The Global State of Structural Quality in Business Applications

Dr. Bill Curtis
Sr. VP & Chief Scientist, CAST Software
Director, Consortium for IT Software Quality (CISQ)

CEE–SEC(R)
November 1, 2012
Bad Structural Quality Is Expensive

Knight Capital Says Trading Glitch Cost It $440 Million

London Stock Exchange crippled by online banking outage

Citi Discloses Security Flaw in Its iPhone App

RBS to pay out £125m over computer glitch

BlackBerry Suffers Outage in Europe
“As higher levels of assurance are demanded…testing cannot deliver the level of confidence required at a reasonable cost.”

“The correctness of the code is rarely the weakest link.”

“…a failure to satisfy a non-functional requirement can be critical, even catastrophic…non-functional requirements are sometimes difficult to verify. We cannot write a test case to verify a system’s reliability…The ability to associate code to non-functional properties can be a powerful weapon in a software engineer’s arsenal.”
Software Quality Iceberg

Source: Code Complete, Steve McConnell
3 Levels of Structural Quality Analysis

1. **Unit Level**
   - Code style & layout
   - Expression complexity
   - Code documentation
   - Class or program design
   - Basic coding standards
   - Developer level

2. **Technology Level**
   - Single language/technology layer
   - Intra-technology architecture
   - Intra-layer dependencies
   - Inter-program invocation
   - Security vulnerabilities
   - Development team level

3. **System Level**
   - Integration quality
   - Architectural compliance
   - Risk propagation
   - Application security
   - Resiliency checks
   - Transaction integrity
   - Function point
   - Effort estimation
   - Data access control
   - SDK versioning
   - Calibration across technologies
   - IT organization level
Software Engineering’s 4th Wave

1. Languages
   - What: 3rd & 4th generation languages, structured programming
   - When: 1965-1980
   - Why: Give developers greater power for expressing and understanding their programs

2. Methods
   - What: Design methods, CASE tools
   - When: 1980-1990
   - Why: Give developers better methods and tools for constructing software systems

3. Process
   - What: CMM/CMMI, ITIL, PMBOK, Agile
   - When: 1990-2002
   - Why: Provide a more disciplined environment for professional work using best practices

4. Product
   - What: Architecture, Structural Quality, Reuse
   - When: 2002
   - Why: Ensure software is constructed to standards that meet its lifetime demands
Architecturally Complex Defects

A structural flaw involving interactions among multiple components that reside in different application layers

80% of architecturally complex defects touch an Architectural Hotspot—a badly designed component causing problems

Architectural hotspots provide a roadmap for remediating the worst risk, rework, and cost drivers
System Level analysis allows detection architectural hotspots
CAST’s Application Intelligence Platform

Language Parsers
- Oracle PL/SQL
- Sybase T-SQL
- SQL Server T-SQL
- IBM SQL/PSM
- C, C++, C#
- Pro C
- Cobol
- CICS
- Visual Basic
- VB.Net
- ASP.Net
- Java, J2EE
- JSP
- XML
- HTML
- Javascript
- VBScript
- PHP
- PowerBuilder
- Oracle Forms
- PeopleSoft
- SAP ABAP, Netweaver
- Tibco
- Business Objects
- Universal Analyzer for other languages

Application Analysis
Evaluation of 1200+ coding & architectural rules

Application meta-data

Detected Violations
- Expensive operation in loop
- Static vs. pooled connections
- Complex query on big table
- Large indices on big table
- Empty CATCH block
- Uncontrolled data access
- Poor memory management
- Opened resource not closed
- SQL injection
- Cross-site scripting
- Buffer overflow
- Uncontrolled format string
- Unstructured code
- Misuse of inheritance
- Lack of comments
- Violated naming convention
- Highly coupled component
- Duplicated code
- Index modified in loop
- High cyclomatic complexity

Quality Measurements
- Performance
- Robustness
- Security
- Transferability
- Changeability
Appmarq Structural Quality Repository

- CAST’s repository of structural quality data
  - 745 Applications
  - 160 Companies, 14 Countries
  - 321,259,160 Lines of Code; 59,511,706 Violations
Structural Quality Unrelated to Size

$r = .02$

$r^2 = .00$
...Except for COBOL

\[ r = -0.33 \]
\[ r^2 = 0.11 \]
Security Scores by Language
Performance Scores by Language
Changeability Scores by Method
No Differences by Source or Shore

SOURCE

SHORE
Structural Analysis Reduces Risks/Costs

TELECOM CLIENT STUDY OVER 24 MONTHS

Before structural analysis at the System Level

System test defects

New critical violations

Initiation of System Level structural analysis

Order Management
Inventory Management
Billing
Customer Service

Code
No RC
Non Code
Projected Count

Trend line

Bill Curtis 121101
Recent CISQ Events

OMG Architecture Board approved the Automated Function Point spec for a 3-month public review leading to final approval at the Dec. OMG meeting.

On 9/12 CISQ released specifications for automated measures of Reliability, Performance Efficiency, Security, and Maintainability.
Global Trends

- Reducing operational risk is valued over reducing cost of ownership
- Code produced with Agile methods could have higher cost of ownership
- Sourcing and shoring choices do not affect structural quality
- Structural quality measures are being used as Service Level Agreements in contracts

But......

- STRUCTURAL QUALITY MUST IMPROVE