System Assurance and Related Standards

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

OBJECT MANAGEMENT GROUP

Acknowledgments

- Djenana Campara, CEO KDM Analybics
  - 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

Agenda

- Introduction & Overview
- Defining Assurance
- Establishing Assurance
- Assurance Standards
  - Structured Assurance Case Metamodel
  - Operational Threat & Risk Model
  - Software Fault Patterns Metamodel
  - Tool Output Integration Framework
  - Dependability Assurance Framework

Achieving Cyber Security by …

This beauty behind me was driven only 1000 miles a year by a little old lady from Pasadena!

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

End Goal

ASSURANCE

Information, Assets & Services

are

Protected Against Compromise

DEFINING ASSURANCE

What is Assurance?

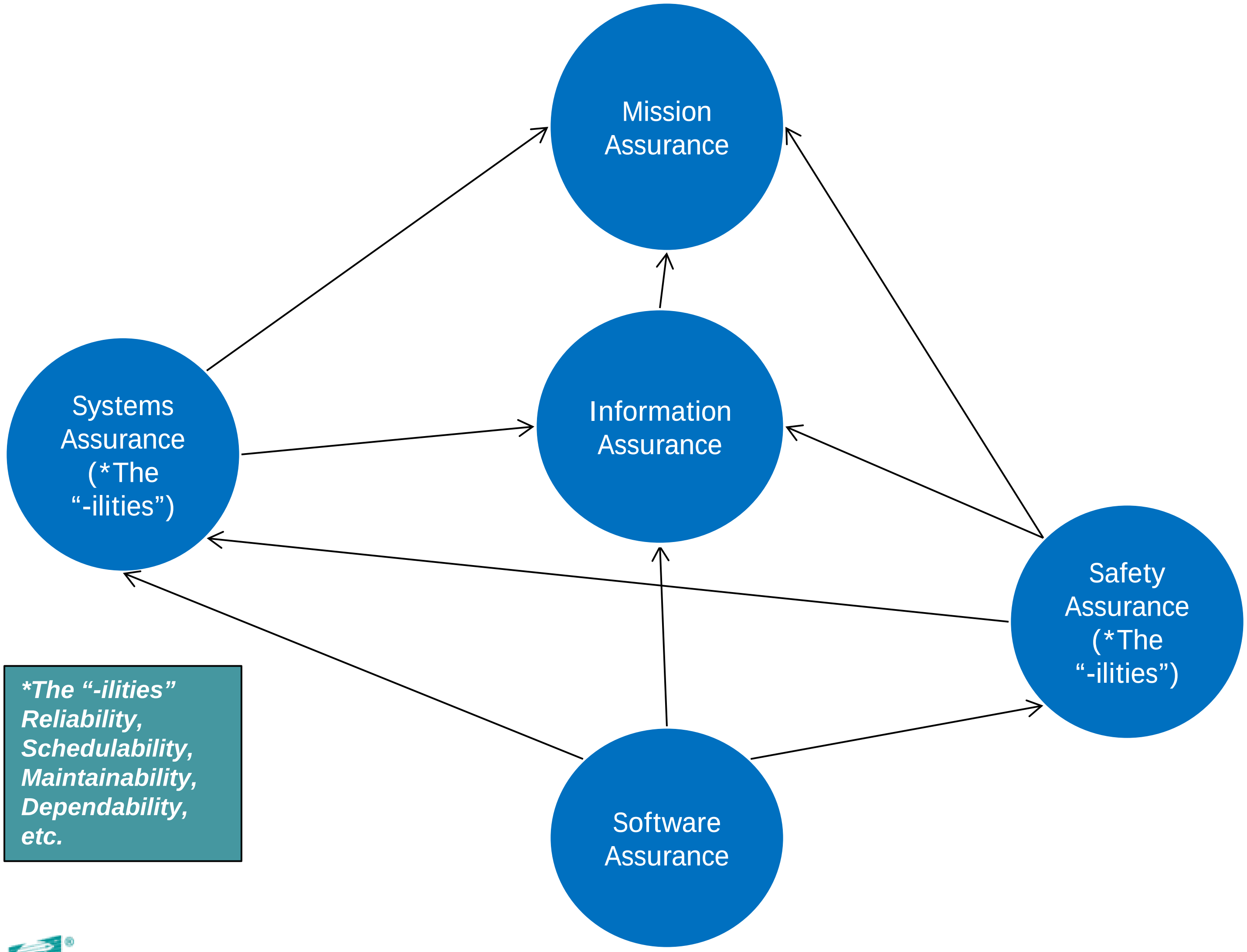
- **Assurance** is the **measure of confidence** that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy. - CNSS 4009 IA Glossary
- **Information Assurance (IA)** are measures that protect and defend information 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)

providing *confidence* in

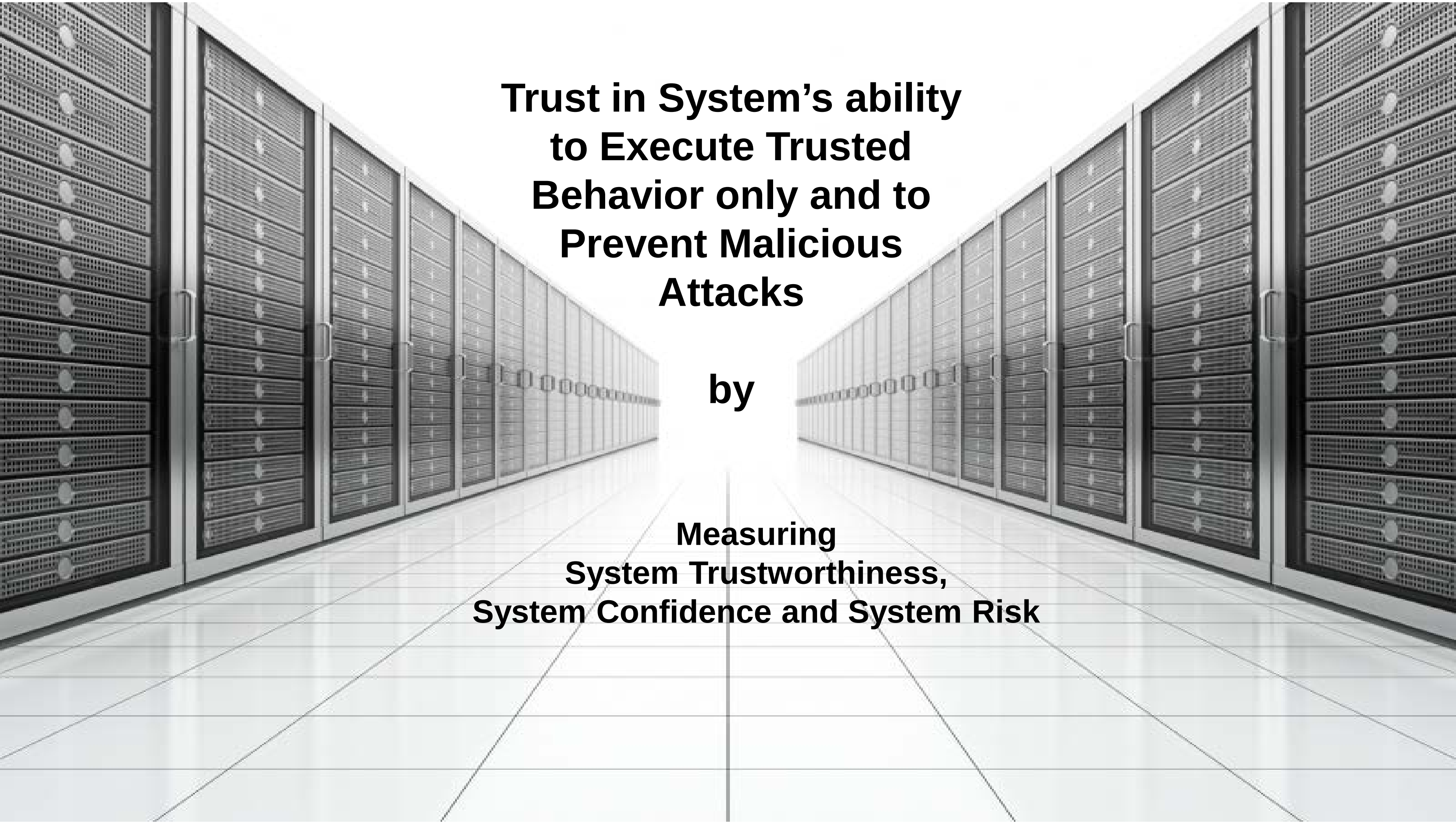
- **Mission Assurance (MA)** is the ability of operators to achieve their mission, continue critical processes, and protect people and assets in the face of internal and external attack (both physical and cyber), unforeseen environmental or operational changes, and system malfunctions. *(See notes page for further description.) – MITRE Systems Engineering Guide*
- **Mission Assurance (cyberspace).** Measures required to accomplish essential objectives of missions in a contested environment. Mission assurance entails prioritizing mission essential functions, mapping mission dependence on cyberspace, identifying vulnerabilities, and mitigating risk of known vulnerabilities (AFDD 3-12, Cyberspace Operations, 2010).
- **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


Mission Assurance
Systems Assurance (*The "-ilities")
Information Assurance
Safety Assurance (*The "-ilities")
Software Assurance

The "-ilities" Reliability, Schedulability, Maintainability, Dependability, etc.

Addressing Stakeholders' Need for Trust



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

by

Measuring
System Trustworthiness,
System Confidence and System Risk

Delivering System Assurance in any Domain:

Delivering System Predictability and Reducing Uncertainty

1. **Specify Assurance Case**
   - Supplier must 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

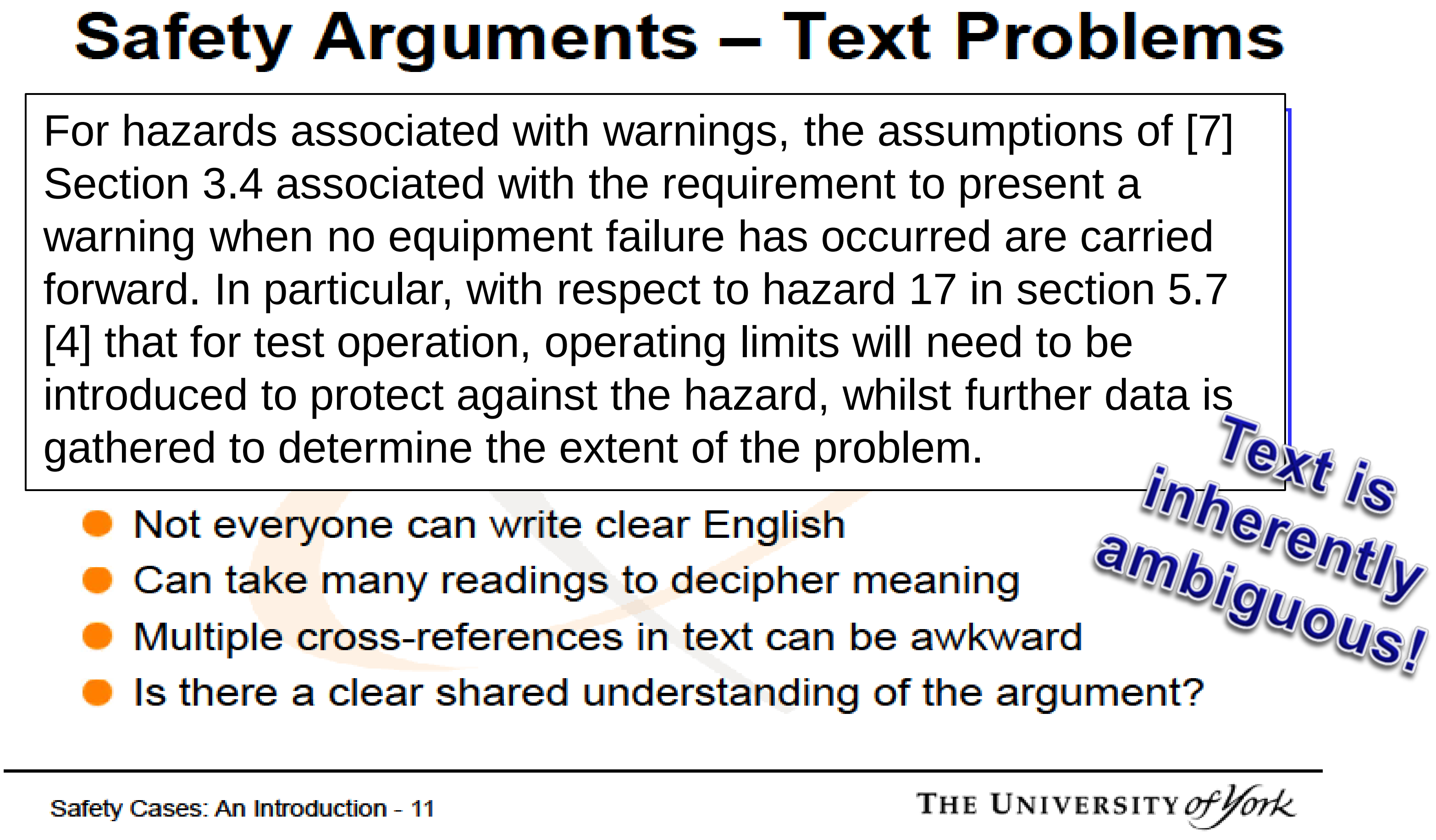
Summary of Challenges

- 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 system artifacts that implements them
  - 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

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

My thanks to colleague Prof. Tim Kelly

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



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.

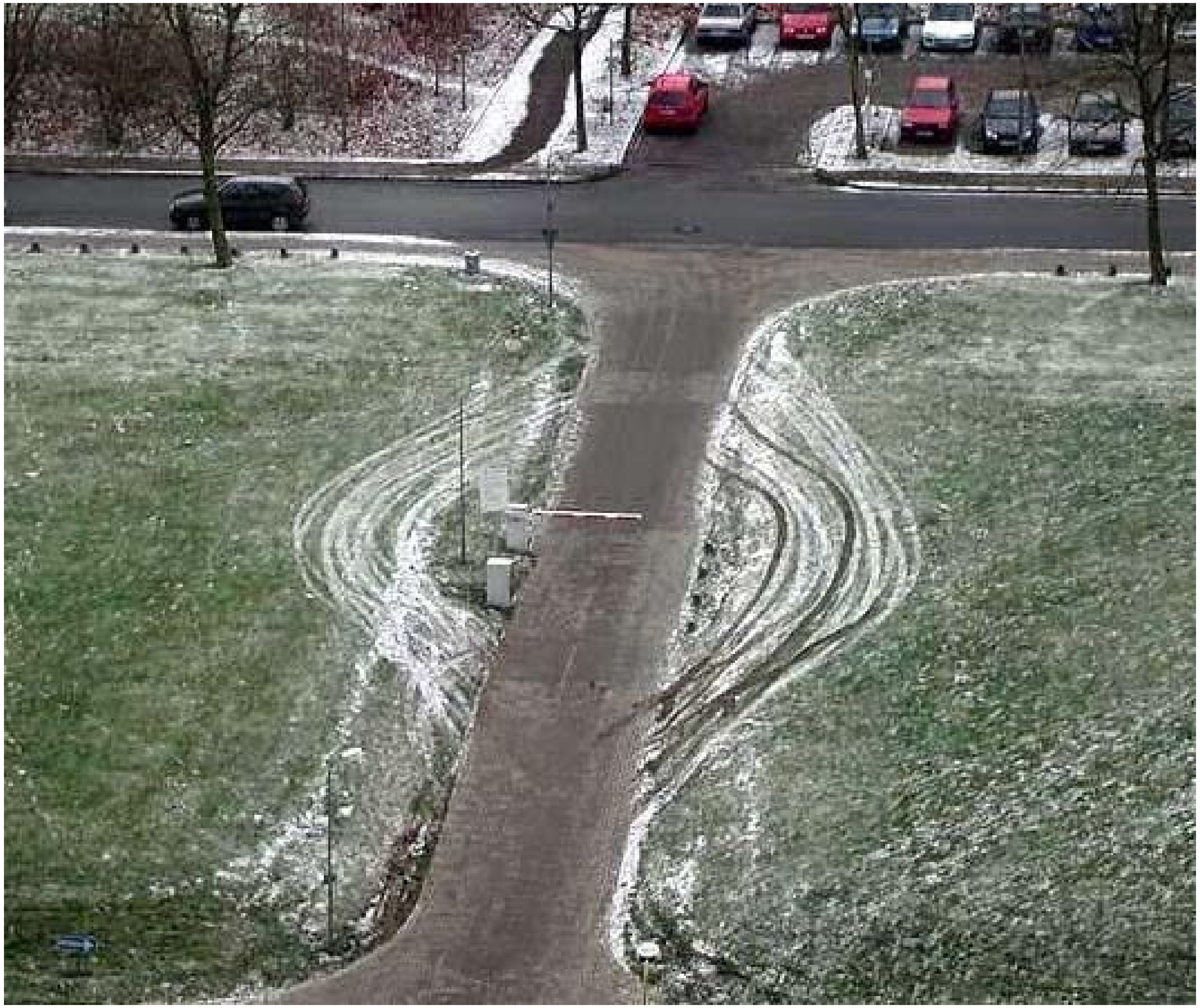
- Not everyone can write clear English
- Can take many readings to decipher meaning
- Multiple cross-references in text can be awkward
- Is there a clear shared understanding of the argument?

Text is inherently ambiguous!

Safety Cases: An Introduction - 11

THE UNIVERSITY of York

One Picture is Worth a Thousand Words!



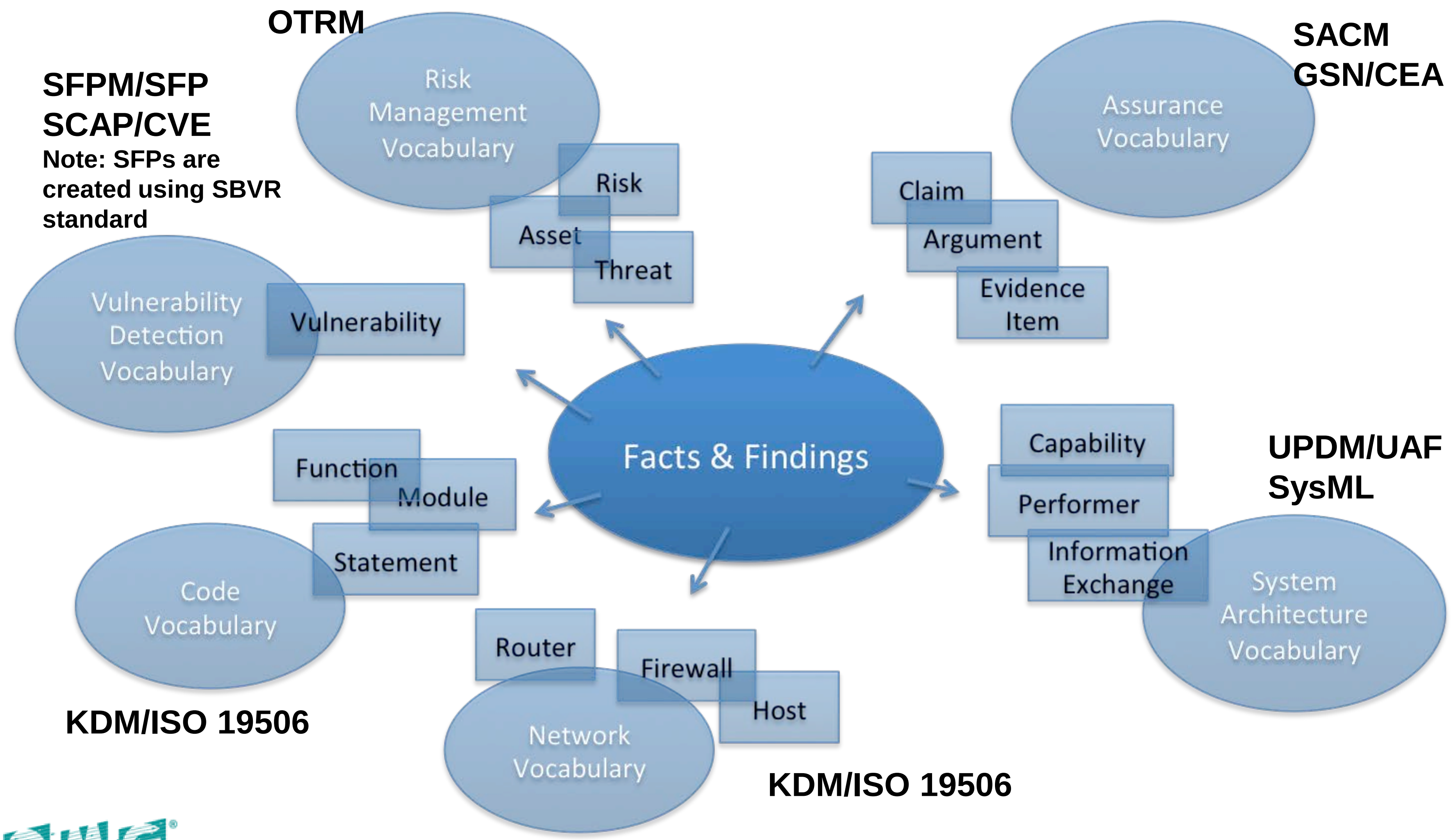
Addressing Challenges: OMG Software/System Assurance Ecosystem

Set of integrated standards

- OMG-ISO/IEC 19506 Knowledge Discovery Metamodel
  - Achieving system transparency in unified way
- OMG Structured Assurance Case Metamodel
  - Intended for presenting Assurance Case and providing end-to-end traceability: requirement-to-artifact
  - Goal Structured Notation (GSN) / Claims Arguments Evidence (CAE)
- OMG Unified Architectural Framework (Formally DoDAF & MODAF information)
  - UML Profile for DODAF/MODAF:UPDM)
- OMG System Engineering Modeling Language (SysML)
- OMG Semantics of Business Vocabularies and Rules (SBVR)
  - For formally capturing knowledge about weakness space: weaknesses & vulnerabilities
- OMG Structured Metrics Metamodel (SMM)
  - Representing libraries of system and assurance metrics
- OMG Operational Threat & Risk Model (OTRM) - standardization in progress
- OMG Software Fault Patterns (SFP) Metamodel standardization in progress
- OMG Tool Output Integration Framework - SCA tool execution reporting standardization in progress
- NIST Security Automation Protocol (SCAP)

Ecosystem Foundation: Common Fact Model

Data Fusion & Semantic Integration



OTRM

SFPM/SFP
SCAP/CVE

Note: SFPs are created using SBVR standard

SACM
GSN/CEA

UPDM/UAF
SysML

KDM/ISO 19506

KDM/ISO 19506

Trustworthiness

Standards **---------------------** **Integrated Facts**	**Engineering**	**Risk**	**Assurance**
Operational Environment	Operational Views (UPDM/UAF or SysML)	OTRM	SACM, GSN/CAE (Claim & Argument)
Architecture	UPDM/UAF SysML SFPM & SFPs SCAP (CVE) SMM & Measures	SCAP (CVSS)	SACM-Evidence Measure
Implementation	KDM SFPM & SFPs SCAP (CVE) SMM & Measures	SCAP (CVSS)	SACM-Evidence Measure
Assessment	Evidence	Risk Measure	Confidence Measure

Goal: Evidence exist for "HIGH Confidence that Risk is LOW"

Utilization of Assurance Modeling Tools

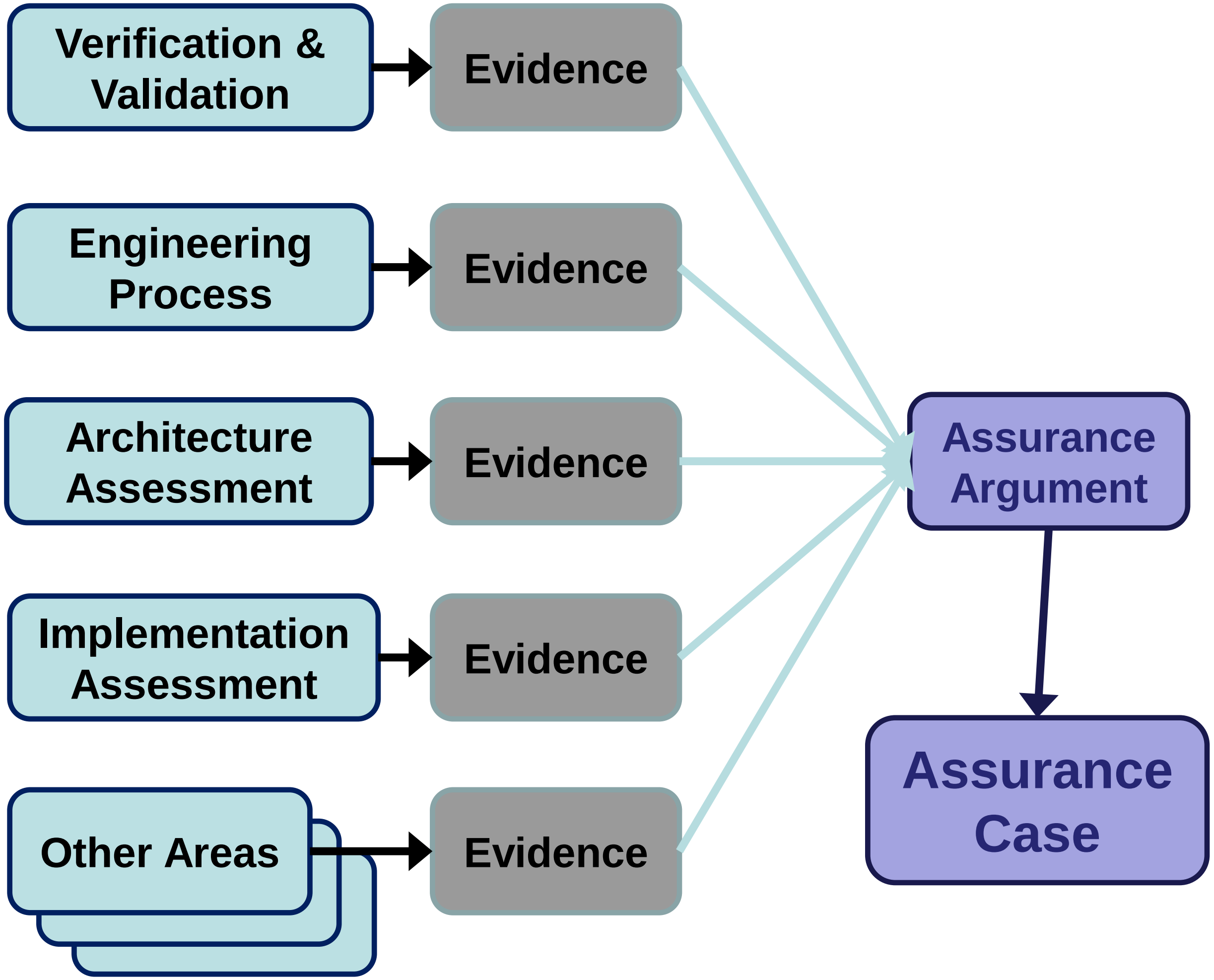
ESTABLISHING ASSURANCE

System Assurance Reduces ~~(Eliminates)~~ 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 safeguards

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

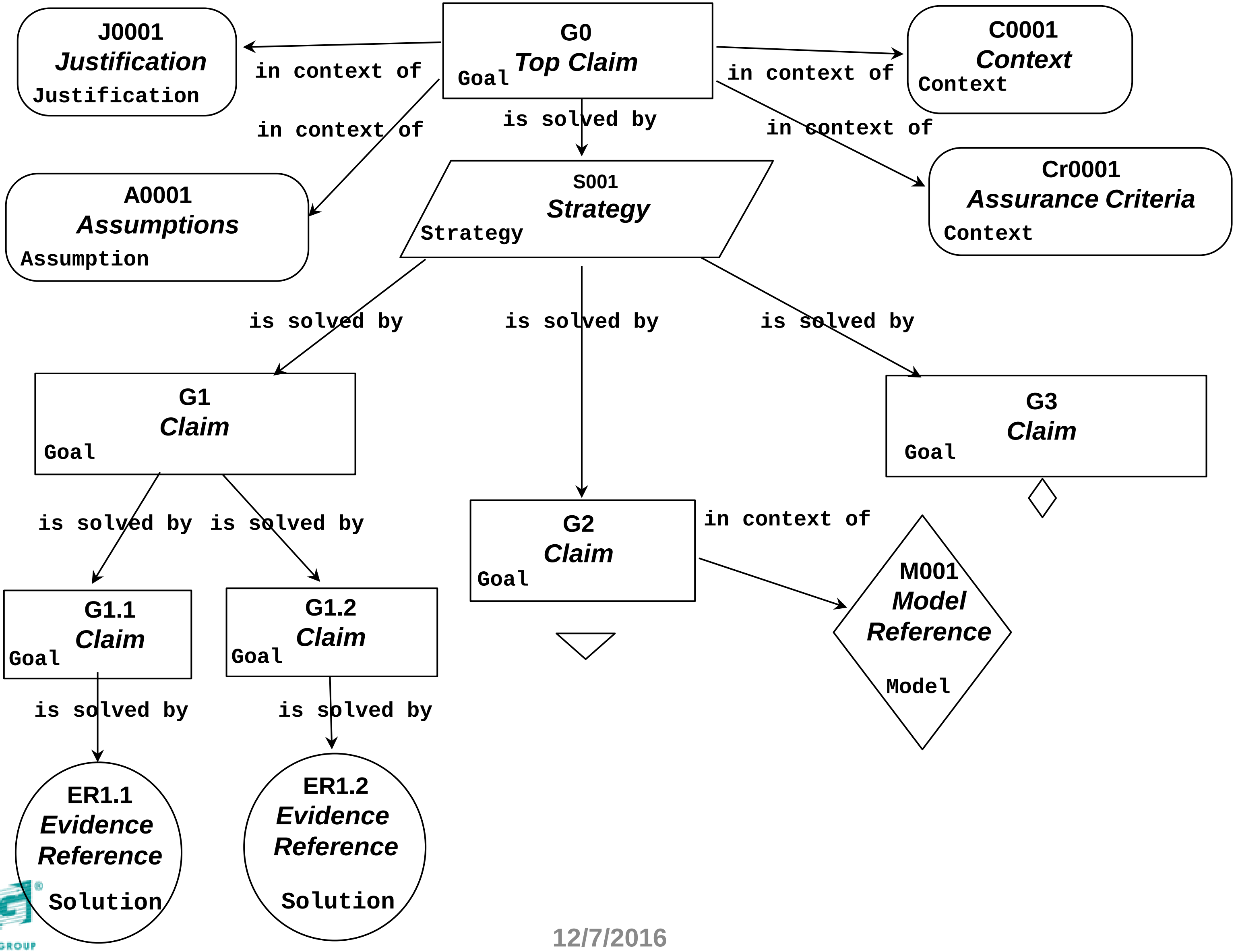


TYPES OF EVIDENCE FOR AN ASSURANCE CASE

Confidence demands objectivity, scientific method and cost-effectiveness

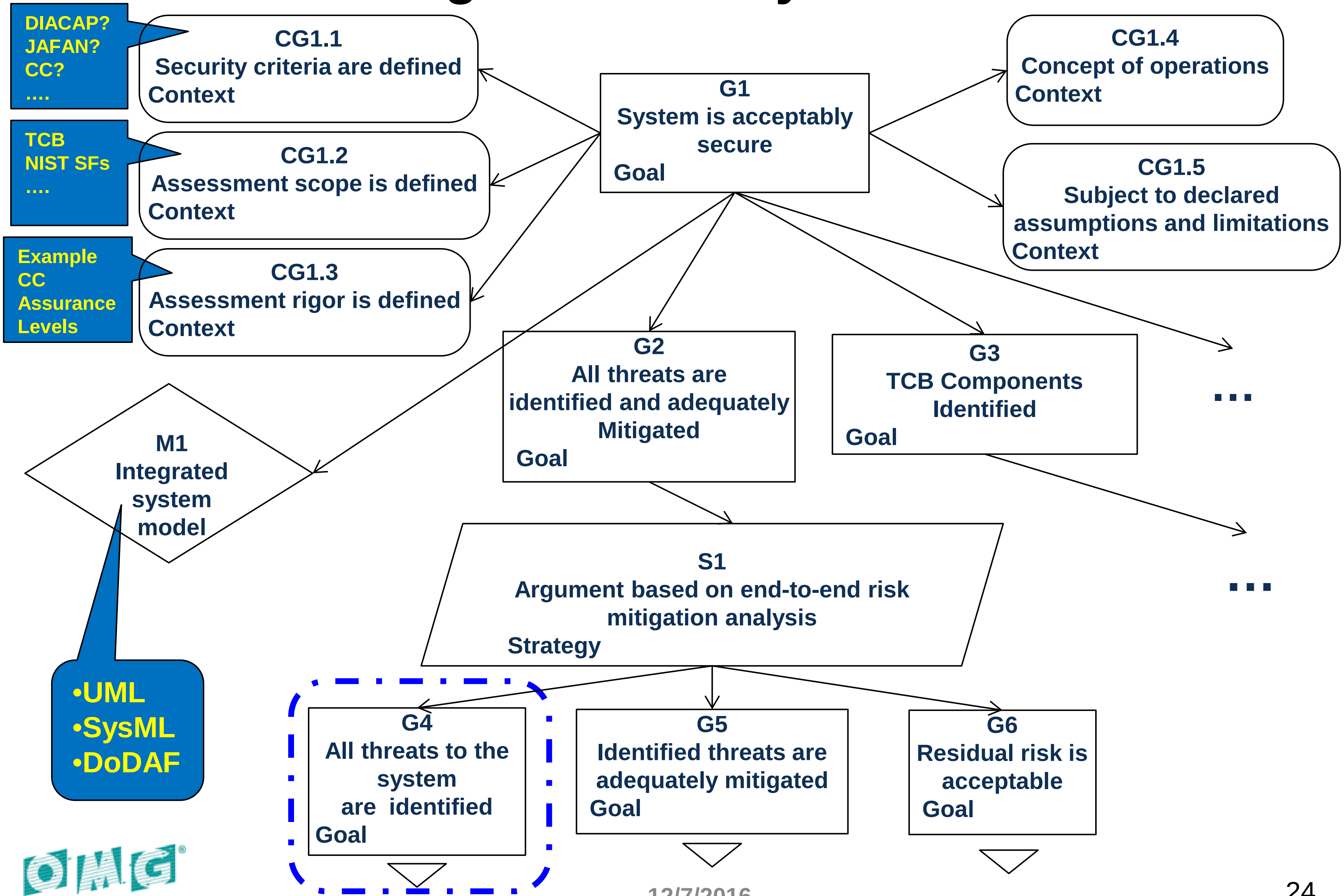
OMG STRUCTURED ASSURANCE CASE METAMODEL (SACM)

OMG’s Structured Assurance Case Metamodel



12/7/2016

Establishing the Security Assurance Case



DIACAP?
JAFAN?
CC?
….

CG1.1
Security criteria are defined
Context

TCB
NIST SFs
….

CG1.2
Assessment scope is defined
Context

Example
CC
Assurance
Levels

CG1.3
Assessment rigor is defined
Context

G1
System is acceptably secure
Goal

CG1.4
Concept of operations
Context

CG1.5
Subject to declared assumptions and limitations
Context

G2
All threats are identified and adequately Mitigated
Goal

G3
TCB Components Identified
Goal

…

M1
Integrated system model

- •UML
- •SysML
- •DoDAF

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

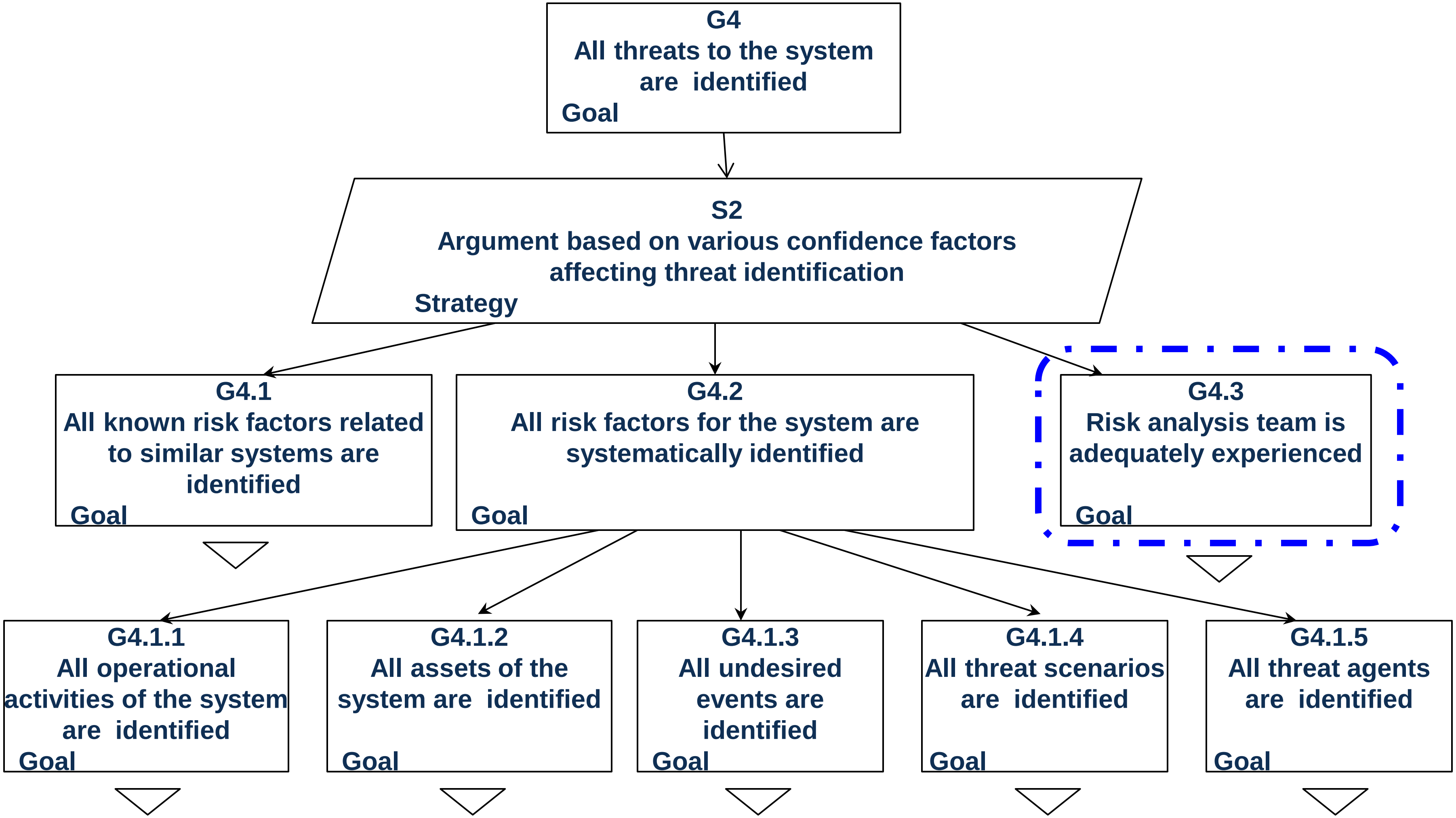
…

G4
All threats to the system are identified
Goal

G5
Identified threats are adequately mitigated
Goal

G6
Residual risk is acceptable
Goal

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

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

G4.3
Risk analysis team is adequately experienced
Goal

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

G4.1.2
All assets of the system are identified
Goal

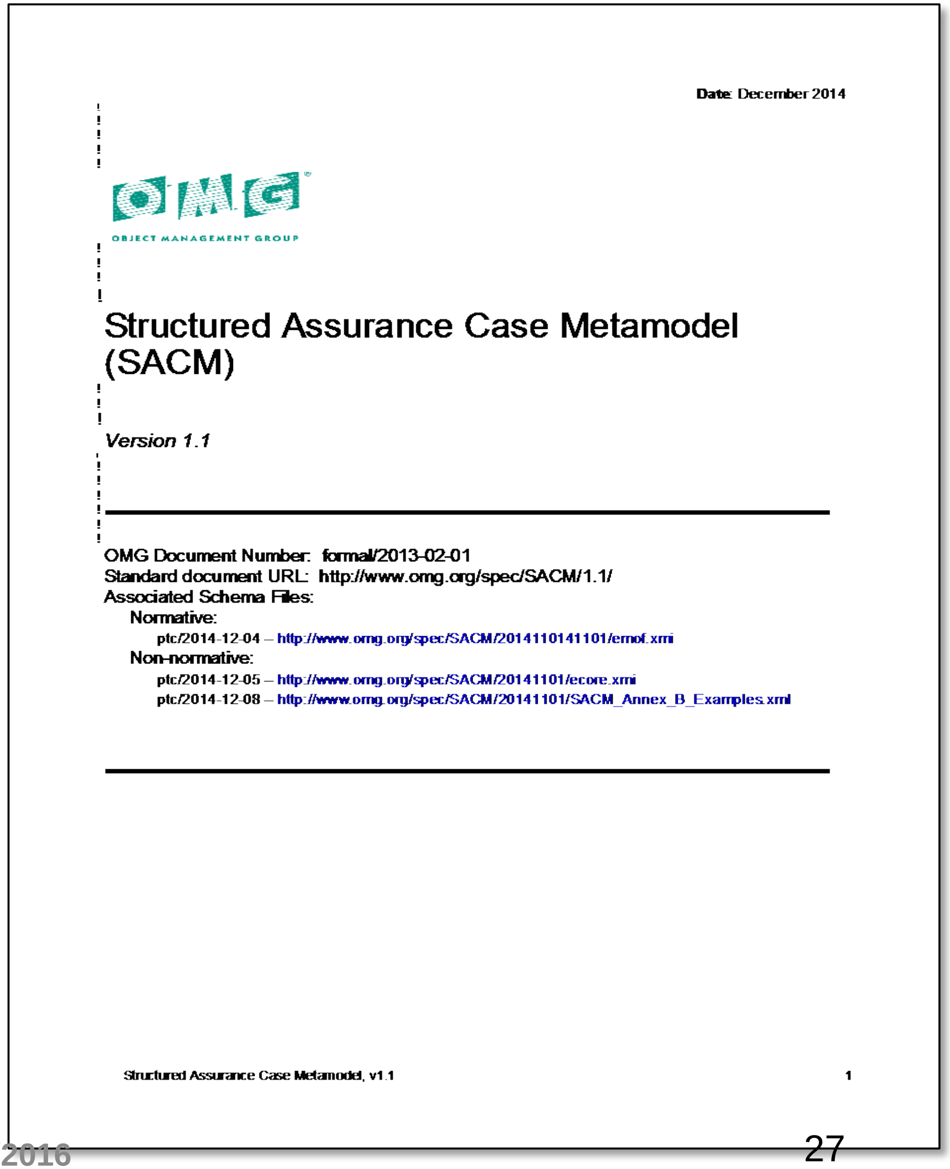
G4.1.3
All undesired events are identified
Goal

G4.1.4
All threat scenarios are identified
Goal

G4.1.5
All threat agents are identified
Goal

OMG - Structured Assurance Case Metamodel

1.0 → 1.1 → 2.0



Date: December 2014

Structured Assurance Case Metamodel (SACM)

Version 1.1

OMG Document Number: formal/2013-02-01
Standard document URL: http://www.omg.org/spec/SACM/1.1/
Associated Schema Files:
Normative:
ptc/2014-12-04 – http://www.omg.org/spec/SACM/20141101/emof.xmi
Non-normative:
ptc/2014-12-05 – http://www.omg.org/spec/SACM/20141101/ecore.xmi
ptc/2014-12-08 – http://www.omg.org/spec/SACM/20141101/SACM_Annex_B_Examples.xml

Structured Assurance Case Metamodel, v1.1 1

Tools for Assurance Cases

- Assurance and Safety Case Environment (ASCE)

  http://www.adelard.com/services/SafetyCaseStructuring/
- Astah GSN http://astah.net/editions/gsn
- CertWare http://nasa.github.io/CertWare/
- AdvoCATE: An Assurance Case Automation Toolset http://rd.springer.com/chapter/10.1007%2F978-3-642-33675-1_2
- Assurance Case Editor (ACEdit)

  https://code.google.com/p/acedit/
- D-Case Editor: A Typed Assurance Case Editor

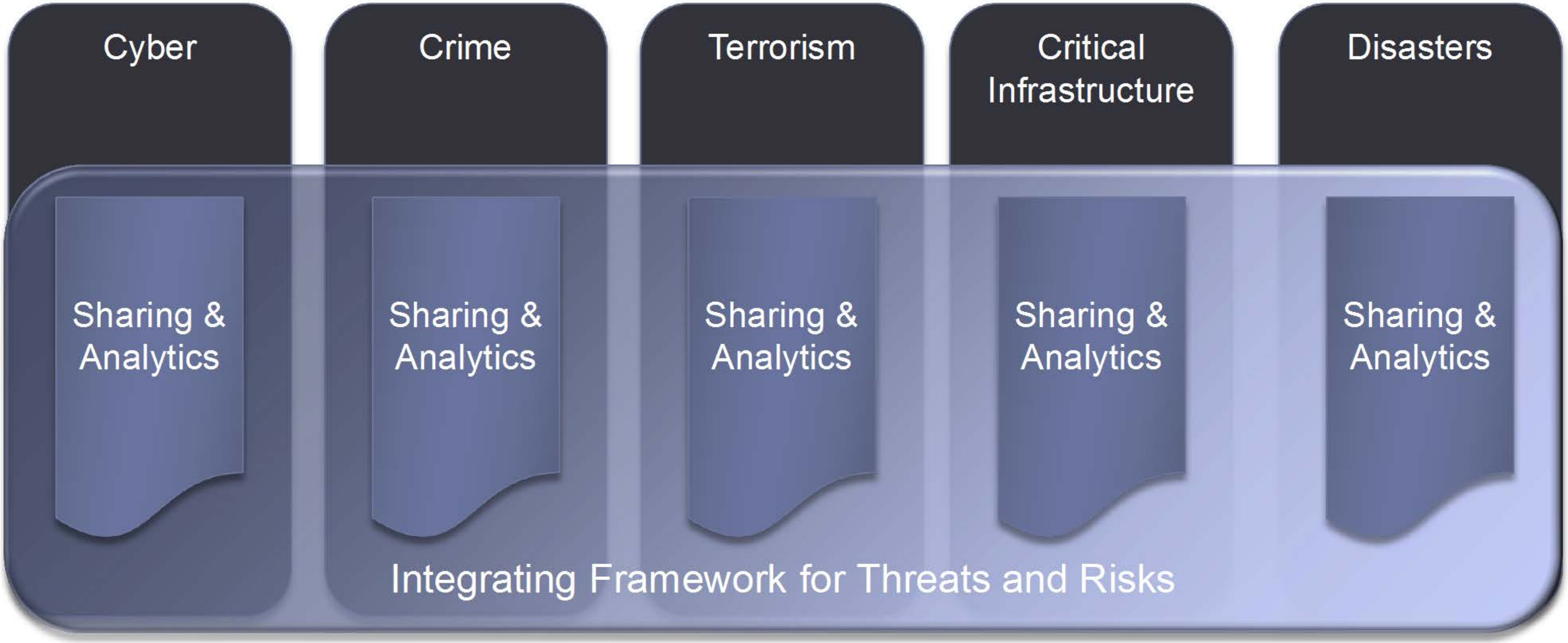
  https://github.com/d-case/d-case_editor

UML Operational Threat & Risk Model Request for Proposal

OMG Document: SysA/2014-06-06

THREAT RISK SHARING AND ANALYTICS

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

The Opportunity

- Integrated threat and risk management across
  - Domains
    - Cyber, Criminal, Terrorism, Critical Infrastructure, Natural disasters, others…
  - Products and technologies
    - Enterprise risk management, cyber tools, disaster planning, etc…
  - Organizations
    - Government (Global, National, State, Local, Tribal), Non-governmental organizations, Commercial
- 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

OMG SOFTWARE FAULT PATTERN METAMODEL (SFPM)

Overview of the SFP Metamodel

- SFP Metamodel (SFPM) further defines the technical elements involved in a definition of a faulty computation
  - Structural elements of a catalog
    - Named clusters of faulty computations
    - Subclusters
    - Named SFPs
  - Identified parameters for each SFP
  - Linkage to CWE catalog
    - Set of CWEs in each cluster
    - Mapping between parameter values that uniquely identify a CWE as an instance of a SFP
    - Identified gaps in CWE coverage of clusters
    - Identified overlaps between related CWEs
    - Notes and recommendations for restructuring CWE
  - Elements of SFPs (indicators, conditions, etc.)
  - References to shared software elements in each SFP
    - This allows for full definition of the context of a faulty computation
    - This formalizes the relations between the clusters

Contractual Formalization in SBVR

OS Command Injection

CWE ID: 78

Description: A software system that **accepts and executes input in the form of operating system commands** (e.g. system(), exec(), open()) could allow an attacker with lesser privileges than the target software to execute commands with the elevated privileges of the executing process.

Captures & rationalizes original vocabulary

OS Command Injection Contractual Formal Definition:

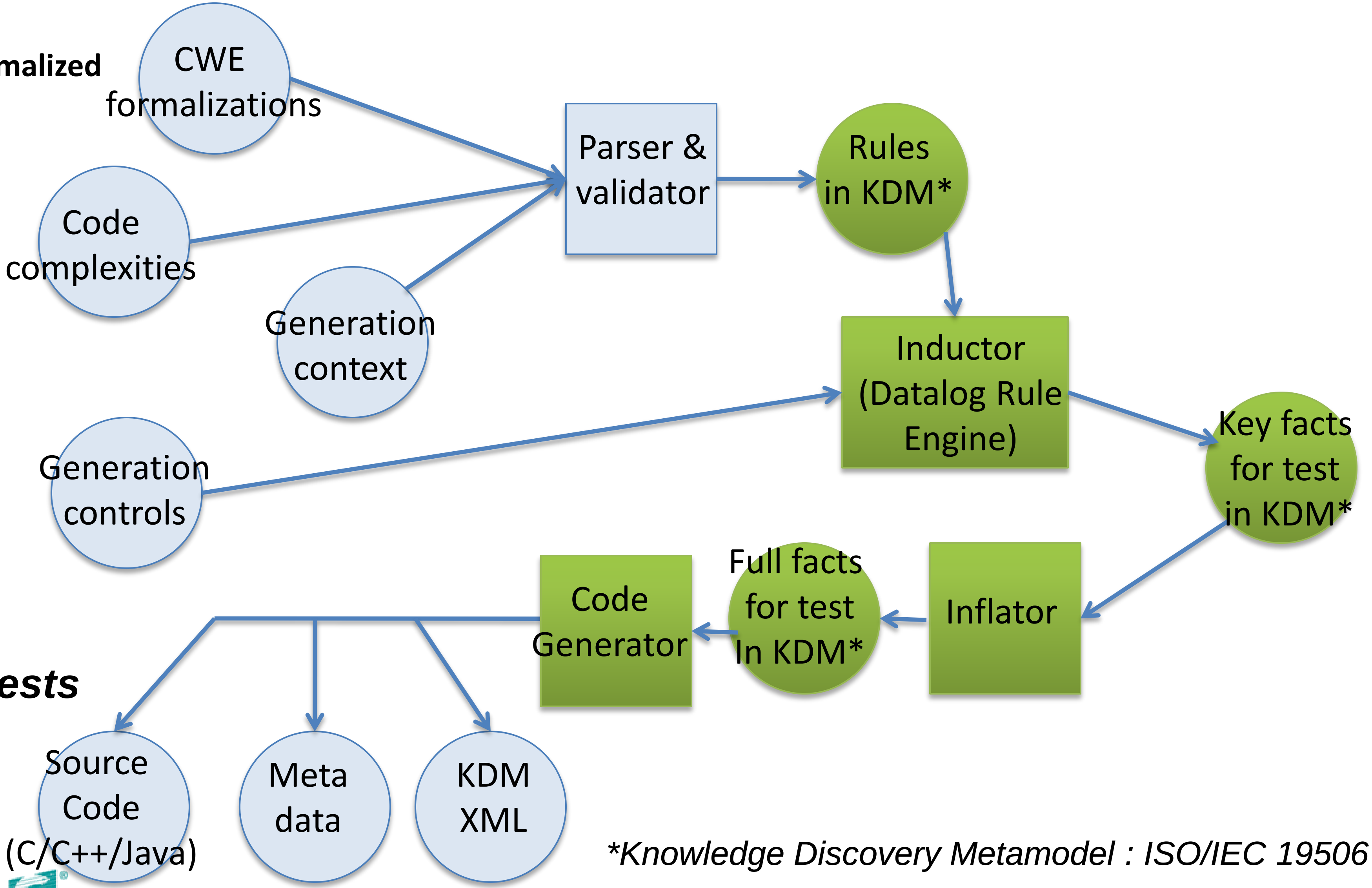
OS Command Injection weakness is a weakness where the start statement of the code path *accepts* input and the end statement of the code path *performs an* operating system command where the input *is part of* the operating system command and the input *contains command syntax*.

Formal contractual definition is further reviewed and agreed upon by the stakeholders

Good approach but high cost for 632 CWEs and still does not guaranty systematic and comprehensive coverage of weakness space

KDM Analytics' Test Case Generator

27 Formalized CWEs



~4 M tests

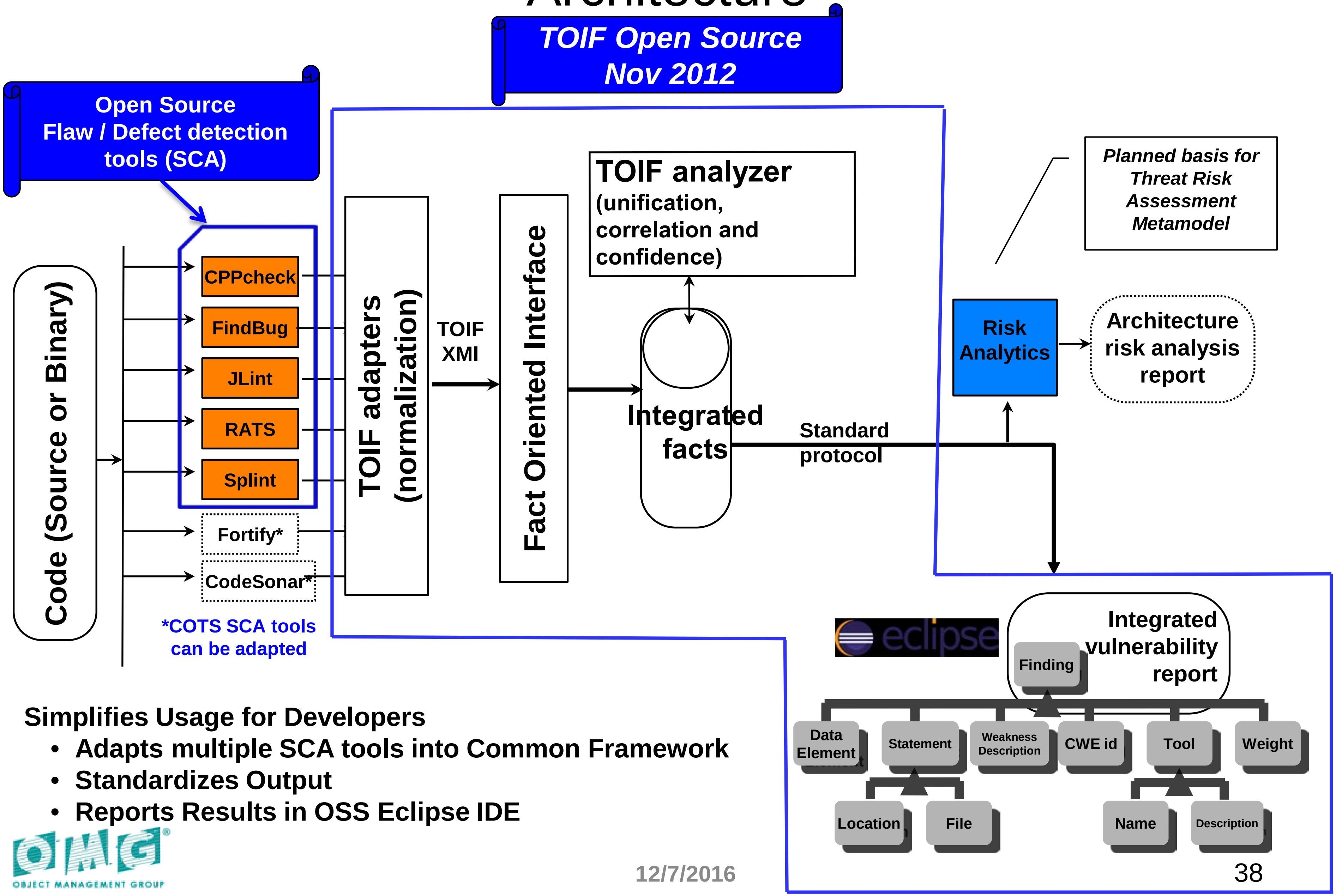
**Knowledge Discovery Metamodel : ISO/IEC 19506*

OMG TOOL OUTPUT INTEGRATION FRAMEWORK (TOIF)

Tool Output Integration Framework

- **Tool Output Integration Framework (TOIF) initially developed in 2012 (Released as Open Source)**
  - **Funded by DHS SBIR program - SBIR Topic Number: H-SB09.2-004 Software Testing and Vulnerability Analysis. (Data Access Technologies and KDM Analytics)**
- **TOIF is an extensible open source software flaw detection Framework.**
  - **Integrates multiple static code analysis tools as “data feeds” into the repository**
    - **Open source machinery: adaptors to 5 open source tools, merger, viewer, repository**
    - **Users can integrate additional Commercial and OSS SCA tools**
  - **Collates findings from several tools (Uses Existing Standards)**
    - **OMG Knowledge Discovery Metamodel (KDM), also ISO/IEC 19506**
    - **Standardizes outputs of various tools for uniform review of information**
- **Blade TOIF is enhanced tool executing entirely inside of Eclipse.**

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

DOMAIN SPECIFIC ASSURANCE STANDARD

Dependability Assurance Framework For Safety-Sensitive Consumer Devices

Dr. Kenji Taguchi, AIST
Mr. Isashi Uchida, IPA
Mr. Hiroyuki Haruyama, IPA
Mr. Hiroshi Miyazaki, Fujitsu
Mr. Satoru Watanabe, TOYOTA
Dr. Naoya Ishizaki, TOYOTA
Dr. Yutaka Matsuno, U of Electro-Communications

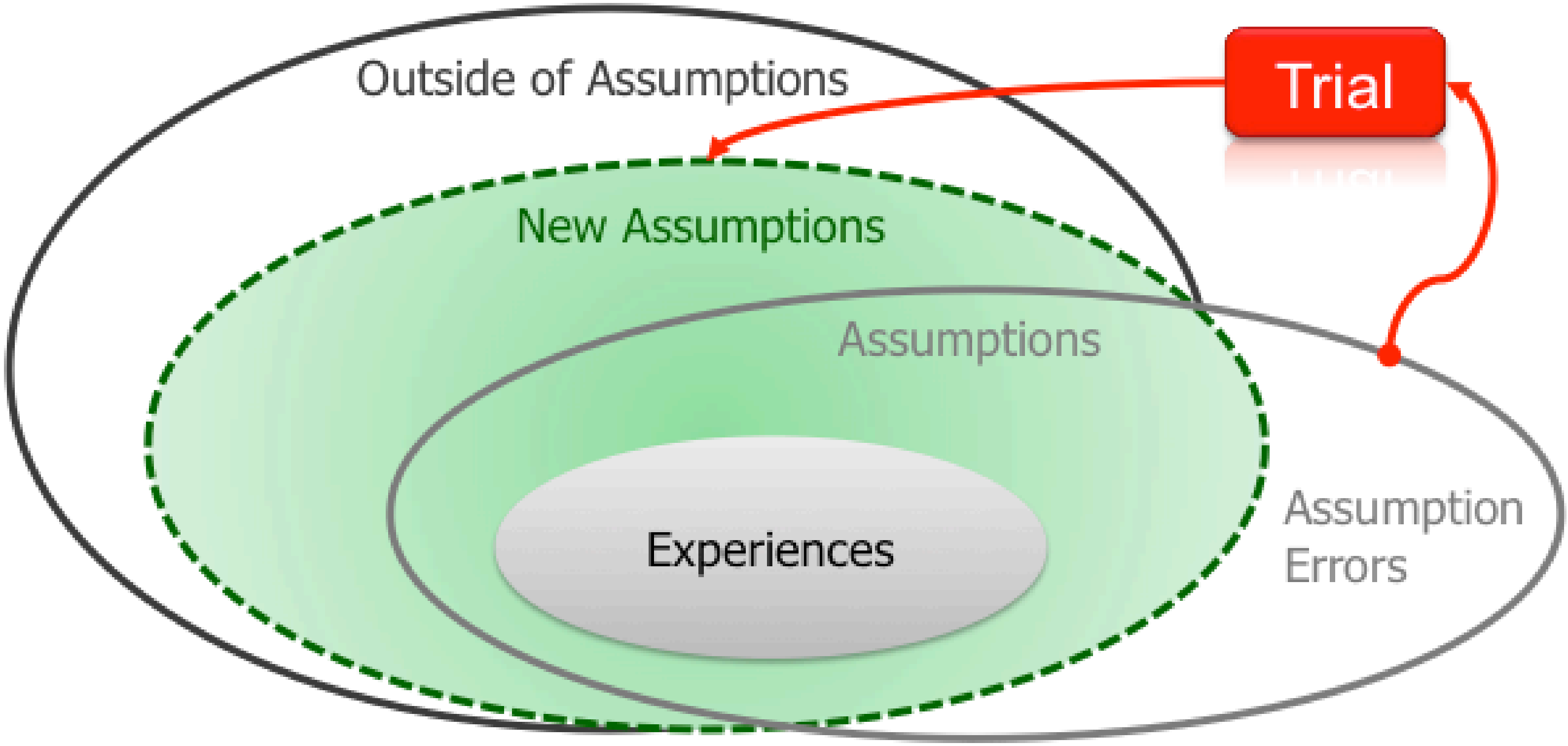
What are Consumer Devices?

	Factory machineries 	Consumer devices
The number of the production	A few to Many	A huge number
Users	Experts	General users
Cost	High	Sufficiently low
Maintenance	Real field (strongly managed)	Users, Service stations (weekly managed)
Environment	Factory environment (almost stable)	Factory environment
		User environment (Open, dynamic and diverse)

Consumer devices are industrial products used by general end users such as automobiles, service robots, consumer electronics, smart houses and so on.

Fundamental Approach

◆ Need to ensure the dependability in open/diverse/dynamic env.

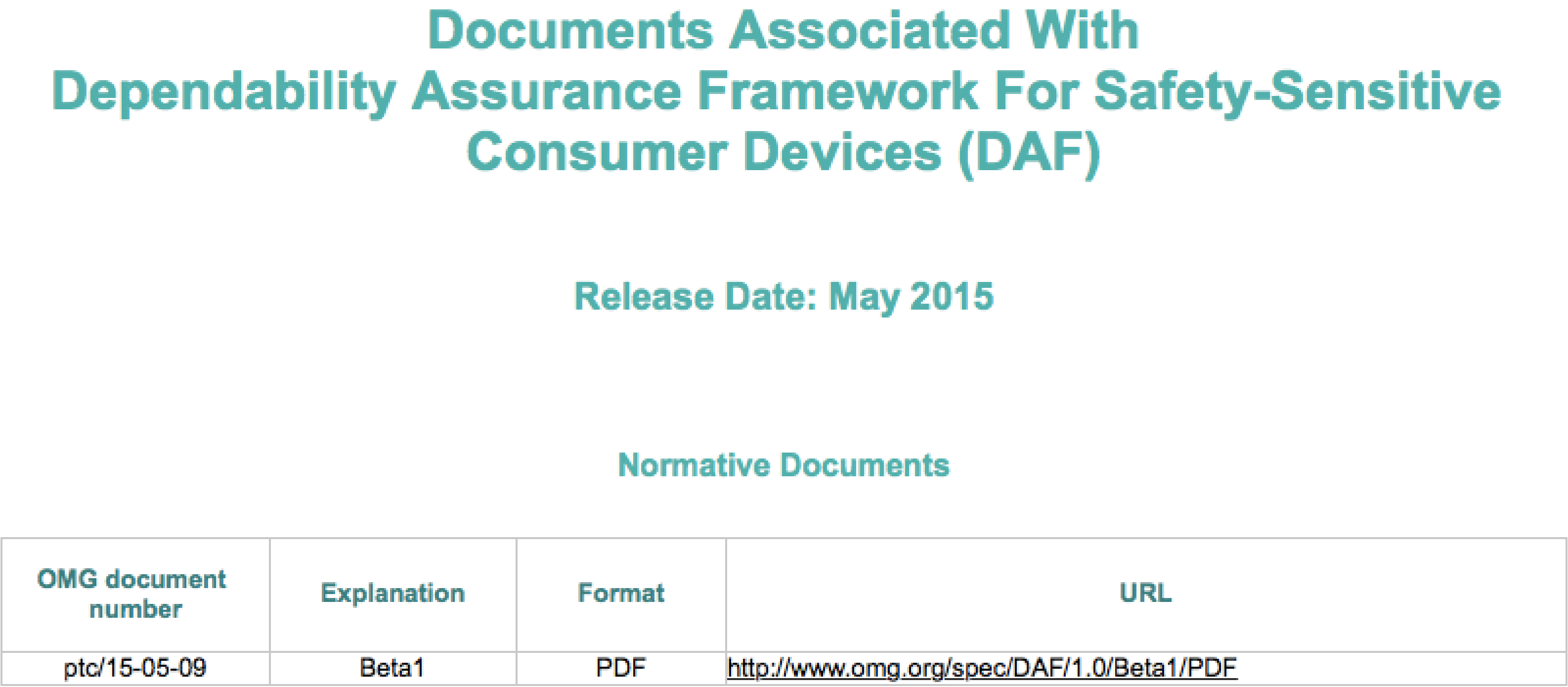


■We believe all auto companies well manage "known" factors.
■To ensure the safety and reliability (what we could call "Dependability", "unknown factors" must be well addressed.
➔ Iteration is fundamental approach to explore/find out unknown factors.

Key Capabilities of DAF

- Umbrella Standard for Safety, Reliability, Maintainability, …
  - DCM: Dependability Concept Model
- DAC Template: Template for dependability argumentation
- DPM: Dependability assurance process

More Information on DAF Standard



Documents Associated With Dependability Assurance Framework For Safety-Sensitive Consumer Devices (DAF)

Release Date: May 2015

Normative Documents

OMG document number	Explanation	Format	URL
ptc/15-05-09	Beta1	PDF	http://www.omg.org/spec/DAF/1.0/Beta1/PDF

Dr. Ben Calloni, PE, CISSP, OCRES

LM Fellow Embedded Cybersecurity

ben.a.calloni@lmco.com

THANK YOU

Questions?

TARGET
DATA
Then he slithered and slunk,
with a smile most unpleasant,
and he took the identities
that they'd used to buy presents.
Bish.
TRIBUNE-REVIEW
APOLOGIES TO SEUSS AND JONES