STI 11-109

Perspective on Probabilistic Methods for Safety and Reliability Assessments

Frank Groen
NASA OSMA

Presented at Trilateral Meeting, ESTEC, The Netherlands
Aug 31 – Sep 2, 2011

Overview

- Summary of modeling methods, applications
- Criticisms and concerns
  - Implementation
  - Application
- Final considerations

NASA Modeling Approaches

- Reliability Block Diagram / MIL-217
  - Translation of functional design into success-logic
  - Prescriptive, bottoms-up quantification approach
  - Typically conservative point estimates
  - Limited ability to represent multiple failure scenarios

- Fault Tree / Event Tree
  - Static accident scenario models and failure logic
  - Quantification at higher (e.g. sub-system) level based on combination of data, models, judgment
  - Intent: be less conservative, consider uncertainties

NASA Modeling Approaches (cont'd)

- Physics-Based/Functional Simulation
  - Emulation of system behavior
  - Better representation of dynamic effects, interactions
  - Monte Carlo approaches to address uncertainty (variability and lack of knowledge)
  - Requires more expertise, resources

Domains of Application

- Human Space Flight
  - Increasing emphasis on risk-informed design
  - New policy: Agency specifies risk tolerance for missions
  - Used in architectural, design, operational decisions
  - FT/ET primary modeling approach
  - Simulation for selected problems, e.g., abort

- Robotic Space Flight
  - Programs set mission duration, reliability requirements
  - RBD/MIL-217 more prevalent
  - Conservative estimates used as method of assurance

Criticisms and Concerns: Implementation

- "Estimates are not credible"
  - Difficulty addressing unknown unknowns, maturation
  - Hard-to-quantify phenomena (e.g., software behavior)
  - Lack of consistency with qualitative analyses
  - False suggestion of accuracy (e.g., point estimates, standards-based bottom-up assessments)
  - MTBF focus when random failure is minor contributor
  - Limited modeling and review expertise
  - Limited documented experience, feeling for results

Criticisms and Concerns: Application

- "Too much focus on total risk, top risk drivers only"
  - Lack of clear hazard-level risk criteria weakens case for addressing small contributors
  - Mix of traditional review-based and risk-informed approaches is not straightforward
- "No added value; Yet another SMA requirement"
  - Diverse problems require diverse models
  - Prescription and application of methods without a clear tie to program objectives is not beneficial
  - Application independent of other safety and reliability evaluations leads to (perception of) incoherence

Considerations

- In a risk-informed context, approaches involving sole verification of probabilistic requirements via prescribed methods and databases are problematic
  - Instead, require a credible case that criteria are met
  - Avoid risk of stagnant practices
- By default, aim to develop realistic estimates while accounting for uncertainties
  - Give suppliers responsibility and flexibility to utilize best available methods and data (incl. counter-data)
  - Introduce analysis protocols only as needed
  - Improve evaluation of flight experience to support analyses and reviews