Evaluation of Safety-Critical Software

David L. Parnas, A.John van Schouwen, and Shu Po Kwan
1990 June CACM

Wei Huang and Zhenxiao Yang

Overview

- Safety-Critical Software
  - Software that have safety-critical function in applications.
- Evaluation of Safety-Critical Software
  - Software Reviewability
  - Reliability Assessment
  - ...

Software Reviewability

Review --- Document --- Reviewers

- Functional requirement review
  - Requirement document
  - Engineers who understand whole system
- Software structure review
  - Module specification
  - Experienced software engineers
- Internal module review
  - Module design document
  - Experienced software engineers
- Code review
  - Actual code
  - Experienced users of hardware and compilers
- Test plan review
  - Test plan
  - Specialists in software testing

Review relationships between documents
Reliability Assessment

- Finite State Machines
- Hypothesis Testing
  \[ h \text{... reliability} \]
  \[ (1-h)^N = M \text{... no failure probability during testing} \]
  \[ (1-M) \text{... The confidence level we believe h} \]

<table>
<thead>
<tr>
<th>N</th>
<th>( M = (1-h)^N )</th>
</tr>
</thead>
<tbody>
<tr>
<td>500</td>
<td>0.60638</td>
</tr>
<tr>
<td>1000</td>
<td>0.3679</td>
</tr>
<tr>
<td>2000</td>
<td>0.13520</td>
</tr>
<tr>
<td>5000</td>
<td>0.04971</td>
</tr>
<tr>
<td>4000</td>
<td>0.01828</td>
</tr>
<tr>
<td>5000</td>
<td>0.00672</td>
</tr>
</tbody>
</table>

Contributions

- Software reviewability and **structured document**
  - **Hypothesis** statistical **testing** model

First Related Paper

**Predicting Software Reliability**

**From Testing Taking Into Account**

**Other Knowledge About A program**

L. Strigini and A. Bertolino

*QW'96*
Bayesian Inference To Statistical Testing

- Pay attention to evidence other than testing itself.
- Estimate a prior probability.
- T independent tests
- Posterior probability

\[ b_i(\theta) = \frac{P(\theta | \text{Data}_i)P(\text{Data}_i)}{\int P(\theta | \text{Data}_i)P(\text{Data}_i) d\theta} \]

\[ P_{\text{pass}} = P(\text{program has satisfactory failure rate} | \text{program passed } T \text{ tests}) = \frac{1}{b} \]

Bayesian Inference To Statistical Testing (cont’)

- Related to Parnas’ Paper

- Parnas’ hypothesis statistical testing
- Choose test data according to operational profile
- This method does not accept failure
Second Related Paper

Estimating Software Reliability with Hypothesis Testing
Denise M. Wall
1996 Sep CRL Report No. 263

Hypergeometric Model

- $\Theta$ is the error rate we can accept
- $p > \Theta$, we can not accept $p$
- $\beta$ is probability a product being erroneously accepted
  \[
  \beta = \frac{U - (1 - \Theta)^U}{U}
  \]
  \[
  \beta < \frac{U - (1 - \Theta)^U}{U}
  \]

Compared to Parnas’ Binomial Model

- Binomial Model
  - $\beta = (1-p)^n$
  - $\beta < (1-\Theta)^n$

- More precise
  - Example $U=10$, $n=7$
    - $\beta < 0.47$ for binomial model
    - $\beta < 0.3$ for hypergeometric model
Third Related Paper

Applying HyperText Structures to Software Documentation
J.C. French, J.C. Knight and A.L. Powell
1997 Information Processing and Management

SLEUTH
- A vehicle for software documentation management
- Objective
  - Navigate through individual documents
  - Information query
  - Hypertext is the way

Related to Parnas’ Paper
- Document architecture in SLUETH is similar to Parnas’ idea
- Extended Parnas’ paper by providing a software document management tool
Indirectly Related Paper

Software Documents, Their Relationships and Properties
J. Han
APSEC94

Syntax Tree

- Documents, inter- and intra-documentation representation: syntax trees

```
  EnDoc
    /     \
  ProgDoc  Text
    \     / \
  FigDoc  Doc
          /  \
        Prog
```

Similarity to Parnas’ Paper

- Documentation types
  - Requirement document, Specification documents, Design document Implementation documents

- Document structural relation -- Document Consistency in Parnas’ Paper
  - Coarse-grained inter-document relationships
  - Fine-grained inter-document relationships
  - Fine-grained intra-document relationships