System Assurance and Related Standards

Dr. Ben Calloni, P.E., CISSP, OCRES
Lockheed Martin Fellow, Cybersecurity

- Lockheed Martin Representative to OMG
  - OMG Board of Directors
  - Co-chair OMG System Assurance Task Force

Acknowledgments

- Djenana Campara, KDM Analytics CEO
  - Co-chair System Assurance Task Force
  - OMG BoD
- Dr. Kenji Taguchi, AIST
  - Co-chair System Assurance Task Force
- 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
  - Dependability Assurance Framework

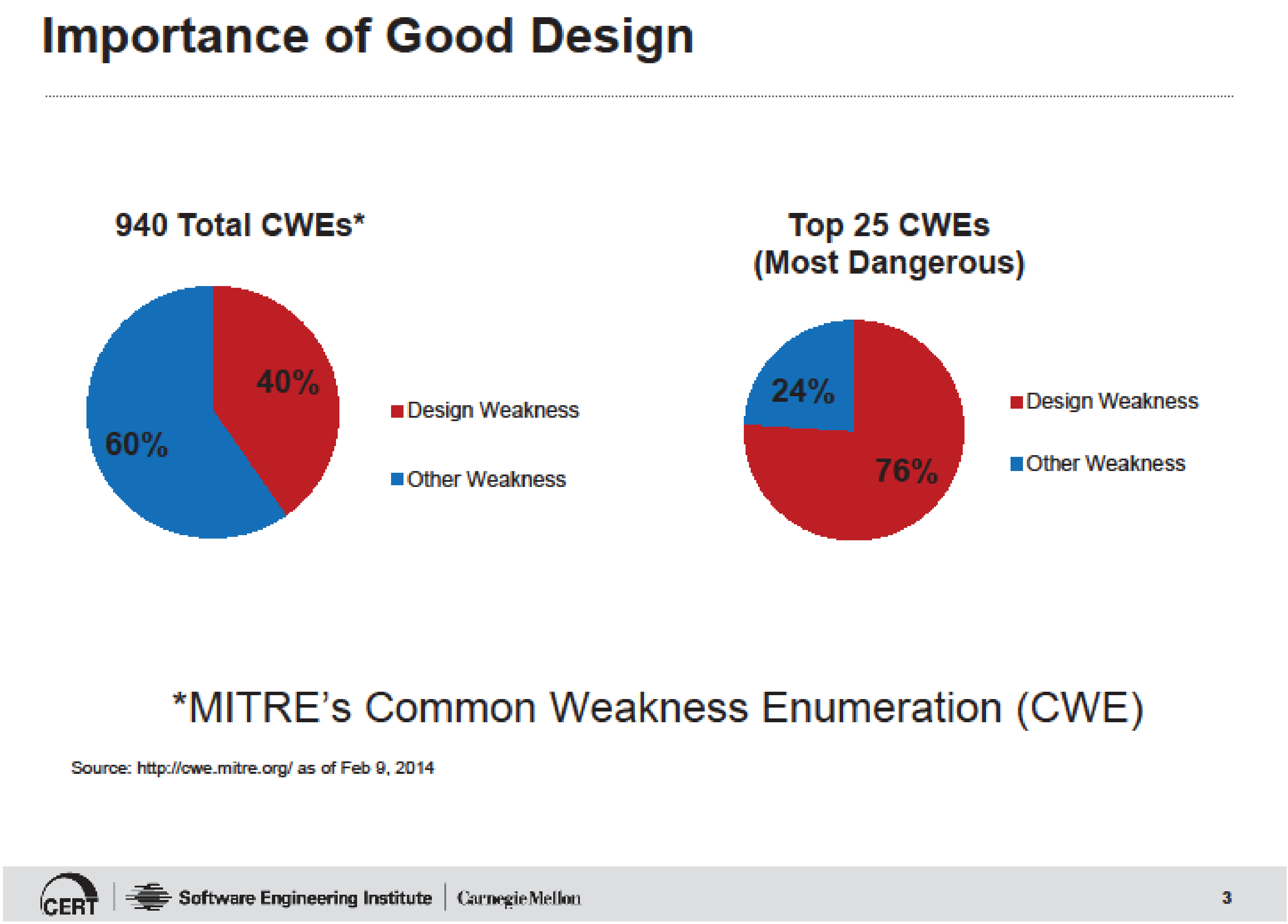
OMG System Assurance Task Force (SysA TF)

- 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

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



Importance of Good Design

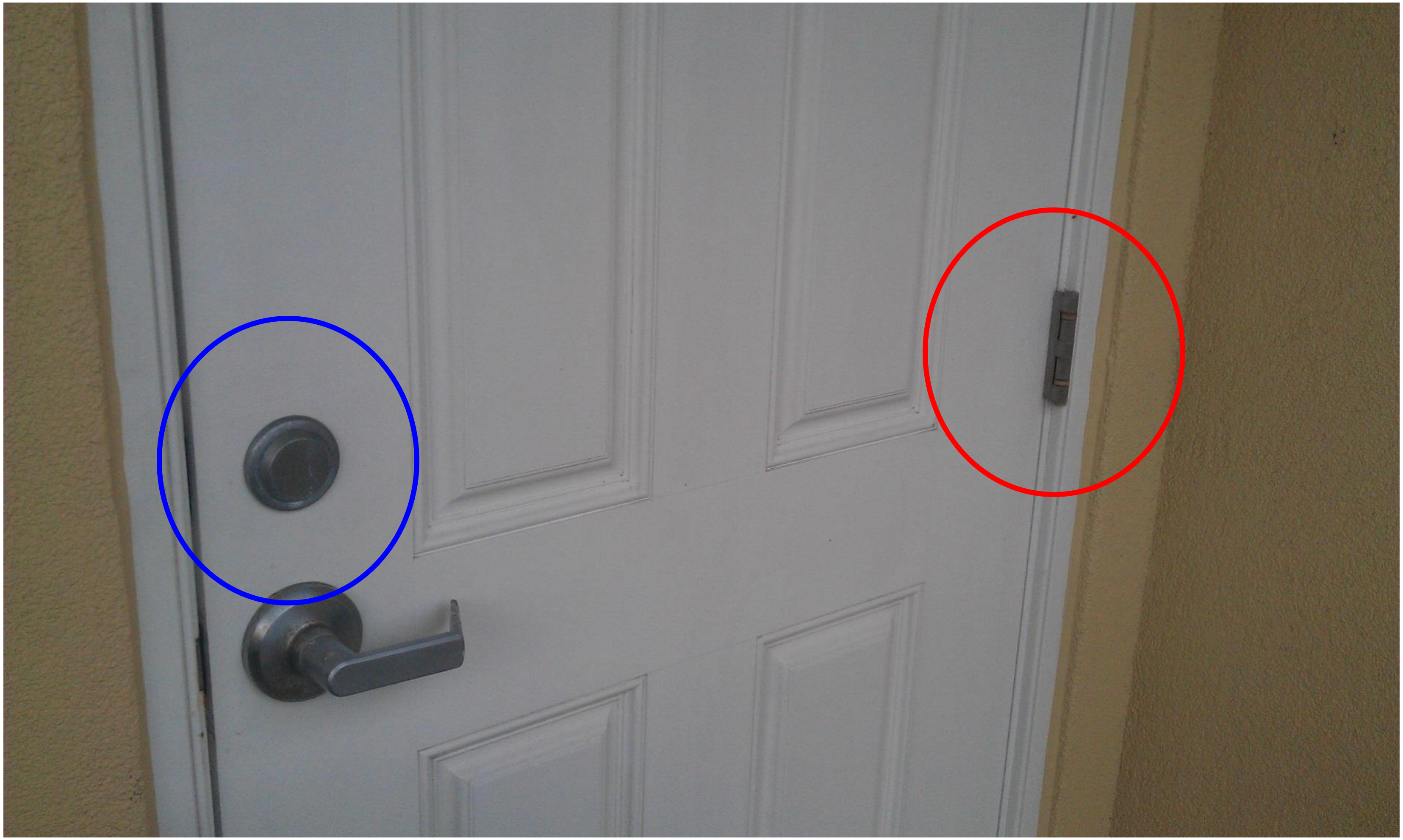
940 Total CWEs*

Top 25 CWEs (Most Dangerous)

*MITRE's Common Weakness Enumeration (CWE)

Source: http://cwe.mitre.org/ as of Feb 9, 2014

Security Features != Security Features



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

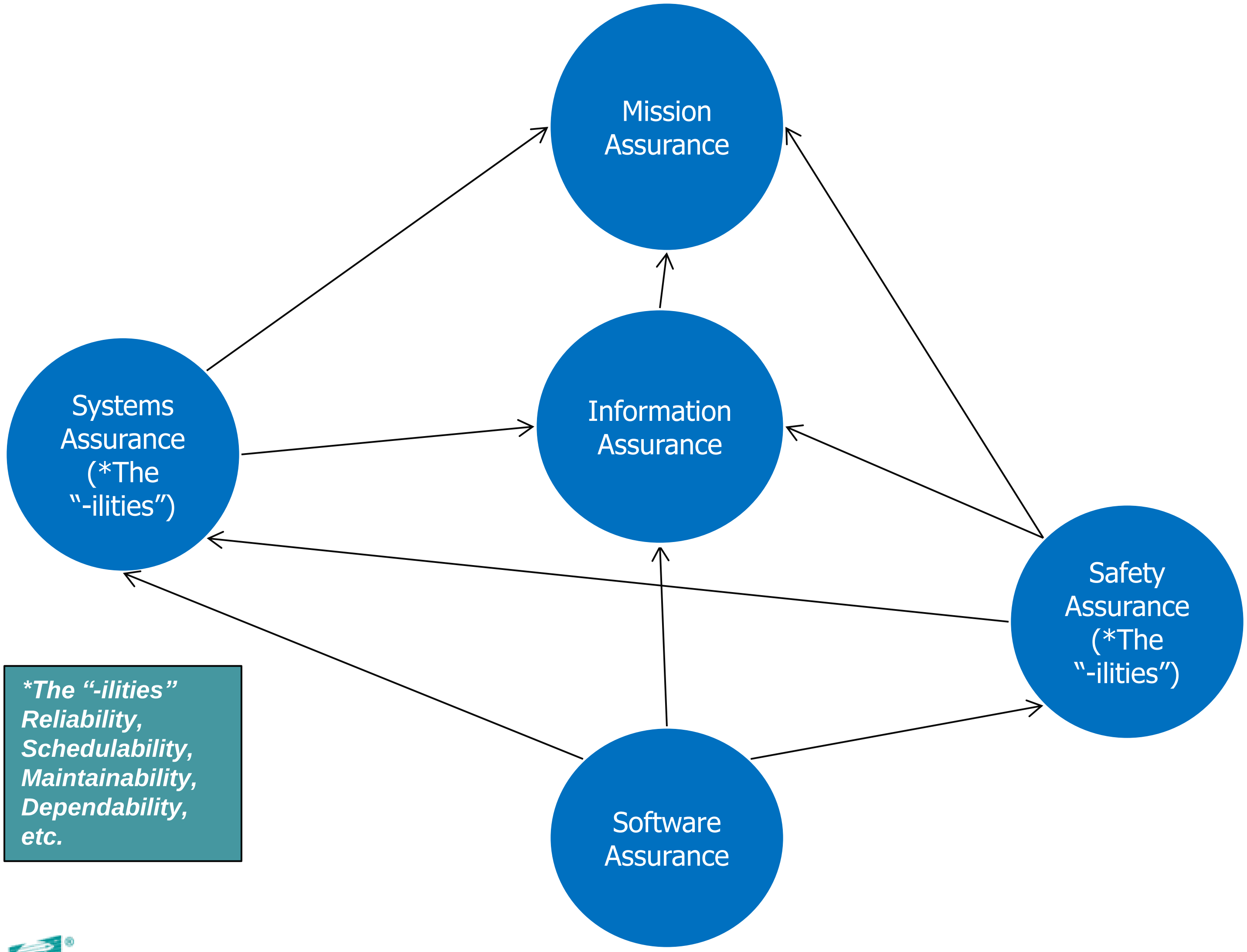
- **Software Assurance (SwA)** is the justified **confidence** that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during the life cycle. - CNSS 4009 IA Glossary

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*
- **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

Information Assurance

Systems Assurance (*The "-ilities")

Safety Assurance (*The "-ilities")

Software Assurance

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

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

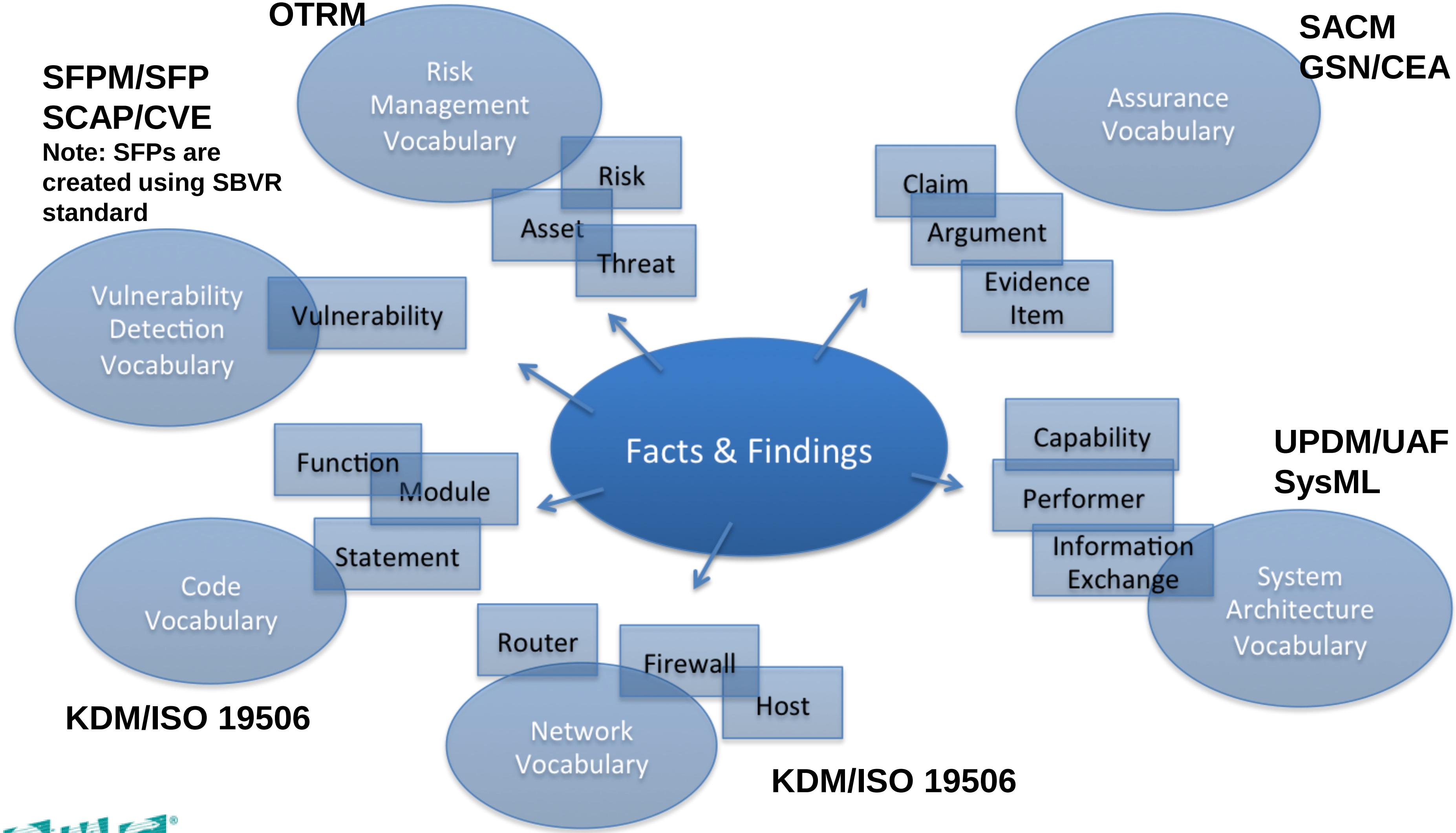
Addressing Challenges: OMG Software/System Assurance Ecosystem

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 UML Profile for DODAF/MODAF (UPDM) / UAF
  - Formally representing DoDAF & MODAF information
- 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
- NIST Security Automation Protocol (SCAP)

Ecosystem Foundation: Common Fact Model

Data Fusion & Semantic Integration



OTRM

Risk Management Vocabulary

Risk

Asset

Threat

SFPM/SFP
SCAP/CVE
Note: SFPs are created using SBVR standard

Vulnerability Detection Vocabulary

Vulnerability

SACM
GSN/CEA

Assurance Vocabulary

Claim

Argument

Evidence Item

Facts & Findings

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

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 Acceptable”

Utilization of Assurance Modeling Tools

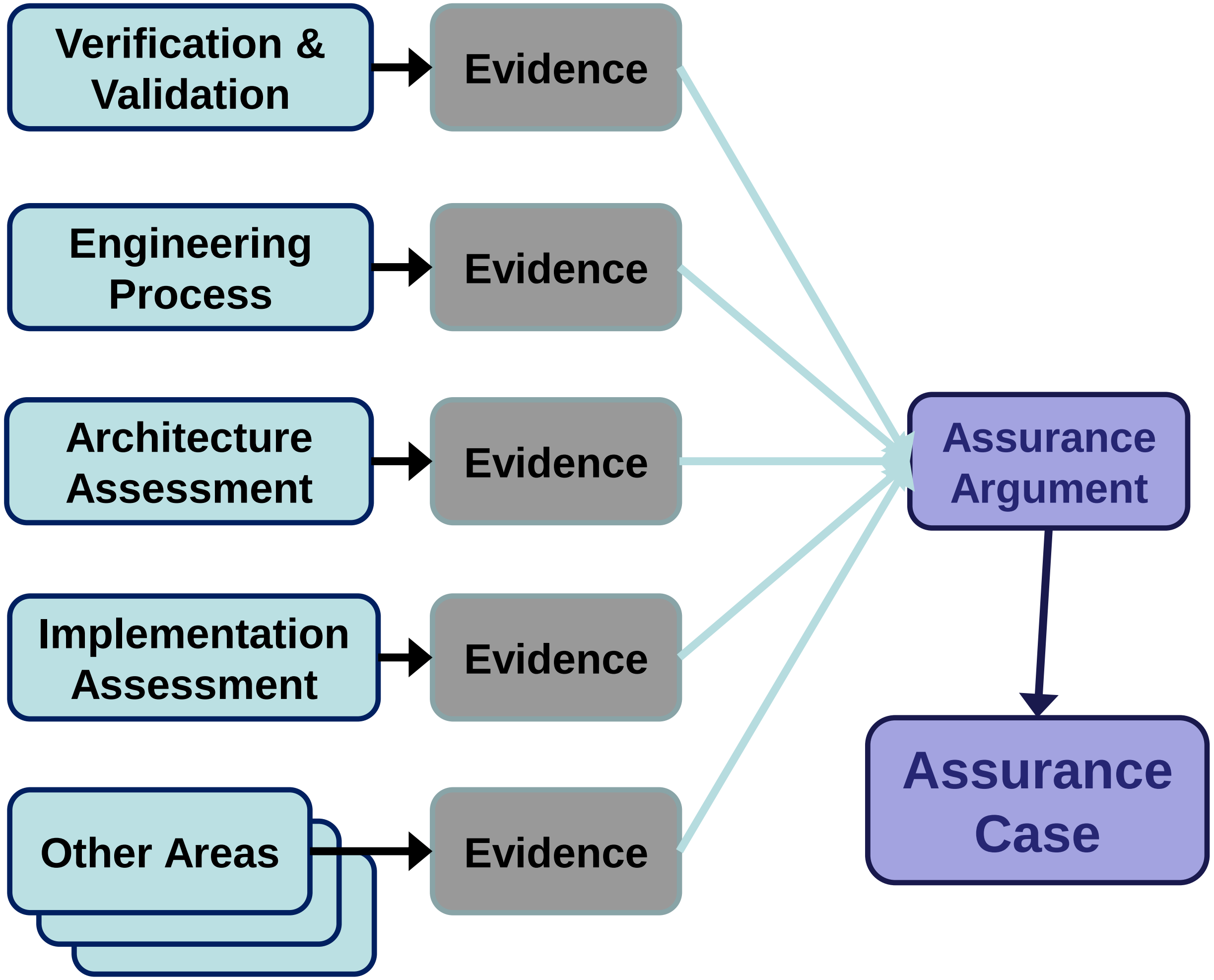
ESTABLISHING ASSURANCE

System Assurance Reduces 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

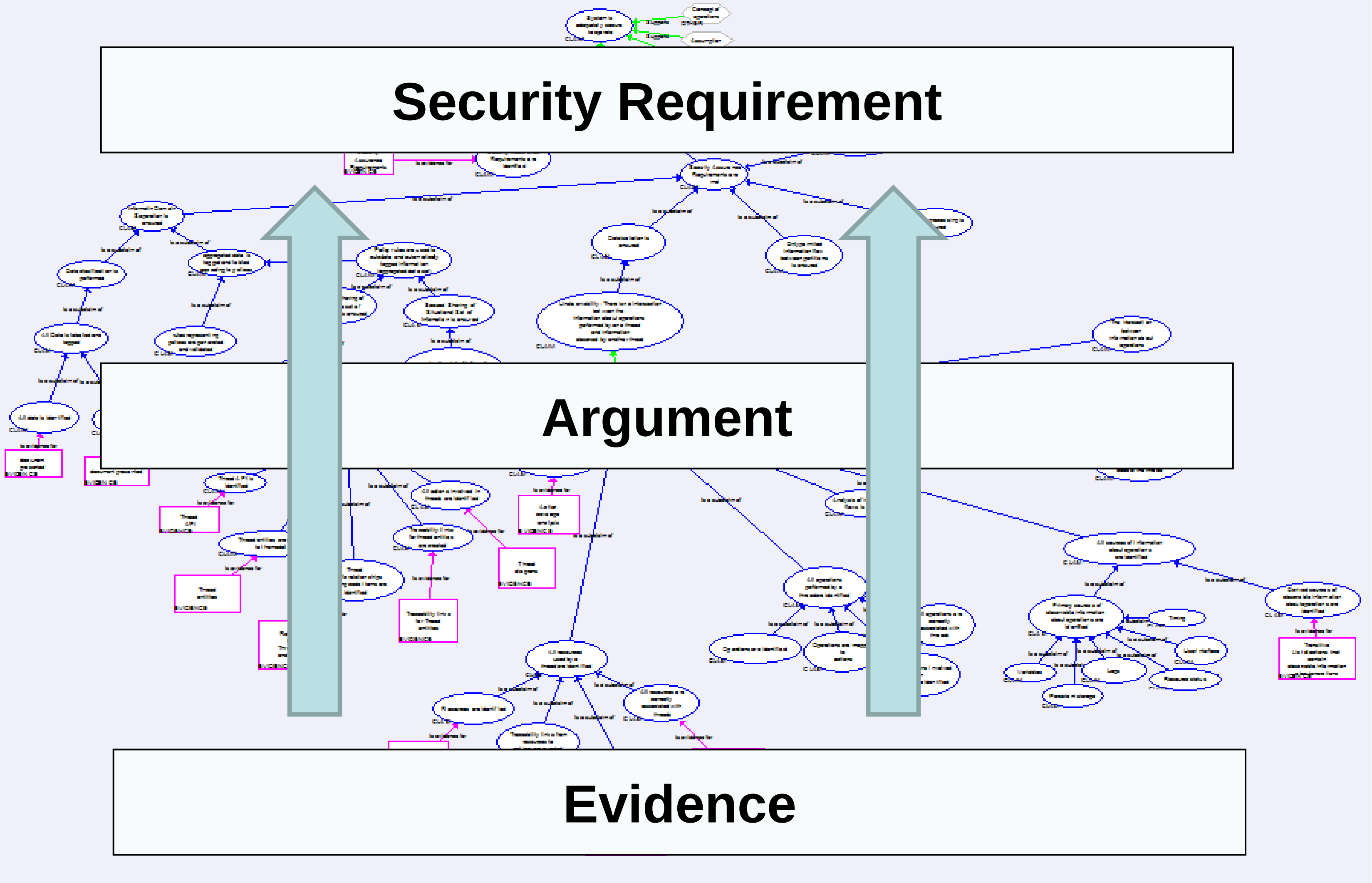
The result of System Assurance is justified **confidence** delivered in the form of an **Assurance Case**



TYPES OF EVIDENCE FOR AN ASSURANCE CASE

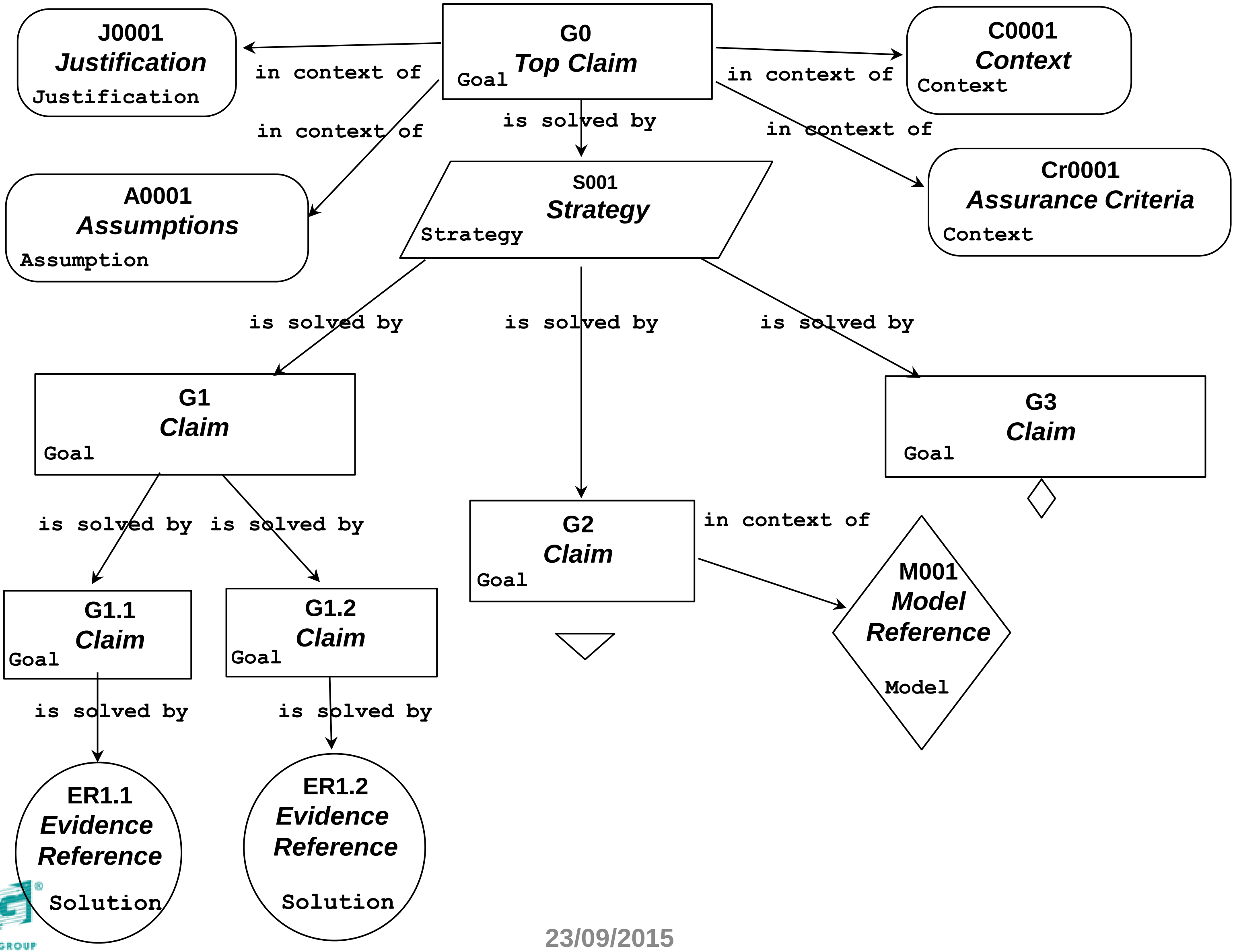
Confidence demands objectivity, scientific method and cost-effectiveness

Sample of Assurance Case

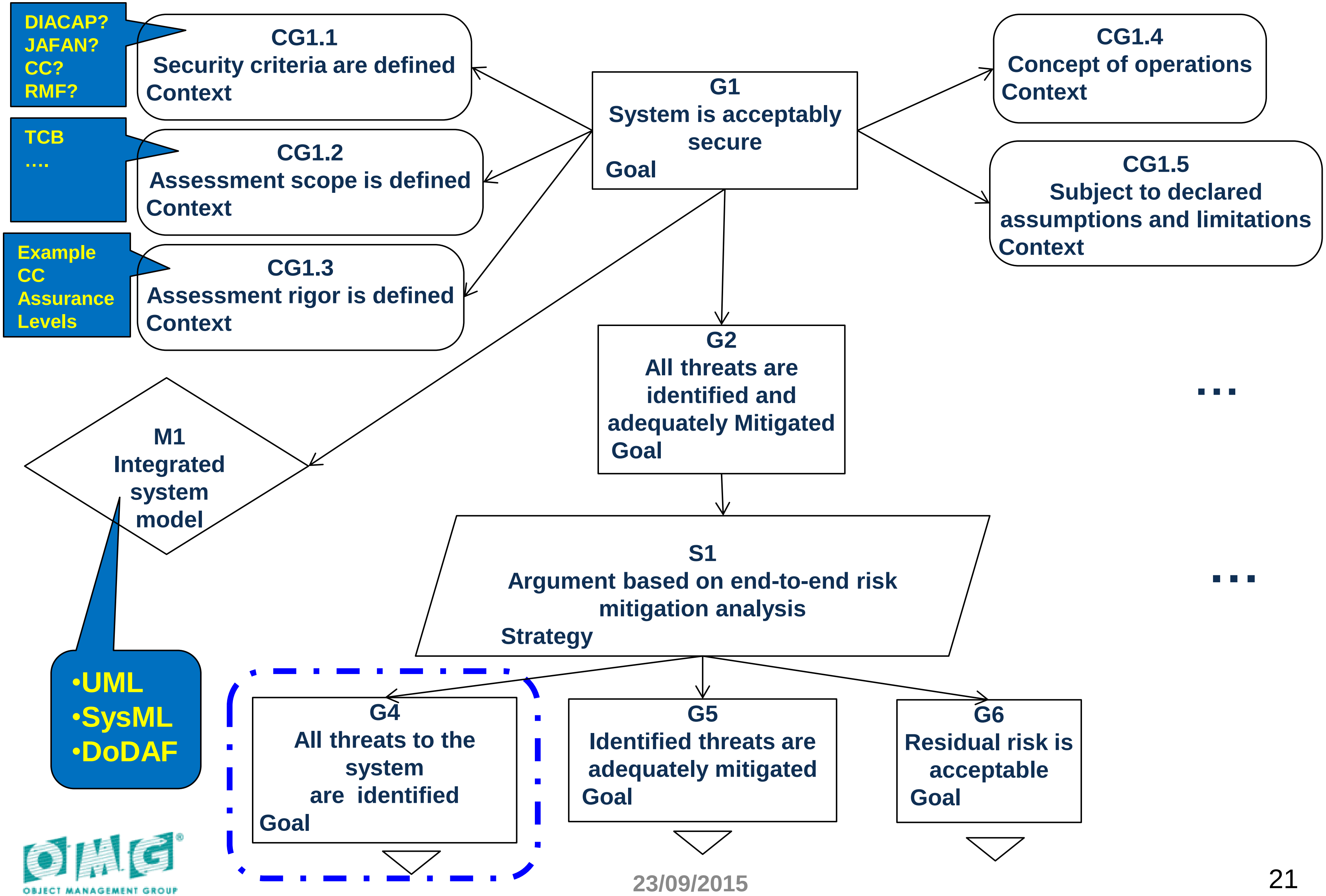


OMG STRUCTURED ASSURANCE CASE METAMODEL (SACM)

OMG’s Structured Assurance Case Metamodel



Establishing the Security Assurance Case



DIACAP?
JAFAN?
CC?
RMF?

CG1.1
Security criteria are defined
Context

TCB
….

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

…

M1
Integrated system model

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

…

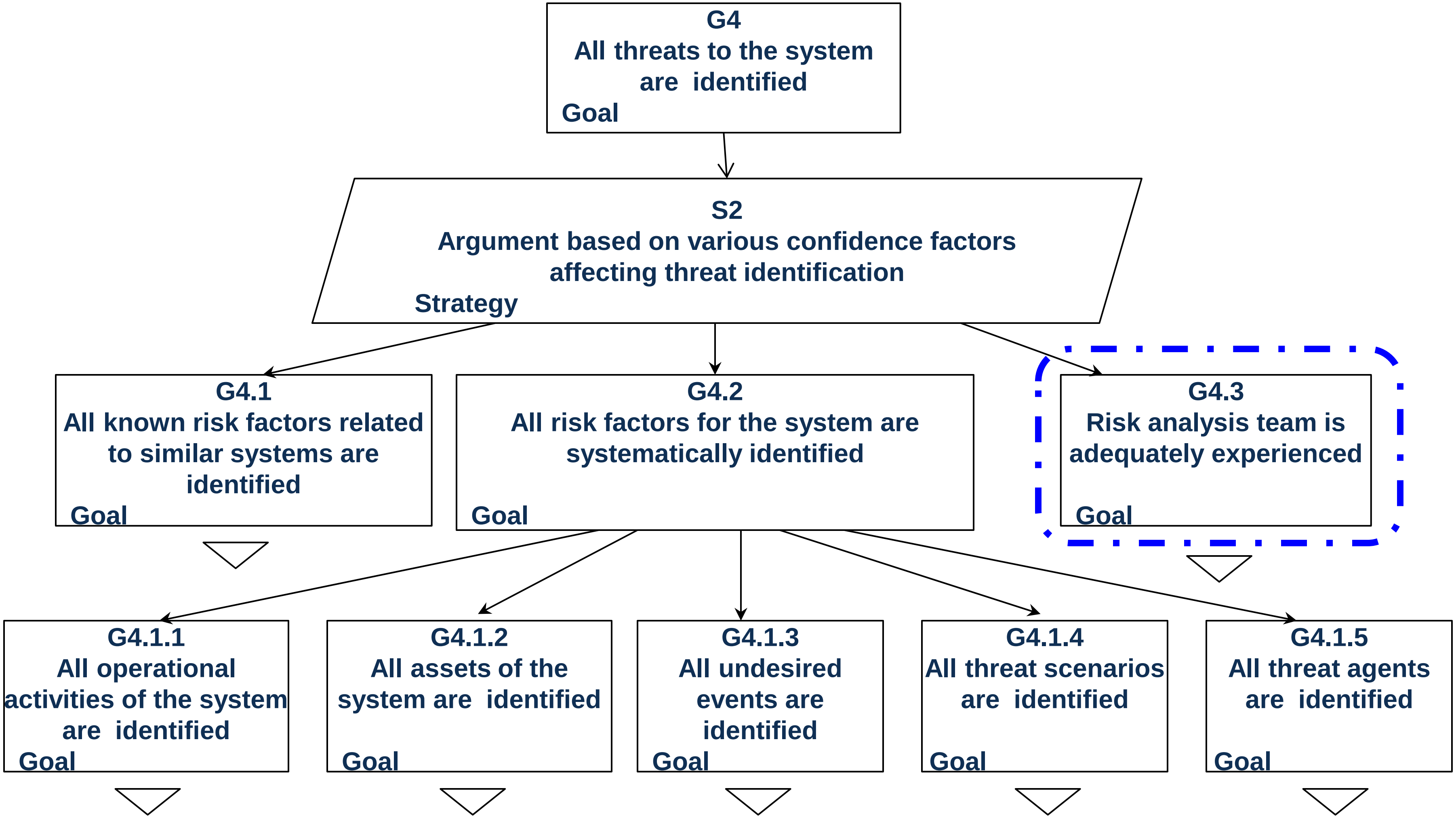
- UML
- SysML
- DoDAF

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

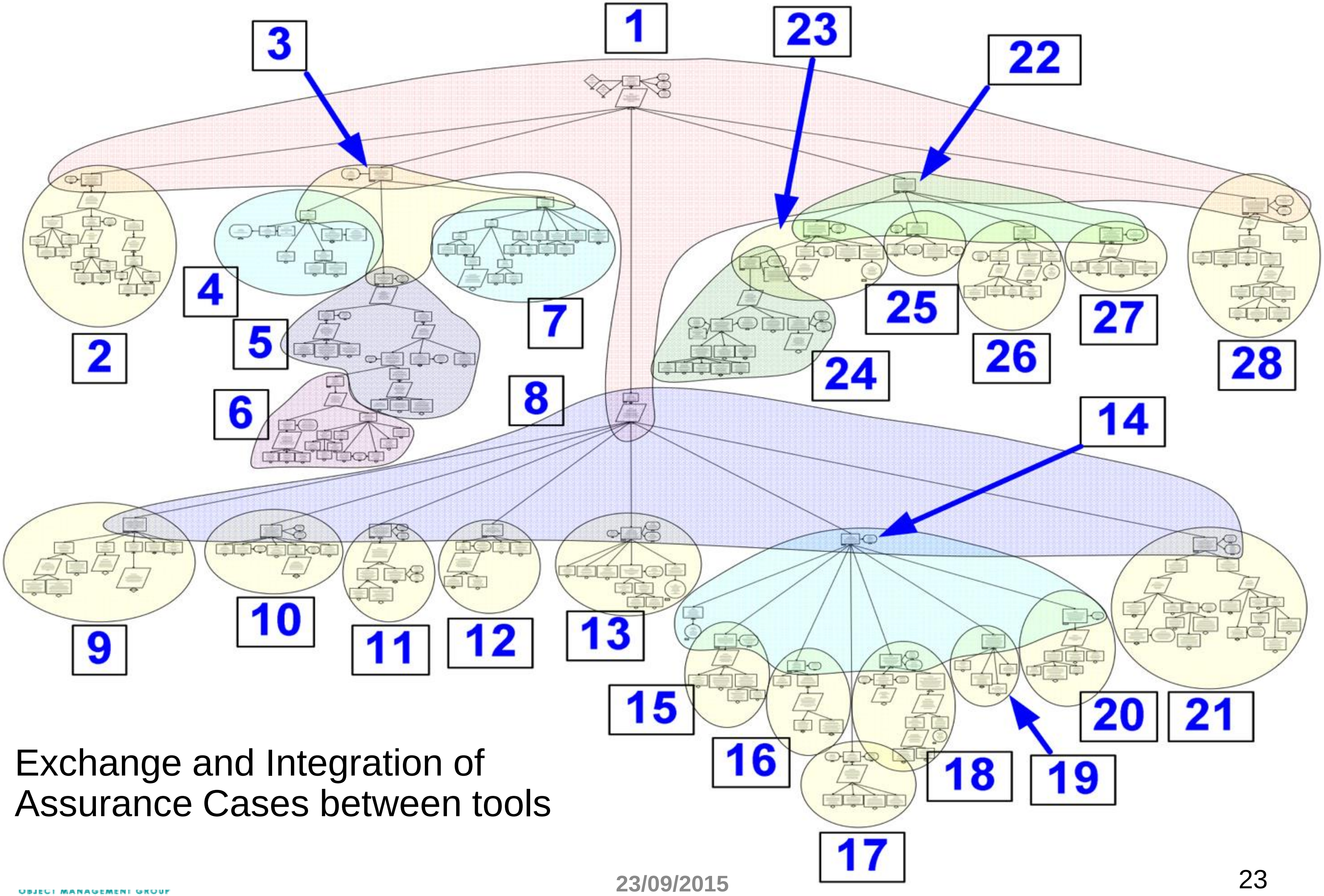
G4.1.3
All undesired events are identified
Goal

G4.1.4
All threat scenarios are identified
Goal

G4.1.5
All threat agents are identified
Goal

23/09/2015

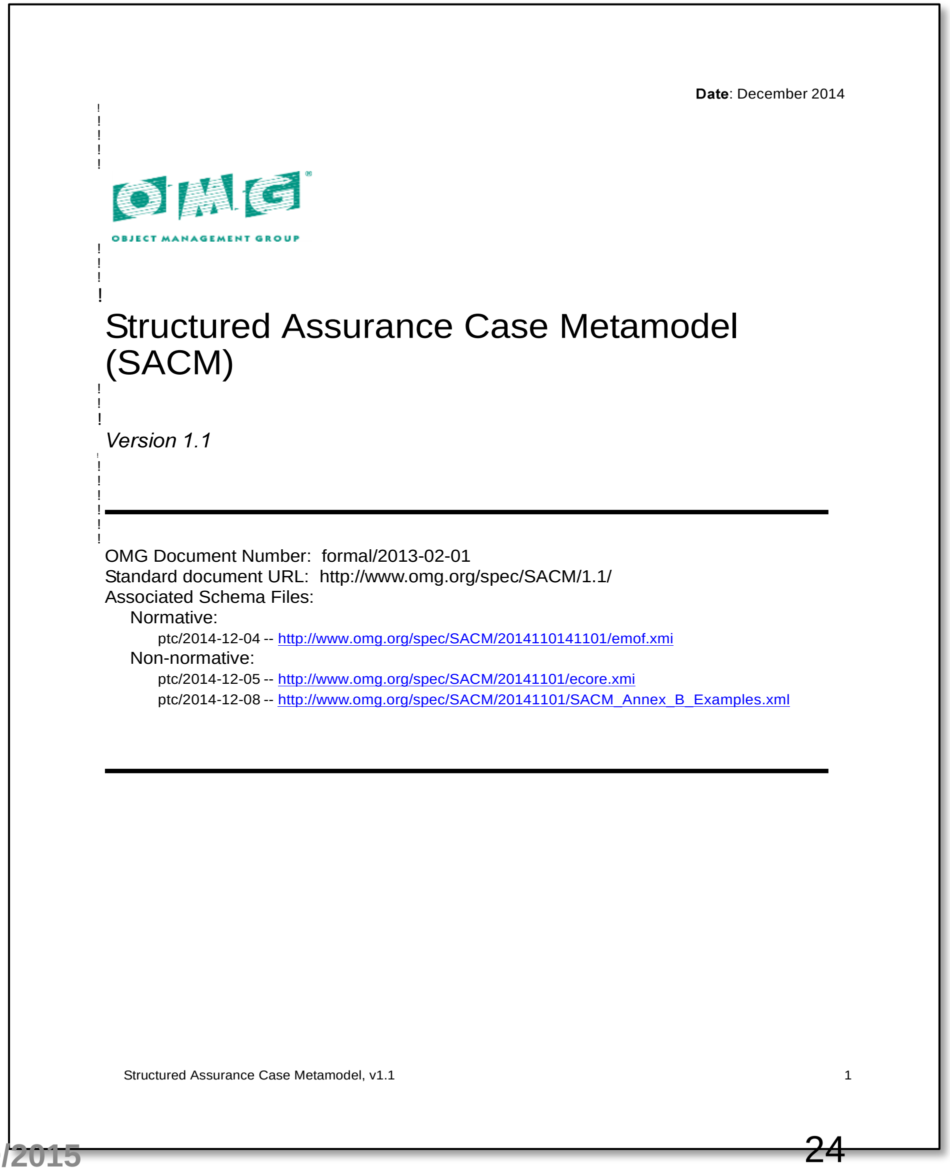
OMG’s Structured Assurance Case Metamodel (SACM)



Exchange and Integration of Assurance Cases between tools

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/2014110141101/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

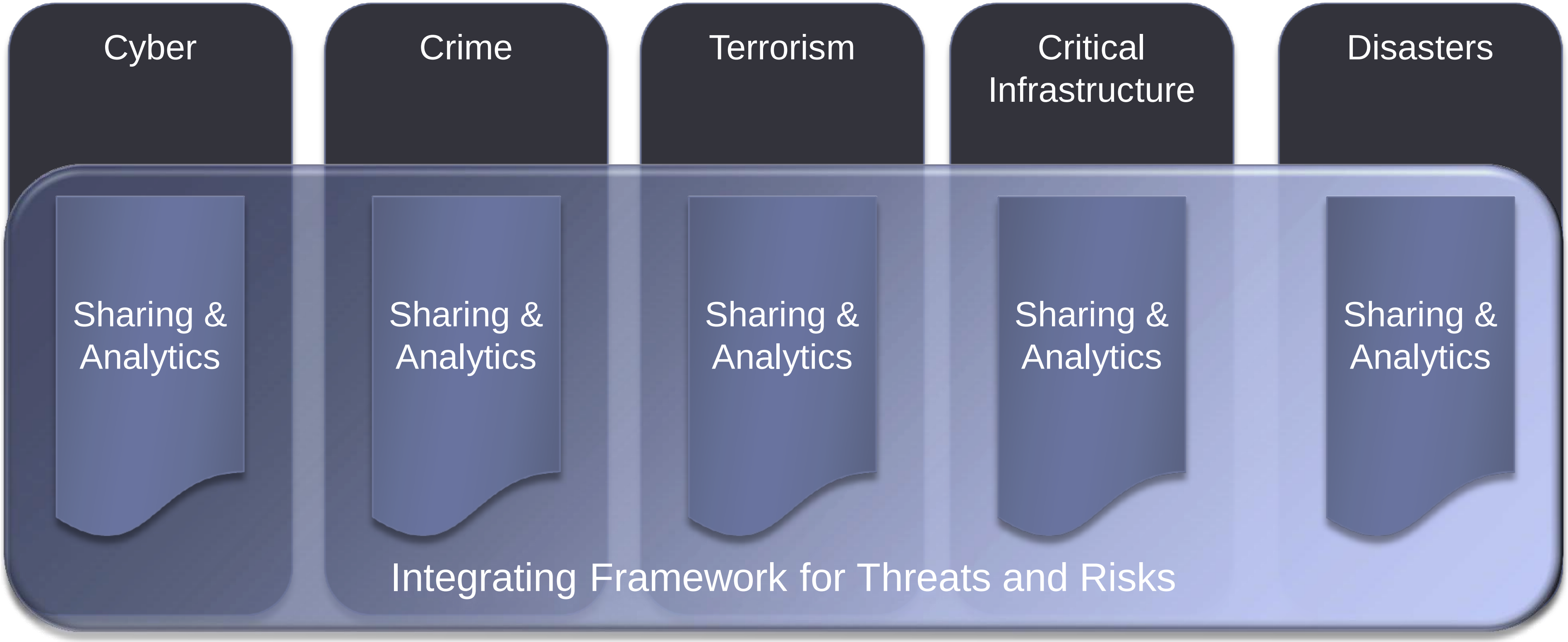
THREAT RISK SHARING AND ANALYTICS

Objective of RFP

- This RFP calls for
  - a conceptual model for operational threats and risks
  - unifies the semantics
  - provides a bridge across multiple threat / risk schema and interfaces.
- The conceptual model will be
  - informed by high-level concepts as defined by the Cyber domain,
  - existing NIEM domains and
  - other applicable domains, but is not specific to those domains.

Enables combined Cyber, physical, criminal/natural threats, and risks to be federated, understood and responded to effectively.

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)

What is Software Fault Pattern (SFP)?

- SFP'is'a'generalized'descrip0on'of'a'*family* of' computa0ons'with'a'certain'common'[illegible]
  - provides'a'jus0fiable'taxonomy'of'[illegible]s
  - focuses'at'recognizable'*risk indicators* (things'that'are'discernable'in'the' code)'
  - focuses'at'invariant'*patterns*'and'their'*parameters*'[illegible]
  - as'comprehensive'*machine-consumable content*

- 'this'approach'introduces'a'common'methodology'and a common'vocabulary'leading'to' crea0on'of'common'interTexchangeable'machineTconsumable'content'to'improve'system' assurance'
  - 'including'be[er'vulnerability'detec0on'tools'
  - 'risk'analysis'tools'
  - 'system'assessment'tools'

Buffer Overflow, Stack Smashing, Heap Overflow are all Memory Mismanagement!

Overview of the SFP Metamodel

- SFP Metamodel (SFPM) defines the technical elements involved in a definition of a faulty computation
  - Structural elements of a catalog
  - Identified parameters for each SFP
  - Linkage to CWE catalog
  - Elements of SFPs (indicators, conditions, etc.)
  - References to shared software elements in each SFP

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 is Safety?

- Safety is freedom from accidents or losses.
  - No such thing as 100% safe, but a level of confidence that likelihood of an unsafe event is acceptably low.
- Safety is not reliability!
  - Reliability is the *(preferably high)* probability that a system will perform its intended function satisfactorily.
- Safety is not security!
  - Security is protection or defense against sentient, willful attack, interference, or espionage.

- The term dependability is used to refer to the superset of safety, reliability, and security

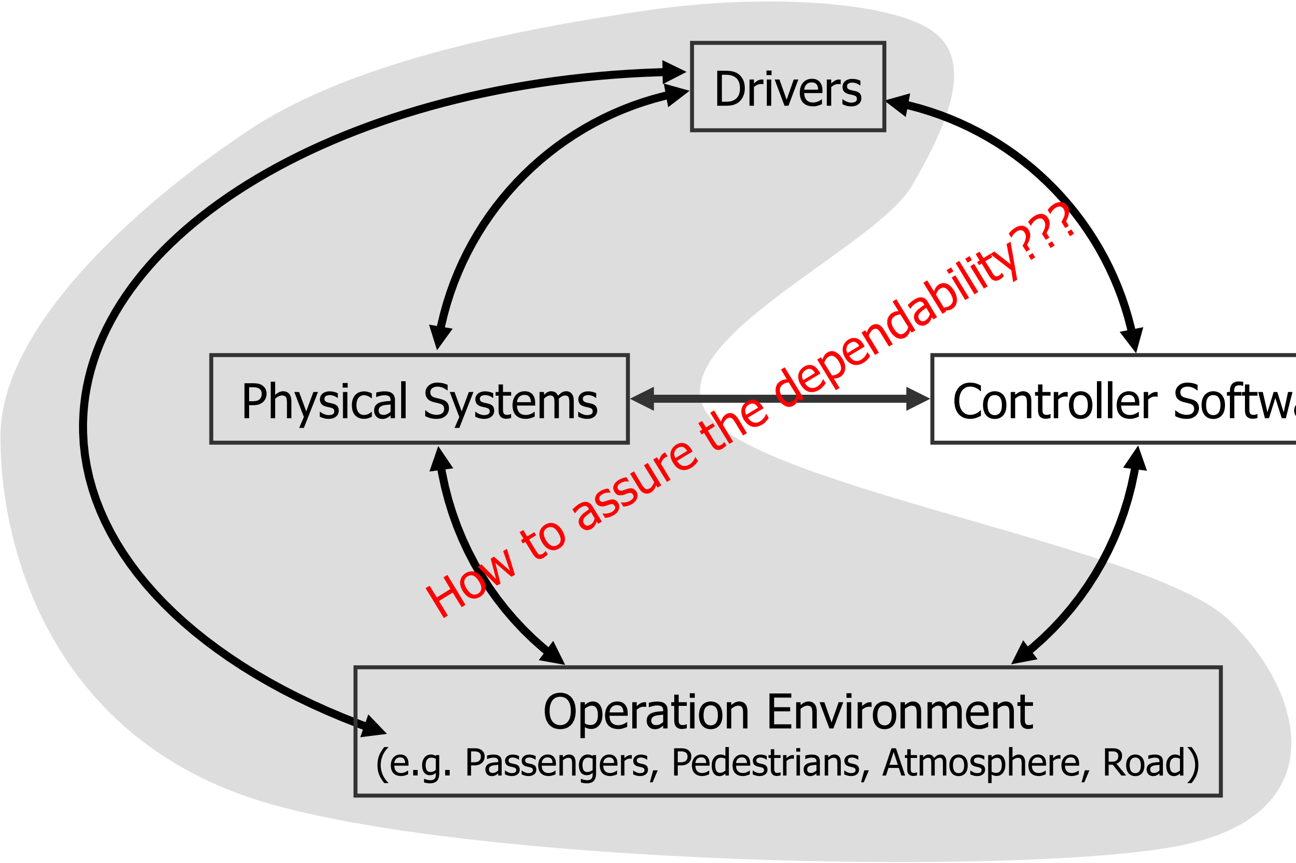
People place "trust" in a system when dependability is demonstrably acceptable!

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.

Characteristics of Consumer Devices


Drivers
Physical Systems
Controller Software
Operation Environment
(e.g. Passengers, Pedestrians, Atmosphere, Road)
How to assure the dependability???

There are frequent interactions between physical system and control software in open, diverse, and dynamic environment.

Challenges in existing standard

◇Functional Safety

■To secure Safety by measures to make risks put under less than "acceptable" rate

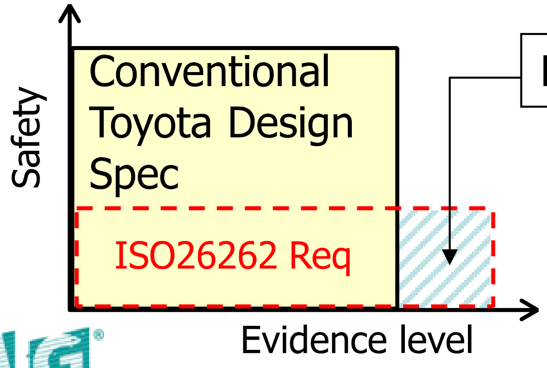
◇ISO26262

- ◆ **2011/Nov : Established and issued**
- ◆**Scope : E/E systems related to Safety only**

◇Requirements Mapping for ISO26262 and Toyota Safety/Quality

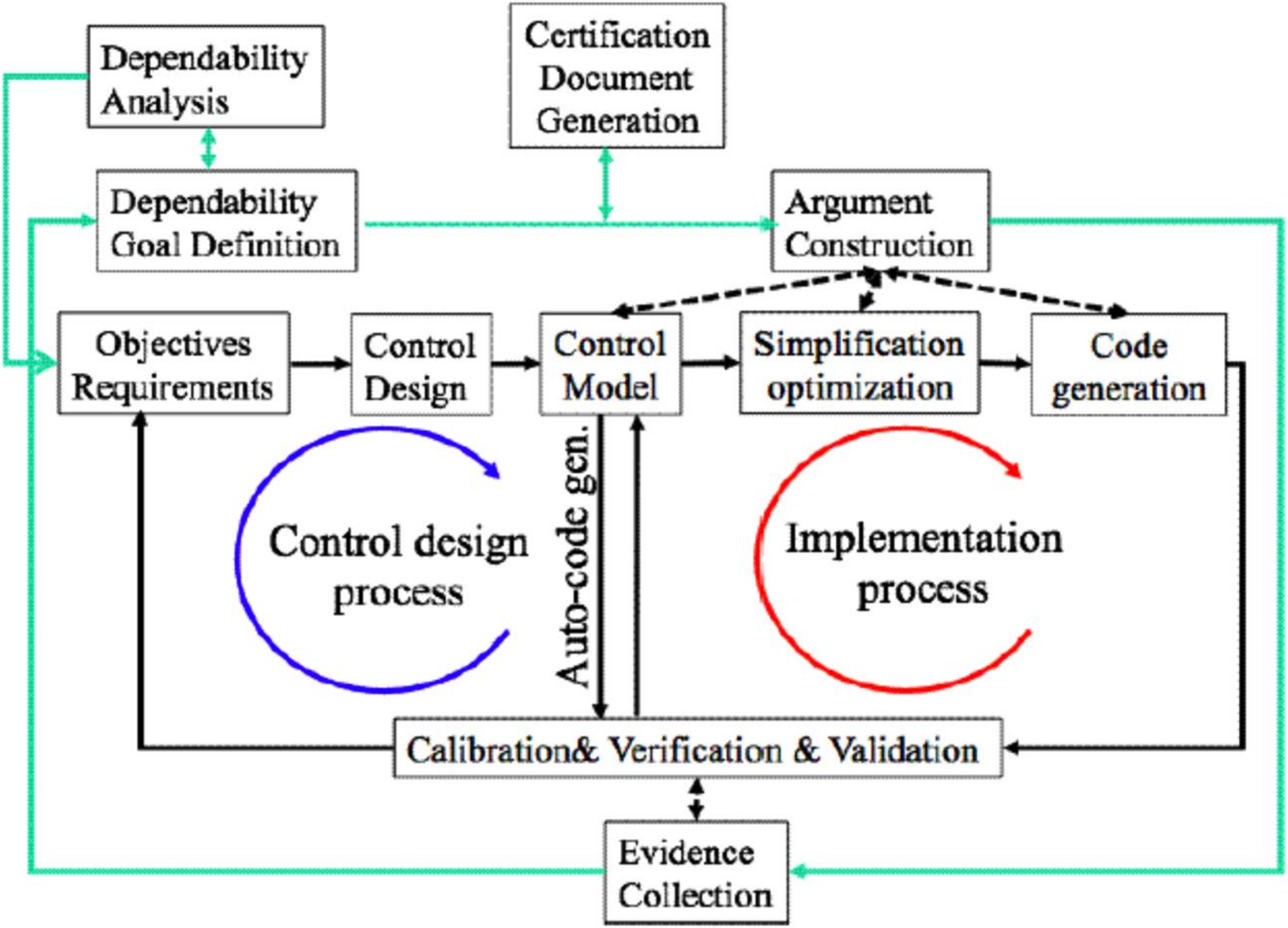
◆ ISO26262 regulates minimum safety design requirements
(ex: Engine stall is out of scope)

⇒ Need to design systems to conventional Toyota Safety/Quality standards as well.



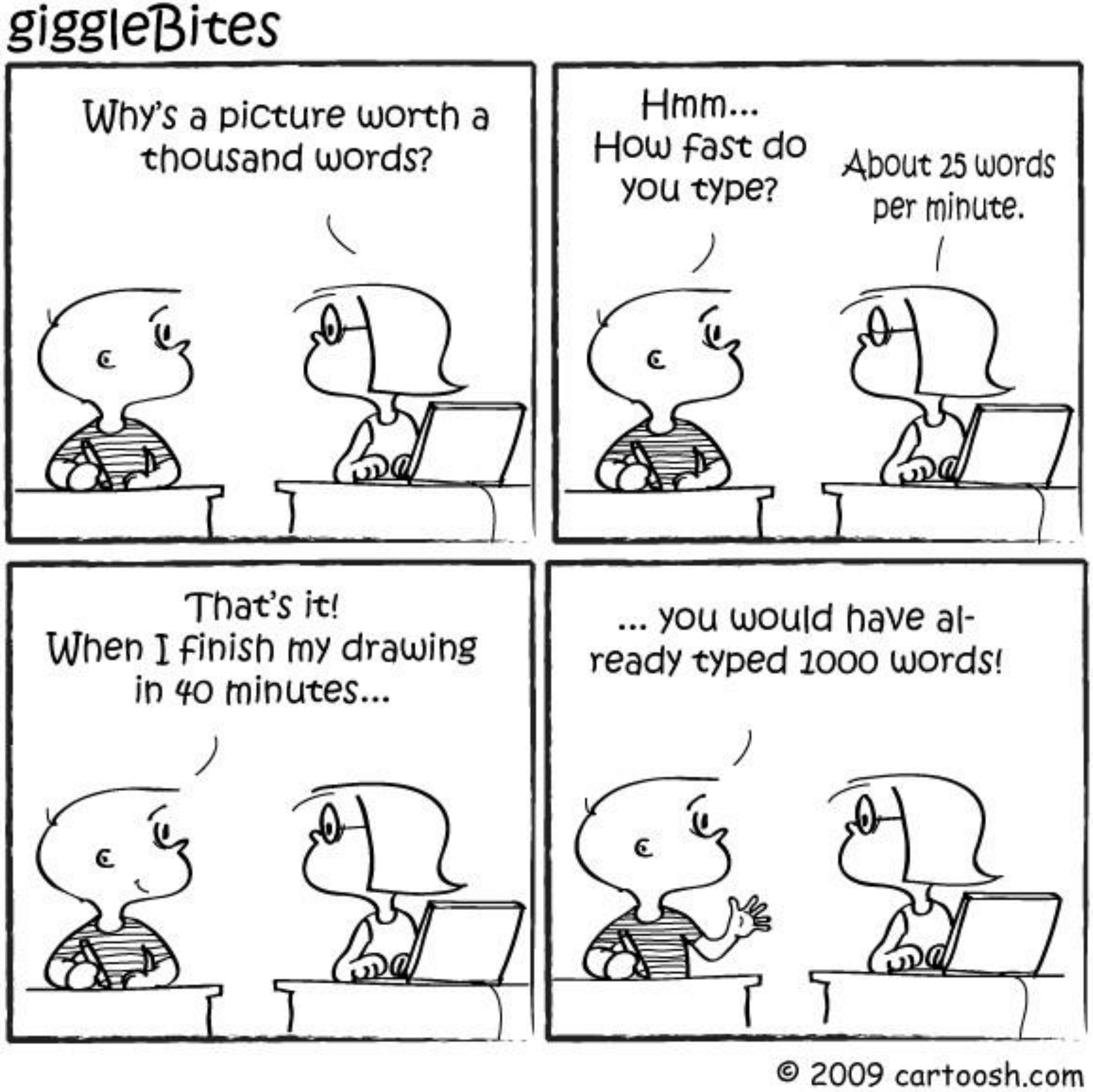
Keep evidence to prove design for accountability for others

Need to address all of Toyota safety standard together with ISO26262


Dependability Analysis
Certification Document Generation
Dependability Goal Definition
Argument Construction
Objectives Requirements
Control Design
Control Model
Simplification optimization
Code generation
Auto-code gen.
Control design process
Implementation process
Calibration& Verification & Validation
Evidence Collection

Key Capabilities of DAF

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


giggleBites
Why's a picture worth a thousand words?
Hmm... How fast do you type?
About 25 words per minute.
That's it! When I finish my drawing in 40 minutes...
... you would have already typed 1000 words!
© 2009 cartoosh.com

Dr. Ben Calloni, P.E., CISSP, OCRES

E-mail: ben.a.calloni@lmco.com

THANK YOU