The Software Assurance Ecosystem:

OMG's Approach to Systems & Software Assurance

Dr. Richard Mark Soley

Chairman and CEO

Object Management Group, Inc.

With thanks to the OMG Systems Assurance Domain Task Force, especially Dr. Ben Calloni

OMG
OBJECT MANAGEMENT GROUP

OMG's Mission

- Develop an architecture, using appropriate technology, for modeling & distributed application integration, guaranteeing:
  - reusability of components
  - interoperability & portability
  - basis in commercially available software
- Specifications *freely available*
- Implementations exist
- Member-controlled not-for-profit

OBJECT MANAGEMENT GROUP

Who Are OMG?

- Adaptive
- Atego
- Boeing
- Business Rules Group
- CA Technologies
- Citigroup
- CSC
- EADS
- EDS
- Energistics
- Fair, Isaac
- Firestar Software
- Fujitsu
- HCL
- Hewlett Packard
- Hitachi
- HSBC
- IBM
- Lockheed Martin
- MEGA International
- Microsoft
- MITRE
- Model Driven Solutions
- National Archives
- NEC
- NIST
- No Magic
- NTT DoCoMo
- Northrop Grumman
- OASIS
- OIS
- Oracle
- PrismTech
- Real-Time Innov.
- SAP
- TCS
- Tether's End
- THALES
- Unisys
- W3C

OMG OBJECT MANAGEMENT GROUP

OMG & Modeling

- Best known for key standards in modeling languages:
  - UML (broad software & systems)
  - SysML (systems engineering)
  - SoaML (service-oriented architectures)
  - BPMN (business processes)
  - CWM (data warehouses)
  - MOF (modeling languages)

OBJECT MANAGEMENT GROUP

OMG's Focus

- Three key "infrastructure" standards foci:
  - Modeling
  - Middleware
  - Real-time & other specialized systems
- More than 20 "vertical market" foci:
  - Healthcare
  - Financial services
  - Robotics
  - Etc.

OBJECT MANAGEMENT GROUP

OMG Systems Assurance Task Force

- The Task Force (SysA TF) is focusing across all OMG vertical applications domains
  - Existing: healthcare, finance, military, manufacturing, telecommunications, etc.
  - New: smart energy grid, automotive
- Three co-chairs
  - Ms. Djenana Campara, KDM Analytics
  - Dr. Ben Calloni, Lockheed Martin
  - Mr. Paul Work, Raytheon

OMG
OBJECT MANAGEMENT GROUP

SysA TF Strategy & Focus

- Strategy
  - Establish a common framework for analysis and exchange of information related to systems assurance and trustworthiness. This trustworthiness will assist in facilitating systems that better support Security, Safety, Software and Information Assurance

- Immediate focus of SysA TF is to complete work related to
  - Software Assurance (SwA) Ecosystem - **common framework for presenting and analyzing properties of system trustworthiness** that
    - leverages and connects existing OMG specifications and identifies new specifications that need to be developed to complete the framework
    - provides integrated tooling environments for different tool types
    - Is architected to improve software system analysis and achieve higher automation of risk analysis

Delivering System Assurance:

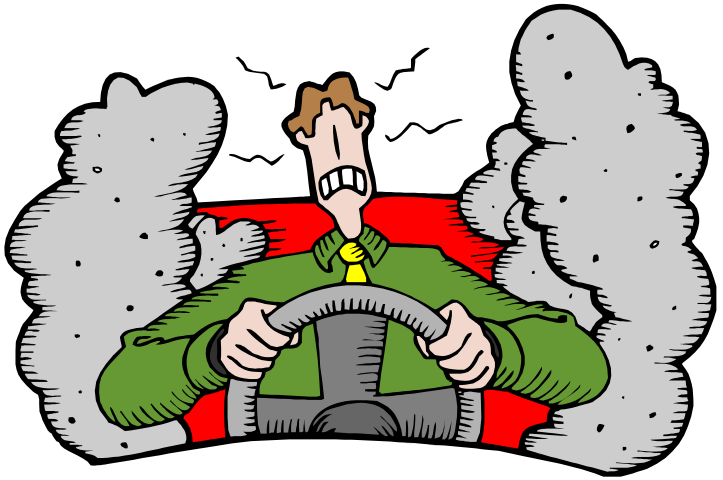
Delivering System Predictability and Reducing Uncertainty

- Software Assurance (SwA) is 3 step process
  1. **Specify Assurance Case**
     - Enable supplier to make **bounded assurance claims** about safety, security and/or dependability of systems, product or services
  2. **Obtain Evidence for Assurance Case**
     - Perform software assurance assessment to justify claims of meeting a set of requirements through a structure of sub-claims, arguments, and supporting evidence
     - Collecting Evidence and verifying claims' compliance is complex and costly process
  3. **Use Assurance Case to calculate and mitigate risk**
     - Exam non compliant claims and their evidence to calculate risk and identify course of actions to mitigate it
- Each stakeholder will have their own risk assessment – e.g. security, liability, performance, compliance

Currently, SwA 3 step process is informal, subjective & manual

Limitations of Current Assessment Approaches

- There is currently a lack of formalized methodology between high level policy claims and evidence means a laborious, unrepeatable (I.e., subjective), lengthy and costly certification process
- Current assessment approaches resist automation

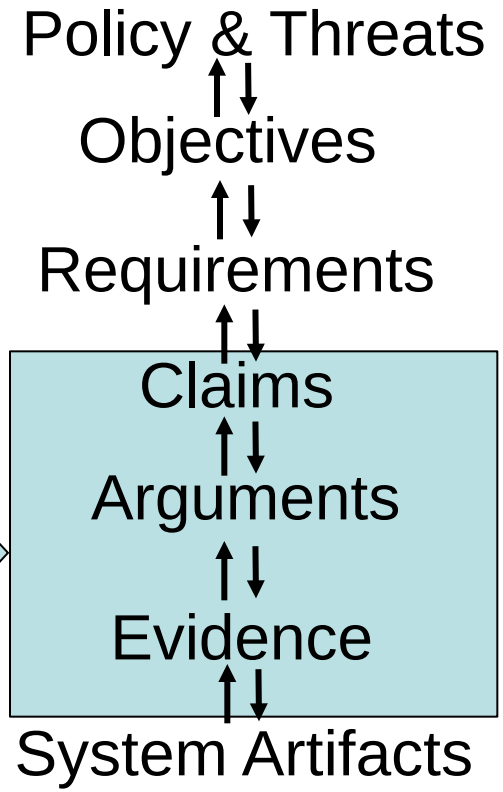


OMG OBJECT MANAGEMENT GROUP

The SwA Process

Claim:
"It rained last night!"

Methodology Gap



OBJECT MANAGEMENT GROUP

Improving System Assessments:
Systematic, Objective and Automated

Key Requirements:

1. Specified assurance compliance points through formal specification
2. Transparency of software process & systems
3. End-to-end Traceability: *from code to models to evidence to arguments to security requirements to policy*
4. Standards based Integrated tooling environment

Together, these requirements enable the management of system knowledge and knowledge about properties, providing a high degree of transparency, traceability and automation

OMG OBJECT MANAGEMENT GROUP

The Software Assurance Ecosystem: Turning Challenge into Solution

- The SwA Ecosystem is a formal framework for analysis and exchange of information related to software security and trustworthiness
- The SwA Ecosystem provides a technical environment in which formalized claims, arguments and evidence can be brought together with formalized and abstracted software system representations to support high automation and high fidelity analysis.
- The SwA Ecosystem is based entirely on ISO/OMG Open Standards:
  - Semantics of Business Vocabulary and Rules (SBVR)
  - Knowledge Discovery Metamodel (KDM)
  - Structure Metrics Metamodel (SMM)
  - Structured Assurance Case Metamodel (SACM) (Adopted June 2010)
    - Software Assurance Evidence Metamodel (SAEM)
    - Argumentation Metamodel (ARM)
- The SwA Ecosystem is architected with a focus on providing fundamental improvements in analysis

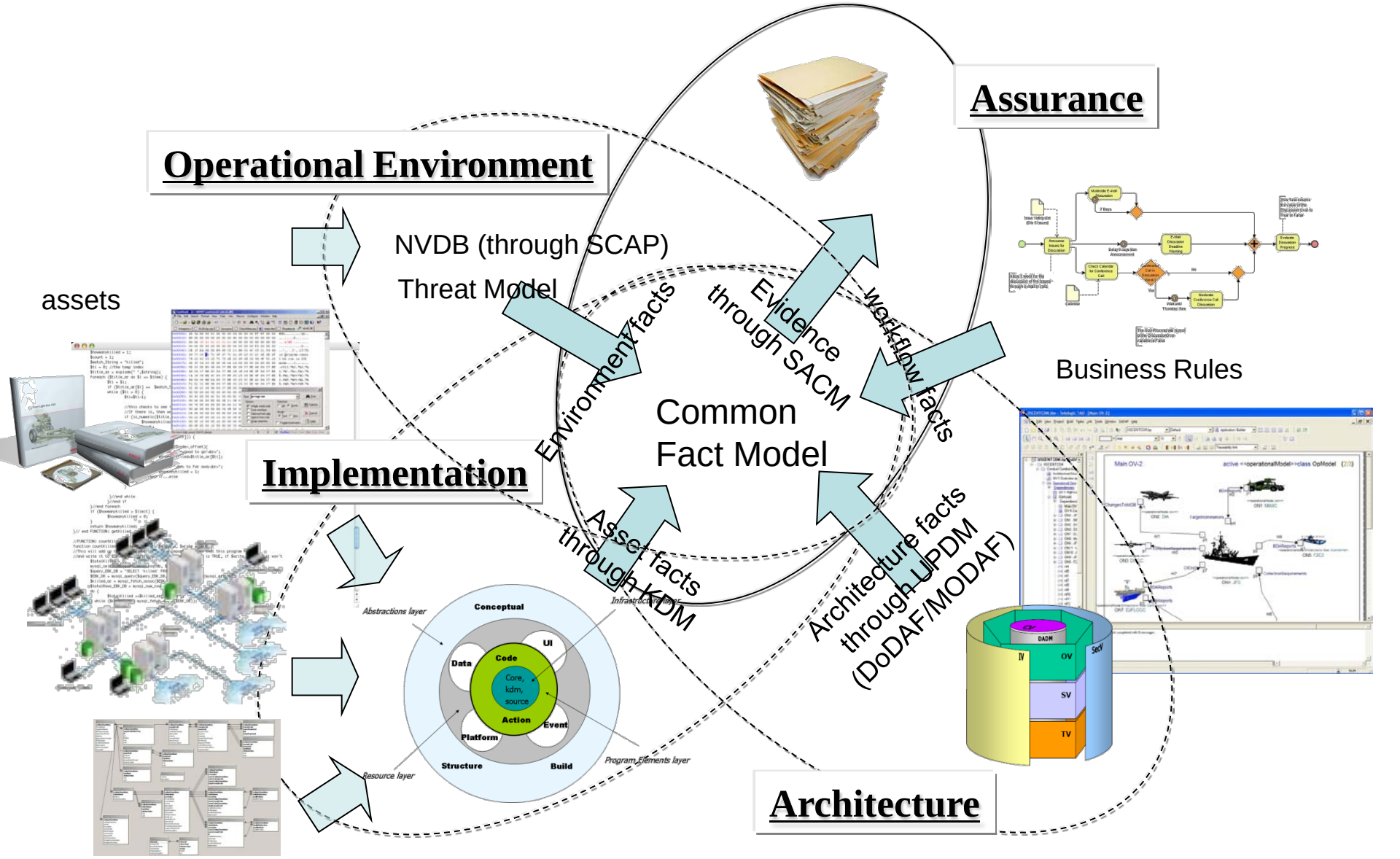
Leveraging what we already have through SwA Ecosystem

- The Software Assurance Ecosystem enables industry and government agencies to **leverage** and **connect** existing policies, practices, processes and tools, in an affordable and efficient manner

- The key enabler is the Software Assurance (SwA) Ecosystem **Infrastructure**
  - an open standards-based integrated tooling environment that dramatically reduces the cost of software assurance activities
    - Integrates different communities: Formal Methods, Assurance Case, Reverse Engineering and Static Analysis, and Dynamic Analysis for a System Assurance solution
    - Enables different tools to interoperate
    - Introduces many new vendors to ecosystem because they each leverage parts of the tool chain

Where We are Going: Expanding the SwA Ecosystem

Common Fact Model



Software Assurance Ecosystem: *The Formal Framework for System Assessments with Focus on Automation*

Tools Interoperability and Unified Reporting Environment

Process Docs & Artifacts

Requirements/Design Docs & Artifacts

Reports, Risk Analysis, etc

Process, People & Documentation Evaluation Environment

- Some point tools to assist evaluators but mainly manual work
- Claims in Formal SBVR vocabulary
- Evidence in Formal SBVR vocabulary
- Large scope requires large effort
- **Supported by The Open Group's UDEF***

Process, People, documentation Evidence

Formalized Specifications

Assurance Case Repository

- Formalized in SBVR vocabulary
- Automated verification of claims against evidence
- Highly automated and sophisticated risk assessments using transitive inter-evidence point relationships

Supported by the following standards:
- ISO/IEC 15026
- ISO/TC 37 / OMG SBVR
- OMG ARM
- OMG SAEM
- Software Fault Patterns (Target late 2011)
- UML Security Policy Extensions (planned)

Software System / Architecture Evaluation

- Many integrated & highly automated tools to assist evaluators
- Claims and Evidence in Formal vocabulary
- **Combination of tools and ISO/OMG standards**
- Standardized SW System Representation In KDM
- Large scope capable (system of systems)
- Iterative extraction and analysis for rules

Supported by ISO/IEC 19506

Software system Technical Evidence

Executable Specifications

SFP(CWE)

IA Controls

Protection Profiles

Hardware Environment

Software System Artifacts

Data Structures

Summary of the SwA Ecosystem Approach

- Normalized uniform common fact model
  - Separation of data feeds from reasoning
  - Standards-based
- Assurance case and SBVR
  - Representation of substantive reasoning
  - Natural language
- End-to-end multi-segment Traceability models
  - Code to state diagrams
  - Code to architecture
  - Code to conceptual model
  - Code to evidence determined by arguments
  - Evidence to arguments
  - Arguments to policy
- Focus on polynomial path-based properties
  - Instead of exponential state-based properties
- Arguments are “executable” queries to the fact model

Key Value of the SwA

The Key Value of the SwA Ecosystem Approach is End-to-end Traceability:

from code
to models
to evidence
to arguments
to security requirements to policy

For More Information

- OMG Systems Assurance Domain Task Force: http://sysa.omg.org/
- OMG General Information: http://www.omg.org/
- Richard Soley: soley@omg.org