Software Security Issues in the Industrial Internet

Dr. Bill Curtis
Executive Director
CISQ
Consortium for IT Software Quality

What is CISQ?

CISQ Consortium for IT Software Quality

Carnegie Mellon Software Engineering Institute

OMG OBJECT MANAGEMENT GROUP

Co-founders

IT Executives → **CISQ** ← **Technical Experts**

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

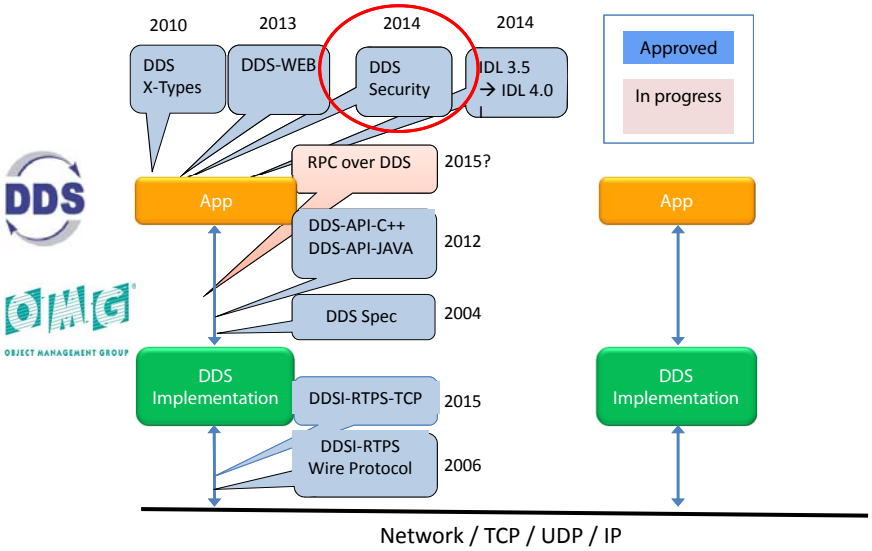
accenture · Cognizant · Booz | Allen | Hamilton strategy and technology consultants · CAST Achieve Insight. Deliver Excellence. · HUAWEI

CISQ
Consortium for IT Software Quality

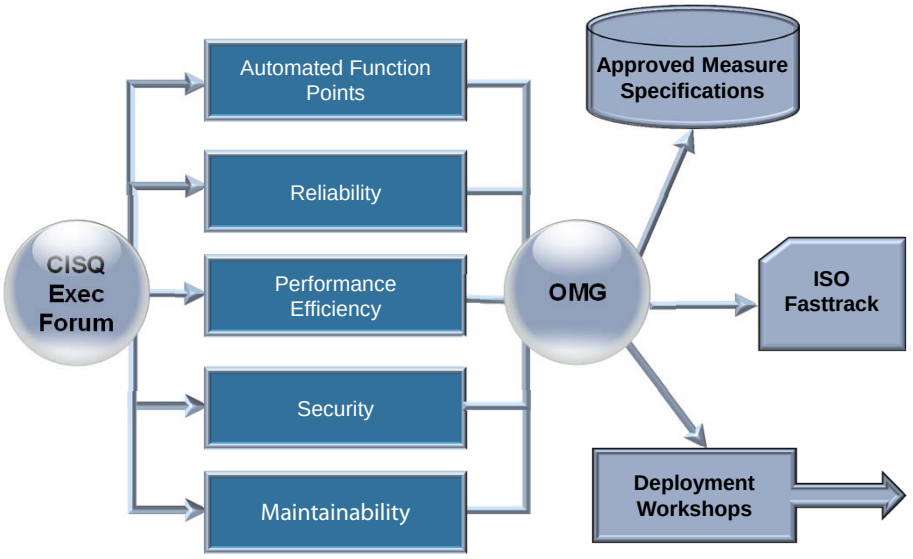
Medium	Issues	Standards
Policy	Who controls content, links, storage, etc.	??
Message	Format, encryption, exchange, etc.	DDS
Communication	Networks, Wifi, cables, sensor hubs,	DDS
Software	Weaknesses, vulnerabilities, etc.	CISQ
Hardware	Authentic, dependable	Manufacturer?

CISQ
Consortium for IT Software Quality

DDS Specification Family



CISQ/OMG Standards Process



January 1, 2016 5

CISQ Measures Violations

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

January 1, 2016 6

Top 22 CWEs in the Security Measure

- **CWE-22** Path Traversal Improper Input Neutralization
- **CWE-78** OS Command Injection Improper Input Neutralization
- **CWE-79** Cross-site Scripting Improper Input Neutralization
- **CWE-89** SQL Injection Improper Input Neutralization
- **CWE-120** Buffer Copy without Checking Size of Input
- **CWE-129** Array Index Improper Input Neutralization
- **CWE-134** Format String Improper Input Neutralization
- **CWE-252** Unchecked Return Parameter of Control Element Accessing Resource
- **CWE-327** Broken or Risky Cryptographic Algorithm Usage
- **CWE-396** Declaration of Catch for Generic Exception
- **CWE-397** Declaration of Throws for Generic Exception
- **CWE-434** File Upload Improper Input Neutralization
- **CWE-456** Storable and Member Data Element Missing Initialization
- **CWE-606** Unchecked Input for Loop Condition
- **CWE-667** Shared Resource Improper Locking
- **CWE-672** Expired or Released Resource Usage
- **CWE-681** Numeric Types Incorrect Conversion
- **CWE-706** Name or Reference Resolution Improper Input Neutralization
- **CWE-772** Missing Release of Resource after Effective Lifetime
- **CWE-789** Uncontrolled Memory Allocation
- **CWE-798** Hard-Coded Credentials Usage for Remote Authentication
- **CWE-835** Loop with Unreachable Exit Condition ('Infinite Loop')

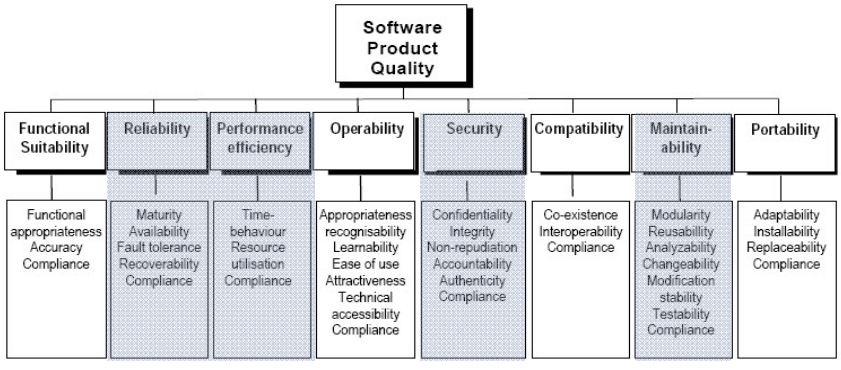
Robert Martin
MITRE

Common Weakness Enumeration
cwe.mitre.org

7

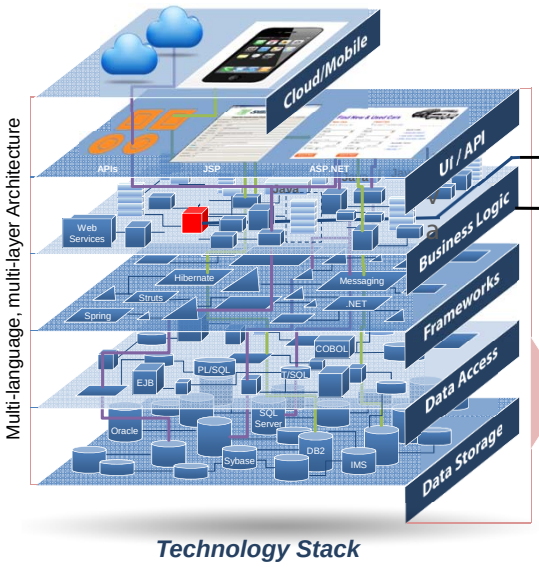
How Do CISQ Measures Relate to ISO?

- ISO 25000 series replaces ISO/IEC 9126 (Parts 1-4)
- 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

CISQ Measures the 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

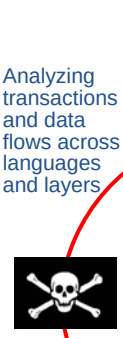
3 System Level

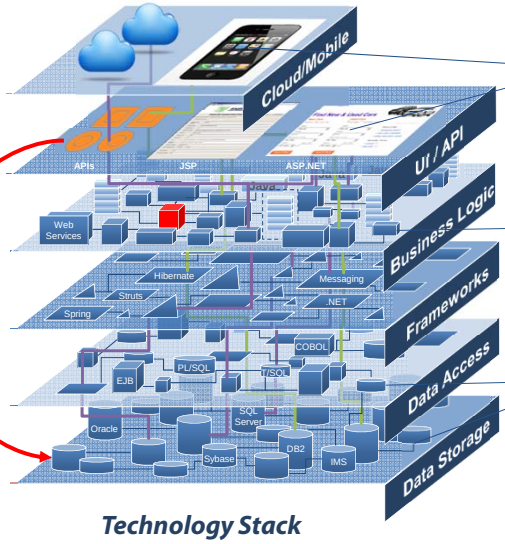
- Integration quality
- Architectural compliance
- Risk propagation
- Application security
- Resiliency checks
- Transaction integrity
- Function point,
- Effort estimation
- Data access control
- SDK versioning
- Calibration across technologies
- IT organization level

Challenges in the Technology Stack

Multi-language, Multi-layer Architecture

Analyzing transactions and data flows across languages and layers





Entry

Filtering, Authentication

Access

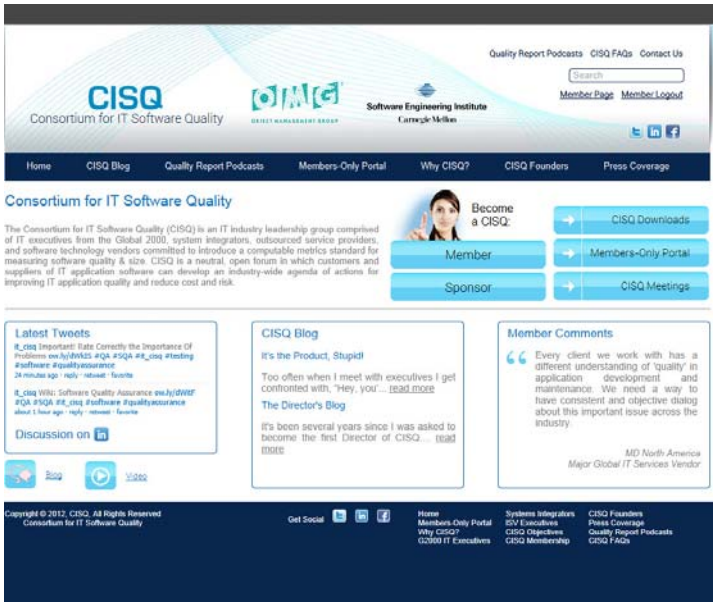
10

CISQ Observations on the Security Measure

- **High correlation between Security and Reliability weaknesses**
  - **Constructs that can crash the system can also provide pathways to unauthorized access**
  - **Poor quality code is insecure code (Carol Woody's research at SEI)**
- **Greater challenges in automated detection of some security weaknesses compared to detecting many other quality characteristics**

11

CISQ Membership is Free www.it-cisq.org



12