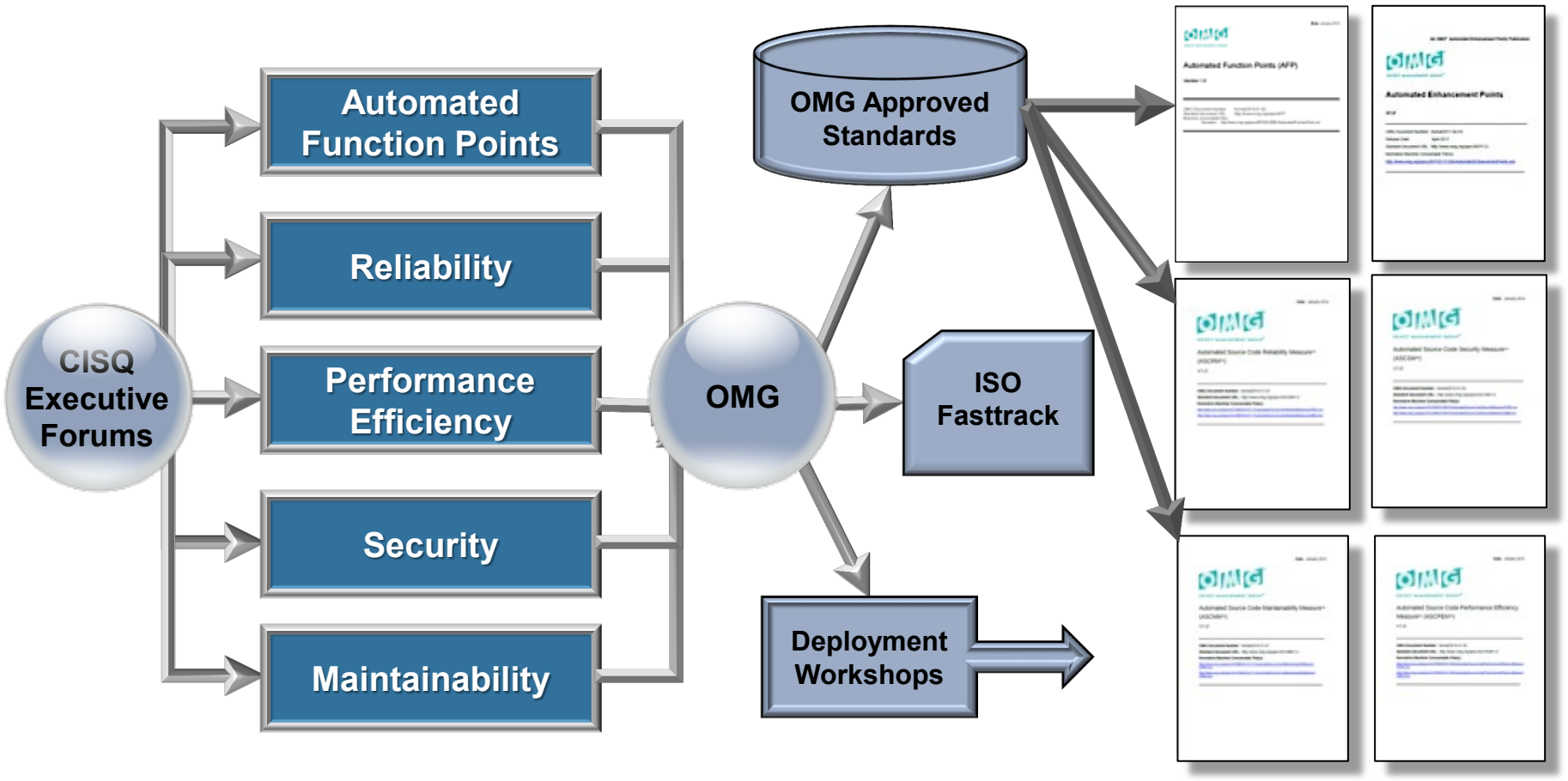
CISQ™

Consortium for Information & Software Quality

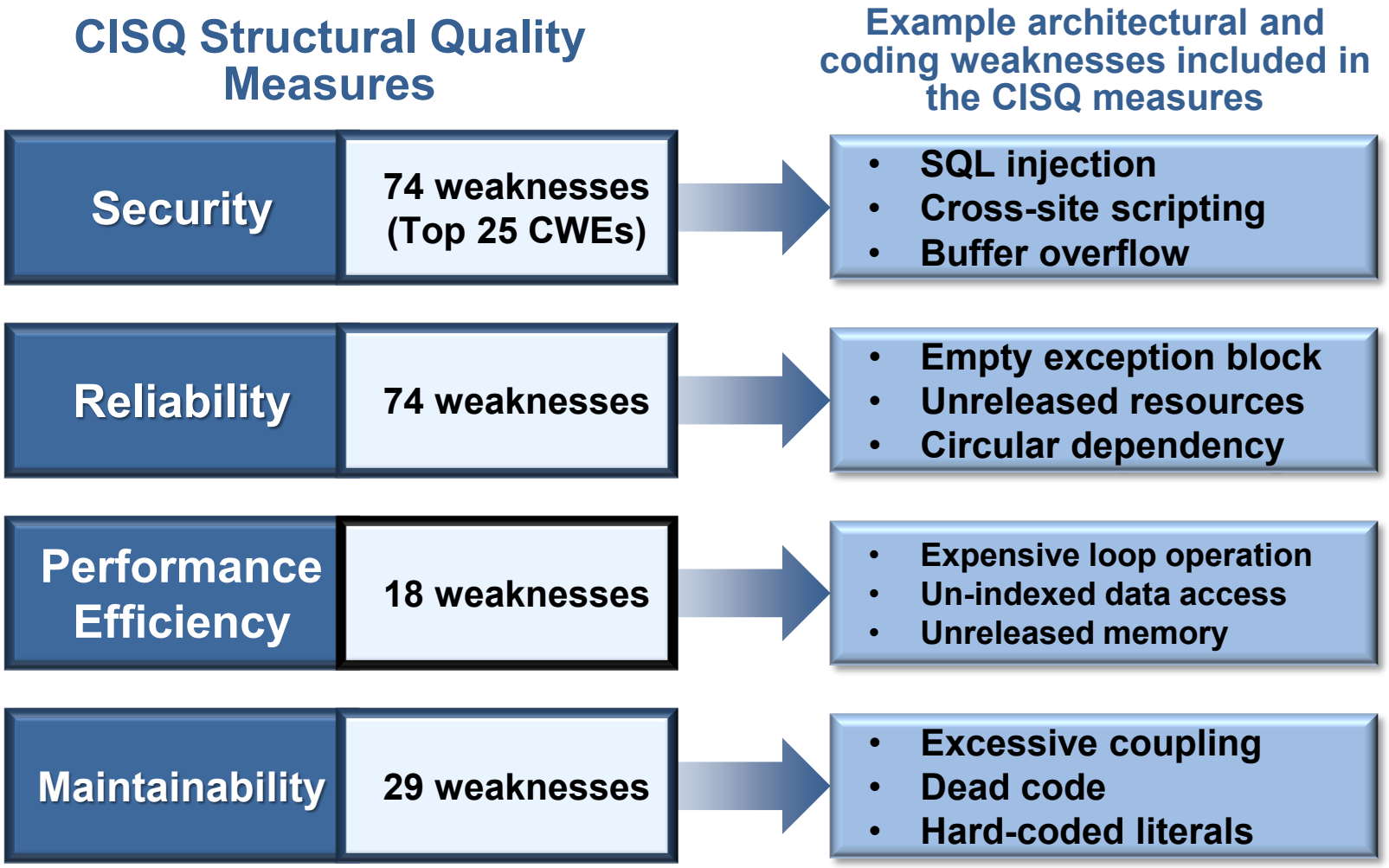
Model Based System Engineering (MBSE) Quality

Dave Norton
Executive Director

What We Do



Typical Areas for CISQ



An international team of experts selected the weaknesses to include in CISQ measures based on the severity of their impact on operational problems or cost of ownership.

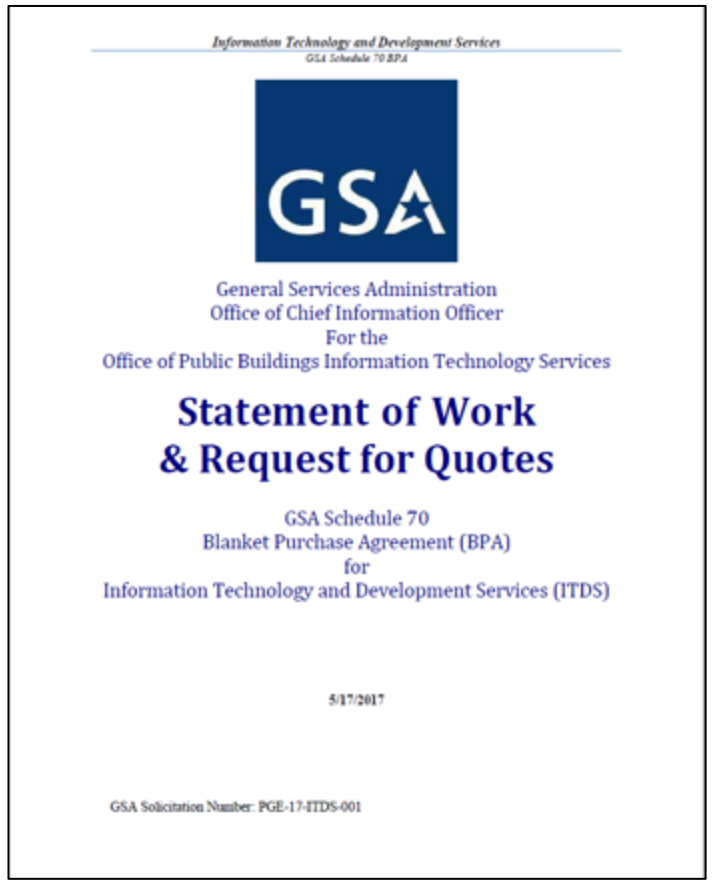
Only weaknesses considered severe enough that they must be remediated were included in the OMG standards.

The OMG standards are being submitted to ISO 25000.

CISQ
Consortium for Information & Software Quality™

We Make it Practical

Sample RFP



Information Technology and Development Services
GSA Schedule 70 BPA

GSA

General Services Administration
Office of Chief Information Officer
For the
Office of Public Buildings Information Technology Services

Statement of Work & Request for Quotes

GSA Schedule 70
Blanket Purchase Agreement (BPA)
for
Information Technology and Development Services (ITDS)

5/17/2017

GSA Solicitation Number: PGE-17-ITDS-001

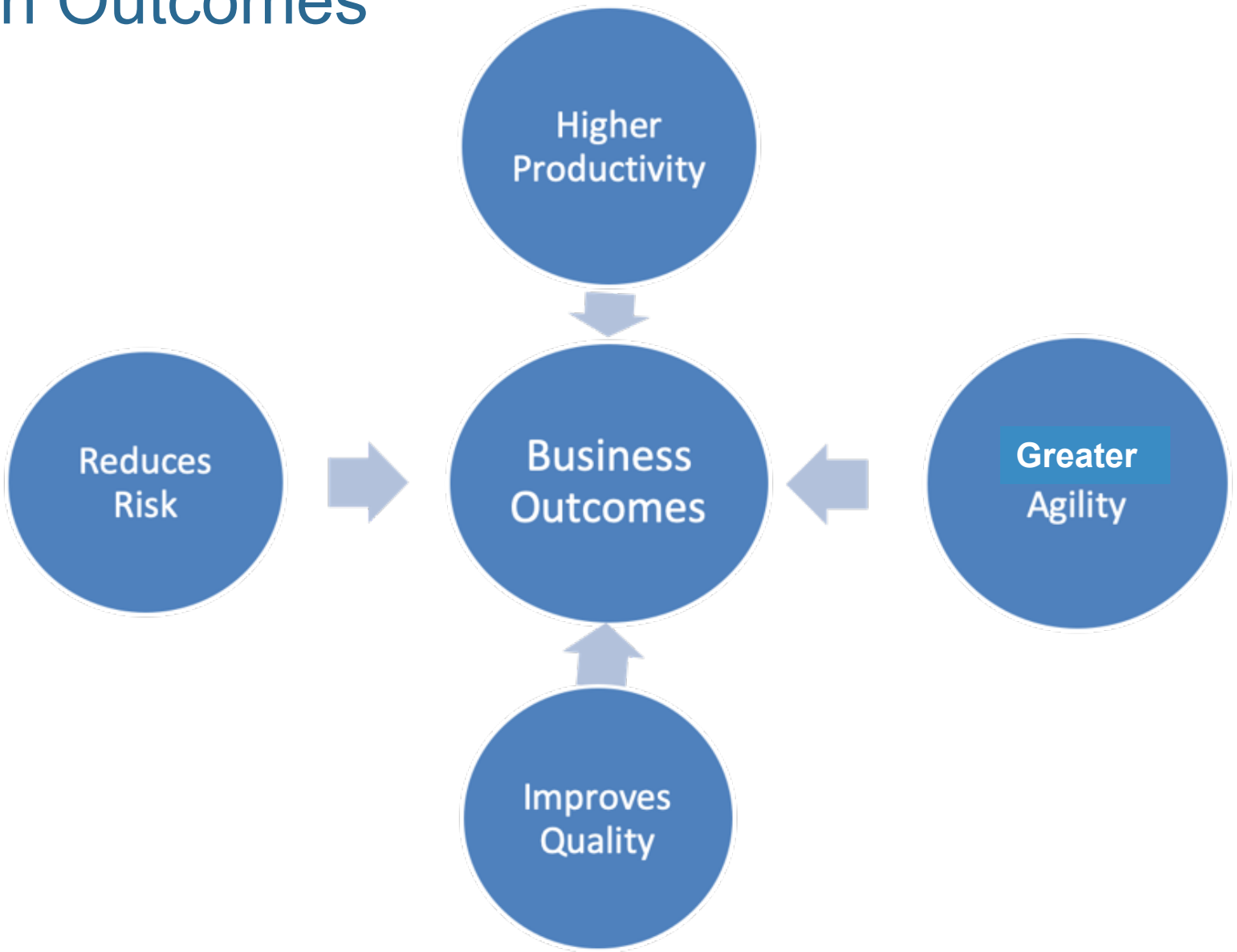
CISQ has been referenced by the U.S. General Services Administration (GSA), formally citing CISQ requirements in a Information Technology (IT) statement of work from the Office of the CIO for the Office of Public Buildings. GSA is an independent agency of the U.S. government that supports general services of Federal agencies.

See page 21, section 5.9 in GSA's document, Schedule 70 Blank Purchase Agreement for IT and Development Services…

"PB-ITS (Project Based IT Services) is seeking to establish code quality standards for its existing code base, as well as new development tasks. As an emerging standard, PB-ITS references the Consortium for Information Software Quality (CISQ) for guidance on how to measure, evaluate and improve software."

CISQ
Consortium for Information & Software Quality™

Focus on Outcomes



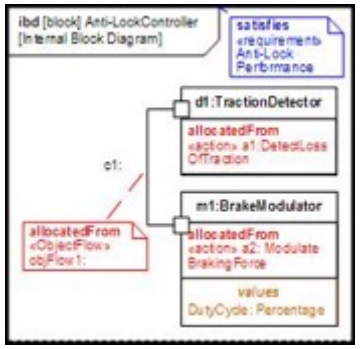
CISQ Membership

Recap on MBSE

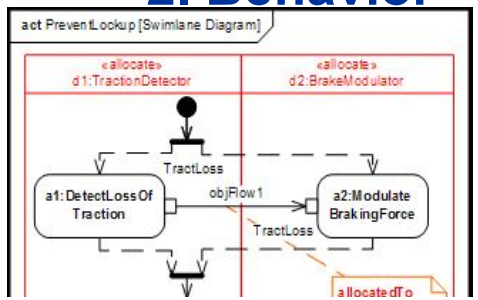
Model	Based	Systems	Engineering
Ontology	Analysis	Operational Engineering	Process
Abstraction	Decisions	CPS	Practices
Semantics	Planning	SoS	Methods
Syntax	Risk	Social	Frameworks
Algorithms	Collaboration		Maturity Models
Viewpoints	Implementation		
Authoritative	Support		

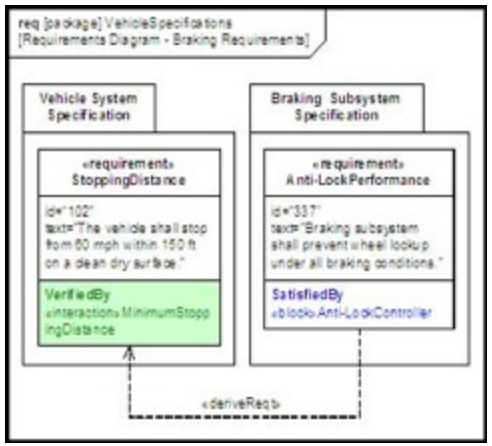
OMG SysML Narrowing the Conceptual Gap

1. Structure

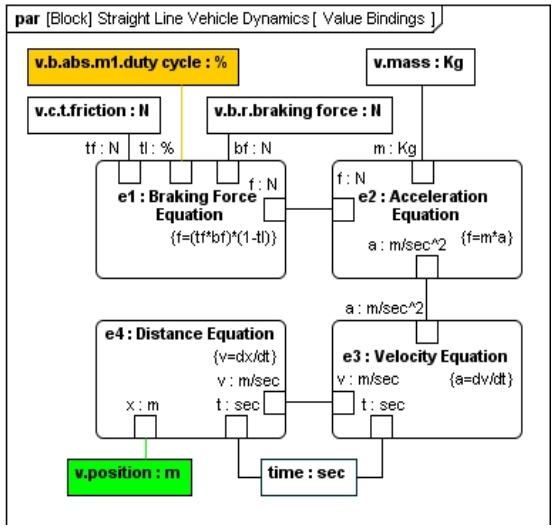


2. Behavior

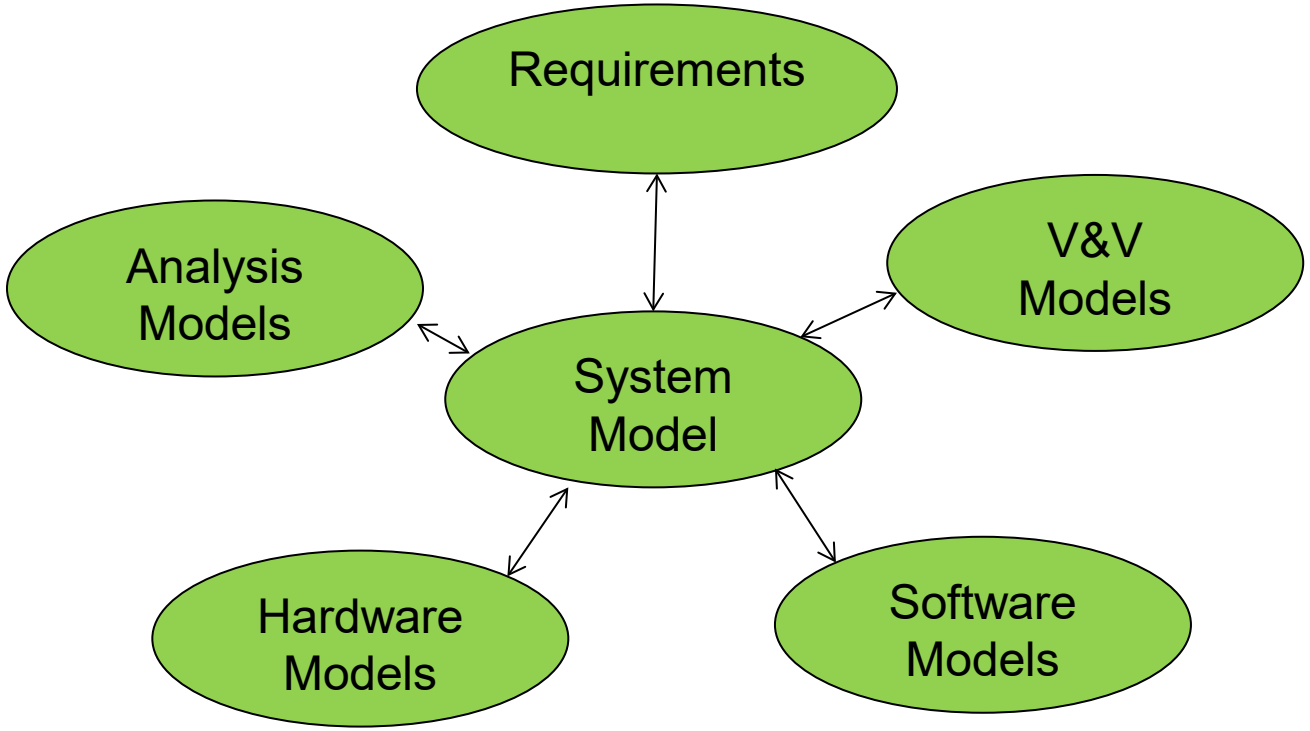




3. Requirements



4. Parametrics



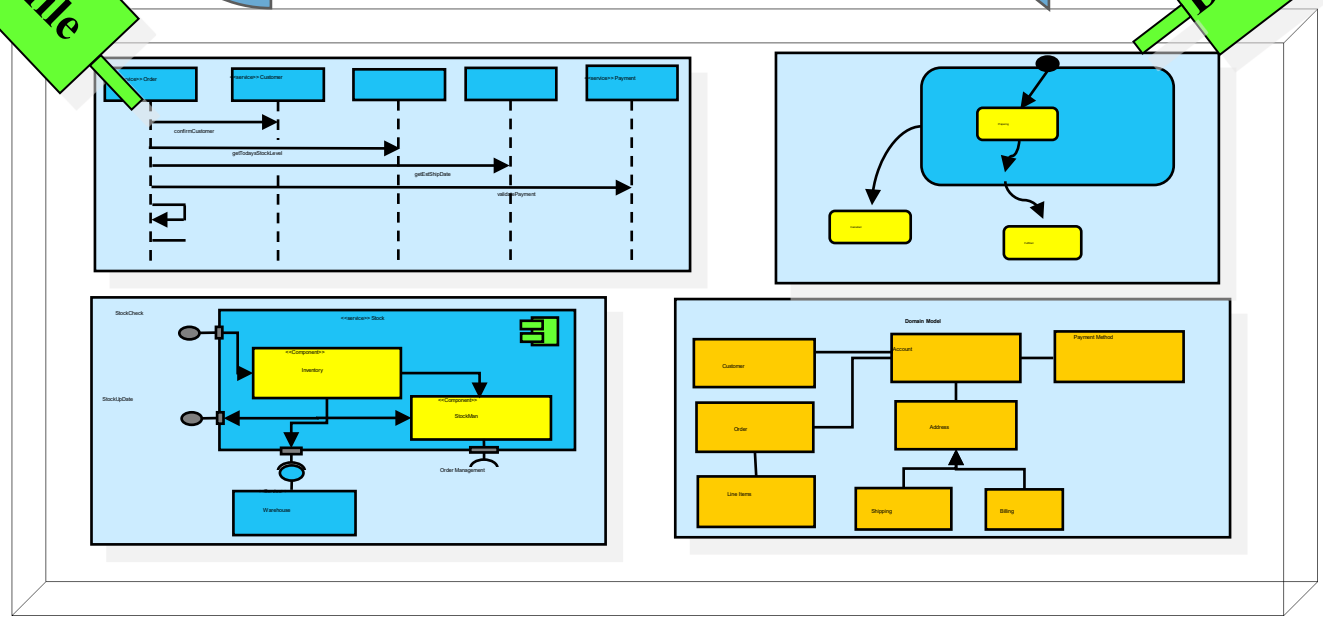
CISQ
Consortium for Information & Software Quality™

Physical World

Quality Profile

Domain Profiles

System Model

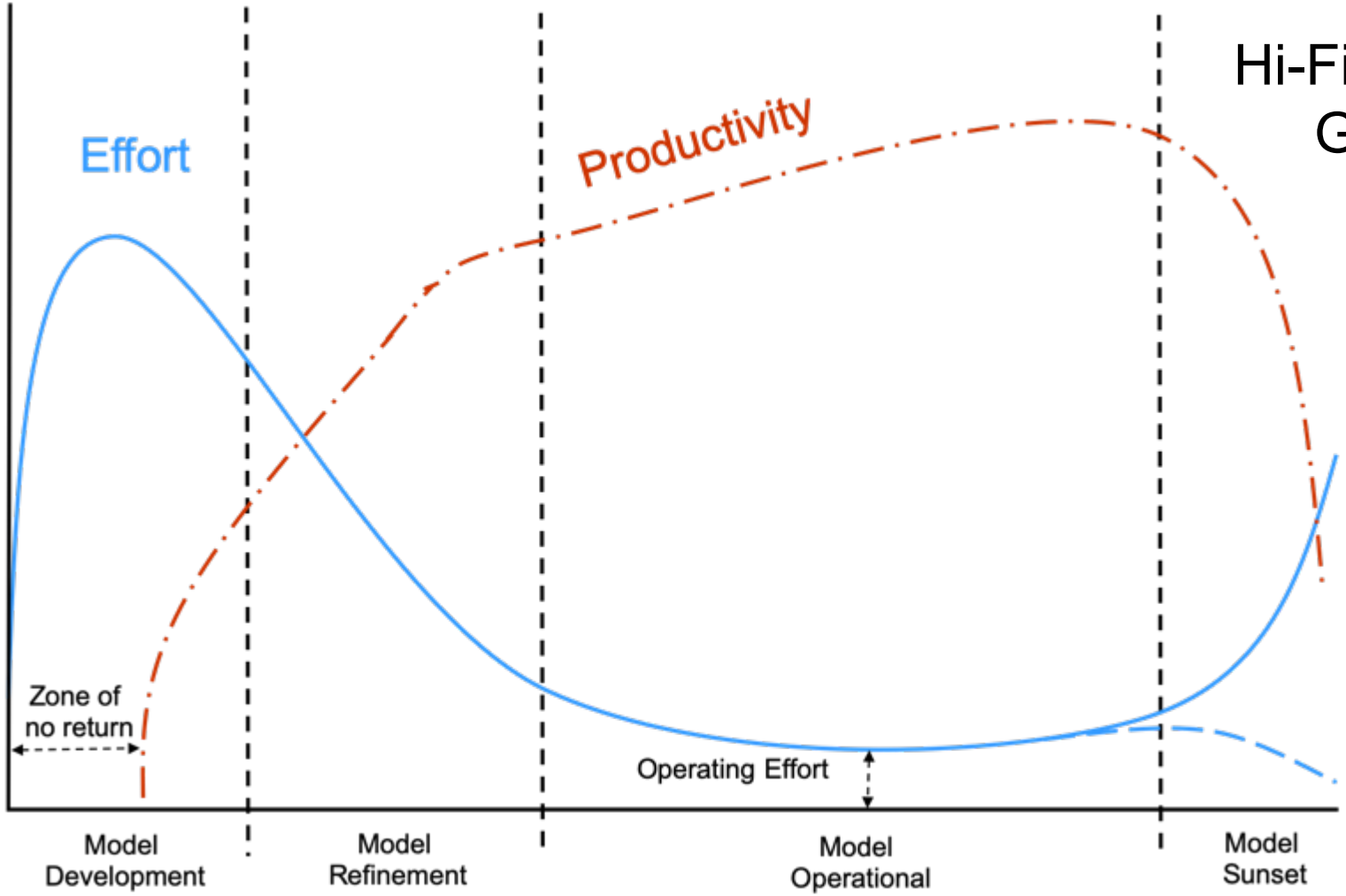


The Model is ***Marked*** up ready for transformation,

Architect

(Model element mapping)

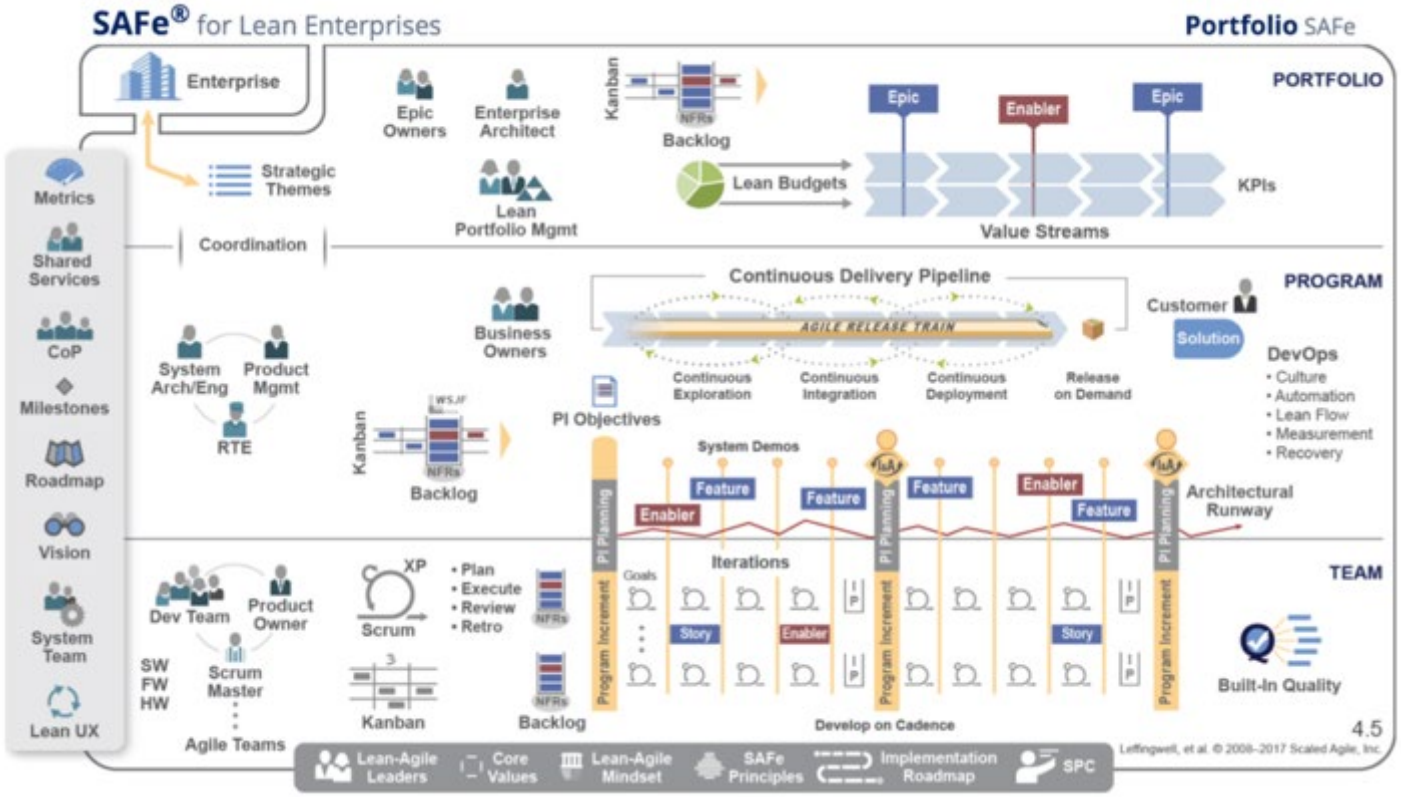
MBSE Is For Life, Not Just Initial Development



Hi-Fidelity MBSE Models Have Greater Value and Utility

CISQ
Consortium for Information & Software Quality™

MBSE and Enterprise Agile

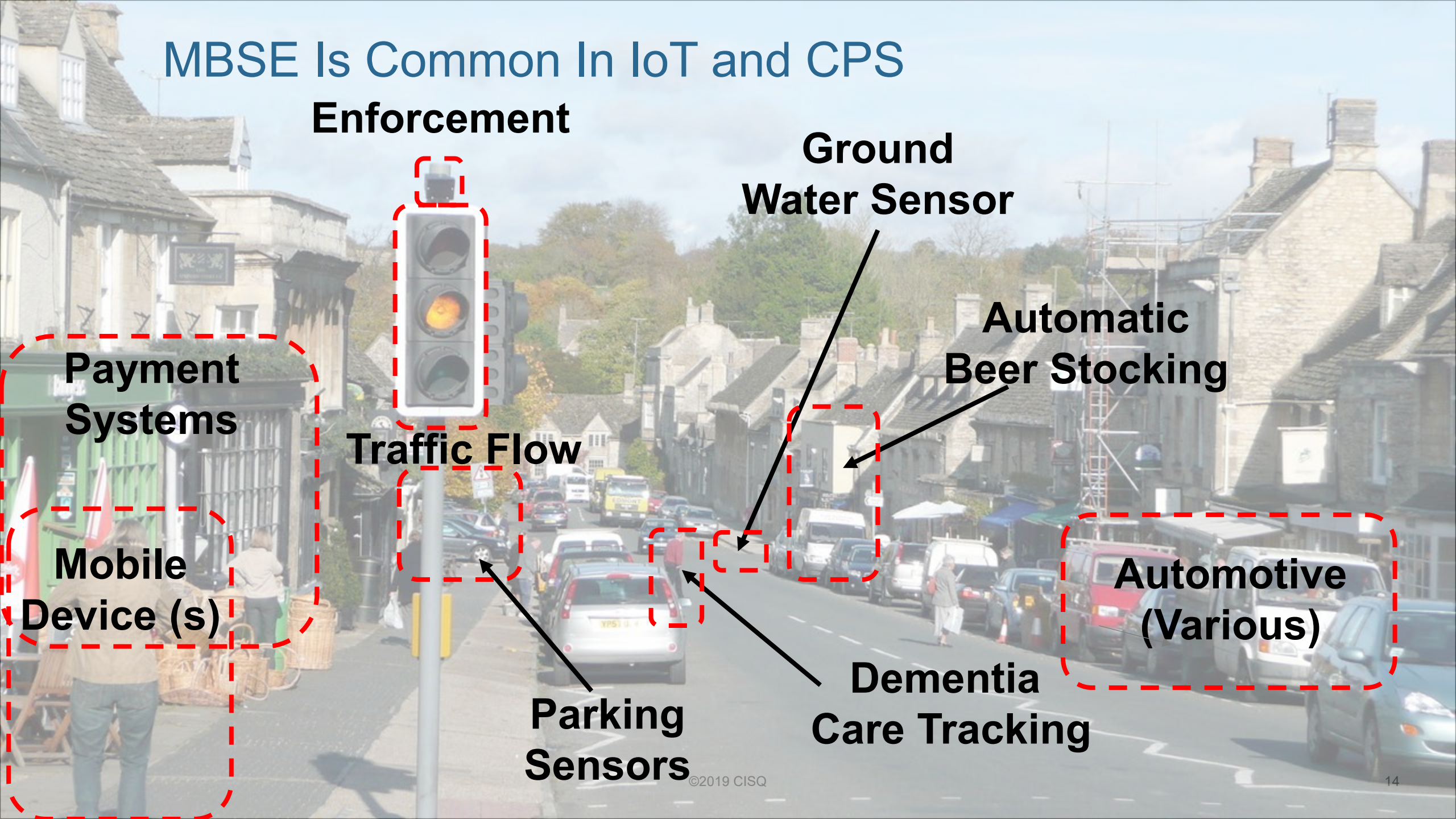


SAFe has the concept of MBSE.

You can use MBSE without a enterprise agile framework, but it is harder.

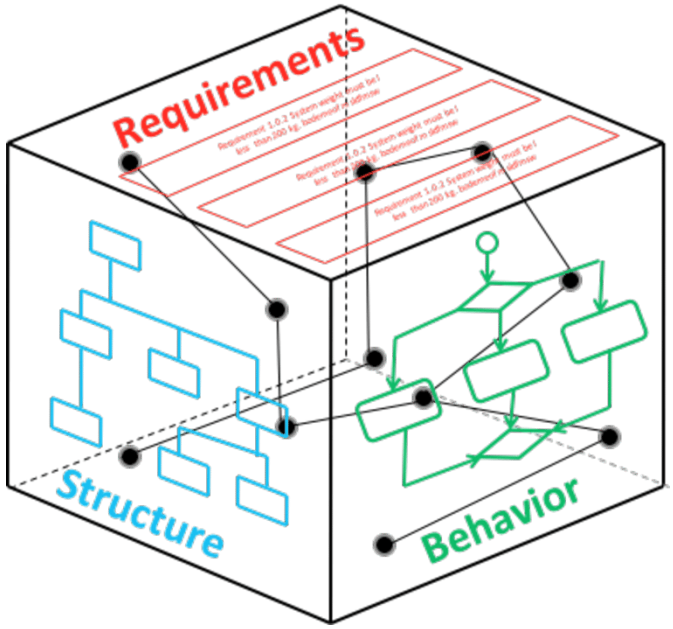
Why The Increasing Interest ?

MBSE Is Common In IoT and CPS



So What's The Problem ?

Model Generated Code Needs To Be Of High Quality



avaJava.com Web Tutorials - Eclipse

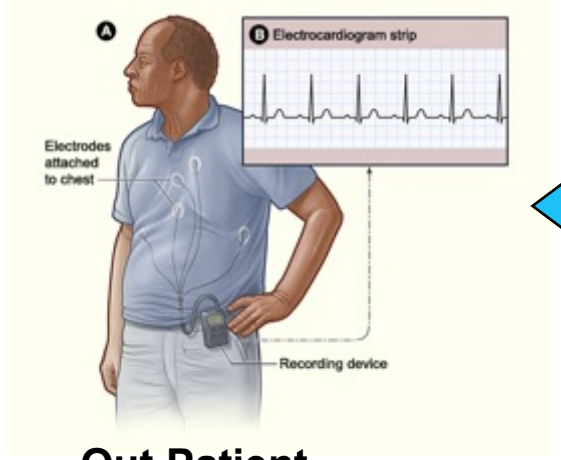
TestServlet.java

```
1  package my;
2
3  import java.io.IOException;
4
5  import javax.servlet.Servlet;
6  import javax.servlet.ServletException;
7  import javax.servlet.http.HttpServlet;
8  import javax.servlet.http.HttpServletRequest;
9  import javax.servlet.http.HttpServletResponse;
10
11 public class TestServlet extends HttpServlet implements Servlet {
12     static final long serialVersionUID = 1L;
13
14     public TestServlet() {
15         super();
16     }
17
18     protected void doGet(HttpServletRequest request,
19             HttpServletResponse response) throws ServletException, IOException {
20         doPost(request, response);
21     }
22
23     protected void doPost(HttpServletRequest request,
24             HttpServletResponse response) throws ServletException, IOException {
25         response.getWriter().println("blah");
26     }
27 }
```

How do I create a profile to format Java code in Eclipse?

A Digital Ecosystem is a System of Systems –A Weakness In One Can Be A Weakness In All

For Example In Banking Over 21% Of Incidents 3rd Party Related (UK FCA 2019)



Out Patient

Mobile Device

Telecommunication Network

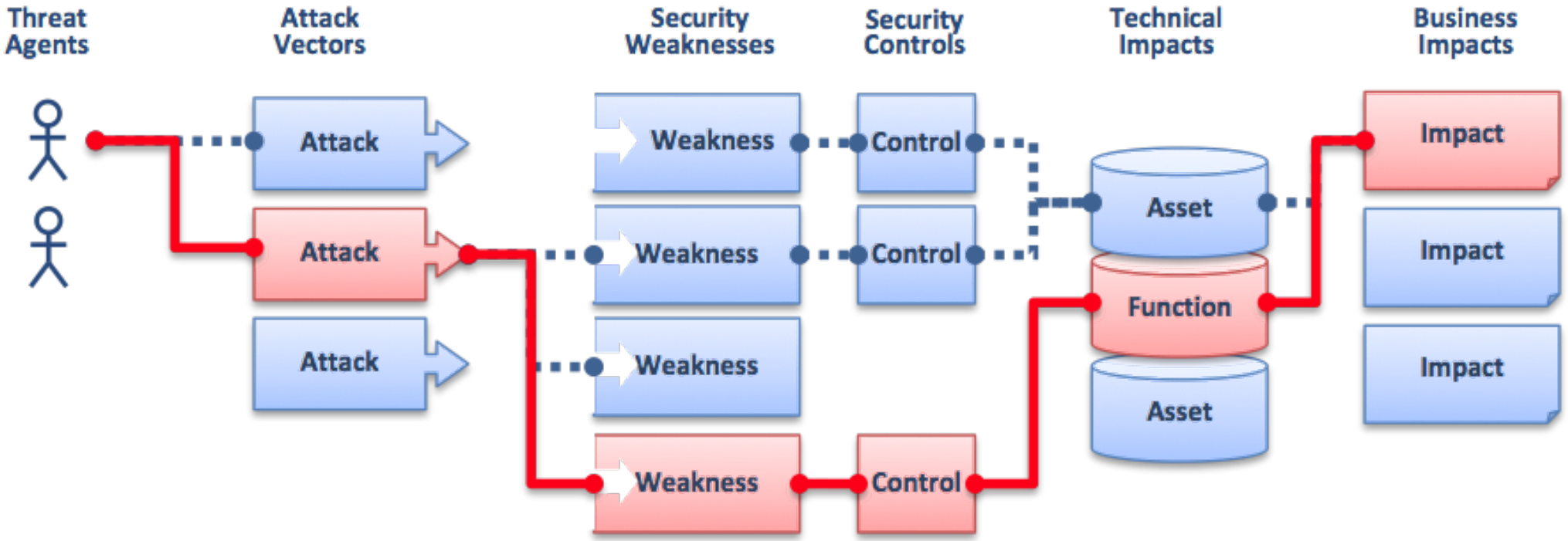
Local Doctor Patient System

Emergency Services

Cardiovascular Monitor Application

Healthcare Provider

MBSE & Digital Twins Are The New Attack Vector, The Greater The Model Fidelity The Greater The To An Attacker

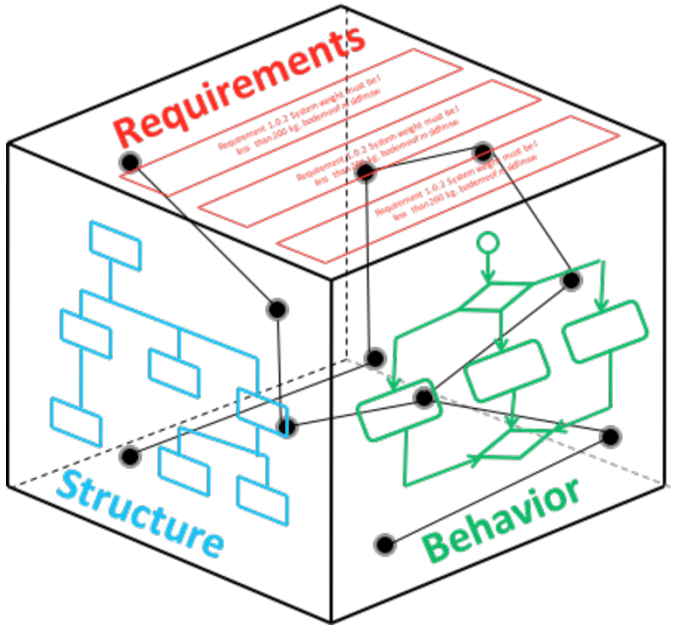


Bottom Line – Poor Model Leads To Poor Outcomes

Higher Carbon Foot Print

Poor Performance

Harder To Maintain



Higher TCO

Poor Reliability

Poor Security

Low Trustworthiness

So What Is CISQ Doing About It ?

Build On What Have – CISQ Quality Standards Based On Common Weakness Enumeration (CWE) & Technical Debt

CWE is an enumeration (list) of software architecture, design, or **code** weaknesses.

Weaknesses are defined as flaws, bugs, faults, or other errors, that create vulnerabilities that can be exploited by both internal and external forces.

Weaknesses can be found in software implementation, **code**, design, and architecture

CWE Analysis Already Best Practice At The Code Level

- **OWASP Top 10 Vulnerabilities**—most critical web application security risks – CWEs & CVEs
- **OWASP Application Security Verification Std v4.0** – 14 categories guide automated unit & integration tests – most all verification checks have corresponding CWEs
- **SANS/CWE Top 25** — most commonly encountered cyber weakness enumerators (CWEs),
- **CISQ Object Management Group (OMG)** Automated Source Code Measures for technical debt & structural quality (Security, Reliability, Performance Efficiency & Maintainability) – all based on CWEs

Shift-Left – Move Code Weakness and Vulnerability Analysis Into The Model

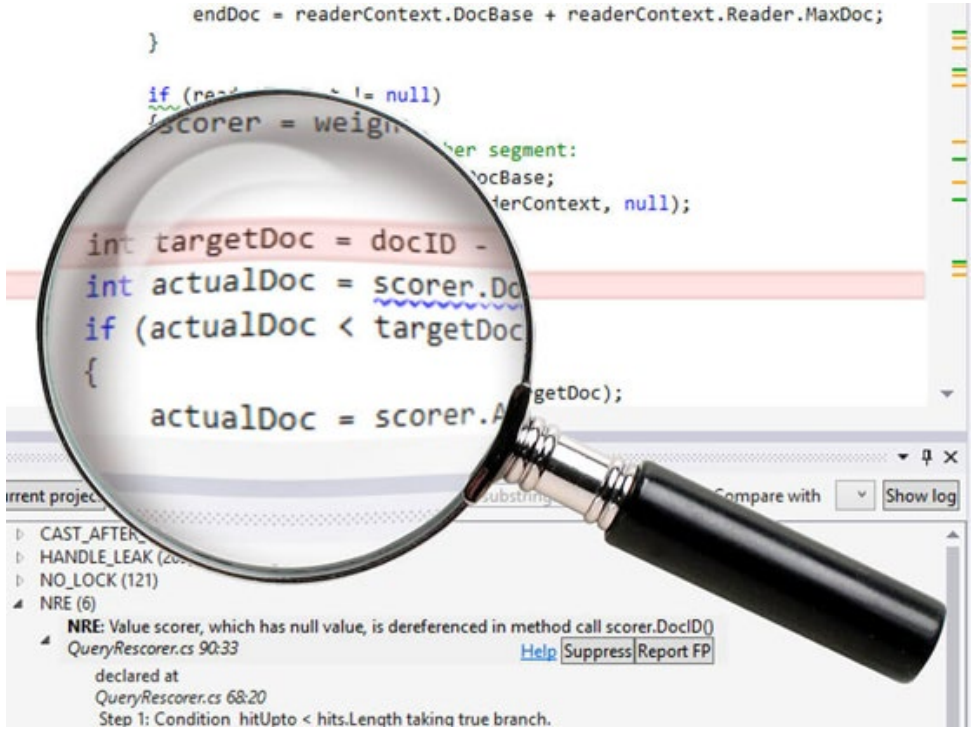
avaJava.com Web Tutorials - Eclipse

TestServlet.java

```
1  package my;
2
3  import java.io.IOException;
4
5  import javax.servlet.Servlet;
6  import javax.servlet.ServletException;
7  import javax.servlet.http.HttpServlet;
8  import javax.servlet.http.HttpServletRequest;
9  import javax.servlet.http.HttpServletResponse;
10
11 public class TestServlet extends HttpServlet implements Servlet {
12     static final long serialVersionUID = 1L;
13
14     public TestServlet() {
15         super();
16     }
17
18     protected void doGet(HttpServletRequest request,
19             HttpServletResponse response) throws ServletException, IOException {
20         doPost(request, response);
21     }
22
23     protected void doPost(HttpServletRequest request,
24             HttpServletResponse response) throws ServletException, IOException {
25         response.getWriter().println("blah");
26     }
27 }
```

How do I create a profile to format Java code in Eclipse?

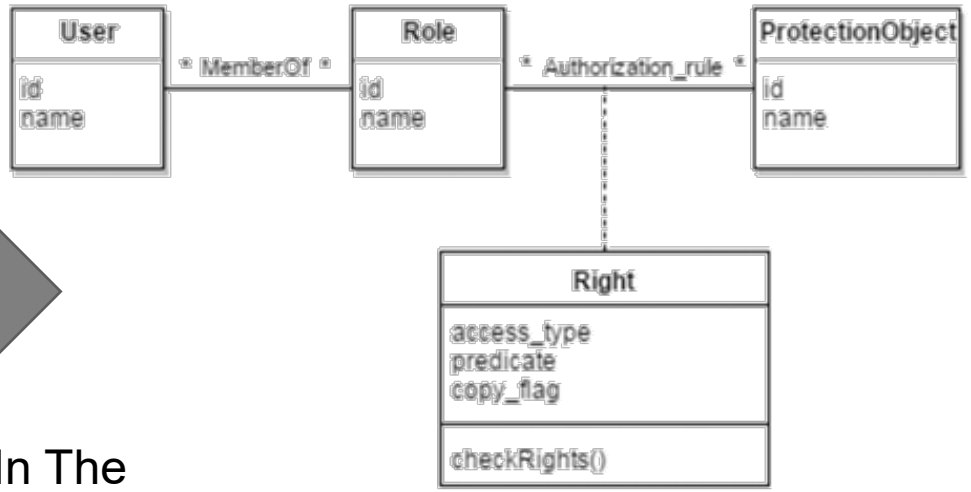
CWE Discovered At Code Level Using Static Analysis



CISQ
Consortium for Information & Software Quality™

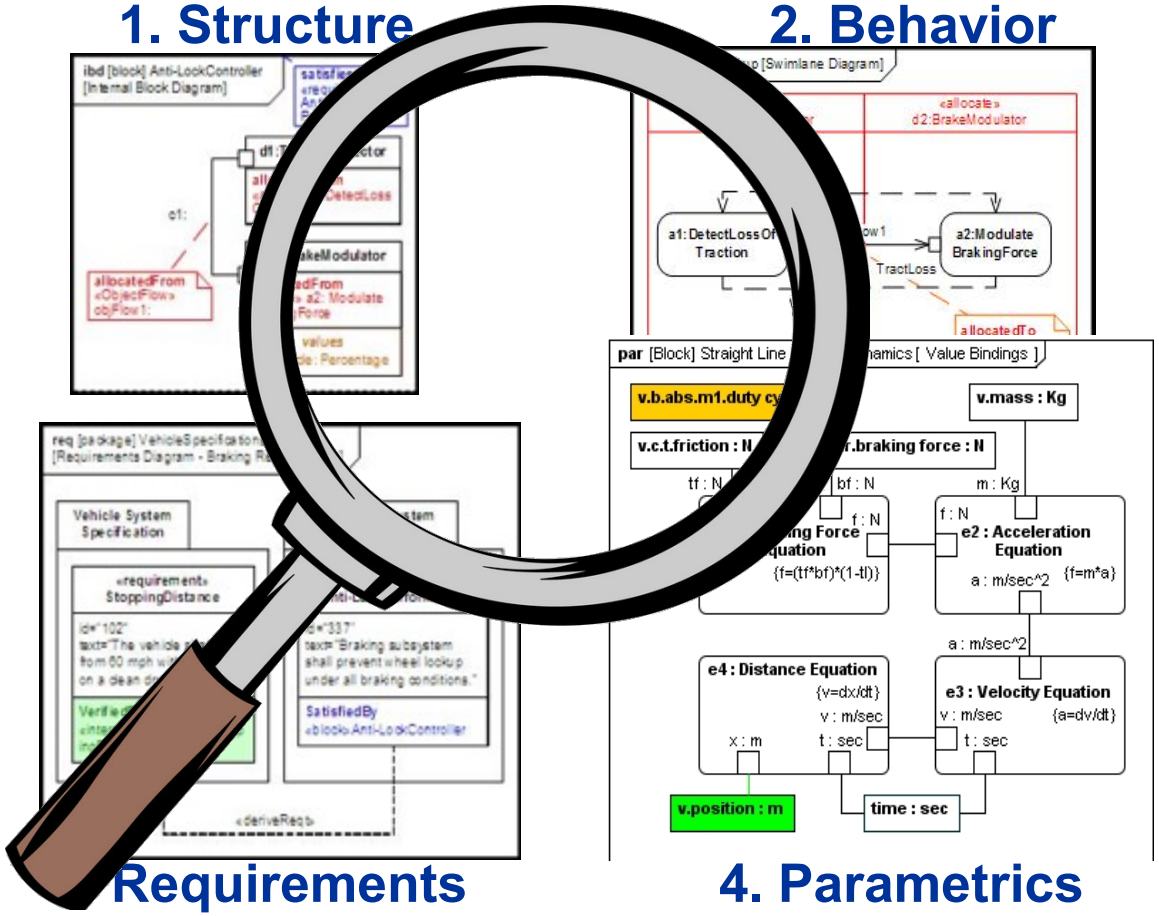
Formalize Normative Model Specification For The CWE's

CWE-284: Improper Access Control
Weakness ID: 284 Abstraction: Class, Structure: Simple
Description: The software does not restrict or incorrectly restricts access to a resource from an unauthorized actor.
Extended Description: Access control involves the use of several protection mechanisms such as: • Authentication (proving the identity of an actor) • Authorization (ensuring that a given actor can access a resource), and • Accountability (tracking of activities that were performed) When any mechanism is not applied or otherwise fails, attackers can compromise the security of the software by gaining privileges, reading sensitive information, executing commands, evading detection, etc. There are two distinct behaviors that can introduce access control weaknesses: • Specification: incorrect privileges, permissions, ownership, etc. are explicitly specified for either the user or the resource (for example, setting a password file to be world-writable, or giving administrator capabilities to a guest user). This action could be performed by the program or the administrator. • Enforcement: the mechanism contains errors that prevent it from properly enforcing the specified access control requirements (e.g., allowing the user to specify their own privileges, or allowing a syntactically-incorrect ACL to produce insecure settings). This problem occurs withinthe program itself, in that it does not actually enforce the intended security policy that the administrator specifies.



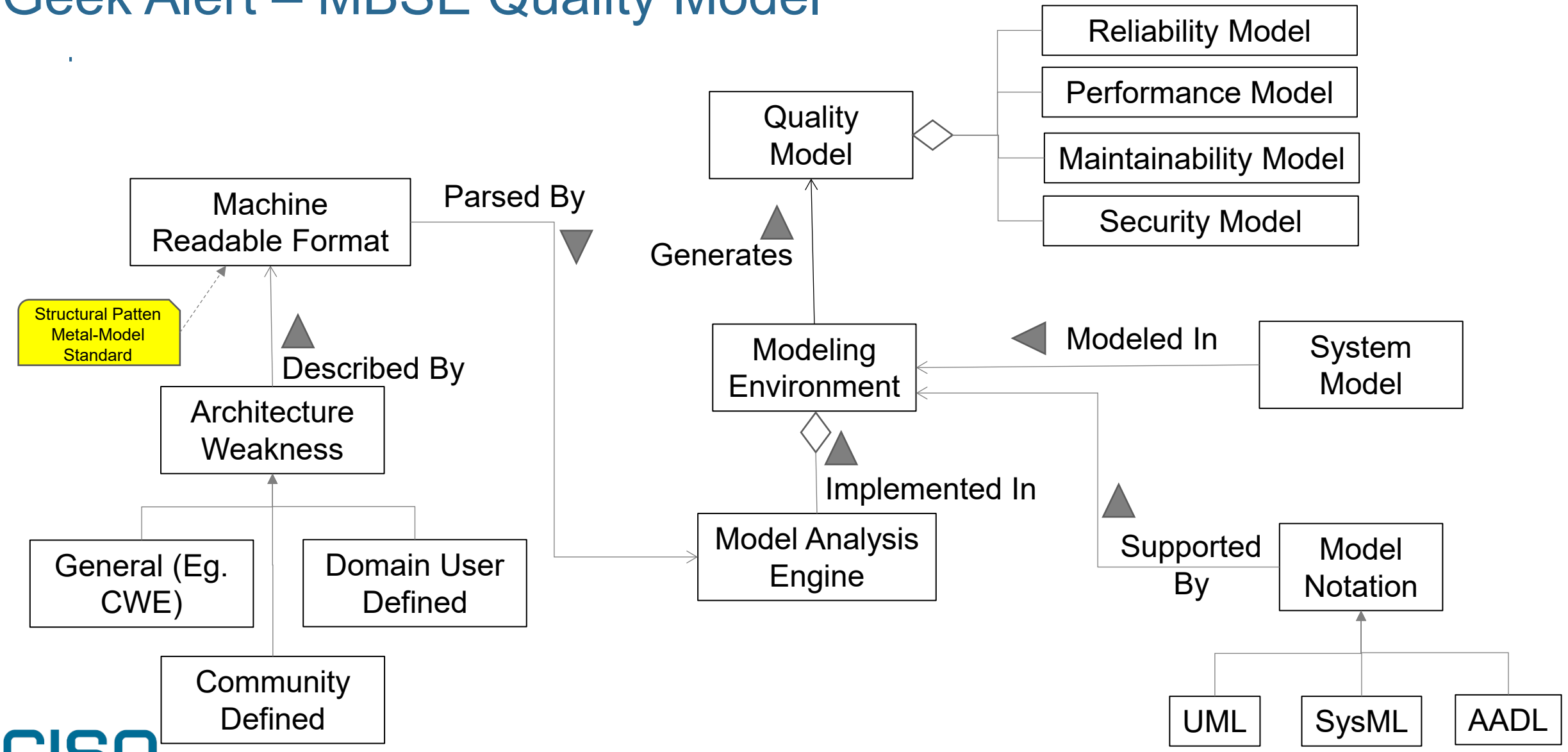
CWE Visible In The Model

The New Standard Will Allow CWE Analysis Before Anything Is Generated



CISQ
Consortium for IT Software Quality™

Geek Alert – MBSE Quality Model



What Will The Standard Give You ?

- Model Validation Earlier In the MBSE Life Cycle - 1:40 to 1:60 ratio in cost compared to code review and testing
- A Way Of Certifying The MBSE Environment Regard Generated (CWE) Code Weakness
- Certify Supplier MBSE Quality Against (CWE) Code Weakness
- Consistent Model Validation Across The Ecosystem
- Improved Quality, Lower Risk and Happier Customer

Help Us Develop The Next Generation Of Digital Standards

Individual Membership

Stay updated on this work and network with members in the community. Individual membership is free.

- Subscribe to CISQ's email list
- Receive updates on the standards
- Receive technical guidance documents
- Receive event invitations

Corporate Membership

Contribute to the standards and participate in deployment activities. Sponsorship is open to companies, government agencies, not-for-profit, and academic institutions.

- Team members participate in working groups
- An executive joins the Governing Board
- Your organization is listed as a supporter of all CISQ events, including complimentary passes and an exhibit table
- See benefits of corporate membership

CISQ
Consortium for IT Software Quality™

Thank You

 Founded 2010

 3,000+ members

 750+ companies

 7 adopted standards

 www.it-cisq.org

David Norton
Executive Director
david.norton@it-cisq.org

CISQ
Consortium for IT Software Quality™