Managing Software Risks in Software Intensive Systems with Metrics and Measures

Robert A. Martin
30 January 2003
Discussion Outline

- **Introduction**
  - Managing S/W Quality Issues by Measuring Risks

- **Background**
  - S/W Quality Risks
  - Metrics and Measures

- **Discussion**
  - Components of a SW Risk Management Framework
  - Adapting to Handle OO Specific Risks

- **Summary**
  - Using SW Risk Assessments to Manage
  - Transferring to Industry and Academia
If, To Manage You Must Measure… How Do You Measure an Abstract Concept Like Software Risk?
One Method of Assessing Software Risks
Looking Beyond Errors To Judge The Risks in Software

- Traditionally, most software organizations have focused on:
  - Managing the initial development schedule
  - Managing the development costs
  - Providing desired initial functionality to users
- Maintainability issues are frequently deferred until the product is fielded
- Why should a look at risks focus on the long-term perspective?
  - Software outlives hardware
  - Tightening budgets motivating code re-use efforts
  - Decisions made early in development may mean the difference between updating code and re-engineering it

Historically, eighty cents out of every dollar spent on software goes toward maintenance.
Introduction:
MITRE’s Software Risk Assessment Work

0 Wanted a framework for assessing lifecycle quality issues
0 Desired a flexible methodology for assessing risks in s/w systems
   - Apply to any language, any platform, any architecture, …
   - To be supported by a set of assessment technologies
   - Must be an objective s/w-centric profile of the risks
0 The resultant risk profiles have been used:
   - Selecting contractors based on quality of past efforts
   - Monitoring software quality during development
   - Identifying potential development process changes
   - Guiding future migration decisions
0 MITRE’s framework, methods, and tools have been proven
   - > 100 Systems, ~ 51 million lines of code, >52 languages from a multitude of architectures (UNIX varieties, VMS, MVS, Windows, Macintosh)
   - Systems range from 4K to 6,254K lines of code -- average of 500K
Discussion Outline

0 Introduction
   - Managing S/W Quality Issues by Measuring Risks

0 Background
   - S/W Quality Risks
     - Metrics and Measures

0 Discussion
   - Components of a SW Risk Management Framework
   - Adapting to Handle OO Specific Risks

0 Summary
   - Using SW Risk Assessments to Manage
   - Transferring to Industry and Academia
Software Risks Impact on Quality Are Not Well Defined

- Most will agree they want their systems to be reliable, maintainable, evolvable, portable, open, etc.
- Most people can't agree on what, specifically, reliable, maintainable, evolvable, portable, open, etc. actually mean or how to measure such qualities for an arbitrary body of code.
- Commercial software tools and metrics provide insights into implementations but typically do not provide any sense of higher context for lifecycle issues.

Our definition: A quality system minimizes the risks to the system.
Developers Can Provide Plenty of Complications to a System’s Software Risks

PORTABLE?? OF COURSE IT’S PORTABLE. THE WHOLE THING FITS ON ONE TAPE.
Establishing a Framework for Measuring Risks

- Many areas can help minimize a system’s risks
  - Some are well studied and have full fledged disciplines, technologies, and examination methodologies in place
  - Specifically: requirements traceability, functional completeness, and system testability are well established areas of study
- The other life-cycle risk areas have received less attention but have enormous potential for reducing the levels and types of risk in the systems fielded
- Much to draw from:
  Rome Air Development Center work and others
  - McCall et al. in 1977
  - Bowen et al. in 1984
  - Kitchenham et al.’s ESPRIT REQUEST project, 1987 & 1989…
There Are Several Frameworks for Evaluating and Monitoring S/W Quality Risks

- RADC-McCall et al 1977
- RADC-Bowen et al 1984
- Rome Laboratory Software Quality Framework
- ESPRIT REQUEST Kitchenham et al 1987
- ESPRIT REQUEST Kitchenham et al 1989
- Dromey 1992-1995
- Rome Laboratory -- SQT2 -- Software Quality Technology Transfer Consortium QUES
- AFOTEC Software Assessment Team Pamphlets
- USAF SSG SEP code review

Computer Technology
- Processing Power
- Memory Sizes
- Disk Sizes

Assessment Technology
Discussion Outline

0 Introduction
   - Managing S/W Quality Issues by Measuring Risks
0 Background
   - S/W Quality Risks
   - Metrics and Measures
0 Discussion
   - Components of a SW Risk Management Framework
   - Adapting to Handle OO Specific Risks
0 Summary
   - Using SW Risk Assessments to Manage
   - Transferring to Industry and Academia
Targeted Attributes Of Our S/W Quality Risk Assessment Methodology

The assessment should be:
- repeatable (independent of the assessor(s))
- independent of language, architecture, platform
- “cheap” to perform
- not dependent on presence of “all” code
- provide detailed insight into the software risks
- software centric
- based on artifacts only
- examine all artifacts of the system
  = source code (including scripts, data, …)
  = supporting documentation (both internal and external to the code) and standards
- leverage automation where-ever possible
Guiding Principles: Breadth, Depth, and Repeatability

- The evaluation of each quality issue should have a specific scope and context as well as a defined scoring criteria.
- Define context for ratings (ideal, good, marginal, and fail)
  - limiting choices increases repeatability
- Use a mixture of:
  - Hard metrics (cyclomatic complexity, flow complexity, …)
  - Objective measures (type of information available, existence
  - Subjective measures (use of white space, usefulness
- The Metrics and Objective Measures attributes can have a scope of all of the code of the system
- The Measures which require cognitive reasoning need to be scoped more narrowly (7/7/7 per language)
- Provide a software tools framework to guide and assist evaluators & provide context and control of the process
Discussion Outline

0 Introduction
   - Managing S/W Quality Issues by Measuring Risks
0 Background
   - S/W Quality Risks
   - Metrics and Measures
0 Discussion
   - Components of a SW Risk Management Framework
   - Adapting to Handle OO Specific Risks
0 Summary
   - Using SW Risk Assessments to Manage
   - Transferring to Industry and Academia
Bridging the Gap between The Measurable and Unmeasurable

Software Quality Analysis Frameworks

Maintainability
Evolvability
Portability
Descriptiveness

Quality Concepts

Complexity Set-Use SLOC Count API Utilization Coding Standards

Metrics & Measures

MITRE
S/W Quality Risk Frameworks: Scope and Focus Can Differ

**Boehm et. al. RADC Original Quality Factors 1977**

- Measurable Property
  - device independence
  - completeness
  - accuracy
  - device efficiency
  - accessibility
  - human engineering
  - communicativeness
  - self-descriptiveness
  - maintainability

- Perceived Aspect of Quality
  - portability
  - reliability
  - efficiency
  - human engineering
  - testability
  - understandability
  - modifiability

**McCall et. al. RADC Modified Quality Model 1984**

- Measurable Property
  - testability
  - completeness
  - consistency
  - accuracy
  - error tolerance
  - execution efficiency
  - storage efficiency
  - access control
  - access audit
  - operability
  - training
  - communicativeness
  - simplicity
  - self-descriptiveness

- Perceived Aspect of Quality
  - correctness
  - reliability
  - efficiency
  - integrity
  - testability
  - usability
  - maintainability
  - simplicity
  - consistency
  - testability
  - maintainability
  - modularity

**MITRE SQAE™ Quality Factors 1992 2003**

- Measurable Property
  - independence
  - consistency
  - design simplicity
  - documentation
  - modularity
  - anomaly control
  - self-descriptiveness

- Perceived Aspect of Quality
  - maintainability
  - evolvability
  - descriptiveness
  - portability

**AFOTEC Supportability Assessment Factors 1991 1996**

- Measurable Property
  - discriptiveness
  - executability
  - organization
  - simplicity
  - modularity
  - consistency
  - testability
  - expandability
  - convention

- Perceived Aspect of Quality
  - maintainability

- requirements issues
- testing issues
Test & Requirements Issues are Addressed - So We Focused on S/W Attribute Issues

MITRE SQAE™
Quality Factors

1992 - 2003

Measurable Property

- independence
- consistency
- design simplicity
- documentation
- modularity
- anomaly control
- self-descriptiveness

Perceived Aspect of Quality

- maintainability
- evolvability
- descriptiveness
- portability

MITRE SQAETM - software attributes

1991 - 1996

- software attributes

1977

Boehm et. al. RADC

Original Quality Factors

1984

McCall et. al. RADC

Modified Quality Model

1992

MITRE SQAE™
Quality Factors

1992 - 2003
Methodology and Process: The Software Quality Assessment Exercise (SQAE™)

Approach: Assess the level of risk in the Quality Areas by examining the underlying attributes of the code and documentation.

Components of the Software Quality Areas

- Portability
- Evolvability
- Maintainability
- Descriptiveness
- Independence
- Anomaly Control
- Design Simplicity
- Self-Descriptiveness
- Documentation
- Consistency
- Modularity

Quality Risk Profile: Risk Mitigators

- Coding Standards
- Software Development Plan
- Design Documents
- Detailed Design
- Source Code

Quality Risk Profile: Risk Drivers

- Source Code and Listings
- Specific Questions about the Code and Documentation

Approach: Assess the level of risk in the Quality Areas by examining the underlying attributes of the code and documentation.
Putting the Pieces Together

Maintainability

- Design
- Simplicity
- Consistency
- Modularity
- Self-Descriptiveness
- Anomaly Control
- Documentation

Evolvability

- Self-Descriptiveness
- Design
- Simplicity
- Modularity
- Anomaly Control
- Documentation

Portability

- Modularity
- Independence
- Self-Descriptiveness
- Documentation

“Documentation”

- Documentation
- Self-Descriptiveness

“Modularity”

- Modularity
Details: SQAE™ Areas and Factors

0 Assess software against a defined set of quality areas:
   - Portability
   - Evolvability
   - Maintainability
   - Descriptiveness

0 Quality areas are based on a set of seven components:
   - Consistency (15 attributes)
   - Independence (8 attributes)
   - Modularity (10 attributes)
   - Documentation (16 attributes)
   - Self Descriptiveness (11 attributes)
   - Anomaly Control (5 attributes)
   - Design Simplicity (11 attributes)
## Details of the SQAE™
### Quality Component Assessment Questions

#### Independence

Independence comprises two broad groups; software system independence and machine independence. Here the issue is to not tie the system to any specific host environment which would make it difficult or impossible to migrate, evolve, or enhance the system.

<table>
<thead>
<tr>
<th>Software System Independence</th>
<th>Factor Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1 - Does the software avoid all usage of specific pathnames/filenames?</td>
<td>(100)</td>
</tr>
<tr>
<td>2.2 - Is the software free of machine, OS and vendor specific extensions?</td>
<td>(200)</td>
</tr>
<tr>
<td>2.3 - Are system dependent functions, etc., in stand-alone modules (not embedded in the code)?</td>
<td>(200)</td>
</tr>
<tr>
<td>2.4 - Are the languages and interface libraries selected standardized and portable? (i.e., ANSI...)</td>
<td>(200)</td>
</tr>
<tr>
<td>2.5 - Does the software avoid the need for any unique compilation in order to run (e.g., a custom post processor to “tweak” the code to run on machine X)?</td>
<td>(100)</td>
</tr>
<tr>
<td>2.6 - Is the generated code (i.e., GUI Builders) able to run without a specific support runtime component?</td>
<td>(100)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Machine Independence</th>
<th>Factor Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.7 - Is the data representation machine independent?</td>
<td>(200)</td>
</tr>
<tr>
<td>2.8 - Are the commercial software components available on other platforms in the same level of functionality?</td>
<td>(200)</td>
</tr>
</tbody>
</table>

#### Modularity

Modularity consists of several facets which each support the concepts of organized separation of functions and minimizes un-noticed couplings between portions of the system.

<table>
<thead>
<tr>
<th>Modularity</th>
<th>Factor Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1 - Is the structure of the design hierarchical in a top-down design within tasking threads?</td>
<td>(200)</td>
</tr>
<tr>
<td>3.2 - Do the functional groupings of units avoid calling units outside their functional area?</td>
<td>(150)</td>
</tr>
<tr>
<td>3.3 - Are machine dependent and I/O functions isolated and encapsulated?</td>
<td>(150)</td>
</tr>
<tr>
<td>3.4 - Are interpreted code bodies (shell scripts and 4GL scripts) protected from accidental or deliberate modification?</td>
<td>(150)</td>
</tr>
<tr>
<td>3.5 - Do all functional procedures represent one function (one-to-one function mapping)?</td>
<td>(150)</td>
</tr>
<tr>
<td>3.6 - Are all commercial software interfaces &amp; APIs, other than GUI Builders, isolated and encapsulated?</td>
<td>(200)</td>
</tr>
<tr>
<td>3.7 - Have symbolic constants been used in place of explicit ones?</td>
<td>(150)</td>
</tr>
<tr>
<td>3.8 - Are symbolic constants defined in an isolated and centralized area?</td>
<td>(100)</td>
</tr>
<tr>
<td>3.9 - Are all variables used exclusively for their declared purposes?</td>
<td>(150)</td>
</tr>
<tr>
<td>3.10 - Has the code been structured to minimize coupling to global variables?</td>
<td>(100)</td>
</tr>
</tbody>
</table>
Examples of Tools Used in Assessing Software Quality Risks

... many tools do not adequately address the use of commercial packages, or easily deal with multi-language applications, or help you correctly interpret their metrics.
# Details of the SQAE™ Framework

**Exercise A** The first exercise area concentrates on those activities that can be accomplished by examining the two largest functional areas of the code. The activities in this exercise are listed below.

<table>
<thead>
<tr>
<th>Exercise</th>
<th>Description</th>
<th>Rating Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.10</td>
<td>Are the naming conventions consistent for functional groupings?</td>
<td>Examine the scheduling modules and one other large functional grouping and cross reference between them. Rating will be either Ideal, Good, Marginal, or Failing. If at least one of the programmers is either consistent or uses distinguishable naming conventions (marginal), if he/she uses both (good), if all programmers do both (ideal).</td>
</tr>
<tr>
<td>2.2</td>
<td>Is the software free of machine, OS and vendor specific extensions?</td>
<td>Examine two large functional groupings of code and cross reference between them and system libraries and known vendor extensions. Rating will be either Ideal, Good, Marginal, or Failing. Score ideal if no instances occur, good if such assumptions affect less than 10% of the packages, marginal for less than 50%, else failing.</td>
</tr>
<tr>
<td>2.3</td>
<td>Are system dependent functions, etc., in stand-alone modules (not embedded in the code)?</td>
<td>Examine all known instantiations OS and vendor specific dependencies for encapsulation/isolation. Rating will be between 1 and 0, where 1 is the higher rating. 1 - (number of embedded dependencies/total number of dependencies)</td>
</tr>
</tbody>
</table>
The Core of the Software Quality Assessment Methodology

Step 1: Identify risks to be evaluated.

Step 2: Determine what is needed to evaluate the risk.

Step 3: Determine whether the needed items are available; if items are not obtainable then discard that risk from the scope of the assessment.

Step 4: Determine how the items will be examined to determine the risk information.

Step 5: Determine how the risk information can be used to definitively identify risky versus mitigant items in the artifacts.

Id potential risk items

Id needed artifacts

Keep if artifacts available

Count, find, search, match?

Definitive: Risk Driver vs. Risk Mitigant
Discussion Outline

0 Introduction
  - Managing S/W Quality Issues by Measuring Risks

0 Background
  - S/W Quality Risks
  - Metrics and Measures

0 Discussion
  - Components of a SW Risk Management Framework
  - Adapting to Handle OO Specific Risks

0 Summary
  - Using SW Risk Assessments to Manage
  - Transferring to Industry and Academia
# Modifications to the SQAE™ to Deal with Object Oriented Design and Development (1 of 2)

**Exercise A** - The first exercise area concentrates on those activities that can be accomplished by examining two large functional areas of the code. The activities in this exercise are listed below.

<table>
<thead>
<tr>
<th></th>
<th>For non-OO design/implementations</th>
<th>For OO design/implementations</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>Is the structure of the design hierarchical in a top-down design within tasking threads? Has the code been structured into cohesive classes? <strong>LOCM</strong> Lack of Cohesion in Methods</td>
<td>Using the two large functional areas of the code from 1.10, run McCabe BattleMap, Refine, or another tool to produce structure chart. Examine. Rating will be between 1 and 0, where 1 is the higher rating. 1 for crisp hierarchy, .6 for discernible hierarchy, 0 if neither.</td>
</tr>
<tr>
<td>3.2</td>
<td>Do the functional groupings of units avoid calling units outside their functional area? Has code been structured into classes to avoid excessive coupling between classes? <strong>CBO</strong> Coupling Between Objects</td>
<td>Ignoring utility and encapsulated service calls, examine the structure chart from 3.1. Rating will be between 1 and 0, where 1 is the higher rating. 1 for strong isolation, .6 for generally isolated, 0 if neither.</td>
</tr>
<tr>
<td>3.10</td>
<td>Has code been structured to minimize coupling to global variables? Have classes been structured into methods to avoid having a large number of methods being invoked for each input message to a class object? <strong>RFC</strong> Response For a Class</td>
<td>Examine the modules from 1.10, using a variable utilization map (such as a Set-Use diagram) and calculate the ratio of global variables used versus the total number of variables used for each procedure. Rating will be between 1 and 0, where 1 is the higher rating. 1 - 20 * the average ratio of global variables to total variables.</td>
</tr>
</tbody>
</table>
Exercise F - The sixth exercise area activities look over all of the code loaded for a variety of tasks. The activities in this exercise are listed below.

7.2 Is the source code of low complexity (e.g., McCabe Cyclomatic…)?

Using the available source code, calculate the Cyclomatic complexity.
Rating will be between 1 and 0, where 1 is the higher rating. Calculate the average Cyclomatic complexities and standard deviation for all functions and procedures. Score will be 1 - \( \frac{\text{average + s.d.} - 15}{0.02} \).

For non-OO design/implementations
For OO design/implementations

7.7 Is the code segmented into procedure bodies that can be understood easily?

Using the available source code, examine the code.
Rating will be between 1 and 0, where 1 is the higher rating. 1 for all procedure bodies are less than two pages @ 50 lines per page, .8 for 80% are less than two pages, .5 for 50% are less than two pages, and 0 otherwise.

For non-OO design/implementations
For OO design/implementations

7.9 Have all procedures been structured to avoid excessive nesting?

Using the available source code, calculate the average and standard deviation of the nesting levels.
Rating will be between 1 and 0, where 1 is the higher rating. Score will be the ratio of 13 / \( \frac{\text{average squared + one sigma squared}}{0.02} \) with a maximum score of 1.

For non-OO design/implementations
For OO design/implementations

Using the available code, examine the methods of each class and calculate the sum of the Cyclomatic complexities for each method in a class. Calculate the average and standard deviation of the class complexities.
Rating will be between 1 and 0, where 1 is the higher rating. Score will be 1 - \( \frac{\text{average + s.d.} - 15}{0.02} \).

For non-OO design/implementations
For OO design/implementations

Are the classes of low complexity?

Using the available code, count the number of direct sub-classes for each class.
Rating will be between 1 and 0, where 1 is the higher rating. Score will be 1 - 20 * the average ratio of classes to the direct sub-classes.

For non-OO design/implementations
For OO design/implementations

Using the available code, calculate the length of the longest path of inheritance to each module. Calculate the average and standard deviation of the inheritance lengths.
Rating will be between 1 and 0, where 1 is the higher rating. Score will be 1 - \( \frac{\text{average + s.d.} - 15}{0.02} \).

For non-OO design/implementations
For OO design/implementations

Has code been organized into classes and sub-classes that can be understood easily?

Using the available code, calculate the Weighted Methods Per Class (WMC), Number of Children (NOC), and Depth of Inheritance Tree of a Class (DIT) for each class.

For non-OO design/implementations
For OO design/implementations
Discussion Outline

0 Introduction
  - Managing S/W Quality Issues by Measuring Risks
0 Background
  - S/W Quality Risks
  - Metrics and Measures
0 Discussion
  - Components of a SW Risk Management Framework
  - Adapting to Handle OO Specific Risks
0 Summary
  - Using SW Risk Assessments to Manage
  - Transferring to Industry and Academia
Having An Understanding Software Quality Risks Can Be Used In...

**The Selection of Contractors**

**Reviews of SI/W Releases for a Project Office**

**Selection of Migration Systems**
Software Quality Assessment Uses

Understanding the Software’s quality can:
- Allow for evaluation of a contractor based on quality of past products
- Allow for in-progress corrections to a development effort
- Guide future migration decisions
- Provide for the rapid identification of the sources of risk
  = in understandable & actionable terms for mgmt
  = in fine detail for the technologists
- Provide a broad review of the software lifecycle risks associated with multi-component systems
- Allow risk comparisons for systems independent of language, platform, architecture, …
- Guide the build, buy, or re-use decisions
Reporting the Results of a Software Quality Risk Assessment Exercise

Both a Software Quality Risk Assessment Report and (if desired) a Briefing version are available.
# SQAE™ Foundation

<table>
<thead>
<tr>
<th>Project A</th>
<th>Project B</th>
<th>...</th>
<th>Project CZ</th>
<th>Total of Projects</th>
</tr>
</thead>
<tbody>
<tr>
<td>112,000 LOC</td>
<td>558,000 LOC</td>
<td>58,000 LOC</td>
<td>51,173,315 LOC</td>
<td></td>
</tr>
<tr>
<td>Ada, C, Shell, TAE+, SQL, X, MOTIF, Stored Procedures</td>
<td>C, Shell, X, MOTIF</td>
<td>Ada, C, ELF, ezX, SQL, X, MOTIF</td>
<td>Ada, C, FORTRAN, COBOL, shell, TAE+, SQL, X, MOTIF, UIL, Stored Procedures, GEL, ELF, ezX, ...</td>
<td></td>
</tr>
<tr>
<td>Top Level Design Doc</td>
<td>SDD</td>
<td>SPS</td>
<td>Top Level Design Doc</td>
<td>Top Level Design Doc</td>
</tr>
<tr>
<td>SDD</td>
<td>SDP</td>
<td>SDD</td>
<td>SDP</td>
<td>SPS</td>
</tr>
<tr>
<td>Product Literature</td>
<td>Design and Code Stnds</td>
<td>Product Literature</td>
<td>Product Literature</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Design and Code Stnds</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This Chart Contains Representative Assessment Results
### SQAE™ Finding Examples:
#### Mitigators, Drivers, & Other Observations

<table>
<thead>
<tr>
<th>Risk Mitigators</th>
<th>Risk Drivers</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 Naming conventions used for modules and variables helps understand the code’s functionality.</td>
<td>0 Level of isolation and encapsulation of dependencies on platform and COTS packages varies between programmers</td>
</tr>
<tr>
<td>0 Good use of white space and indentation.</td>
<td>0 Use of environmental variables is undocumented and inconsistently done</td>
</tr>
<tr>
<td>0 Modules are easily viewed at once (&lt; 100 LOC)</td>
<td>0 Lack of written standards for naming conventions, error handling, data definitions, etc</td>
</tr>
<tr>
<td>0 Good functional documentation with high-level design.</td>
<td>0 Lack of standards for naming conventions, error handling data definitions, I/O, etc</td>
</tr>
<tr>
<td>0 Good design documentation, showing data and control flows.</td>
<td>0 Design documentation is poorly organized, incomplete, and at a very high level</td>
</tr>
<tr>
<td>0 Good developer documentation for supported APIs.</td>
<td>0 No low-level design information or functional allocation of software in documentation</td>
</tr>
<tr>
<td>0 Good top-down hierarchical structure to code.</td>
<td>0 Machine generated code documentation is inconsistent with the developed code documentation</td>
</tr>
<tr>
<td>0 Modules use straightforward algorithms in a linear fashion.</td>
<td>0 Machine generated code is undocumented</td>
</tr>
<tr>
<td>0 System dependencies are to readily available COTS software.</td>
<td>0 Procedure and file names depend on path for uniqueness</td>
</tr>
<tr>
<td>0 Code is of low complexity.</td>
<td>0 Hard coded absolute filenames/paths used</td>
</tr>
<tr>
<td>0 Logic flow through individual procedures is easy to follow.</td>
<td>0 UNIX commands hardcoded in the code</td>
</tr>
<tr>
<td>0 Disciplined coding standards followed by the programmers.</td>
<td>0 Hard coded variables used when symbolic constants should have been used</td>
</tr>
<tr>
<td>0 Considerable effort made to use POSIX calls throughout.</td>
<td>0 There are some machine dependent data representations</td>
</tr>
<tr>
<td>0 System dependencies platform or COTS are encapsulated.</td>
<td>0 Code is not ANSI standard</td>
</tr>
<tr>
<td></td>
<td>0 Variables used for other than their declared purpose</td>
</tr>
<tr>
<td></td>
<td>0 No low-level control and task flows in documentation</td>
</tr>
<tr>
<td></td>
<td>0 No prologs for the majority of the modules</td>
</tr>
<tr>
<td></td>
<td>0 Inadequate indexing of documentation</td>
</tr>
<tr>
<td></td>
<td>0 Excessive use of global variables</td>
</tr>
<tr>
<td></td>
<td>0 Input error checking is not consistently applied</td>
</tr>
<tr>
<td></td>
<td>0 System dependent on a proprietary language for some functions related to integration with COTS</td>
</tr>
<tr>
<td></td>
<td>0 Lack of consistency in the code between programmers</td>
</tr>
<tr>
<td></td>
<td>0 No isolation or encapsulation of dependencies on platform or COTS</td>
</tr>
<tr>
<td></td>
<td>0 System tied to a proprietary language for procedural processing and data access</td>
</tr>
<tr>
<td></td>
<td>0 System is dependent on a proprietary run-time environment</td>
</tr>
<tr>
<td></td>
<td>0 Fourteen violations of one of the few company coding standards</td>
</tr>
<tr>
<td></td>
<td>0 Two percent of the code modules are overly large, more than 100 LOC</td>
</tr>
</tbody>
</table>

### Other Observations

<table>
<thead>
<tr>
<th>Other Observations</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 No documented method for other languages to call services</td>
</tr>
<tr>
<td>0 “Man pages” are out of date for some APIs</td>
</tr>
<tr>
<td>0 Number of modules may be excessive</td>
</tr>
<tr>
<td>0 COTS screen description files use standard X-Windows resource file formats</td>
</tr>
<tr>
<td>0 Proprietary language does not support data typing</td>
</tr>
<tr>
<td>0 In the vendor’s proprietary language, variables are never explicitly declared</td>
</tr>
<tr>
<td>0 SQL is only used for ~10% of the code that accesses the database</td>
</tr>
<tr>
<td>0 Complete source code for gnu Perl was included as part of deliverable subsystem source code</td>
</tr>
</tbody>
</table>

---

This Chart Contains Representative Assessment Results
Examples of Feedback

Application’s Primary Strengths: Integrator Perspective

- Isolation of dependencies
  - Effort has been made to segregate code so that actual processing algorithms are buffered from platform and COTS dependencies.
  - This buffering lowers the system’s sensitivity to changes in its operating environment.
  - Should the platform change significantly (New OS, new COTS Database, etc) code rewrites and unit tests should be restricted to distinct areas rather than rippling throughout.

Application’s Primary Weaknesses: Integrator Perspective

- Descriptiveness
  - The provided documentation addresses aspects of the system only at the highest level and does not detail essential low level information:
    - System dependencies
    - Knowledge domains required for maintenance
    - Input data tolerance and valid range of value definitions
    - Specific data flow descriptions
    - Policies for error handling
  - The code itself is poorly documented internally and makes frequent use of programming constructs which hinder readability and traceability
Sample Assessment Results for Multiple Developers

Maintainability  Evolvability  Portability  Descriptiveness

Quality Area Risk Profiles

Software Quality Factor Risk Profiles

Consistency  Independence  Modularity

Documentation  Self-Descriptiveness  Anomaly Control  Design Simplicity

Key
Data Series 1 = Reference
Data Series 2 = Prj 1 Vndr A
Data Series 3 = Prj 2 Vndr A
Data Series 4 = Prj 1 Vndr B
Data Series 5 = Prj 2 Vndr B
Data Series 6 = Prj 1 Vndr C
Data Series 7 = Prj 2 Vndr C
Data Series 8 = Mean & Range of 40 Systems
Examples of Software Quality Risk Profiles (3D)
Summary:
The Value of the SQAE™

- Easy to learn and apply for experienced developers
- Can provide an independent, objective assessment with community norms of key metrics for comparison of a project with the practices of its peers.
- Follows a repeatable process
- Provides specific detail findings
- Minimal effort to accomplish (5 - 6 staff weeks per system)
  - How large the application is, the number of different languages used, and the type of assessment desired
  - A small level of additional effort is needed when we run into a language we have not previously encountered
- Framework for comparing and contrasting systems
- Provides mechanism for obtaining a “past performance” measure of contractors
- Brings out lifecycle concerns and issues
- Proven ability to adapt to technology changes and the changes in software development methodologies
Summary: The Value of a SQAE™ (Concluded)

- Can be used as a pro-active framework for stating quality reqt’s
  - Many quality measures are easily restated as req’ts for coding & design stds
  - Can use as part of an award fee determination
  - SOW words to ensure Government has access to code and doc’s

- A variety of Government customers have been interested in the continued application of our work
  - Augmentation of the SEI SCE to look at product as well as process
  - Supports Air Force “supportability assessment” task
  - Helping compare and contrast legacy systems

- Assessments have been consistent with “other” opinions including the developer’s

- Can track assessed contractors through project milestones
  - Comparing risk drivers and risk mitigators experienced vs. Software Quality Assessment risk profile
Discussion Outline

0 Introduction
   - Managing S/W Quality Issues by Measuring Risks
0 Background
   - S/W Quality Risks
   - Metrics and Measures
0 Discussion
   - Components of a SW Risk Management Framework
   - Adapting to Handle OO Specific Risks
0 Summary
   - Using SW Risk Assessments to Manage
   - Transferring to Industry and Academia
Direct and Indirect Technology Transfers of SQAE™ Methods and Tools

SQAE™ Licensees:
- 1996 - Mitretek
- 1997 - Lockheed Martin
- 1998 - General Dynamics Info. Systems
- 2001 - Ecole de technologie superieure

Organizations Who’s SW was Assessed:

IEEE CS May 1994
Managing Software Quality May 1996
STSC April 1995
SEI/SEPG July 1996
INCOSCE July 1996
STSC April 1998
STSC May 2002
STSC May 2003

1998/1999

ISO 9126-1
Languages from Product Assessments By Percentage of Assessed LOC

100 Systems with approximately 51 Million Lines of Code Assessed
SQAE™ Experience-Base
?'s

CONTACT INFO:
Robert A. Martin
781-271-3001
ramartin@mitre.org
Why Are We Interested In S/W Risk Anyway?

Software Quality Teams must do more than remove errors!

MITRE
So, the SQAE is Only One Example of the Risk Assessments that use Metrics and Measures
Metadata and Data Handling
Quality Factors

Quality of Metadata and Data Handling
- Maintainability
- Evolvability
- Portability
- Descriptiveness

Consistency
- LDM-PDM Congruence
- Standardized Data Access
- Standardized Data Transfer

Independence
- Standards Use
- OS/Machine Dependencies
- Platform Availability
- Run-time Issues
- 3rd Party Tools

Design Simplicity
- Schema
- Customizations
- Data Model
- Exclusive Naming
- Performance Mgmt

Anomaly Control
- Data Integrity
- Transaction Control
- Consistent Error Hndlg
- Concurrency Mgmt
- Recovery

Modularity
- GUI Code
- Encapsulation
- GUI Code Isolation

Documentation
- Data Dictionary
- 4GL Use
- Design
- I/O Handling
- Data Flow

Self-Descriptiveness
- 4 GL Design Tools
- DBMS Design Tools

Standards Use
- OS/Machine Dependencies
- Platform Availability
- Run-time Issues
- 3rd Party Tools

Schema
- Customizations
- Data Model
- Exclusive Naming
- Performance Mgmt

Data Integrity
- Transaction Control
- Consistent Error Handling
- Concurrency Management
- Recovery

GUI Code
- Encapsulation
- GUI Code Isolation

OS/Machine Dependencies
- Platform Availability
- Run-time Issues
- 3rd Party Tools

Standards Use
- 4GL Use
- Design
- I/O Handling
- Data Flow
A “Design Review-time” View of the SQAE

**Coding Standards, Software Development Plan, Design Documents, etc.**

**A-SPEC**

**SDP**

**Detailed Design**

**SQAE Quality Factors**

- Independence
- Design Simplicity
- Modularity
- Consistency
- Anomaly Control
- Documentation
- Self Descriptiveness

MITRE
Augmented SCE:
Implementation Schedule/Activities

Summary
Initial Planning, Detailed Preparation Work, IFPP Material Development:
Assessment Activities per contractor (Process team visits cover 3 projects, Product team evaluates 2 of those 3 projects):
Report Generation and Briefing Creation/Delivery
- Initial Planning, Detailed Preparation Work, IFPP Material Development: 4 staff weeks
- Assessment Activities per contractor: 7 staff weeks per contractor
- Report Generation and Briefing Creation/Delivery: 10 staff weeks

Key:
- Initial Planning
- Detailed Preparation Work
- IFPP Material Development
- Review Submittals/Plan Sch.
- Process Assessment
- Proposal Material Review
- General Information Feed
- Visit Preparation/Tailoring
- Visit Findings Capture
- Develop Report
- Products to Customer

MITRE