

## 9 Digit Stakes... ...and the Measurement Stack

Dr. Bill Curtis  
SVP and Chief Scientist, CAST Research Labs  
Director, Consortium for IT Software Quality

### Bill's December 2011 Trip

**OWASP Top 10 – 2013 Edition**

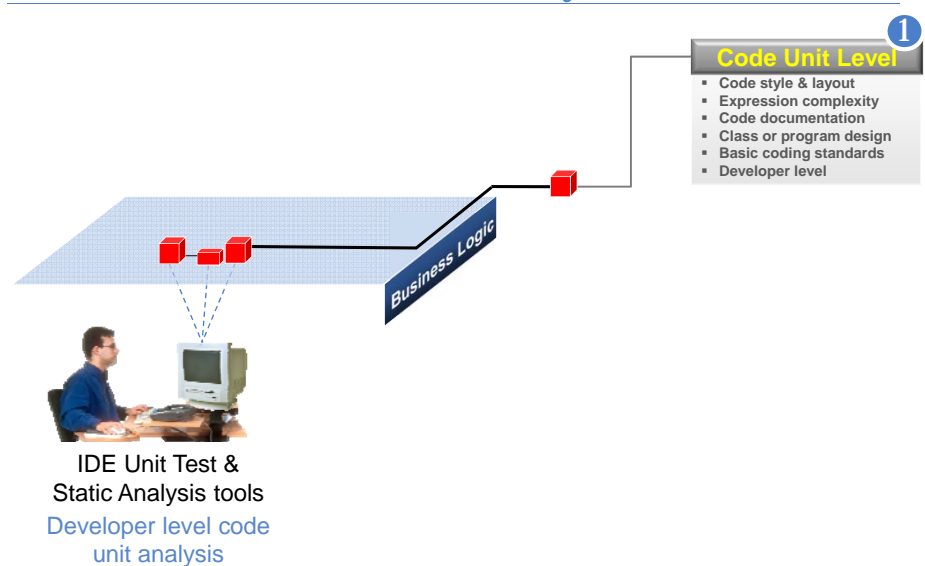
- A1 Injection
- A2 Broken Authentication and Session Management
- A3 Cross-Site Scripting (XSS)
- A4 Insecure Direct Object References
- A5 Security Misconfiguration
- A6 Sensitive Data Exposure
- A7 Missing Function Level Access Control
- A8 Cross-Site Request Forgery (CSRF)
- A9 Using Known Vulnerable Components – New (prev Misconfiguration")
- A10 Unvalidated Redirects and Forwards

## It's 10AM, Do You Know Where Your Money Is ?

**No man's property is safe while Wall Street is in session !**

CAST Confidential

## Code Unit Level — Pre-Build Analysis

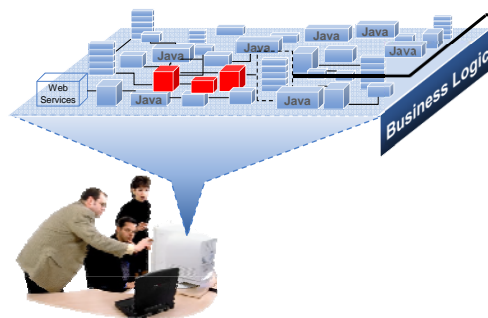


CAST Confidential

3

CAST

## Technology Level — Post-Build Analysis



Single language  
static analysis tools  
Quality Assurance

### 1 Code Unit Level

- Code style & layout
- Expression complexity
- Code documentation
- Class or program design
- Basic coding standards
- Developer level

### 2 Technology Level

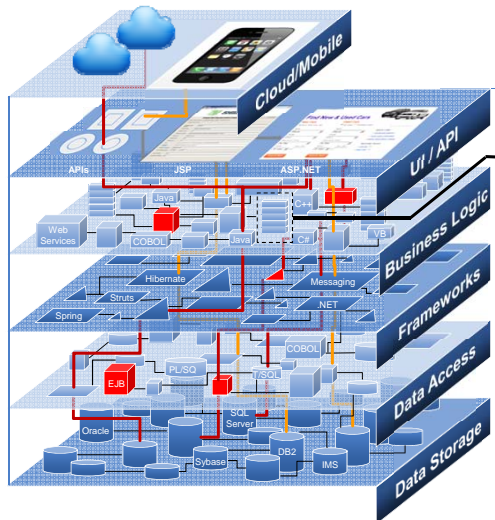
- Single language/technology layer
- Intra-technology architecture
- Intra-layer dependencies
- Design & structure
- Inter-program invocation
- Security vulnerabilities
- Development team level

CAST Confidential

4

CAST

## System Level — System Integration Analysis



### 1 Code 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
- Design & structure
- Inter-program invocation
- Security vulnerabilities
- Development team level

### 3 Application Stack Level

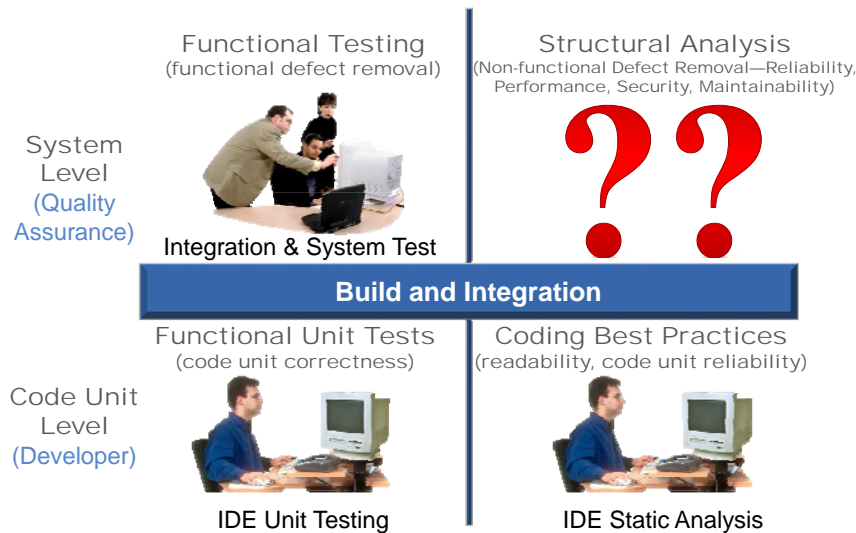
- Integration quality
- Architectural compliance
- Risk propagation
- Application security
- Resiliency checks
- Transaction integrity
- Function point, Effort estimation
- Data access control
- SDK versioning
- Calibration across technologies
- IT organization level

CAST Confidential

5

CAST

## The QA Gap

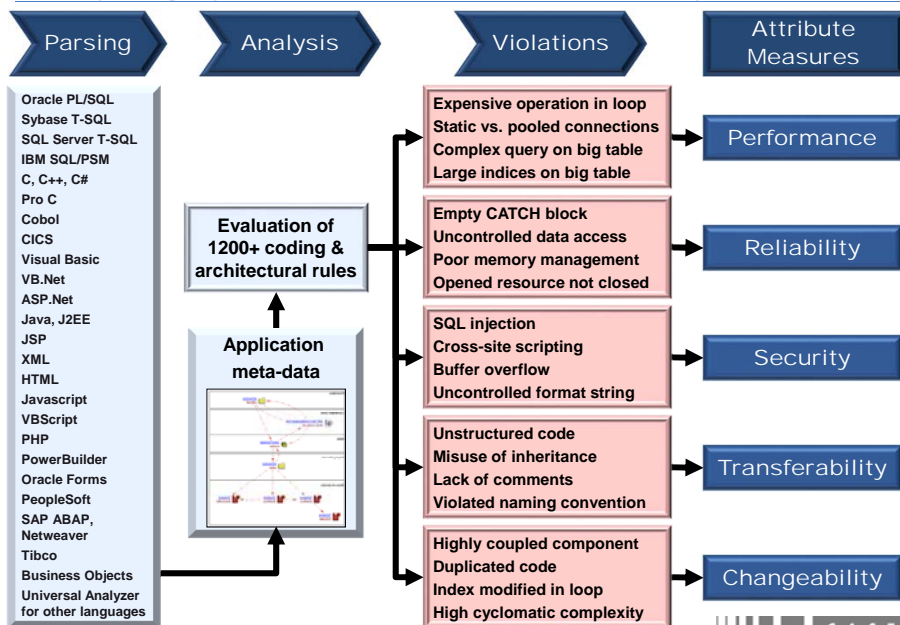


CAST Confidential

6

CAST

## Analyzing System Level Structural Quality



CAST Confidential

7

CAST

## Architecturally-Complex, Multi-Component Defects

Study of defects across 1 open source, 2 large NASA applications

Observation	% of cases
Fixes mapping to $\geq 2$ files	$\approx 60\%$
Fixes mapping to $\geq 3$ files	$\approx 30\text{-}40\%$
Fixes mapping to $\geq 2$ components	$\approx 10\text{-}36\%$
Fixes mapping to $\geq 2$ subsystems	$\approx 10\text{-}20\%$
Spread of faults	80% of faults in 20% of files

M. Hamill & K. Goseva-Popstojanova (2009). Common faults in software fault and failure data. *IEEE Transactions of Software Engineering*, 35 (4), 484-496.

CAST Confidential

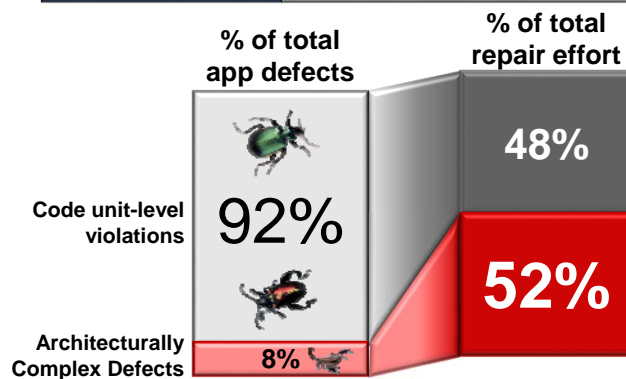
8



## 2) Detect Architecturally Complex Defects

**Architecturally Complex Defect**

A structural flaw involving interactions among multiple components, often residing in different subsystems

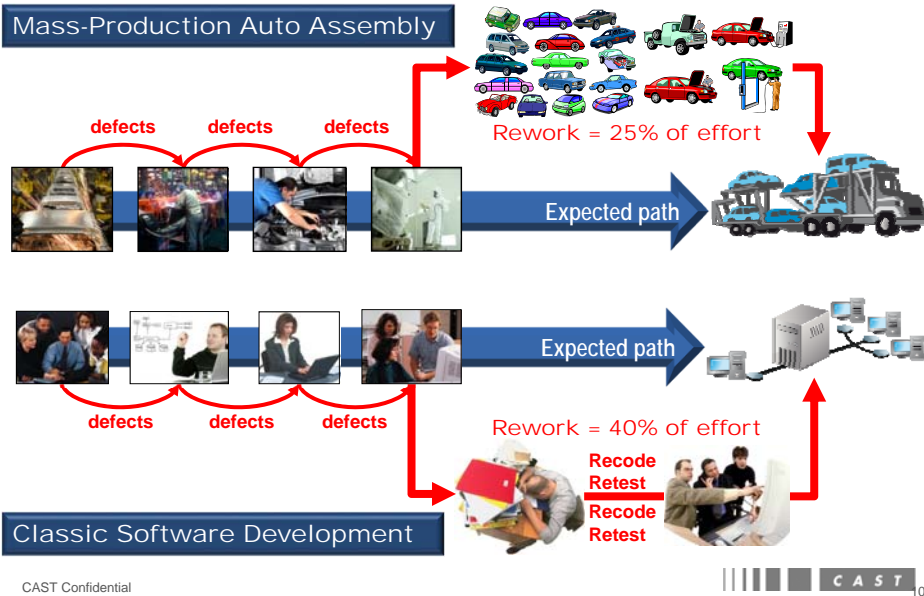


CAST Confidential

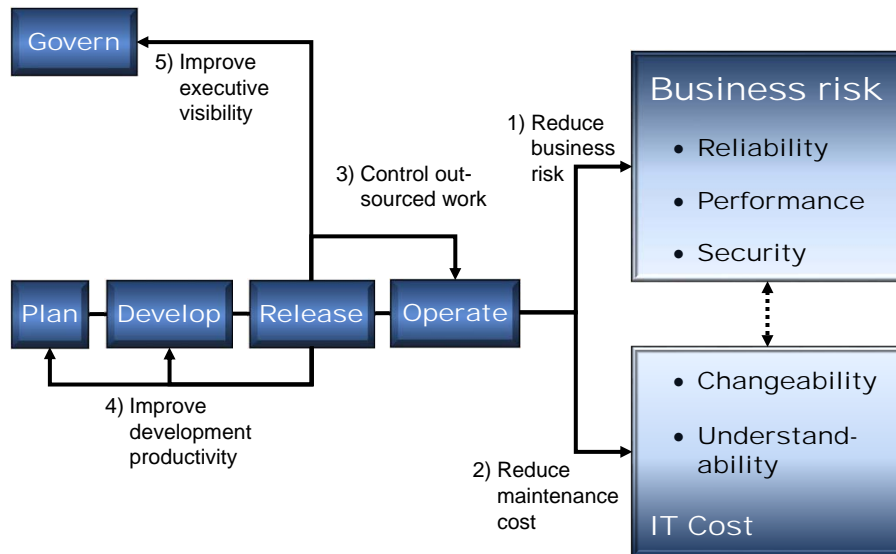
9



## Productivity and Rework — Detroit Was Better



## Five Purposes for Software Measurement

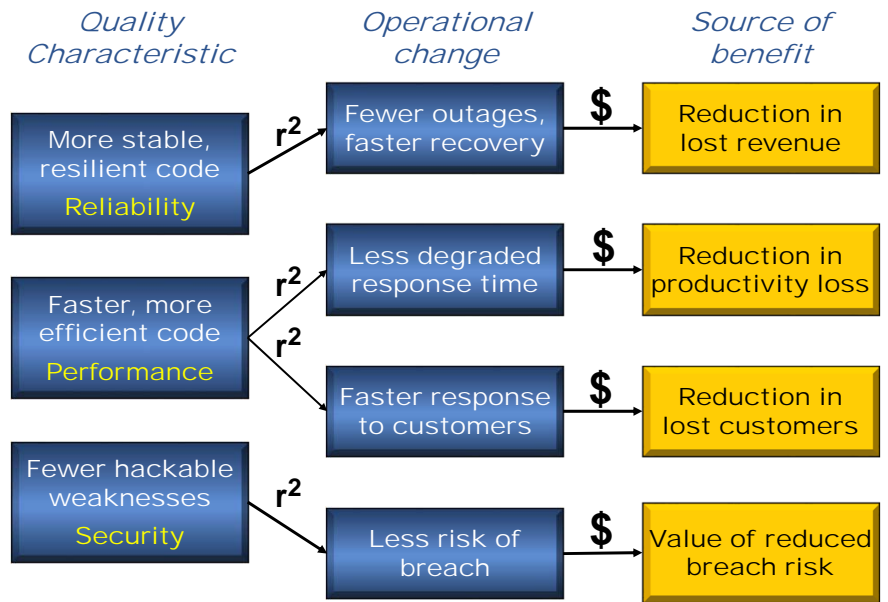


CAST Confidential

11

CAST

## Structural Quality in Business Risk Terms



CAST Confidential

12

CAST

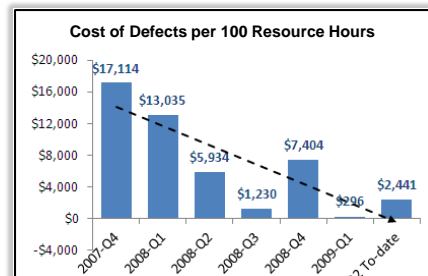
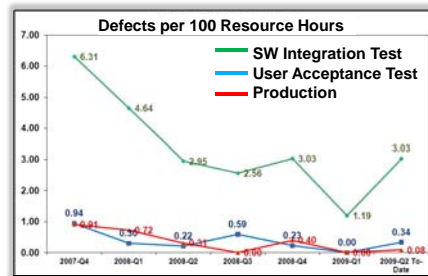
## Case Study 1 — Major US Consumer Bank

### Situation

- Retirement services, >\$100B in assets
- 75 supported application
- Complex technology environment
- IT-intensive business process
- Initiated structural quality analysis 4Q07

### Result

- Sustained reduction in test and production defects
- 7X reduction in defect costs



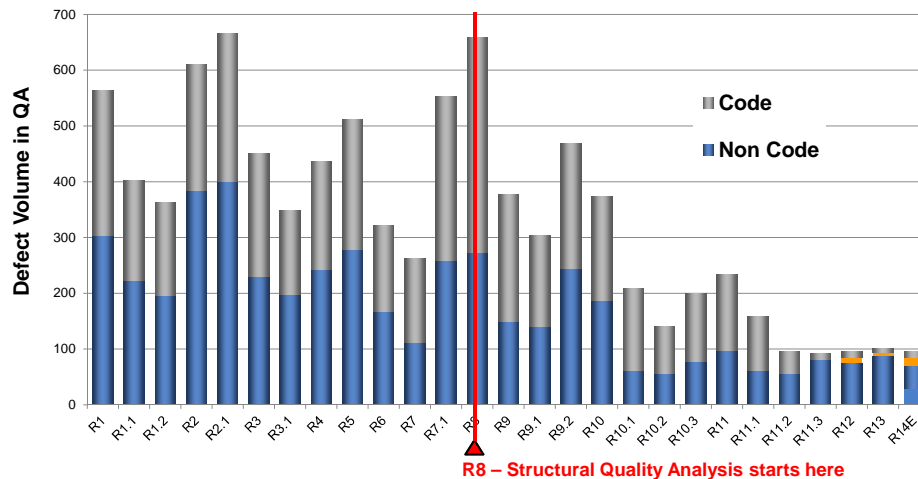
CAST Confidential

13

CAST

## Case Study 2 — Large Telco Reduces Defect Costs

- Order Management System (OMS)
- J2EE, VB, ASP, OMS Oracle, XML, Amdocs Enabler
- Multi-year development, >\$100m per year, 6 releases PY, runaway costs,



CAST Confidential

14

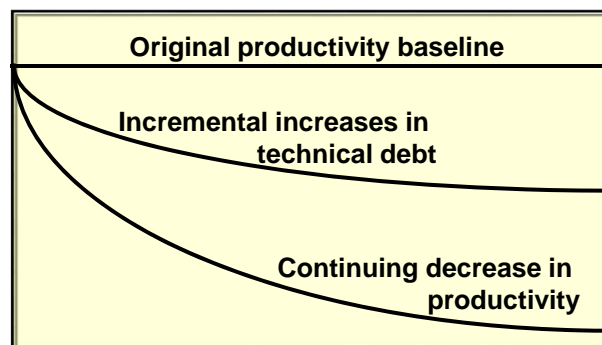
CAST

## Rethinking Productivity Measurement

$$\text{Release Productivity} = \frac{\text{Volume of code developed, modified, or deleted}}{\text{Total effort expended on the release}}$$

Productivity baseline —

a value in a monotonically declining function that compares the amount of product produced to the effort required to produce it  
... unless you take action



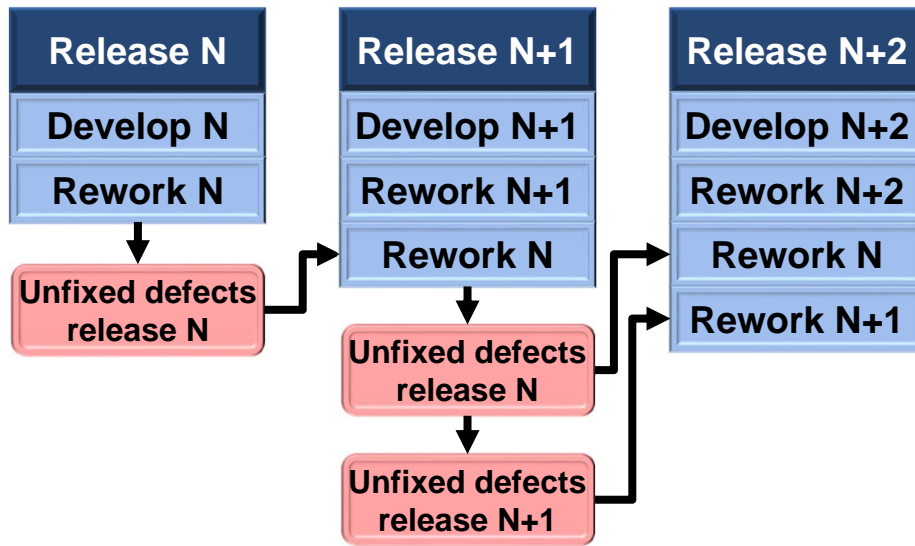
CAST Confidential

15

CAST



## Technical Debt = Carry-forward Rework

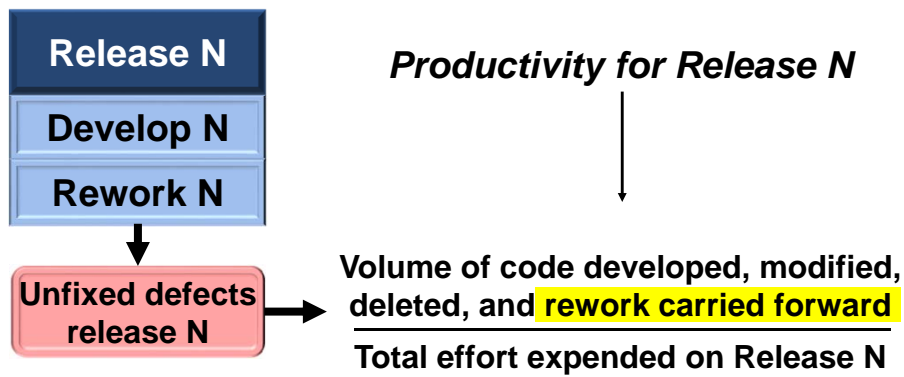


CAST Confidential

16



## Adjust Productivity for Technical Debt

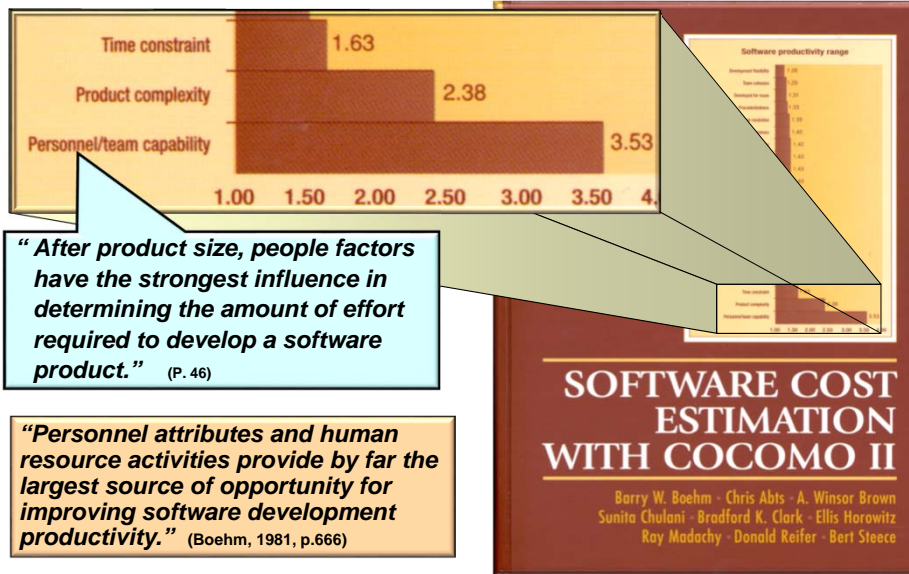


CAST Confidential

17



## What Predominates Software Variation



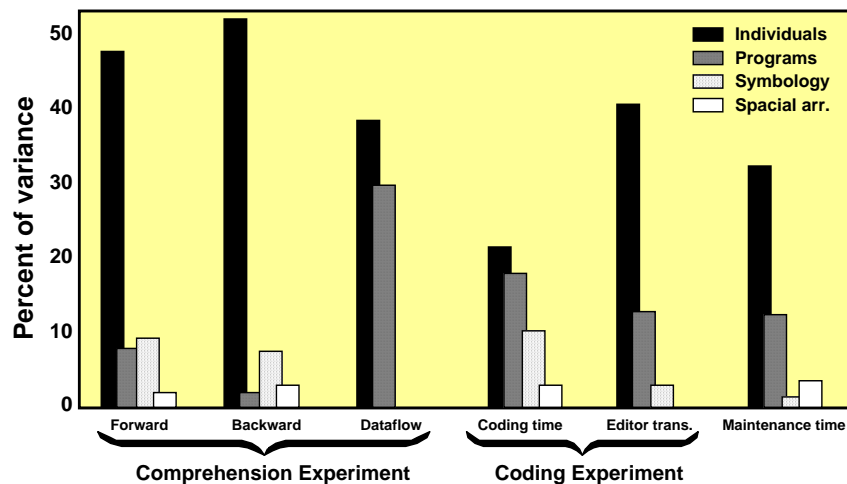
CAST Confidential

Boehm, et. al (2000)

18

CAST

## Programmer Variation Swamps Everything

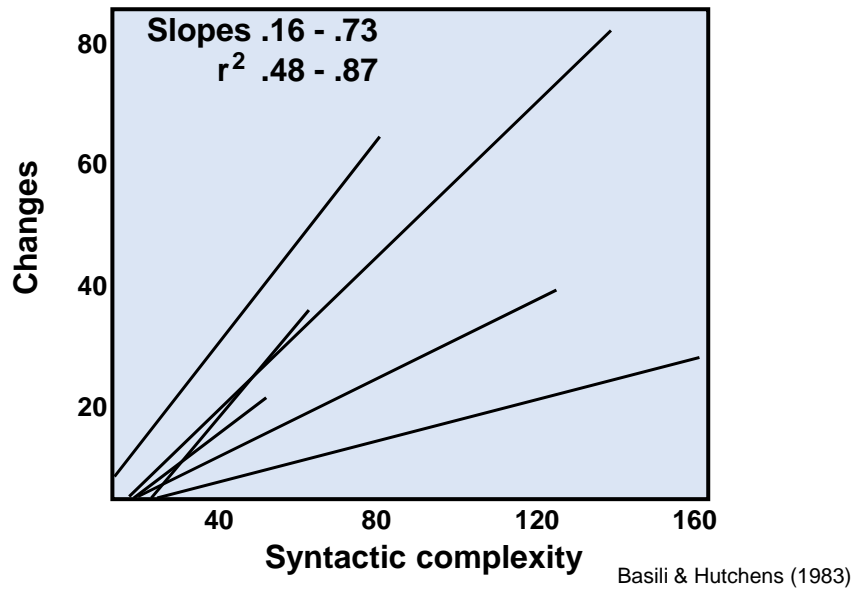


CAST Confidential

19

CAST

## Complexity Profiles for Individual Developers

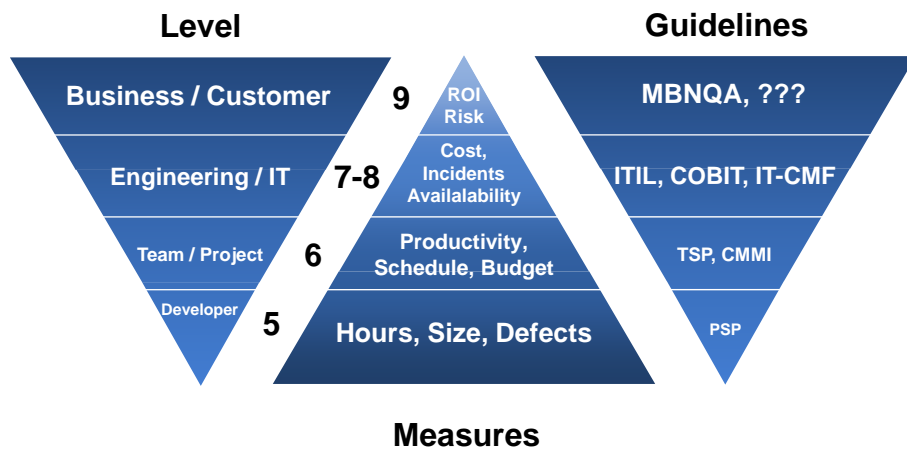


CAST Confidential

20

CAST

## The Measurement Stack

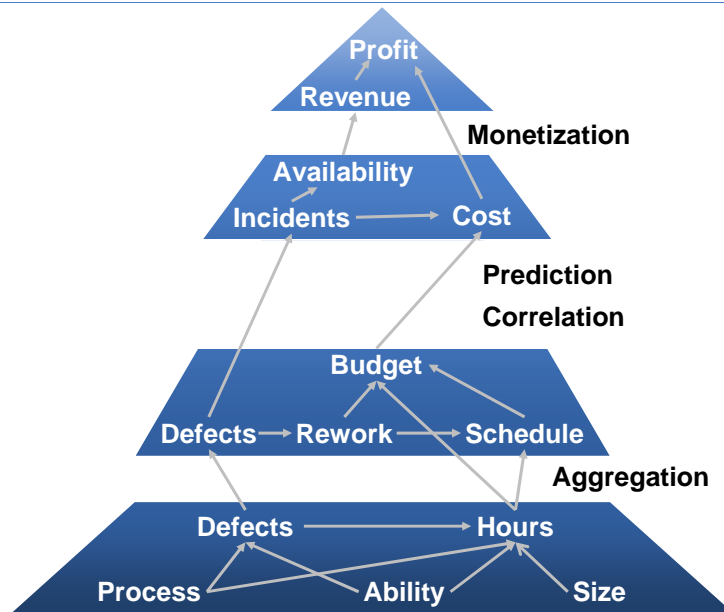


CAST Confidential

21

CAST

## Value Transitions in the Measurement Stack



CAST Confidential

22



## Consortium for IT Software Quality



- Co-sponsored by SEI and the Object Management Group (OMG)
- 24 original member companies
- Objective to standardize code level measurement of software attributes
- Automated Function Points now a supported specification of OMG

CAST Confidential

23



## [www.it-cisq.org](http://www.it-cisq.org) — Membership Is Free

The screenshot shows the CISQ website homepage. At the top, there's a header with the CISQ logo (Consortium for IT Software Quality), the Software Engineering Institute Carnegie Mellon logo, and navigation links for Quality Report Podcasts, CISQ FAQs, and Contact Us. A search bar and links for Member Page and Member Logout are also present. Below the header is a dark blue navigation bar with links: Home, CISQ Blog, Quality Report Podcasts, Members-Only Portal, Why CISQ?, CISQ Founders, and Press Coverage. The main content area features a 'Become a CISQ' section with a 'Member' button and a 'Sponsor' button. To the right of this are buttons for 'CISQ Downloads', 'Members-Only Portal', and 'CISQ Meetings'. Below this is a 'Latest Tweets' section with two tweets about CISQ's importance and a link to a discussion on LinkedIn. Next to it is a 'CISQ Blog' section with a post titled 'It's the Product, Stupid!' and a link to 'The Director's Blog'. To the right of the blog is a 'Member Comments' section with a quote from MD North America, a Major Global IT Services Vendor. At the bottom, there's a dark blue footer with copyright information (Copyright © 2012, CISQ, All Rights Reserved), social media links (Twitter, LinkedIn, Facebook), and a list of links including Home, Members-Only Portal, Why CISQ?, CISQ Founders, CISQ Downloads, CISQ Podcasts, CISQ Membership, CISQ Executives, CISQ Founders, Press Coverage, Quality Report Podcasts, and CISQ FAQs.

Quality Report Podcasts CISQ FAQs Contact Us

Search

Member Page Member Logout

CISQ Consortium for IT Software Quality

Software Engineering Institute Carnegie Mellon

Home CISQ Blog Quality Report Podcasts Members-Only Portal Why CISQ? CISQ Founders Press Coverage

Consortium for IT Software Quality

The Consortium for IT Software Quality (CISQ) is an IT industry leadership group comprised of IT executives from the Global 2000, system integrators, outsourced service providers, and software technology vendors committed to introduce a computable metrics standard for measuring software quality & size. CISQ is a neutral, open forum in which customers and suppliers of IT application software can develop an industry-wide agenda of actions for improving IT application quality and reduce cost and risk.

Become a CISQ

Member

Sponsor

CISQ Downloads

Members-Only Portal

CISQ Meetings

Latest Tweets

#cisq Important! Rate Correctly the Importance Of Problems on #OWS #Q&A #SQA #it\_cisq #testing #software #qualityassurance

24 minutes ago · reply · retweet · favorite

#cisq With Software Quality Assurance on #OWS #Q&A #SQA #it\_cisq #software #qualityassurance about 1 hour ago · reply · retweet · favorite

Discussion on LinkedIn

CISQ Blog

It's the Product, Stupid!

Too often when I meet with executives I get confronted with, "Hey, you..." [read more](#)

The Director's Blog

It's been several years since I was asked to become the first Director of CISQ... [read more](#)

Member Comments

“Every client we work with has a different understanding of 'quality' in application development and maintenance. We need a way to have consistent and objective dialog about this important issue across the industry.”

MD North America  
Major Global IT Services Vendor

Copyright © 2012, CISQ, All Rights Reserved  
Consortium for IT Software Quality

Get Social

Home  
Members-Only Portal  
Why CISQ?  
CISQ Founders  
CISQ Downloads  
CISQ Podcasts  
CISQ Membership  
CISQ Executives  
CISQ Founders  
Press Coverage  
Quality Report Podcasts  
CISQ FAQs