Cyber Risk and Related Standards

Djenana Campara
CEO, KDM Analytics

- KDM Analytics' Representative to OMG
  - OMG Board of Directors
  - Co-chair OMG System Assurance Task Force

OBJECT MANAGEMENT GROUP

Acknowledgments

- Dr. Ben Calloni, Lockheed Martin
  - Co-chair System Assurance Task Force
  - OMG BoD
- Robert Martin, MITRE
  - Chair, Structured Assurance Case Metamodel RTF
- Dr. Nikolai Mansourov, KDM Analytics
  - Chair, Knowledge Discovery Metamodel (KDM) RTF

Cyber Security

Trust in System's ability to Execute Trusted Behavior Only and to Prevent Malicious Attacks

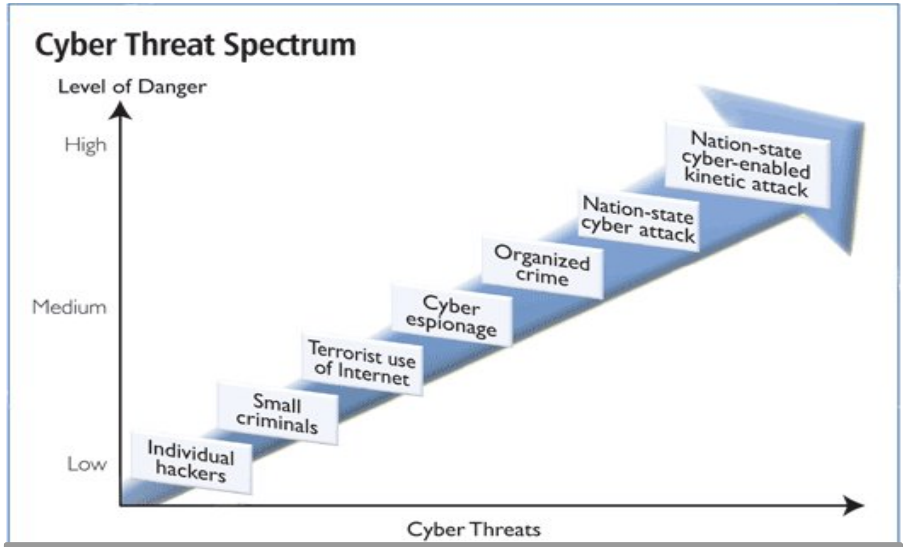
with objective to

Protect Information, Assets & Services Against Compromise

Achieving Cyber Security by …

NOT

Here is why-NOT



Source:
Meeting the Cybersecurity Challenge: Empowering Stakeholders and Ensuring Coordination", Prieto & Bucci, IBM, October 2009

- Accelerating frequency and severity of cyber threats & attacks
  - impact of attack increases along all point of the threat spectrum however severe damage can be done at all points along the spectrum
- Ever-increasing complexity of cyber systems
  - Lack of comprehension of such a systems
  - Luck of understanding intricate attack options, assessing vulnerabilities
- Relaxed security in legacy systems
  - Complex, multiple technologies with multiple suppliers systems resist retrofitting security

Motivation of today's cyber attack includes:

- **Espionage & Competitive Intelligence**
- **Data corruption & Operation Interruption**
- **Disgruntled employees**

It Starts by Understanding Threat

- Not enough to trust credentials
- Firewall is no longer sufficient protection
- Ignorance MUST NOT be an option
  - Organized Crime
  - Smart and knowledge sharing Hackers

Effective threat mitigation can only be achieved through identifying, analyzing, classifying and understanding the threat and related risk

Threat Characterization

Cheap and Easy

- Uses technology readily available on the internet

Ubiquitous and agile

- Comes from Anywhere and it can strike Anytime

Increased Sophistication

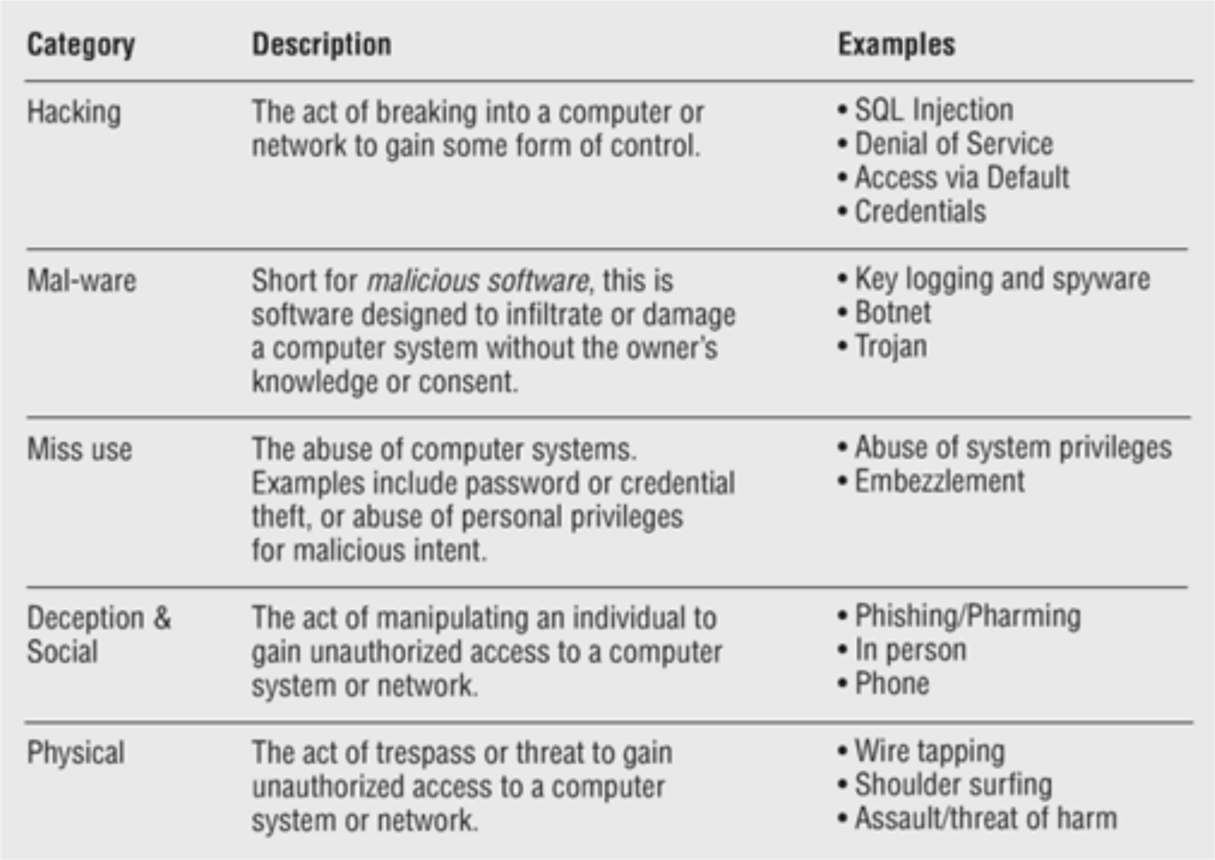
- Organized and knowledge sharing, more difficult to track attacks (use of complex routing, proxies and dummy hosts)

Proliferation

- As use of computers and network broadens, everyone is a node in a network and open to cyber attacks

Unless the threat is addressed, the network-centric concept of operations is at Risk.

Threat Categorization



Category	Description	Examples
Hacking	The act of breaking into a computer or network to gain some form of control.	• SQL Injection • Denial of Service • Access via Default • Credentials
Mal-ware	Short for *malicious software*, this is software designed to infiltrate or damage a computer system without the owner's knowledge or consent.	• Key logging and spyware • Botnet • Trojan
Miss use	The abuse of computer systems. Examples include password or credential theft, or abuse of personal privileges for malicious intent.	• Abuse of system privileges • Embezzlement
Deception & Social	The act of manipulating an individual to gain unauthorized access to a computer system or network.	• Phishing/Pharming • In person • Phone
Physical	The act of trespass or threat to gain unauthorized access to a computer system or network.	• Wire tapping • Shoulder surfing • Assault/threat of harm

- **Any or all these threat types can bring vast array of techniques and technologies to bear**

Source: IBM Global Business Services, " Cyber Defense: Understanding and Combating the threat", Feb. 2010

Threats and Impacts

CONFIDENTIALITY
INTEGRITY
AVAILABILITY

- Eavesdropping
- Exploitation

- Spoofing
- Non-Repudiation

- Jamming
- Denial of Service

Preventing Even Bigger Impact

- Target for current and future cyber attacks could take multiple forms and impacts
- Ranging from National Security, Economy to Social, such as loss of human lives

Technology to mount such an attack already EXISTS

Cybersecurity: Constantly Evolving Challenge

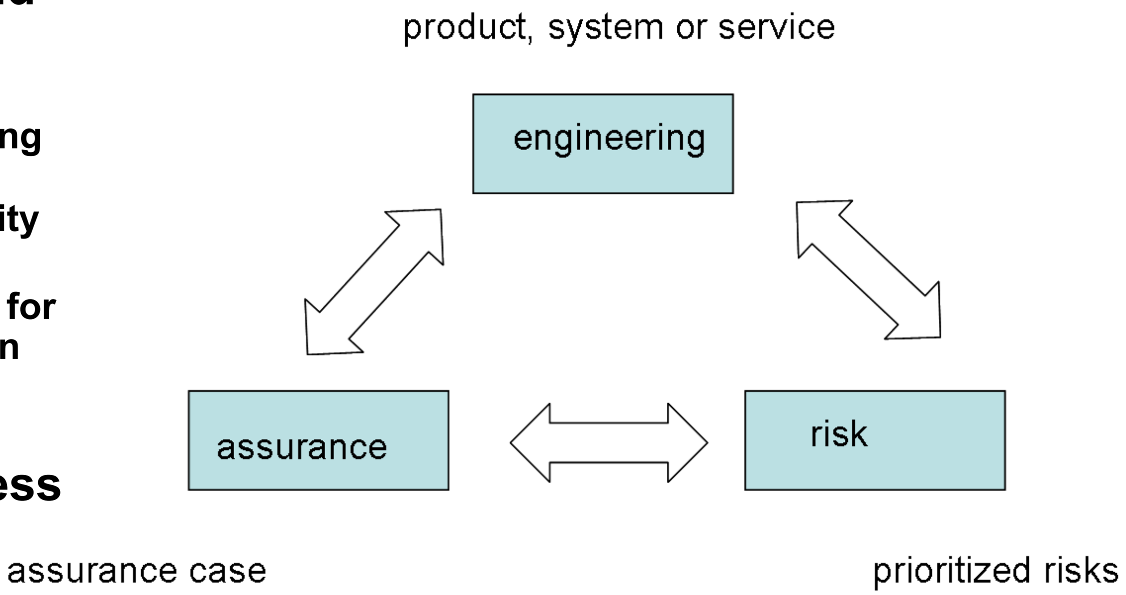
- The Government concern:
  - cyber threat environment is evolving more rapidly than the government's ability to keep pace

- Effective mitigation can only be achieved through a combination of technical and nontechnical counter measures
  - Comprehensive Threat-Risk Assessment solution to facilitate Cybersecurity decisions
    - Cyber Infrastructure matching systems combined enormity and complexity must be accompanied by comprehensive Risk Assessment solutions
  - Constant training of employees
  - Adequate security polices

There is no one tool nor one vendor that can address all aspects of evolving challenges – we need collective defenders effort throughout SLC

Interrelationships of Assurance, Engineering and Risk

- **Engineering, Assurance and Risk are intimately related**
  - **To assure a system means to ensure that System Engineering principles were correctly followed in meeting the security goals.**
  - **Additional guidance provided for System Assurance is based on the identifying threats and prioritizing risks**
- **Today, the risk mgmt 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.**



Integrated Engineering, Assurance and Risk Facts to Assess System's Trustworthiness

Summary of Technical Challenges

- Key Challenges
  - Systematic coverage of the system 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 implemented artifacts
  - Effective and systematic measurement of the 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
  - Specifications for a suite of integrated tools providing end-to-end solution

Overcoming these challenges will enable automation: a requirement for cost-effective and objective risk assessment process

Addressing Challenges

Top down operational analysis

Bottom up vulnerability analysis

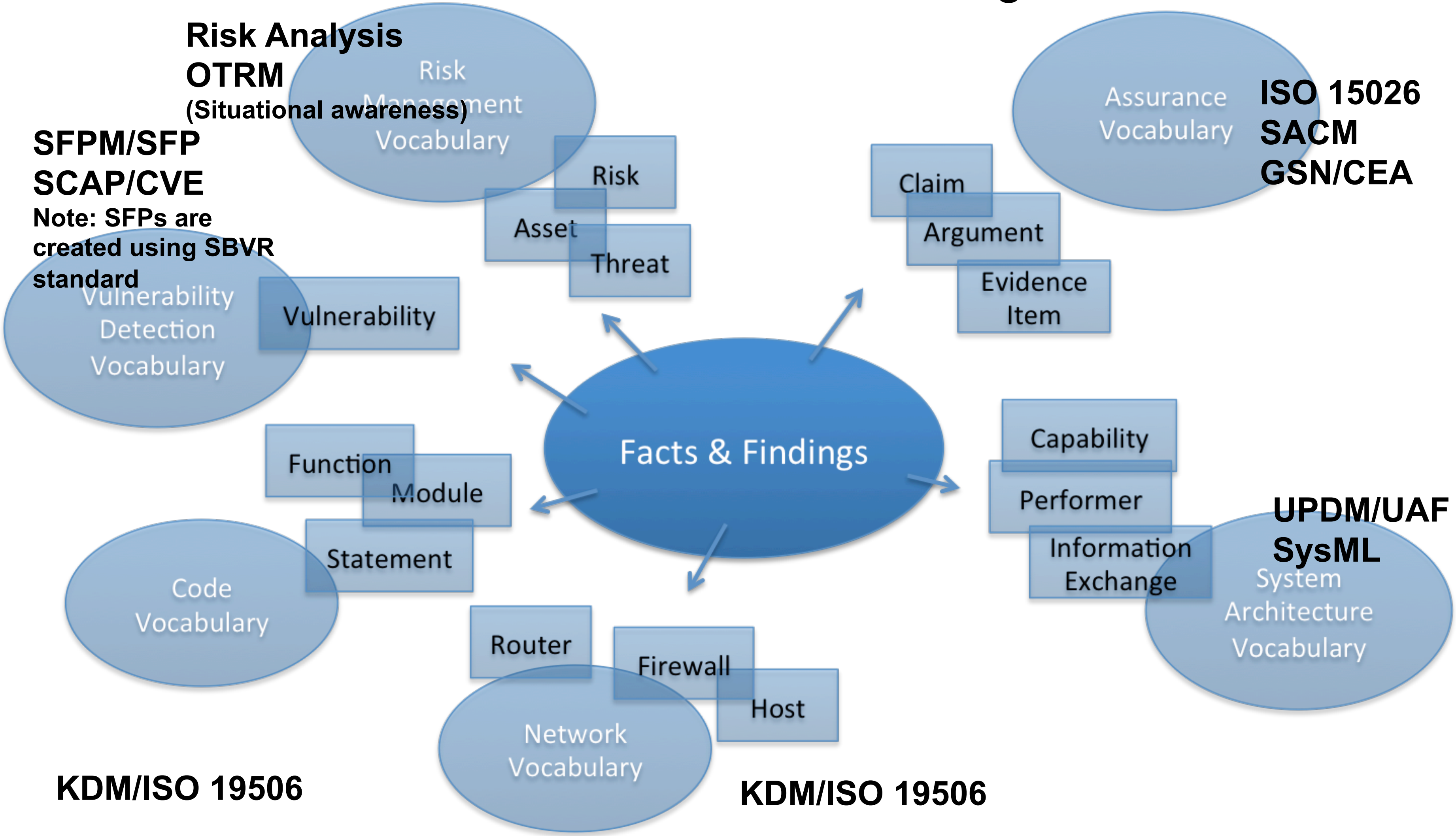
System Life Cycle	Engineering	Risk	Assurance
Operational	Operational Views (UPDM/UAF or SysML)	Risk Analysis (RA), NIST 800-37 OTRM	ISO/IEC 15026; SACM, GSN/CAE (Claim & Argument)
Architecture	UPDM/UAF SysML SFPM & SFPs X.1520 (SCAP-CVE) X.1524 (CWE)	Risk Analysis, X.1521 (SCAP-CVSS) X.1525 (CWSS)	ISO/IEC 15026; SACM, GSN/CAE; Open Group Dependability Assurance (O-DA) (Evidence Measure)
Implementation	KDM SFPM & SFPs X.1520 (SCAP-CVE) X.1524 (CWE)	Risk Analysis, X.1521 (SCAP-CVSS) X.1525 (CWSS)	ISO/IEC 15026; SACM, GSN/CAE (Evidence Measure)
Assessment	**Evidence**	**Risk Measure**	**Confidence Measure**

Provided Evidence supports notion of HIGH Confidence in the Risk Measure

Enabling a top-down, operational risk analysis followed by bottom-up, targeted vulnerability analysis to produce effective measurement, prioritization and mediation of the risks posed by system vulnerabilities

Ecosystem Foundation: Common Fact Model

Data Fusion & Semantic Integration



Facts & Findings

Risk Analysis
OTRM
(Situational awareness)

Risk Management Vocabulary

Risk

Asset

Threat

SFPM/SFP
SCAP/CVE

Note: SFPs are created using SBVR standard

Vulnerability Detection Vocabulary

Vulnerability

Assurance Vocabulary

ISO 15026
SACM
GSN/CEA

Claim

Argument

Evidence Item

Function

Module

Statement

Code Vocabulary

KDM/ISO 19506

Router

Firewall

Host

Network Vocabulary

KDM/ISO 19506

Capability

Performer

Information Exchange

System Architecture Vocabulary

UPDM/UAF
SysML

Tools integration possible only through standards

Everything Starts with Engineering …

- UPDM / UAFP
  - is a visual modeling standard that supports the DoDAF 2.0, MODAF, NAF and Security Views from DNDAF
  - UAFP v 1.0 supports the capability to:
    - model architectures for a broad range of complex systems, which may include hardware, software, data, personnel, and facility elements;
    - model consistent architectures for system-of-systems (SoS) down to lower levels of design and implementation;
    - support the analysis, specification, design, and verification of complex systems; and
    - improve the ability to exchange architecture information among related tools that are SysML based and tools that are based on other standards.

This engineering step already gives us an opportunity to consider security assurance and risk assessment resulting in security being built-in

Risk Analysis Specification: Work In Progress

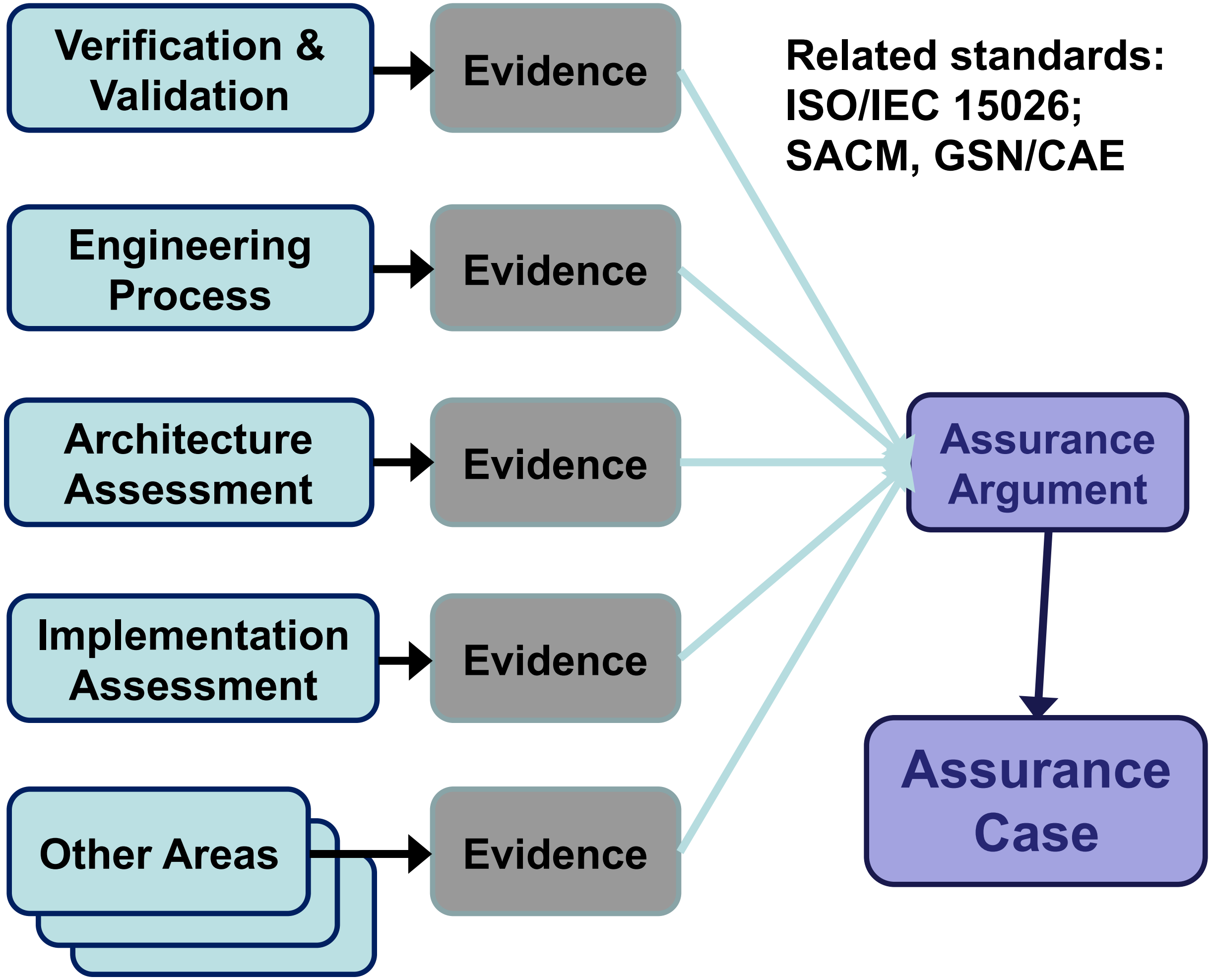
- Facilitating capability of understanding intricate attack options, assessing vulnerabilities and further facilitating decision-making in the area of risk management, including decisions related to investment into appropriate security controls
- Benefits:
  1. Risk analysis is performed in the context of operational architecture
     - Vulnerability characteristics are identified
  2. The riskiest system components are identified
     - The system components are systematically ranked based on their operational impact;
  3. More effective resource allocation and prioritization is enabled
     - Targeted "bottom-up vulnerability analysis' is performed to evaluate the riskiest component(s) against vulnerability characteristics.
  4. Optimized mitigation options could be determined
     - the outcomes of the operational impact and vulnerability analysis are linked to the corresponding vulnerability mitigation options;
  5. The quantitative measurements of the operational impact and vulnerabilities are provided
     - the contribution of individual access points and components as well as the effectiveness of mitigation options can be measured

Establishing Assurance - Reducing Uncertainty

While Assurance does not provide additional security services or safeguards, it does serve to reduce the uncertainty associated with vulnerabilities resulting from

- Bad practices
- Incorrect & inefficient safeguards

The result of System Assurance is justified **confidence** delivered in the form of an **Assurance Case**



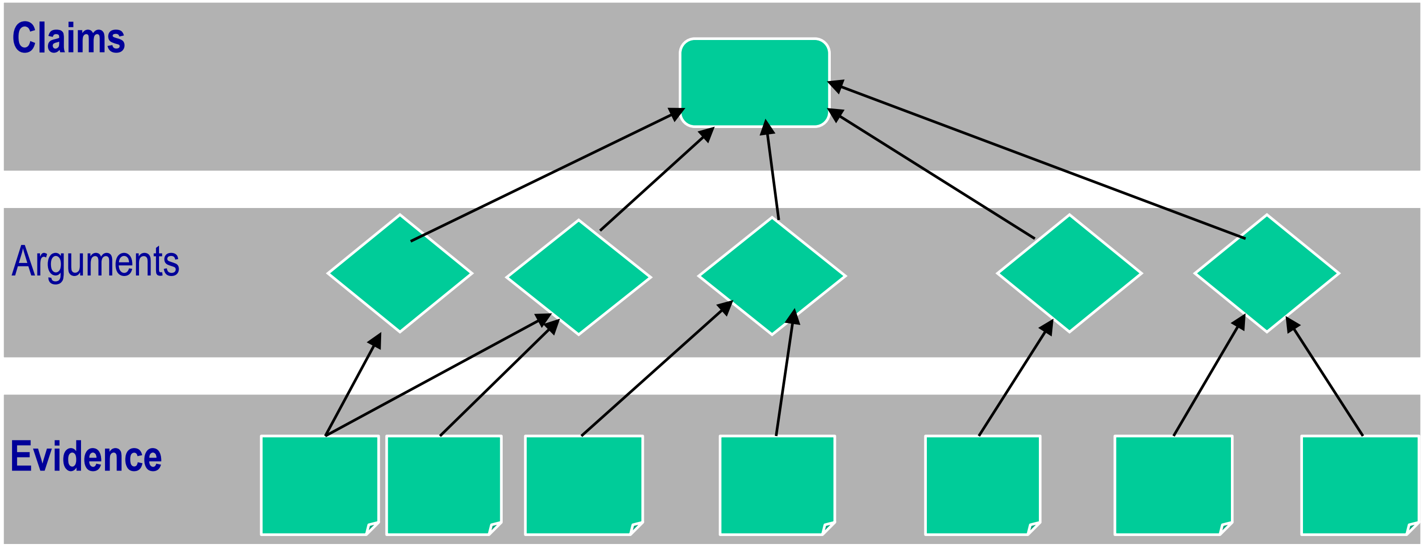
Related standards: ISO/IEC 15026; SACM, GSN/CAE

TYPES OF EVIDENCE FOR AN ASSURANCE CASE

Confidence demands objectivity, scientific method and cost-effectiveness

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***



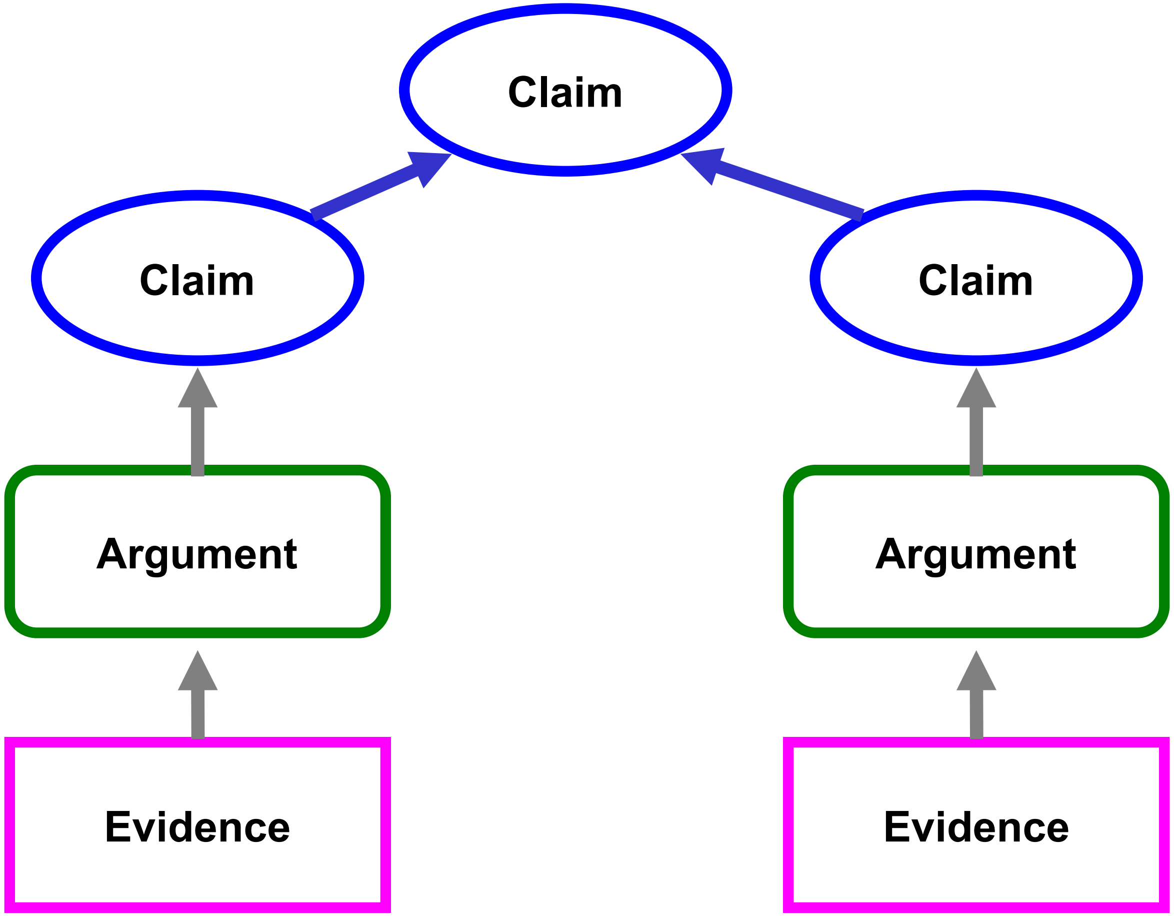
C A E 15+ Years Aviation Safety

Claims, Arguments, and Evidence

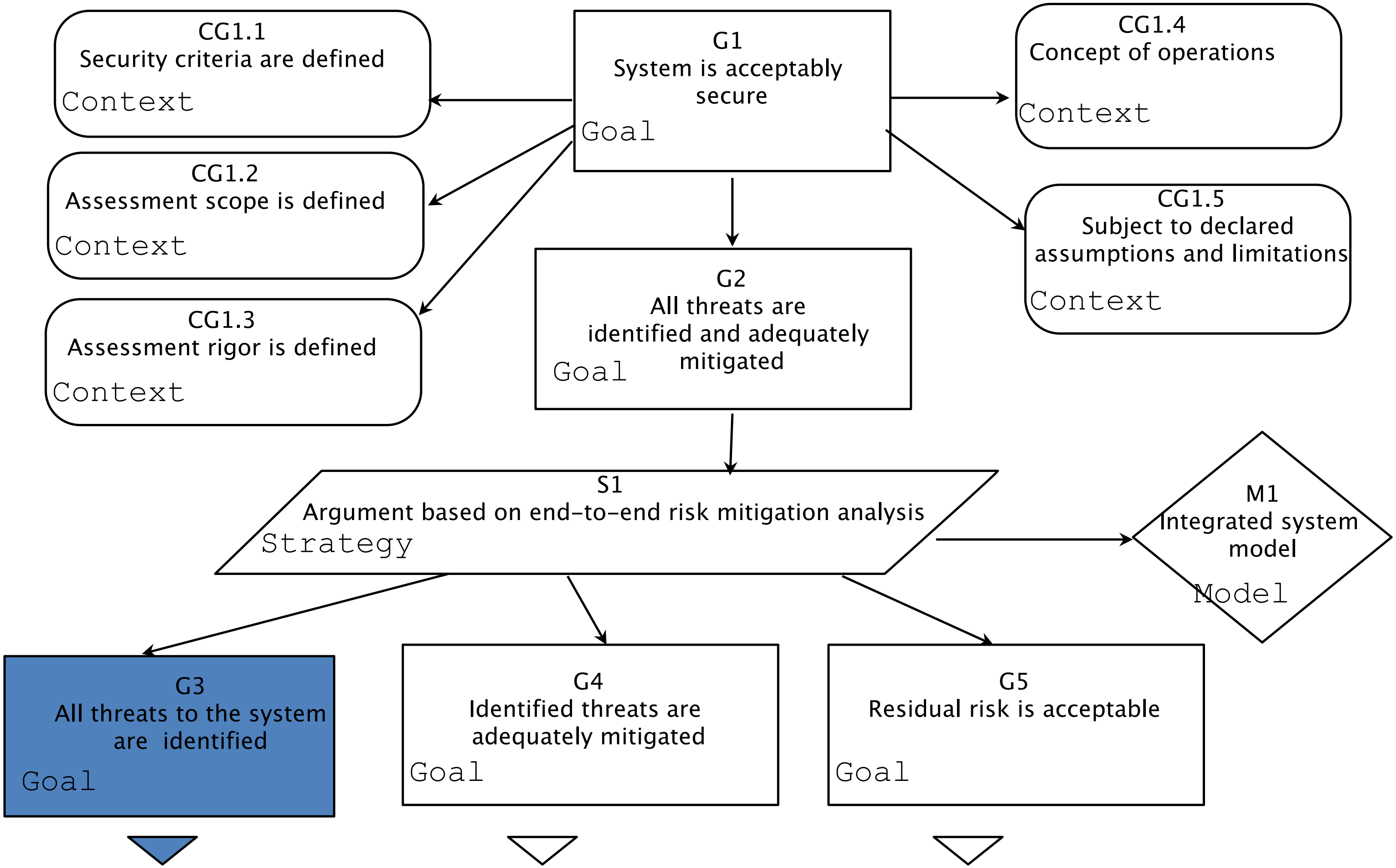
Claim = assertion to be proven

Argument = how evidence supports claim

Evidence = required documentation



Risk-based Assurance Case: Risk Mitigation Argument



CG1.1
Security criteria are defined
Context

G1
System is acceptably secure
Goal

CG1.4
Concept of operations
Context

CG1.2
Assessment scope is defined
Context

CG1.5
Subject to declared assumptions and limitations
Context

CG1.3
Assessment rigor is defined
Context

G2
All threats are identified and adequately mitigated
Goal

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

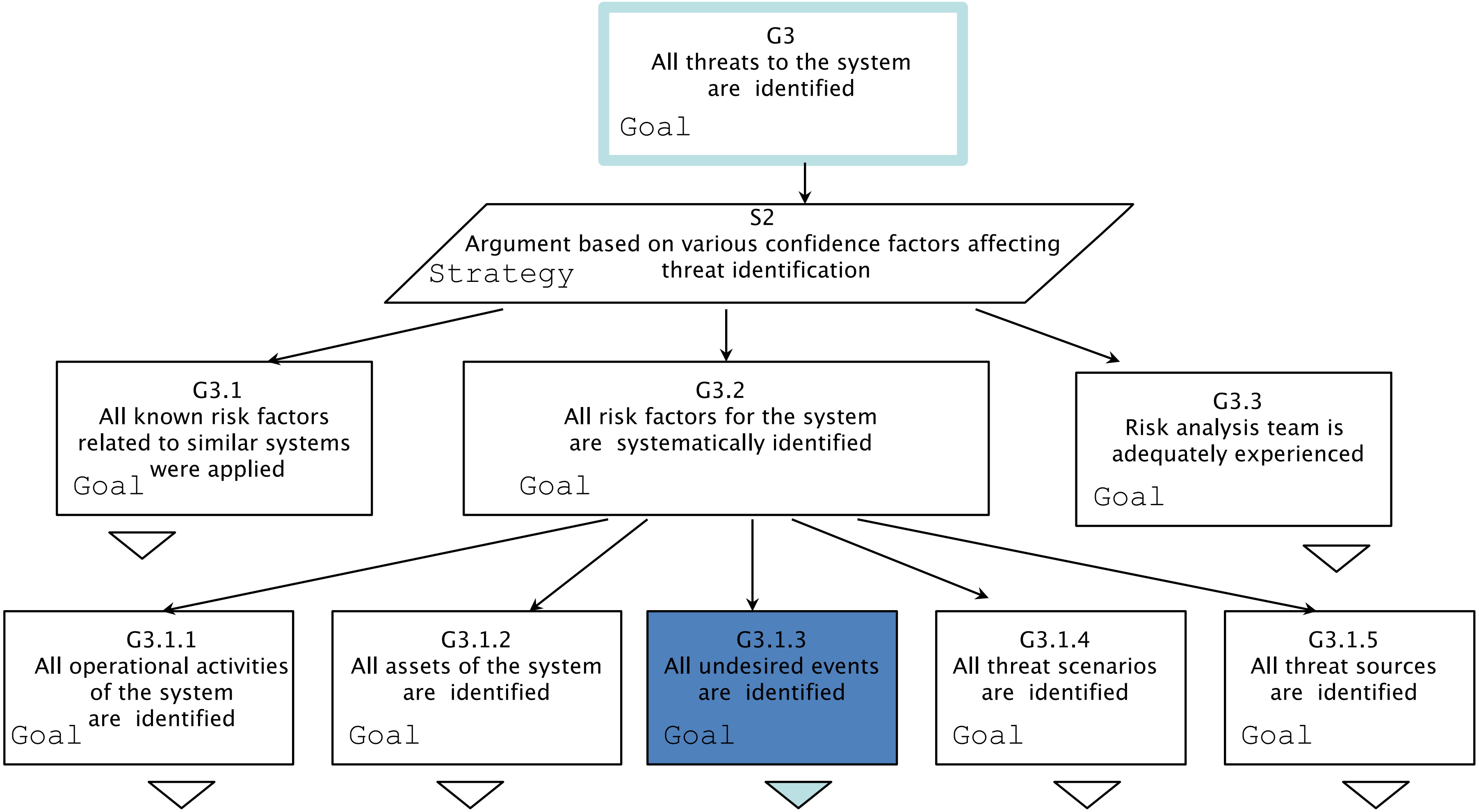
M1
Integrated system model
Model

G3
All threats to the system are identified
Goal

G4
Identified threats are adequately mitigated
Goal

G5
Residual risk is acceptable
Goal

Risk-based Assurance Case: Threat Identification (G3)



G3
All threats to the system are identified
Goal

S2
Argument based on various confidence factors affecting threat identification
Strategy

G3.1
All known risk factors related to similar systems were applied
Goal

G3.2
All risk factors for the system are systematically identified
Goal

G3.3
Risk analysis team is adequately experienced
Goal

G3.1.1
All operational activities of the system are identified
Goal

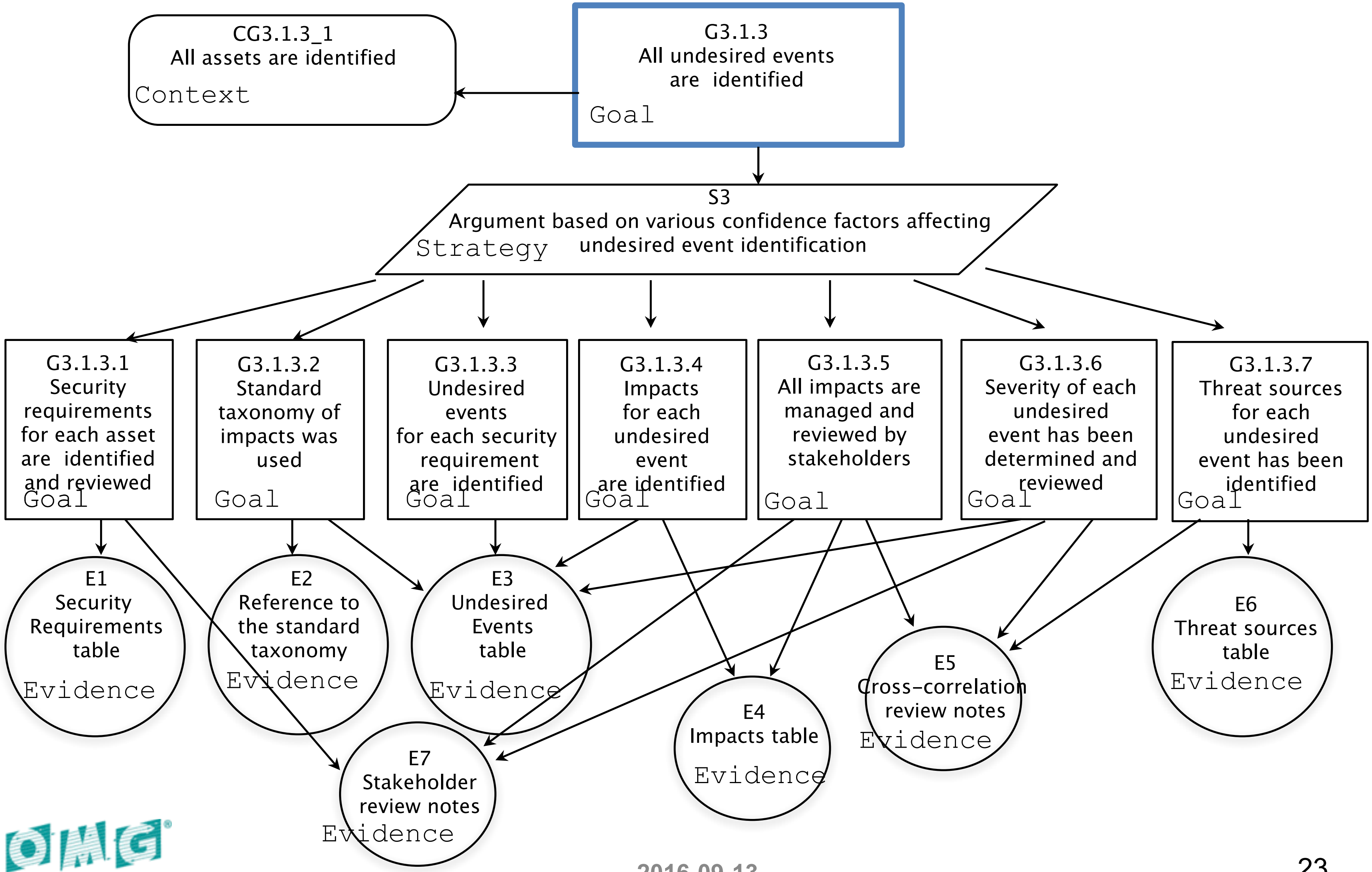
G3.1.2
All assets of the system are identified
Goal

G3.1.3
All undesired events are identified
Goal

G3.1.4
All threat scenarios are identified
Goal

G3.1.5
All threat sources are identified
Goal

Risk-based Assurance Case: Undesired Events (G3.1.3)



CG3.1.3_1
All assets are identified
Context

G3.1.3
All undesired events are identified
Goal

S3
Argument based on various confidence factors affecting undesired event identification
Strategy

G3.1.3.1
Security requirements for each asset are identified and reviewed
Goal

G3.1.3.2
Standard taxonomy of impacts was used
Goal

G3.1.3.3
Undesired events for each security requirement are identified
Goal

G3.1.3.4
Impacts for each undesired event are identified
Goal

G3.1.3.5
All impacts are managed and reviewed by stakeholders
Goal

G3.1.3.6
Severity of each undesired event has been determined and reviewed
Goal

G3.1.3.7
Threat sources for each undesired event has been identified
Goal

E1
Security Requirements table
Evidence

E2
Reference to the standard taxonomy
Evidence

E3
Undesired Events table
Evidence

E4
Impacts table
Evidence

E5
Cross-correlation review notes
Evidence

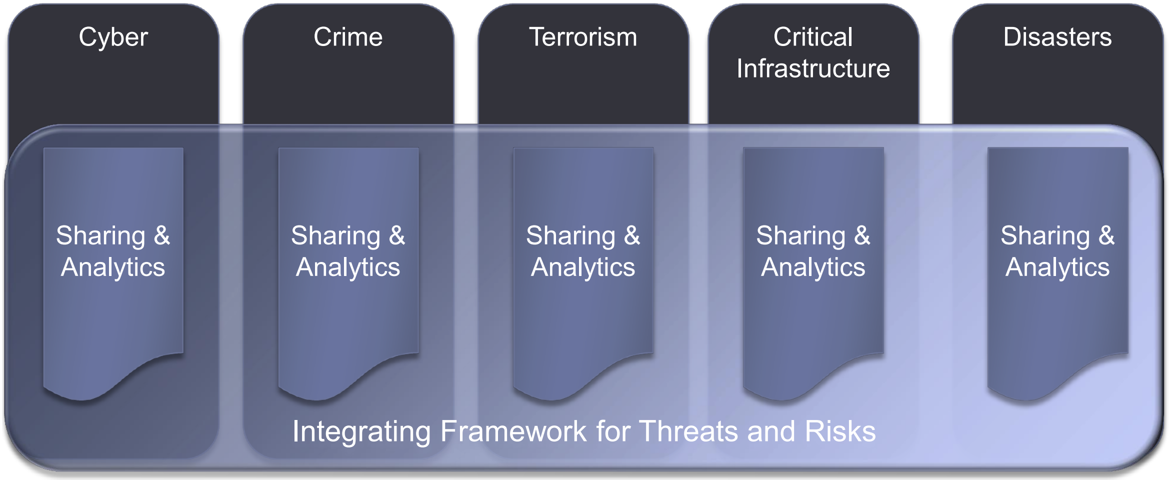
E6
Threat sources table
Evidence

E7
Stakeholder review notes
Evidence

Operational Threat Risk Model (OTRM)

conceptual model for operational threats and risks that unifies the semantics of and can provide a bridge across multiple threat and risk schemas and interfaces

Goal: An integrating framework



An integrating framework that helps us deal with all aspects of a risk or incident

A federation of risk and threat information sharing and analytics capabilities

Integrated threat and risk management across

- Domains
- Products and technologies
- Organizations

Leading to

- Shared awareness of threats and risks
- Federated information analytics (including “big data”)
- Improved mitigation of threats and risk
- Situational awareness in real time
- Ability to respond and recover

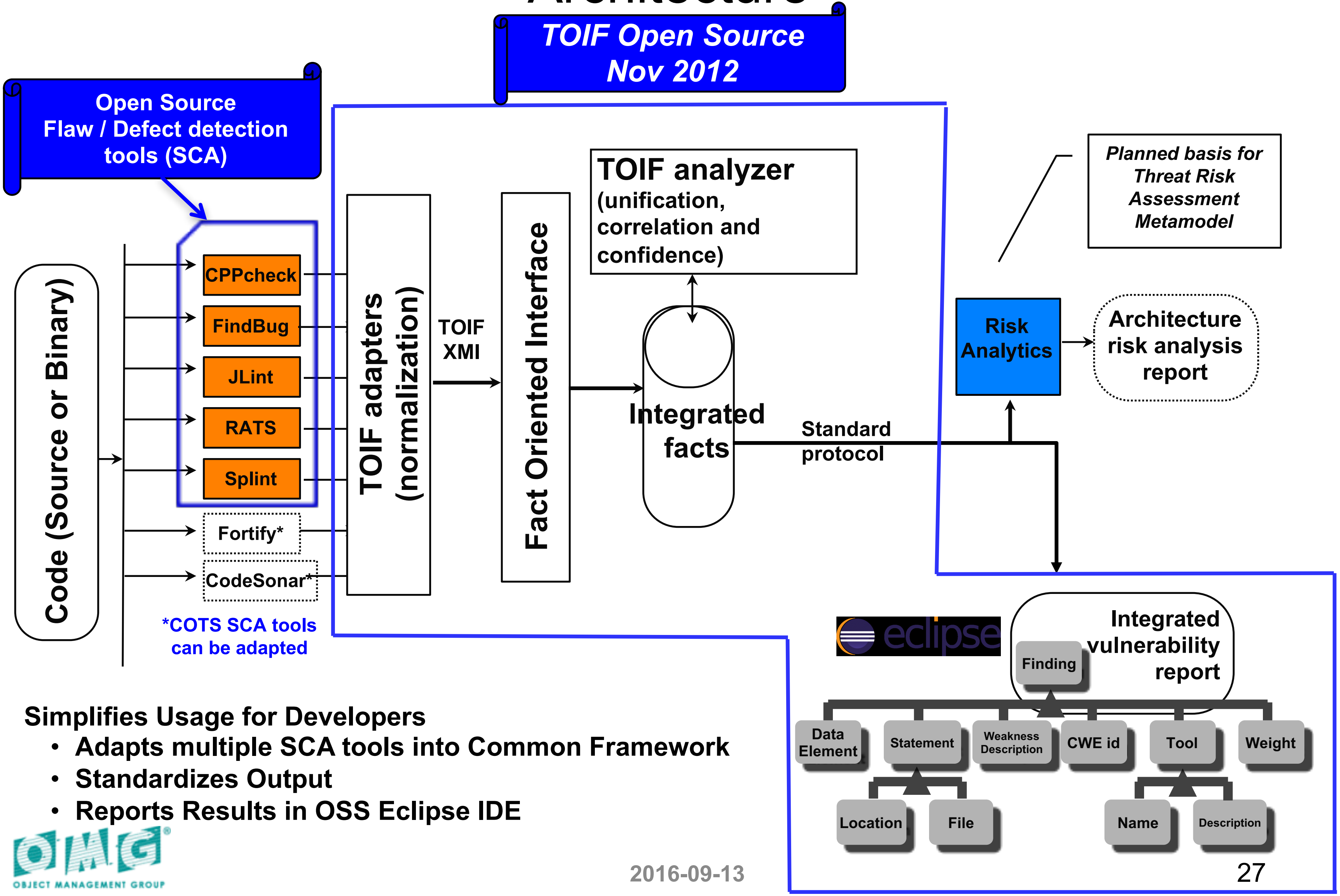
Bottom-Up Vulnerability Analysis

- Supported by set of integrated OMG standards
  - Knowledge Discovery Metamodel (KDM) - ISO/IEC 19506
    - Ontology for software systems and their operating environments, that defines common metadata required for deep semantic integration of Application Lifecycle Management tools
  - Software Fault Pattern Metamodel & Software Fault Patterns (WIP)
    - Generalized description of family of computations with certain common faults & fully discernable in code
    - Related to CWEs
  - X.1520 (SCAP-CVE)
    - Known Vulnerabilities in existing systems captured in National Vulnerability Database
  - X.1524 (CWE)
    - Common Weakness Enumeration – a list of software weaknesses that could have security implications

Example specification for a suite of integrated tools

TOOLS OUTPUT INTEGRATION FRAMEWORK (TOIF)

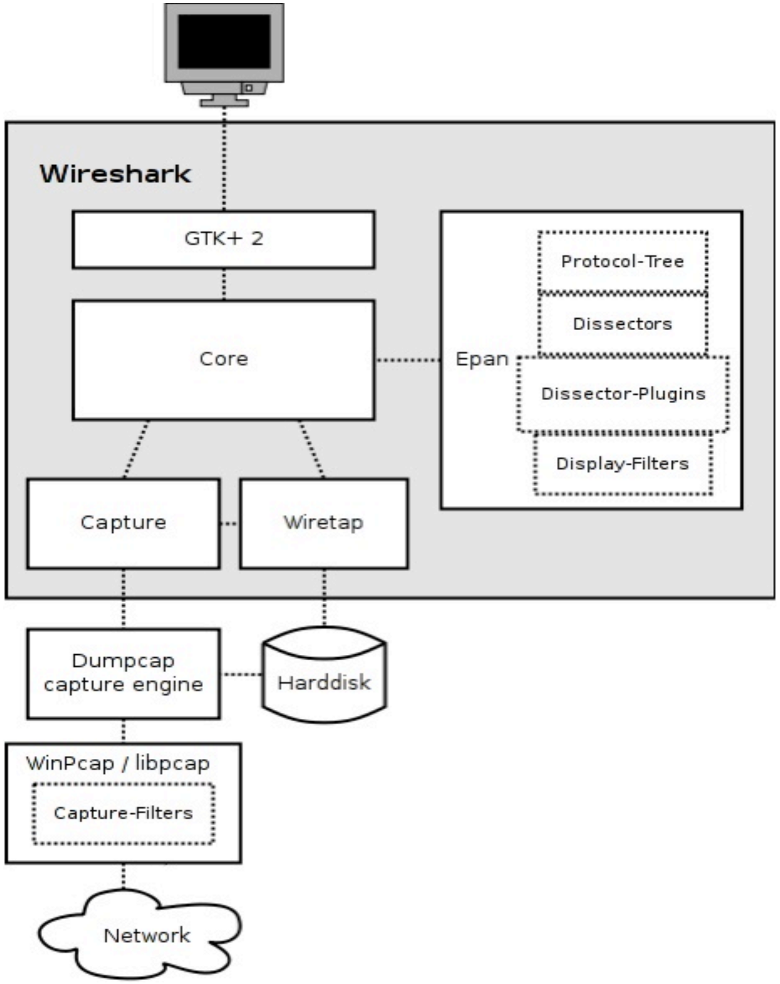
Tools Output Integration Framework (TOIF) Architecture

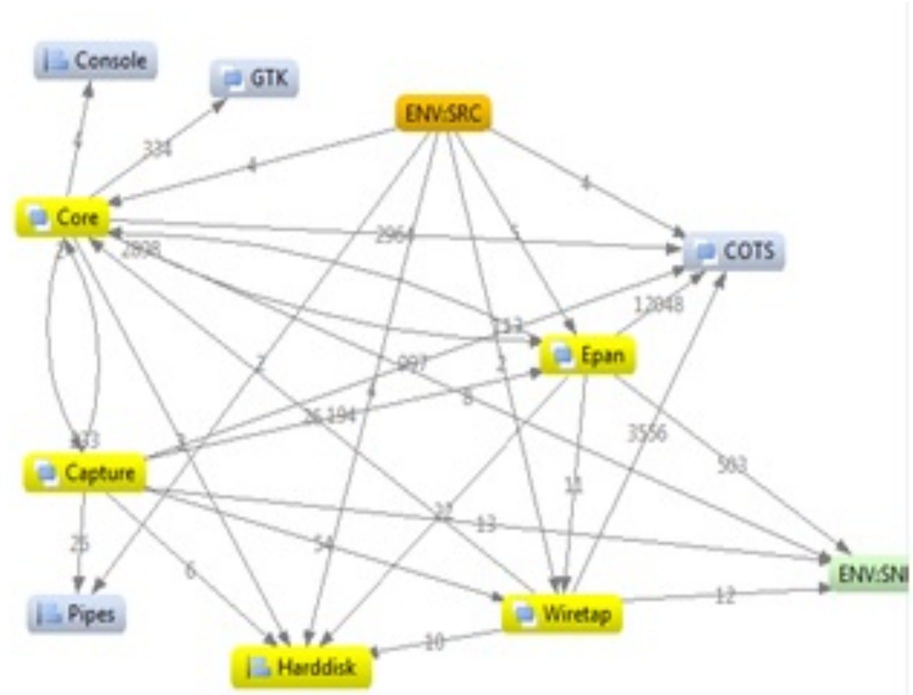


Simplifies Usage for Developers

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

Software Risk Analyzer



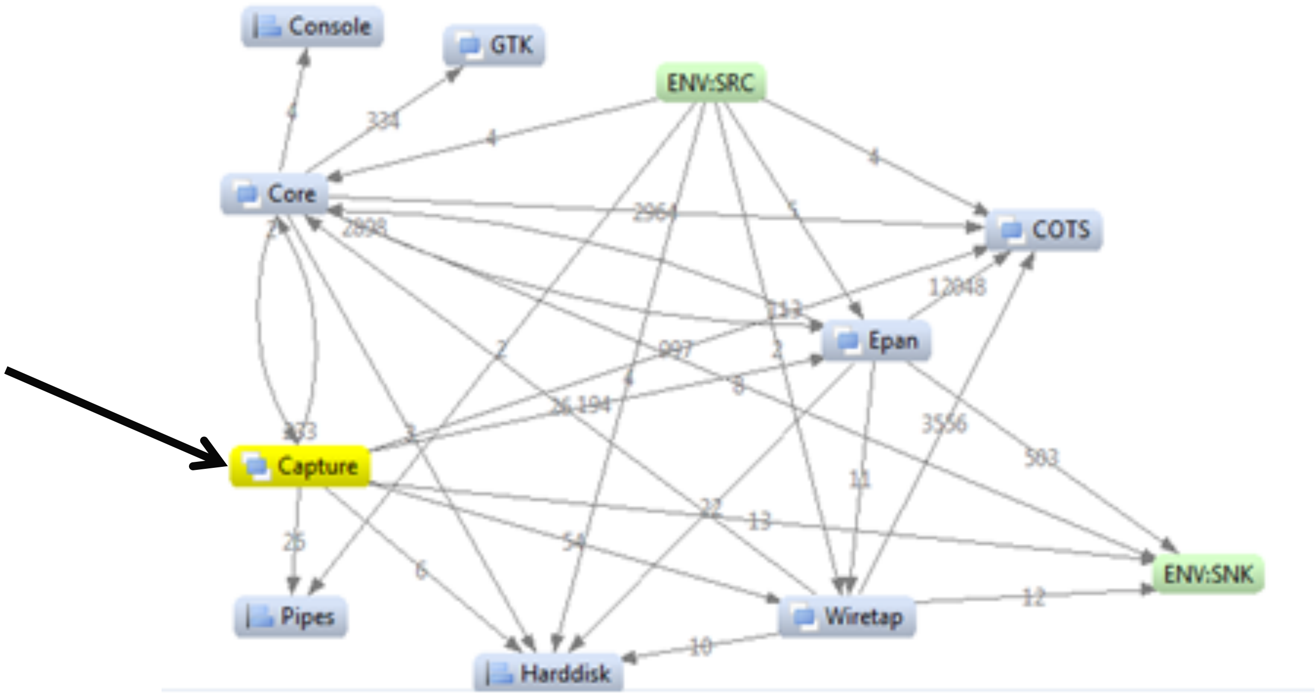


Compare the Design Information to Implemented Code

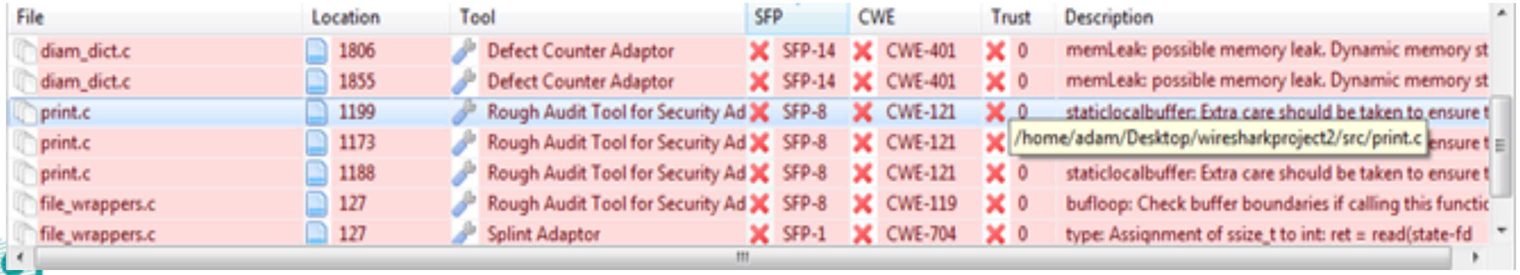
Threat Risk Analysis of Attack Paths

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	✗	/home/adam/Desktop/wiresharkproject2/src/print.c ensure t
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

Conclusion

- All these standards and Frameworks are already supported by tools
- Lockheed Martin's performed evaluations
  - 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%.

Djenana Campara

E-mail: djenana@kdmanalytics.com

THANK YOU