



Software Assurance Ecosystem Status Update

Djenana Campara

President, Hatha Systems

Board Director, Object Management Group (OMG)

Co-Chair Software Assurance and Architecture Driven
Modernization, OMG

OMG Software Assurance Special Interest Group (SwA SIG)



- Security Focus
 - Objective: Create standard-based infrastructure that enables
 - Software Systems to ensure
 - only trusted code is executed
 - malicious attacks are prevented
 - » Software bugs are #1 cause for attacks
 - Suppliers to make an assurance claim about security, safety and/or dependability of system, product or service to address risk management
 - Challenge: A dependency on development and operational environment - The system is only secure as the weakest link
 - A strong dependency on supply chain to deliver supporting components
 - Considerations of SOA and SoS

Addressing Challenges through Software Assurance: Delivering System Predictability and Reducing Uncertainty



- Basic Principles
 - For each software artifact of interest, there exist a set of **claims** (generally related to safety and security) about the software artifact, a set of facts (collectively called **evidence**) about the software artifact, and a set of **assurance arguments** that use the evidence to show that the software artifact does, in fact, satisfy the claims.

Assurance of the system is presented through an Assurance Case (AC): set of auditable claims, arguments and evidence created to support the contention that a defined system/service will satisfy the particular requirements through supporting arguments and evidence



Software Assurance (SwA) is 3 step process

1. Specify Assurance Case

- Enable supplier to make bounded assurance claims about security and dependability of system/component

2. Obtain Evidence for Assurance Case

- perform software assurance assessment to justify claims to meet a set of requirements through a structure of sub-claims, arguments, and supporting evidence

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

This 3 step process needs to be comprehensive, objective & automated with reproducible results

Achieving Comprehensiveness, Objectivity and Automation



Key requirements:

1. Transparency into software systems
 - Transparency of engineering process and software products for comprehensive analysis
 - Reduce the risk created when an individual programmer is the sole source of knowledge about a given application
2. Specified assurance compliance points
 - Security property rules used for compliance checking need to be expressed in a formalized way - removing all ambiguity
 - currently, analysis is determined by content locked in stove piped tools with limited to no possibility to extend or redefine usage to meet specific needs.
3. Comprehensive tooling
 - It is imperative to achieve seamless integration of multiple variety of tools to create SwA solution for comprehensive analysis
 - Currently available tools have no significant overlap in their offerings, comprehensive analysis requires the integration of multiple tools
 - Tools integration is very costly since existing tools do not follow standards for expressing/representing analysis results, making it extremely difficult (if not imposable) to integrate/review the results.

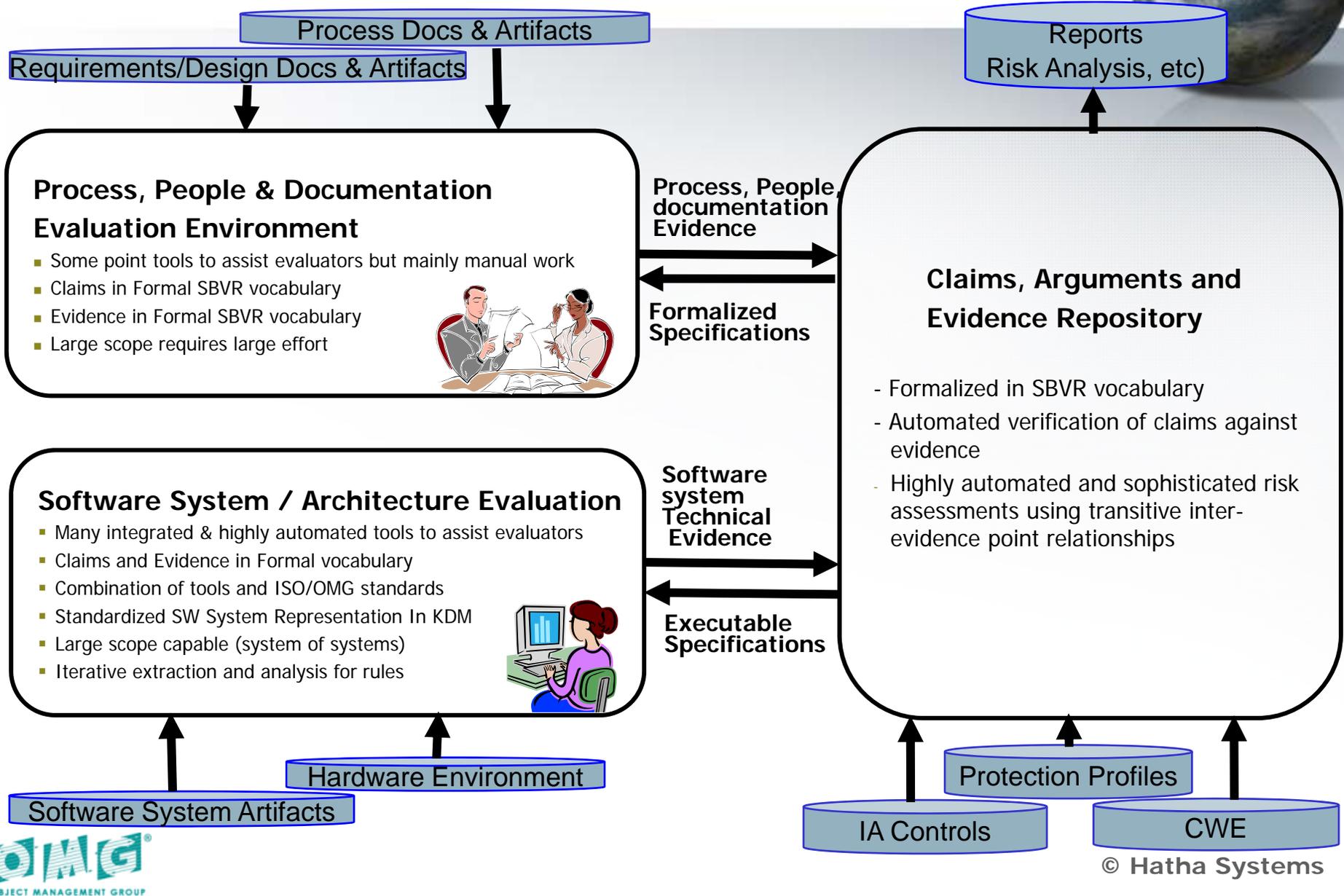
Standard-based Approach to Solution



- SwA Ecosystem
 - Standard-based integrated tooling environment that dramatically reduces the cost of software assurance activities
 - Based entirely on ISO/OMG Open Standards
 - Semantics of Business Vocabulary and Rules (SBVR)
 - Knowledge Discovery Metamodel (KDM)
 - Software Assurance Metamodel (SAM)

Software Assurance Ecosystem: The Formal Framework

The value of formalization extends beyond software systems to include related process, people and documentation



SwA Ecosystem - Status Update



- Standard-based integrated tooling environment that dramatically reduces the cost of software assurance activities
- Based entirely on OMG Open Standards
 - Semantics of Business Vocabulary and Rules (SBVR)
 - Revision 1.1 in process
 - New open source project
 - Knowledge Discovery Metamodel (KDM)
 - Revision 1.1 published
 - Software Assurance Metamodel (SAM) - Broken down in 2 parts
 - Argumentation Metamodel
 - related to representation of Claims and Arguments – Request for Comments on Submitted Spec will be published in March 2009
 - Evidence Metamodel
 - Joint Submission presented - completion date set for the end of 2009
 - It consists of 3 major parts: core framework, imported ontology and audit (signing authority) information

SwA Ecosystem - Status Update

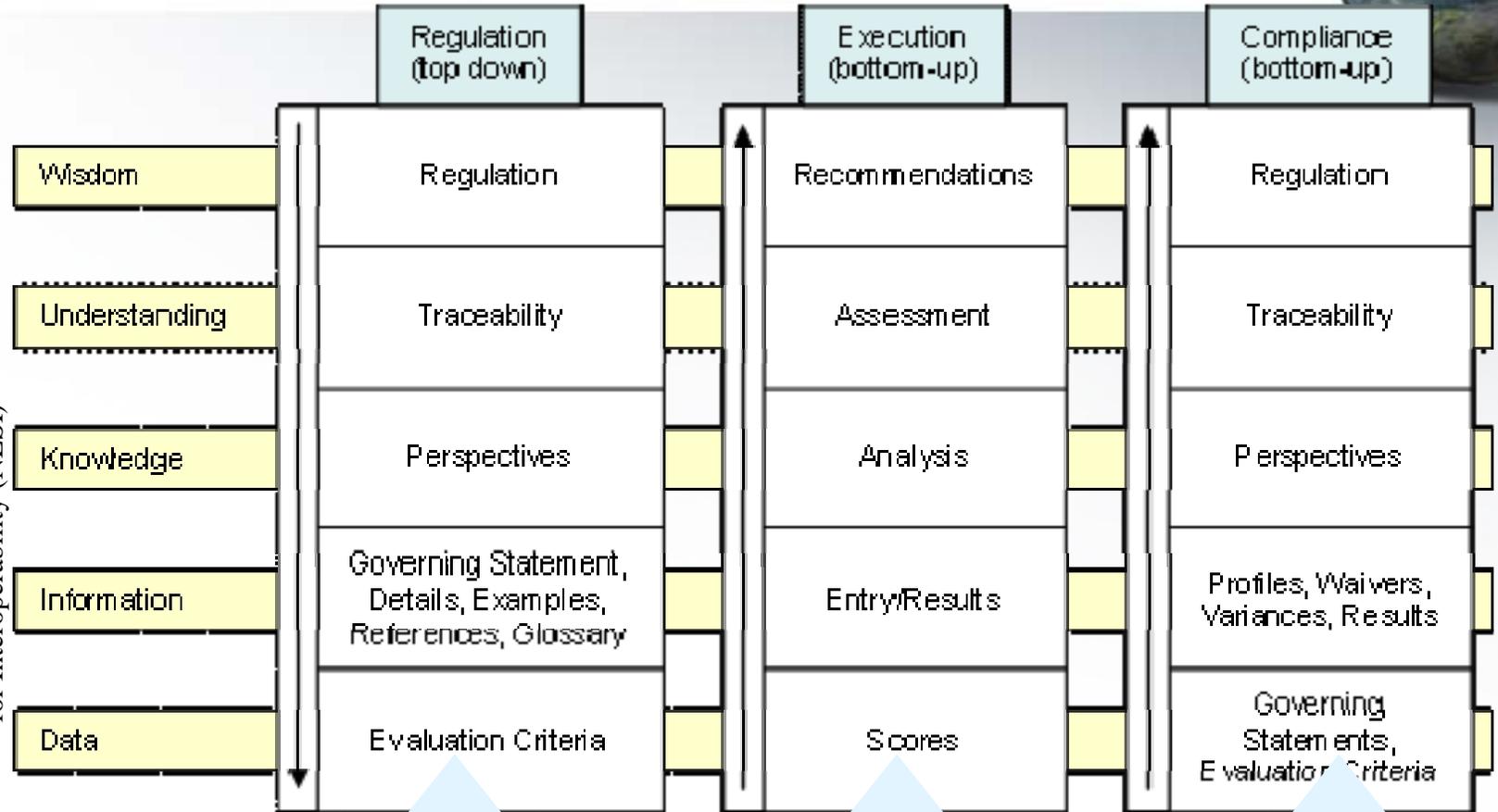


- Recent addition to Ecosystem is Software Metrics Metamodel (SMM)
 - Beside presenting measurement and metrics information group will focus on defining libraries of metrics that support decision making in area of modernization, quality and security assurance
- New work started in area of Governance of Assurance Cases (ACs) titled Management of Regulations and Compliance (MRC) focusing on
 - Decision making process for AC
 - Dependences and correlation of multiple ACs
 - Risk assessment process



Governance of Assurance Cases

Framework for NESI Governance Model
US Navy Net-Centric Enterprise Solutions
for Interoperability (NESI)



Claims Arguments

Claims Arguments Evidence

Claims Arguments Evidence Evidence Evidence