

# **Achieving High Assurance:** Formal, Informal, and Combined Approaches

Jeff Tian (tian@engr.smu.edu)  
Southern Methodist University  
Dallas, Texas, USA

## **Contents**

- HA: Qualitative or Quantitative?
- A Risk-Based Combined Approach
- Applicability and Effectiveness

---

## Qualitative vs Quantification HA

---

- Many aspects/attributes to high assurance, some qualitative and some quantitative.
  
- **Qualitative** HA aspects:
  - ▷ Safety: largely qualitative.
  - ▷ Fault tolerance.
  - ▷ Security, etc.
  - ▷ Some attempts to quantify the above.
  - ▷ Analysis: causal, type, distribution...
  
- **Quantitative** HA aspects:
  - ▷ Reliability: failure-rate, MTTF, etc.
  - ▷ Availability: % for system/subsystems.
  - ▷ Performance: measurement/modeling.
  - ▷ Analysis: statistical/other modeling

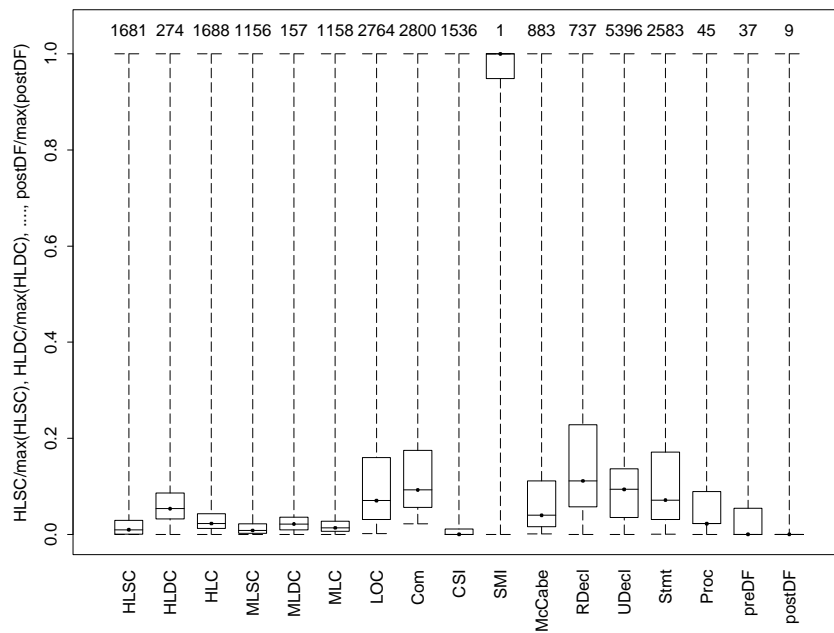
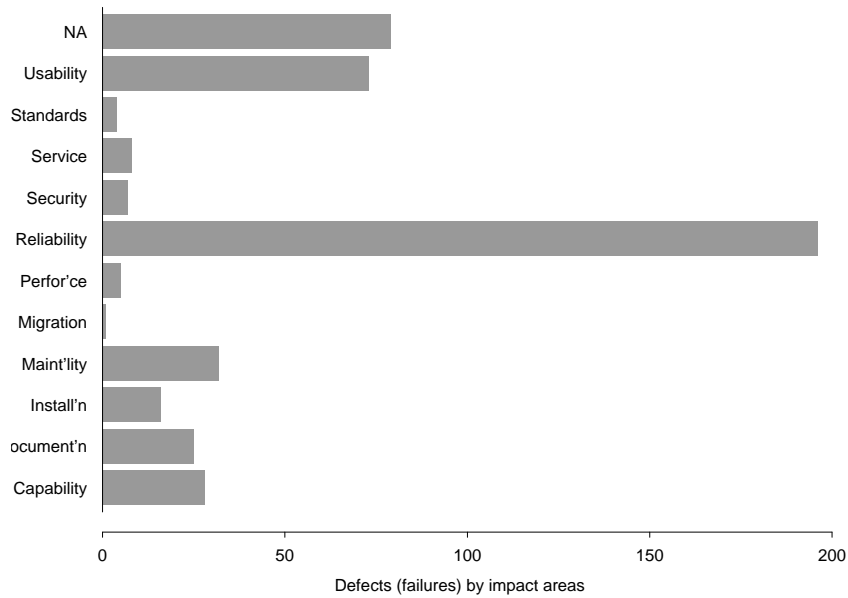
---

## Approaches for HA

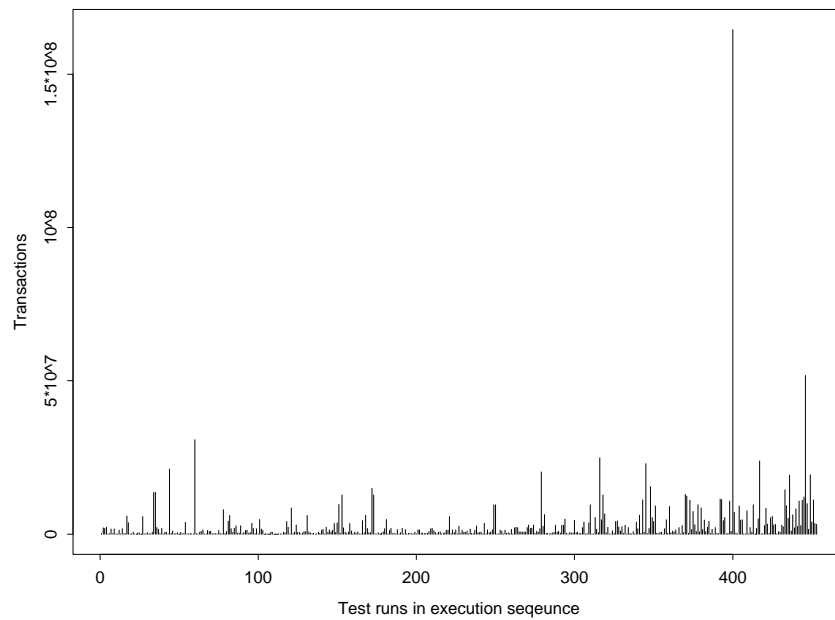
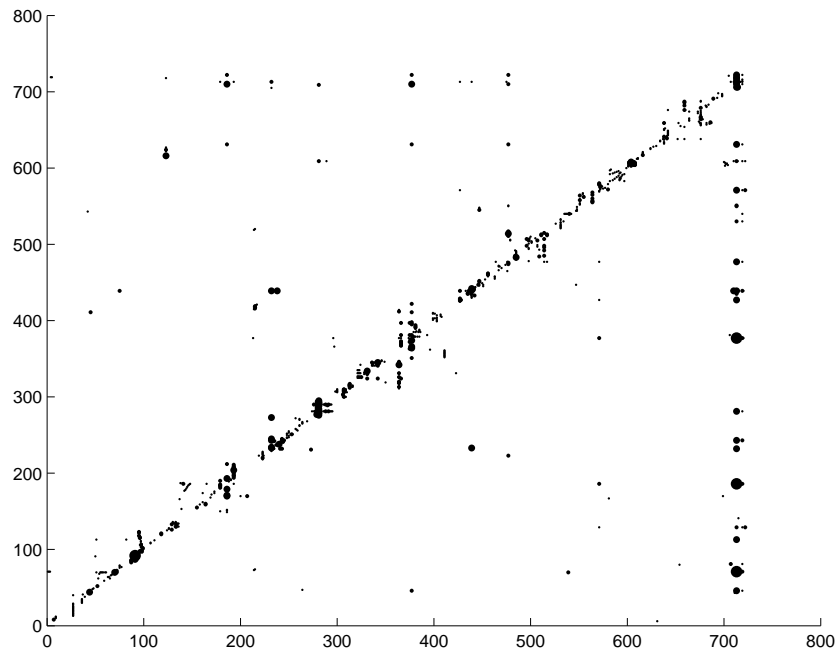
---

- Formal approaches
  
- Informal approaches
  
- A risk-based, combined approach:
  - ▷ Which aspect to focus on?
    - qualitative vs quantitative
  - ▷ Where to focus our effort?
    - uniform/coverage vs non-uniform
  - ▷ Basis for non-uniform focus:
    - risks and leverages/opportunities
  - ▷ How to focus:
    - risk characterization (HA aspect)
    - risk identification (techniques?)
    - risk resolution (coupled with above)

# Risk: Defect/Metrics Data



# Risk: Usage/Workload Data



## Risk and HA

---

- **Risk:** Highly uneven distribution of quality, defect, cost, usage, performance, etc.
  - ▷ “80:20” rule or Pareto’s principle.
  - ▷ Focus: high-risk/high-leverage units.
  - ▷ Risk can be turned into opportunities.
  
- Leveraging risks into opportunities for HA:
  - ▷ risk characterization
    - HA aspect of concern as starting point
    - identification/collection of related data
  - ▷ risk identification
    - qualitative risk id techniques
    - quantitative risk id techniques
  - ▷ risk resolution
    - direct negation of identified risks
    - influence factors  $\Rightarrow$  preventive
    - impact factors  $\Rightarrow$  tolerance

## Risk Characterization: Perspectives

---

- HA aspects manifested to different parties.
  
- External risk to customers/users
  - ▷ Most of the HA aspects are based on external customer/user perspectives.
  - ▷ E.g.: *Reliability* = probability of failure-free operations for a period or input-set
    - usage-based statistical testing (UBST)
    - risk-based reliability improvement
  
- Internal risk to software organizations:
  - ▷ Internal defects affect many HA aspects.
  - ▷ Cost, process, technology risks.
  - ▷ Internal risks↓ ⇒ external risks↓.
  - ▷ Indirect risk identification & reduction.

---

## Risk Identification

---

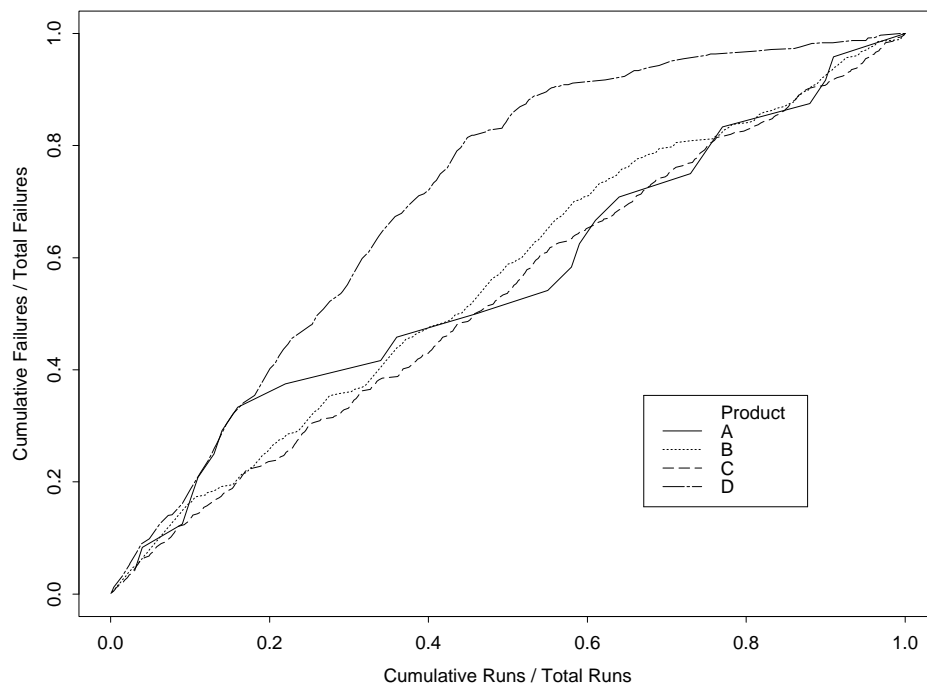
- Qualitative risk identification:
  - ▷ Causal analysis, root cause analysis etc.
  - ▷ Ishikawa's fishbone diagrams.
  - ▷ FTA: Fault tree analysis.
  - ▷ ETA: Event tree analysis.
  - ▷ FMEA: Failure mode/effects analysis.
  - ▷ ... involving subjective elements
  
- Quantitative risk identification:
  - ▷ Many statistical analyses
  - ▷ Traditional: correlation, regression, etc.
  - ▷ New: PCA, DA, TBM, etc.
  - ▷ AI/learning: NN, OSR, GA, etc.
  - ▷ ... requiring large amounts of data

## Risk Resolution and Management

---

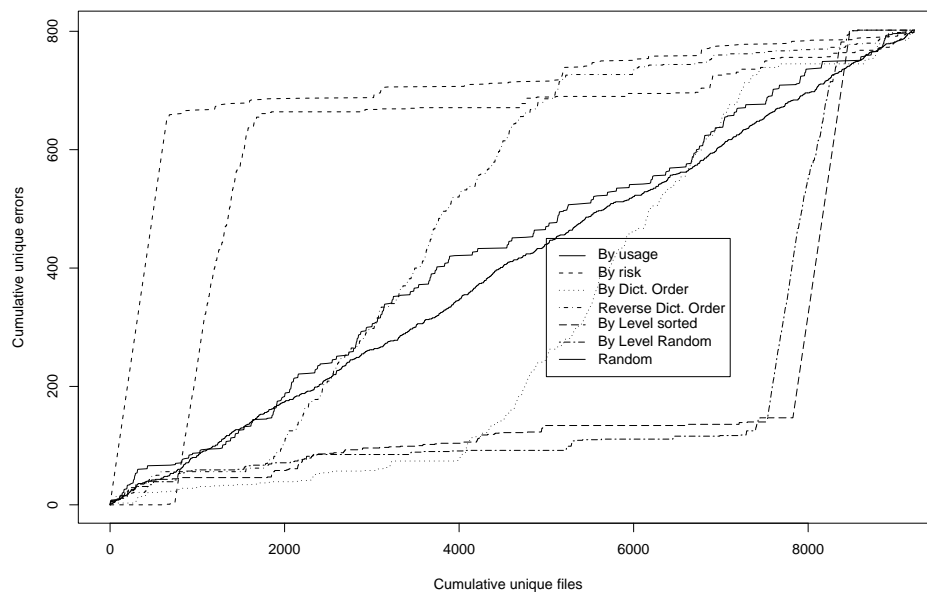
- Direct negation of identified risks
  - ▷ focused testing of high-usage areas
  - ▷ focus on defect-prone modules
  - ▷ rework/restructuring to reduce risks
  - ▷ remedial actions for current projects
  
- Influence factors and pre-conditions:
  - ▷ preventive measures
  - ▷ applied to similar/future projects
  
- Impact factors and consequences:
  - ▷ fault tolerance
  - ▷ other features/barriers/controls
  - ▷ applied to future (and current?) projects

## Example: Accelerated Reliability Growth



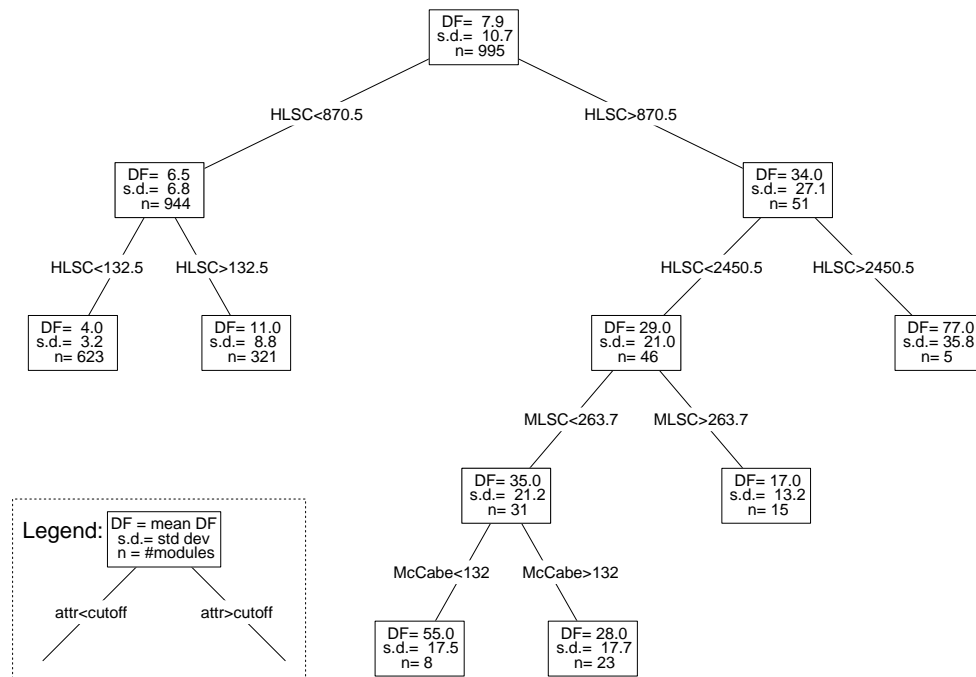
- Focused/accelerated reliability improvement via tree-based reliability models (TBRMs) for IBM products (above)
- New: Reliability and technical performance analysis via hypothesis testing and data envelopment analysis (DEA) for Lockheed Martin software by Siok/Tian, HASE 3a.

## Example: Web Reliability Assurance



- Different web sites: SMU/KDE/AMS
  - ▷ reliability growth simulation:
    - ≈ 2/3 defect reduction in 1 month
  - ▷ accelerated reliability growth via (ODC inspired) risk identification (above)
  - ▷ new: Alaeddine/Tian, HASE'07 6c.

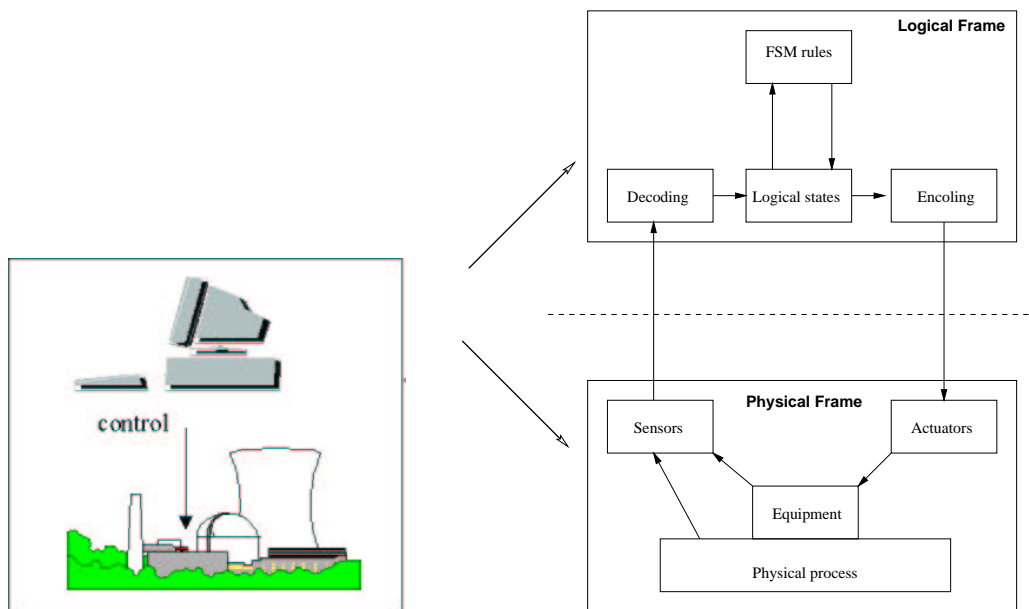
## Example: Focused Defect-Reduction



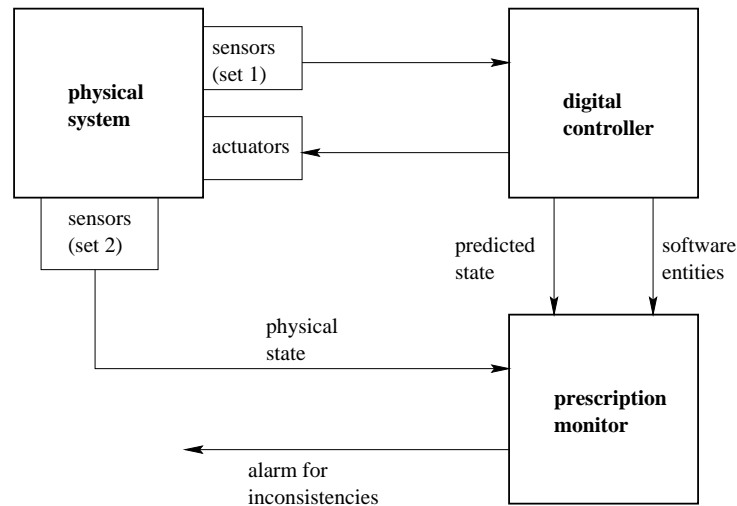
- TBDM for defect↓ and quality↑ applied to IBM, Nortel, and OpenSource Products.
- Related: Formal hypothesis testing (HT) to compare high-defect vs high-complexity modules.

## Example: Safety Analysis

- TFM: Two-Frame-Model
  - ▷ Physical and logical frame
  - ▷ Focus: interface/interaction problems



## Example: Safety Improvement



- Prescriptive specification checking:
  - ▷ Analyze sources of hazard
    - frame inconsistencies, sub-types
  - ▷ Derive systematic assertions
  - ▷ Dynamically check the assertions
  - ▷ Positive simulation results

## Summary and Perspectives

---

- A risk-based combined approach to HA:
  - ▷ 80:20 rule  $\Rightarrow$  risk focus
  - ▷ usage-based statistical testing
  - ▷ defect-prone module characterization
  - ▷ risk-based reliability improvement
  - ▷ frame consistency checking for safety
  
- Positive impact on different systems:
  - ▷ Commercial/defense software: reliability $\uparrow$
  - ▷ Web-based: heterogeneity/quality
  - ▷ Embedded: safety/performance
  
- Future integration with other formal and informal approaches.