SYSTEMS ENGINEERING RESEARCH CENTER

SERC TALKS

WELCOME

How Can We Advance Structural Quality Analysis with Standards and Machine Learning?

Bill Curtis, Executive Director, Consortium for IT Software Quality (CISQ), Senior VP & Chief Scientist, CAST Software; Head of CAST Research Labs

October 3 | 1:00 PM ET

- ❑ Today's session will be recorded.
- ❑ An archive of today's talk will be available at: www.sercuarc.org/serc-talks/
- ❑ Use the Q&A box to queue questions, reserving the chat box for comments, and questions will be answered during the last 5-10 minutes of the session.
- ❑ If you are connected via the dial-in information only, please email questions or comments to SERCtalks@stevens.edu.
- ❑ Any issues? Use the chat feature for any technical difficulties or other comments, or email SERCtalks@stevens.edu.

How Can We Advance Structural Quality Analysis with Standards and Machine Learning?

SERC Webinar
October 3, 2018

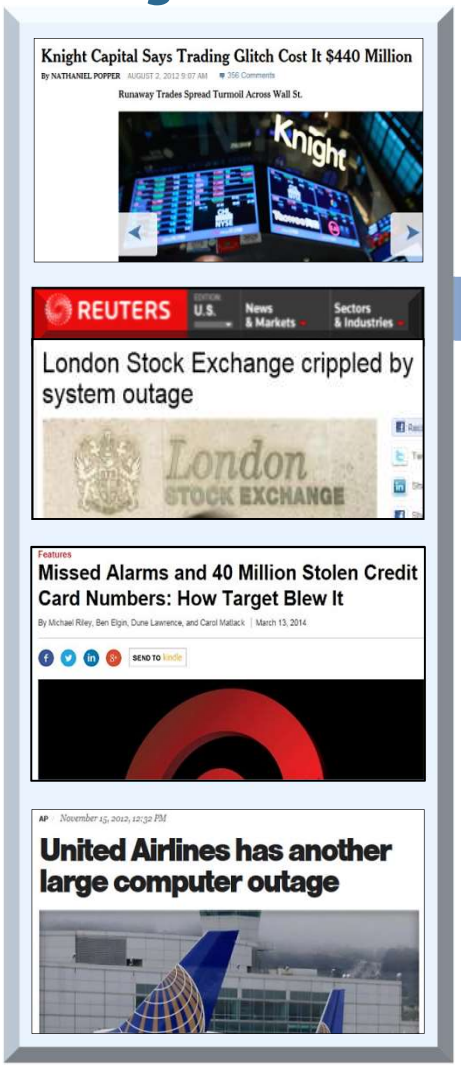
Dr. Bill Curtis
Executive Director, CISQ

CISQ
Consortium for IT Software Quality

CISQ
Consortium for IT Software Quality

Era of the 9-Digit Glitch

9-Digit Glitches



now affect

- Board of Directors
- CEO, COO, CFO
- Business VPs
- Corporate Auditors
- CIO

accountable for

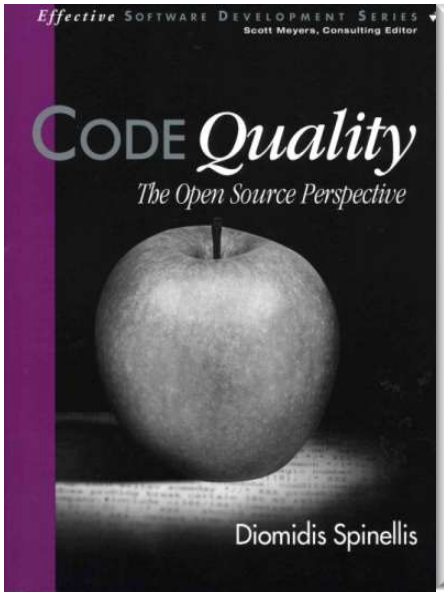
- Governance
- Financial outcomes
- Risk management
- Brand protection
- Customer experience

Structural Quality Standards to Evaluate Application Risk

Evolving the Definition of Quality

Quality ~~The degree to which a product meets its specified requirements~~

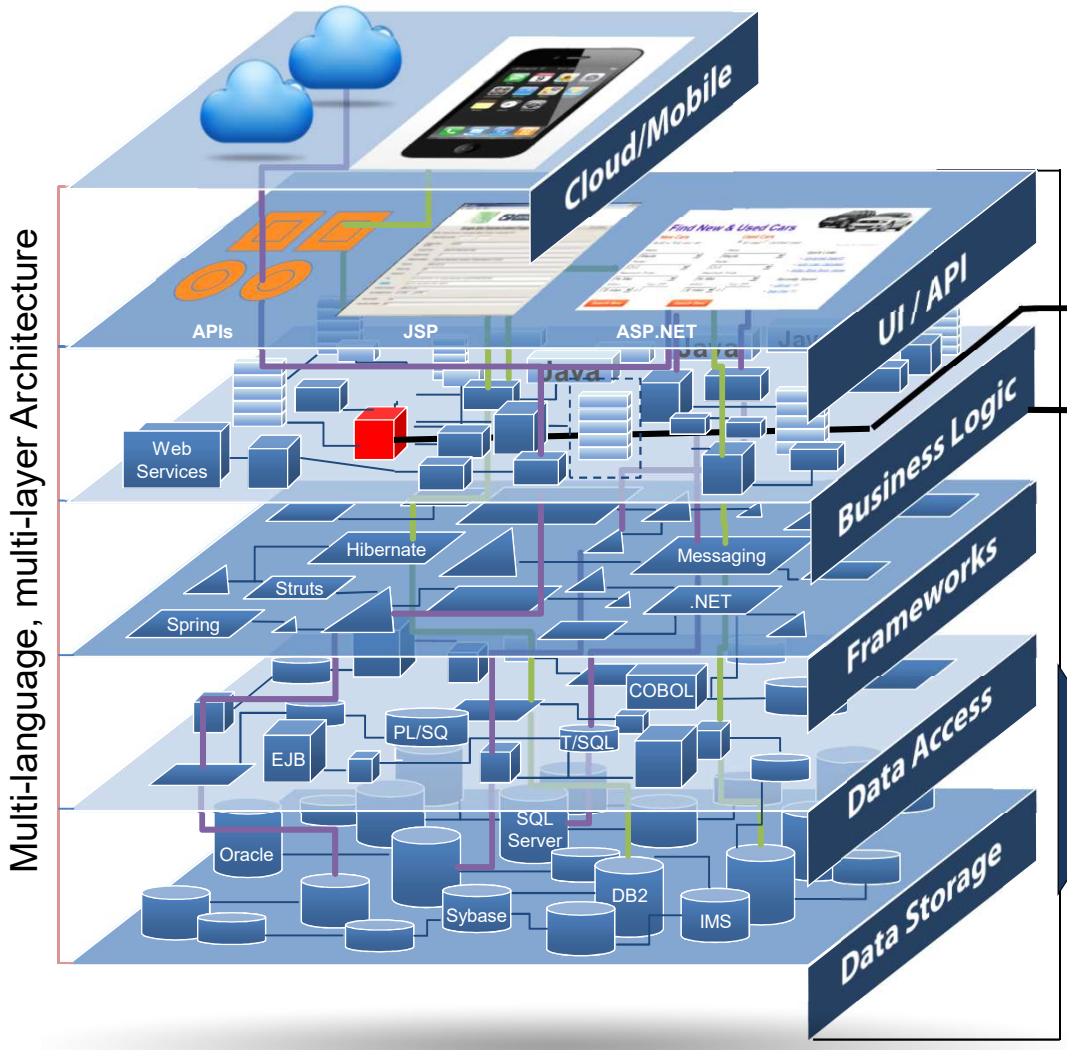
Problem — Customers struggle to state functional requirements. They do not understand non-functional requirements.



"…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."

CISQ
Consortium for IT Software Quality

Apps Are a Technology Stack



Technology Stack

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

CISQ
Consortium for IT Software Quality

4th Wave in Software Engineering

What: Architecture, Structural measures, Reuse

When: 2002➔

Why: Improve engineering of software products

What: CMM, ITIL, PMBOK, Agile

When: 1990-2002

Why: Improve software management and discipline

What: Design methods, CASE tools

When: 1980-1990

Why: Give developers better aids to construct systems

What: 3rd & 4th generation languages, structured programming

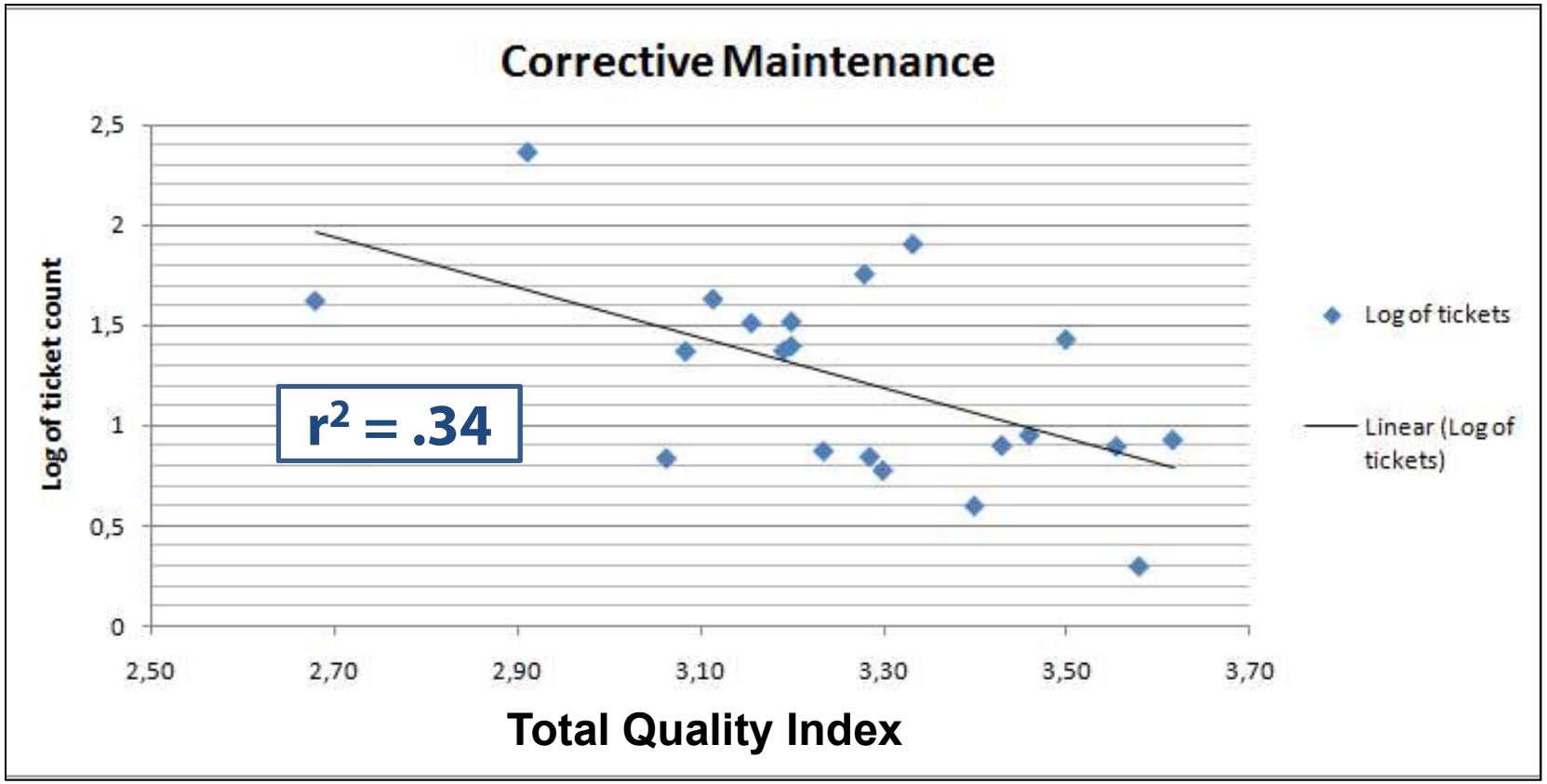
When: 1965-1980

Why: Give developers greater power for expressing programs

CISQ
Consortium for IT Software Quality

Structural Quality & Corrective Maintenance

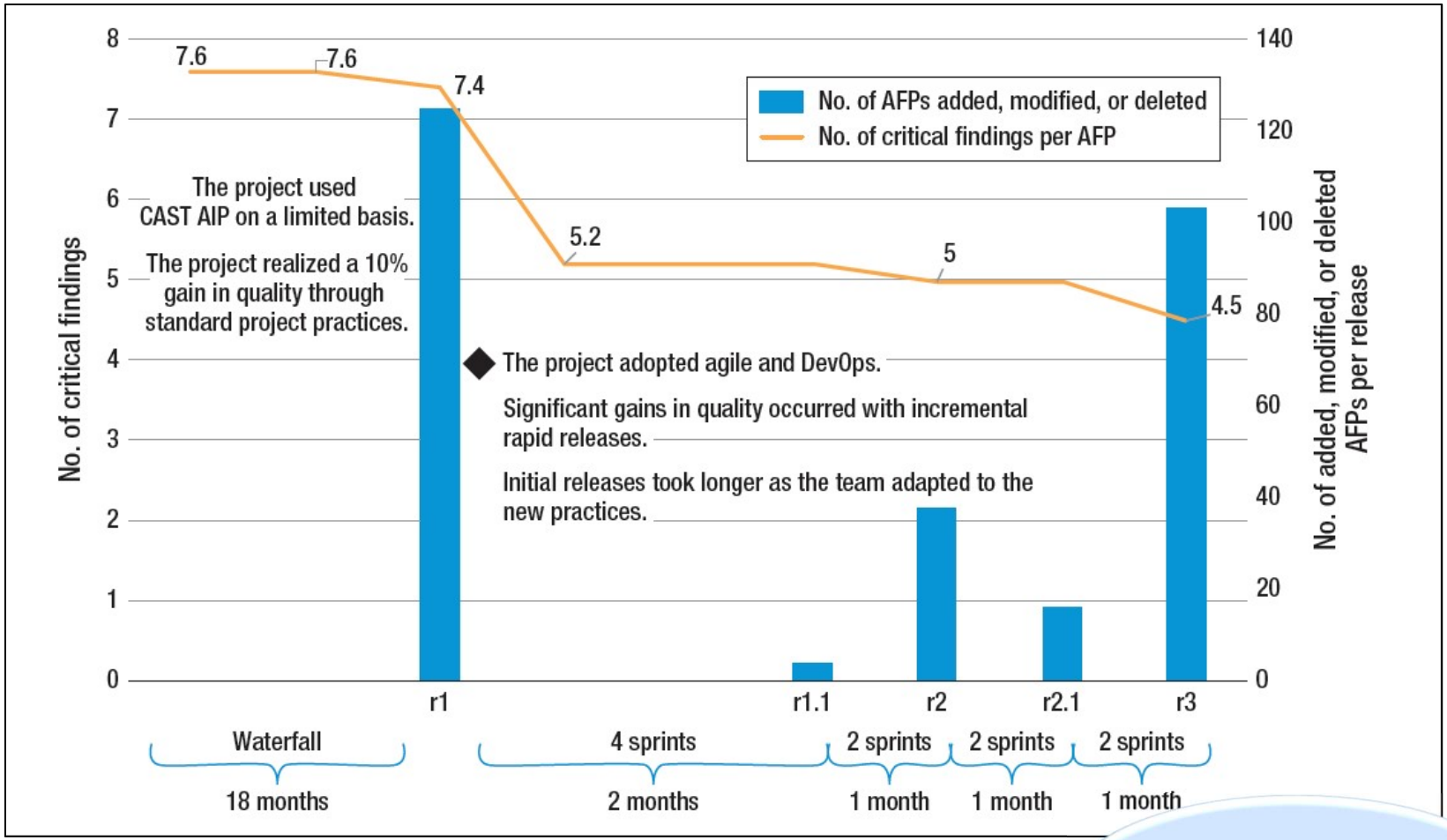
Study of structural quality measures and corrective maintenance effort across 20 customers in a large global system integrator



TQI increase of .24 decreased corrective maintenance effort by 50%

Measuring an Agile/DevOps Transformation

Agile/DevOps transformation at Fannie Mae

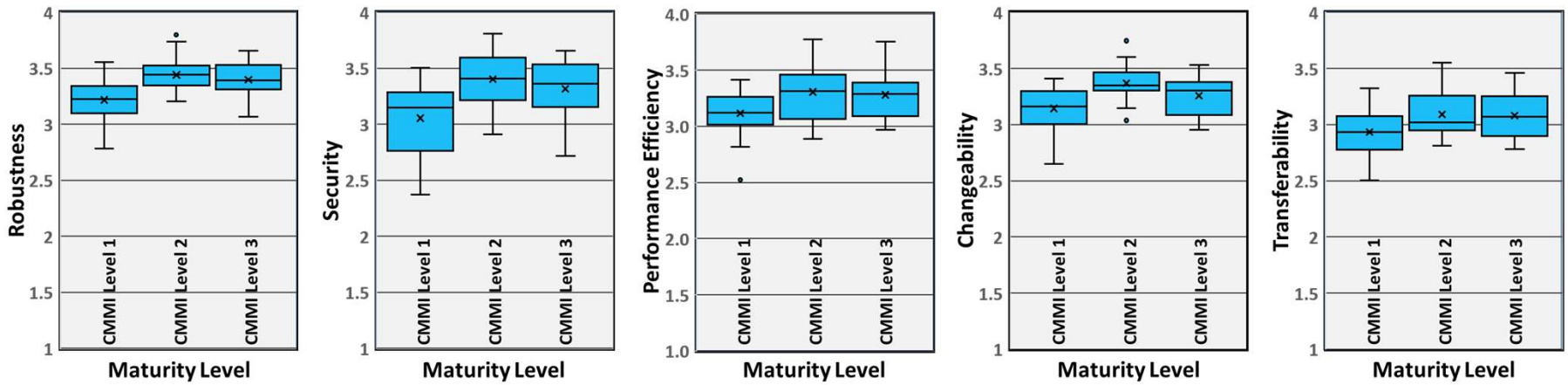


41% fewer defects per AFP by r3

Barry Snyder & Bill Curtis (2018). Using Analytics to Guide Improvement During an Agile DevOps Transformation, *IEEE Software*, Jan/Feb 2018.

CISQ
Consortium for IT Software Quality

Maturity Affects Quality — Level 1 Worst



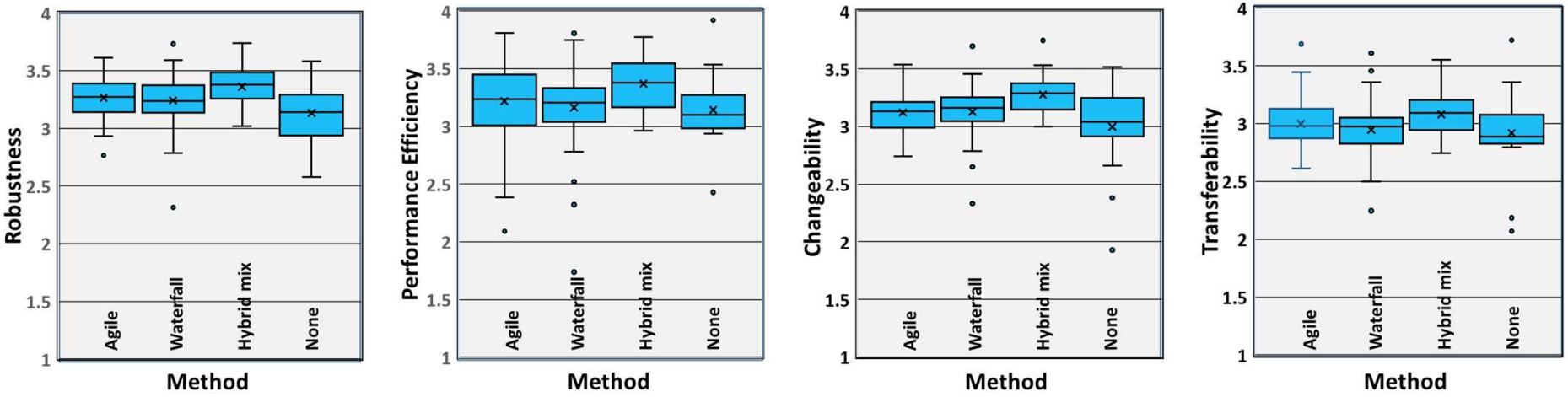
	# apps	Robust	Security	Perform	Change	Transfer
CMMI Level 3	22	3.40	3.32	3.28	3.26	3.08
CMMI Level 2	27	3.44	3.40	3.31	3.37	3.09
CMMI Level 1	23	3.22	3.06	3.11	3.14	2.93
% variance explained		28%	25%	15%	24%	12%

Java EE applications analyzed with CAST Application Intelligence Platform — scale is 1.0 to 4.0

Stabilizing project schedules and baselines (Level 2) allows developers to work in an orderly professional way. Standardizing processes (Level 3) did not improve structural quality and may have its benefits more on economy of scale issues.

CISQ
Consortium for IT Software Quality

Method Affects Quality — Hybrid best



	# apps	Robust	Security	Perform	Change	Transfer
Hybrid mix	51	3.36	3.27	3.37	3.27	3.08
Agile	77	3.26	3.14	3.22	3.12	3.00
Waterfall	60	3.24	3.21	3.16	3.13	2.95
None	20	3.13	3.15	3.14	3.00	2.92
% variance explained		10%	n.s.	6%	14%	6%

Java EE applications analyzed with CAST Application Intelligence Platform — scale is 1.0 to 4.0

Hybrid method's mix of early attention to architecture combined with structural analysis in short cycle iterations produces the best structural quality outcomes.

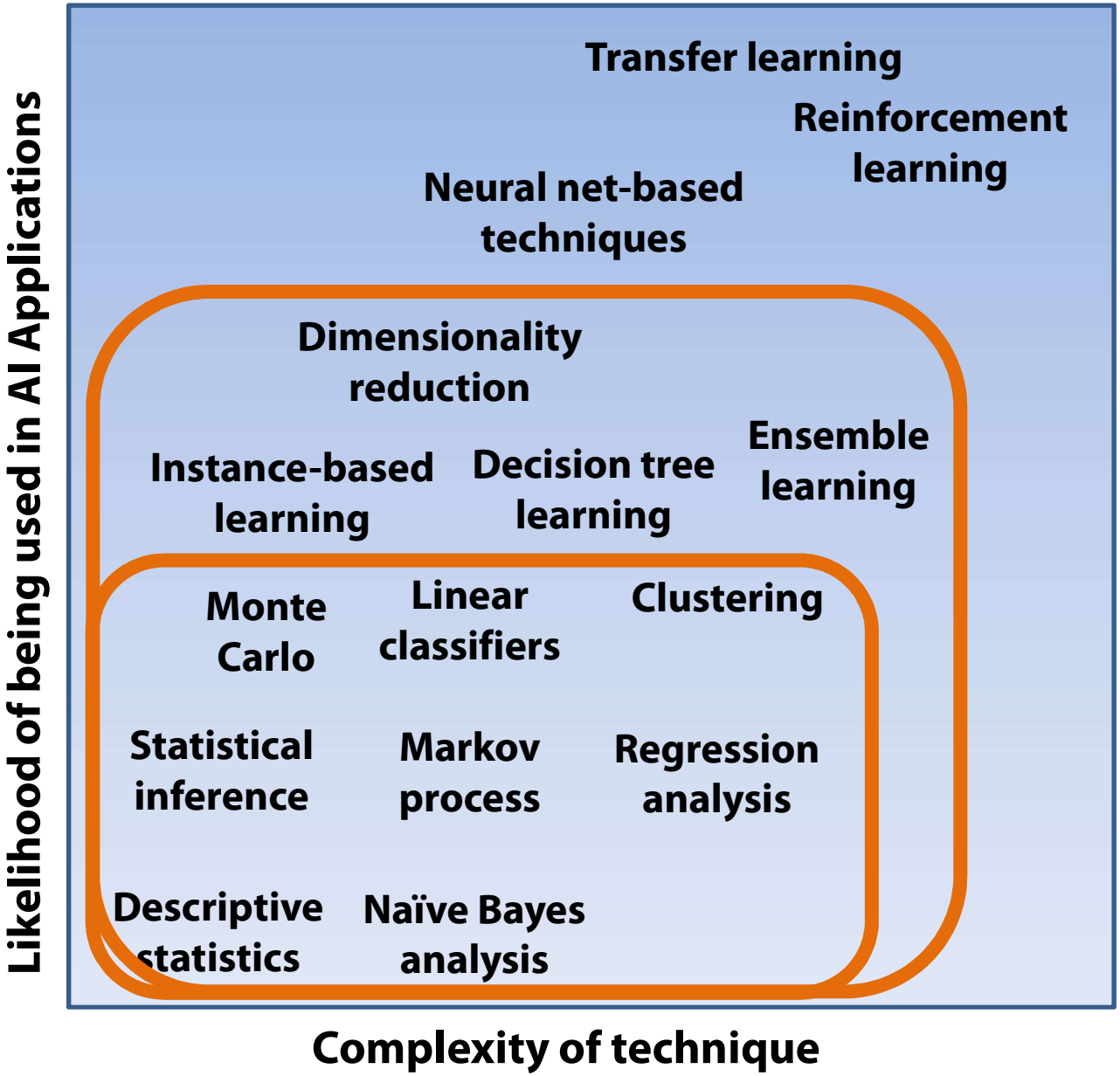
CISQ
Consortium for IT Software Quality

Machine Learning

Machine Learning	• Creating and using models learned from data • Learning without being explicitly programmed • Performance improves as more data is analyzed
Methods	• Statistical ⟶ model fitting ⟶ Predict • Unsupervised → model discovery ⟶ Suggest • Supervised ⟶ model training ⟶ Categorize • Reinforcement→ outcome training ⟶ Predict
Some Use Cases	• Defect prediction ⟶ regression methods • Behavior prediction ⟶ supervised learning • Micro-service discovery ⟶ clustering, training

CISQ
Consortium for IT Software Quality

Comparison of Machine Learning Methods



Reinforcement

Supervised

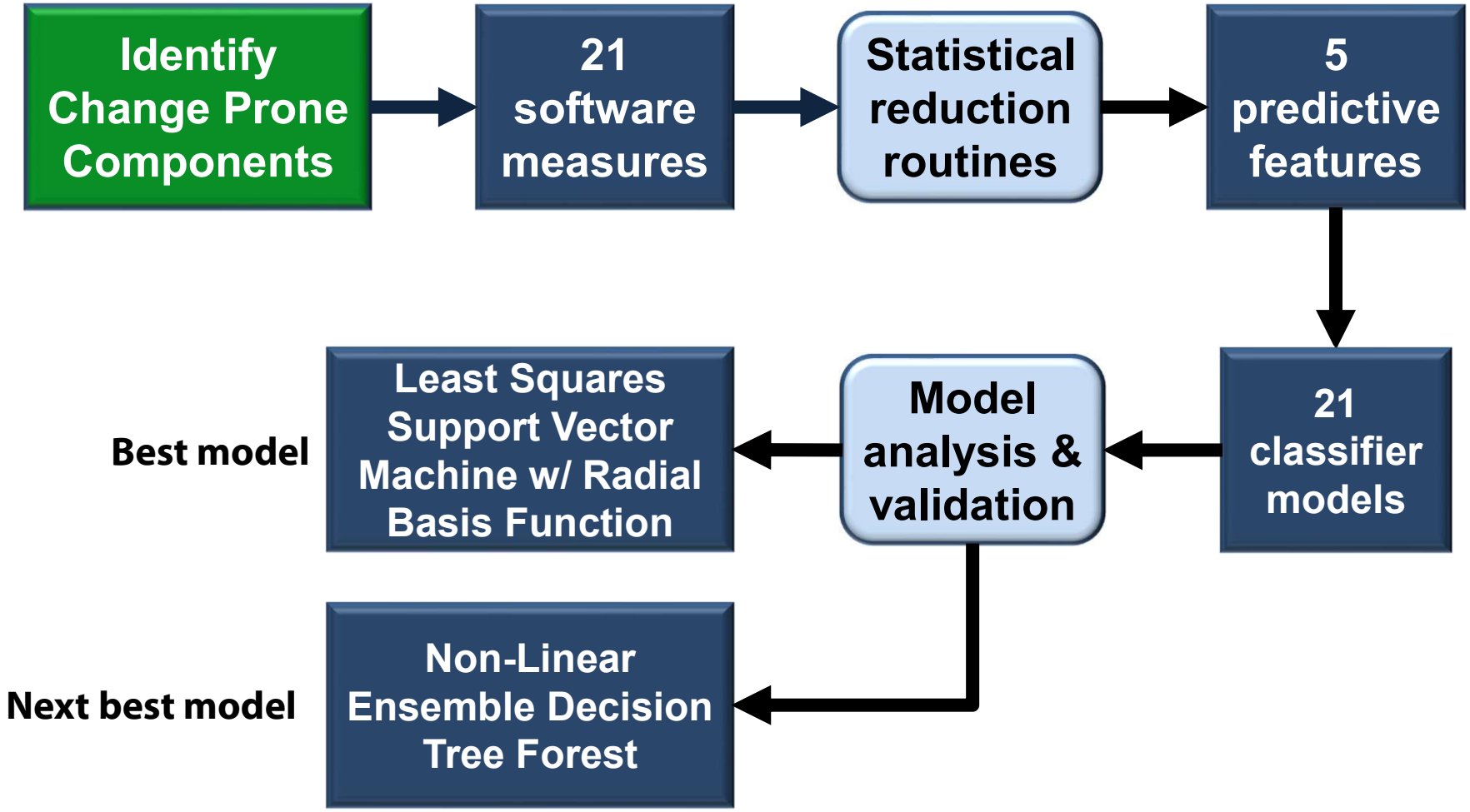
Unsupervised

Statistical

Notes from the AI frontier: Applications and value of deep learning
M. Chui, J. Manyika, M. Miremadi, N. Henke, R. Chung, P. Nel, & S. Malhotra
McKinsey Global Institute

CISQ
Consortium for IT Software Quality

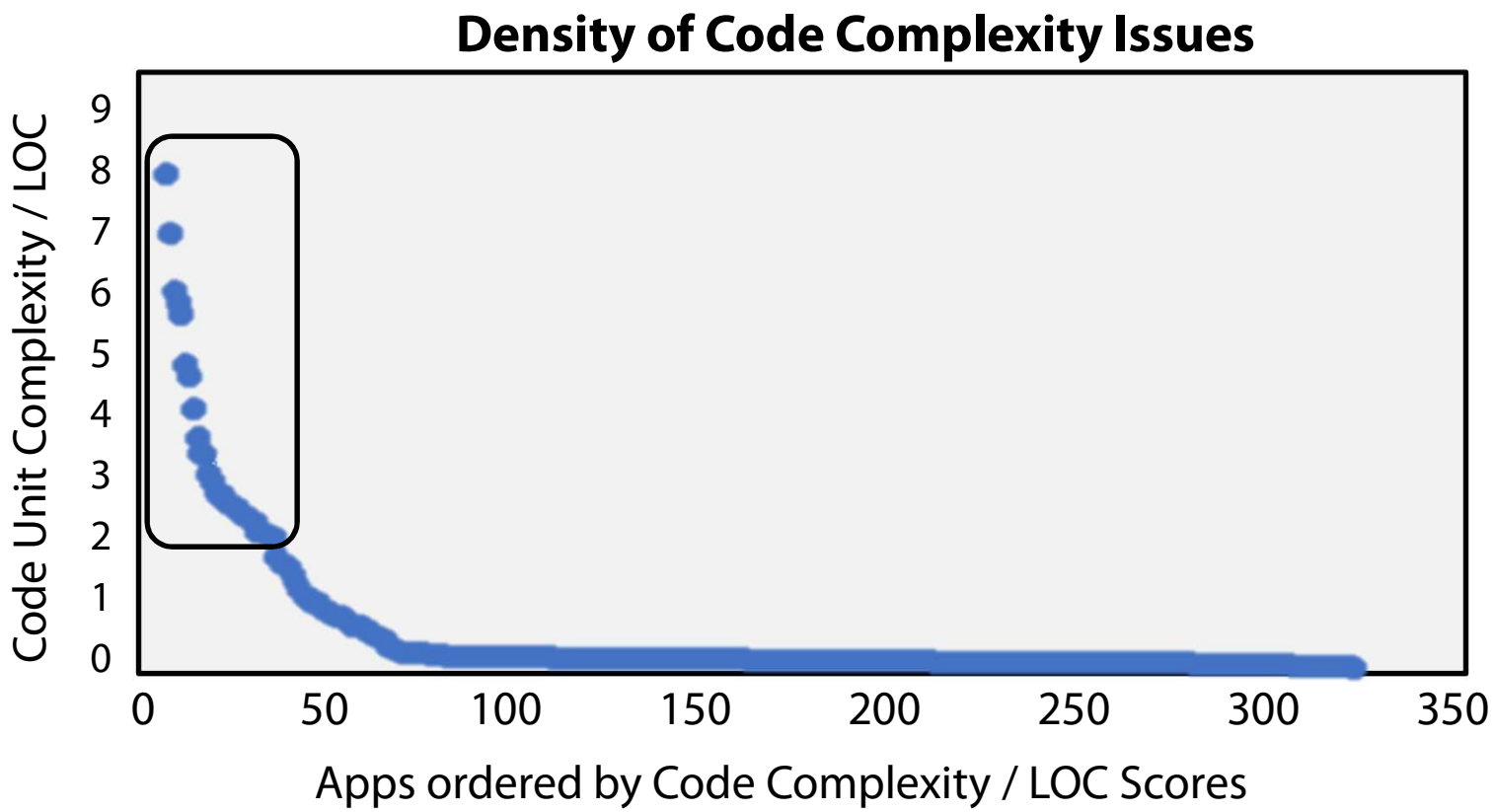
Machine Learning Workflow



L. Kumar & A. Sureka (2017). A Comparative Study of Different Source Code Metrics and Machine Learning Algorithms for Predicting Change Proneness of Object Oriented Systems. Proceedings of ISEC'18.

CISQ
Consortium for IT Software Quality

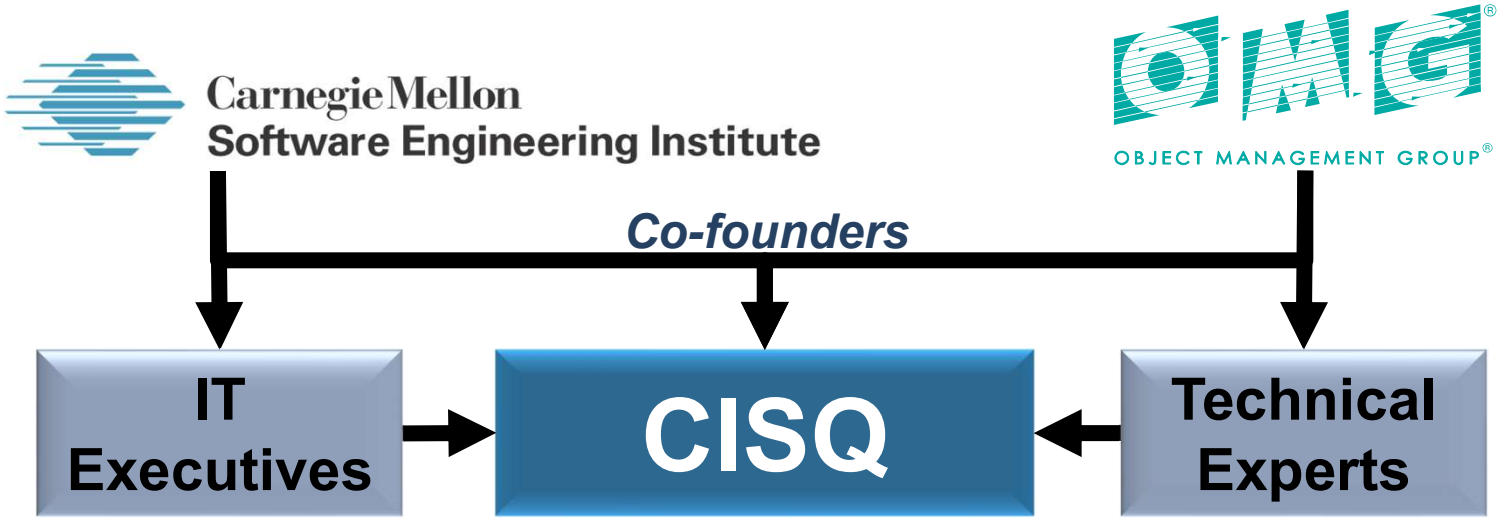
Does Machine Learning Add Capability?



Would a machine learning application add significantly better prediction than a simpler measure ?

The power of machine learning may be in identifying issues long before they are evident from simpler measures

Consortium for IT Software Quality (CISQ)



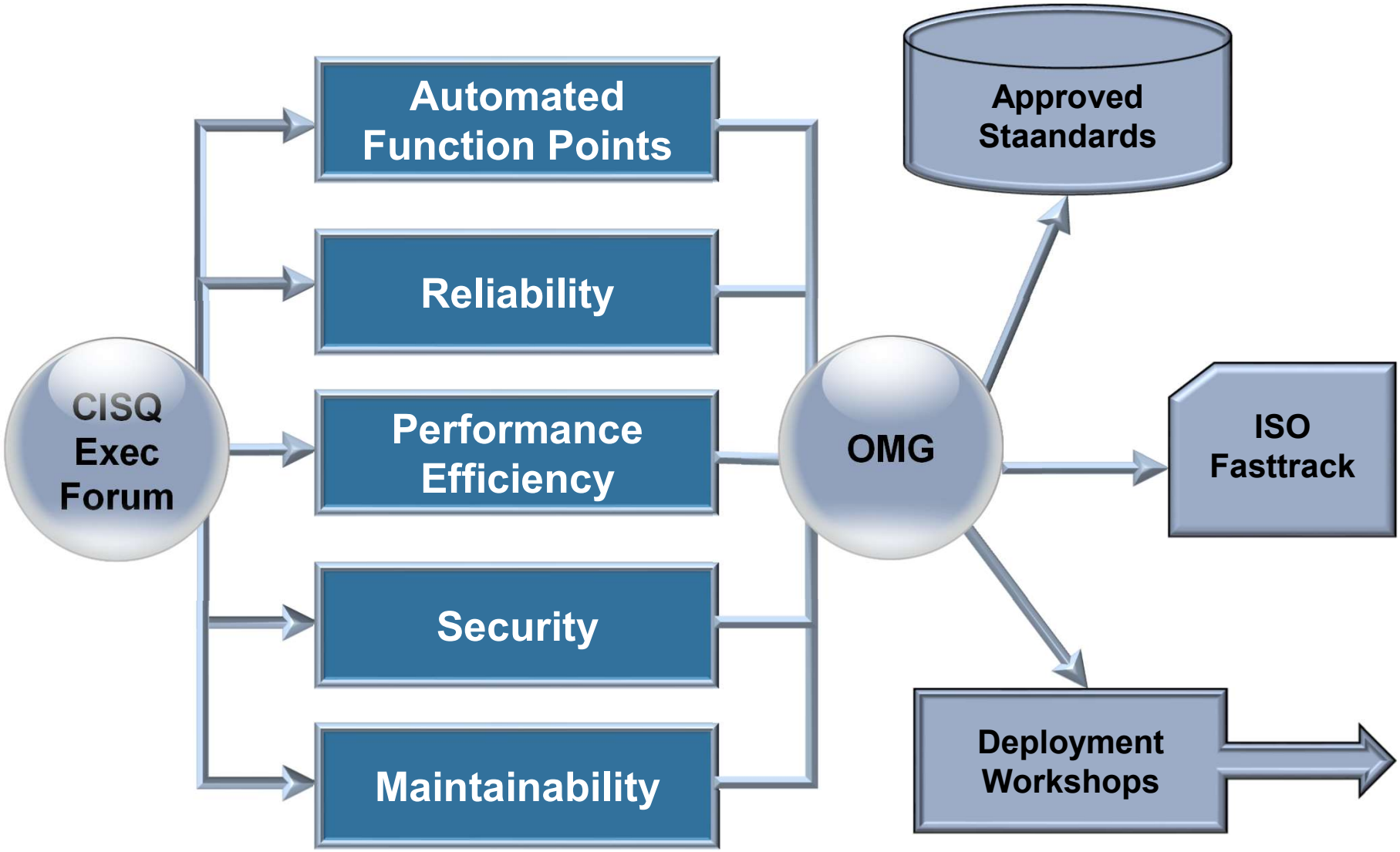
OMG Special Interest Group

CISQ is chartered to define automatable measures of software size and quality that can be measured in the source code, and promote them to become Approved Specifications of the OMG®

CISQ Sponsors

Synopsys, Cognizant, SHPI, Tech Mahindra, CAST, CGI, Northrop Grumman

CISQ/OMG Standards Process



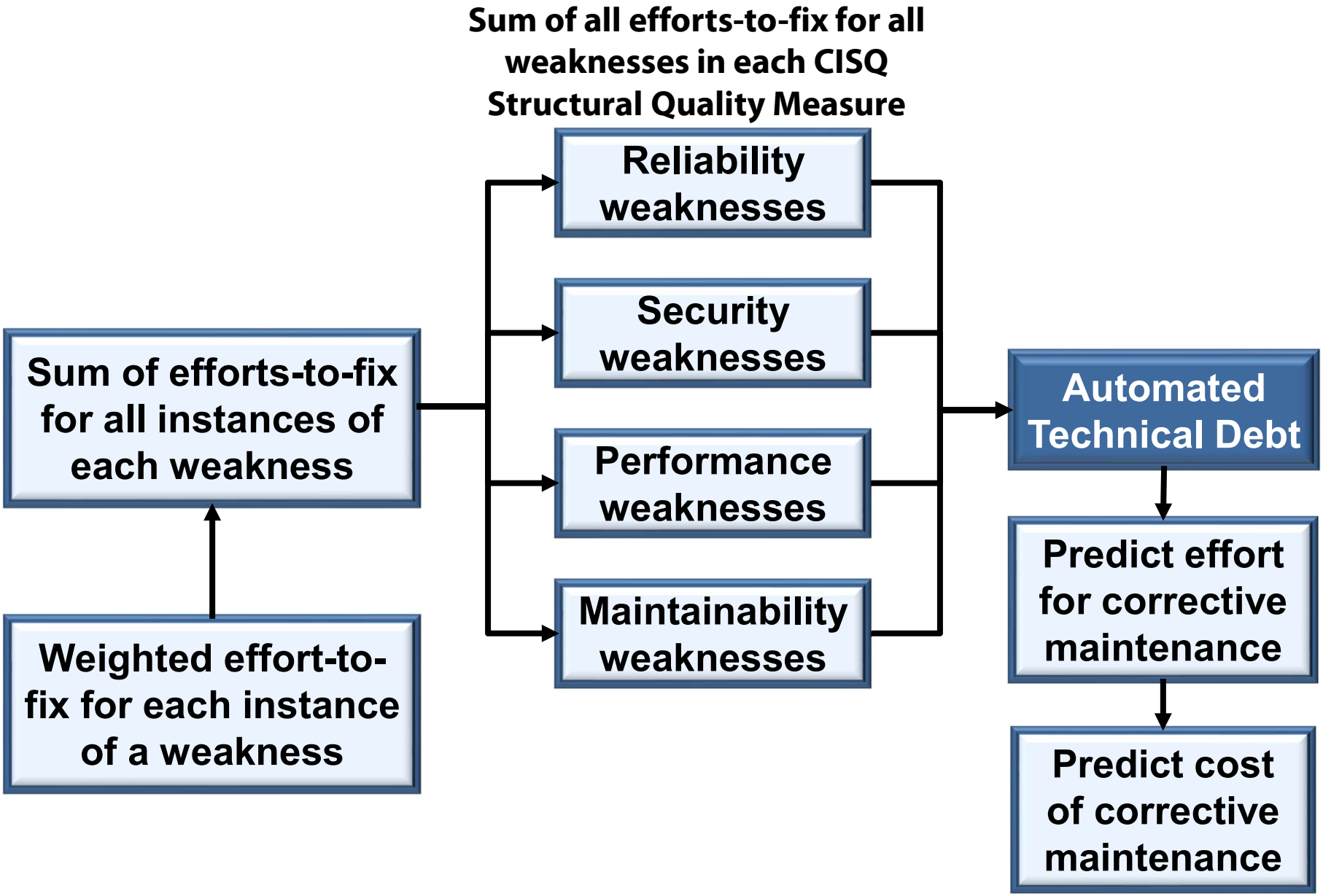
17

CISQ
Consortium for IT Software Quality

CISQ Structural Quality Measures

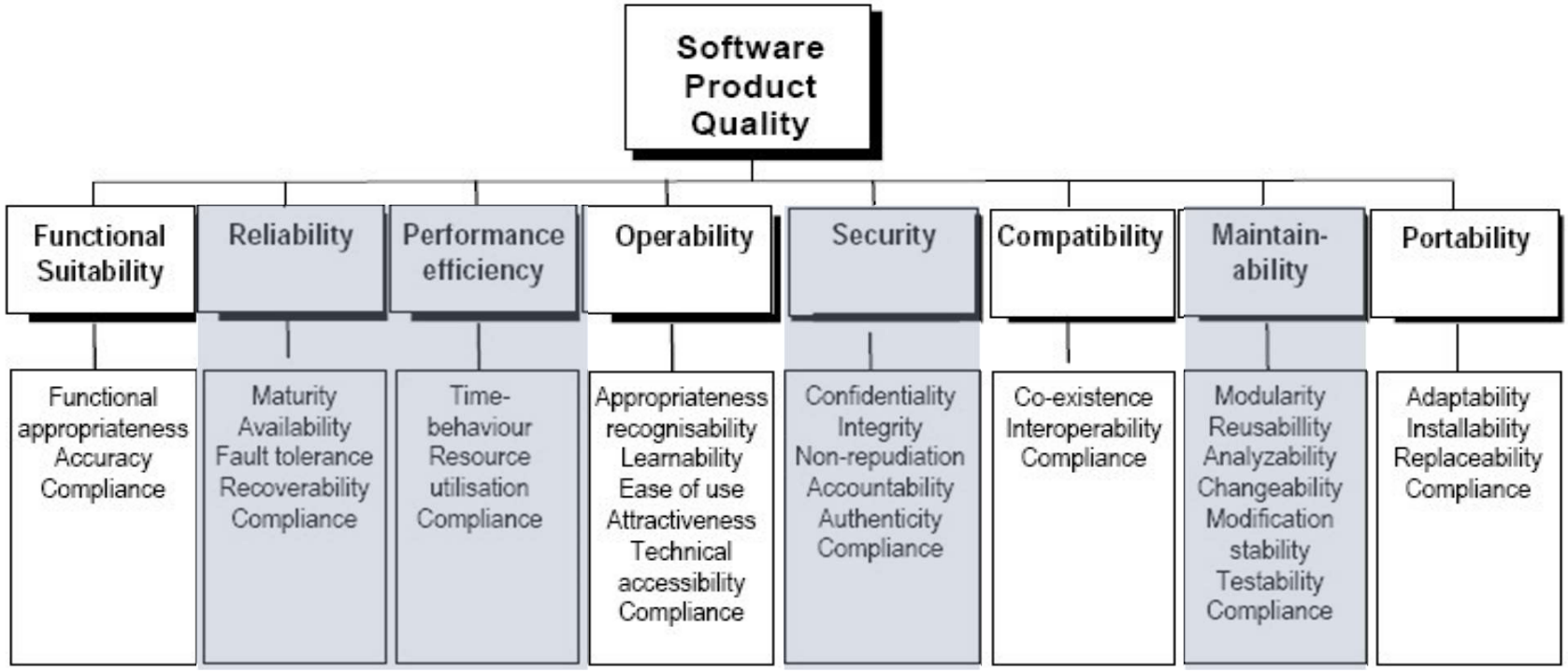
CISQ Structural Quality Characteristic Measures		Example architectural and coding violations included
Security	22 weaknesses (Top 25 CWEs)	• SQL injection • Cross-site scripting • Buffer overflow
Reliability	29 weaknesses	• Empty exception block • Unreleased resources • Poor error handling
Performance Efficiency	15 weaknesses	• Expensive loop operation • Un-indexed data access • Unreleased memory
Maintainability	20 weaknesses	• Excessive coupling • Dead code • Hard-coded literals

CISQ Automated Technical Debt Measure



CISQ and ISO 25000 Standards

- **ISO 25010 defines quality characteristics and sub-characteristics**
- **CISQ conforms to ISO 25010 quality characteristic definitions**
- **ISO 25023 defines measures, but not at the source code level**
- **CISQ supplements ISO 25023 with source code level measures**



CISQ defined automatable measures for quality characteristics highlighted in blue

Trustworthy Systems Manifesto

As a greater portion of mission, business, and safety critical functionality is committed to software, we hold the following propositions as paramount:

1. **Engineering discipline in product and process**
2. **Quality assurance to risk tolerance thresholds**
3. **Traceable provenance of all system components**
4. **Proactive defense of the system and its data**
5. **Resilient and safe operations**

CISQ Membership is Free www.it-cisq.org

CISQ
Consortium for IT Software Quality

FOUNDED BY:
Software Engineering Institute
Carnegie Mellon
OMG
OBJECT MANAGEMENT GROUP®

FAQs Contact Us
Search
Member Login

Standards | Programs | Use Cases | Members Area | Events | About CISQ

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 introducing computable metrics standards 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 to reduce cost and risk.

Visit the Cyber Resilience Summit Knowledge Repository

Become a CISQ:

- Member → CISQ Members Area
- Sponsor → CISQ Events

CISQ Sponsors

CGI | CAST | Cognizant | SHPI | Northrop Grumman | Synopsys | Tech Mahindra

Upcoming Events

SYSTEMS ENGINEERING RESEARCH CENTER

SERC TALKS

UPCOMING TALKS:

"Systems and Software Qualities Tradespace Analysis" Series

"Why Are Ontologies and Languages for Software Quality Increasingly Important?"

Xavier Franch, Full Professor, Polytechnic University of Catalonia (BarcelonaTech)

December 11 | 1:00 PM ET

Please visit the SERC Talks page for more information and updates.

SERC Annual Events | November 7-8

10 YEARS of SERC

Recognizing a decade of contributions to systems engineering research

WEDNESDAY
NOVEMBER
7 2018

SERC DOCTORAL STUDENTS FORUM

Reception to immediately follow at 5pm

Time: 12:00 - 5:00PM

THURSDAY
NOVEMBER
8 2018

SERC SPONSOR RESEARCH REVIEW

Time: 8:00AM - 5:00PM

LOCATION: FHI360 CONFERENCE CENTER
1825 CONNECTICUT AVE NW, 8TH FLOOR,
WASHINGTON, DC 20009

REGISTER TODAY

Events are free to Academia and Government participants; Industry attendees are charged a nominal fee.

sercuarc.org/event/sdsf-2018
sercuarc.org/event/ssrr-2018

Deadline to Register: October 26

We invite you to visit the collections of research reviews online: ***https://sercuarc.org/research-reviews/***

FOR MORE INFORMATION:
Ms. Monica Brito
mbrito@stevens.edu

SYSTEMS ENGINEERING RESEARCH CENTER

SERC TALKS

Thank you for joining us!

Please check back on the SERC website for today's recording and future SERC Talks information!

Subscribe and follow SERC on these channels:

CONTACT

Editor-in-Chief: Dr. Barry Boehm, University of Southern California – boehm@usc.edu

Webinar Coordinator: Ms. Mimi Marcus, Stevens Institute of Technology – SERCtalks@stevens.edu