“OMG: Not your Father’s CORBA Organization Any Longer”

The OMG System Assurance Task Force’s SwA Ecosystem

Dr. Ben Calloni, P.E. CISSP, CEH, OCRES Professional
Lockheed Martin Fellow, Software Security
Lockheed Martin Aeronautics Company, FTW
Lockheed Martin Representative to OMG
OMG Board of Directors
Co-chair OMG System Assurance Task Force

Djenana Campara,
CEO KDM Analytics
OMG Board of Directors
Co-chair OMG System Assurance Task Force


http://tubbotwins.wordpress.com
$495
NO JOB
Trust me.

Defining Assurance

- Assurance provides the members of society a basis for *believing certain assertions*
- Assurance Processes provide the *foundation for a belief system*
- 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

- Dependability defined as the superset of availability, integrity, reliability, safety, and security -

People place "trust" in a system when dependability is demonstrably acceptable!

Delivering System Assurance (SysA)

- Assurance is 3 step process
  1. Specify Assurance Case
  2. Obtain Evidence for Assurance Case
  3. Use Assurance Case to calculate and mitigate risk

- Historically, Security Assurance is Informal, Subjective & Manual

No Perfect Safety/Security
Every System will have Residual Risk

The Goal

- Key Challenges
  - Objective and cost-effective assurance process
  - **Reduce ambiguity** associated with system weakness space
  - Systematic coverage of the weakness space
  - Effective and systematic measurement of the risk

Modeling Analysis to achieve high confidence in system trustworthiness.

Addressing the Challenges

- Addressing challenges through set of integrated standards
  - Define a semi-formal methodology to address weakness space coverage
  - 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

Tools integration possible only through standards

OMG System & Software Assurance Ecosystem

Operational Mission

CONOPS
Security Policy
Environment
…

Attack Patterns

C&A
Fed by
Interoperable Models

Threat Risk Assessment

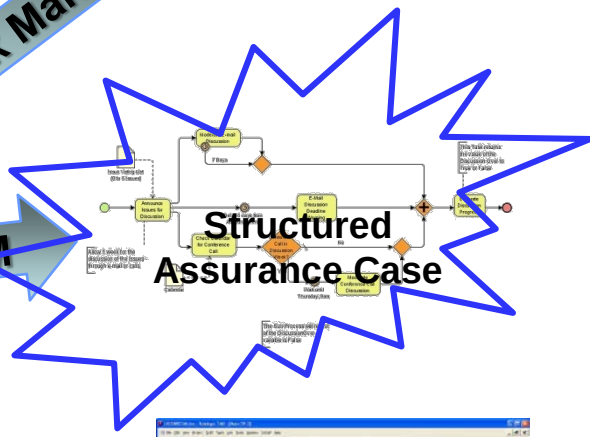
Operational Facts

NVDB

Sys Risk Manager

SACM

Common Fact Model
(Evidence)

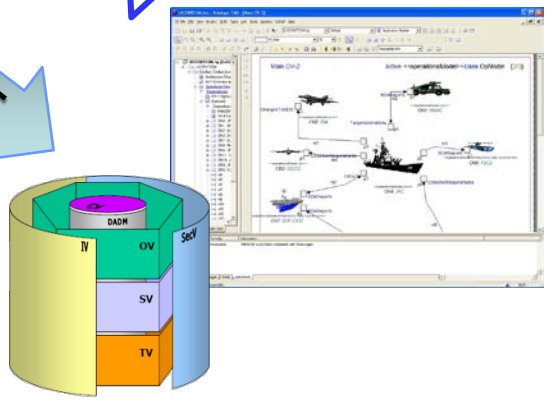


S/W Risk Analyzer

TOIF

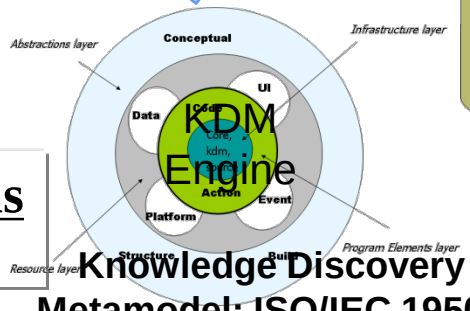
Facts

DODAF



Software

Software Fault Patterns
(Formalized CWE's)



Knowledge Discovery Metamodel: ISO/IEC 19506

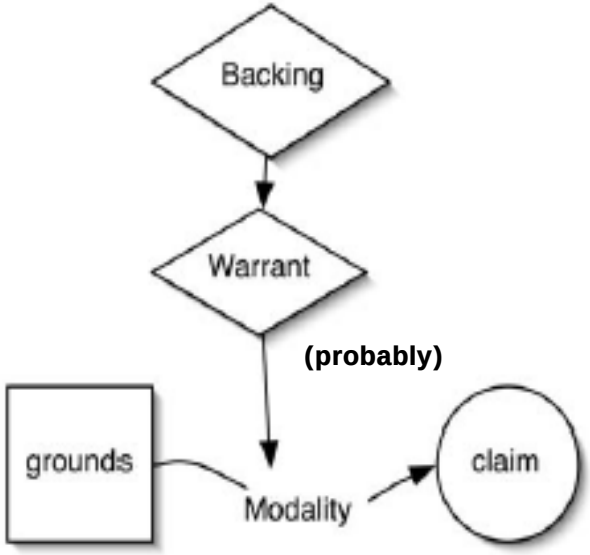
Architecture

OBJECT MANAGEMENT GROUP

Assurance Claims with Support of 'Substantial' Reasoning

Stephen Toulmin, 1958

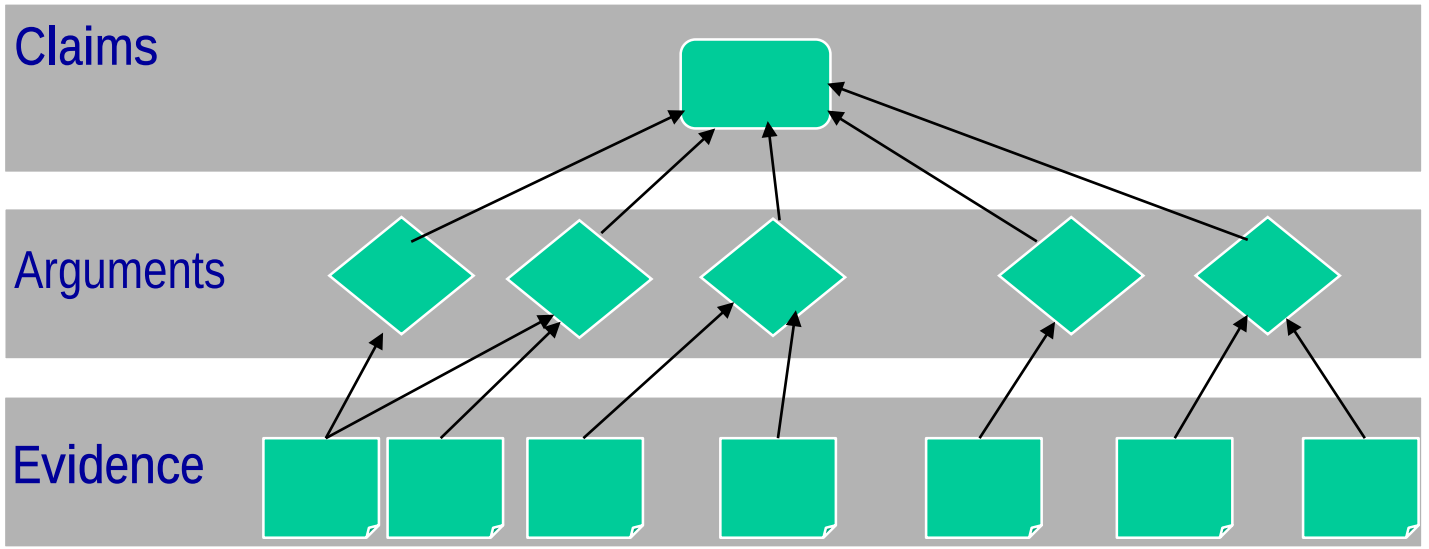
- Claims (Conclusion) are assertions put forward for general acceptance
- Grounds are the justification for claim based on specific Facts, Evidence, or Data about a precise situation that clarify and make good a claim.
- Warrant is the basis of the reasoning from the grounds to the claim is articulated.
  - Toulmin coined the term "warrant" for "substantial argument".
- Modality are statements indicating the general ways of argument being applied in a particular case and implicitly relied on and whose trustworthiness is well established.
- The basis of the warrant might be questioned, so "Backing" for the warrant may be introduced. Backing might be the validation of the scientific and engineering laws used.



http://en.wikipedia.org/wiki/Stephen_Toulmin

Assurance and Evidence (NIST SP800-160)

- Assurance is best grounded in relevant and credible evidence used to substantiate a claim
  - ***"the system is acceptably*** safe / ***secure"***
- An *assurance case* relate claims and evidence
  - ***Via structured argumentation and argument patterns***
  - ***Automated via assurance case tools***

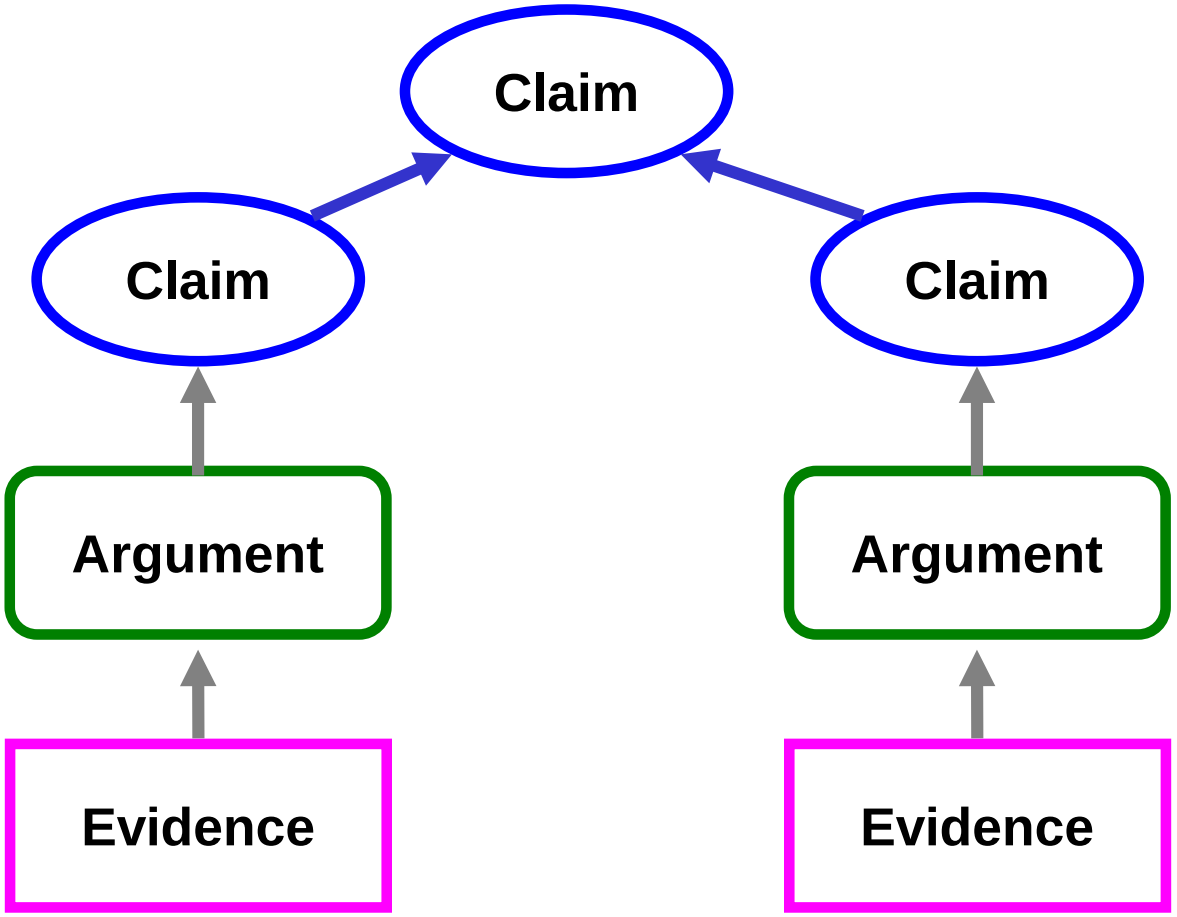


Claims, Arguments, and Evidence

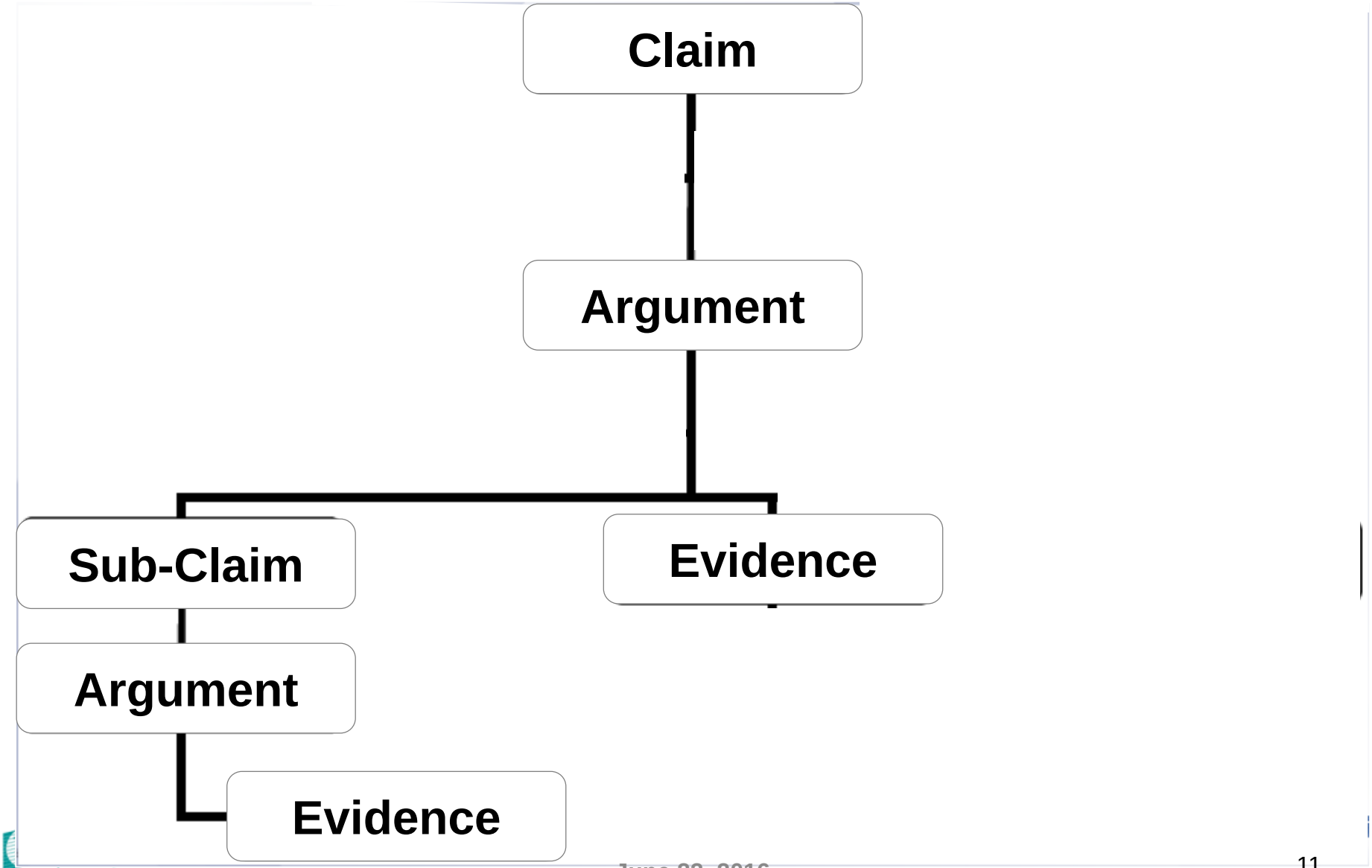
Claim = assertion to be proven

Argument = how evidence supports claim

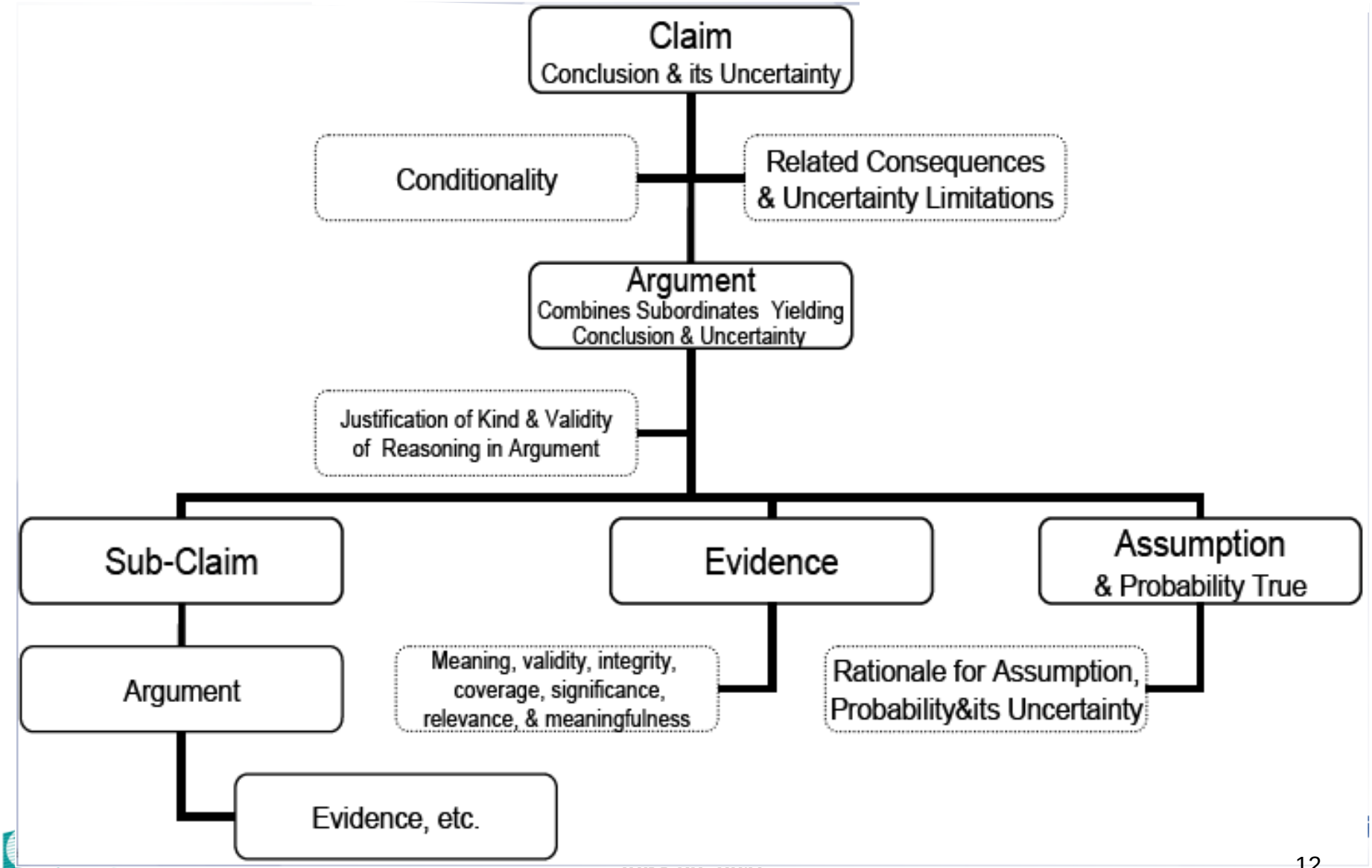
Evidence = required documentation



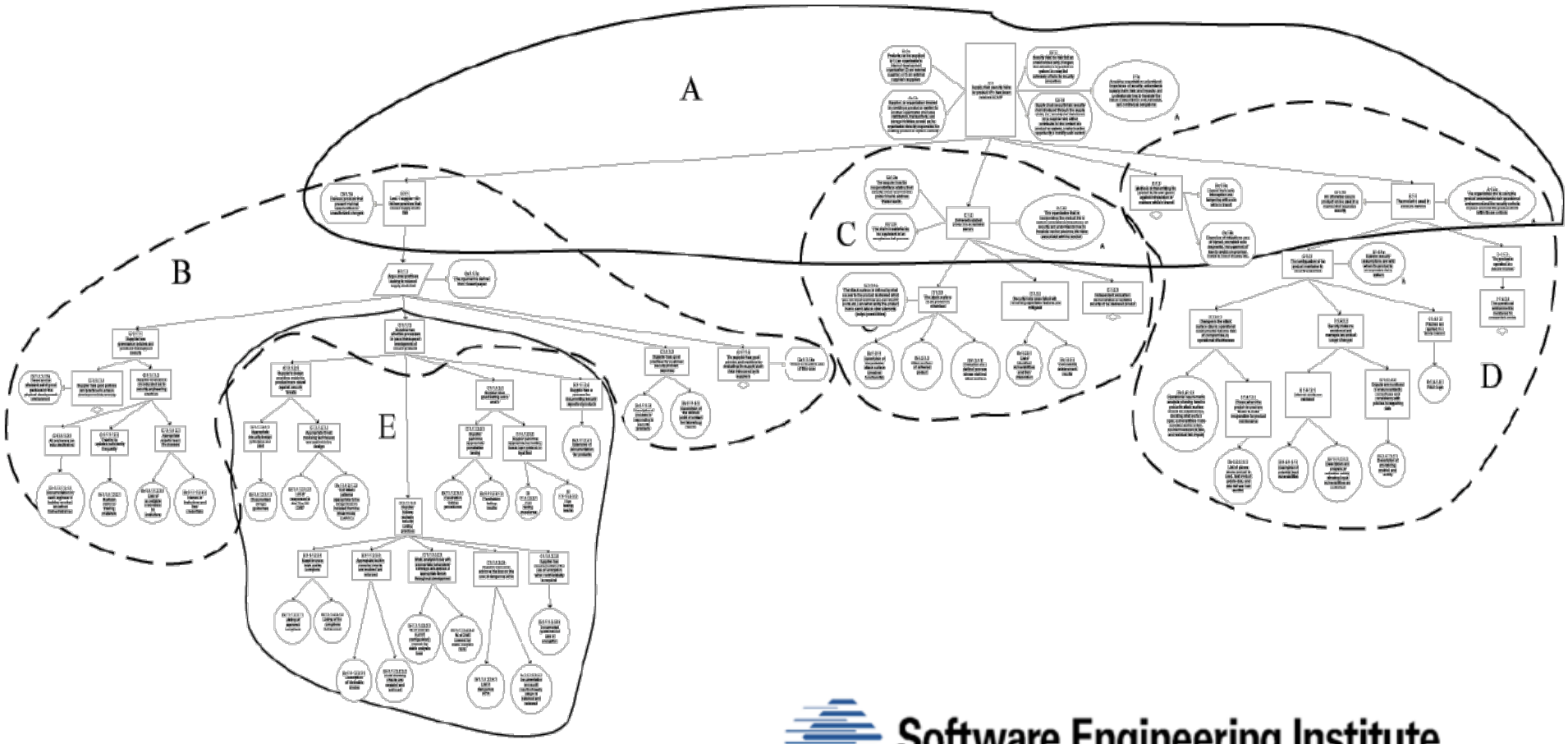
ISO/IEC 15026: Systems & Software Assurance
15026 Part 2: The Assurance Case (Claims-Evidence-Argument)



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



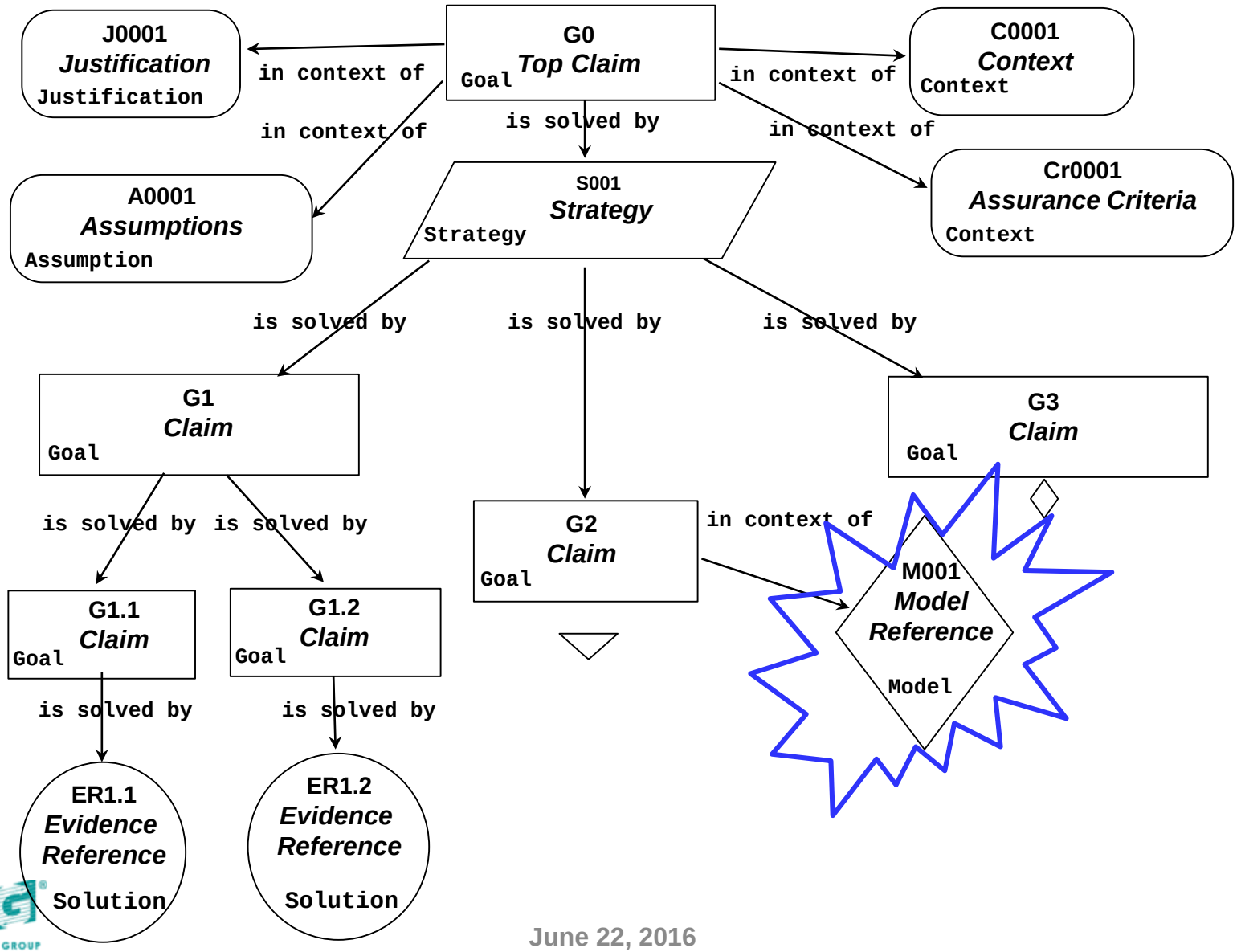
Assurance Cases Can Be Large & Composed of Other Assurance Cases



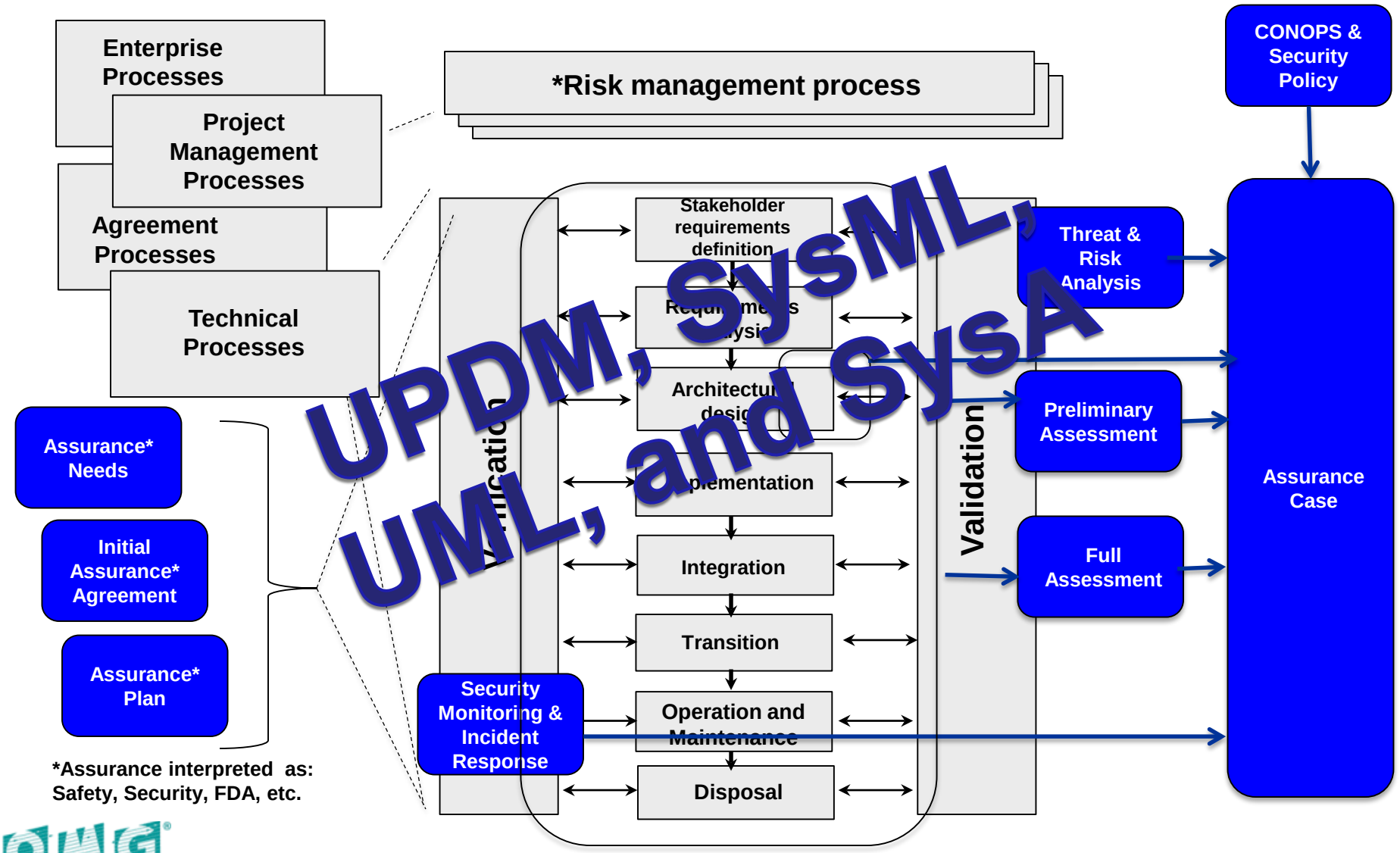
Software Engineering Institute

A: Overview of Assurance Case
B: Supplier Practices Reduce Supply Chain Risk
C: Developed/Updated Product is Acceptably Secure
D: Delivered/Updated Product is Acceptably Secure & The Product is Used in a Secure Manner
E: Supplier Has Effective Processes in Place to Support Secure Development

OMG's Structured Assurance Case Metamodel

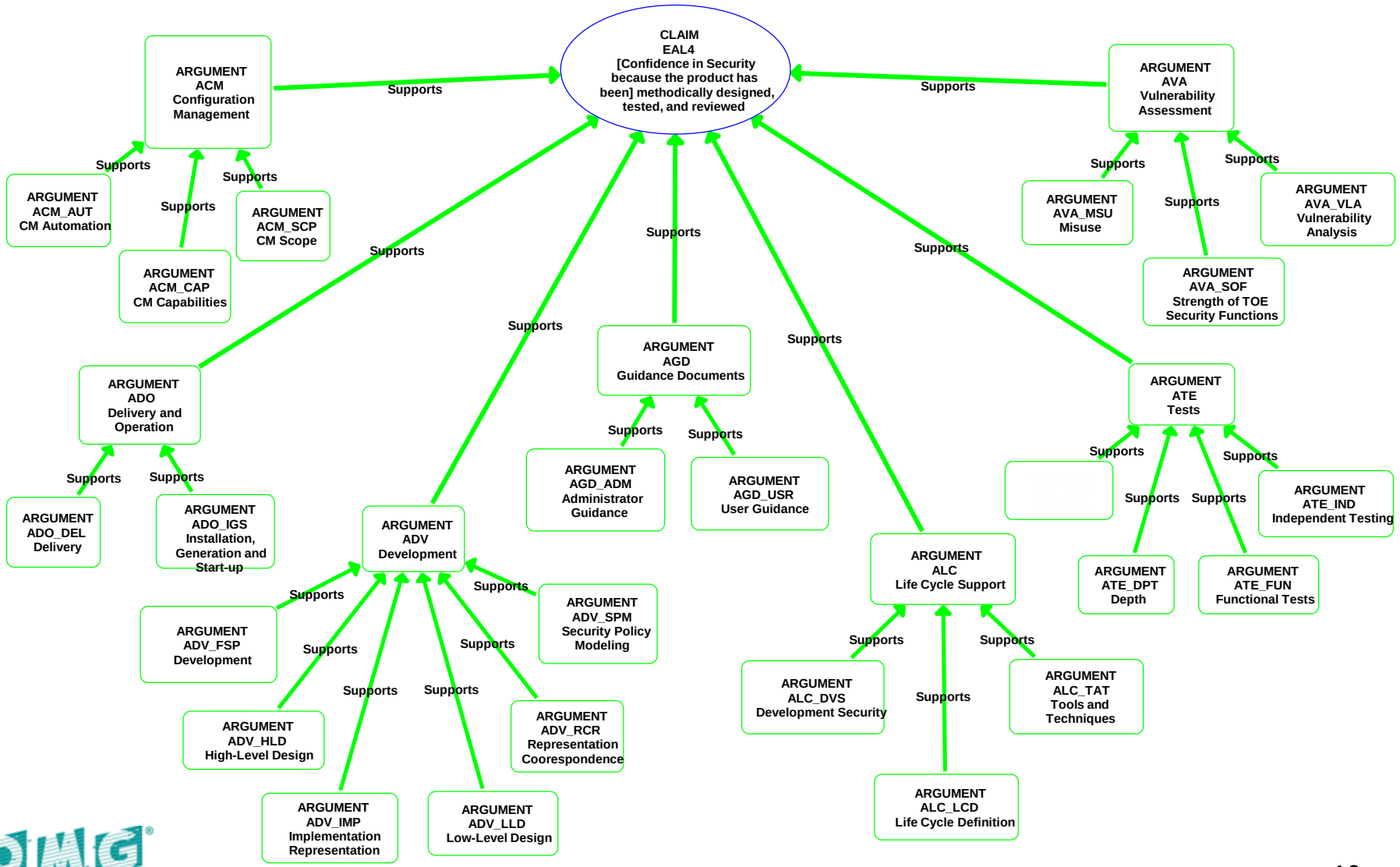


Assurance as Part of Systems and Software Engineering - System Lifecycle (ISO 15288:2008)

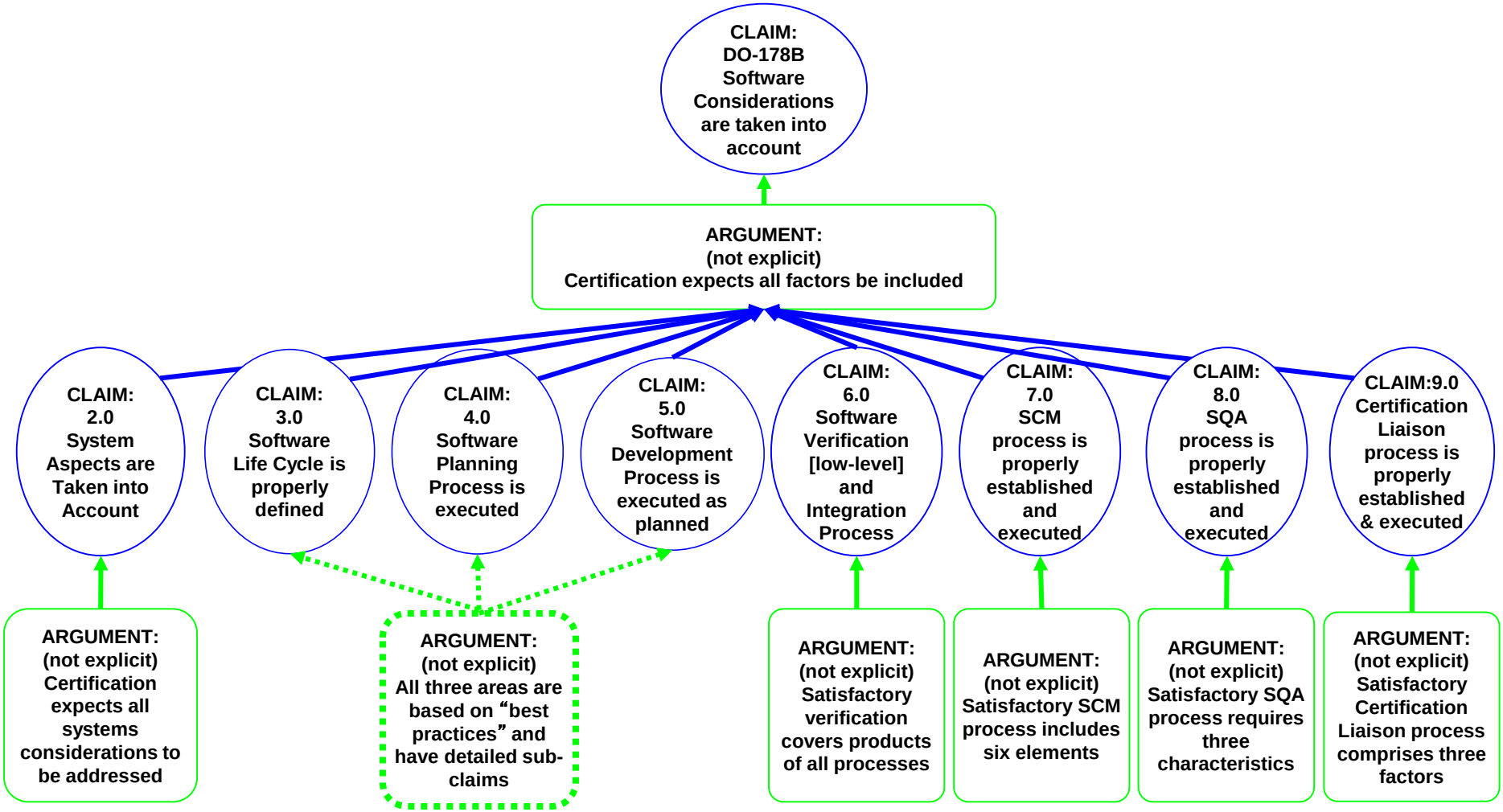


*risk to cost / schedule

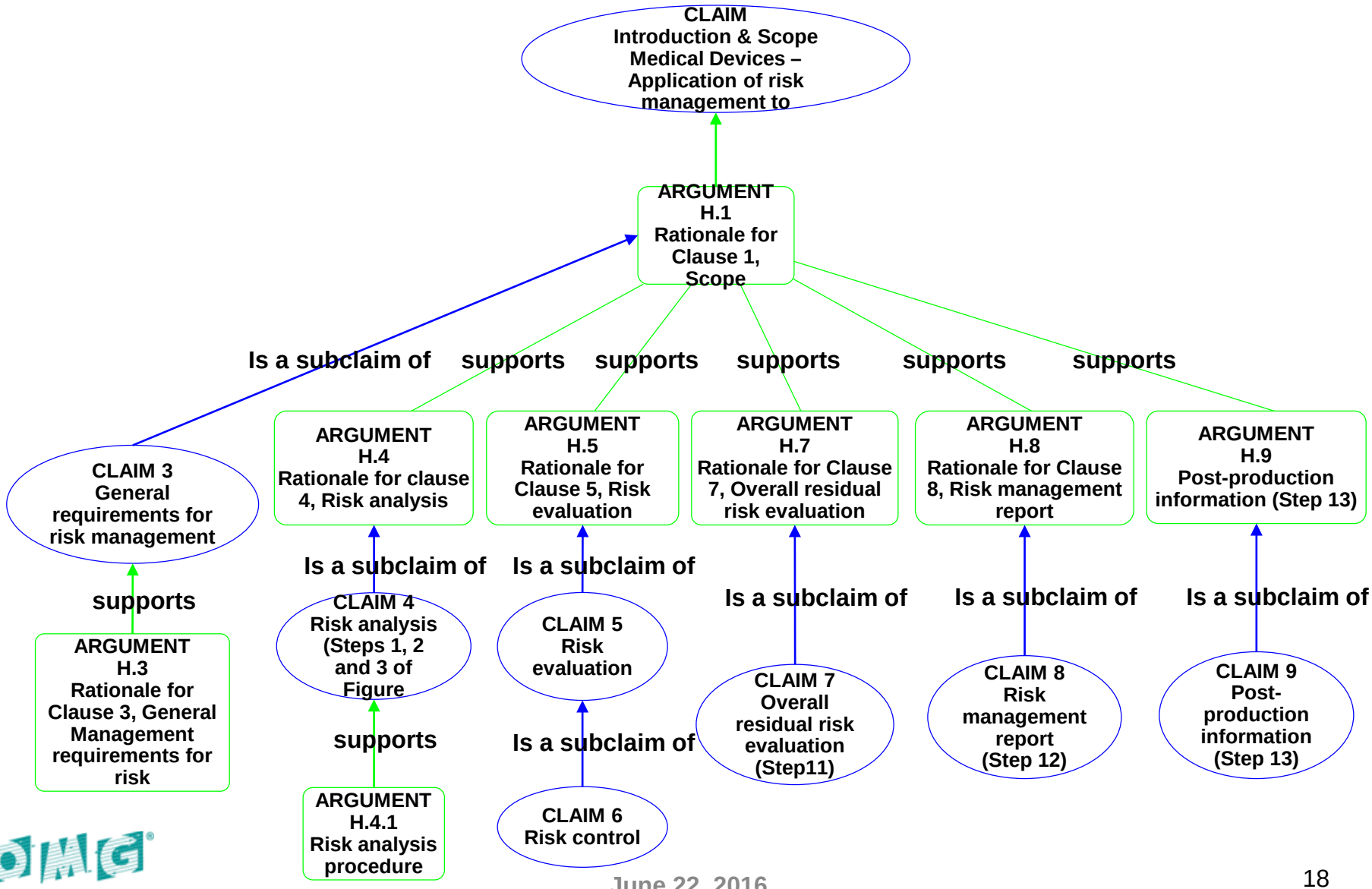
The Common Criteria – Top Level



RTCA/DO-178B – Top Level



ISO 14971 Medical Devices – Top Level



OMG System & Software Assurance Ecosystem

Operational Mission

CONOPS
Security Policy
Environment
…

Attack Patterns

A&A
Fed by
Interoperable Models

Threat Risk Assessment

Operational Facts

NVDB

Sys Risk Manager

SACM

Common Fact Model
(Evidence)

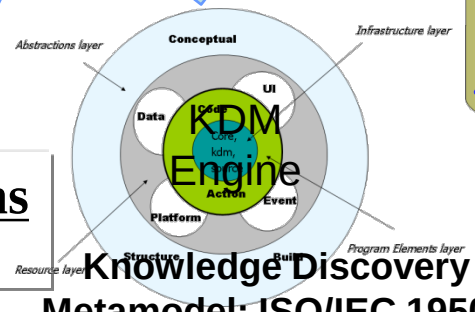
Structured Assurance Case

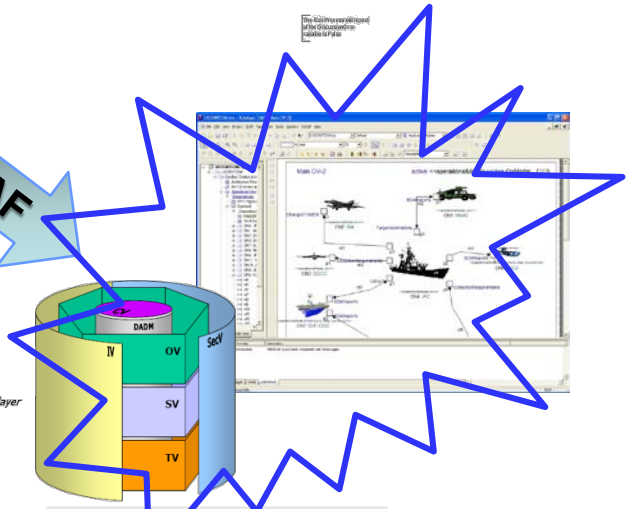
DODAF

S/W Risk Analyzer

TOIF

Facts





Software

Software Fault Patterns
(Formalized CWE's)

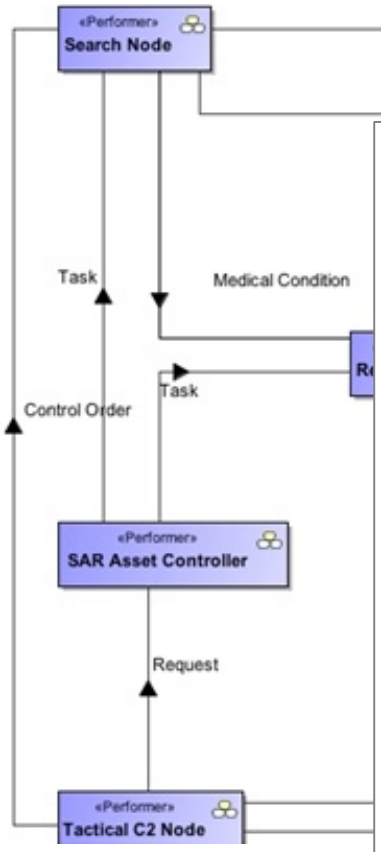
Architecture

Knowledge Discovery Metamodel: ISO/IEC 19506

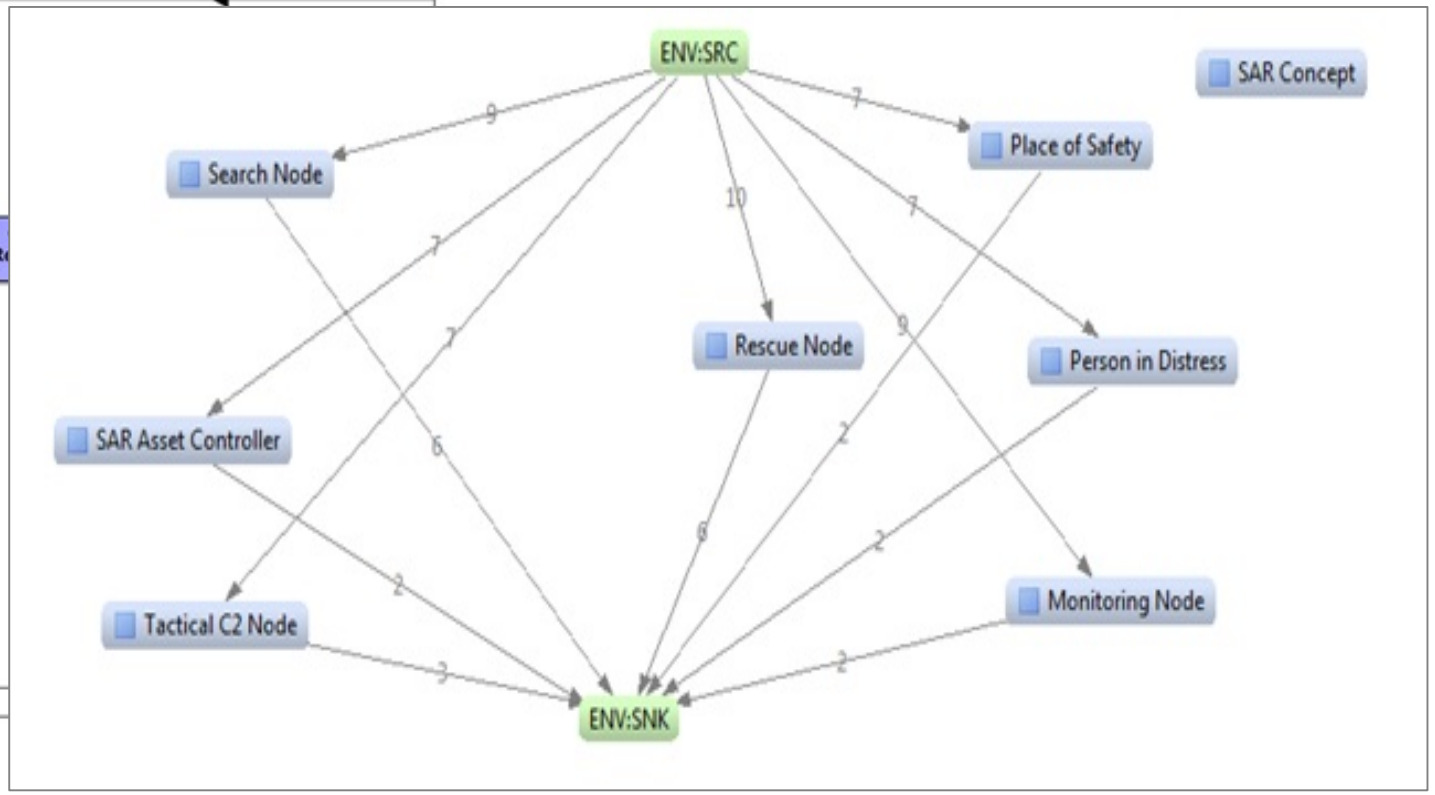
OBJECT MANAGEMENT GROUP

Is the Model Complete?

OV-2 View in DoDAF Model

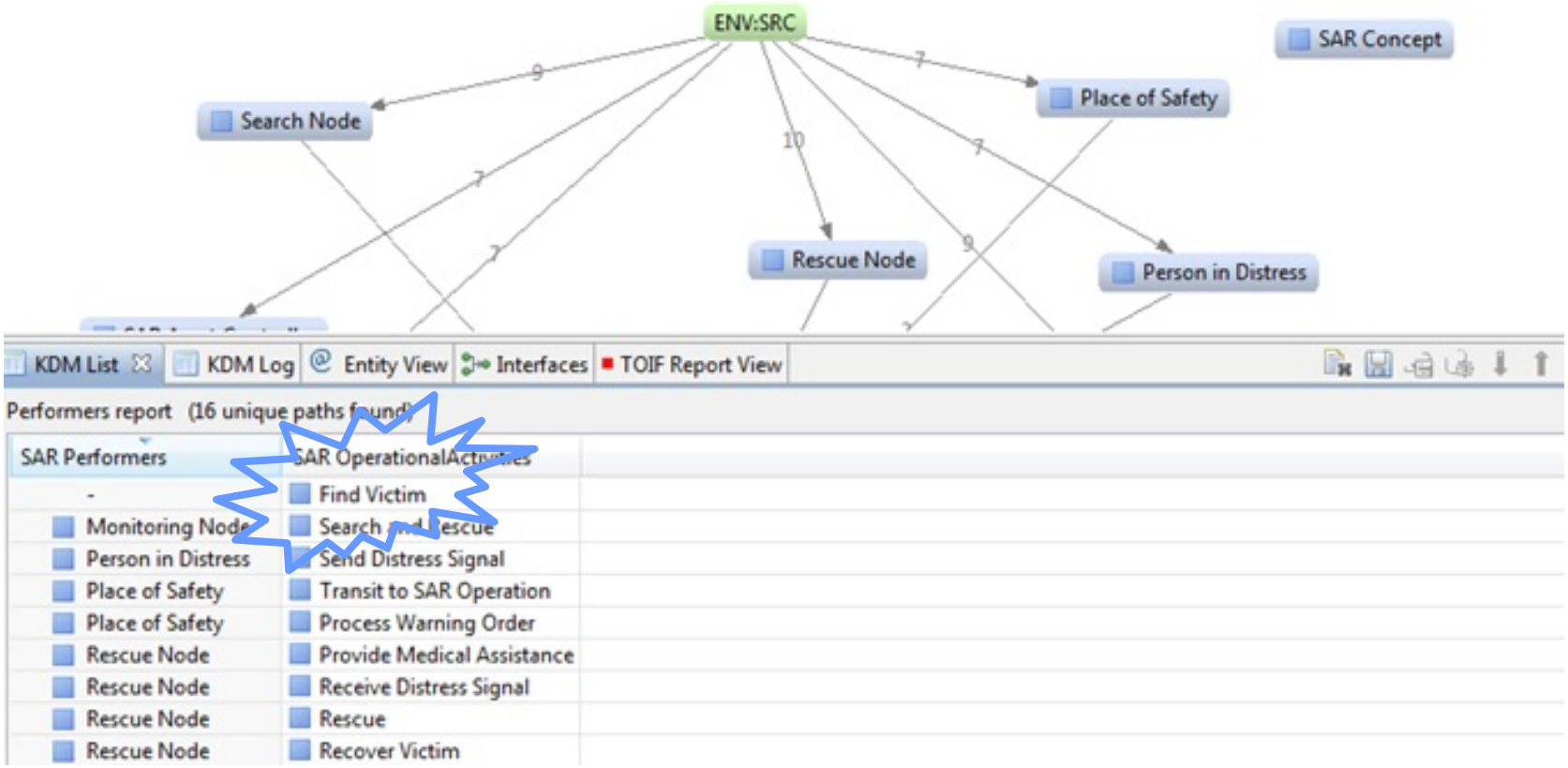


North Sea Search and Rescue DoDAF Model



Actual Performers Found by Risk Manager

Analysis of Operational Activities



Full Analysis of DoDAF Model

SAR Performers	SAR ExchangeElements	SAR Performers
-	Aircraft Instruction	-
-	Message	-
-	Life Preserver Instruction	-
-	Request for Assistance	-
-	Boat Instruction	-
-	Name	-
-	Medical Advice	-
-	Weather Forecast	-
-	Beacon Instruction	-
-	Reported Location	-
-	-	Person in Distress
-	-	SAR Concept
Monitoring Node	Track Info	Tactical C2 Node
Person in Distress	Distress Signal	Search Node
Person in Distress	Distress Signal	Monitoring Node
Person in Distress	Distress Signal	Rescue Node
Place of Safety	-	-
Rescue Node	Medical Condition1	Monitoring Node
Rescue Node	Updated Location	Monitoring Node
SAR Asset Controller	Task1	Search Node
SAR Asset Controller	Task	Rescue Node
SAR Concept	-	-
Search Node	Warning Order	Place of Safety
Search Node	Medical Condition	Rescue Node
Tactical C2 Node	Control Order1	Search Node
Tactical C2 Node	Control Order	Rescue Node
Tactical C2 Node	Request	SAR Asset Controller

OMG System & Software Assurance Ecosystem

Operational Mission

CONOPS
Security Policy
Environment
…

Attack Patterns

A&A
Fed by
Interoperable Models

Threat Risk Assessment

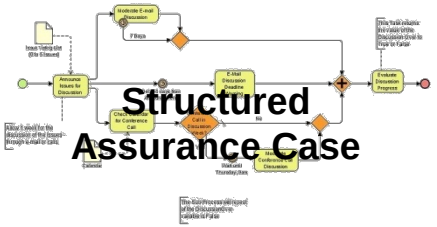
Operational Facts

NVDB

Sys Risk Manager

SACM

Common Fact Model
(Evidence)

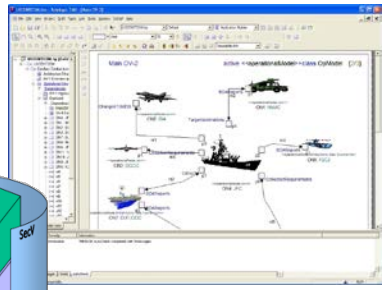


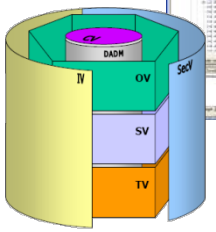
S/W Risk Analyzer

TOIF

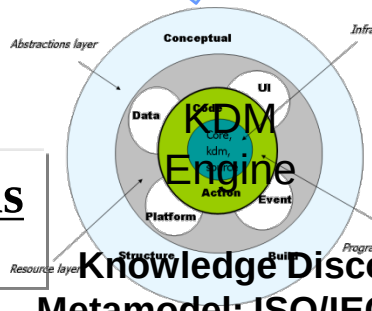
Facts

DODAF





Software Fault Patterns
(Formalized CWE's)

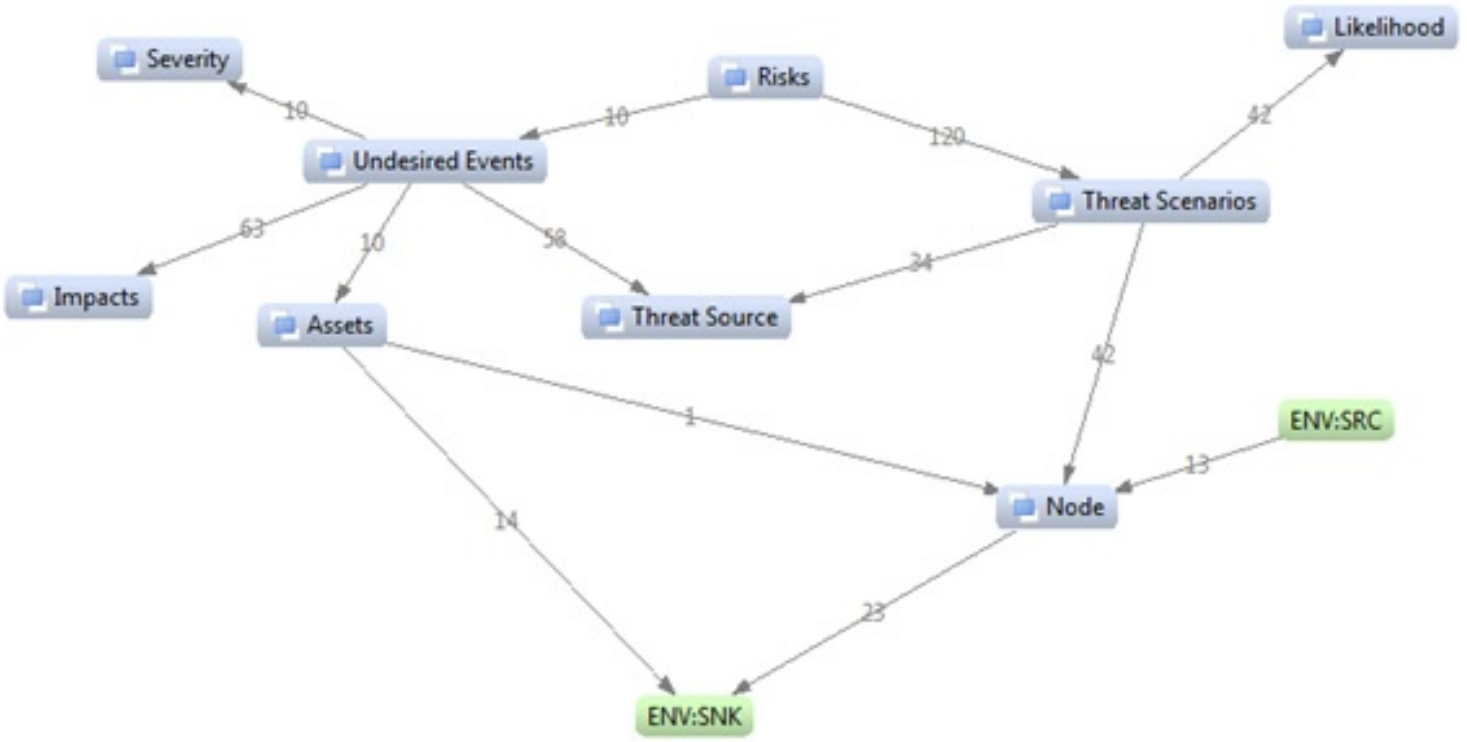


Architecture

Knowledge Discovery Metamodel: ISO/IEC 19506

OBJECT MANAGEMENT GROUP

Threat Modeling



http://www.omg.org/hot-topics/threat-modeling.htm

OMG System & Software Assurance Ecosystem

Operational Mission

CONOPS
Security Policy
Environment
…

Attack Patterns

A&A
Fed by
Interoperable Models

Threat Risk Assessment

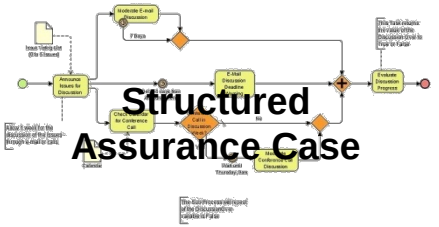
Operational Facts

NVDB

Sys Risk Manager

SACM

Common Fact Model
(Evidence)

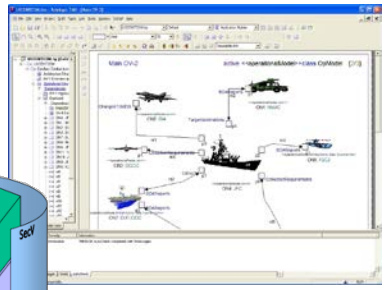


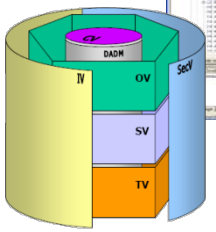
S/W Risk Analyzer

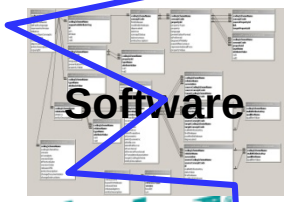
TOIF

Facts

DODAF

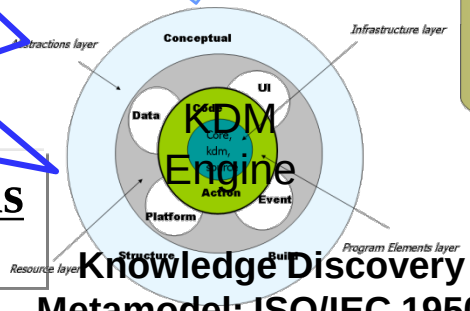






Software

Software Fault Patterns
(Formalized CWE's)

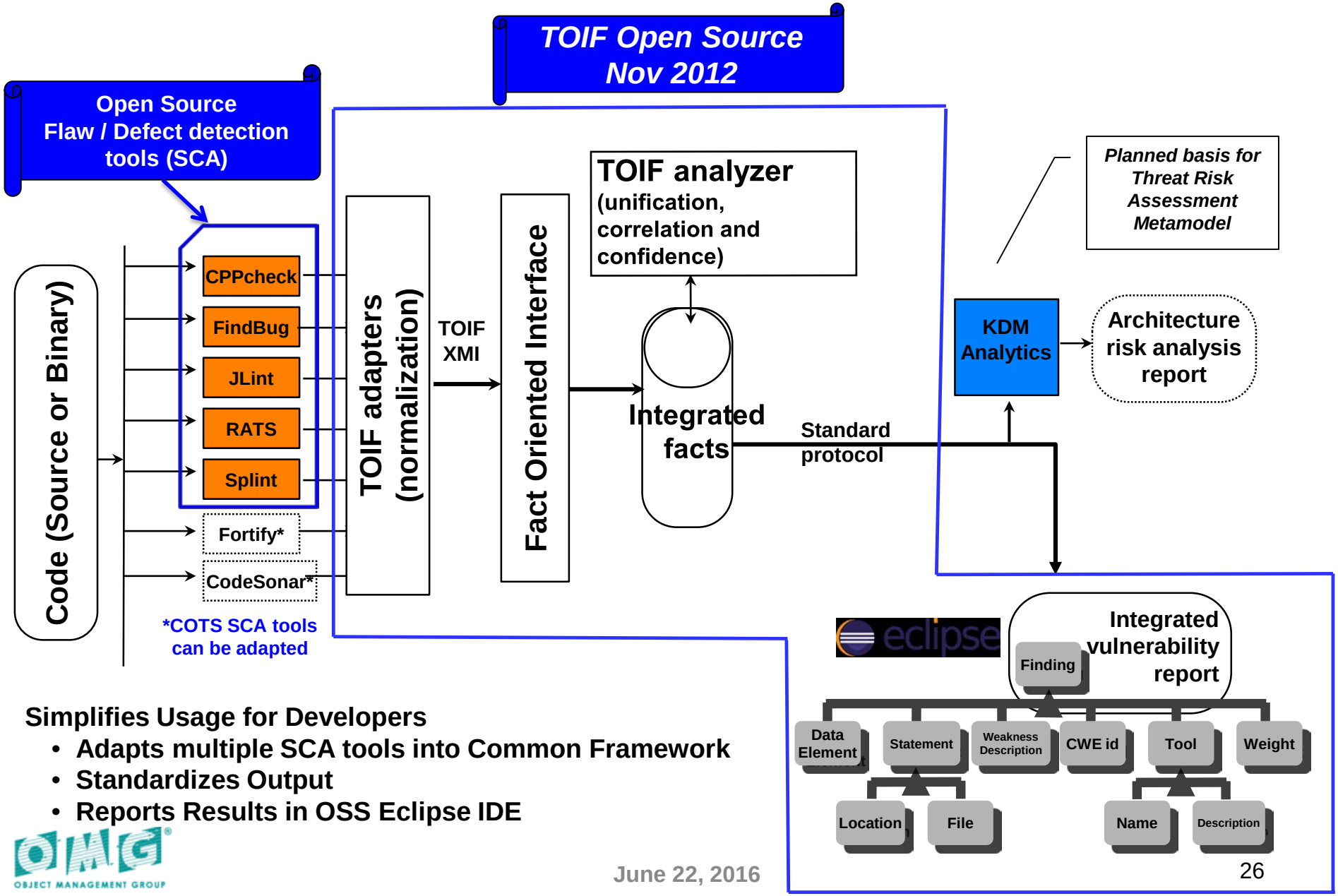


Knowledge Discovery Metamodel: ISO/IEC 19506

Architecture

OBJECT MANAGEMENT GROUP

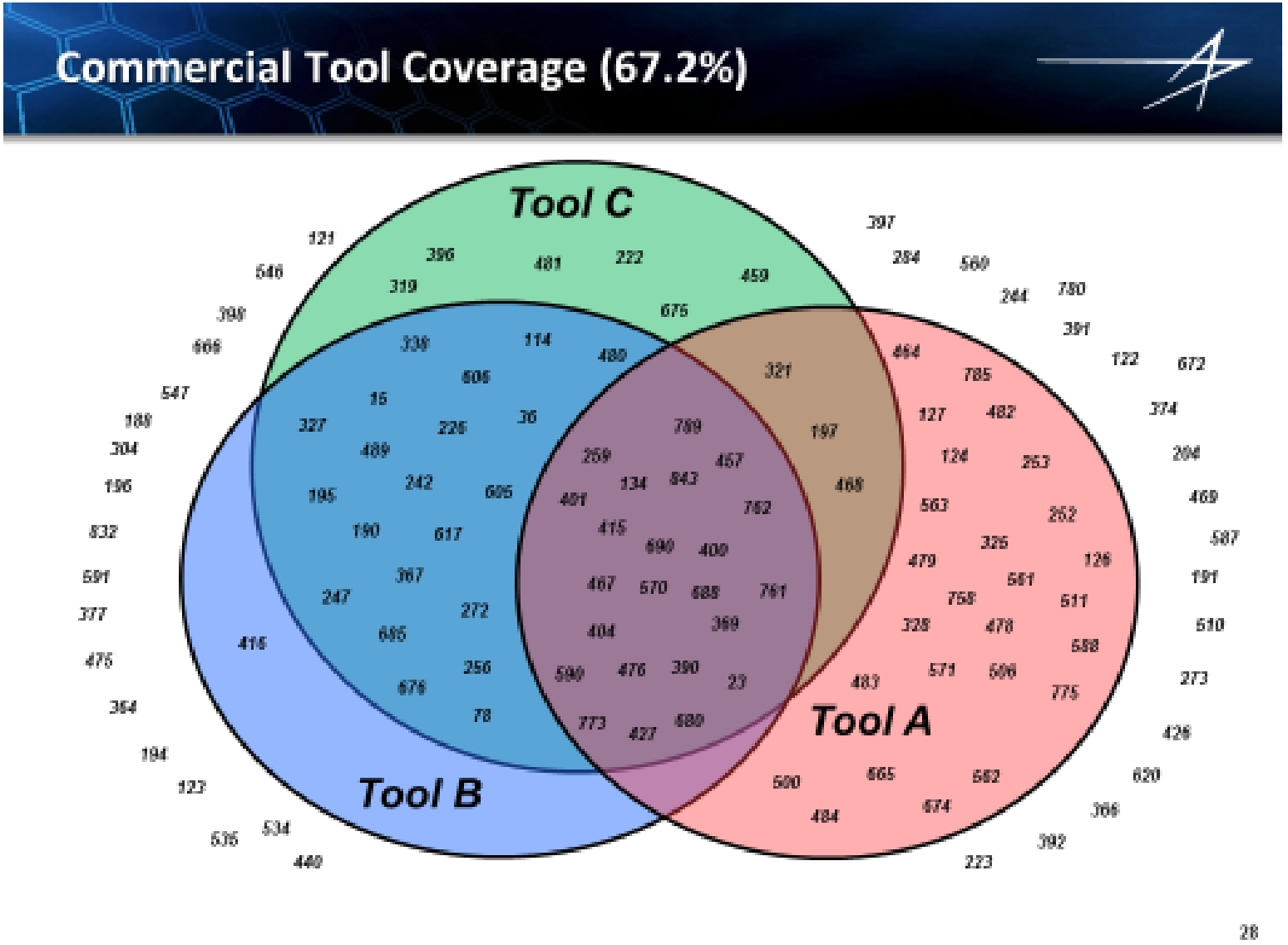
TOIF Architecture



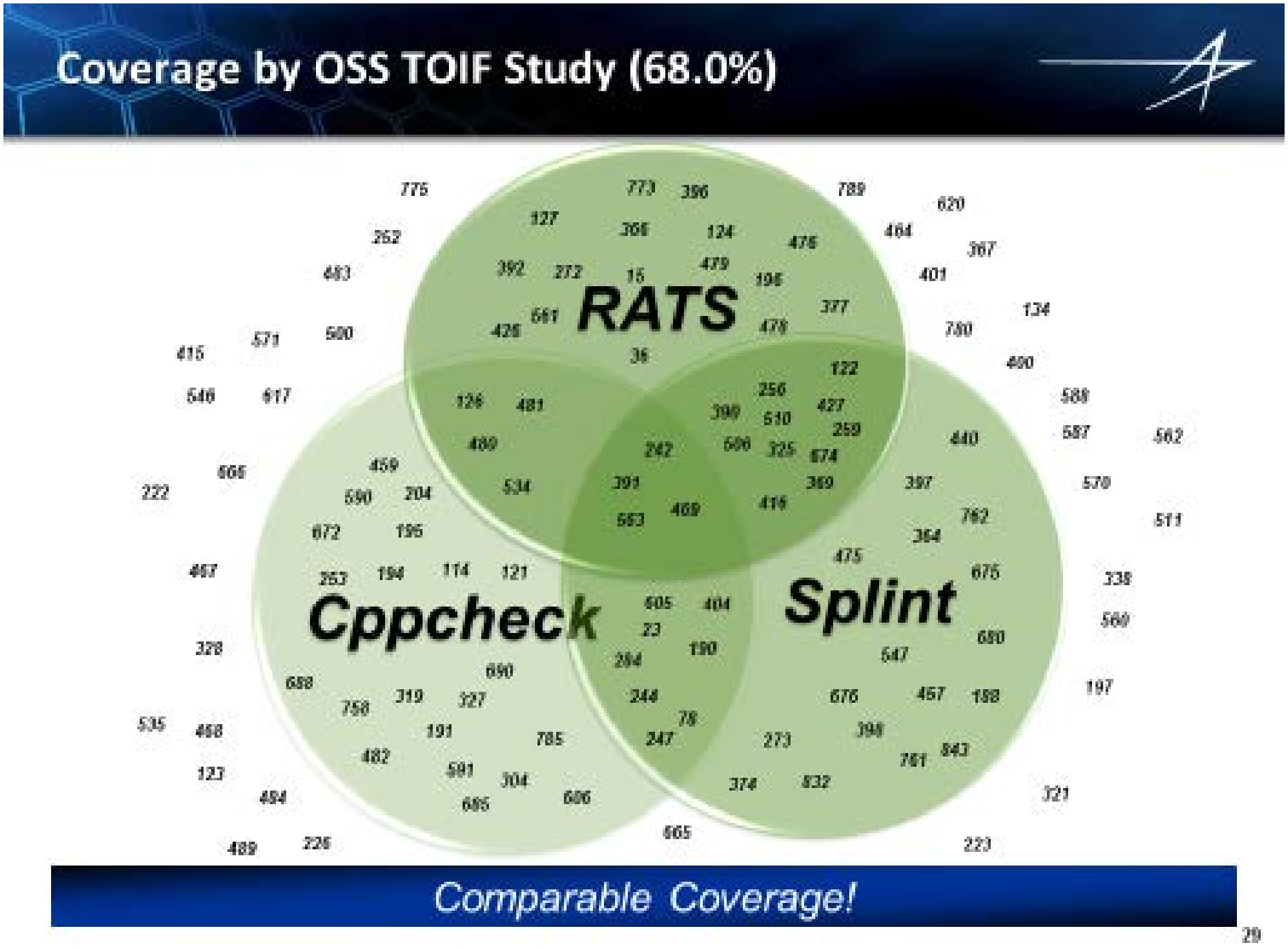
Simplifies Usage for Developers

- **Adapts multiple SCA tools into Common Framework**
- **Standardizes Output**
- **Reports Results in OSS Eclipse IDE**

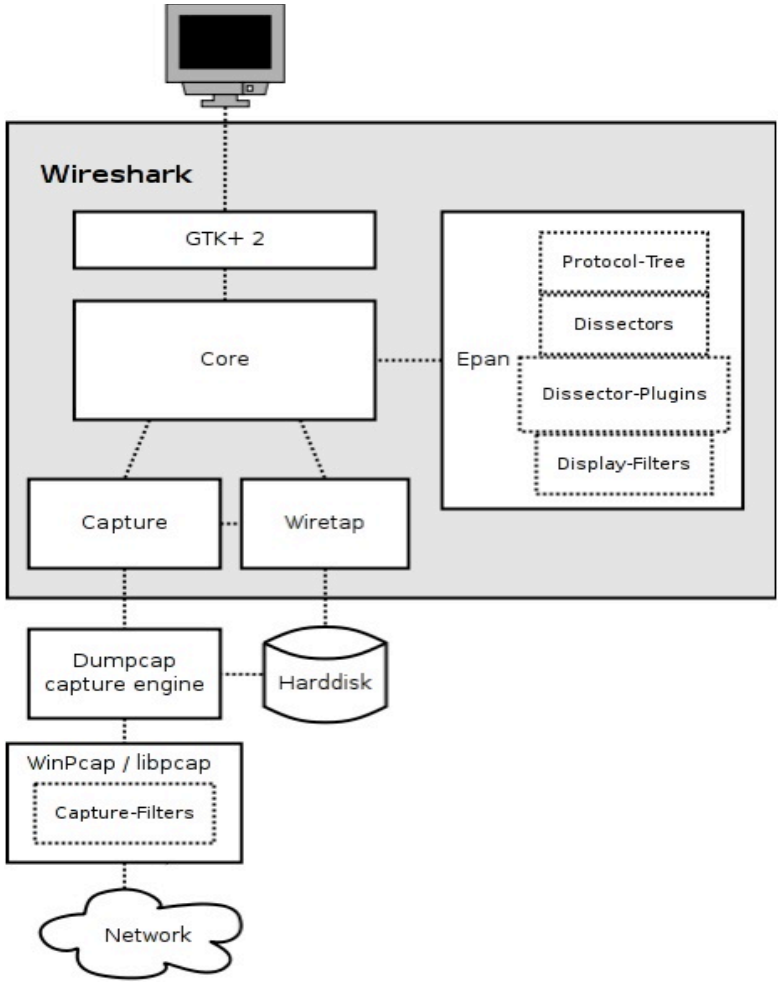
Reported at IEEE Metrocon 2014

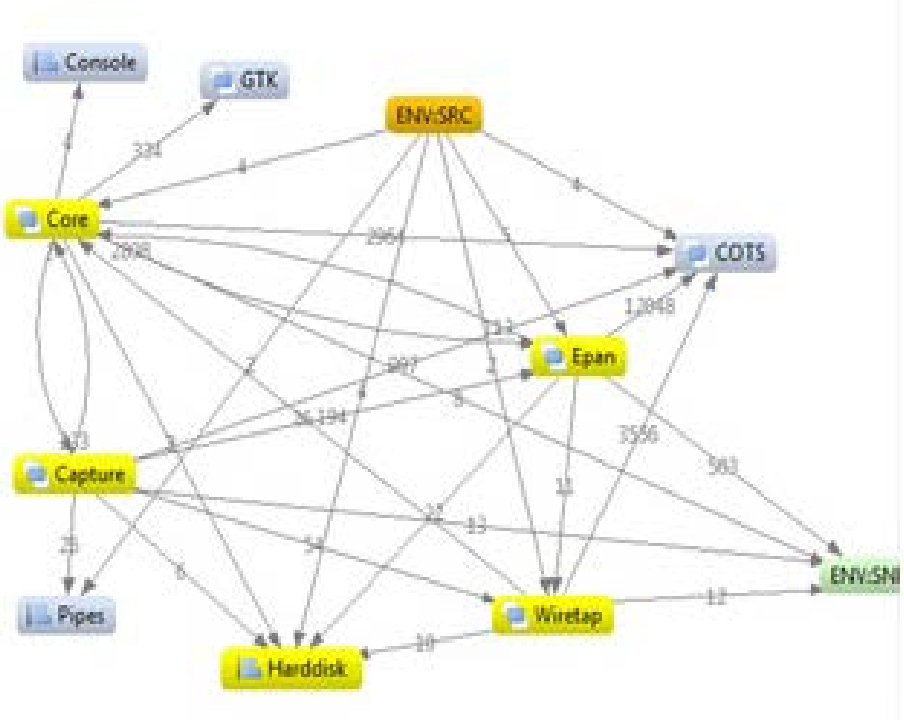


Reported at IEEE Metrocon 2014



Software Risk Analyzer



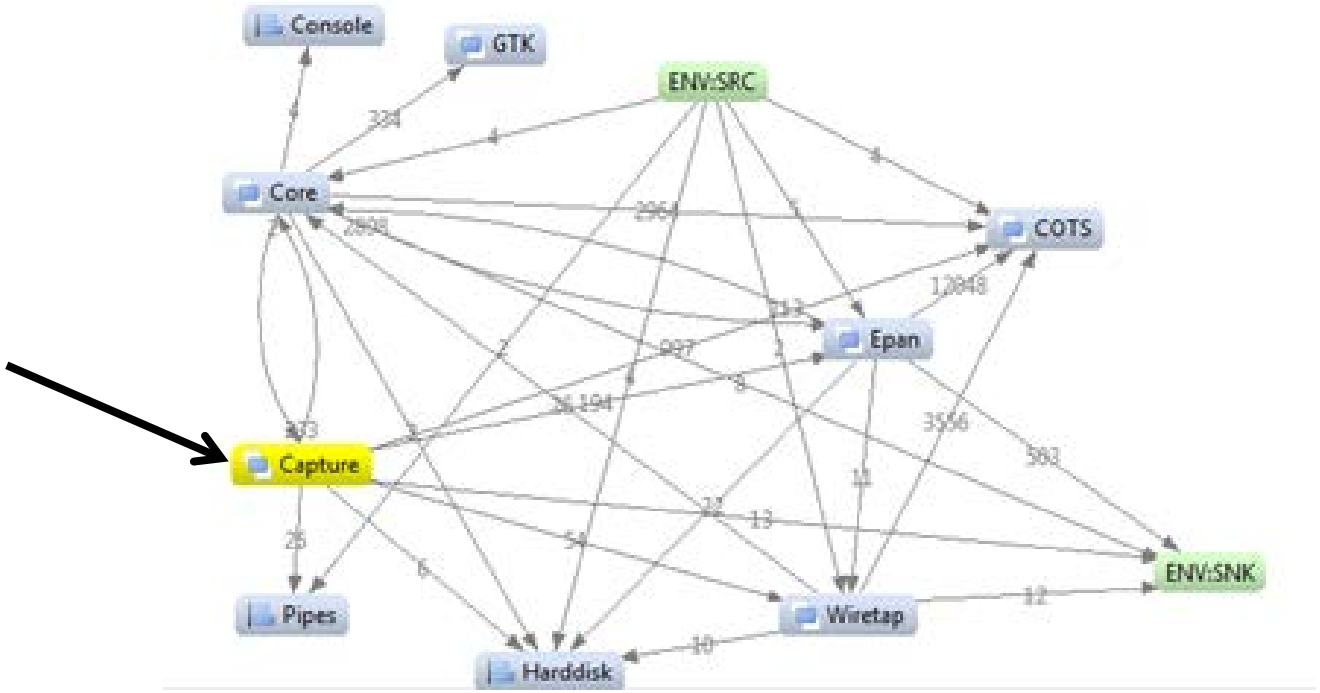


Compare the Design Information to Implemented Code

Threat Risk Analysis of Attack Paths

The architectural component where the buffer overflow is happening.

Threat Risk Analysis discovers attacker has direct access to “Capture Module”



Software Flaw Findings from TOIF

File	Location	Tool	SFP	CWE	Trust	Description
diam_dict.c	1806	Defect Counter Adaptor	SFP-14	CWE-401	0	memLeak: possible memory leak. Dynamic memory st
diam_dict.c	1855	Defect Counter Adaptor	SFP-14	CWE-401	0	memLeak: possible memory leak. Dynamic memory st
print.c	1199	Rough Audit Tool for Security Ad	SFP-8	CWE-121	0	staticlocalbuffer: Extra care should be taken to ensure t
print.c	1173	Rough Audit Tool for Security Ad	SFP-8	CWE-121	0	/home/adam/Desktop/wiresharkproject2/src/print.c
print.c	1188	Rough Audit Tool for Security Ad	SFP-8	CWE-121	0	staticlocalbuffer: Extra care should be taken to ensure t
file_wrappers.c	127	Rough Audit Tool for Security Ad	SFP-8	CWE-119	0	bufloop: Check buffer boundaries if calling this functic
file_wrappers.c	127	Splint Adaptor	SFP-1	CWE-704	0	type: Assignment of ssize_t to int: ret = read(state-fd

OMG System & Software Assurance Ecosystem

Operational Mission

CONOPS
Security Policy
Environment
…

Attack Patterns

A&A
Fed by
Interoperable Models

Threat Risk Assessment

Implementation

System Artifacts
- Req.
- Use Cases
- Design
- Data Flow Diagrams
- STIGs
- …

Operational Facts

NVDB

Sys Risk Manager

SACM

TBD

S/W Risk Analyzer

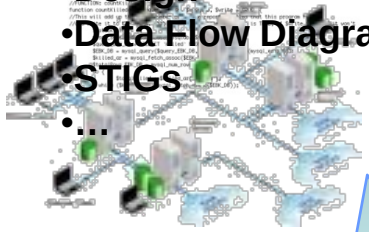
TOIF

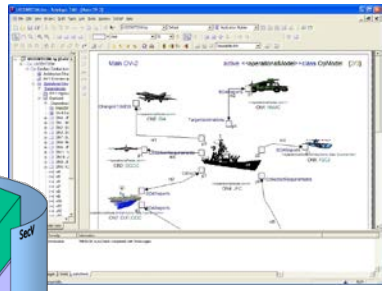
Facts

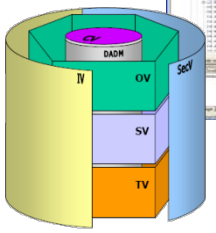
DODAF

Common Fact Model
(Evidence)

Structured Assurance Case

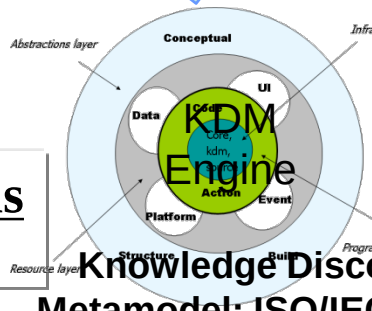






Software

Software Fault Patterns
(Formalized CWE's)



Knowledge Discovery Metamodel: ISO/IEC 19506

Architecture

OBJECT MANAGEMENT GROUP

Weakness Detection Tool vs. SwA Tool Suite: Different Requirements

SwA Key Report Requirements / Weakness Detection Tools	Detected Weakness (W) Set	Path Coverage Breadth per W	Path Coverage Depth per W	Path Coverage Completeness per W	Layered Services	Source code Trace
Sw Assurance Ecosystem	Open, (Rule-based)	Full, transparent	Full, configurable, transparent	Full, transparent	Y	Y
Source Code Static Analysis	Extensible, usually closed	Can be opportunistic, not transparent	Limited to app layer, can be opportunistic, not transparent	Limited to app layer, no coverage data available	N	Y
Binary Static Analysis	With limitations	Can be opportunistic, not transparent	Can be opportunistic, not transparent	Can be opportunistic, not transparent	Y	Y
Penetration Testing	Only vulnerability	Limited by complexity	Limited by complexity	Unknown	Y	N

Conclusion

- Structured Assurance Models
  - Bring structured order to chaos
  - Interrelated Claims – Arguments – Evidence between various sources of evidence
- System Risk Manager
  - Analysis of DoDAF model Operation, System, … Views
  - Automated Gap Assessments in Models
  - Threat Risk Assessment capability on DoDAF models
- TOIF and Risk Analyzer tools have demonstrated
  - Significant improvement in Software Flaw and Vulnerability assessments
  - Lower labor costs
  - Significantly lower tool costs

OMG System Assurance Modeling Tools can Reduce Security Engineering Life-cycle costs 20-50%.