Reasoning about the Value of Dependability: iDAVE Model

LiGuo Huang, Barry Boehm, Apurva Jain
liguohua, boehm, apurvaja@usc.edu
iDAVE Model Objectives

• iDAVE: Information Dependability Attribute Value Estimation

• Problem: how to make decisions about a software-intensive system’s dependability level
  – Involve strong economic decisions

• Use iDAVE model to estimate and track software dependability ROI
  – Achieve the desired values for software dependability attributes
  – Help analyze and select the most effective software dependability strategies
iDAVE Model Overview

• Cost Estimating relationships (CER’s) from the Constructive Cost Model COCOMO II
• Dependability estimating relationships (DER’s) from the Constructive Quality Model COQUALMO
• Value estimating relationships (VER’s) supplied by the system’s stakeholders
iDAVE Model Framework

iDAVE

Cost estimating relationships (CER's):
Cost = \( f \) \[ \begin{bmatrix} \text{IP capabilities (size)}, \\
\text{project attributes} \end{bmatrix} \]

Dependability attribute estimating relationships (DER's):
\( D_i = g_i \) \[ \begin{bmatrix} \text{dependability investments}, \\
\text{project attributes} \end{bmatrix} \]

Value estimating relationships (VER's):
\( V_j = h_j \) \[ \begin{bmatrix} \text{IP capabilities}, \\
\text{dependability levels } D_i \end{bmatrix} \]

Time-phased
- Cost
- Dependability attribute levels \( D_i \)
- Value components \( V_j \)
- Return on investment

10/22/2003

©USC-CSE
COQUALMO Overview

COCOMO II

COQUALMO

Defect Introduction Model

Defect Removal Model

Software development effort, cost and schedule estimate

Number of residual defects
Defect density per unit of size

Software Size Estimate

Software platform, Project, product and personnel attributes

Defect removal profile levels
Automation, Reviews, Testing

©USC-CSE
## COQUALMO Defect Removal Rating Scales

<table>
<thead>
<tr>
<th></th>
<th>Very Low</th>
<th>Low</th>
<th>Nominal</th>
<th>High</th>
<th>Very High</th>
<th>Extra High</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Automated Analysis</strong></td>
<td>Simple compiler syntax checking</td>
<td>Basic compiler capabilities</td>
<td>Compiler extension</td>
<td>Intermediate-level module</td>
<td>More elaborate req./design Basic dist-processing</td>
<td>Formalized specification, verification. Advanced dist-processing</td>
</tr>
<tr>
<td><strong>Peer Reviews</strong></td>
<td>No peer review</td>
<td>Ad-hoc informal walk-through</td>
<td>Well-defined preparation, minimal follow-up</td>
<td>Formal review roles and Well-trained people and basic checklist</td>
<td>Root cause analysis, formal follow Using historical data</td>
<td>Extensive review checklist Statistical control</td>
</tr>
<tr>
<td><strong>Execution Testing and Tools</strong></td>
<td>No testing</td>
<td>Ad-hoc test and debug</td>
<td>Basic test criteria based on checklist</td>
<td>Well-defined test seq. and basic test coverage tool system</td>
<td>More advance test tools, preparation. Dist-monitoring</td>
<td>Highly advanced tools, model-based test, extensive stress test</td>
</tr>
</tbody>
</table>

COCOMO II p.263
iDAVE Tool

Step 1: Overall Project Information

- Project Name
- SLOC
- COCOMO II Cost Drivers (except RELY)
iDAVE Tool

— Define System Dependability Level

• System dependability level represented by RELY cost driver rating

• *Two approaches* to define the system dependability level
  – RELY rating determines defect removal profiles
  – Weighted average of defect removal factors determines RELY rating

• Starting from the baseline dependability investments
COCOMO II Cost/Reliability Tradeoff
- Calibrated to 161 projects

<table>
<thead>
<tr>
<th>RELY rating</th>
<th>MTBF (hrs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very High</td>
<td>300K</td>
</tr>
<tr>
<td>High</td>
<td>10K</td>
</tr>
<tr>
<td>Nominal</td>
<td>300</td>
</tr>
<tr>
<td>Low</td>
<td>10</td>
</tr>
<tr>
<td>Very Low</td>
<td>1</td>
</tr>
</tbody>
</table>

If RELY = Extra High, MTBF = 1Mhrs
iDAVE Tool

— Step 2: Previous Dependability Ratings (approach I)

Dependability cost driver: RELY

Three COQUALMO defect removal factors

Defect density

MTBF

MTBF

MTBF

MTBF

MTBF

MTBF

MTBF

MTBF
iDAVE Tool

—— Step 2: Previous Dependability Ratings (approach II)

Three COQUALMO defect removal factors ratings

Weights of three defect removal factors

Dependability cost driver: RELY
iDAVE Tool

Step 4: Display ROI Analysis Results

- Total Mission Value
- MTTR
- Availability = MTBF/(MTBF + MTTR)
- \( \Delta \) Availability: \( \Delta \) Value
- Cost, Value, ROI analysis results
iDAVE Analysis
– Planetary Rover

• Top priority dependability attribute: survivability (JPL)
  – Without survivability, your first failure is your last
  – With survivable elements, always a chance to recover
    • With communication, can create fixes from Earth

• Availability: a proxy for survivability
  – Increase MTBF (mean time between failures)
  – Decrease MTTR (mean time to repair)
  – Availability = MTBF/(MTBF+MTTR)
Representative Rover Availability ROI Parameters

• Total Mission value = Cost = $300M
• Software cost (RELY = Nominal) = $20M
• MTTR = 150 hours
  – About a week to diagnose, reprogram, recover
• Value of X% availability increase = $300M(X/100)
• Baseline dependability investment level: High
Cost to Achieve Extra High Reliability

- Analysis tools and analysis -- $2M
- Formal peer reviews -- 1M
- Advanced test tools, execution -- 3M

Total -- $6M

• Corresponds to 30% added cost for Independent V&V
## ROI Analysis Results: Increasing MTBF

<table>
<thead>
<tr>
<th>RELY Rating</th>
<th>MTBF (hrs)</th>
<th>MTTR (hrs)</th>
<th>Avail.</th>
<th>Loss ($M)</th>
<th>Increased Value ($M)</th>
<th>Cost ($M)</th>
<th>Δ Cost ($M)</th>
<th>ROI</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>10,000</td>
<td>150</td>
<td>0.9852</td>
<td>4.44</td>
<td>0</td>
<td>22</td>
<td>0</td>
<td>----</td>
</tr>
<tr>
<td>Very High</td>
<td>300,000</td>
<td>150</td>
<td>0.9995</td>
<td>0.15</td>
<td>4.29</td>
<td>25.2</td>
<td>3.2</td>
<td>0.32</td>
</tr>
<tr>
<td>Extra High</td>
<td>1M</td>
<td>150</td>
<td>0.99985</td>
<td>0.045</td>
<td>0.105</td>
<td>31.2</td>
<td>6.0</td>
<td>-0.98</td>
</tr>
</tbody>
</table>
iDAVE Analysis
– Sierra Mountainbikes Order Processing

• Baseline Business Case Analysis
  – Estimated total sales: $531M
  – Software cost (RELY = Nominal): $3.45M
  – Mean time to repair (MTTR): 3 hrs
  – Assume 1% downtime, 1% lost sales and profits
  – Baseline dependability investment level: Nominal
ROI Analysis Results Comparison

iDAVE ROI Analysis Results On Increasing Dependability Investment Levels
(starting from baseline investments)

<table>
<thead>
<tr>
<th>Dependability Investment Levels</th>
<th>ROI</th>
</tr>
</thead>
<tbody>
<tr>
<td>N→H</td>
<td>15.1</td>
</tr>
<tr>
<td>H→VH</td>
<td>0.32</td>
</tr>
<tr>
<td>VH→XH</td>
<td>-0.8</td>
</tr>
</tbody>
</table>

Sierra Order Processing

Planetary Rover
User Feedback and Future Work

• Planetary Rover (JPL)
  – Worth pursuing and calibrating to project experience
  – Joint research proposal submitted
  – Value loss underestimated: serious failure impact reputation, cause delays in future mission preparations

• Supply Chain Software Developers
  – Stopping at High RELY level appropriate
  – Value loss function actually nonlinear

• Need to extend model to additional dependability attributes.
  – Safety, Security, Accuracy, and Performance Assurance