left[\prod_{i=1}^{N} \left(\frac{\beta}{\eta}\right)\left(\frac{t_{f_i}}{\eta}\right)^{\beta-1} e^{-\left(\frac{t_{f_i}}{\eta}\right)^{\beta}} \right] \right.$$

$$\left. * \left[\prod_{j=1}^{M} e^{-\left(\frac{t_{s_j}}{\eta}\right)^{\beta}} \right] \left(\frac{1}{\eta}\right)\left(\frac{1}{\beta}\right) d\eta\, d\beta \right\} dt_f \Bigg) dR(T)$$

= f(data)

where: $R_c(T)$ is the critical reliability at service life T, and

data is the set of product failure service lives $\left\{t_{f_1}, t_{f_2}, \cdots, t_{f_N}\right\}$ and

the set of service lives for products that have not failed $\left\{t_{s_1}, t_{s_2}, \cdots, t_{s_M}\right\}$

Full derivation of this equation can be found at:

http://nomtbf.com/2012/07/whats-all-the-fuss-about-bayesian-reliability-analysis-2/

Possible to Solve?

- **Analytically?** ***No!***
- **Using numerical Methods, including ordinary Monte Carlo?** ***No!***
- **With Markov Chain Monte Carlo?**

Yes!

It's so Easy!

- **Build the MCMC samplers for the Weibull parameters, η & β**
  - **Form Likelihood using data, select objective models for parameters**
  - **Multiply and sample using Metropolis-Hastings algorithm**
- **Obtain N joint samples η_i and β_i**
- **Evaluate the reliability equation at 100K miles at all N joint samples to get N samples of reliability at 100K miles**

$$R_i(100k|data) = e^{-\left(\frac{100k}{\eta_i}\right)^{\beta_i}}$$

- **Count the number of samples of reliability at 100K miles >95%, divide by N**

$$I(R(100k) > .95|data) = \frac{\sum_{i=1}^{N} \left\{ 1, R_i(100k|data) > .95 \right\}}{N}$$

What We Did

$$P\left(R\left(T\right)\geq R_c\left(T\right)\mid data\right)=1-\int_0^{R_c(T)}pd\left(R\left(T\right)\mid data\right)dR\left(T\right)$$

$$\propto 1-\int_0^{R_c(T)}pd\left(\int_T^{\infty}\left\{\int_0^{\infty}\int_0^{\infty}\left[\left(\frac{\beta}{\eta}\right)\left(\frac{t_f}{\eta}\right)^{\beta-1}e^{-\left(\frac{t_f}{\eta}\right)^{\beta}}\right]\left[\prod_{i=1}^{N}\left(\frac{\beta}{\eta}\right)\left(\frac{t_{f_i}}{\eta}\right)^{\beta-1}e^{-\left(\frac{t_{f_i}}{\eta}\right)^{\beta}}\right]\right.\right.$$

$$\left.\left.*\left[\prod_{j=1}^{M}e^{-\left(\frac{t_{s_j}}{\eta}\right)^{\beta}}\right]\left(\frac{1}{\eta}\right)\left(\frac{1}{\beta}\right)d\eta\,d\beta\right\}dt_f\right)dR\left(T\right)$$

where: $R_c\left(T\right)$ is the critical reliability at service life T, and

data is the set of product failure service lives $\left\{t_{f_1},t_{f_2},\cdots,t_{f_N}\right\}$ and

the set of service lives for products that have not failed $\left\{t_{s_1},t_{s_2},\cdots,t_{s_M}\right\}$

- **In four simple steps, we:**
- **Solved *That* equation**
- **Solved a complex integral transform**
- **In fact, never even needed *That* equation!**

Pre-posterior Distributions

- **In design, we don't have a clue as to what distributions to use in our PRA for the engineering specialties.**
  - **We haven't built anything yet that could give us any data.**
  - **Most PRA practitioners *assume* distributions – they just guess**
  - **Most engineers are conservative on the technical, and optimistic on schedule and budget.**
  - **Conservative guesses compound**

A Solution to Avoid Assumptions in a PRA

- **Use pre-posterior distributions based on objective uncertainty models**
  - **Select the most general model for the data type, and objective uncertainty models for the parameters**
  - **Multiply the likelihood for a new datum by the objective uncertainty models for the parameters.**
  - **Integrate out the parameters**
- **Result is an objective distribution that can be sampled for use in the PRA**
- **Done with Markov Chain Monte Carlo, as easily as the Zeus 5000 SUV reliability verification**

Summary

- **Dealing with the Engineering Specialties can be tough**
- **Or it can be easy with modern methods**
  - **Requires good SE practices**
  - **Requires modern statistical practices**
  - **And a little coding**
- **But you can do amazing things**

Contact Information

- **Numerous published papers, references, and free codes at www.attwaterconsulting.com**
- **Always looking for new, exciting, and challenging problems to solve so I can write more papers**
- **Contact Me!**
  - **e-mail: mark.powell@attwaterconsulting.com**
  - **Telephone: +1 208 521 2941**
- ***Link with me*: http://www.linkedin.com/in/attwatermarkpowell**

Bonus Examples

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)**
- **NASA performed a single test**
  - **One CTB only**
  - **8,000 successful zipper cycles**
- **Relevant question**

How Sure can we be from the ONE 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
- **Full Disclosure of Assumptions (*not really questionable*):**
  - **Zipper cycling cannot improve reliability of the CTB zipper**
  - **At least 62.4% of CTB failures will occur before 30,000 cycles**
- **No stated maximum acceptable *Risk* – so Parameterize**

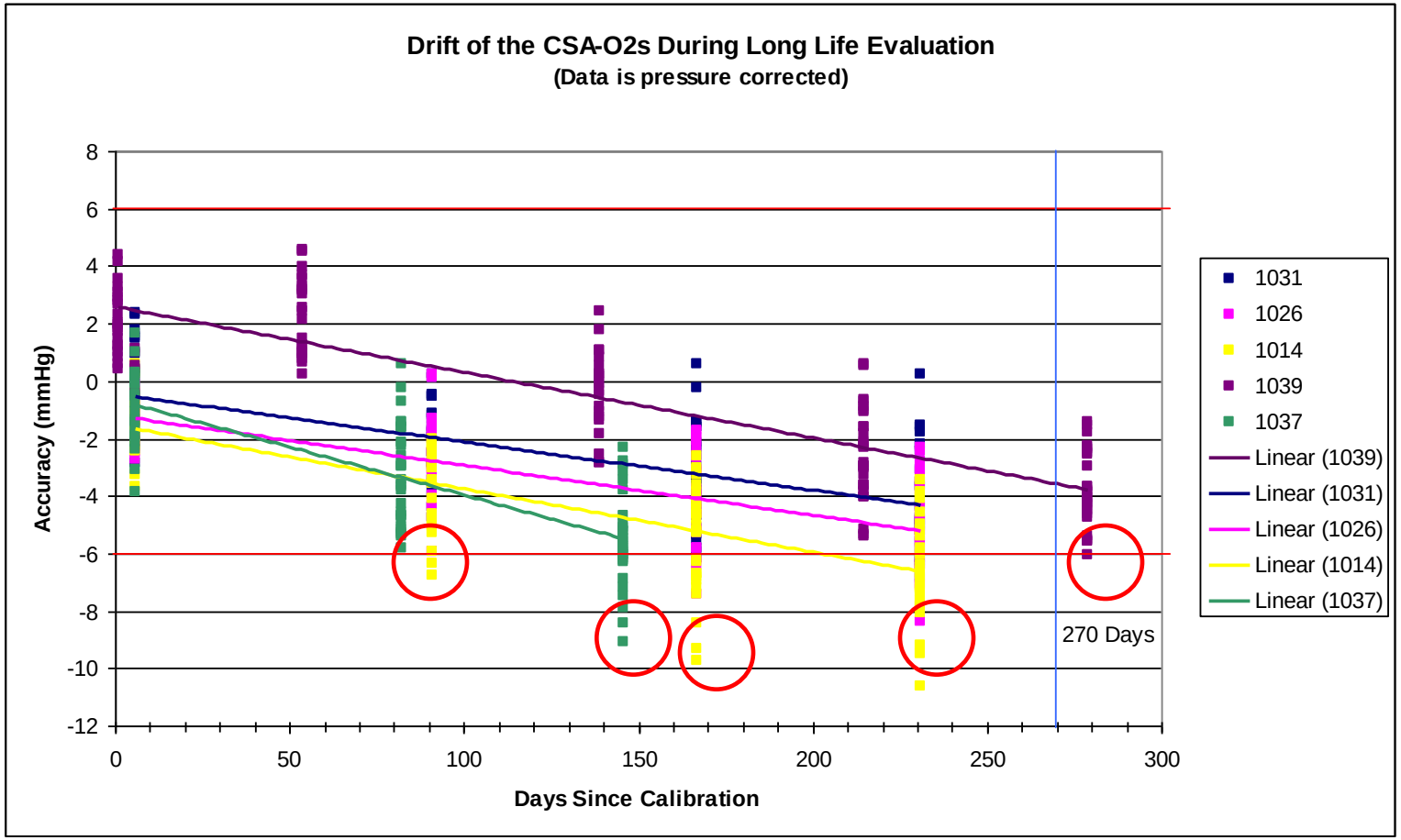
Risk of CTB Zipper Failure by 2K Cycles (R_{2K})	Assurance Provided by Test Results P(True R_{2K}< R_{2K})
1%	75%
5%	88%
10%	94%
20%	98%

Could Not be Solved Without Markov Chain Monte Carlo Methods!

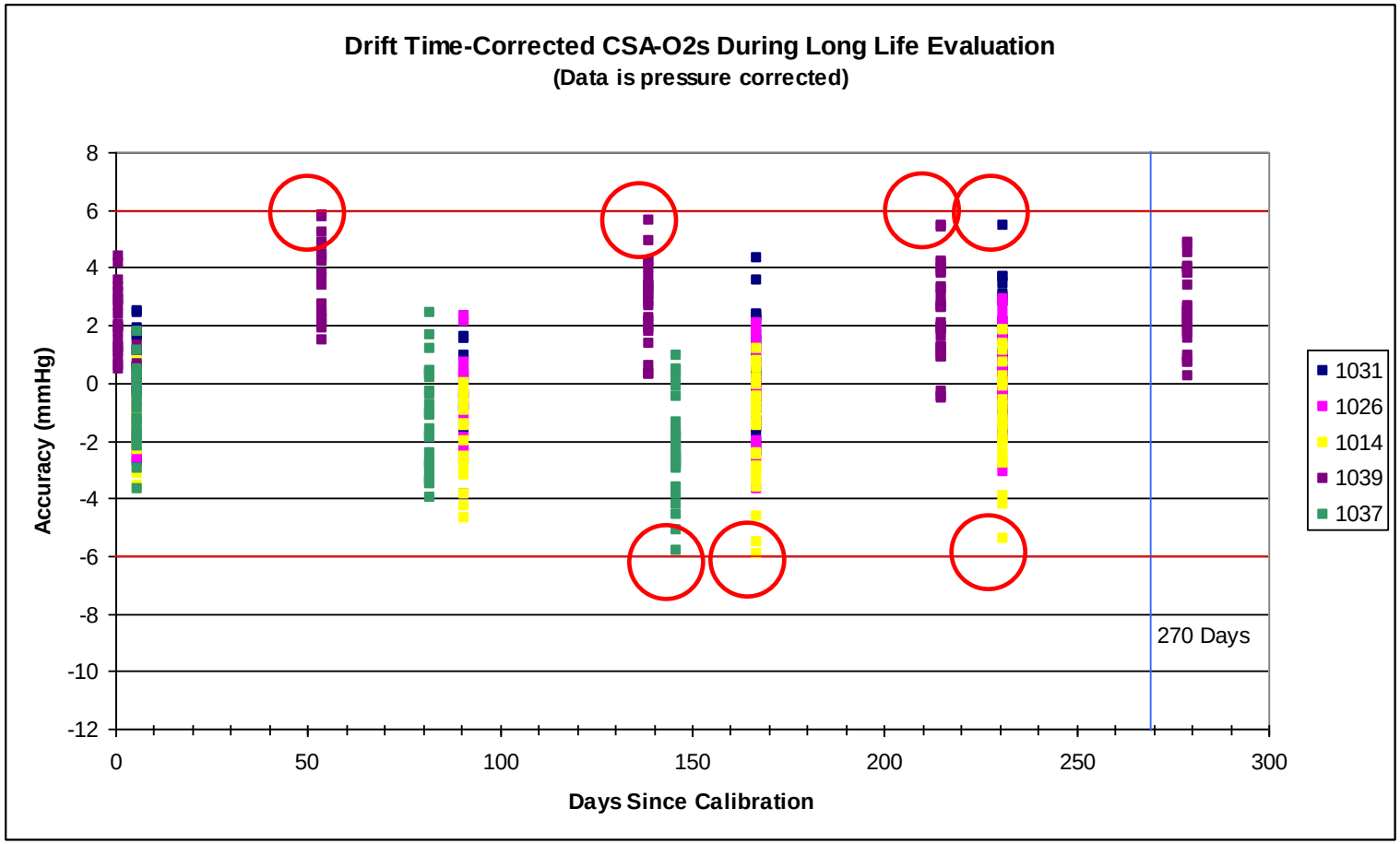
Example: ISS O_2 Sensor Drift

- **Problem: Space Station EVA Prep 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?**

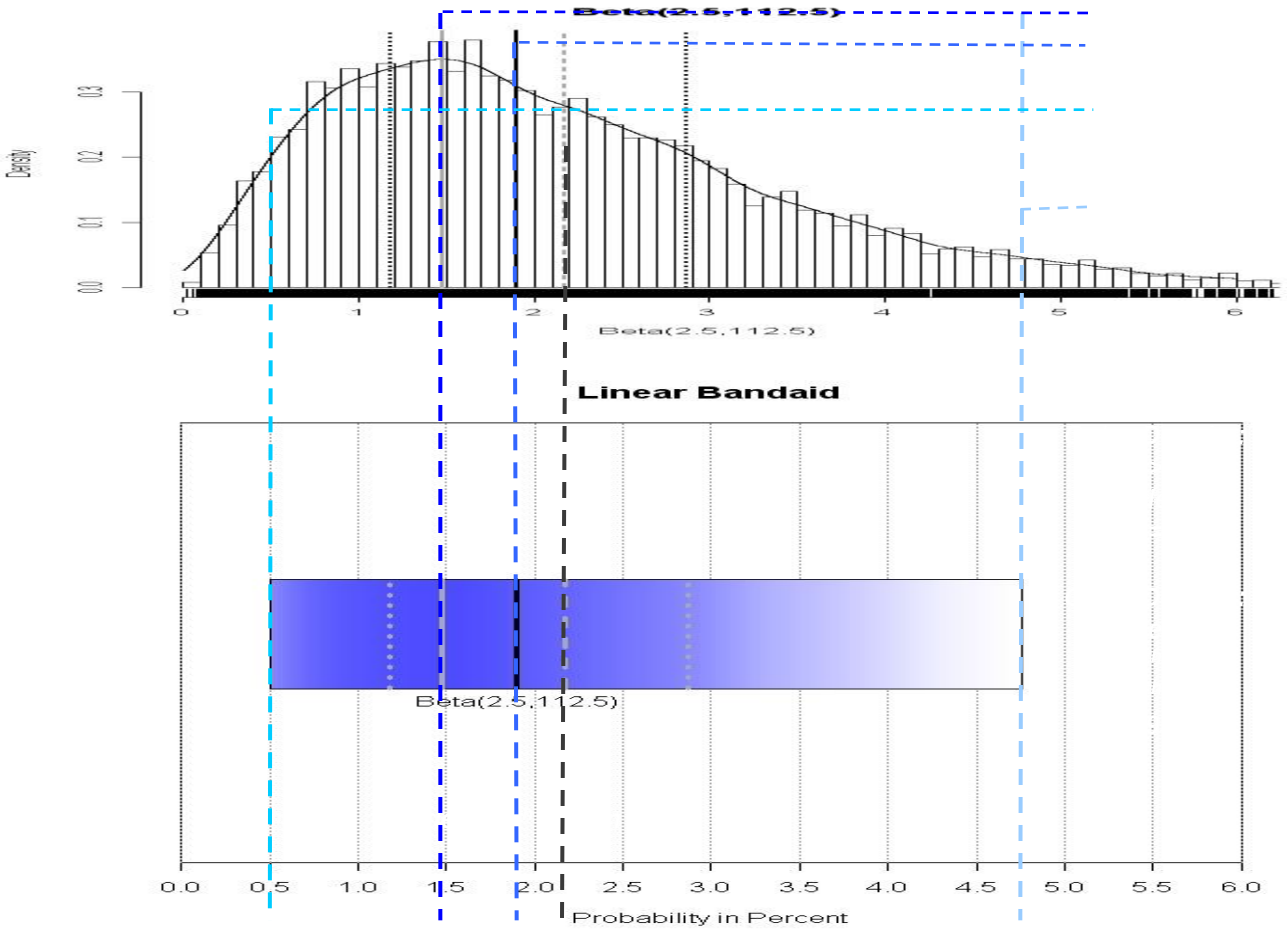
O_2 Sensor Test Data



Drift Corrected O_2 Sensor Data



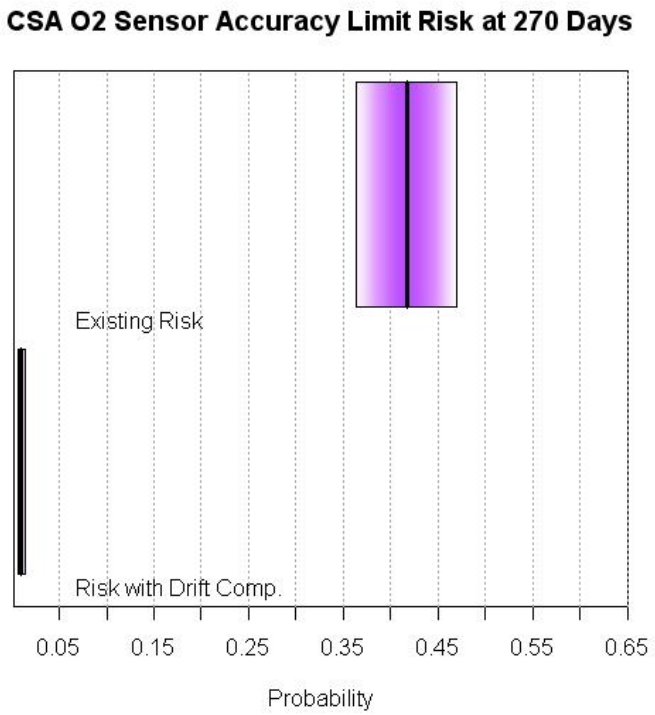
Aside: Risk Density Strips

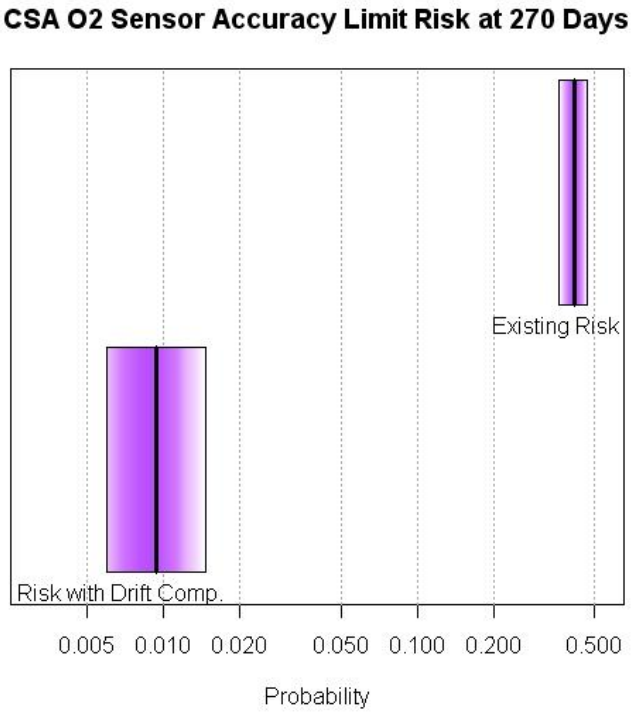


- Great way to display *Risk* distributions
- Great for comparing *Risks*
- Left side at 5%
- Right side at 95%
- Color density proportional to probability density
- Bar at Mode or Median helps

Risk Density Strip codes available free on www.attwaterconsulting.com

O_2 Sensor Risk: Before and After Drift Correction





Linear Scale ***Logarithmic Scale***

O_2 Sensor Risk Summary

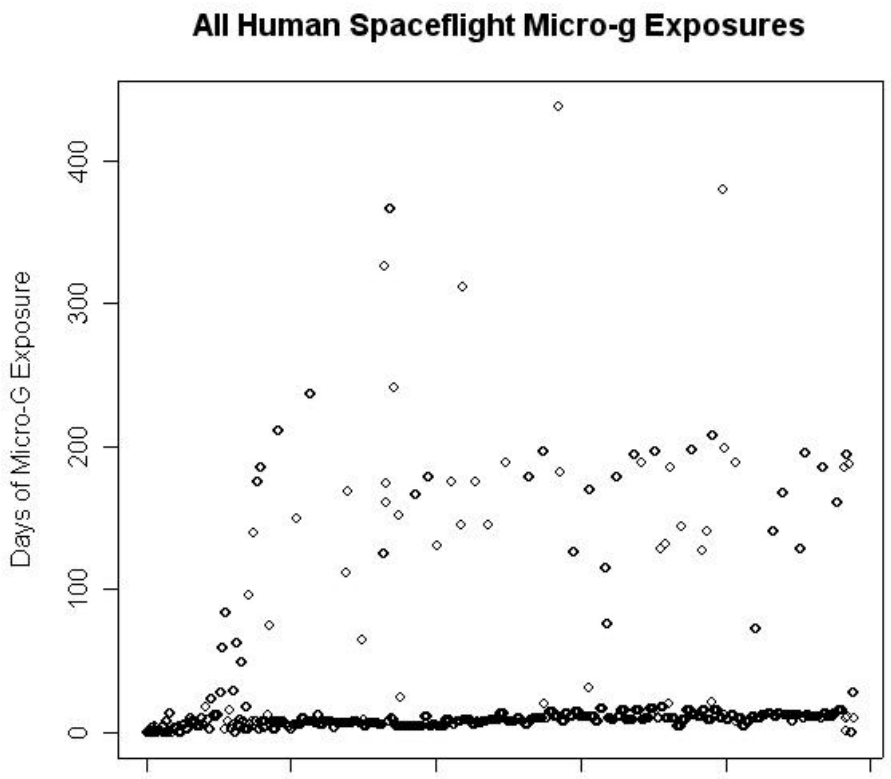
- **Without drift compensation, *Risk* of exceeding accuracy limits at 270 days is 36-46% (with *90% assurance*)**
- **With drift compensation, *95% Sure Risk* of exceeding accuracy limits at 270 days is < 1.5%**
- **Additional O_2 level compensation could reduce *Risk* further**
- ***No Assumptions Needed***

Could Not be Solved Without Markov Chain Monte Carlo Methods!

Example: Astronaut Bone Fracture Risk

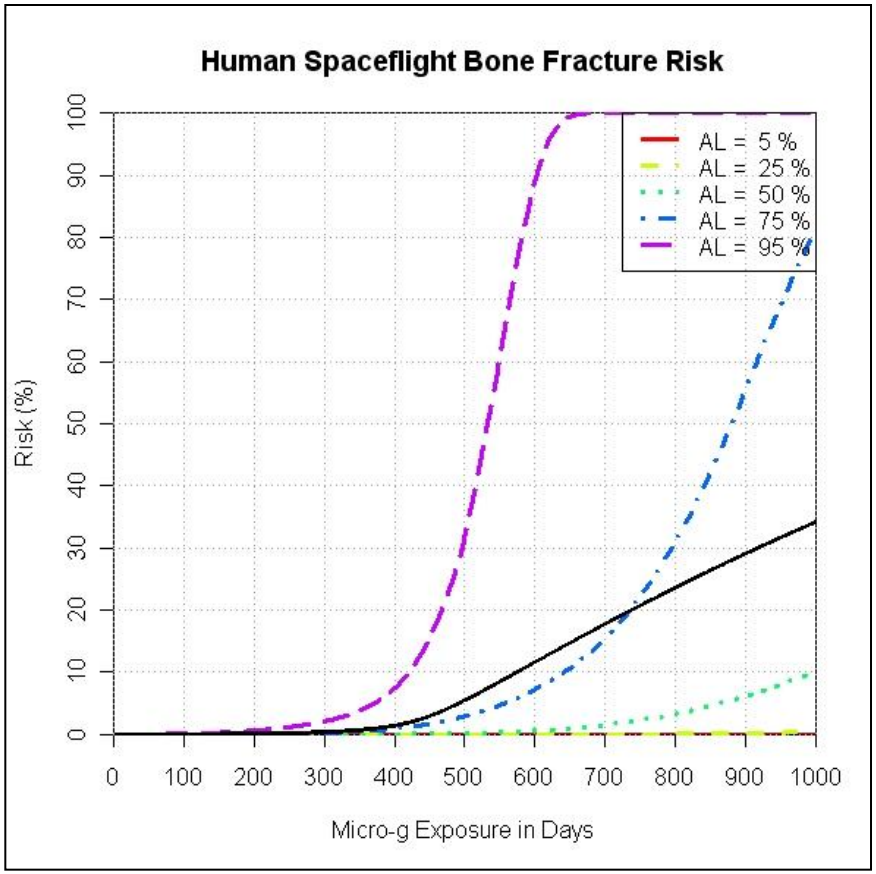
- **On-orbit astronaut bone fractures could have severe consequences.**
  - **To the Astronaut**
  - **To the Mission**
- **Very low probability event – No astronaut has ever broken a bone during a μG mission in history.**
- **Example *Risk* Questions**
  - **What is the *Risk* of bone fracture for long Mars missions?**
  - **How much will the *Risk* increase if International Space Station missions extend from 180 to 365 days?**

The Available Information (the data)



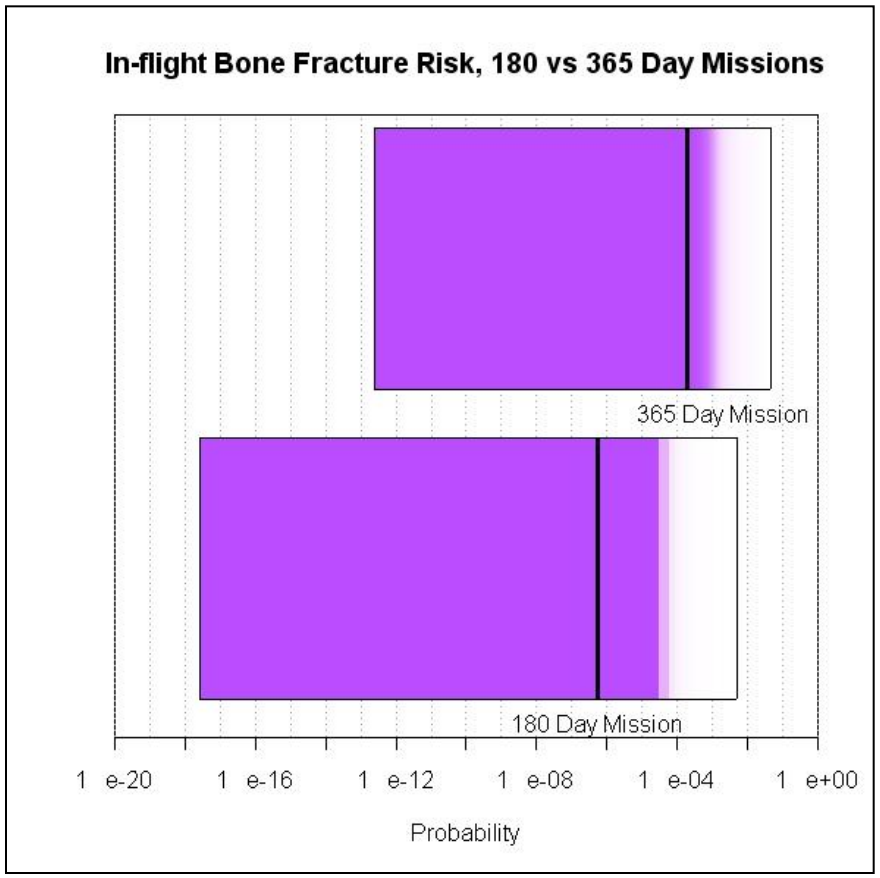
- **977 astronaut μG missions of varying lengths (as of May 2005)**
- **No events observed**
  - **No bones broken**
  - **Did observe 977 μG missions without a broken bone**

Risk Results Parameterized for μG Mission Duration



- **Plotted various assurance levels**
- **As a function of μG mission duration**
- **For Mars missions of 270 days – we can be 95% certain that *Risk* of fracture during the mission is < 3%, based on the information available**
- **Quantified result consistent with *Intuition!***

The ISS Mission Extension Question



- ***Risk*** **Density Strip legend**
  - **Left side at 5th quantile**
  - **Right side at 95th quantile**
  - **Color density proportional to probability density**
  - **Black bar at median (50th quantile)**
- **Can you feel better about making such a decision?**