New Methods for Realistically Assessing Safety

Mark A. Powell
Mechanical Engineering
Systems Engineering
University of Idaho

Introduction

- **System Safety**
  More Visible and Important than Ever!
- **Topics for This Evening**
  - **Back to System Safety *Basics***
  - **System Safety *State of the Art***
  - ***New Methods* for Assessing System Safety**
    - **Introduce and Describe Only, *not Derive***
    - **Detailed Examples in Future Seminars**
  - **Candidate Application: NASA/JSC Orbital Debris Avoidance Safety Flight Rule**
  - **Closing and Questions**

Back to Basics

- **System Safety *Assures* that Acceptable Risks are *not Exceeded* for the System**
- **Risk**
  - **A Combination of Probability of a Mishap Occurring and the Probability that Unacceptable Consequences Occur given the Mishap Occurs**
  - **P(*Consequences* > *Acceptable*|*Mishap*)P(*Mishap*)**
- **Risk Assessment: a *statistical estimate* of the Risk, an *Uncertain Value* of a Probability**
- **Assurance - *Probability Measures on an Uncertain Quantity***
- **What we Often Forget**
  - **Successful System Safety provides Assurance that Acceptable Risks are not Exceeded**
  - **Assurance is measured using *Probability***
  - **Assurance *is a Probability of Achieving a Probability!!!***

A Few More Basics

- ***Simplified*** **View of the Process**
  - **Hazard/Mishap Analysis (FMEA, FMECA, PRA)**
  - **Risk Assessment (Quantification of Risk - Statistics)**
  - **Risk Management (Tracking and Mitigation of Risk)**
- **Fundamental Objective -** ***Achieve*** **Assurance** ***of Acceptable Level of Safety*** **(Mishap Risk)**
  - **Requires** ***Establishment*** **of the Acceptable Level of Mishap Risk**
  - **Requires** ***Establishment*** **of the Acceptable Assurance Level that the Acceptable Level of Risk is not Exceeded**
  - **Requires** ***Realistic*** **Assessments of Assurance that the Acceptable Level of Risk is not Exceeded**
  - **If Unacceptable, Requires** ***Mitigation*** **(Decisions) to** ***Improve*** **Our Assurance that Mishap Risk is below the Acceptable Level**

System Safety: State of the Art

- **A *Risk Management Process* per NASA/DoD Safety Manuals**
  - **NASA: NPG 8715_3**
  - **DoD: MIL-STD-882D, etc.**
- **Probabilistic Risk Assessment (PRA)**
  - **Modern Approach Using *Conditional Relationships* and *Conditional Probability/Statistical* Formulations**
  - **NASA Manual: *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*, 31 March 2002, NASA Office of Safety and Mission Assurance (OSMA)**
  - **DoD Manuals: Inherent but not Emphasized in 882**
- **System Safety - *Very Difficult* to Properly Engineer and Verify *Realistically***

Where it Gets Difficult: Risk Assessment

- **Risk Assessment *Realism* is Mandatory**
  - **If Inherently *Risk Tolerant* - Unacceptable Risks and Mishaps**
  - **If Inherently *Risk Averse* (too conservative) - Unfeasible Mitigations and Too Costly**
  - **Both can produce *Decision Maker* Paralysis and/or *Stress***
- **The Difficulty: *It's in the Statistics***
  - **Few Mishap Data - Engineer Distrust**
  - **Many Non-mishap Data (censored data) - Usable?**
  - **Probability Modeling for Risk Assessments from Mishap Data is Often *Impossible***
  - **Thus, Impossible to *Quantify* Assurance that Acceptable Risks are not Exceeded**

Details on the Difficulty

- **Mishap Data Always Analyzed with a *Statistical Procedure***
  - **Data include Mishaps, *and* Lack of Mishaps**
  - **Risk Assessments (estimates) based on Data are *always* Statistics Themselves**
  - **Risk Assessments (estimates) are *always* Uncertain**
- **Assurance Quantified by *Integrating* the Risk Assessment (estimate) Uncertainty Model**
- **In Engineering, Rarely is it Possible to *Know* the Risk Assessment (estimate) Uncertainty Model**
  - **Without the Uncertainty Model, We *cannot* Quantify Assurance**
  - **Usually Rely on Decision Maker *Comfort* with the Risk Assessment or Best Engineering Judgment or Seat of the Pants *Feel* about the Problem and *the* Assessment Value**
- **Usually, Assurance Quantification is *Ignored* in Safety Decision because it is not Possible to Know**

A Word on PRA

- **Great for Hazard/Mishap Analysis and Modeling**
- **Great for Risk Tracking and Mitigation**
- **Great *Theoretically* for Assurance Quantification for Risk Assessment**
  - **Only Theoretically - works beautifully for some Special and Simple, *Textbook* Problems**
  - **Usually produces an *unidentifiable*, *analytically intractable* Uncertainty Model for the Risk Assessment (estimate)**
- **So, Risk Assessors Revert to *Classical* Statistical Procedures**
  - **Always Introduces *Conservatism* - Well Documented, but not Well Advertised**
  - **Cannot Produce an Uncertainty Model for the Risk Estimate**
  - **Can only provide Seat of the Pants *feel* for Assurance - no Quantification Possible for Assurance**
  - ***But*, Can make a Safety Decision, Often *Painfully Conservative***

The Impact of Reverting to Classical Procedures

- ***At Best*: Safety Decisions Using Classical Procedures are *Overconservative* and *More Costly* than Needed**
  - **VAFB Launch Example - Overconservatism from Applying *Fudge Factors* (RSOR 2000) Reduces Launch Rate**
  - **Reduced Launch Rate Reduces Launch Income**
- ***At Worst*: Safety Decisions Using Classical Procedures are *Arbitrary***
  - **A Risk Assessment (Estimate) Below the Acceptable Level May be at a Very Low Probability Level -**
    $$P(R_{True} < R_{AccLev} \mid R_{Est} < R_{AccLev}) = 1E\text{-}4$$
  - **A Risk Assessment (Estimate) Above the Acceptable Level May be at a Very High Probability Level -**
    $$P(R_{True} < R_{AccLev} \mid R_{Est} > R_{AccLev}) = 0.9999$$
  - **Using Classical Procedures, *Impossible* to Compute these Probability Levels**

New Methods for Risk Assessment

- ***Monte Carlo*** **Methods are Tried, True, and Time Tested for Computing Probability Integrals**
  - ***Numerical Method*** **of Sampling an Uncertainty (Probability) Model and Calculating Probabilities**
  - ***Could Work for Safety*** **Assurance Quantification, but** ***Must*** **Know the Risk Uncertainty (Probability) Model -** ***We Don't***
- **In Mid 1990's,** ***New Methods*** **for Monte Carlo (re)Discovered**
  - **European Biostatisticians Needed to Use PRA for Risky Decisions for Experimental Drug and Surgical Treatments**
  - **Faced Same Problems as in Engineering - PRA produced Unidentifiable and Analytically Intractable Uncertainty Models**
  - **Rediscovered and Applied** ***Markov Chain Monte Carlo*** **(*MCMC*) Methods**
  - ***MCMC*** **Methods Allow Complete Sampling of Unidentifiable and Analytically Intractable Uncertainty Models**
  - **Numerical Monte Carlo Safety Assurance Integrals Possible**

Markov Chain Monte Carlo

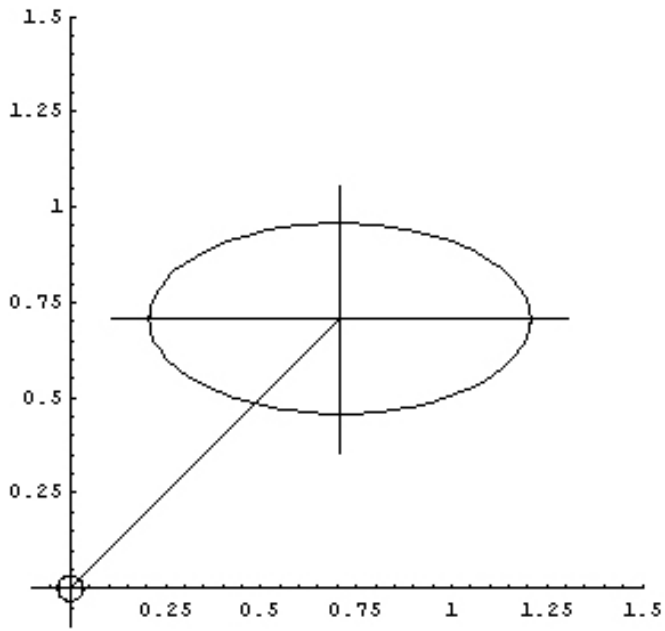
- ***Normal Monte Carlo*** **Sampling Provides** ***Independent*** **Random Samples - no Sample to Sample Correlation**
- **Markov Chains Also Provide Random samples, but have** ***Sample to Sample Correlation***
- **For Approximating Numerical Integrals,** ***Who Cares?!!!***
- **Simplest Example of a Markov Chain - the** ***Drunkard's Walk*** **Problem from Physics**
- ***MCMC*** **Unique Capabilities**
  - **Can Sample** ***any*** **Uncertainty Model, Analytically Tractable or not, Proper or Not -** ***PRA Can Work!***
  - **Algorithms are** ***Unbelievably*** **Simple**
  - **Detailed Examples with Real Data for other Engineering Specialties in later Seminars**
  - **Resources for** ***MCMC*** **provided at end of Presentation**

NASA/JSC Orbital Debris Avoidance Flight Rule

- **Space Junk**
  - **Average Mass: 1,000 pounds Mass**
  - **Collision Relative Velocity: 11.4 km/s**
- **NASA/JSC Orbital Debris Avoidance Flight Rules (abridged) for Shuttle and International Space Station**
  - ***Risk Management Approach* for impending Conjunctions**
  - ***Estimated* Probability of Collision P_c Exceeds Red *Threshold* (1E-4), Maneuver to Avoid Collision (with Caveats)**
  - ***Estimated* Probability of Collision P_c Exceeds Yellow *Threshold* (1E-5), Plan Maneuver to Avoid Collision and Possibly Execute (with Caveats)**
  - ***Based Solely* on Calculated Risk Estimate P_c**
  - **Flight Director Assurance is based on *Feel* Only - *No Safety* Assurance *is Quantified* (not possible with System Safety State of the Art)**

The P_c Estimate

- **Basic Data**
  - ***Least Squares estimates*** **of debris object position and covariance matrix from USSPACECOM Radar Data**
  - ***Least Squares estimates*** **for NASA asset from NASA or USSPACECOM tracking or GPS**
- **The Calculation**
  - **Position and covariance estimates *Assumed* to be True Values of Position Means and Covariances**
  - ***Defines*** **a Nice Multivariate Gaussian Uncertainty Model**
  - ***Integrate*** **this Multivariate Gaussian Model over circle surrounding NASA asset to get P_c**



$$P_c = \iint_{Circle} \frac{1}{2\pi\sigma_x\sigma_y} e^{-\frac{1}{2}\left(\frac{(x-x_0)^2}{\sigma_x^2}+\frac{(y-y_0)^2}{\sigma_y^2}\right)} dx\,dy$$

P_c Estimate Notes

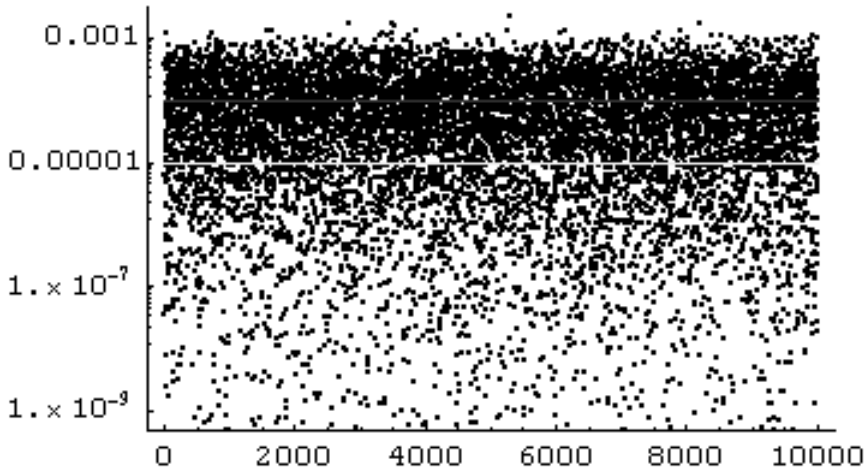
- **Least Squares Position Estimates are *Sample Means* - Uncertainty Modeled by Multivariate *Student-t* Model**
- **Least Squares Covariance Matrix Estimates are *Sample Covariances* - Uncertainty Modeled by Multivariate Generalized *Chi-square* (Wishart) Model**
- **Uncertainty Model for P_c is *Impossible to Know***
  - ***Non-linear Combination* of Student-t Models and Wishart Models in the Integral Calculation**
  - ***Analytically Intractable* Uncertainty Model for P_c - Impossible to Quantify Assurance P_c below Red or Yellow Thresholds with System Safety State of the Art**
  - **Best Hope: Central Limit Theorem Applies and P_c is at 50% Probability (Assurance) Level**

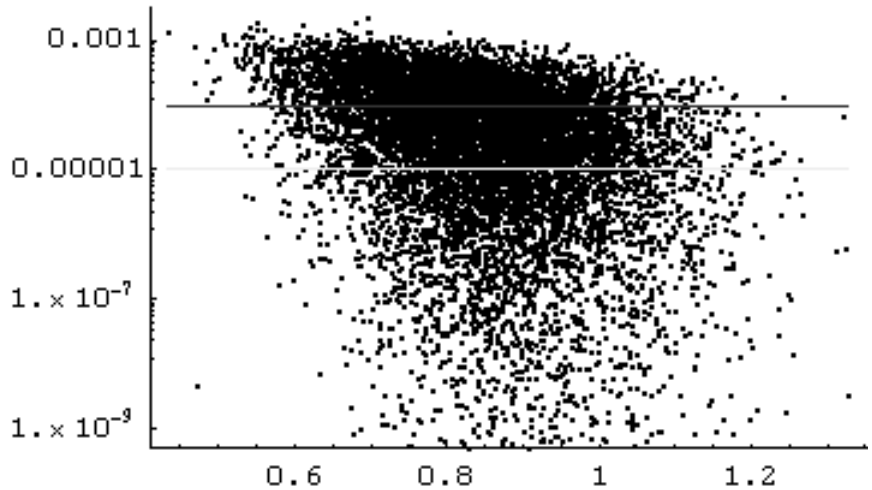
Illustration of the Problem

- **Easy: Simply Use Normal Monte Carlo**
  - **Pick a *Truth Scenario* with *Known* Uncertainty models where the true P_c is just above the 10^{-4} Red Threshold (using multivariate Gaussian models)**
  - **Use Monte Carlo to pick *N* sets Sample Position Means and Sample Covariances from the *Truth Uncertainty Models***
- **For each Sample Mean and Covariance, Make the Truth *Assumption* and Use the P_c Equation (integral) to calculate a Sample of P_c**
- **Histogram the samples of P_c and look at the Unknowable Uncertainty Model for P_c**

Graphical Results

- True P_c = 1.0662 x 10^{-4}, just above Maneuver Threshold
- N = 10,000 sets of Sample Mean and Sample Covariance Matrix samples for P_c Integral Calculation



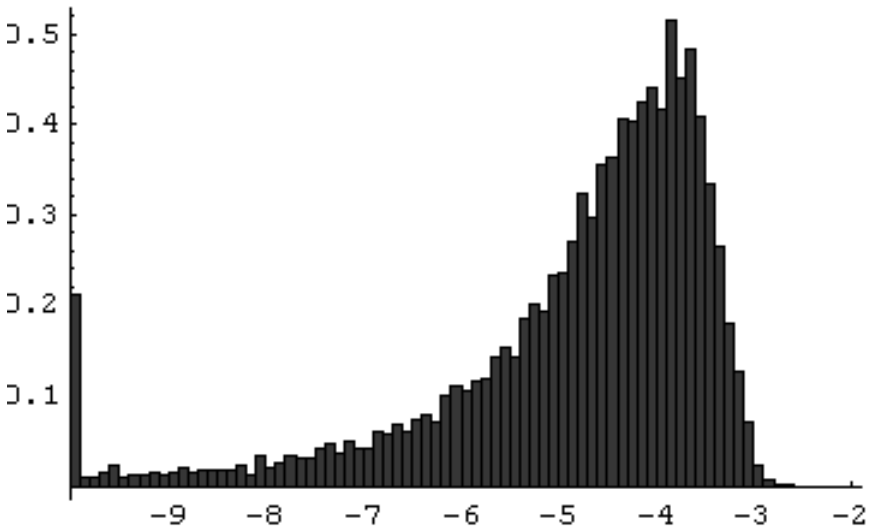


Scatter of P_c Samples **Joint Density – P_c vs Miss Distance**

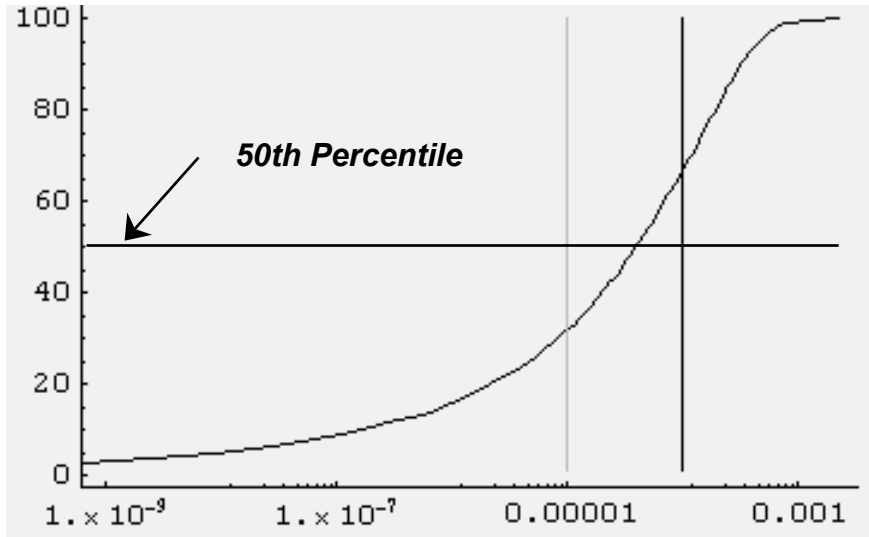
Red Line – Maneuver Threshold, Yellow Line – Planning Threshold

P_c jumps around over 7 orders of magnitude!

More Graphical Results



Histogram of P_c (Log scale)



Cumulative Distribution of P_c

P_c is definitely not Gaussian Distributed!

Synopsis of the Illustration

- **As is Obvious in the Previous Charts, when TRUE P_c is just above the Red Threshold**
  - **Will Observe P_c above Red Threshold and *Perform Needed* Maneuver *ONLY 33% of the time***
  - **Will Observe P_c above Yellow but not Red Threshold and *Plan Needed* Maneuver *ONLY 35% of the time***
  - **Will Observe P_c below Yellow Threshold and *NOT Even Plan Needed* Maneuver *32% of the time***
- **Decision based on this sample of P_c is Truly *Arbitrary* using State of the Art System Safety**
- **Using PRA and MCMC we can Enable the Flight Directors to Make *Much Better and More Comfortable* Orbital Debris Avoidance Decisions!**

The PRA/MCMC Solution

- **Select an Acceptable Assurance *Level***
  - ***Risk Tolerant*: e.g., 90% Assurance - want to be >90% sure Threshold is exceeded before Acting (planning and/or executing a maneuver)**
  - ***Risk Averse*: e.g., 10% Assurance - if >10% sure Threshold is exceeded, Act**
- **Use PRA to Formulate Uncertainty Model for P_c**
  - **Use Least Squares Estimates of Position and Covariance as Input - Same Data Input**
  - **Will be Analytically Intractable and Unknowable**
- **Use *MCMC* to Compute Value of P_c at Chosen Assurance Level - e.g., P_{c10} or P_{c90}**
- **Use this Value of P_{cXX} as input for the Current Flight Rules**

Synopsis

- **System Safety State of the Art is *Very Difficult* for Engineering Problems**
- ***PRA* Offers Hope for Engineering Problems, but Usually Produces Analytically Intractable Solutions in Risk Assessment**
- **Reversions to Classical Methods produce**
  - ***Overconservative* and *Costly* Mitigations**
  - **Decision Maker Stress**
- **New Methods (*MCMC*) Enable full Use of *PRA* to Realistically Assess and Assure Safety**

Upcoming Seminar Series Topics

- **Reliability Assurance - 13 November 2003**
  - **Based on US Coast Guard C130 RAM Problem**
  - **2002 International INCOSE Symposium Best Paper Award**
- **Verification Planning - 4 December 2003**
  - **Optimal Cost Test Plan Development for Ford**
  - **Upcoming IEEE Article**
- **Markov Chain Monte Carlo Algorithms (next year)**
- **Possible Future Topics in the Series (next year)**
  - **Logistics**
  - **Flight Rule Development**
  - **PRA Applications**
  - **Others by Request**

INCOSE

- **Texas Gulf Coast Chapter Sponsorship of Seminar**
- **Contact:**
  - **Jonette Stecklein (Chapter President)**
  - **E-mail: jonette.m.stecklein1@jsc.nasa.gov**

UHCL Systems Engineering Program

- **Joint Sponsorship of Seminar**
- **Contact:**
  - **Dr. Jim Helm**
  - **E-mail: helm@cl.uh.edu**

For More Information

- **Mark Powell Contact Information**
  - **Faculty Website: www.if.uidaho.edu/~powell**
  - **E-mail: powell@if.uidaho.edu**
  - **Telephone: 208-282-7936**
- **Copies of Seminar Series Charts**
  - **Published on Faculty Website**
  - **Available Post Seminar Presentation**

Questions

References

Abernethy, Robert B., *The New Weibull Handbook, Fourth Edition*. Robert B. Abernethy, North Palm Beach, Florida, 2000.

Anderson, Theodore Wilbur, *An Introduction to Multivariate Statistical Analysis, 2nd Edition*. John Wiley & Sons, Inc., New York, 1984.

Berger, James O., *Statistical Decision Theory and Bayesian Analysis, Second Edition*. Springer-Verlag, New York, 1980.

Box, George E. P., and Tiao, George C., *Bayesian Inference in Statistical Analysis*. John Wiley & Sons, Inc., New York, 1973.

Clemen, Robert T., and Reilly, Terence, *Making Hard Decisions*. Duxbury, Pacific Grove, CA, 2001.

Daniels, Jesse, Werner, Paul W., and Bahill, A. Terry, *Quantitative Methods for Tradeoff Analyses*. *Systems Engineering*, Volume 4, John Wiley & Sons, Inc., New York, 2001.

Gamerman, Dani, *Markov Chain Monte Carlo*. Chapman & Hall, London, 1997.

George, Larry, *The Bathtub Curve Doesn't Always Hold Water*; http://www.asqrd.org/articleBathtub. American Society for Quality, Reliability Division, 2002.

Gilks, W. R., Richardson, S., and Spiegelhalter, D. J., *Markov Chain Monte Carlo in Practice*. Chapman & Hall, Boca Raton, Florida, 1996.

Hammond, John S., Keeney, Ralph L., and Raiffa, Howard, *Smart Choices, A Practical Guide to Making Better Decisions*. Harvard Business School Press, Boston, 1999.

More References

Jefferys, William H., and Berger, James O., *Ockham's Razor and Bayesian Analysis*. *American Scientist*, Volume 80, Research Triangle Park, NC, 1992.

Jeffreys, Harold, *Theory of Probability*. Oxford University Press, Oxford, 1961.

Krause, Andreas, and Olson, Melvin, *The Basics of S and S-Plus*. Springer-Verlag, New York, 2000.

Raiffa, Howard, and Schlaifer, Robert, *Applied Statistical Decision Theory*. John Wiley & Sons, Inc., New York, 1960.

Relex Software Corporation, *Relex Failure Data Analysis*; http://www.relexsoftware.com/. Relex Software Corporation, Greensburg, Pennsylvania, 2002.

Reliasoft Corporation, *Life Data Analysis Reference*. Reliasoft Publishing, Tucson, Arizona, 1997.

Schmitt, Samuel A., *Measuring Uncertainty, An Elementary Introduction to Bayesian Statistics*. Addison-Wesley Publishing Company, Inc., Phillipines, 1969.

Sivia, D. S., *Data Analysis, A Bayesian Tutorial*. Oxford University Press, Oxford, 1996.

Venables, William N., and Ripley, Brian D., *Modern Applied Statistics with S-Plus*. Springer-Verlag, New York, 1999.

Williams, David, *Probability with Martingales*. Cambridge University Press, Cambridge, 1991.