Reducing Autonomy Risks through Rational Selection of Verification Strategies

Julian Richardson, RIACS/NASA Ames Research Center
Barry Boehm, Ray Madachy, LiGuo Huang, University of Southern California
Dan Port, Rick Kazman, University of Hawaii

GSAW 2006
March 29, 2006
Understanding Autonomy Risks

• Autonomy high payoff technology for NASA:
  – e.g.: automated rendezvous and docking, ISHM; deep space

• But there are barriers to use:
  – little heritage, hard to ensure correctness, new failure modes

• *Aim to assist identification and quantification of risks for (autonomy) software*

• Key risk quantities:
  – Risk Exposure \( \text{RE} = \text{Prob(Loss)} \times \text{Size(Loss)} \)
  – Risk Leverage \( \text{RL} = (\text{RE(before)} - \text{RE(after)}) / \text{mitigation cost} \)
Software Defect Detection Opportunity Tree

Defect Detection and Removal
- Rqts.
- Design
- Code

Automated Analysis
- Completeness checking
- Consistency checking
  - Views, interfaces, behavior, pre/post conditions
- Traceability checking
- Compliance checking
  - Models, assertions, standards

Reviewing
- Peer reviews, inspections
- Architecture Review Boards
- Pair programming

Testing
- Requirements & design
- Structural
- Operational profile
- Usage (alpha, beta)
- Regression
- Value/Risk - based
- Test automation
Orthogonal Defect Classification
- Chillarege, 1996

Percent within activity

<table>
<thead>
<tr>
<th>Activity</th>
<th>Function</th>
<th>Assignment</th>
<th>Interface</th>
<th>Timing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design</td>
<td>40</td>
<td>30</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Code review</td>
<td>40</td>
<td>30</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Function test</td>
<td>25</td>
<td>20</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>System test</td>
<td>20</td>
<td>30</td>
<td>20</td>
<td>20</td>
</tr>
</tbody>
</table>
Current COQUALMO System

COQUALMO

Defect Introduction Model

Defect Removal Model

Software Size Estimate

Software platform, Project, product and personnel attributes

Defect removal profile levels Automation, Reviews, Testing

Software development effort, cost and schedule estimate

Number of residual defects Defect density per unit of size
### Defects versus V&V Tools

<table>
<thead>
<tr>
<th>Severity</th>
<th>Polyspace</th>
<th>Model Checking</th>
<th>Runtime Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Divide by 0</strong></td>
<td>1</td>
<td>X</td>
<td>1</td>
</tr>
<tr>
<td><strong>Uninitialized Variable</strong></td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td><strong>Deadlock Race</strong></td>
<td>X</td>
<td>X</td>
<td>3</td>
</tr>
<tr>
<td><strong>Array bounds</strong></td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td><strong>Math functions</strong></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>Resource contention</strong></td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td><strong>Error Handling</strong></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>Return codes</strong></td>
<td>1</td>
<td>?</td>
<td>1</td>
</tr>
</tbody>
</table>

**Tool/Technique mitigation for each defect**

- Two columns:
  - Left: Our expectation
  - Right: Experimental results
- 1 (good), 2 (OK), 3 (can detect), X (cannot detect), ? (don’t know)
Risk Exposure Calculation

Checklist/taxonomy

- Risk
- Development
- Requirements
- Design
- Code
  - Incompleteness
  - Runtime errors
  - Ambiguity
  - Numerical errors
  - Traceability

Historical risk frequency data

- Requirements defects
- Design defects
- Coding defects

User selects applicable subtypes from taxonomy

- inconsistency
- creep
- volatility
- performance
- numerical stability
- initialization
- external interfaces

Applicable risks e.g.

COQUALMO

EXPERT COCOMO

Macro-Risk

Project Development Attributes

Risk exposure for each risk for this project

Risk Exposure Calculation

<table>
<thead>
<tr>
<th>Incompleteness</th>
<th>Ambiguity</th>
<th>Traceability</th>
<th>Runtime errors</th>
<th>Numerical errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>4000</td>
<td>1500</td>
<td>10000</td>
<td>6000</td>
<td>900</td>
</tr>
<tr>
<td>10000</td>
<td></td>
<td></td>
<td>4000</td>
<td>1000</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total risk exposure

Σ 8

Project Development Attributes

©USC-CSE

3/29/06
RL-Prioritized Risk Mitigation

- random
- strategic method
- expert prioritization
- random 2
- random 3
Macro-Risk Sources

• Plans, Schedules, Budgets
  – Late, inadequate V&V, testbeds; lack of slack

• Contracts, Reviews
  – Overfocus on functions, hardware, nominal case
  – Lowest-cost labor, no retention incentives

• Systems of Systems, COTS
  – Inconsistent assumptions, interfaces, protocols; dynamism

• Change/Risk Management
  – Requirements creep, bureaucracy, SoS scalability

• KPP Trades
  – Safety/security/availability/performance/evolvability/scalability