Working Together to Build Confidence

# Threat and Risk Analysis Metamodel

System Assurance Task Force

Nikolai Mansourov
CTO, KDM Analytics

nick@kdmanalytics.com

# *Agenda*

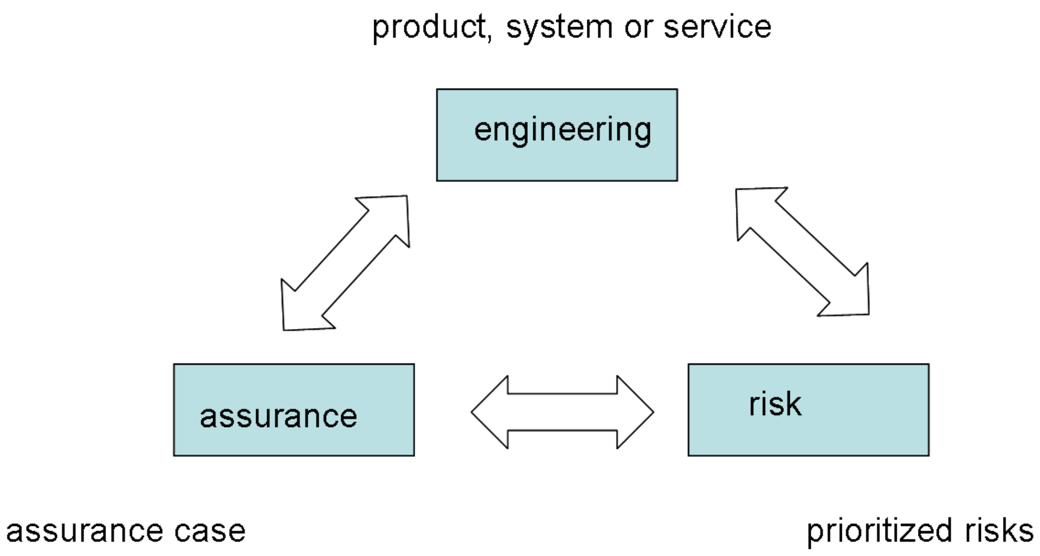
- The Big Picture – OMG Systems Assurance Ecosystem
  - Standard protocols for exchanging knowledge for assurance
- Threat and Risk knowledge in the context of the Ecosystem
- Current approach and discussion

# *Status*

- Keynote presentation by Joe Jarzombek, Director Software Assurance, National Cybersecurity Division, DHS, March, 2008
  - “Need to Assurance Standards in Mitigating Risks for the Enterprise”
- Roadmap discussions within SysA TF, 2008
  - The OMG System Assurance Ecosystem concept
- Initial discussions on Risk Analysis Metamodel
  - Yoshihira Nakabo (AIST), 2010
- RFI
  - Released September 2010
  - Deadline for response March 2011
  - Responses 2011: Thales, Toyota, AIST
- RPF – planned March 2013

# *Engineering, Assurance and Risk*

- Engineering, Assurance and Risk are intimately related
  - To assure a system means to demonstrate that System Engineering principles were correctly followed in meeting the security goals.
  - Additional guidance provided for System Assurance is based on the developing 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.



product, system or service

engineering

assurance

risk

assurance case

prioritized risks

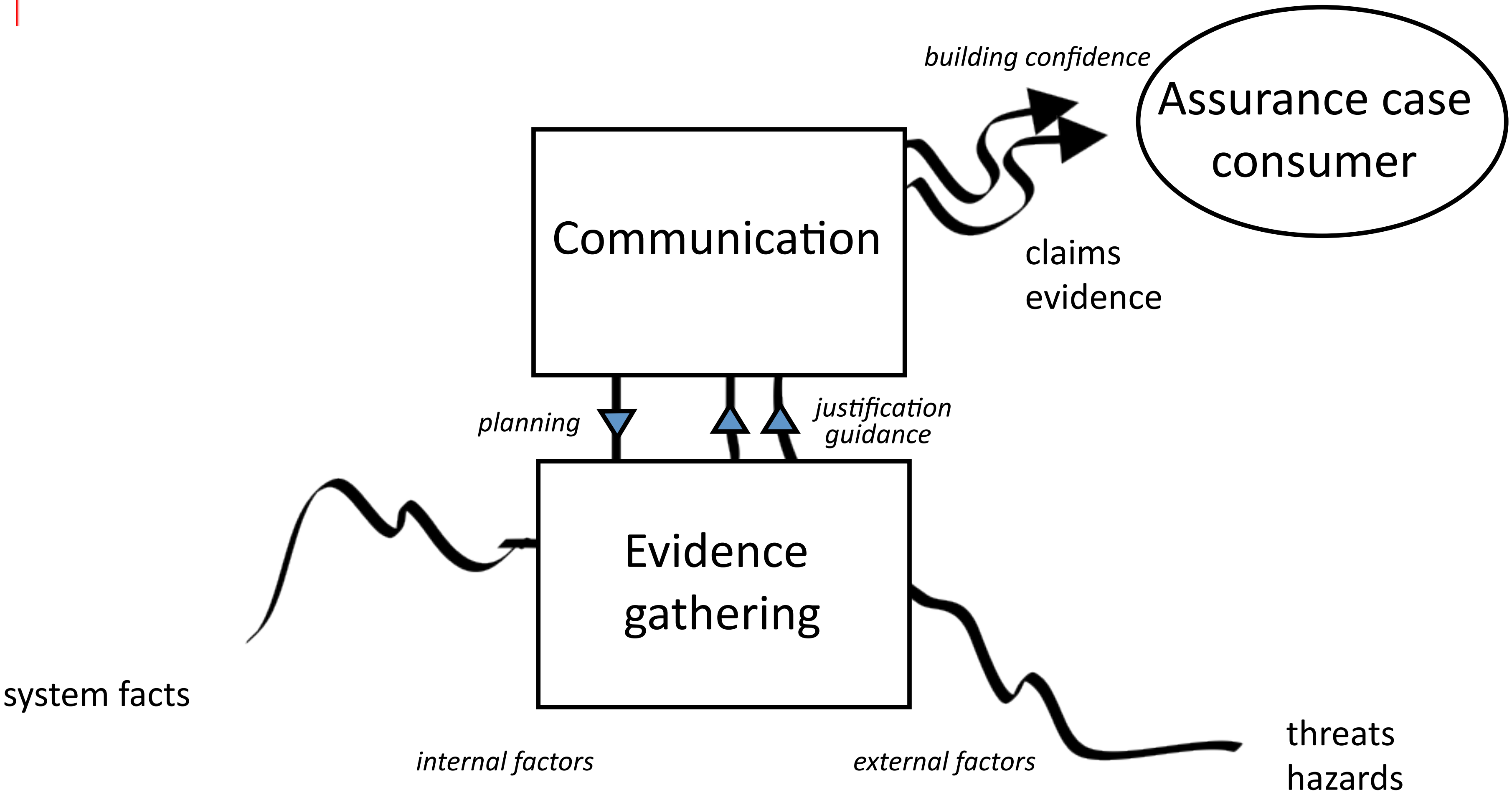
# *What is system assurance?*

- System performs a mission within a certain operational environment
- There are hazards and threats within the environment that can lead to mishaps and failures
- In order to prevent mishaps and failures, countermeasures are added to the system

- *But how do we know that the countermeasures are effective against the known threats and hazards?*

- System assurance is about making *justified claims* about the effectiveness of the countermeasures against threats and hazards. Claims are supported by evidence.

# *Systems Assurance: Knowledge-intensive product*



*building confidence*

Assurance case consumer

Communication

claims

evidence

*planning*

*justification*

*guidance*

Evidence gathering

system facts

*internal factors*

*external factors*

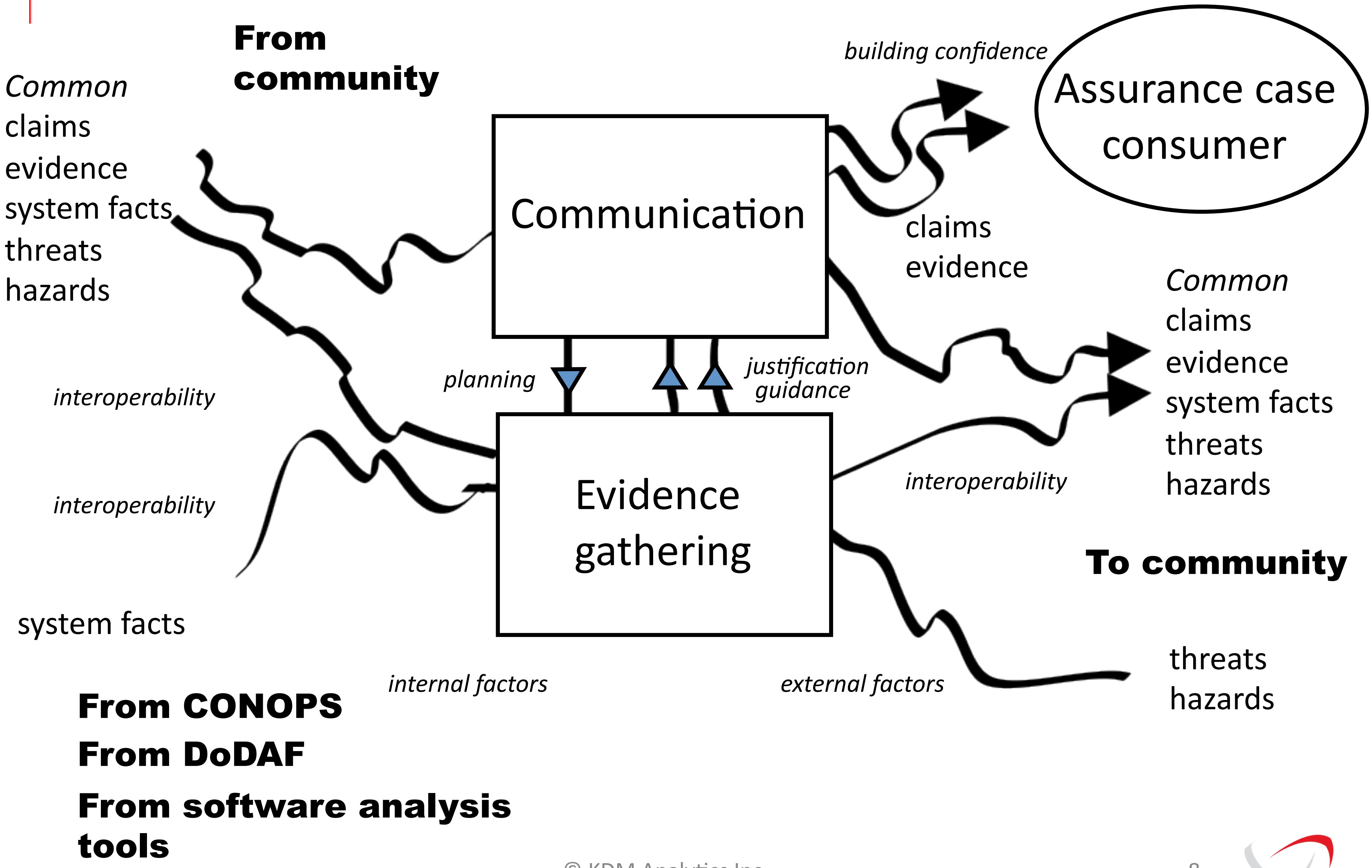
threats

hazards

# *Knowledge exchanges in system assurance*

- System assurance involves two key processes
  - evidence gathering
    - collection of the evidence from the system life cycle
    - system analysis
    - analysis of evidence
  - communication
    - clear, comprehensive, defendable argument that explains the evidence
    - development of the assurance case is driven by existing evidence
    - assurance argument provides guidance for evidence collection

# *Interoperability for Systems Assurance*



**From community**

*Common*
claims
evidence
system facts
threats
hazards

*interoperability*

*interoperability*

system facts

**From CONOPS**

**From DoDAF**

**From software analysis tools**

*internal factors*

Communication

*planning*

*justification guidance*

Evidence gathering

*building confidence*

Assurance case consumer

claims
evidence

*Common*
claims
evidence
system facts
threats
hazards

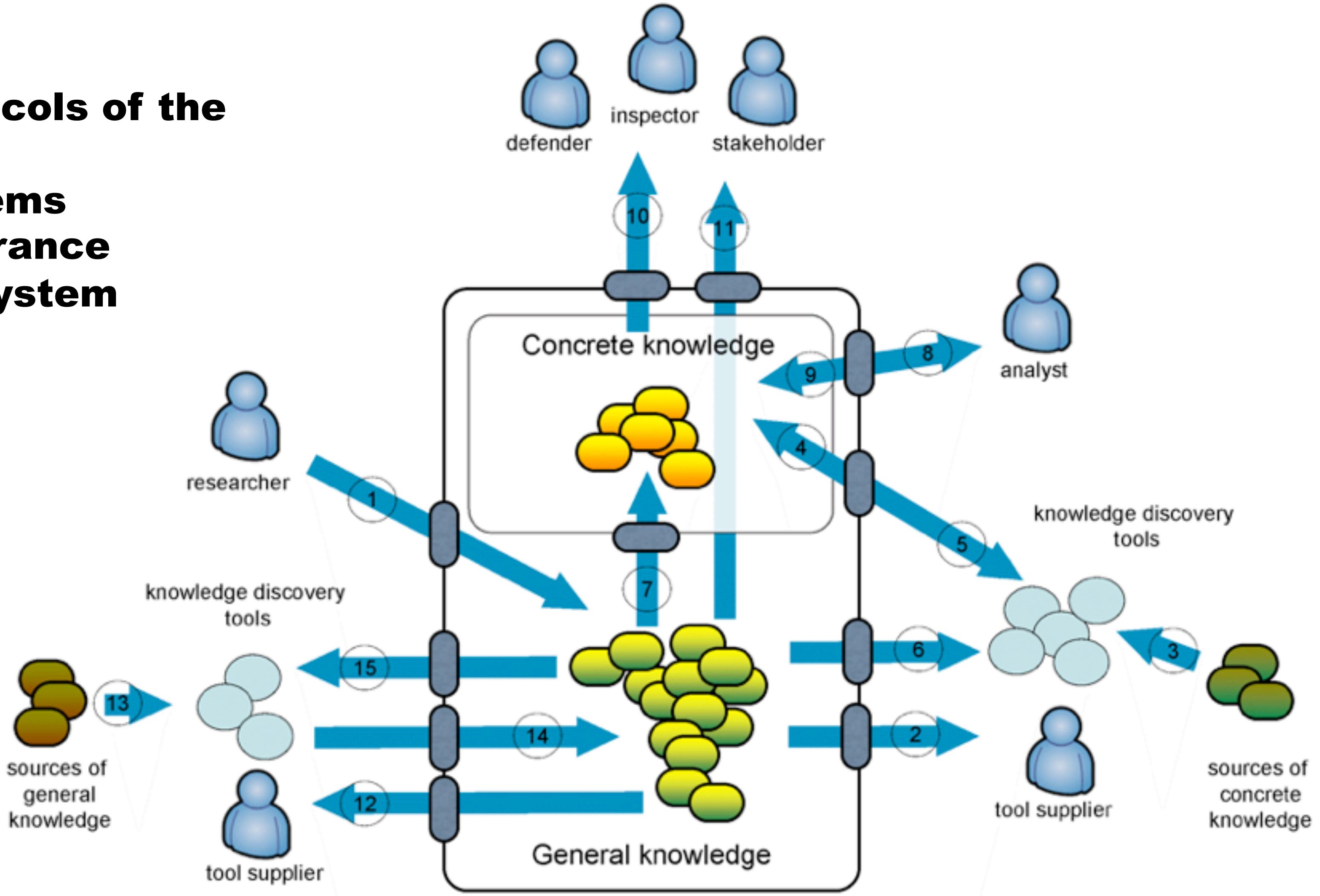
*interoperability*

**To community**

*external factors*

threats
hazards

# Protocols of the OMG Systems Assurance Ecosystem

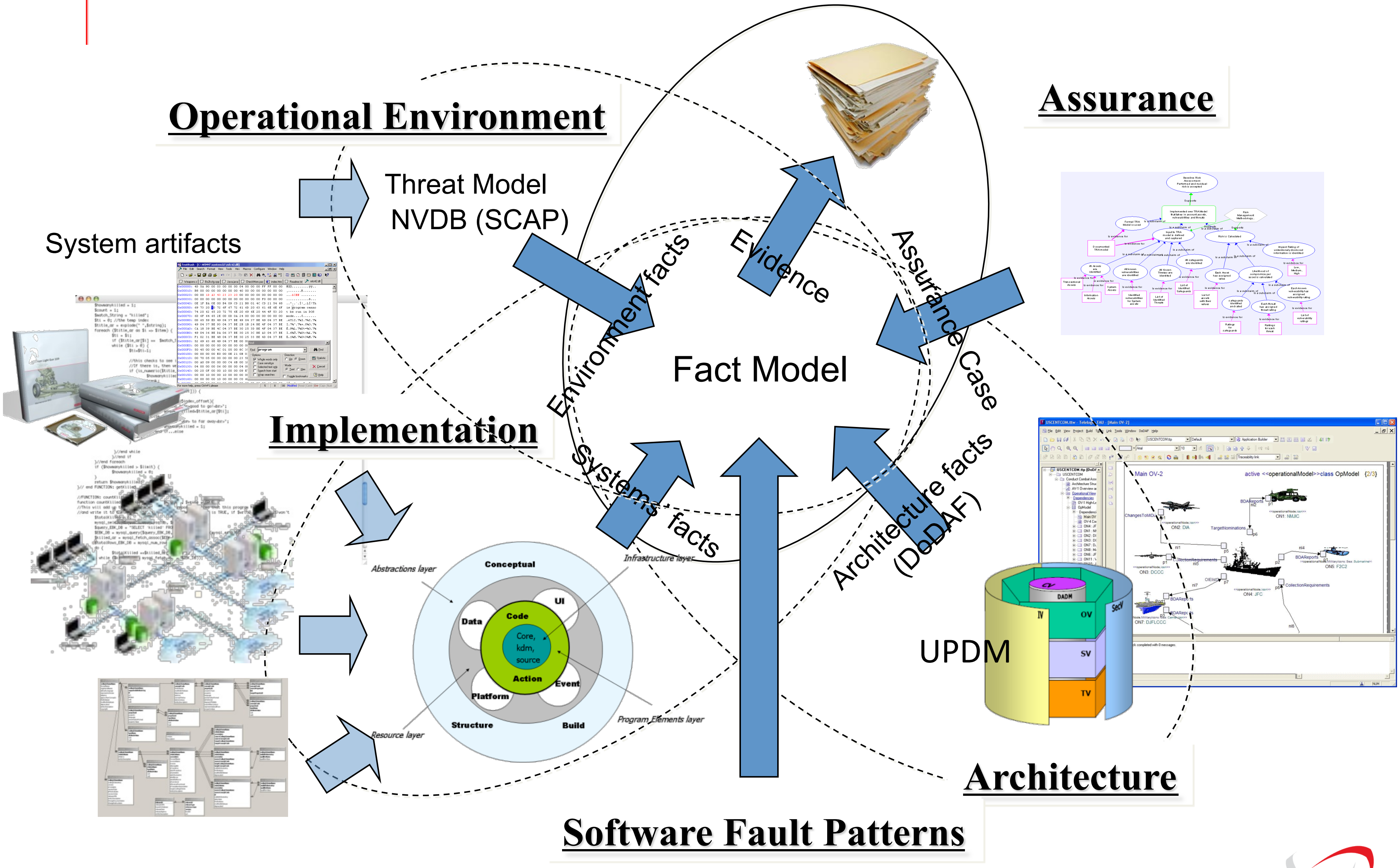


## Protocols of the OMG Systems Assurance Ecosystem

- *Structured Assurance Case Metamodel (SACM):*
  - *Argumentation Metamodel*: standard protocol for exchanging assurance arguments
  - *Evidence Metamodel*: standard protocol for managing and exchanging evidence
- *Knowledge Discovery Metamodel (KDM)*: standard protocol for exchanging system/implementation facts
  - *Now also ISO/IEC 19506*
- UPDM for exchanging operational facts
- *Semantics of Business Vocabularies and Rules (SBVR)*: standard protocol for exchanging vocabularies and precise statements
- *Threats and Risk Metamodel*
  - work in progress

# *Common Fact Model:*

## *Collecting system knowledge through set of integrated standards*



Operational Environment

Threat Model
NVDB (SCAP)

System artifacts

Assurance

Environment facts

Evidence

Assurance Case

Fact Model

Implementation

Systems' facts

Architecture facts (DoDAF)

UPDM

Architecture

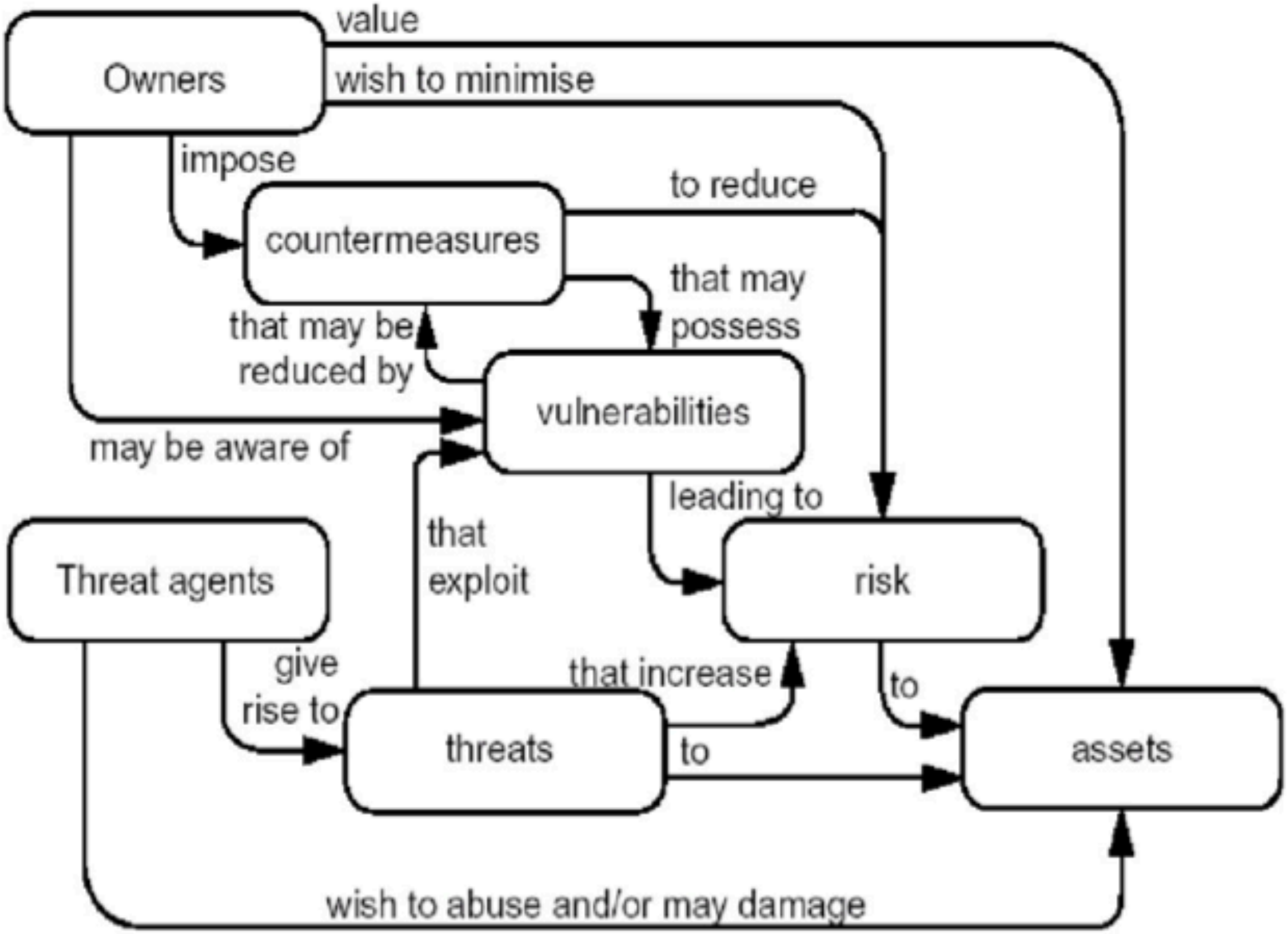
Software Fault Patterns

# *Fact-oriented assurance*

- Fact-oriented involves the following:
  - Facts are *assertions* that are considered to be elementary to be understood and agreed upon without the need for further justification.
  - Facts involve assertions of *existence* of certain objects, *characteristics* of objects and assertions of certain *relations* between these objects.
  - Evidence is the collection of relevant facts. Evidence needs to be gathered among the myriads of facts that can be known.
  - Fact-oriented assurance develops claims based on the available facts. On the other hand, the assurance argument helps planning the evidence gathering, which helps focus on only those fact-finding activities that support the assurance argument
  - Fact-oriented also has a certain technical meaning: all knowledge items are uniformly treated as facts (objects and relationships), which facilitates their integration. Facts are stored in a physical repository

# *KNOWLEDGE OF THREATS AND RISKS*

# *Security concepts and relationships (ISO 15408)*

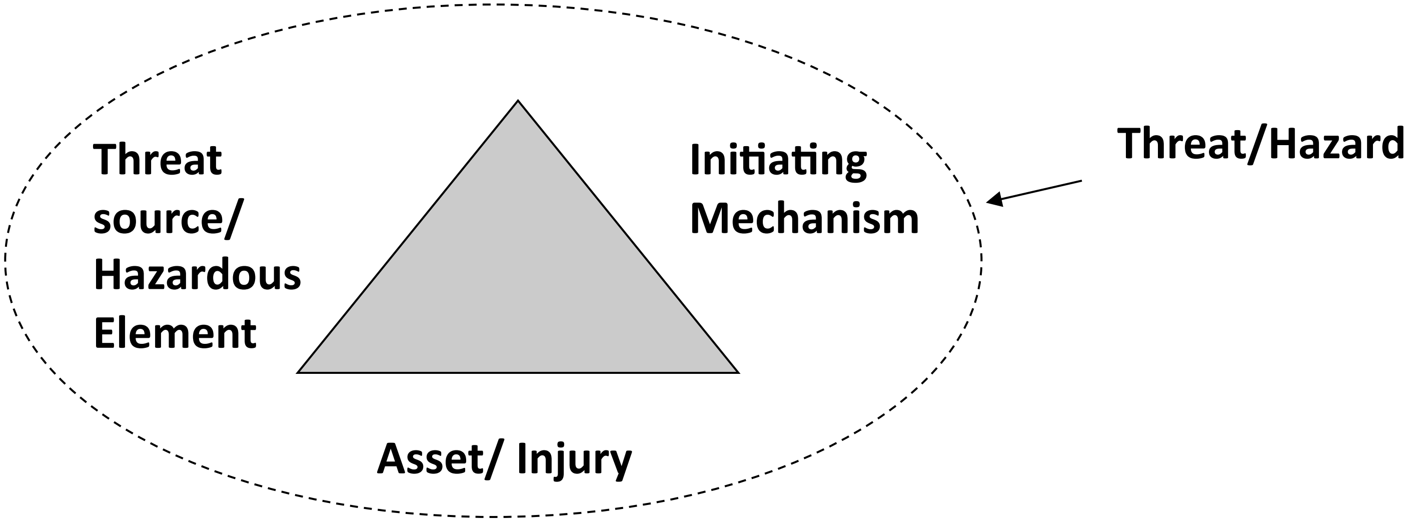


# *Existing methodologies*

- ISO/IEC 13335
- ISO/IEC 15408
- ISO/IEC 15443
- ISO/IEC 27001
- CRAMM (UK)
- EBIOS (France)
- Mehari (France)
- Magerit (Spain)
- HTRA (Canada)
- NIST SP-800-30 (US)
- Octave (SEI CMU)
- RiskAn (Czech Rep)
- Microsoft Threat analysis Methodology
- others

**Challenges:**
**1) no interoperability;**
**2) few approaches are systematic enough to provide assurance**

# *Towards common information elements*



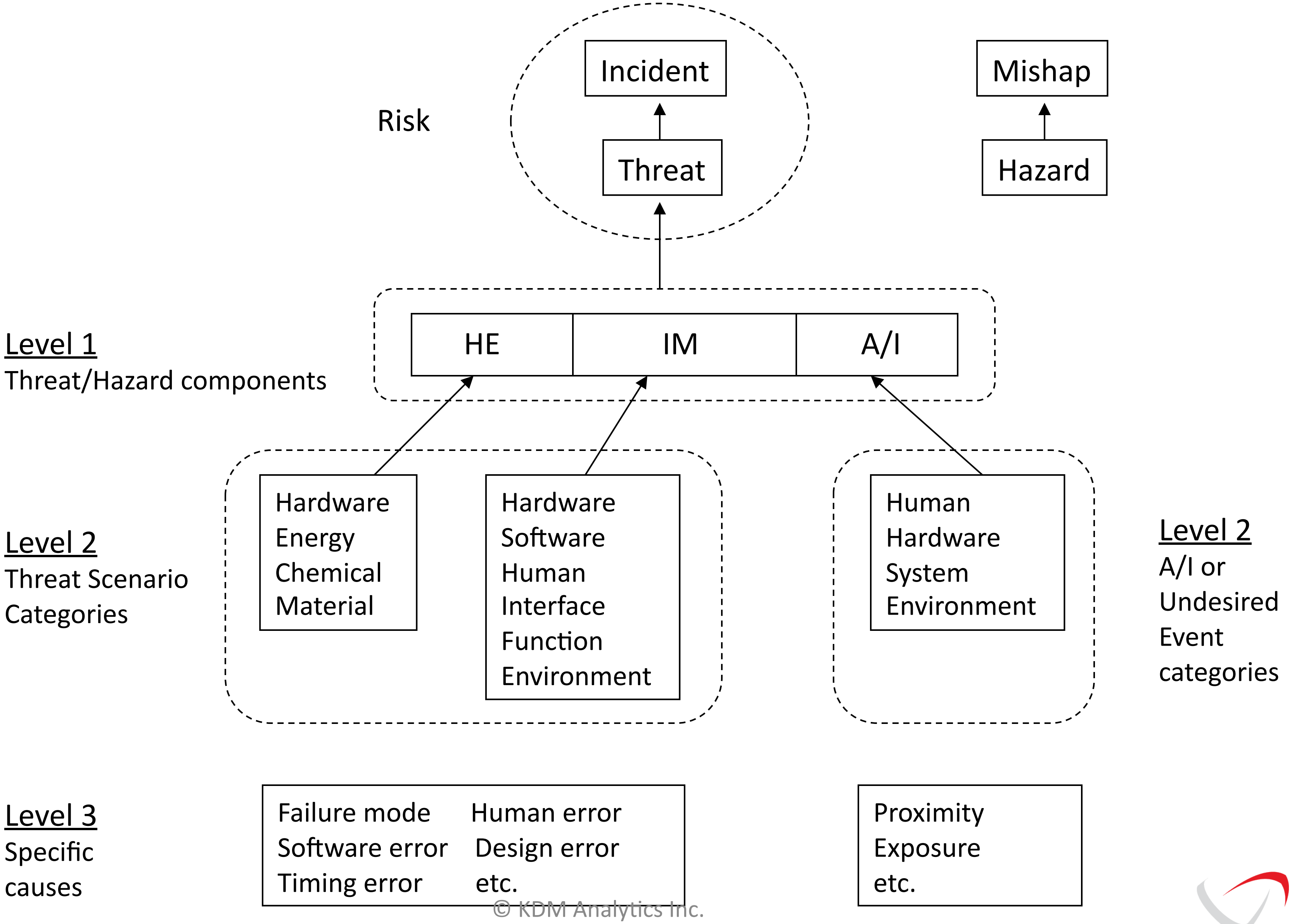
**Threat/Hazard**

Worker could be electrocuted by touching exposed contacts in electrical panel containing high voltage.

**Threat/Hazard Components**

| | | |
|---|---|---|
| Worker | Asset | Undesired event |
| could be electrocuted | Injury | |
| by touching | IM | Threat scenario |
| exposed contacts in electrical panel | IM | |
| containing high voltage | HE | |

# *Enumerate components to systematically identify risks*



Risk

Incident

Threat

Mishap

Hazard

Level 1

Threat/Hazard components

HE

IM

A/I

Level 2

Threat Scenario Categories

Hardware
Energy
Chemical
Material

Hardware
Software
Human
Interface
Function
Environment

Human
Hardware
System
Environment

Level 2

A/I or Undesired Event categories

Level 3

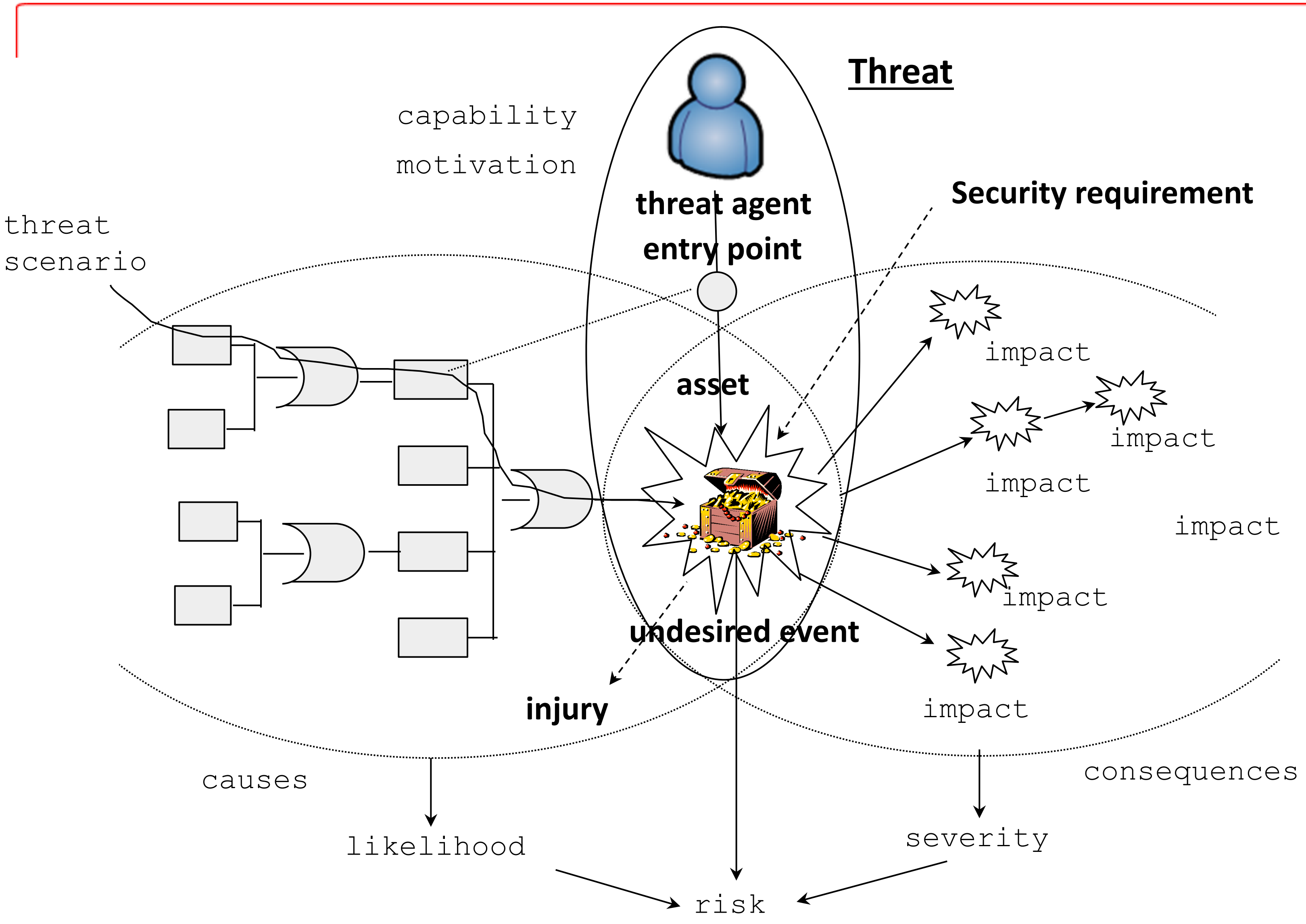
Specific causes

Failure mode
Software error
Timing error

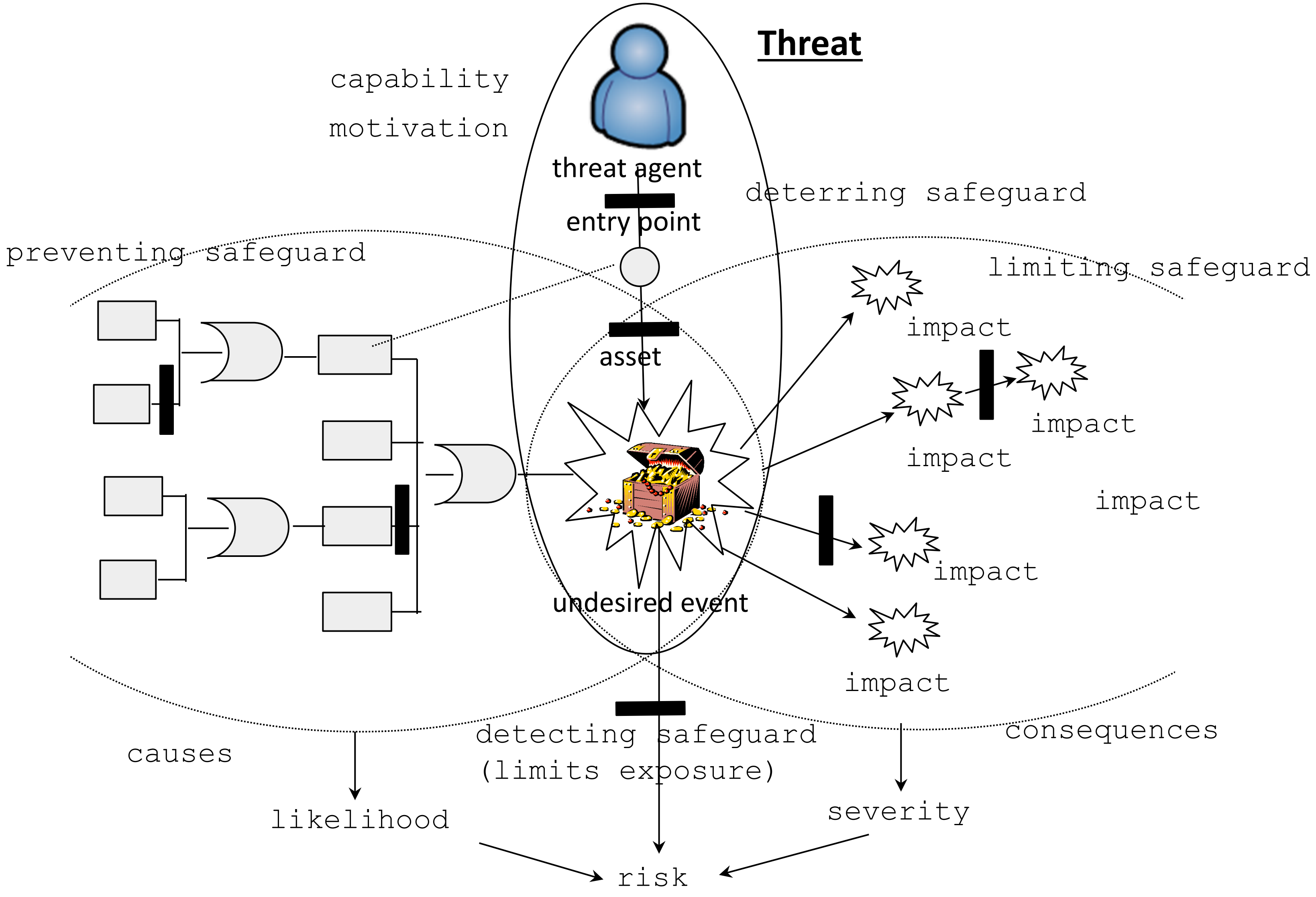
Human error
Design error
etc.

Proximity
Exposure
etc.

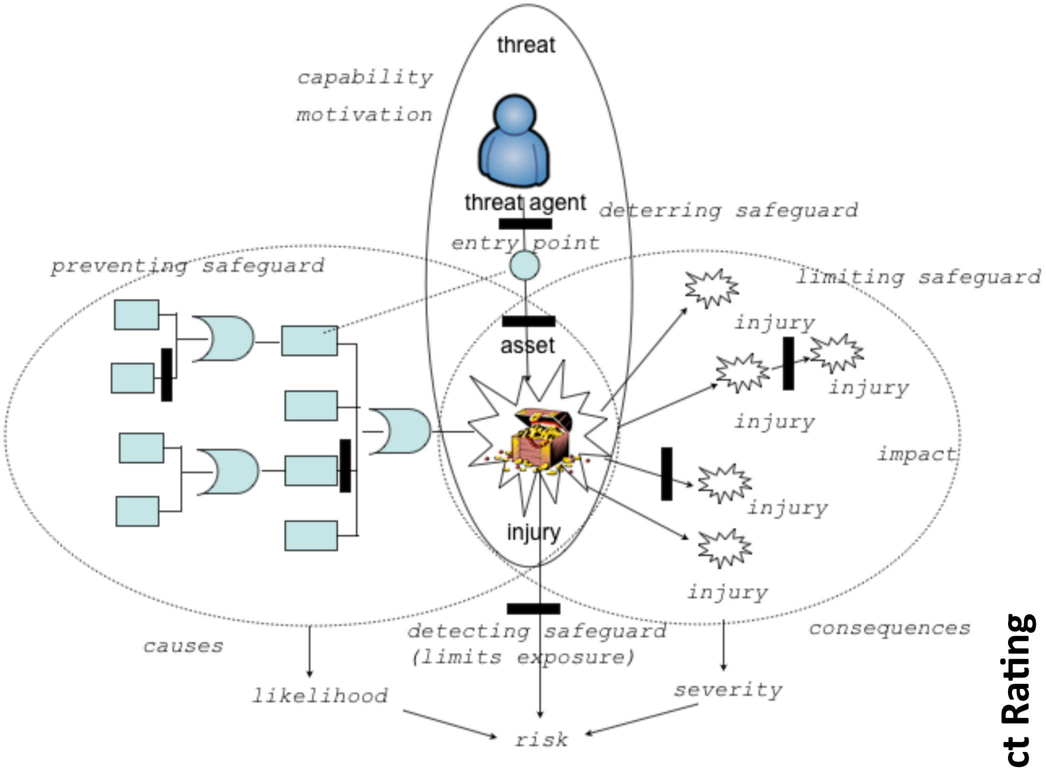
# *Fact-oriented threat and risk analysis*



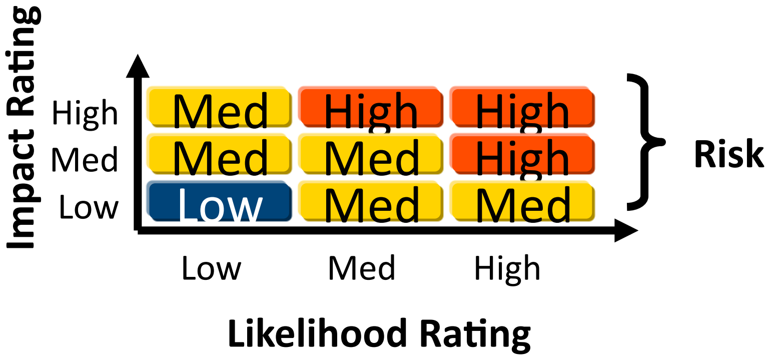
# *Safeguards*


Threat
capability
motivation
threat agent
entry point
deterring safeguard
preventing safeguard
limiting safeguard
asset
impact
impact
impact
impact
impact
impact
undesired event
causes
detecting safeguard
(limits exposure)
consequences
likelihood
severity
risk

# *Risk Calculation*



Risk = ∫(Severity of Impact, Likelihood)

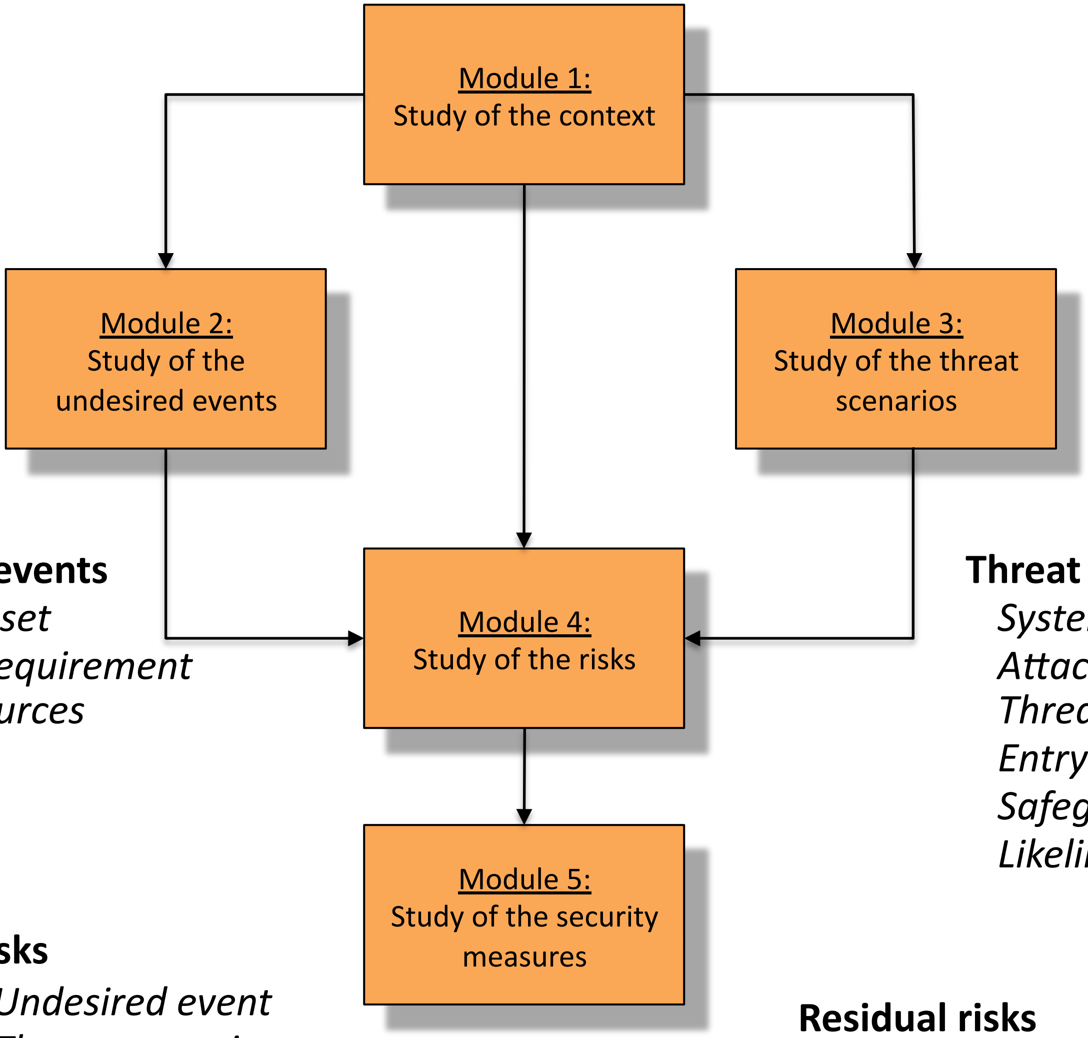


| Impact Rating | Low | Med | High |
|---|---|---|---|
| High | Med | High | High |
| Med | Med | Med | High |
| Low | Low | Med | Med |

Risk
Likelihood Rating

**Challenge: effective and systematic measurement of the risk**

# *Facts for systematic risk identification*


Module 1:
Study of the context
Module 2:
Study of the undesired events
Module 3:
Study of the threat scenarios
Module 4:
Study of the risks
Module 5:
Study of the security measures

**Mission**
**Operational capabilities**
**Owners**
**Security criteria**
**Critical assets**
**Security requirements**
**System assets**
**System dependencies**
**Threat levels**
**Threat sources**

**Undesired events**

*Critical asset*
*Security requirement*
*Threat sources*
*Impacts*
*Severity*

**Threat Scenarios**

*System asset*
*Attack mode*
*Threat sources*
*Entry points*
*Safeguards*
*Likelihood*

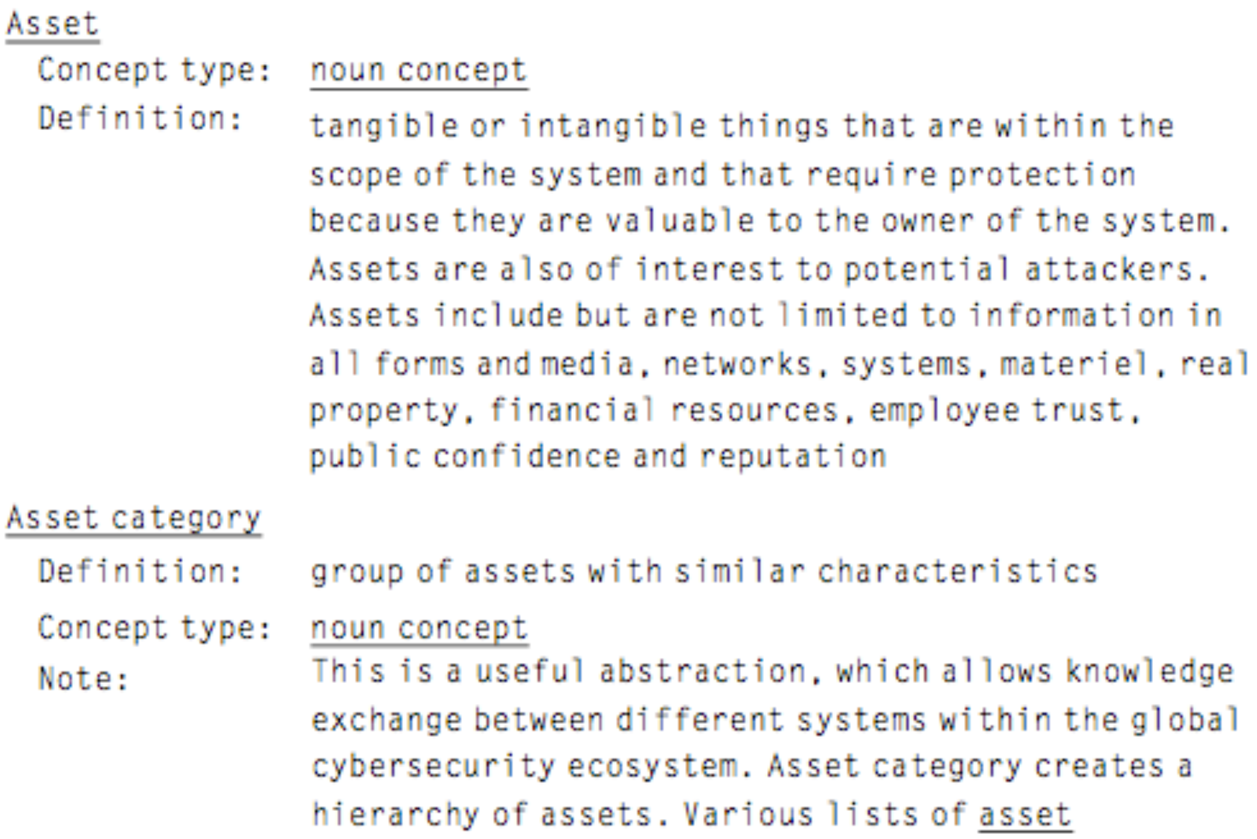
**Risks**

*Undesired event*
*Threat scenario*
*Threat source*
*Level*

**Residual risks**

*Safeguards*
*Level*

# Sample Threat and Risk vocabulary in SBVR SE (1)



Asset

Concept type: noun concept

Definition: tangible or intangible things that are within the scope of the system and that require protection because they are valuable to the owner of the system. Assets are also of interest to potential attackers. Assets include but are not limited to information in all forms and media, networks, systems, materiel, real property, financial resources, employee trust, public confidence and reputation

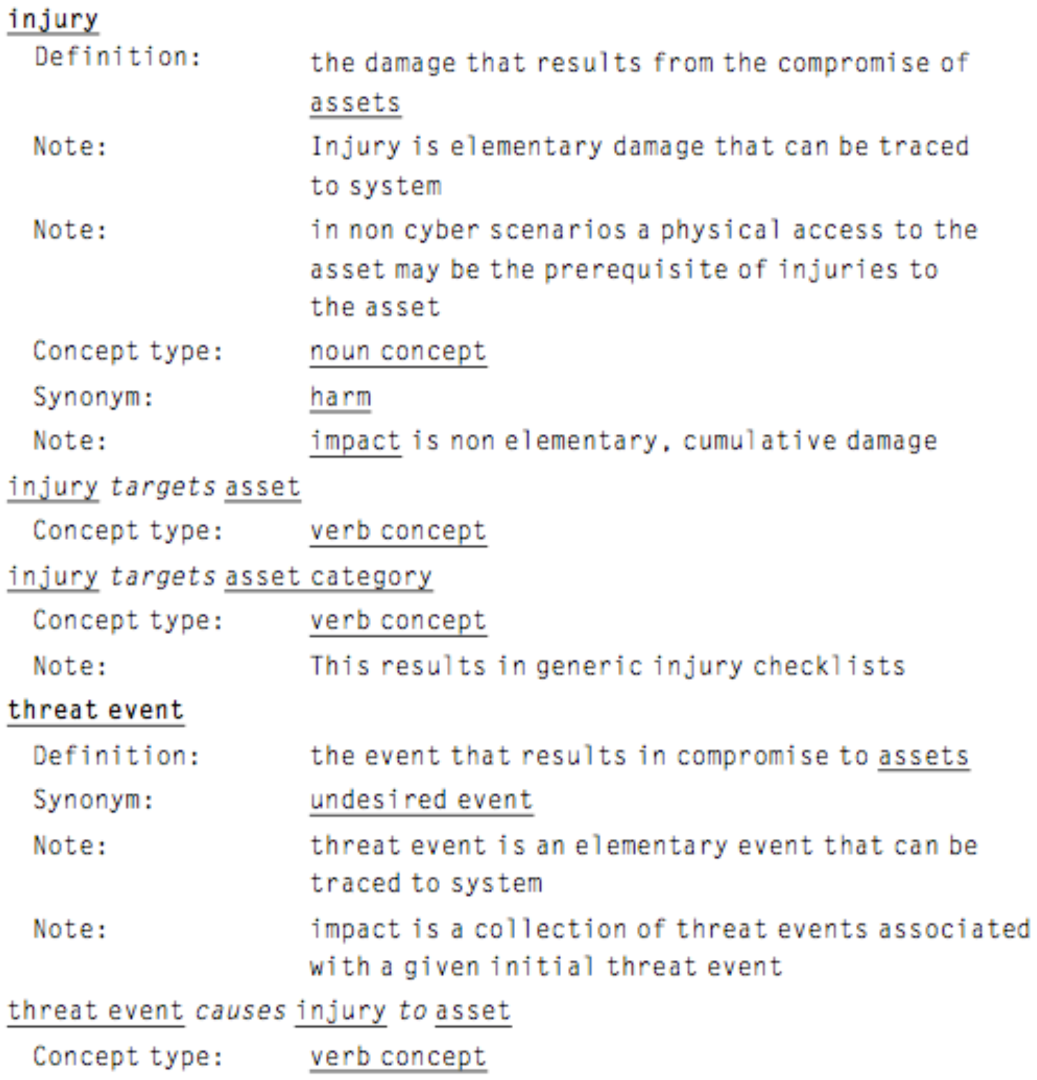
Asset category

Definition: group of assets with similar characteristics

Concept type: noun concept

Note: This is a useful abstraction, which allows knowledge exchange between different systems within the global cybersecurity ecosystem. Asset category creates a hierarchy of assets. Various lists of asset

# *Sample Threat and Risk vocabulary in SBVR SE (2)*



injury

Definition: the damage that results from the compromise of assets

Note: Injury is elementary damage that can be traced to system

Note: in non cyber scenarios a physical access to the asset may be the prerequisite of injuries to the asset

Concept type: noun concept

Synonym: harm

Note: impact is non elementary, cumulative damage

injury *targets* asset

Concept type: verb concept

injury *targets* asset category

Concept type: verb concept

Note: This results in generic injury checklists

**threat event**

Definition: the event that results in compromise to assets

Synonym: undesired event

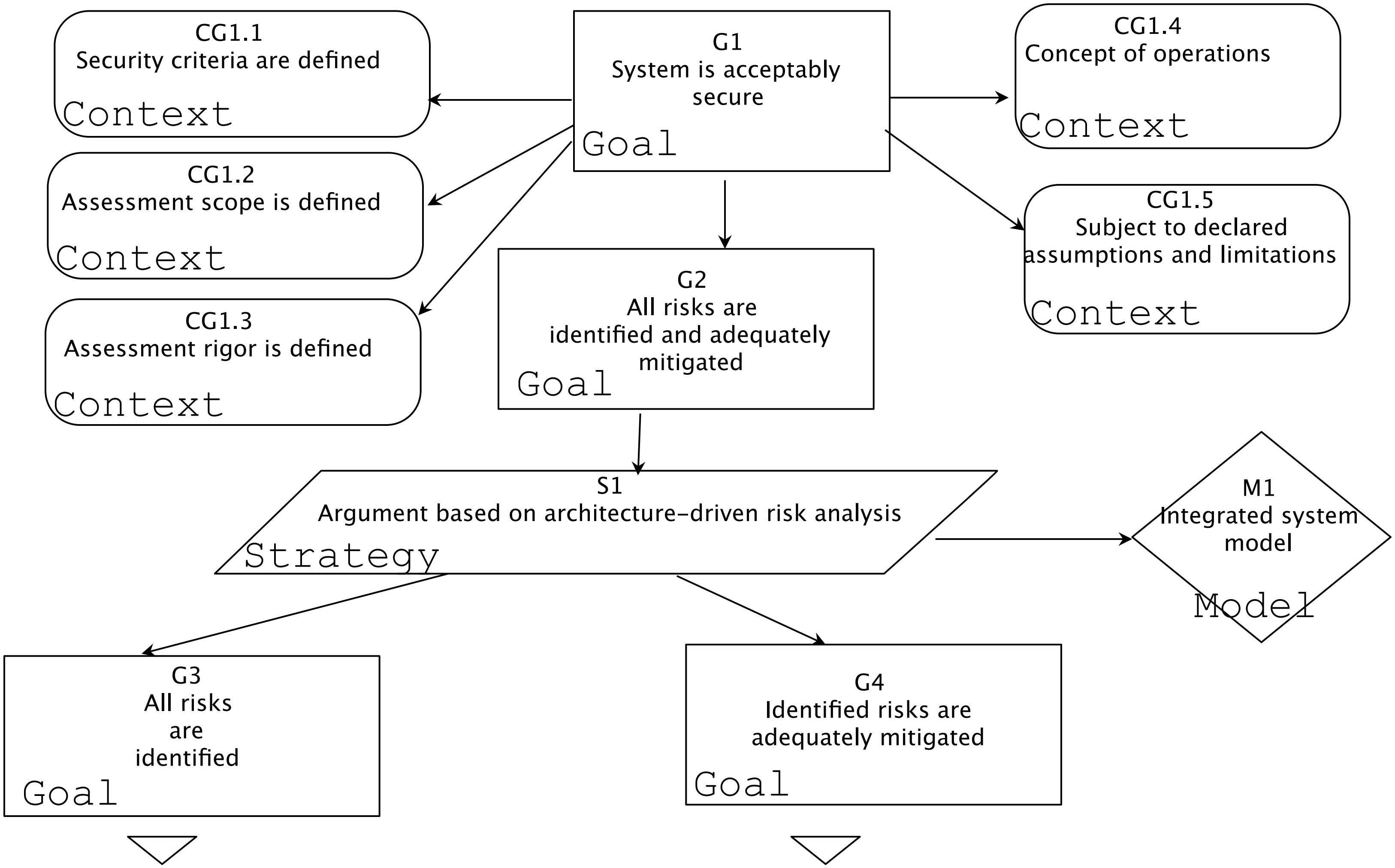
Note: threat event is an elementary event that can be traced to system

Note: impact is a collection of threat events associated with a given initial threat event

threat event *causes* injury *to* asset

Concept type: verb concept

# *Top level assurance case*



CG1.1
Security criteria are defined
Context
CG1.2
Assessment scope is defined
Context
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 risks are identified and adequately mitigated
Goal
S1
Argument based on architecture-driven risk analysis
Strategy
M1
Integrated system model
Model
G3
All risks are identified
Goal
G4
Identified risks are adequately mitigated
Goal

# *STATUS*

# *Approach*

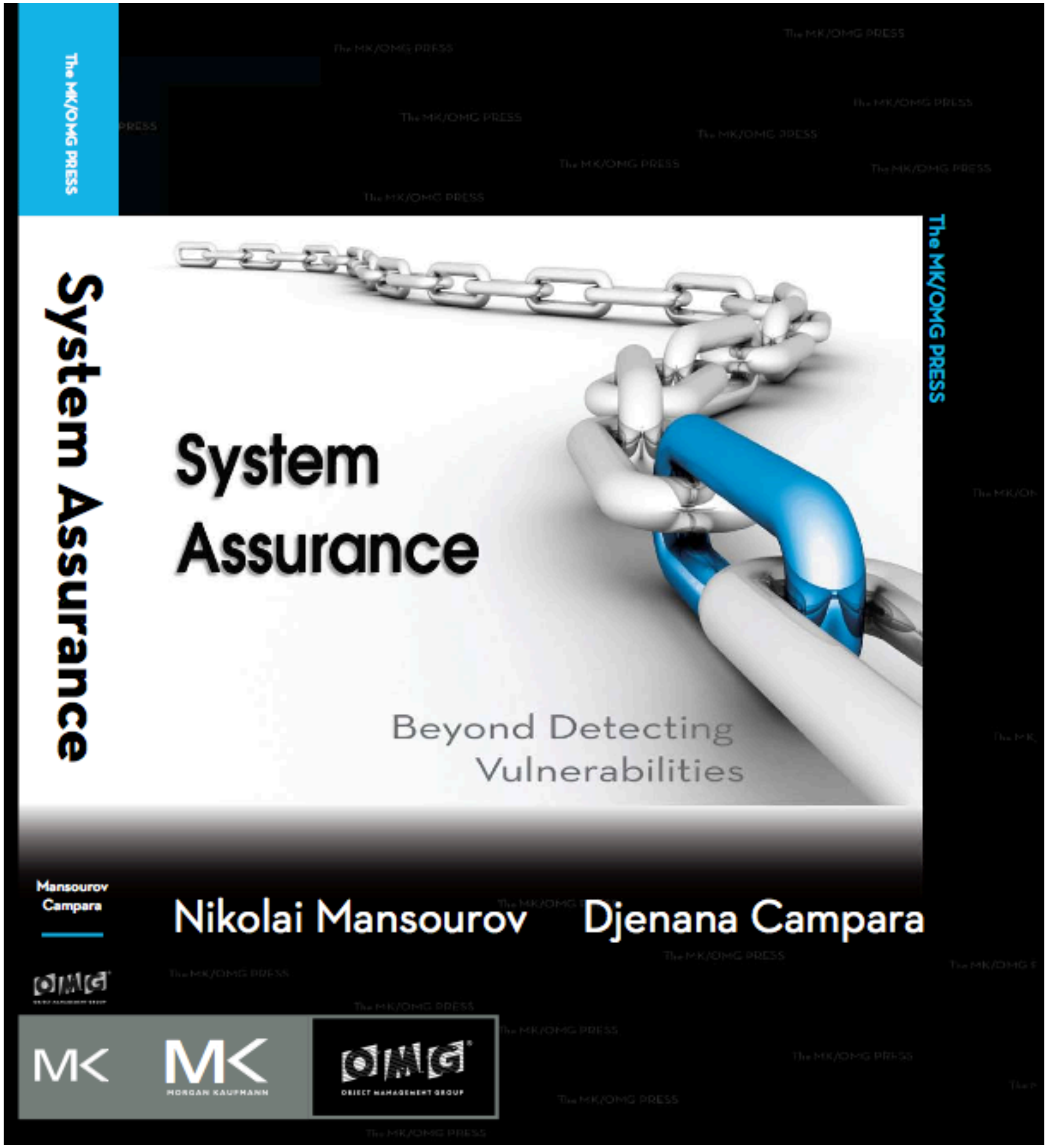
- Key focus: MOF metamodel
    - Aligned with the rest of the OMG System Assurance Ecosystem
    - Fact-oriented: restricted MOF, only entities and relations, aligned with OWL and RDF
        - This approach proved successful in KDM design
- SBVR vocabulary (SBVR Structured English)
    - For consumption within risk management communities
- UML profile to enable use of UML tools for Threat and Risk analysis
    - Aligned with UPDM
- Will coordinate these three representations
    - Experience in Data-Time vocabulary

# *Status*

- Keynote presentation by Joe Jarzombek, Director Software Assurance, National Cybersecurity Division, DHS, March, 2008
  - "Need to Assurance Standards in Mitigating Risks for the Enterprise"
- Roadmap discussions within SysA TF, 2008
  - The OMG System Assurance Ecosystem concept
- Initial discussions on Risk Analysis Metamodel
  - Yoshihira Nakabo (AIST), 2010
- RFI
  - Released September 2010
  - Deadline for response March 2011
  - Responses 2011: Thales, Toyota, AIST
- RPF – planned March 2013

Published
Dec, 2010

Available at
amazon.com



http://www.kdmanalytics.com