Investments in Prevention

- Rules: Security Policy, Procedures
- Tools: Passwords, Firewalls, Encryption
- Awareness, Training, Education
Investments in Response

- Contingency Plans
- Backup Capabilities
- Emergency Drills
Verification

“Are we doing the job right?”

Validation

“Are we doing the right job?”
IEEE Std 1012

IEEE Standard for Software Verification and Validation

foundational component within
IEEE Software Engineering standards series
<table>
<thead>
<tr>
<th>Likelihood</th>
<th>negligible</th>
<th>infrequent</th>
<th>reasonable</th>
</tr>
</thead>
<tbody>
<tr>
<td>consequence</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 1 3 3 1</td>
<td>4 4 4 4 4</td>
<td>4 4 4 4 4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
RISK: “probability that some adverse circumstance will actually occur”

RISK: “any threat to the achievement of one or more key aims of the project”

RISK: “changes in the future that would lead to unacceptable situations”
“Yesterday’s *problems* are today’s *risks*.”

“Today’s *risks* are tomorrow’s *problems*.”
Risk Exposure can be \textit{unacceptable} ... even with \textit{low} probability of occurrence

if \textit{too great a consequence} of occurrence
Risk Management

Risk Exposure =

Likelihood of occurrence \times Consequence of occurrence
Risk Management

Risk Avoidance ➔
reducing probability
of occurrence

Risk Mitigation ➔
reducing consequence
of occurrence
ROI = return investment

RORI = risk exposure reduction reliability investment
Security Risk Exposure =

*Probability* of occurrence

~ frequency of exploitable defects ("vulnerabilities")

X

*Consequence* of occurrence
Security Risk Exposure =

**Probability** of occurrence

(knowledge * skill * resources * motivation)

X

**Consequence** of occurrence
Security Risk Exposure =

\[ \text{Probability of occurrence} \times \text{Consequence of occurrence} \]

Probability of occurrence

(knowledge \times \text{skill} \times \text{resources} \times \text{motivation})

Consequence of occurrence
Risk = \( f \left( \text{threat, vulnerabilities, consequences} \right) \)

Risk Management Parameters

Resilient Military Systems and the Advanced Cyber Threat
Defense Science Board Task Force Report: January 2013
Risk = \( f \left( \text{threat, vulnerabilities, consequences} \right) \)

**Intent** = desire + expectance

**Capabilities** = resources + knowledge
static
assessments

inspections
walkthroughs
audits
reviews
prototyping
simulation
unit testing
integration testing
system testing
acceptance testing
dynamic assessments
3. New reliability measures

3.1 General .................................................................................................................. 4
3.2 Time to next failure (s) (Lyu [B12]) ........................................................................ 4
3.3 Risk factor regression model (Schneidewind [B22]) ................................................. 5
3.4 Remaining failures (Keller and Schneidewind [B11]) .............................................. 6
3.5 Total test time to achieve specified remaining failures (Schneidewind [B20]) ........ 7
3.6 Network reliability (Schneidewind [B19]) ............................................................... 8

4. Modified reliability measures .................................................................................... 10

4.1 Defect density (982 #2) (Fenton and Pfleeger [B5] and Nikora et al. [B17]) .......... 10
4.2 Test coverage index (982 #5) (Binder [B2]) ............................................................ 11
4.3 Requirements compliance (982 #23) (Fischer and Walker [B6]) ............................ 11
4.4 Failure rate (982 #31) (Lyu [B12]) ........................................................................ 12

5. Retained reliability measures ..................................................................................... 13

5.1 Fault density (982 #1) (Musa [B14] and Nikora and Munson [B16]) ....................... 13
5.2 Requirements traceability (982 #7) (Fenton and Pfleeger [B5]) ............................... 15
5.3 Mean time to failure (MTTF) (982 #30) (Lyu [B12] and Musa et al. [B15]) .......... 16
IEEE Std 982.1-2005
IEEE Standard Dictionary of Measures of the Software Aspects of Dependability

Figure B.1—Remaining failures criterion scenario
Figure B.2—Time to Next Failure criterion scenario
# Operational Profile: Distribution of *Uses*

<table>
<thead>
<tr>
<th>Operation</th>
<th>Occurrence probability</th>
<th>Initial test cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter card</td>
<td>.332</td>
<td>66</td>
</tr>
<tr>
<td>Verify PIN</td>
<td>.332</td>
<td>66</td>
</tr>
<tr>
<td>Withdraw checking</td>
<td>.199</td>
<td>40</td>
</tr>
<tr>
<td>Withdraw savings</td>
<td>.066</td>
<td>13</td>
</tr>
<tr>
<td>Deposit checking</td>
<td>.040</td>
<td>8</td>
</tr>
<tr>
<td>Deposit savings</td>
<td>.020</td>
<td>4</td>
</tr>
<tr>
<td>Query status</td>
<td>.00664</td>
<td>1</td>
</tr>
<tr>
<td>Test terminal</td>
<td>.00332</td>
<td>1</td>
</tr>
<tr>
<td>Input to stolen card list</td>
<td>0.00058</td>
<td>0</td>
</tr>
<tr>
<td>Backup files</td>
<td>0.0000023</td>
<td>0</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>1</strong></td>
<td><strong>199</strong></td>
</tr>
</tbody>
</table>
Apply each “classic” tool to software ....

- Check Sheet
- Pareto Diagram
- Units Histogram
- Run Chart
- Scatter Diagram
- Control Chart
- Cause-and-Effect, or Fishbone, Diagram
Apply **checklist/sheet** to software ….

<table>
<thead>
<tr>
<th>Practice/organization</th>
<th>O1</th>
<th>O2</th>
<th>O3</th>
<th>O4</th>
<th>O5</th>
<th>O6</th>
<th>O7</th>
<th>O8</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level 3</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allocated resources</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Assigned responsibilities</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>–</td>
<td>O</td>
</tr>
<tr>
<td>Organizational policy</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>O</td>
</tr>
<tr>
<td>Data collection and use</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Customized material</td>
<td>–</td>
<td>O</td>
<td>O</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Training all</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Defined process</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Code inspections</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Test case inspections</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td><strong>Level 2</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training for leaders</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Design inspections</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Requirement inspections</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Own estimate/average</td>
<td>2.8</td>
<td>2.8</td>
<td>3.3</td>
<td>3</td>
<td>2.7</td>
<td>2</td>
<td>2.5</td>
<td>2</td>
</tr>
</tbody>
</table>

**Sami Kollanus**
Experiences from using ICMM in inspection process assessment
SOFTWARE QUALITY JOURNAL Volume 17, Number 2, 177-187, DOI: 10.1007/s11219-008-9067-2
Apply **Pareto diagram** to software ....

Apply histogram to software ....
Apply **run chart** to software ....

Apply **scatter diagram** to software ....

Apply **control chart** to software ....

Apply **fishbone diagram** to software ....

“NEW” PLANNING / MANAGEMENT TOOLS
Apply **affinity diagram** to software ....

Angélica Caro et al  
A proposal for a set of attributes relevant for Web portal data quality.  
SOFTWARE QUALITY JOURNAL Volume 16, Number 4, 513-542, DOI: 10.1007/s11219-008-9046-7
Apply **relations diagram** to software ....

Apply **tree diagram** to software ....

Jos J. M. Trienekens • Rob J. Kusters • Dennis C. Brussel
Quality specification and metricalization, results from a case-study in a mission-critical software domain
Apply **matrix diagram** to software ....

**Frank Liu et al**

A quantitative approach for setting technical targets based on impact analysis in software quality function deployment (SQFD)


DOI 10.1007/s11219-006-7598-y
Apply **matrix data analysis** to software ....

Jos J. M. Trienekens et al
Entropy based software processes improvement
SOFTWARE QUALITY JOURNAL Volume 17, Number 3, 231-243, DOI: 10.1007/s11219-008-9063-6
Apply **arrow diagram** to software ....

**Kuei-Chen Chiu** et al
Bayesian updating of optimal release time for software systems
SOFTWARE QUALITY JOURNAL Volume 17, Number 1, 99-120, DOI: 10.1007/s11219-008-9060-9
Apply **process decision program chart** to software ....

**Kuei-Chen Chiu** et al
Bayesian updating of optimal release time for software systems
SOFTWARE QUALITY
JOURNAL Volume 17, Number 1, 99-120, DOI: 10.1007/s11219-008-9060-9
<table>
<thead>
<tr>
<th>Time</th>
<th>Session Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>2:30 - 3:30 pm</td>
<td>Resources for the Journey</td>
</tr>
<tr>
<td>3:30 - 4:30 pm</td>
<td>Consolidation and Commitment ... <em>Where to Go From Here</em></td>
</tr>
</tbody>
</table>
stakeholder agreement

operational profiles

reviews

tests

verifiable requirements

fault-tolerant design
IEEE Recommended Practice on Software Reliability

IEEE Reliability Society
Sponsored by the Standards Committee

SOFTWARE RELIABILITY ENGINEERING

More Reliable, Software, Faster and Cheaper

JOHN D. MUSA

SOFTWARE RELIABILITY ENGINEERING

MICHAEL E. LEE, EDITOR
THE RISKS DIGEST
Forum On Risks To The Public In Computers And Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Search RISKS using switches

The RISKS Forum is a moderated digest. Its USENET equivalent is comp.risks

- Vol 26 Issue 10 (Wednesday, 7 August 2012) e Latest Issue
- Vol 26 Issue 05 (Wednesday, 25 July 2012)
- Vol 26 Issue 04 (Tuesday 24 July 2012)

SOFTWARE ENGINEERING ECONOMICS
BARRY W. BOEHM

Balancing Agility and Discipline
A Guide for the Perplexed

Forewords by
Grady Booch, Alastair Cockburn, Arthur E. Pyne

Build Security In
getting a higher return on software assurance
Sponsored by PEC National Cyber Security Division

Navigational Links
Build Security In Home

Build Security In
What is Build Security In?
Build Security In is a collaborative effort that provides practices, tools, guidelines, ideas, principles, and other resources that software developers, architects, and security practitioners can use to build security into software in every phase of its development.
Introduction to Software Security
The Software Assurance Curriculum Project

 Improve Security and Software Assurance: Tackle the CWE Top 25 Most Dangerous Software Errors

The Top 25 CVEs represent the most significant exploitable software defects that have made software so vulnerable. Addressing these will go a long way in securing software, both in development and in operation. Read about the List of Top 25 CWE Most Dangerous Software Errors on the Software Assurance Community Resources and Information Clearinghouse website.
Software Reliability Engineering: More Reliable Software Faster and Cheaper

2nd. Edition

John D. Musa
The CERT\textsuperscript{®} Oracle\textsuperscript{®} Secure Coding Standard for Java\textsuperscript{™}

Fred Long | Dhruv Mohindra | Robert C. Seacord
Dean F. Sutherland | David Svoboda

Secure Coding in C and C++

Robert C. Seacord

Foreword by Richard D. Pakho
CERT Director
Community of Practice → Practical Products

discussion

SMEs
ongoing mentoring

management-sponsored project

on-the-job application

follow-up [virtual] sessions

initial class session
Taz Daughtrey

hdaughtrey@quanterion.com

434 841 5444