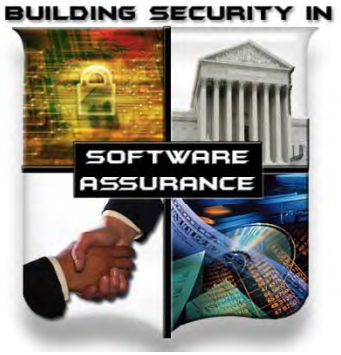
Homeland Security

Commerce

National Defense



Assurance Cases

Robert A. Martin
Sean Barnum

May 2011

MITRE

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
MAY 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Assurance Cases	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Mitre Corporation,202 Burlington Rd,Bedford,MA,01730-1420**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Presented at the 23rd Systems and Software Technology Conference (SSTC), 16-19 May 2011, Salt Lake City, UT. Sponsored in part by the USAF. U.S. Government or Federal Rights License

14. ABSTRACT

15. SUBJECT TERMS

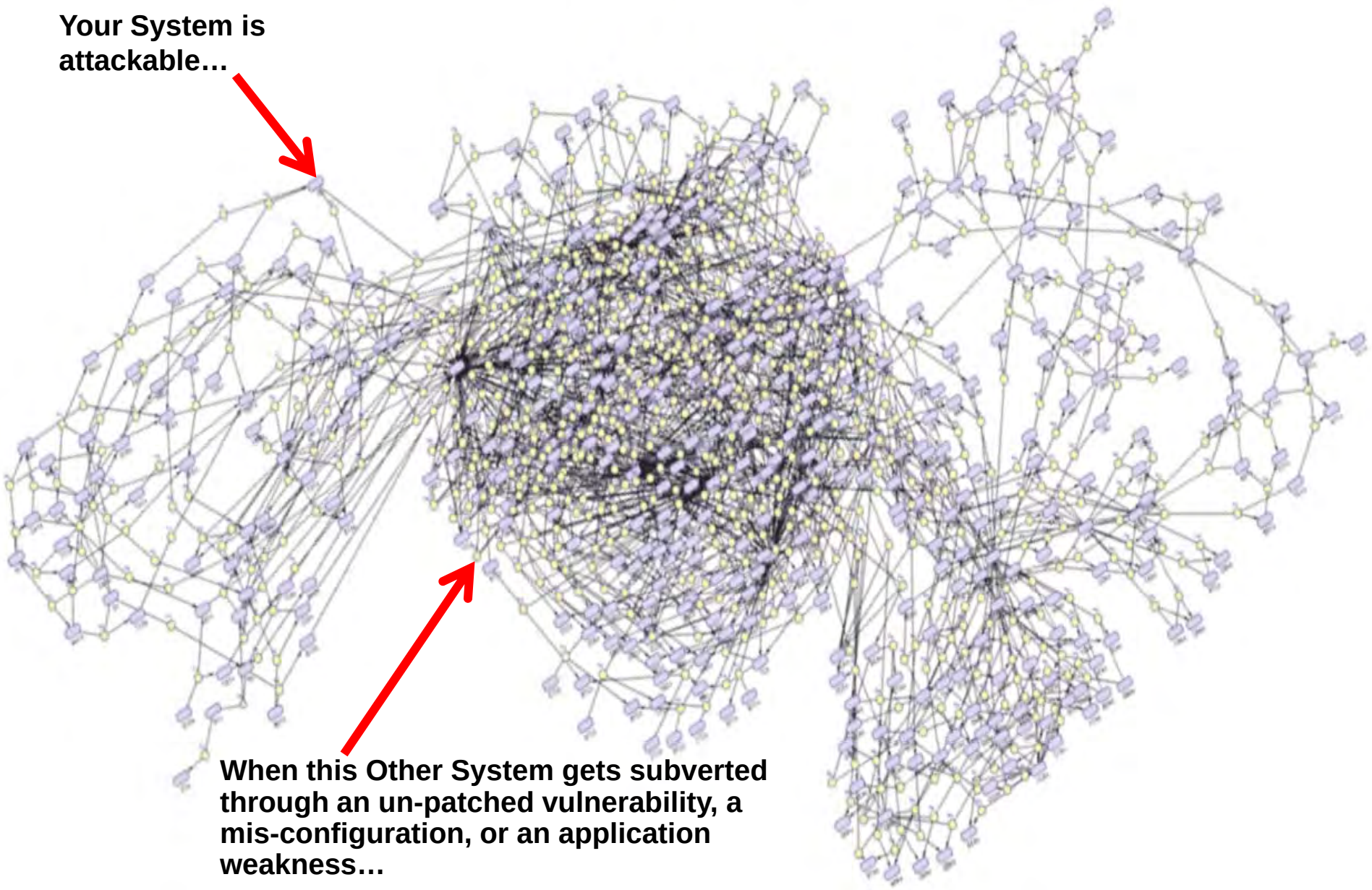
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**21**	

Agenda

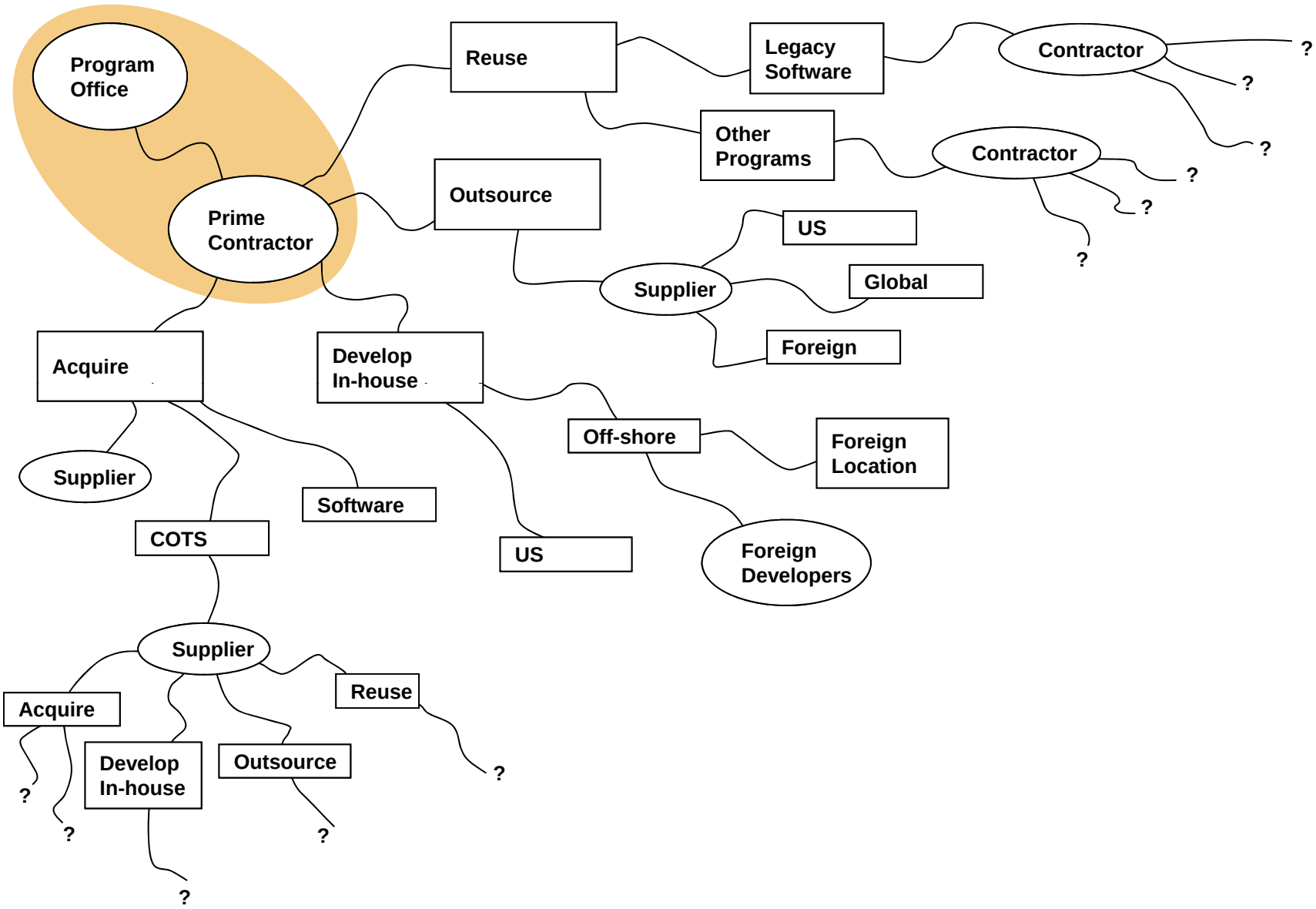
8:00-8:45am	Software Security Knowledge about Applications Weaknesses
9:00-9:45am	Software Security Knowledge about Attack Patterns Against Applications
	Training in Software Security
10:15-11:00am	Software Security Practice
11:15-12:00am	Supporting Capabilities
	Assurance Cases
	Secure Development & Secure Operations

Making Security Measurable™

Today Everything's Connected



The Software Supply Chain



* "Scope of Supplier Expansion and Foreign Involvement" graphic in DACS www.softwaretechnews.com Secure Software Engineering, July 2005 article "Software Development Security: A Risk Management Perspective" synopsis of May 2004 GAO-04-678 report "Defense Acquisition: Knowledge of Software Suppliers Needed to Manage Risks"

What Is an Assurance Case?

Making Security Measurable™

History of Assurance Cases

- Originally Only Safety Cases
  - **Aerospace**
  - **Railways, automated passenger**
  - **Nuclear power**
  - **Off-shore oil**
  - **Defense**
- Security Cases
  - **Use compliance rules more than an assurance case**
- Cases for Business Critical Systems

Making Security Measurable™

Definition of Safety Case

- From Adelard's ASCE manual:

"A documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment."

Making Security Measurable™

Definition of Assurance Case

- Generalizing that definition

  A documented body of evidence that provides a convincing and valid argument that a specified set of critical claims regarding a system's properties are adequately justified for a given application in a given environment.

Making Security Measurable™

Structured Assurance Cases

- Structure is required to make the creation, sharing, analysis, maintenance and automation of such an assurance case practical

- Structured Assurance Cases are composed of structured sets of Claims, Arguments and Evidence
  - **A Claim is a proposition to be assured about the system of concern**
  - **An Argument is a reasoning of why a claim is true**
  - **Evidence is either a fact, a datum, an object, a claim or [recursively] an assurance case which supports an Argument against a Claim**

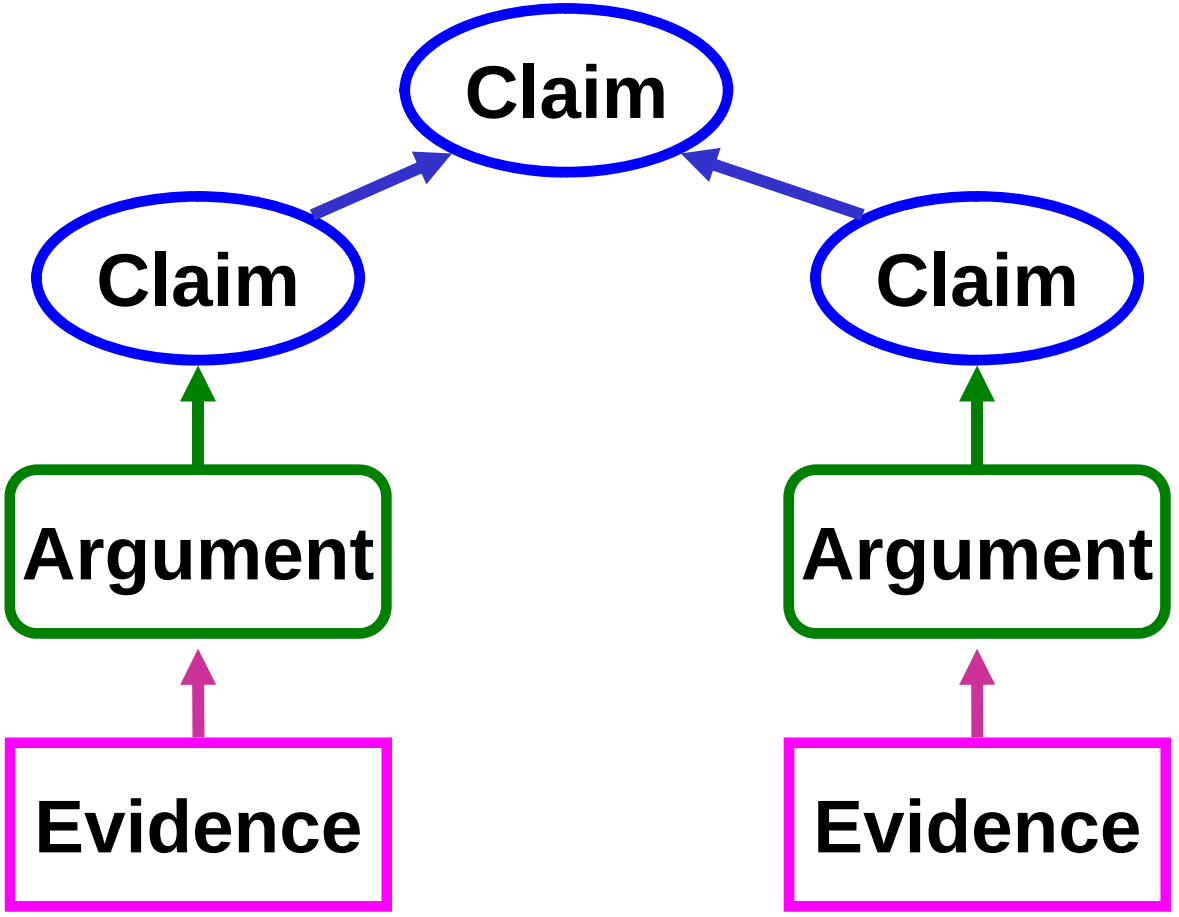
Making Security Measurable™

Extremely Simplified Overview of Structured Assurance Case Content

Claim =
assertion to be proven

Argument =
reasoning supporting a claim

Evidence =
data supporting an Argument



Making Security Measurable™

Need for Standards

- While several different notations exist for safety cases and generalized assurance cases no widely accepted standard currently exists for specifying structured assurance cases within a systems & software assurance domain
- Standards are needed before structured assurance cases can be widely leveraged or made practical through automated tooling
- Coordinated efforts are currently underway in the International Standards Organization (ISO) and the Object Management Group (OMG) to develop these needed standards
  - **ISO 15026 Part 2 (currently published) is a very simple high-level standard outlining the context and basic requirements for structured assurance cases**
  - **The OMG SACM (under development) and supporting OMG standards are targeted at providing at automatable level of detail for structured assurance case specification**

Making Security Measurable™

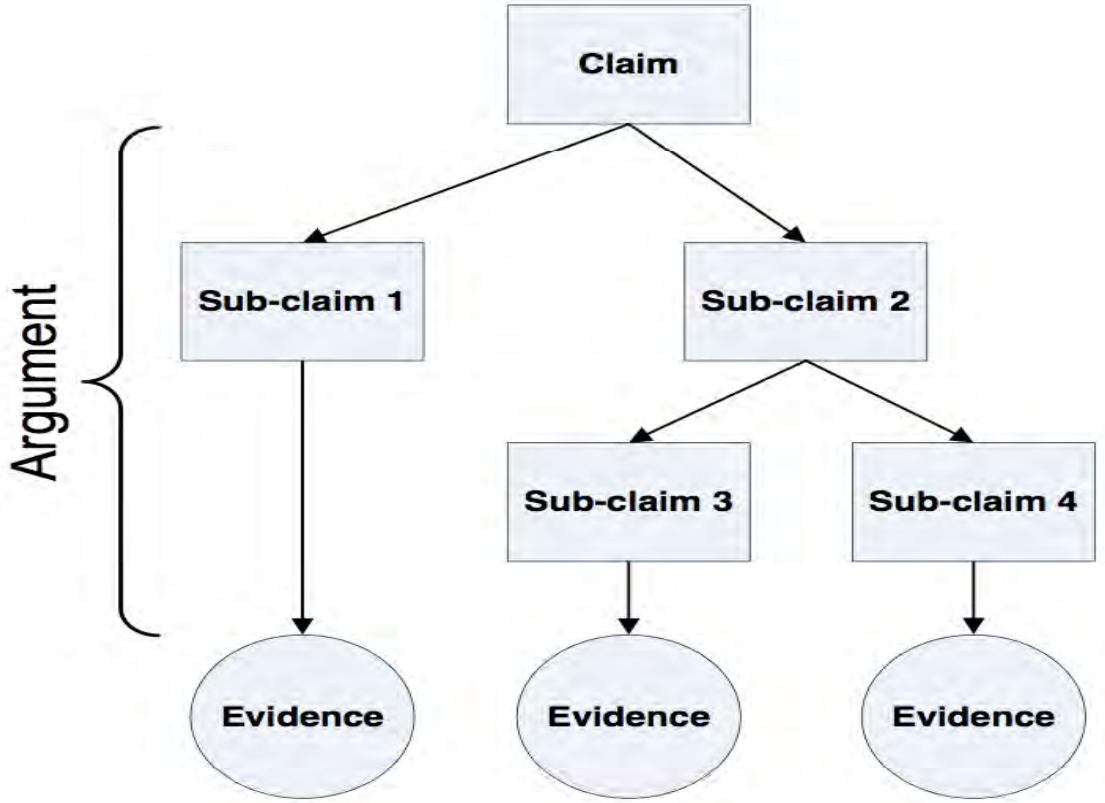
ISO/IEC 15026: A Four-Part Standard

- Planned parts:
  - **15026-1: Concepts and vocabulary (initially a TR2 and then revised to be an IS)**
  - **15026-2: Assurance case (including planning for the assurance case itself)**
  - **15026-3: System integrity levels (a revision of the 1998 standard)**
  - **15026-4: Assurance in the life cycle (including project planning for assurance considerations)**
- Possible additional parts as demand requires and resources permit, e.g.
  - **Assurance analyses and techniques**
  - **Guidance documents**

Making Security Measurable™

ISO/IEC 15026: Systems & Software Assurance

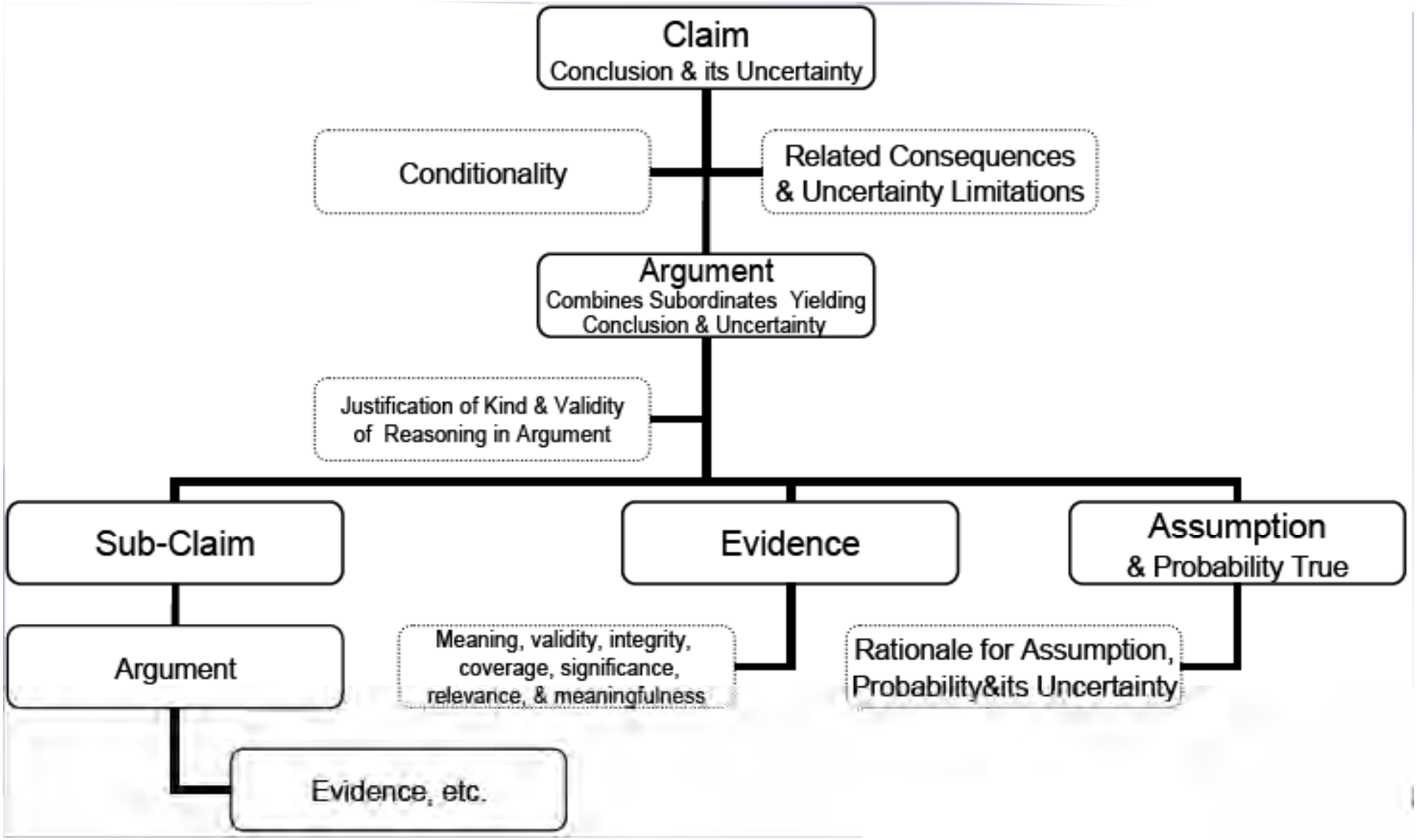
15026 Part 2: The Assurance Case (Claims-Evidence-Argument)



Making Security Measurable™

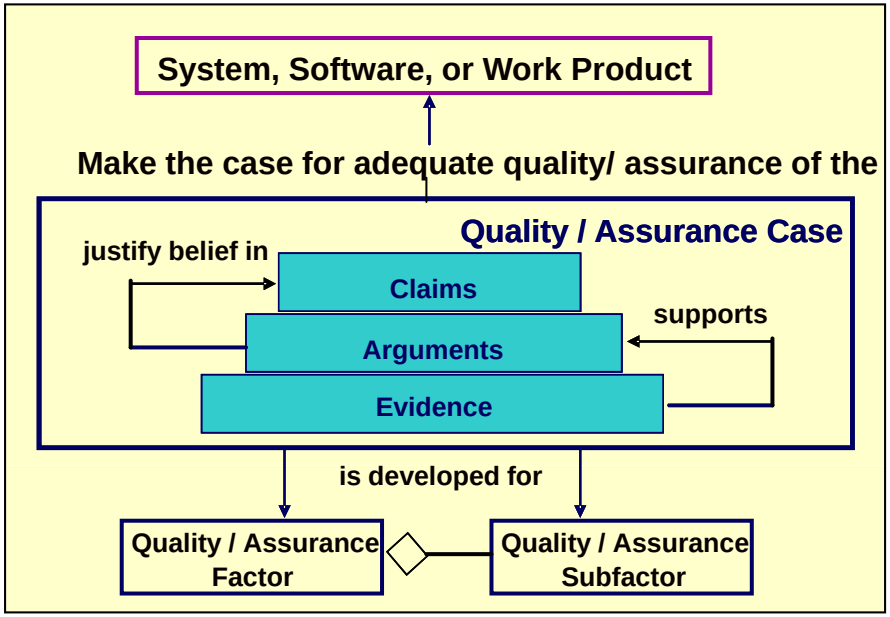
ISO/IEC 15026: Systems & Software Assurance

15026 Part 2: The Assurance Case (Claims-Evidence-Argument)



ISO/IEC/IEEE 15026 Assurance Case

- **Set of structured assurance claims, supported by evidence and reasoning (arguments), that demonstrates how assurance needs have been satisfied.**
  - Shows compliance with assurance objectives
  - Provides an argument for the safety and security of the product or service.
  - Built, collected, and maintained throughout the life cycle
  - Derived from multiple sources



- **Sub-parts**
  - A high level summary
  - Justification that product or service is acceptably safe, secure, or dependable
  - Rationale for claiming a specified level of safety and security
  - Conformance with relevant standards & regulatory requirements
  - The configuration baseline
  - Identified hazards and threats and residual risk of each hazard / threat
  - Operational & support assumptions

Attributes

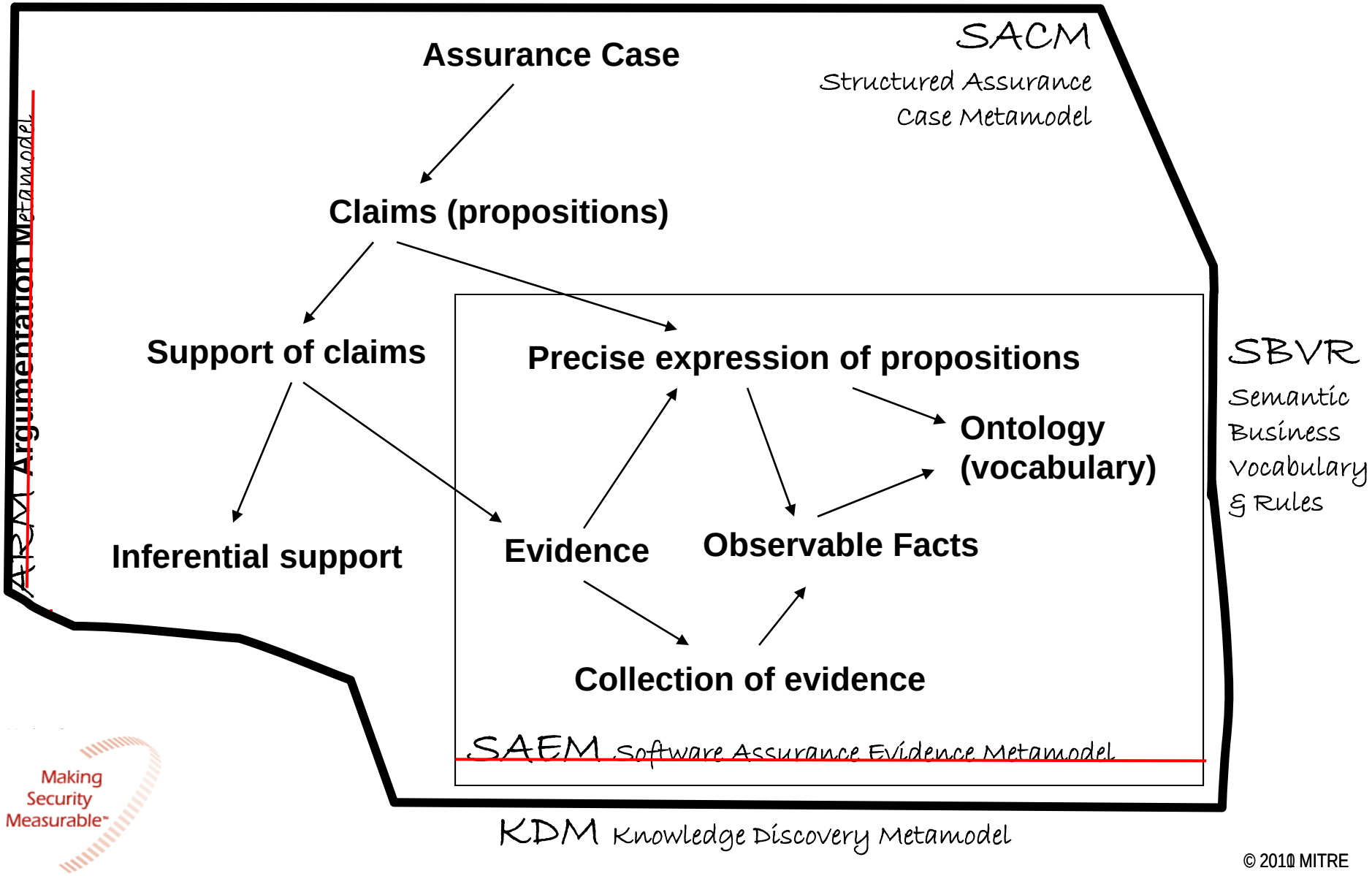
- ❑ Clear
- ❑ Consistent
- ❑ Complete
- ❑ Comprehensible
- ❑ Defensible
- ❑ Bounded
- ❑ Addresses all life cycle stages

Structured Assurance Case Efforts at the OMG

- There are efforts underway within the Object Management Group (OMG) to leverage existing standards and develop new standards for specifying ISO 15026 structured assurance cases in such a way that they will fully support automation
  - **Currently working to integrate two draft standards (the Argumentation Metamodel (ARM) and the Software Assurance Evidence Metamodel (SAEM)) into a single standard (Structured Assurance Case Metamodel (SACM)) for structured assurance case specification**
  - **SACM will also likely leverage the existing OMG Knowledge Discovery Metamodel (KDM) and Semantic Business Vocabulary & Rules (SBVR) standards**

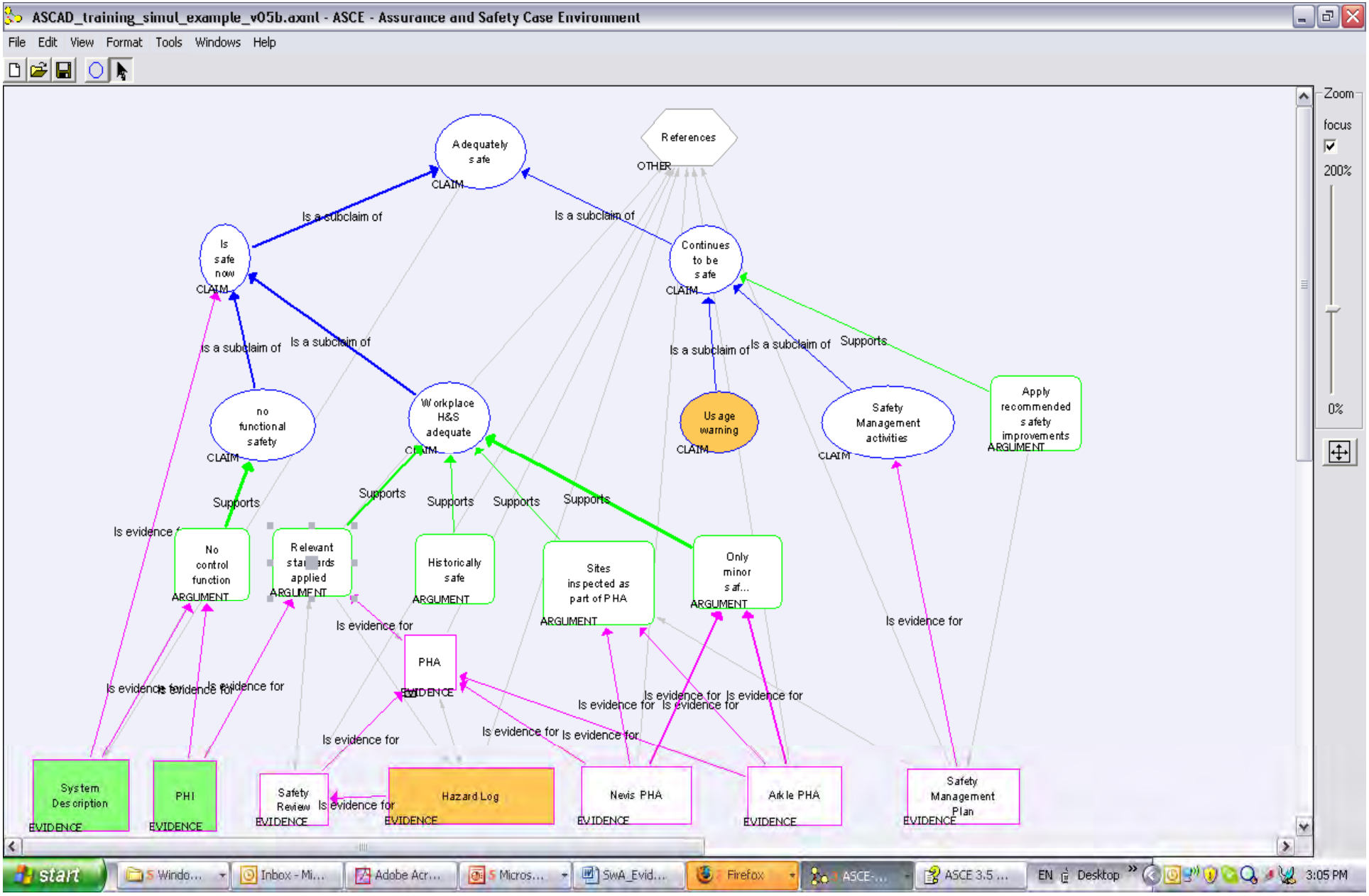
Making Security Measurable™

Object Management Group (OMG)
Systems Assurance Task Force
Claims-Evidence-Arguments Overview



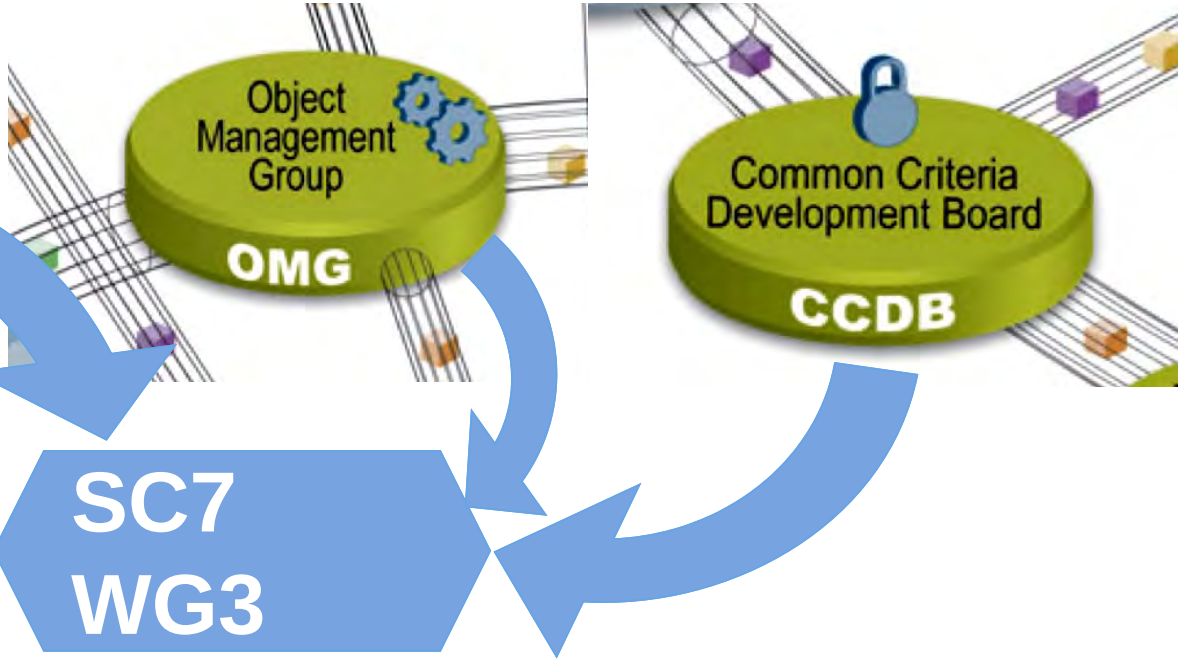
Making Security Measurable™

Structured Safety Assurance tools are commercially available



Use Cases

- Unambiguous specification of security requirements along with clear identification of what evidence will be acceptable to prove them
  - **Unambiguously bound scope of effort**
  - **Focus training and resource management on skills that are actually needed for a given context**
  - **Acquire the appropriate tools and services that are actually needed for a given context**
  - **Enable Acquisition to clearly communicate required assurance and what evidence will be required along with the delivered product**
  - **Guide Security Engineering**
  - **Guide Assurance Analysis**
  - **Guide Testing**
  - **Guide Independent Assessment & Evaluation**
  - **Empower accountability and liability**
- Structured Assurance Cases are composable and reusable



ISO IEC

ISO/IEC JTC 1/SC 27 NXXXX

ISO/IEC JTC 1/SC 27/WG x NXXXXX

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

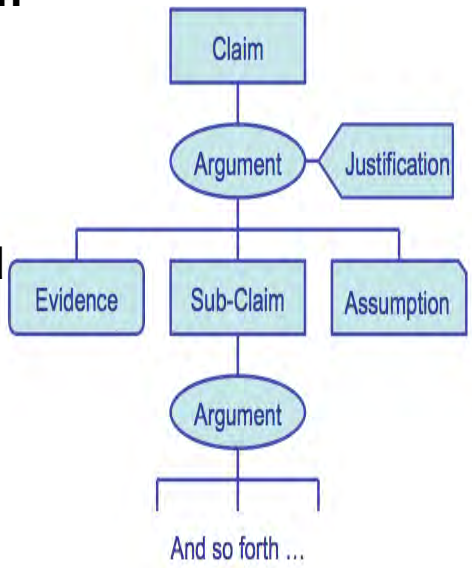
Secretariat: DIN, Germany

DOC TYPE:	NB NWI Proposal for a technical report (TR)
TITLE:	National Body New Work Item Proposal on "Secure software development and evaluation under ISO/IEC 15408 and ISO/IEC 18045"
SOURCE:	INCITS/CS1, National Body of (JS)
DATE:	2010-09-10
PROJECT:	15408 and 18045
STATUS:	This document is circulated for consideration at the forthcoming meeting of SC 2 WG 3 to be held in Redmond (WA, USA) on 2nd – 6th November 2010.
ACTION ID:	ACT
DUE DATE:	
DISTRIBUTION:	P-, O- and L-Members W. Fumy, SC 27 Chairman M. De Soete, SC 27 Vice-Chair E. J. Humphreys, K. Naemura, M. Bañón, M.-C. Kang, K. Rannenberg, WG-Convenors
MEDIUM:	Live ink-server
NO. OF PAGES:	xx

Secretariat ISO/IEC JTC 1/SC 27 –
DIN Deutsches Institut für Normung e. V., Burggrafenstr. 6, 10772 Berlin, Germany
Telephone: + 49 30 2601-0000; Facsimile: + 49 30 2601-1723; E-mail: krystyna.passia@din.de
HTTP://www.jtc1-sc27.din.de/en

Common Criteria v4 CCDB

- **TOE to leverage CAPEC & CWE**
- **ISO/IEC JTC 1/SC 7/WG 3, TR 20004: "Refining Software Vulnerability Analysis Under ISO/IEC 15408 and ISO/IEC 18045"**
- **Also investigating how to leverage ISO/IEC 15026 and OMG's Structured Assurance Case Metamodel (SACM)**



NIAP (U.S.) Evaluation Scheme

- **Above plus**
- **Also investigating how to leverage SCAP**

Questions?

ramartin@mitre.org