HS SEDI
Homeland Security Systems Engineering and
Development Institute

Supporting *Secure Software Acquisition* and *Software Assurance Analysis*

Homeland Security

Software Assurance Analysis & Acquisition

- **Where foundational knowledge about software security is the requirement for Training & Education and Software Security Engineering, a little bit more is required for Secure Software Acquisition and Software Assurance Analysis**
- **To unambiguously define, measure and achieve a desired level of assurance in the products we buy, build and use requires:**
  - Some way to clearly specify the assurance requirements and what level of proof of compliance will be required
  - Some way to practically pull together, analyze and evaluate the measurement results against the specified assurance requirements
  - Some way to understand and prioritize identified gaps between the assurance requirements and the actual product in such a way that intelligent mitigation/remediation decisions can be made
- **This portion of the tutorial will focus on resources/efforts focused at addressing these three needs**

Software Assurance Analysis & Acquisition

- Some way to clearly specify the assurance requirements and what level of proof of compliance will be required

Structured Assurance Cases

- Some way to practically pull together, analyze and evaluate the measurement results against the specified assurance requirements

Software Assurance Findings Expression Schema (SAFES)

- Some way to understand and prioritize identified gaps between the assurance requirements and the actual product in such a way that intelligent mitigation/remediation decisions can be made

Common Weakness Scoring System (CWSS)

HS SEDI
Homeland Security Systems Engineering and
Development Institute

Structured Assurance Cases

Framing the Appropriate Context for Measurable Assurance

Sean Barnum
MITRE

Homeland Security

What Is an Assurance Case?

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**

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.”

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.

Structured Assurance Cases

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

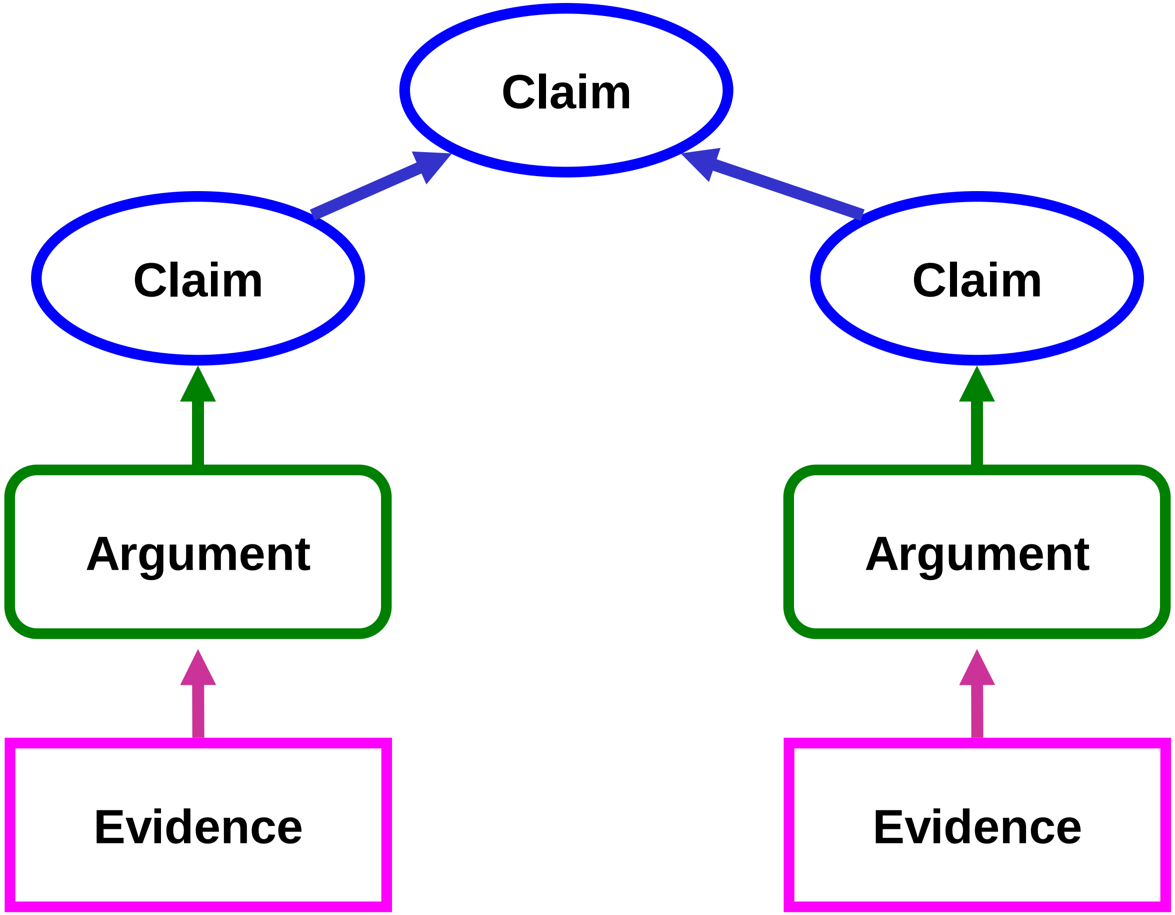
- **Structured Assurance Cases are composed of structured sets of Claims, Arguments and Evidence**
  - A Claim is a proposition to be assured about the system of concern
  - An Argument is a reasoning of why a claim is true
  - Evidence is either a fact, a datum, an object, a claim or [recursively] an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

Extremely Simplified Overview of Structured Assurance Case Content

Claim =
assertion to be proven

Argument =
reasoning supporting a claim

Evidence =
data supporting an Argument



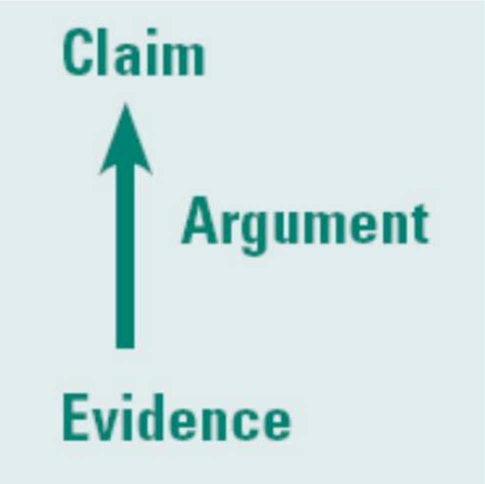
Need for Standards

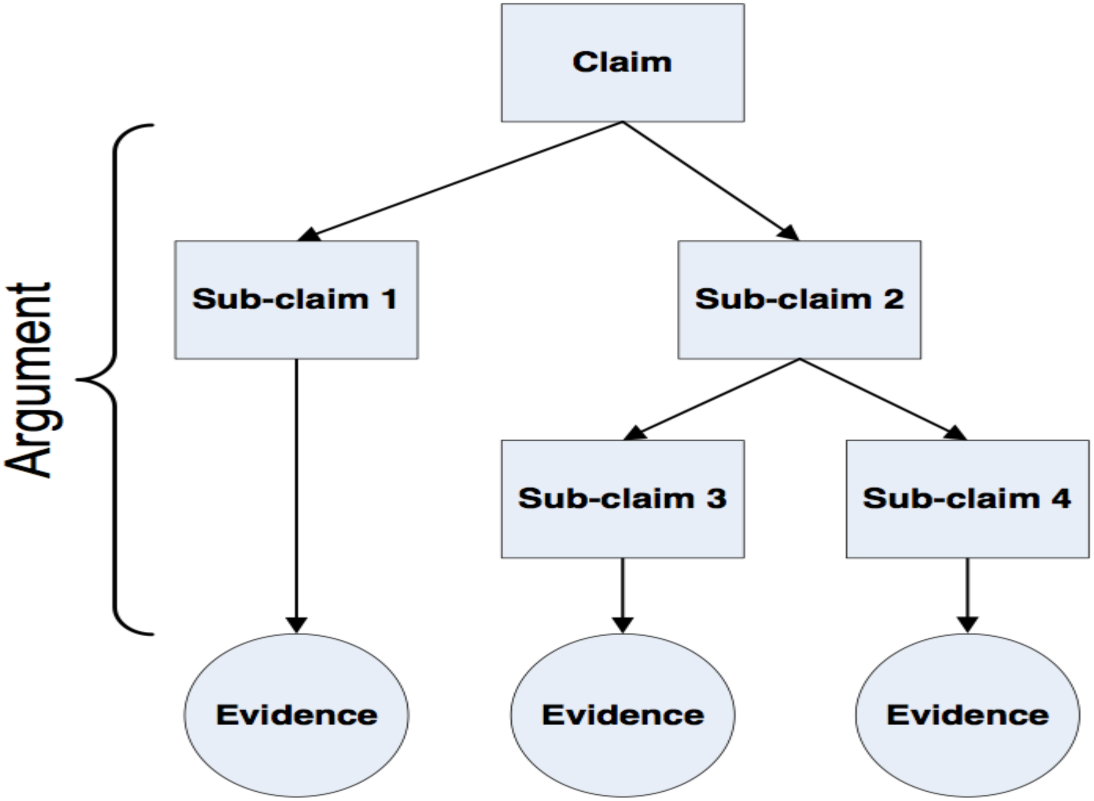
- **While several different notations exist for safety cases and generalized assurance cases no widely accepted standard currently exists for specifying structured assurance cases within a systems & software assurance domain**
- **Standards are needed before structured assurance cases can be widely leveraged 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

ISO/IEC 15026: A Four-Part Standard

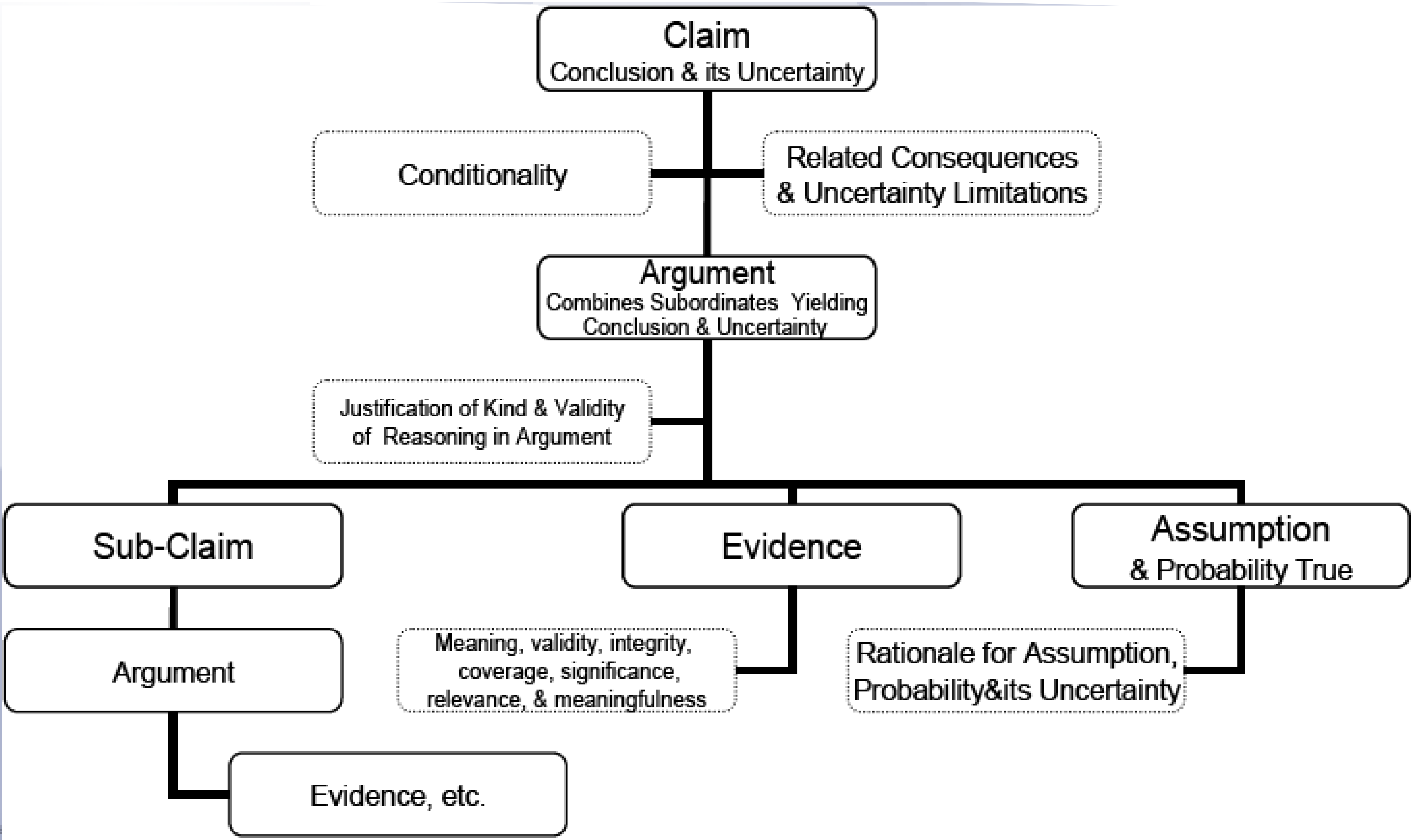
- **Planned parts:**
  - 15026-1: Concepts and vocabulary (initially a TR2 and then revised to be an IS)
  - 15026-2: Assurance case (including planning for the assurance case itself)
  - 15026-3: System integrity levels (a revision of the 1998 standard)
  - 15026-4: Assurance in the life cycle (including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

ISO/IEC 15026: Systems & Software Assurance
15026 Part 2: The Assurance Case (Claims-Evidence-Argument)



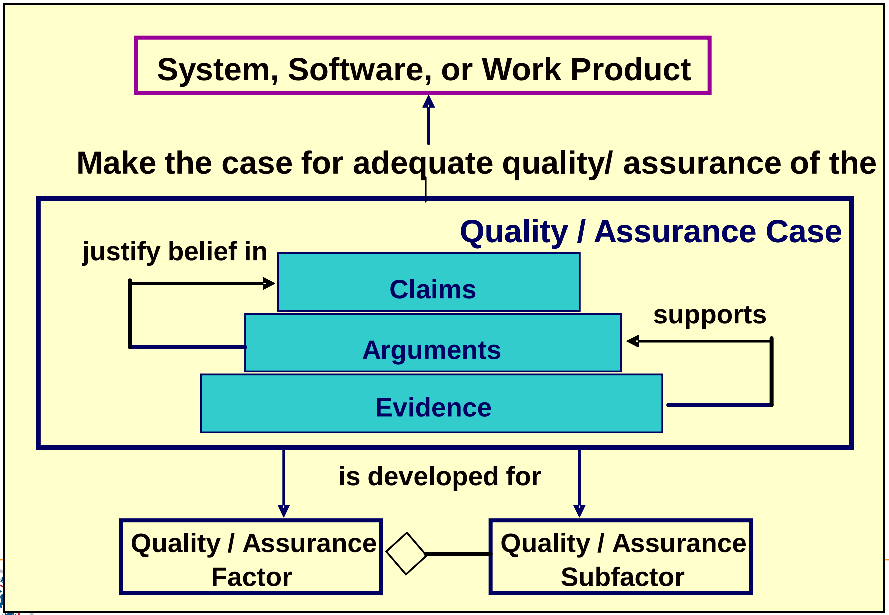


ISO/IEC 15026: Systems & Software Assurance
15026 Part 2: The Assurance Case (Claims-Evidence-Argument)


Claim
Conclusion & its Uncertainty
Conditionality
Related Consequences & Uncertainty Limitations
Argument
Combines Subordinates Yielding Conclusion & Uncertainty
Justification of Kind & Validity of Reasoning in Argument
Sub-Claim
Evidence
Assumption & Probability True
Argument
Meaning, validity, integrity, coverage, significance, relevance, & meaningfulness
Rationale for Assumption, Probability&its Uncertainty
Evidence, etc.

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


System, Software, or Work Product
Make the case for adequate quality/ assurance of the
Quality / Assurance Case
justify belief in
Claims
Arguments
Evidence
supports
is developed for
Quality / Assurance Factor
Quality / Assurance Subfactor

- **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

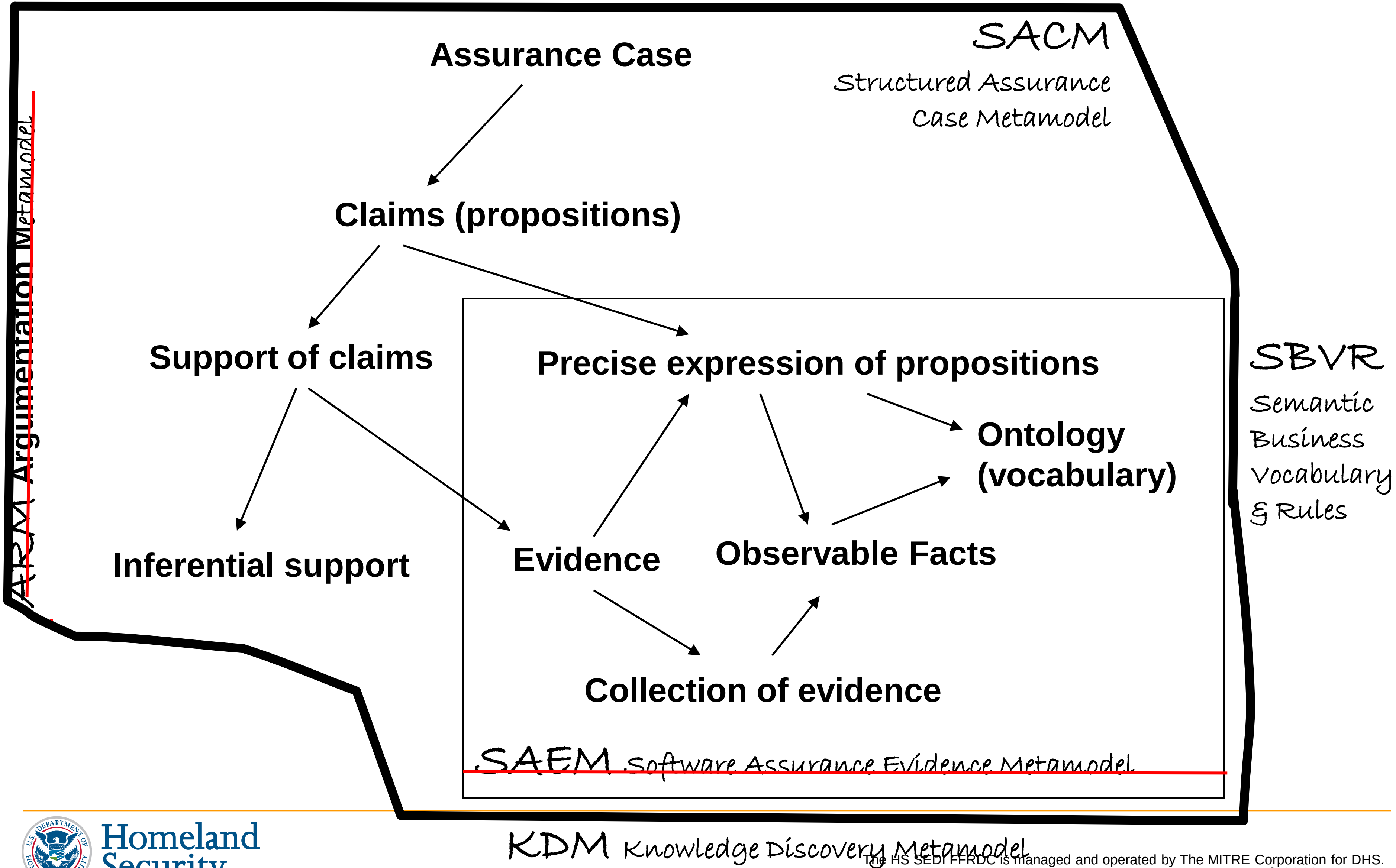
Attributes

- ❑ **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

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



SACM
Structured Assurance
Case Metamodel

Assurance Case

Claims (propositions)

Support of claims

Precise expression of propositions

Ontology
(vocabulary)

Inferential support

Evidence

Observable Facts

Collection of evidence

SAEM Software Assurance Evidence Metamodel

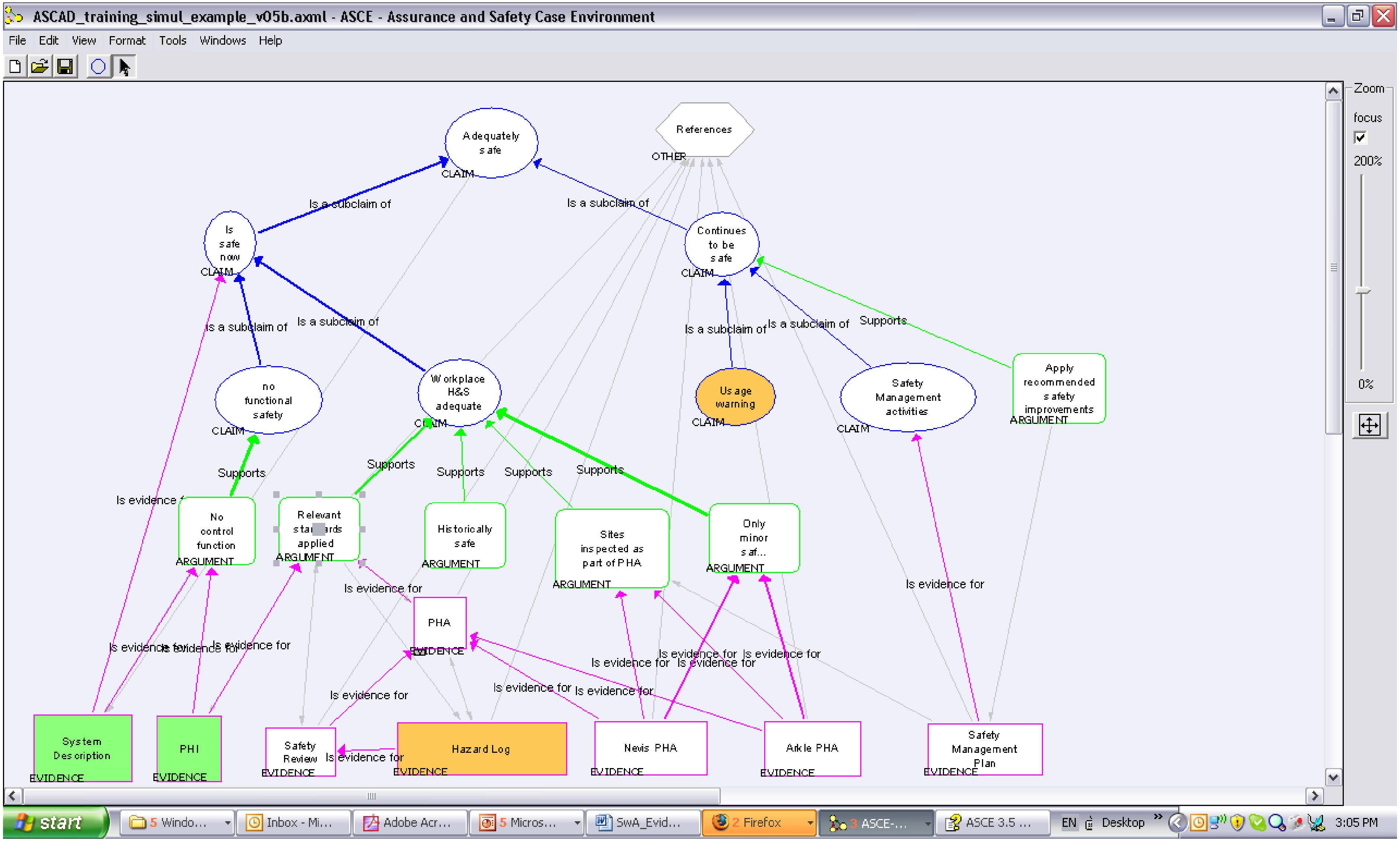
KDM Knowledge Discovery Metamodel

SBVR
Semantic
Business
Vocabulary
& Rules

ARM Argumentation Metamodel

Structured Safety Assurance tools are commercially available

HS SEDI
Homeland Security Systems Engineering and Development Institute

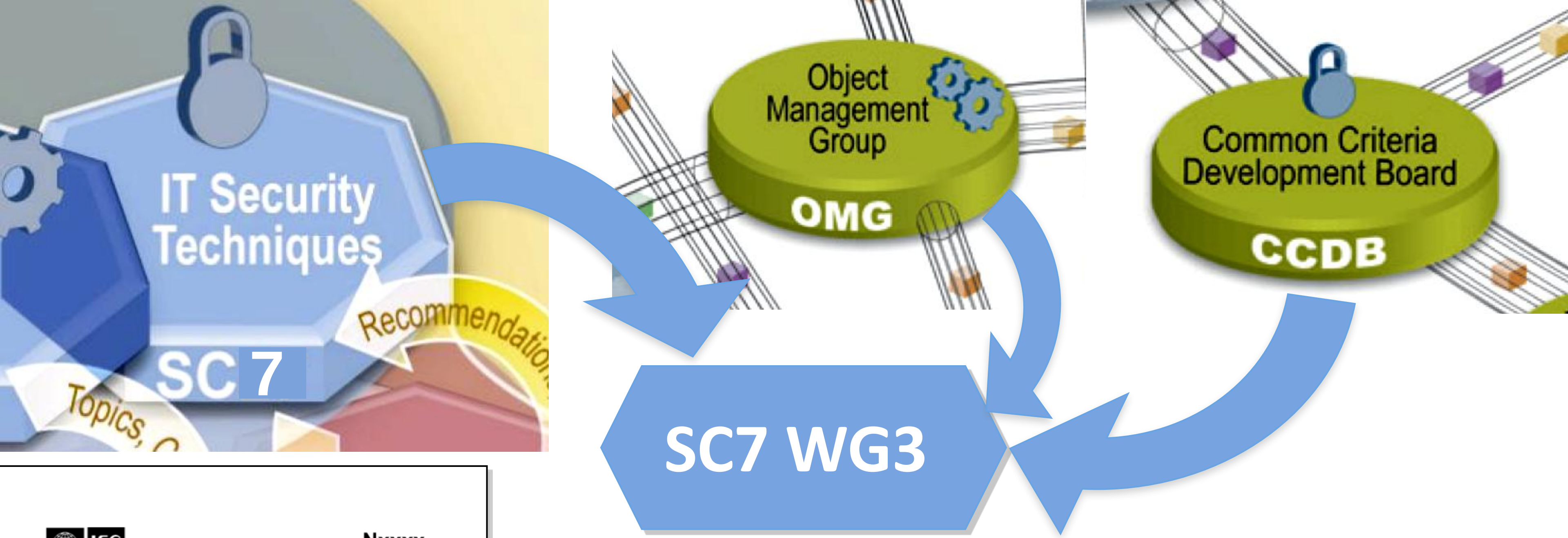


Homeland Security

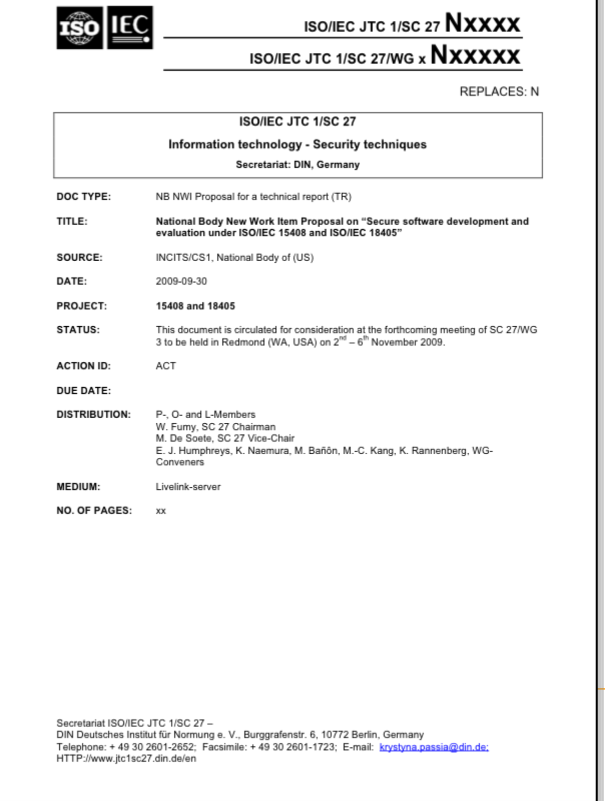
The HS SEDI FFRDC is managed and operated by The MITRE Corporation for DHS.

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**



SC7 WG3



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 18405"**
SOURCE:	INCITS/CS1, National Body of (US)
DATE:	2009-09-30
PROJECT:	**15408 and 18405**
STATUS:	This document is circulated for consideration at the forthcoming meeting of SC 27/WG 3 to be held in Redmond (WA, USA) on 2nd – 6th November 2009.
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. Bañôn, M.-C. Kang, K. Rannenberg, WG-Conveners
MEDIUM:	Livelink-server
NO. OF PAGES:	xx

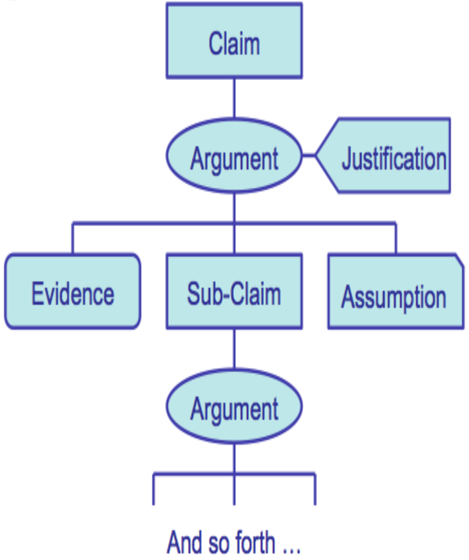
Secretariat ISO/IEC JTC 1/SC 27 –
DIN Deutsches Institut für Normung e. V., Burggrafenstr. 6, 10772 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-1723; E-mail: krystyna.passia@din.de;
HTTP://www.jtc1sc27.din.de/en

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?

Sean Barnum
MITRE
sbarnum@mitre.org

LUNCH

HS SEDI

Homeland Security Systems Engineering and Development Institute

Taming the Tower of Babel: Software Assurance Findings Expression Schema (SAFES)

SAFES

Sean Barnum

MITRE

Homeland Security

Today's Challenge

- **There is no standard reporting format for SwA analysis**
  - Very difficult to combine results of multi-perspective analysis
  - Very difficult to combine results of multi-tool analysis
  - Very inefficient for tool vendors looking to integrate results with other tools (very costly and redundant)
  - Very difficult to trend across assessments from different tools or analysts
  - Very difficult to automate meta-analysis and the assessment process

SAFES Effort

- **Software Assurance Findings Expression Schema (SAFES)**

- **Sponsored by the NSA Center for Assured Software (CAS)**
- **Objectives:**
  - Enable and encourage consistency in software assurance tool, service and analysis practice findings
  - Establish more structured and effectively useful software assurance tool, service and analysis practice results
  - Enable integration of results from multiple software assurance tools, services or analysis practices
  - Enable automated processing of software assurance tool, service or analysis practice results

What is SAFES?

- SAFES in its current form and near-term future is NOT intended to be a *formal* standard
- SAFES is NOT intended to duplicate or replace existing formal standards
- SAFES is intended to fill a gap in the overall standards architecture and adoption approach while aligning and integrating with relevant standards (or portions thereof) as appropriate
- SAFES is an organically emergent common format with minimal burden of change for stakeholders and immediate usefulness

SAFES Approach

Phase 1

- Community collaboration
- Build from state of the practice (considered ~20 tools & services)
- Enhance with state of the art
- Define a comprehensive schema covering all aspects of software assurance analysis reporting

Phase 2

- Enable & demonstrate practical use

Future

- Continually refine for coverage, consistency & efficiency
- Layer the schema into a framework for composable and focused use
- Strive for flexibility and extensibility
- Mature towards formalization

SAFES Initial Scope

- **In-scope perspectives for initial effort:**
  - Static source code analysis
  - Static binary code analysis
  - Web application penetration testing
  - Data security analysis
  - Fuzzing
  - Threat modeling
  - Architectural risk analysis
- **Some vendors actively collaborating others were passively incorporated**

SAFES is a comprehensive and detailed schema

- Info on findings
  - Description
  - Categorization
  - Location
  - Prioritization
  - Correlations
- Info on analysis approach
  - Tool or service
  - Methodology
  - Detection mechanisms

- Info on mitigation
- Info on meta-analysis
- Info on personnel
- Info on application
  - Structure, content & configuration
  - Business/mission and security context
- Info on assurance case
- Info on threat analysis

Key Constructs

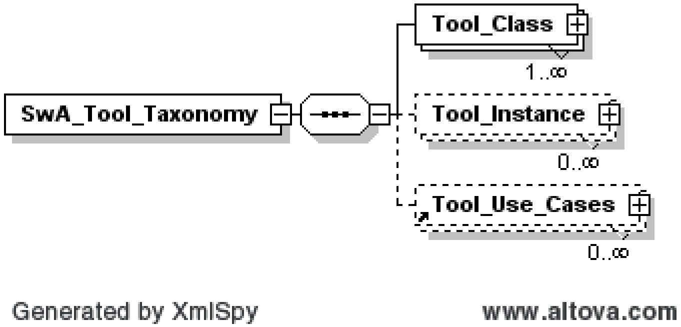
- Sub-Assessment scopes
- Traces
- Report views
- Assurance case
- Finding prioritization
- Tool-Service info
- Findings correlations

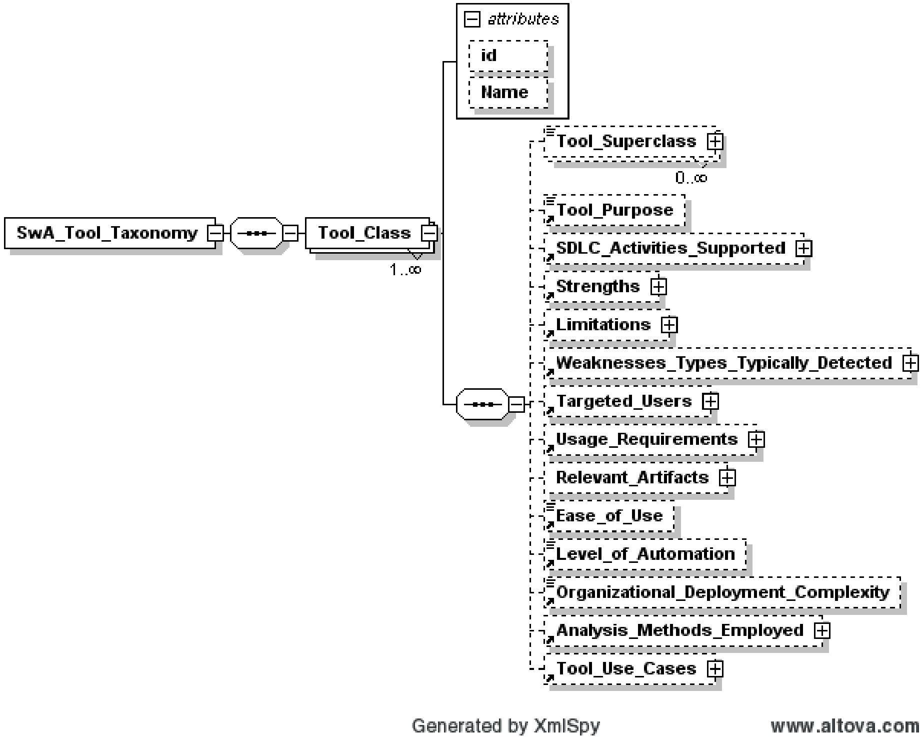
A Sampling of Potential Use Cases

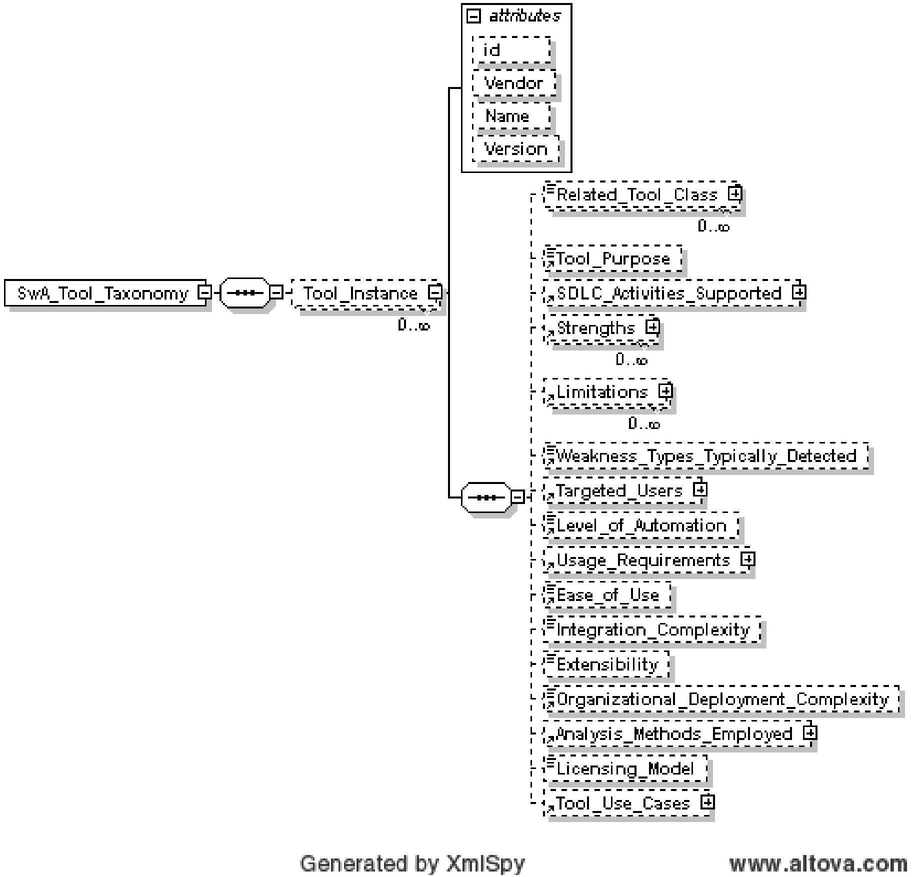
- Understand the Business Context of application
- Identify risks
- Map technical risks to business context
- Map the application attack surface
- Identify relevant threats
- Inventory and characterize assets
- Create threat model
- Define FISMA security categorization (FIPS-199)
- FISMA Security Planning (SP800-18)
- FISMA Risk Assessment (SP800-30)
- Conduct multi-tool/multi-perspective analysis
- Identify false positives
- Characterize risk
- Prioritize risk

- Correlate findings
- Stitch dynamic & static location results
- Integrate automated and manual analysis
- Reuse common mitigation advice
- Create assessment report
- Create different versions of report
- Define an assurance case for an application
- Create an assurance case compliance report
- Import CWE content into local context
- Identify common finding trends across portfolio by technology context
- Maintain analysis accountability
- Identify trends in tool and rule efficacy
- Mapping between various tool level definitions

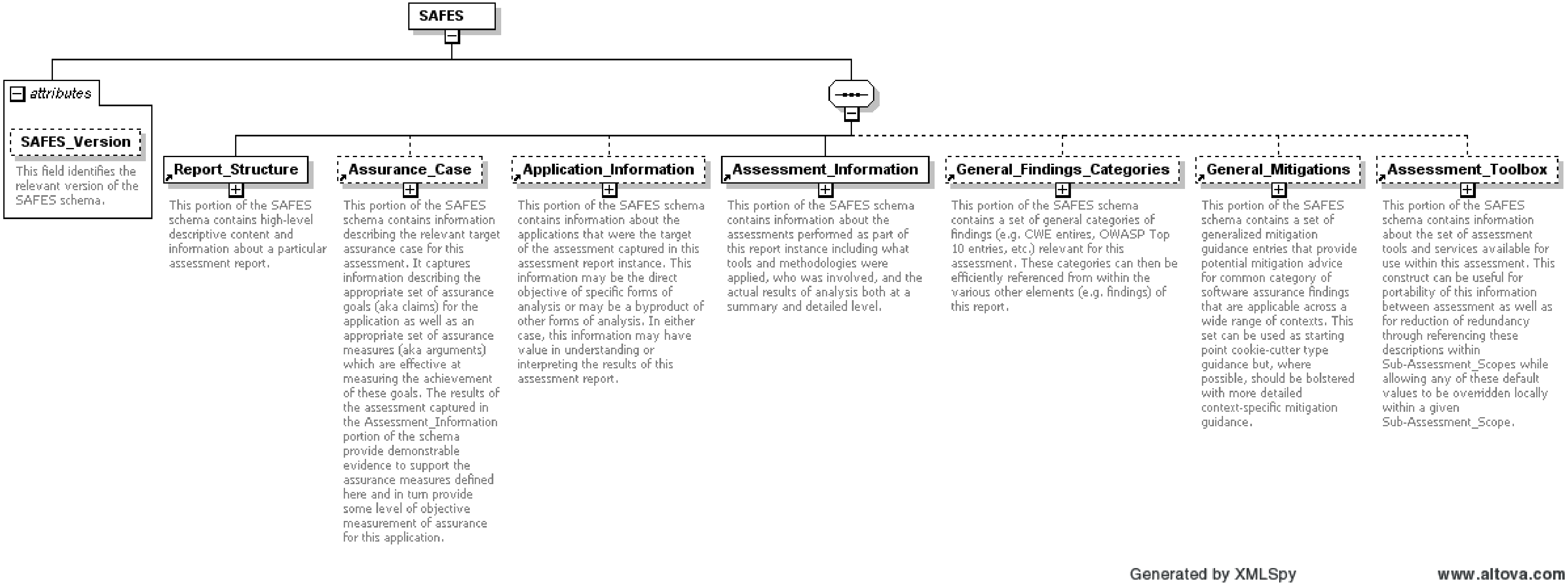
SwA Tool Taxonomy







SAFES Top View



SAFES_Version: This field identifies the relevant version of the SAFES schema.

Report_Structure: This portion of the SAFES schema contains high-level descriptive content and information about a particular assessment report.

Assurance_Case: This portion of the SAFES schema contains information describing the relevant target assurance case for this assessment. It captures information describing the appropriate set of assurance goals (aka claims) for the application as well as an appropriate set of assurance measures (aka arguments) which are effective at measuring the achievement of these goals. The results of the assessment captured in the Assessment_Information portion of the schema provide demonstrable evidence to support the assurance measures defined here and in turn provide some level of objective measurement of assurance for this application.

Application_Information: This portion of the SAFES schema contains information about the applications that were the target of the assessment captured in this assessment report instance. This information may be the direct objective of specific forms of analysis or may be a byproduct of other forms of analysis. In either case, this information may have value in understanding or interpreting the results of this assessment report.

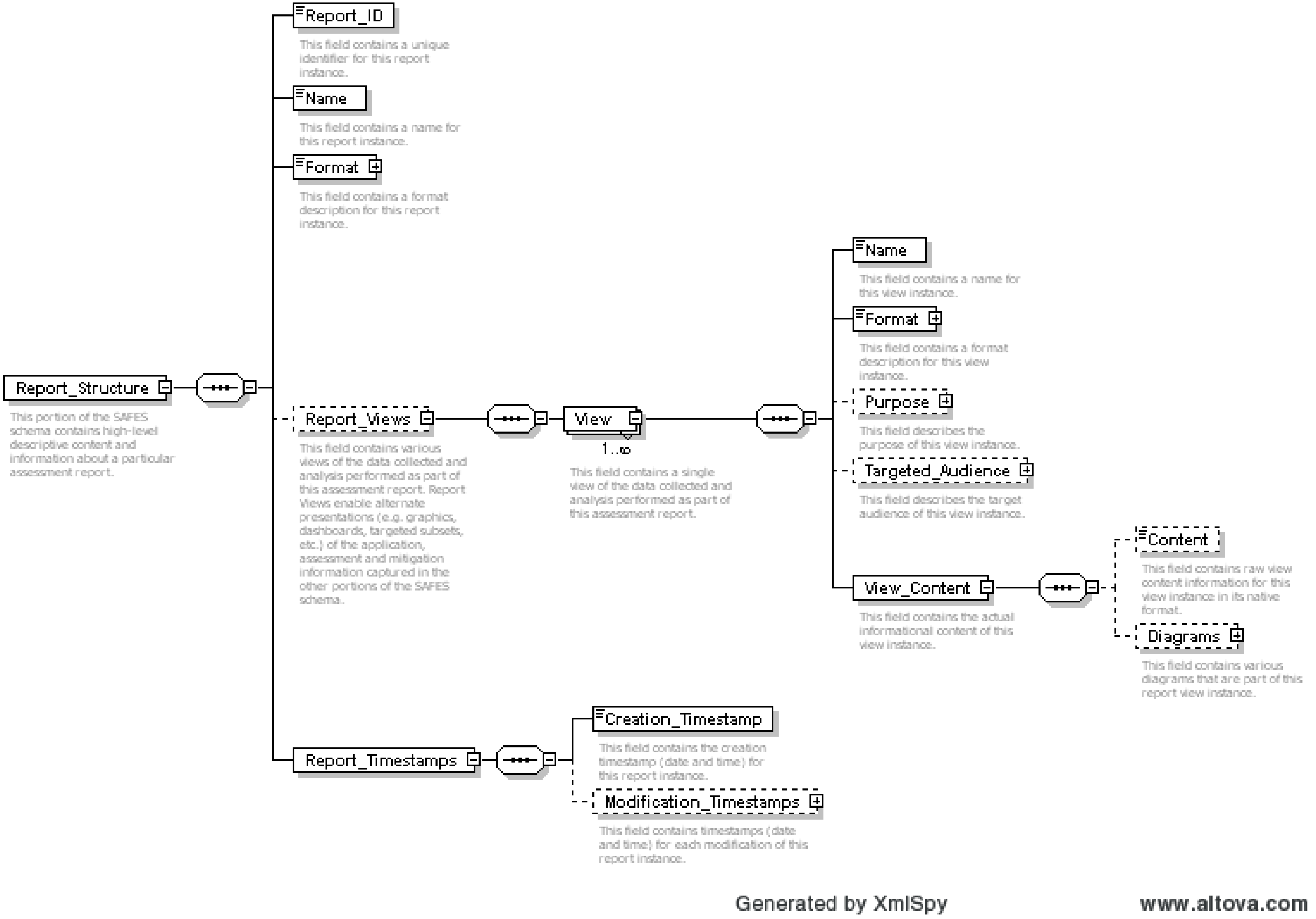
Assessment_Information: This portion of the SAFES schema contains information about the assessments performed as part of this report instance including what tools and methodologies were applied, who was involved, and the actual results of analysis both at a summary and detailed level.

General_Findings_Categories: This portion of the SAFES schema contains a set of general categories of findings (e.g. CWE entires, OWASP Top 10 entries, etc.) relevant for this assessment. These categories can then be efficiently referenced from within the various other elements (e.g. findings) of this report.

General_Mitigations: This portion of the SAFES schema contains a set of generalized mitigation guidance entries that provide potential mitigation advice for common category of software assurance findings that are applicable across a wide range of contexts. This set can be used as starting point cookie-cutter type guidance but, where possible, should be bolstered with more detailed context-specific mitigation guidance.

Assessment_Toolbox: This portion of the SAFES schema contains information about the set of assessment tools and services available for use within this assessment. This construct can be useful for portability of this information between assessment as well as for reduction of redundancy through referencing these descriptions within Sub-Assessment_Scopes while allowing any of these default values to be overridden locally within a given Sub-Assessment_Scope.

Report Structure



Report_Structure

This portion of the SAFES schema contains high-level descriptive content and information about a particular assessment report.

Report_ID

This field contains a unique identifier for this report instance.

Name

This field contains a name for this report instance.

Format

This field contains a format description for this report instance.

Report_Views

This field contains various views of the data collected and analysis performed as part of this assessment report. Report Views enable alternate presentations (e.g. graphics, dashboards, targeted subsets, etc.) of the application, assessment and mitigation information captured in the other portions of the SAFES schema.

View

1..∞

This field contains a single view of the data collected and analysis performed as part of this assessment report.

Name

This field contains a name for this view instance.

Format

This field contains a format description for this view instance.

Purpose

This field describes the purpose of this view instance.

Targeted_Audience

This field describes the target audience of this view instance.

View_Content

This field contains the actual informational content of this view instance.

Content

This field contains raw view content information for this view instance in its native format.

Diagrams

This field contains various diagrams that are part of this report view instance.

Report_Timestamps

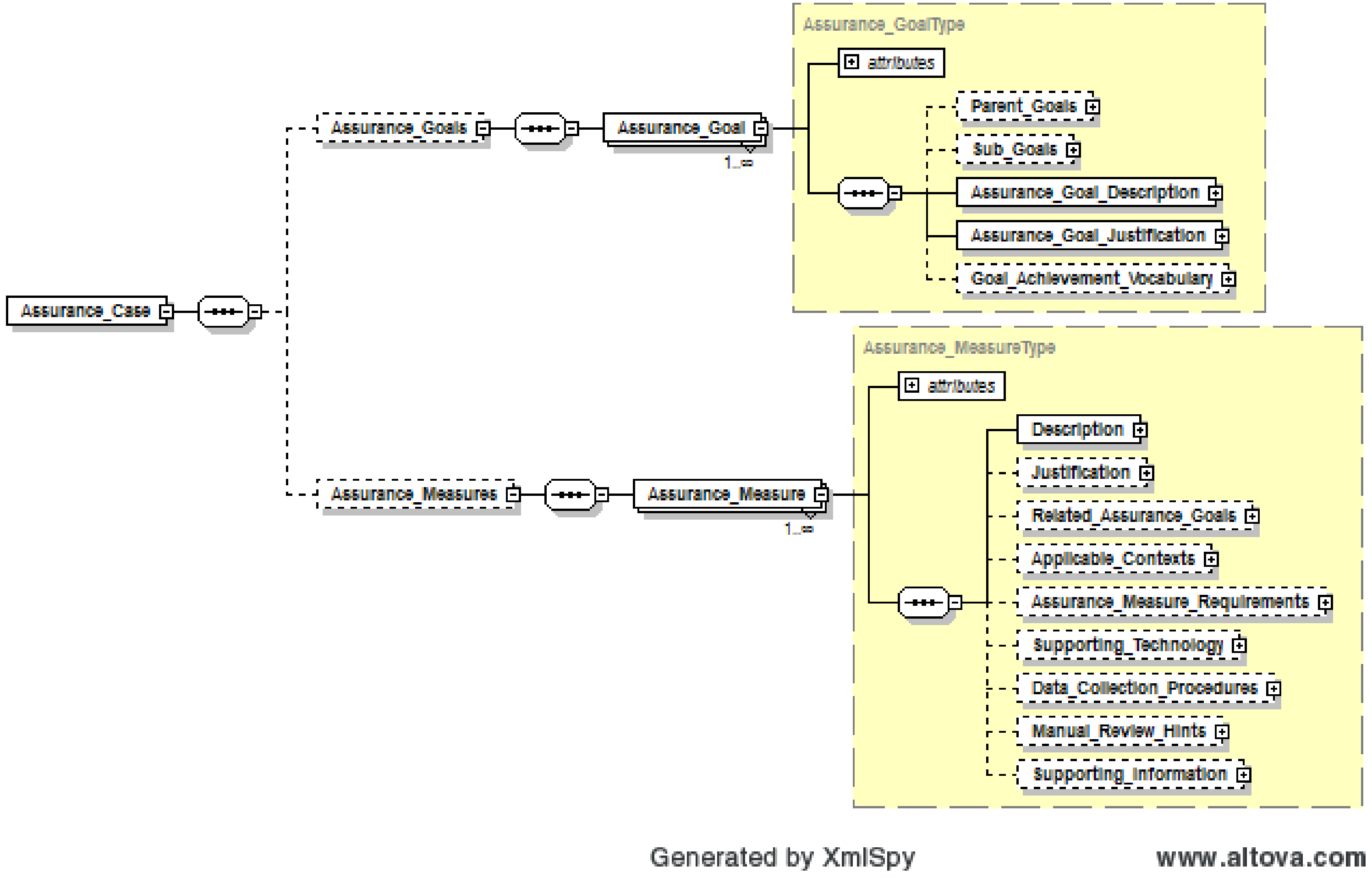
Creation_Timestamp

This field contains the creation timestamp (date and time) for this report instance.

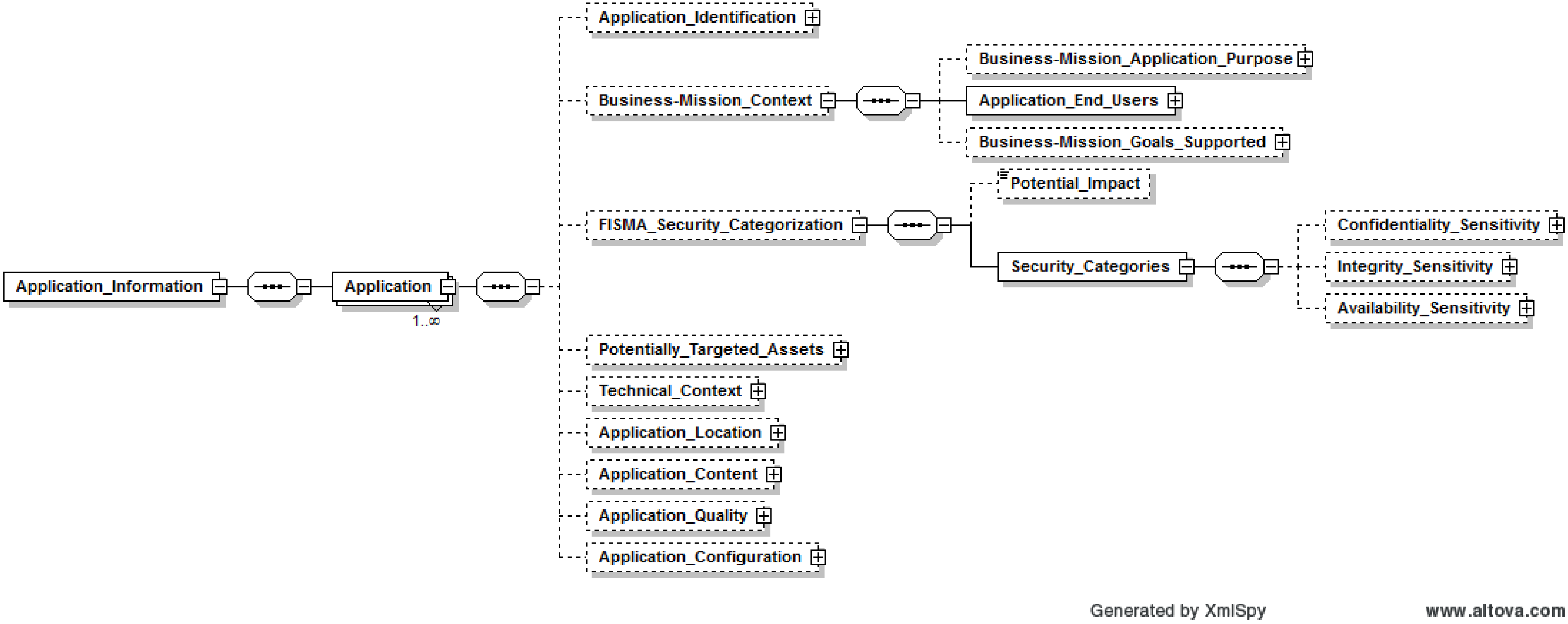
Modification_Timestamps

This field contains timestamps (date and time) for each modification of this report instance.

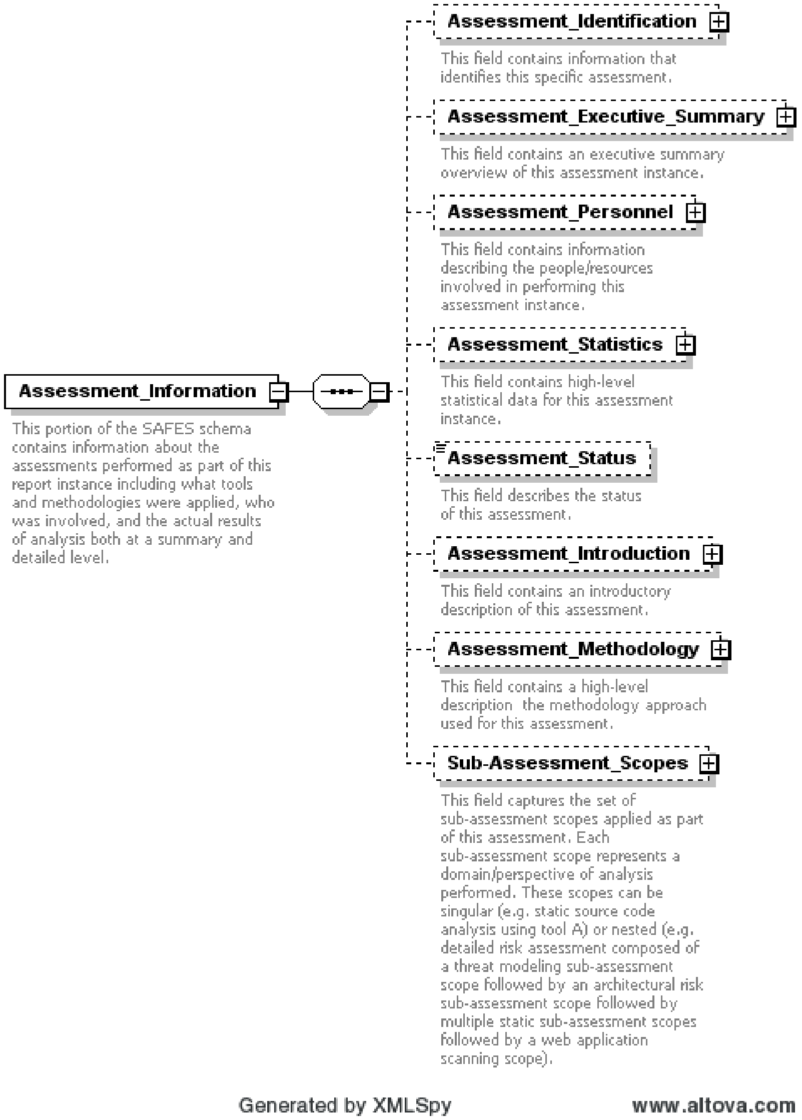
Assurance Case



Application Information



Assessment Information



Assessment_Information

This portion of the SAFES schema contains information about the assessments performed as part of this report instance including what tools and methodologies were applied, who was involved, and the actual results of analysis both at a summary and detailed level.

Assessment_Identification

This field contains information that identifies this specific assessment.

Assessment_Executive_Summary

This field contains an executive summary overview of this assessment instance.

Assessment_Personnel

This field contains information describing the people/resources involved in performing this assessment instance.

Assessment_Statistics

This field contains high-level statistical data for this assessment instance.

Assessment_Status

This field describes the status of this assessment.

Assessment_Introduction

This field contains an introductory description of this assessment.

Assessment_Methodology

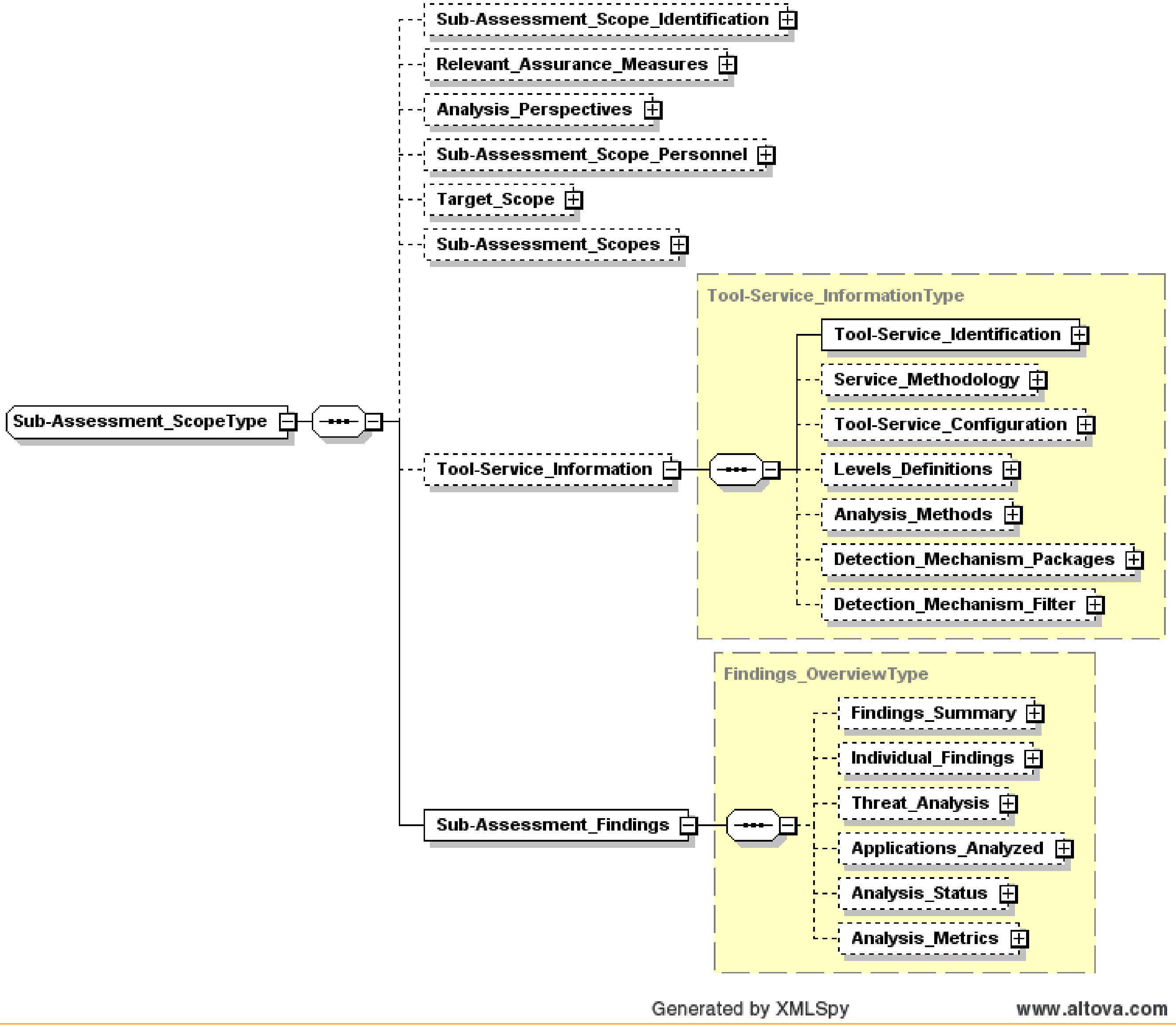
This field contains a high-level description the methodology approach used for this assessment.

Sub-Assessment_Scopes

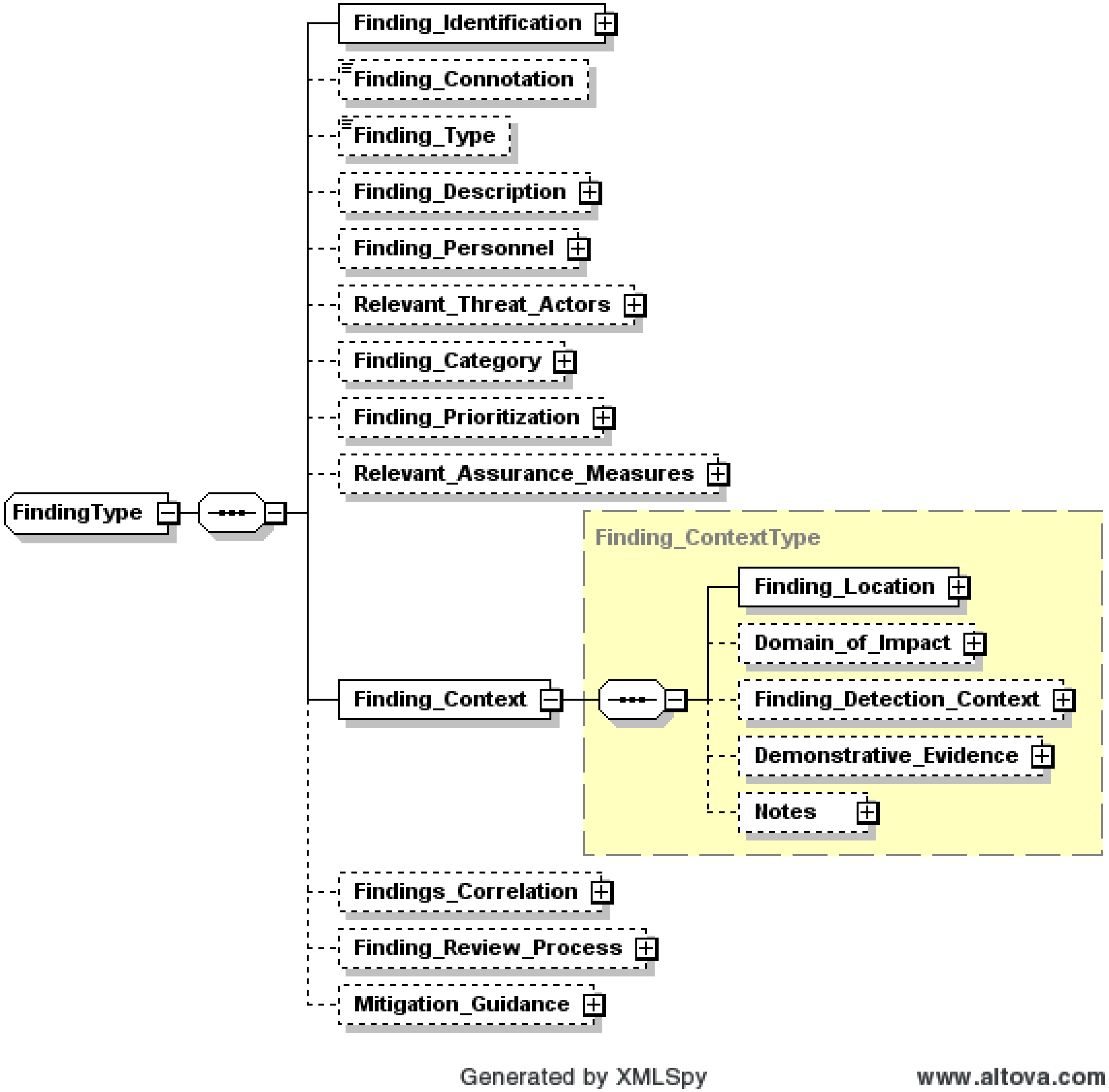
This field captures the set of sub-assessment scopes applied as part of this assessment. Each sub-assessment scope represents a domain/perspective of analysis performed. These scopes can be singular (e.g. static source code analysis using tool A) or nested (e.g. detailed risk assessment composed of a threat modeling sub-assessment scope followed by an architectural risk sub-assessment scope followed by multiple static sub-assessment scopes followed by a web application scanning scope).

Generated by XMLSpy www.altova.com

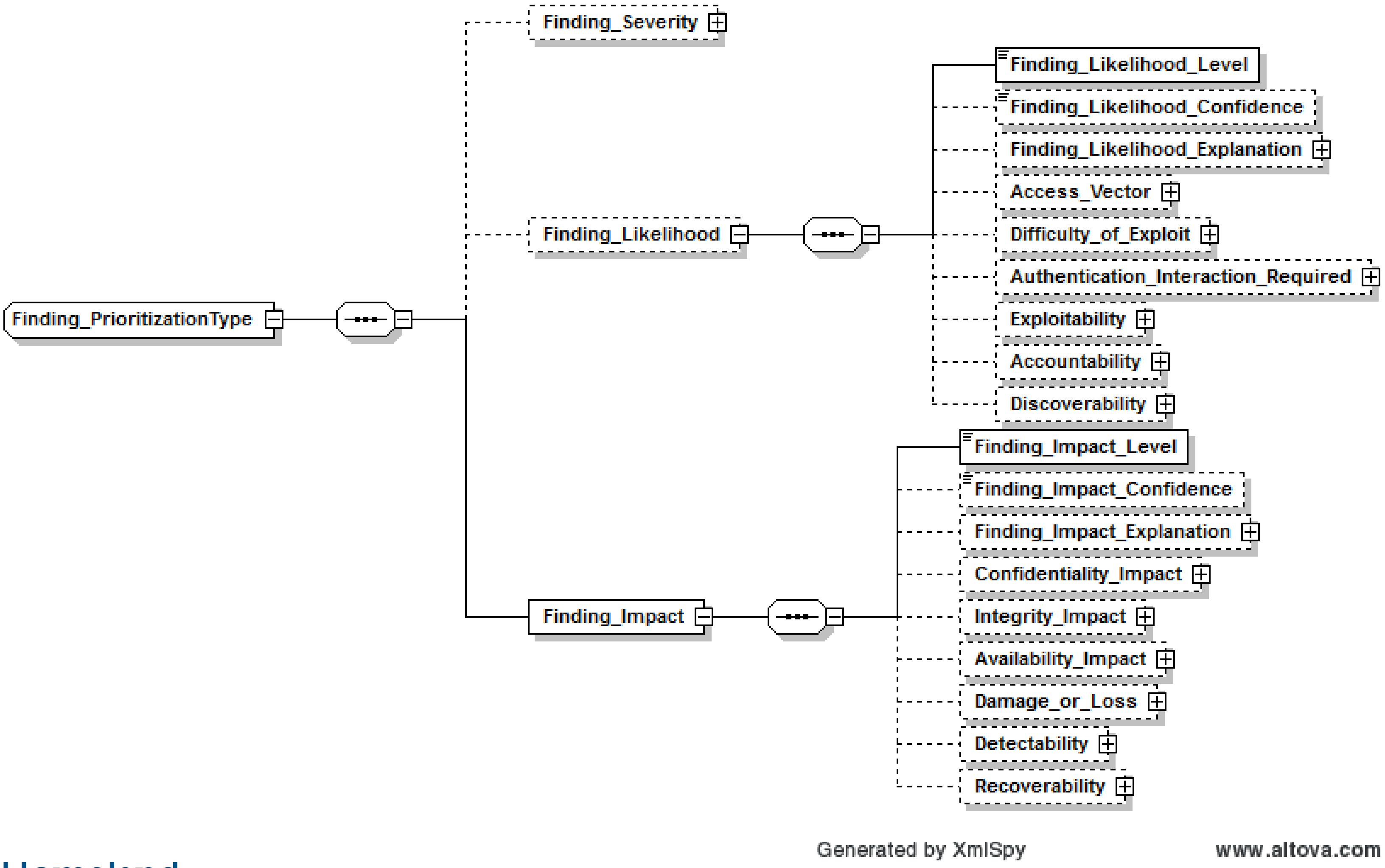
Sub-Assessment Scopes



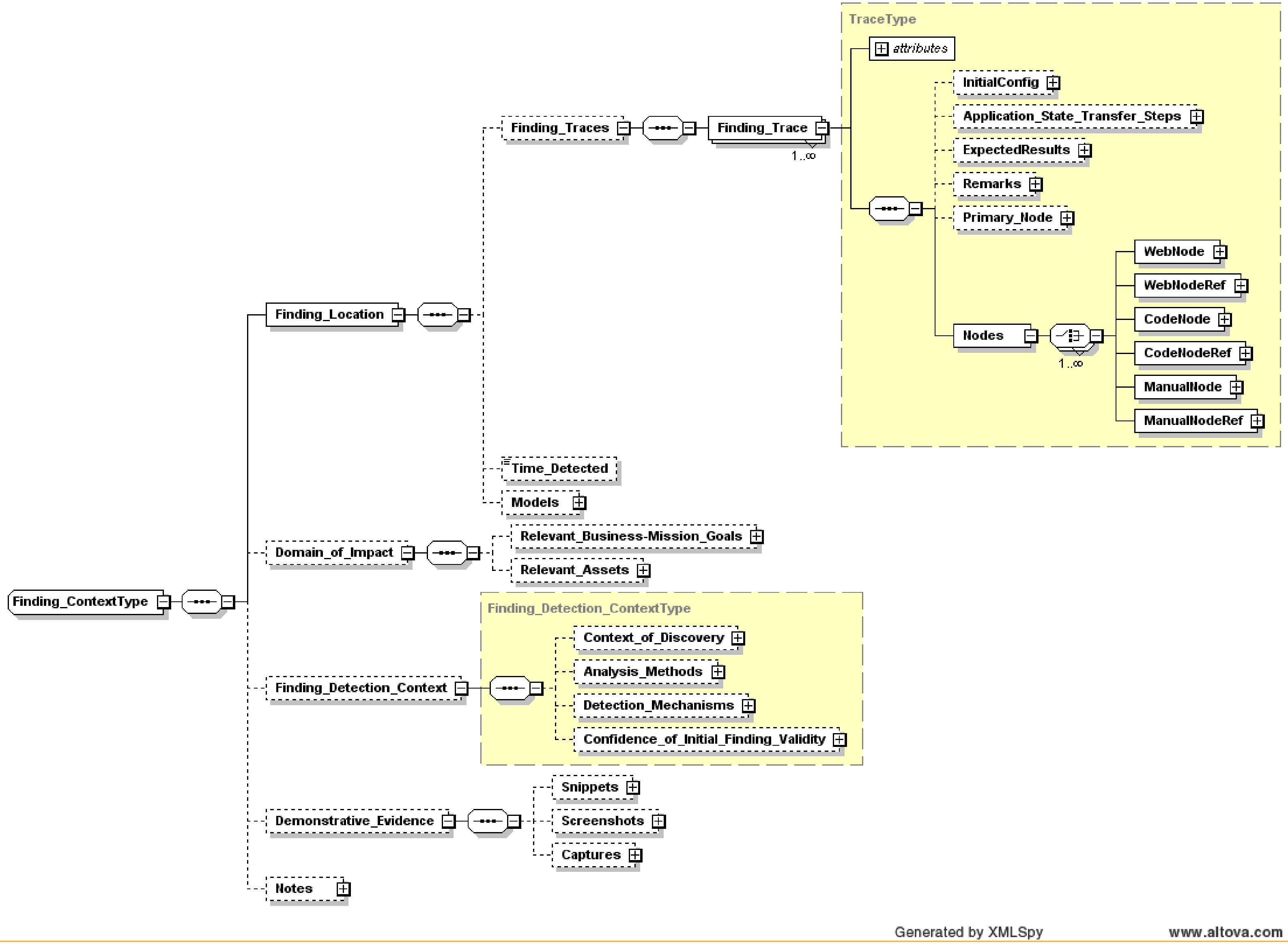
Finding Type



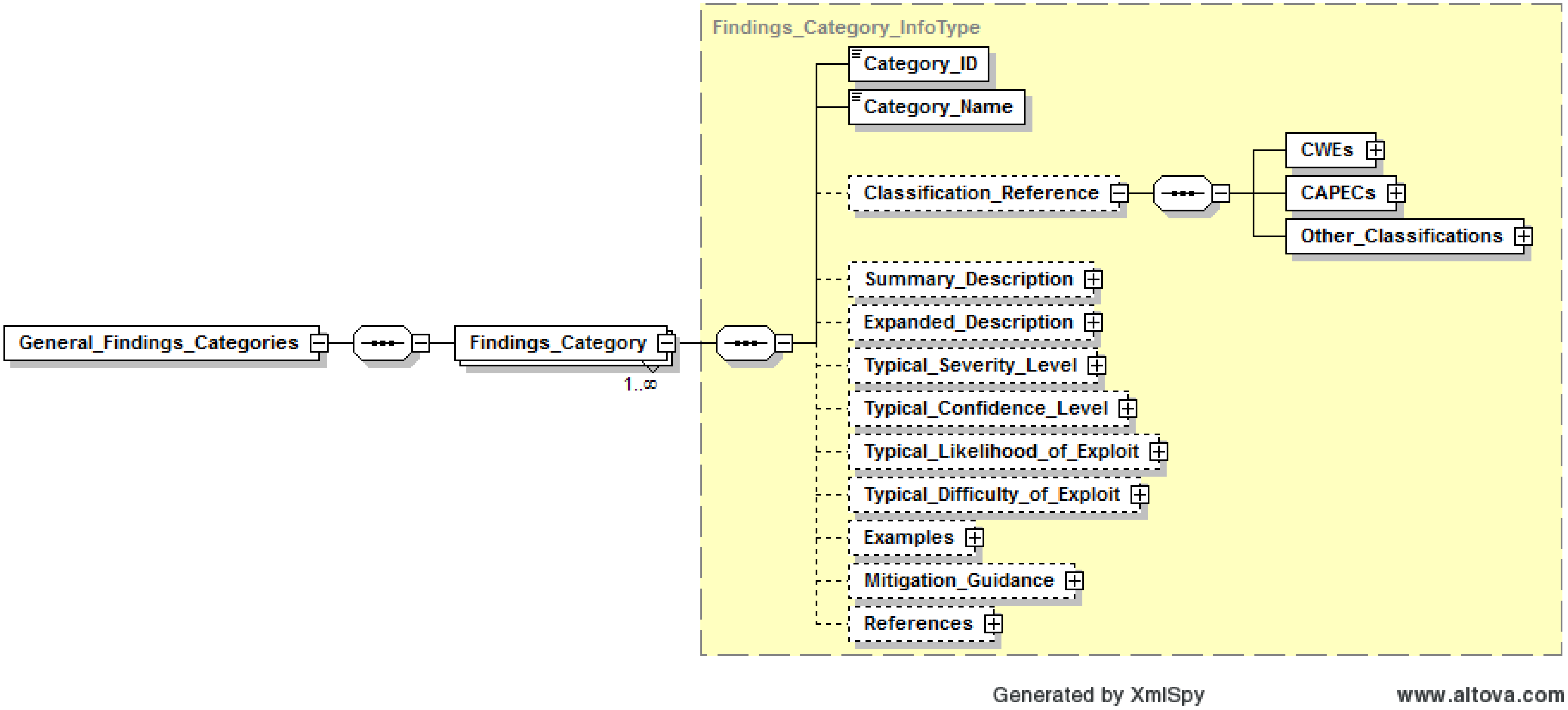
Finding Prioritization



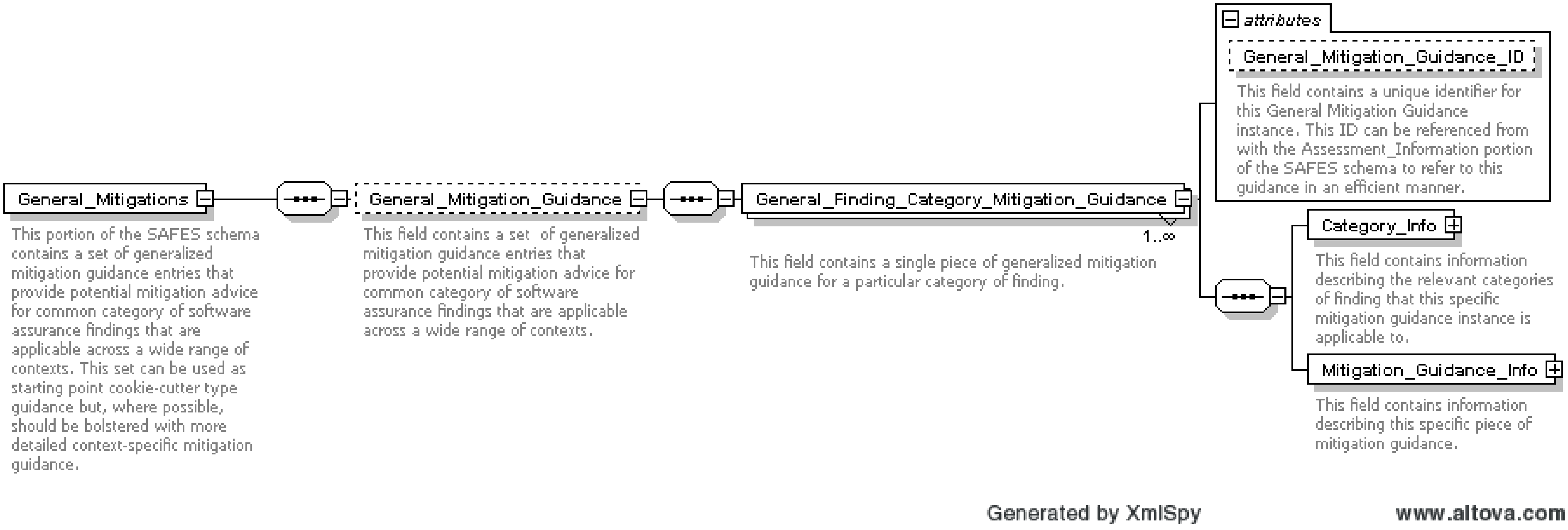
Finding Context



General Finding Categories



General Mitigations



General_Mitigations: This portion of the SAFES schema contains a set of generalized mitigation guidance entries that provide potential mitigation advice for common category of software assurance findings that are applicable across a wide range of contexts. This set can be used as starting point cookie-cutter type guidance but, where possible, should be bolstered with more detailed context-specific mitigation guidance.

General_Mitigation_Guidance: This field contains a set of generalized mitigation guidance entries that provide potential mitigation advice for common category of software assurance findings that are applicable across a wide range of contexts.

General_Finding_Category_Mitigation_Guidance: This field contains a single piece of generalized mitigation guidance for a particular category of finding.

General_Mitigation_Guidance_ID: This field contains a unique identifier for this General Mitigation Guidance instance. This ID can be referenced from with the Assessment_Information portion of the SAFES schema to refer to this guidance in an efficient manner.

Category_Info: This field contains information describing the relevant categories of finding that this specific mitigation guidance instance is applicable to.

Mitigation_Guidance_Info: This field contains information describing this specific piece of mitigation guidance.

SAFES Maturation Paths

- **Usability: primarily focused on efforts surrounding the schema to make it more usable by the community such as native transforms, tooling, etc.**
- **Refinement: primarily focused on improving the quality and coverage of the schema itself with activities such as adding new perspectives, adding new schemas, fixing errors, etc.**
- **Formalization: primarily focused on gradually (as quickly as is prudent and accepted by the targeted user community) incorporating in formal standards-based approaches (vocabulary, structure, etc.) and working towards handoff of development to an appropriate community standards consortium body**

SAFES Phase 2

- Develop 5-10 transforms from native tool output to SAFES (currently for CAS internal use but hopefully will eventually be shared)
- Develop a demonstrative use case example for SAFES
- Develop lightweight initial prototype authoring/editing/reporting tools (very, very simple)
- Develop a real, permanent website as part of MSM
- Coordinate with standards organizations for planning towards future maturation and formalization

SAFES Next Steps Beyond Phase 2

- Identify & support real-world prototype usage of SAFES
- Refine based on feedback
- Refine & extend authoring/editing/reporting tools with the goal of eventually transferring this work to other parties (vendors, open-source projects, consortia, etc.)
- Incorporate coverage for more tools, services & analysis practices
- Work with vendors (and OS projects) to develop more native transforms and encourage native output of SAFES
- Refine for efficiency
- Refine for flexibility (framework layering)
- Refine for formalization towards existing standards

Questions?

Sean Barnum
MITRE
sbarnum@mitre.org