
Dr. Ben Calloni, P.E. CISSP, CEH, OCRES
Lockheed Martin Fellow, Software Security
• Lockheed Martin Representative to OMG
  • OMG Board of Directors
  • Co-chair OMG System Assurance Task Force
• Member of DHS-OSD Software Assurance Forum / WG’s
• Member of Future Airborne Capabilities Environment (FACE) Consortia
  • Conformance Business WG
  • Safety and Security Technical WG
• Lockheed Martin Representative to The Open Group,
  • Member Trusted Technology Forum
• SMU Adjunct Professor, System Security Engineering

Dr. Nikolai Mansourov, CTO KDM Analytics
• Co-Author and Finalization Task Force Chair of the Structured Assurance Case Metamodel

Published by IEEE with permission from Lockheed Martin

OMG slides publicly releasable
©KDM Analytics slides are used with permission.
Overview

- Introduction
- Defining Assurance
- The Object Management Group
- Semi Formal Methodology and Process
- Addressing the Static Code Analysis Stovepipes
- Formalization and Standardization of Weaknesses / Flaws
- Graphical Claims Evidence Arguments
- Addressing Automated Threat Risk Assessment
- Case Study #1: Vulnerability Path Assessment
- Case Study #2: Graphical Threat Risk Assessment
- Concluding Remarks
(HLP)$^2$ – Keep It Simple Stupid! (KISS)

Handle
Horn
Light
Lights
Pressure
Power
My First Job!
Rigorous Aviation Safety

I’ve flown at Mach 2 @ 50,000 ft and
Supersonic at 180 feet **below** Sea Level!

Flight Safety Officer
(No True Accidents!)

Functional Test Pilot

SEAD / DEAD
F-4C Wild Weasel (Hunter)
F-4D Strike (Killer)
Current INFOSEC Software Assurance activities focus on Reducing flaws, weaknesses, or vulnerabilities by:
  • Running Static / Dynamic Code Analysis tools
  • Performing Penetration Testing

BUT......
Security Definition

Basic definition of Vulnerability
• refers to the inability to withstand the effects of a hostile environment
• open to attack or damage

Cyber Vulnerability (CISSP BoK)
1. A flaw* (aka weakness) exists in the system
2. Attacker has access to the flaw, and
3. Attacker has capability to exploit the flaw
   • Examples
     – Lack of security patches
     – Lack of current virus definitions
     – Software Bug
     – Lax physical security

*e.g. Buffer Overflow is still on SANS Top 25 (#3). Industry has known and discussed since 1988!

Defenders can only control these!
2010 Study
Conclusions

- Tools are not interchangeable
- Tools perform differently on different languages
- Complementary tools can be combined to achieve better results
- Each tool failed to report a significant portion of the flaws studied
  - Average tool covered 8 of 13 Weakness Classes
  - Average tool covered 22% of flaws in Weakness Classes covered

Bugs, Flaws and Defects
(from the “safety domain”)

• **Bugs** *(sometimes called “flaws or weaknesses” in the security domain)*
  – Occur at Implementation (lower) level
  – Only exist in code
  – Can often be fixed in a single line of code

• **Flaws**
  – Can exist at all (code / design / requirements) levels
  – Subtle problems that are instantiated in code, but are also present (or missing) in the design
  – Design (or requirement) flaws may require a redesign that can affect multiple areas in the system

• **Defects** encompass both implementation (bugs) and design (flaws) problems
  – May lie dormant for years and surface later in a fielded system
  – Give way to major consequences

---

**Airbus Auto-land Incident (N-version programming)**

April 3, 2014
What is Assurance?

• **Assurance** is the **measure of confidence** that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy. - CNSS 4009 IA Glossary

• **Information Assurance (IA)** are measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities - CNSS 4009 IA Glossary

• **Safety Assurance (SfA)** is providing **confidence** that acceptable risk for the safety of personnel, equipment, facilities, and the public during and from the performance of operations is being achieved. – FAA/NASA

• **Software Assurance (SwA)** is the **justified confidence** that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during the life cycle. - CNSS 4009 IA Glossary
What is Assurance? (2)

- **Mission Assurance (MA)** is the ability of operators to achieve their mission, continue critical processes, and protect people and assets in the face of internal and external attack (both physical and cyber), unforeseen environmental or operational changes, and system malfunctions. (See notes page for further description.) – MITRE Systems Engineering Guide

- **System Assurance (SysA)** is the planned and systematic set of engineering activities necessary to assure that products conform with all applicable system requirements for safety, security, reliability, availability, maintainability, standards, procedures, and regulations, to provide the user with acceptable confidence that the system behaves as intended in the expected operational context. – OMG SysA Task Force
Interrelationships of Assurance

Boeing 777 toilets were certified to FAA high robustness safety requirements to meet Mission Assurance!

*The “-ilities” Reliability, Schedulability, Maintainability, Dependability, etc.

April 3, 2014
Delivering System Assurance in any Domain:
Delivering System Predictability and Reducing Uncertainty

Software Assurance (SwA) is 3 step process

1. Specify Assurance Case
   - Enable supplier to make unambiguous bounded assurance claims about safety, security dependability, etc. of systems, product or services

2. Obtain Evidence for Assurance Case
   - Perform system 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
   - Examine non compliant claims and their evidence to calculate risk and identify course of actions to mitigate it
   - Each stakeholder will have own risk assessment metrics – e.g. security, safety, liability, performance, compliance

Currently, SwA 3 step process is informal, subjective & manual
My thanks to a colleague: Prof. Tim Kelly

Safety Arguments – Text Problems

For hazards associated with warnings, the assumptions of [7] Section 3.4 associated with the requirement to present a warning when no equipment failure has occurred are carried forward. In particular, with respect to hazard 17 in section 5.7 [4] that for test operation, operating limits will need to be introduced to protect against the hazard, whilst further data is gathered to determine the extent of the problem.

- Not everyone can write clear English
- Can take many readings to decipher meaning
- Multiple cross-references in text can be awkward
- Is there a clear shared understanding of the argument?

http://www-users.cs.york.ac.uk/~tpk/04AE-149.pdf
Summary of Challenges

- **Key Challenges**
  - **Systematic coverage of the weakness space**
    - A key step that feeds into the rest of the process – if not properly done, rest of the process is considered add-hock
  - **Reduce ambiguity associated with system weakness space**
    - Often due to requirements and design gaps that includes coverage, definitions and impact
  - **Objective and cost-effective assurance process**
    - Current assurance assessment approaches **resist automation** due to lack of **traceability** and **transparency** between high level security policy/requirement and system artifacts that implements them
  - **Effective and systematic measurement of the residual risk**
    - Today, the risk management process often does not consider assurance issues in an integrated way, resulting in project stakeholders **unknowingly accepting assurance risks** that can have unintended and severe security issues
  - **Actionable tasks to achieve high confidence in system trustworthiness**

Overcoming these challenges will enable automation, a key requirement to a cost-effective, comprehensive, and objective assurance process and effective measure of trustworthiness
Assured Software

“Mitigating Supply Chain Risks requires an understanding and management of Suppliers’ Capabilities, Products and Services”

More comprehensive diagnostic capabilities and standards are needed to support processes and provide transparency for more informed decision-making for mitigating risks to the enterprise

- Joe Jarzombek, PMP, CSSLP
  Director for Software Assurance
  National Cyber Security Division, Homeland Security

- In 2005 Mitch Komaroff, (NII/DoD-CIO) and Ken Hong Fong on behalf of DoD approached OMG to address this via standards.
- In 2007 Mr. Jarzombek also engaged OMG on behalf of DHS
Who Is OMG?

Object Management Group (OMG) factoids:

– Founded in 1989 (Celebrating 25 years in June 2014)

– Over 470 member companies

– The largest and longest standing not-for-profit, open-membership consortium which develops and maintains computer industry specifications.

– Continuously evolving to remain current while retaining a position of thought leadership.

OMG’s processes are designed to standardize existing company technologies where interoperability / interchangeability are necessary to business goals.
OMG’s Best-Known Successes

**Common Object Request Broker Architecture**
- CORBA® remains the only language- and platform-neutral interoperability standard

**Unified Modeling Language**
- UML™ remains the world’s only standardized modeling language

**Business Process Modeling Notation**
- BPMN™ provides businesses with the capability of understanding their internal business procedures

**Common Warehouse Metamodel**
- CWM™, the integration of the last two data warehousing initiatives

**Meta-Object Facility**
- MOF™, the repository standard

**XML Metadata Interchange**
- XMI™, the XML-UML standard
Who Are OMG-ers?

Some of the hundreds of member companies:

- ACORD
- Atego
- BAE Systems
- Boeing
- CA
- Capgemini
- Cordys
- CSC
- DND Canada
- FICO
- Fujitsu
- General Dynamics
- General Electric
- Hewlett Packard
- Harris
- Hitachi
- HSBC
- IBM
- IDA
- KDM Analytics
- Lockheed Martin
- Mayo Clinic
- MIT/Lincoln Labs
- MITRE
- NASA
- Navy UWC & SWC
- NIST
- Northrop Grumman
- No Magic
- OIS
- Oracle
- Progress
- Red Hat
- RTI
- SAP
- Software AG
- SPAWAR
- Sparx Systems
- Toyota
## OMG Organization

<table>
<thead>
<tr>
<th><strong>Architecture Board</strong></th>
<th><strong>Platform TC</strong></th>
<th><strong>Domain TC</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Liaison SC</td>
<td>A &amp; D PTF</td>
<td>BMI DTF</td>
</tr>
<tr>
<td>Object &amp; Reference</td>
<td>ADM PTF</td>
<td>C4I DTF</td>
</tr>
<tr>
<td>Model SC</td>
<td>MARS PTF</td>
<td>Finance DTF</td>
</tr>
<tr>
<td>Spec Mgt SC</td>
<td>SysA PTF</td>
<td>Government DTF</td>
</tr>
<tr>
<td>MDA Users’ SIG</td>
<td>Agent PSIG</td>
<td>Healthcare DTF</td>
</tr>
<tr>
<td>Process</td>
<td>Data Distribution PSIG</td>
<td>Life Sciences DTF</td>
</tr>
<tr>
<td>Metamodels SIG</td>
<td>Japan PSIG</td>
<td>Mfg Tech &amp; Ind. Systems DTF</td>
</tr>
<tr>
<td>SOA SIG</td>
<td>Korea PSIG</td>
<td>Robotics DTF</td>
</tr>
<tr>
<td>IPR SC</td>
<td>Ontology PSIG</td>
<td>S/W Based Comm DTF</td>
</tr>
<tr>
<td>Sustainability SIG</td>
<td>Telecoms PSIG</td>
<td>Space DTF</td>
</tr>
<tr>
<td>Architecture</td>
<td></td>
<td>Crisis Mgmt DSIG</td>
</tr>
<tr>
<td>Ecosystems SIG</td>
<td></td>
<td>Regulatory Compl. DSIG</td>
</tr>
<tr>
<td>Business</td>
<td></td>
<td>SDO DSIG</td>
</tr>
<tr>
<td>Architecture SIG</td>
<td></td>
<td>Sys Eng DSIG</td>
</tr>
</tbody>
</table>

*Software Assurance SIG charted Feb 2006 through Dec 2008
*System Assurance Task Force chartered and began work in March 2009

April 3, 2014
OMG System Assurance Task Force (SysA TF)

• Strategy
  – Establish a common framework for analysis and exchange of information related to system 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
  – SwA Ecosystem - common framework for capturing, graphically presenting, and analyzing properties of system trustworthiness
    • leverages and connects existing OMG / ISO specifications and identifies new specifications that need to be developed to complete framework
    • provides integrated tooling environment for different tool types
    • architected to improve software system analysis and achieve higher automation of risk analysis
Establishing Assurance and Trust

Operational Environment

- CONOPS
- DoD AF OV’s etc.

Attack Patterns

- NVDB (through SCAP)

Threat Risk Assessment / Hazard Analysis

- Word
- PPT
- Excel

Implementation

- System Artifacts
  - Req.
  - Use Cases
  - Design
  - Data Flow Diagrams
  - STIGS
  - etc.

Software Fault Patterns

- (Formalized CWE’s and TOIF results)

C&A

Fed by Assurance Models

- Assurance Models

Architecture

- UPDM*

*UML Profile for DODAF/MODAF

March 29, 2014
• Thesis for R&D work - *All software is part of a larger system.*
  • Must incorporate larger Mission, System, and Information Assurance Engineering approach,
    • leveraging semi-formalisms,
    • automated tool support,
    • to achieve a level of confidence desired.
  • Affordability must be achieved by commercial standardization and economies of scale.

• IRAD
  • *Multiple years dealing with System Security Engineering and System Assurance 2006-2012*
  • AFRL Contract F33615-02-D-4035 (2004-2012) - Embedded Information Systems Reengineering – Technology Demonstration (EISR-TD)
    • *Delivery Order #4, Common Weakness Enumeration Formalizations* (2007-2008)
    • *Delivery Order #6, Vulnerability Path Assessment Demonstration* (2009-2012)
      • Mr. Jahn Luke, PM – USAF, Mr. Mitch Komaroff, NII/DoD-CIO, Funding Agent
      • Dr. Ben Calloni, P.E., PM - Lockheed Martin Aeronautics
      • Ms. Djenana Campara, CEO, PM - KDM Analytics

*Collaborative funding: DHS, OSD/NII, NIST, MITRE, AFRL*
Addressing the Challenges

- Addressing challenges through set of integrated standards
  - Define a *semi-formal methodology* to address weakness space coverage
  - Provide *automated generation* of provably *correct true-positive SCA test cases*. Vet and Standardize test cases
  - Graphically capture *claims and evidence* (common facts) about a system
  - Graphically capture *threat-risk assessment information* about a system
  - Automate *vulnerability path assessments*
  - Specifications for a *suite of integrated tools* providing end-to-end solution
    - No one tool or one vendor can provide solution to address identified challenges
  - *Tools integration possible only through standards*
    - Set of standards are needed requiring tight integration between standards
    - Integration of standards require that they are based of the same technology and they follow the rules of technical development

The only standard organization producing such interoperability standards is the OMG!
Semi Formal Methodology and Process
Confidence Analysis through Assurance Process: Reducing Uncertainty

- **Assurance** does not provide additional security services or safeguards. It serves to reduce the uncertainty associated with systematic identification of weak links and ultimately with vulnerabilities.
  - (e.g. Common Criteria
  - Security Assurance Requirements vs.
  - Security Functional Requirements)

- Product of **System Assurance** is justified confidence delivered in the form of an **Assurance Case**. The Assurance Case is formed by a clear chain of evidence to argument to assurance claims.
Tiered approach to Security Assurance: FORSA

• FORSA\(^1\) (Fact Oriented Repeatable Security Assessment) methodology

• FORSA is a four tiered approach to security assurance that provides a progressively higher level of assurance through fidelity and policy orientation

• Repeatable and systematic way to perform risk assessment and system analysis

• Provides guidance to validation and verification activities as they are performed against the system, as well as the process of risk assessment

FORSA: A Methodology supported by Standards

- FORSA is aligned with the OMG System Assurance Eco-system
  - Standards-based
    - OMG ISO/IEC 19506 Knowledge Discovery Metamodel
    - OMG Structured Assurance Case Metamodel
    - Goal Structured Notation (GSN)
    - UPDM
    - SysML
    - OMG Semantics of Business Vocabularies and Rules
    - OMG Structured Metrics Metamodel
    - OMG Risk Metamodel (standardization in progress)
    - Common Fact Model (standardization in progress)
    - RDF
    - XML
    - MOF
  - Influences standards
  - Part of the growing community built around standards
- FORSA facilitated protocols for knowledge interchange between producers and consumers in cybersecurity space
  - Making it objective and repeatable

April 3, 2014

*Risk management process

- Stakeholder requirements definition
- Requirements analysis
- Architectural design
- Implementation
- Integration
- Transition
- Operation and Maintenance
- Disposal
- Verification
- Validation
- ConOps & Security Policy

- Threat & Risk Analysis
- Preliminary Assessment
- Full Assessment
- Assurance Case

- Enterprise Processes
- Agreement Processes
- Project Management Processes
- Technical Processes

- Assurance* Needs
- Initial Assurance* Agreement
- Assurance* Plan

*Assurance interpreted as: Safety, Security, FDA, etc.

UPDM, SysML, UML, and SysA

April 3, 2014

*risk to cost / schedule
Addressing the SCA Stovepipes
Tool Output Integration Framework Overview

- Normalized Report Output (Useful to SwE's)
- Vulnerability Path Assessment (Workbench)
- Threat Risk Analysis (Blade tool)
  (Useful to SSE / INFOSEC Analysts)

TOIF Released as Open Source
Graphical Claims Evidence Arguments (Common Facts)
OMG’s Structured Assurance Case Metamodel
Establishing the Security Assurance Case

CG1.1 Security criteria are defined
Context

CG1.2 Assessment scope is defined
Context

CG1.3 Assessment rigor is defined
Context

G1 System is acceptably
secure
Goal

G2 All threats are
identified and adequately
Mitigated
Goal

G3 TCB Components
Identified
Goal

G4 All threats to the
system are identified
Goal

G5 Identified threats are
adequately mitigated
Goal

G6 Residual risk is
acceptable
Goal

S1 Argument based on end-to-end risk
mitigation analysis
Strategy

M1 Integrated
system model

Example CC
Assurance Levels

TCB
....

DIACAP? JAFAN? CC? ....

• UML
• SysML
• DoDAF

April 3, 2014
Addressing Automated Threat Risk Assessment (Common Facts)
Identifying the Threats

G4
All threats to the system are identified
Goal

S2
Argument based on various confidence factors affecting threat identification
Strategy

G4.1
All known risk factors related to similar systems are identified
Goal

G4.1.1
All operational activities of the system are identified
Goal

G4.1.2
All assets of the system are identified
Goal

G4.1.3
All undesired events are identified
Goal

G4.1.4
All threat scenarios are identified
Goal

G4.1.5
All threat agents are identified
Goal

G4.2
All risk factors for the system are systematically identified
Goal

G4.3
Risk analysis team is adequately experienced
Goal

April 3, 2014
Case Study #1: Vulnerability Path Assessment
Customer Challenge #1:
Application of TRA / VPA to Software

• Wireshark (Open Source)
  – network protocol analyzer.
  – capture and interactively browse traffic running on a computer network.
  – de facto (and often de jure) standard across many industries and educational institutions.
  – Open Source - project that started in 1998.
  – ~ 2MLOC

• TRA BLADE Tool Statistics (BLADE is name of TRA Tool)
  – Total files analyzed: 1519
  – Run open source tools:
    – number of findings: 18949
"ENV:SRC" element is contextual, to represent subjects that are not part of the current view, but are somewhere else in the fact model. Thus each KWB view represents ALL facts for the selected elements.

All facts related to each Performer, e.g. “Exchange Element is consumed by Performer”

“ENV:SNK” element is contextual, to represent objects that are not part of the current view, but are somewhere else in the fact model. Thus each KWB view represents ALL facts for the selected elements.
Compare as-is with intended architecture to identify surface of attack and associated risks and find out how identified code security issues effect increased risk.
Identified enlarged surface of attack - 4 components accessing Hard Disk (HD) instead one

April 3, 2014
Line of code where Capture component is accessing HD
The architectural component where the buffer overflow is happening
Exploitation path for buffer overflow found that feeds directly into possible remote attack risk.
Case Study #2:
Graphical Threat Risk Assessment
DoDAF Mandate / UPDM Certification

"DoD and its Program Managers require DoDAF-compliant Architectures. Competing companies will prefer to staff an architecture project with UPDM/DoDAF-certified architects" says Walt Okon, Senior Architecture Engineer, DoD-CIO, Architecture & Interoperability Directorate. "Now included in the DoD IT Standards Registry (DISR) 12-1.0, UPDM Version 2.0 is mandated for projects using DoDAF Version 2+ and OMG SysML or UML." – Walt Okon, September 2010 OMG Board of Director’s meeting

"Technical credentials are as important in our profession as degrees and experience" says Brian Wilczynski, Director, Architecture and Interoperability, DoD CIO/DCIO(IE). "The OMG’s UPDM Certification program will help advance the effective use of UPDM in the DoD."

"UPDM certification is the easiest way to comply with the Mandate” says Len Levine of the DoD Executive Agent for IT Standards. “By certifying its staff, a company will confirm to DoD that it has made a commitment to building quality architectures conformant to this DoD-mandated standard. The OCUDA certification program, to include a Model User level certification plus two Model Builder levels, will test architects' readiness to review, require, or deliver sharable architectures and designs. Working together, certified practitioners and users of UPDM and DoDAF will reap the benefits of reuse of information, and sharing of architectural artifacts, models, and viewpoints.”

Lockheed Martin has co-funded the development by OMG of the UPDM Certification Tests and will fund LM Architects (Enterprise and Embedded) to take the exam!
AFRL Challenge #2: Architecture Risk Analysis using DODAF?

• Problem
  – Identify critical components with high confidence in order to minimize the residual risks to the mission of the enterprise

• Challenge
  – Systematic analysis of threats and risks
  – Projecting risks analysis to components in a systematic way
  – Integrating confidence into risk analysis
  – Integrating confidence into architecture analysis

• Solution
  – Common Fact Model
    • All information elements (DoDAF, Threats, Risks, Attacks, Vulnerabilities, etc.) are represented in a uniform way, so that they can be collated and managed together. It is critical to represent complex statements involving all these models (and few more)
    • Semantic Integration of various pre-existing models (such as importing DoDAF facts into the common normalized model)
    • Uniform analytics across the Common Fact Model
  – Systematic methodology for identifying risks
  – Systematic methodology for Architecture Risk Analysis
1. (Prelude) Importing static images from DoDAF
2. Importing DoDAF elements and semantic integration into the Common Fact Model
3. Importing DoDAF facts and semantic integration into the Common Fact Model
4. DoDAF model analytics using the KWB
5. Threat and Risk Analysis using the KWB and the FORSA methodology
6. Projecting the identified risks to the architectural components
1. Importing static images of DoDAF views

DoDAF OV-1 view (static image) imported from No Magic tool

DoDAF views imported from No Magic tool
2. Importing DoDAF elements

Elements of the Common Fact Model, corresponding to the OV-2 view (imported from No Magic tool)

DoDAF OV-2 view (static image) imported from No Magic tool
3. Importing DoDAF facts

Live KDM view showing all DoDAF Performers (collected from all DoDAF views) and related facts.
DoDAF analytics (2)
Threat and Risk Analysis
Assets in the TRA model
System/Software Assurance Ecosystem: The Formal Framework for System Assessments with Focus on Automation

https://buildsecurityin.us-cert.gov/swa/ecosystem.html

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
- Large scale system of systems (DODAF)
- Supported by The Open Group’s UDEF*

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*
  - Iterative extraction and analysis for rules
- *ISO/IEC 19506:2012

Tools Interoperability and Unified Reporting Environment
- Reports, Threat Risk Analysis, etc

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 15026-4:2012 Sys & SwE Assurance
- ISO/TC 37 / OMG SBVR
- OMG Structured Assurance Case Metamodel
- Software Fault Patterns (Target 2013)
- UML Security Policy Extensions (2014)
Thank You!

- Dr. Ben Calloni, P.E., CISSP, CEH, OCRES
  - LM Fellow
  - Lockheed Martin Aeronautics Company
  - Fort Worth, TX
  - ben.a.calloni@lmco.com
  
  - Texas Tech University Distinguished Engineer
  - AIAA Associate Fellow
  - Object Management Group Board of Directors
    - OMG System Assurance Task Force Co-Chair
  - Member of DHS-OSD Software Assurance Forum / WG’s
  - Future Airborne Capabilities Environment consortium
    - Member of Safety / Security Technical WG
    - Member of FACE Conformance Business WG
  - SMU Adjunct Professor, System Security Engineering
Tool Output Integration Framework Architecture