industrial internet
CONSORTIUM

Trustworthiness and Assurance in the Industrial IoT Ecosystem

Robert A. Martin
The MITRE Corporation
Industrial Internet Consortium

30 August 2017

MITRE

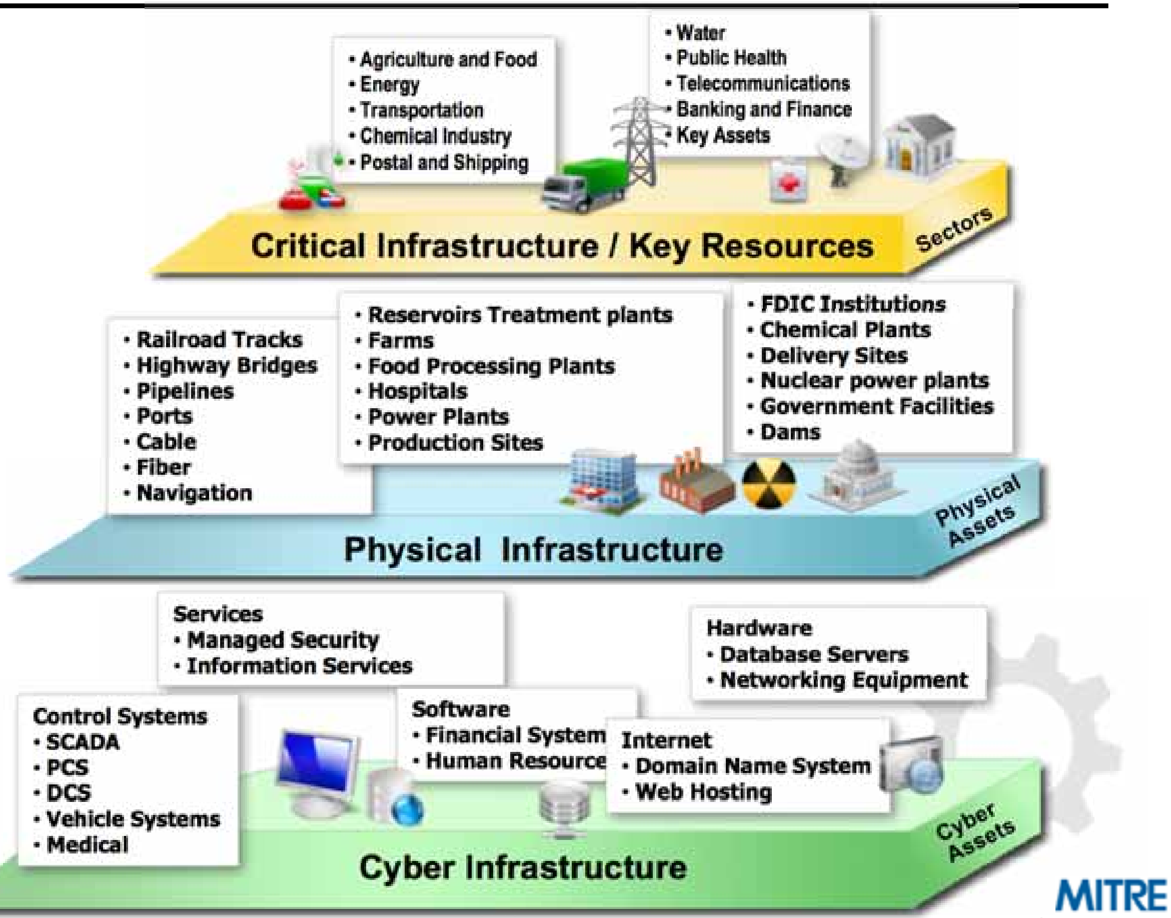
Today's Reality   We Need Confidence in our Software-enabled Connected Cyber Capabilities

Dependencies on software-enabled connected cyber technology is greater then ever

Possibility of disruption is greater than ever because hardware/ software is vulnerable

Loss of confidence alone

an lead to stakeholder actions that disrupt critical business and support activities



- Agriculture and Food
- Energy
- Transportation
- Chemical Industry
- Postal and Shipping

- Water
- Public Health
- Telecommunications
- Banking and Finance
- Key Assets

Critical Infrastructure / Key Resources

Sectors

- Railroad Tracks
- Highway Bridges
- Pipelines
- Ports
- Cable
- Fiber
- Navigation

- Reservoirs Treatment plants
- Farms
- Food Processing Plants
- Hospitals
- Power Plants
- Production Sites

- FDIC Institutions
- Chemical Plants
- Delivery Sites
- Nuclear power plants
- Government Facilities
- Dams

Physical Infrastructure

Physical Assets

Services
- Managed Security
- Information Services

Hardware
- Database Servers
- Networking Equipment

Control Systems
- SCADA
- PCS
- DCS
- Vehicle Systems
- Medical

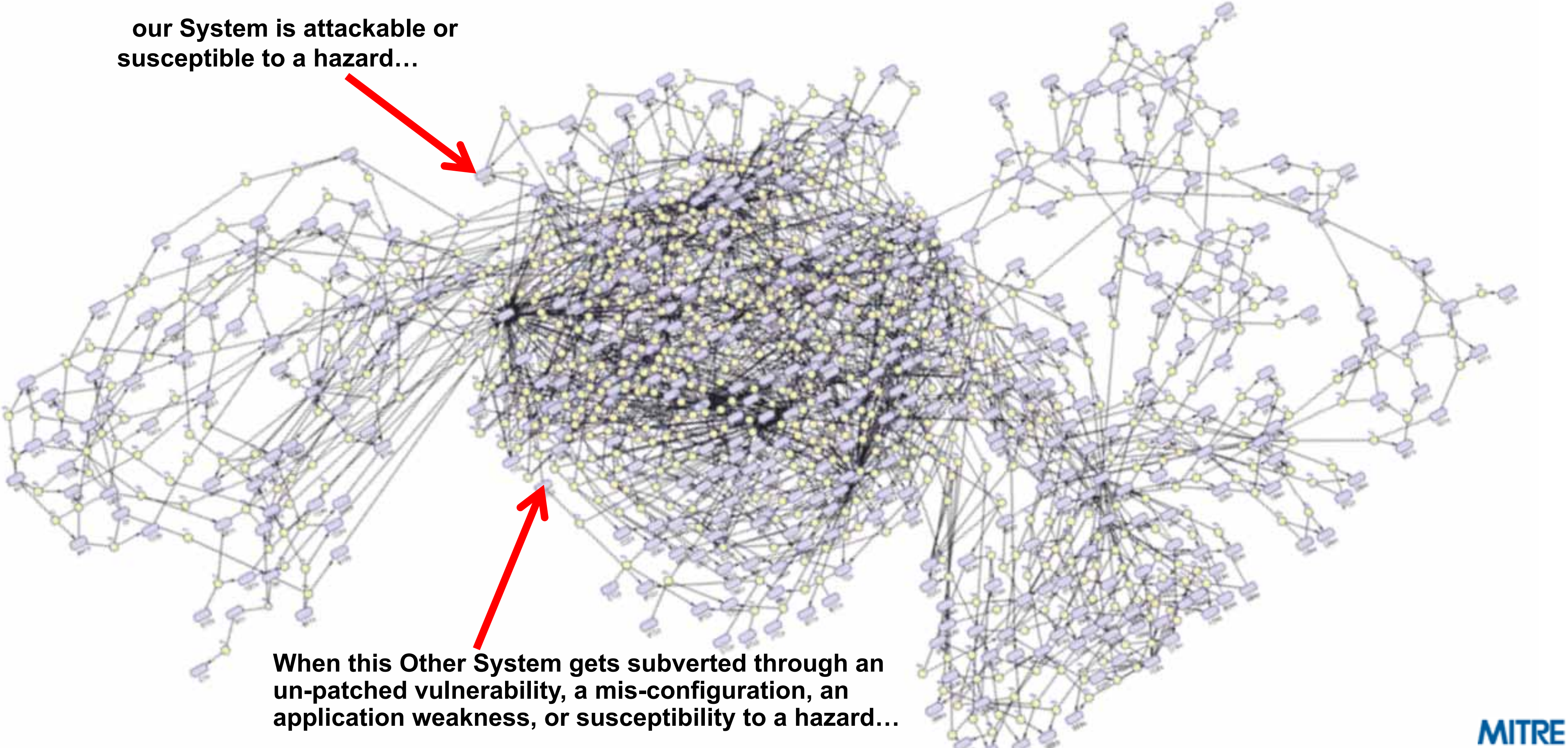
Software
- Financial System
- Human Resource

Internet
- Domain Name System
- Web Hosting

Cyber Infrastructure

Cyber Assets

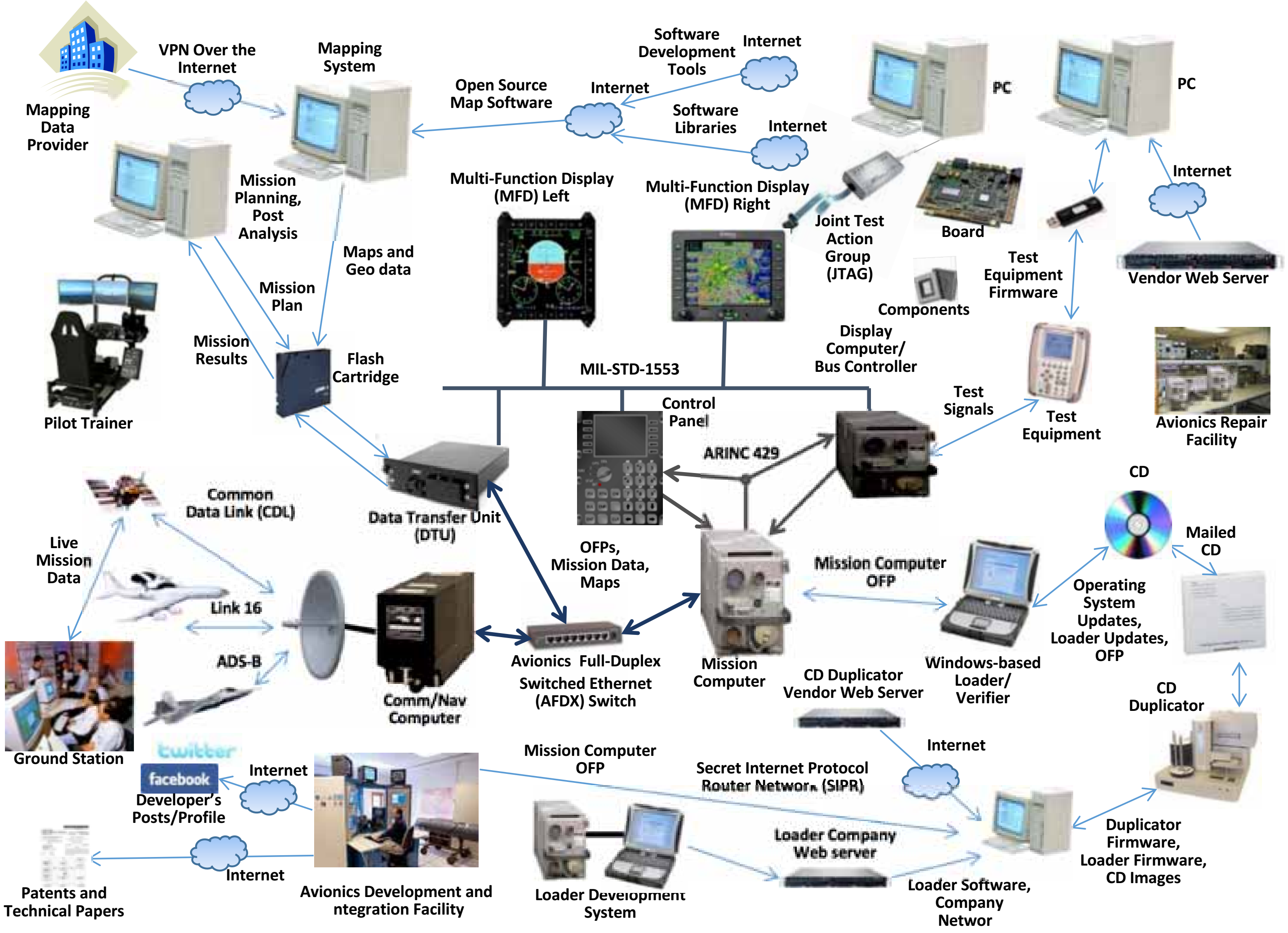
Everything's Cyber Enabled, Connected, and Co-Dependent



our System is attackable or susceptible to a hazard…

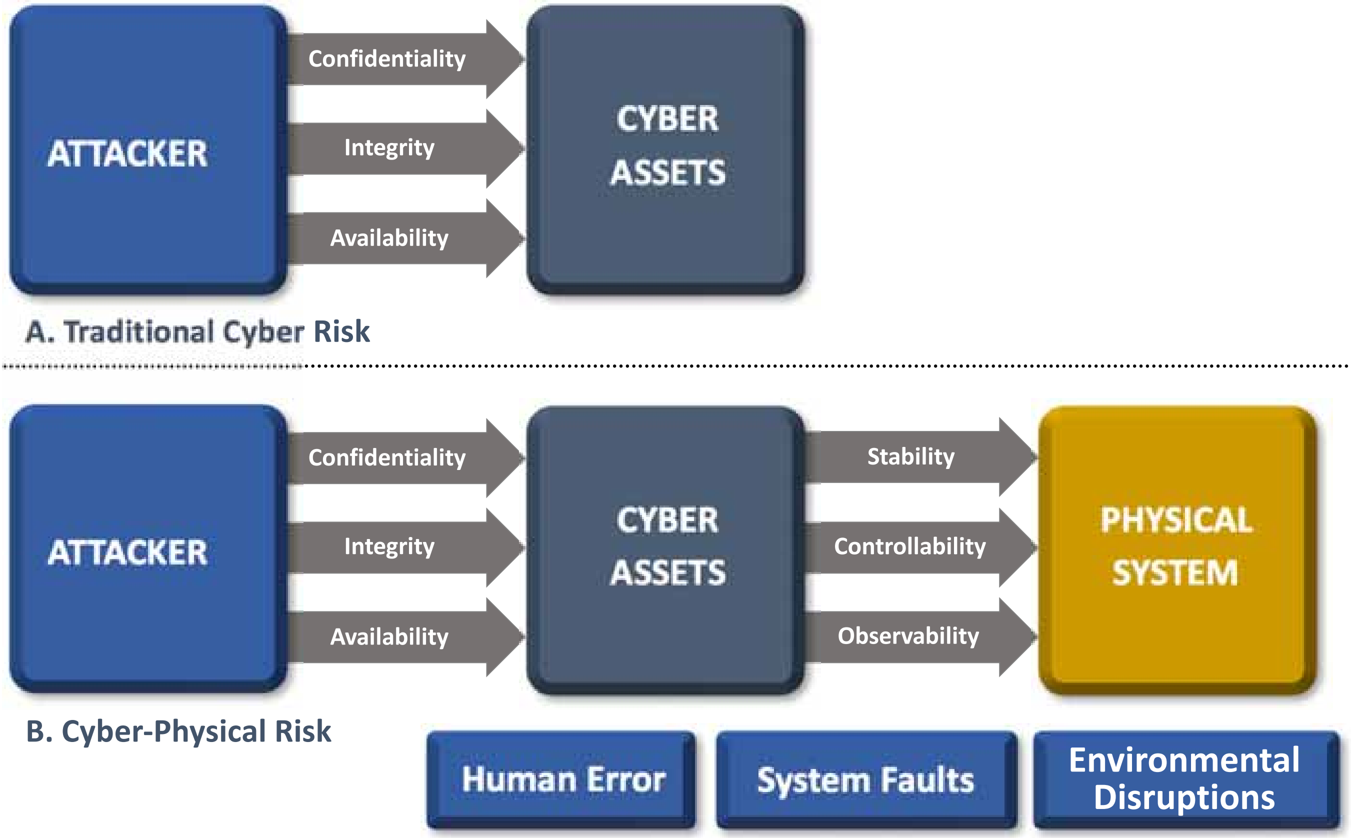
When this Other System gets subverted through an un-patched vulnerability, a mis-configuration, an application weakness, or susceptibility to a hazard…

An Example of Cyber Enabled, Connected, and Co-Dependent…


Mapping Data Provider
VPN Over the Internet
Mapping System
Open Source Map Software
Internet
Software Development Tools
Internet
Software Libraries
Internet
PC
PC
Internet
Mission Planning, Post Analysis
Maps and Geo data
Mission Plan
Mission Results
Flash Cartridge
Multi-Function Display (MFD) Left
Multi-Function Display (MFD) Right
Joint Test Action Group (JTAG)
Board
Test Equipment Firmware
Vendor Web Server
Components
Display Computer/ Bus Controller
MIL-STD-1553
Pilot Trainer
Control Panel
ARINC 429
Test Signals
Test Equipment
Avionics Repair Facility
CD
Common Data Link (CDL)
Data Transfer Unit (DTU)
Live Mission Data
OFPs, Mission Data, Maps
Mailed CD
Mission Computer OFP
Link 16
Operating System Updates, Loader Updates, OFP
ADS-B
Avionics Full-Duplex Switched Ethernet (AFDX) Switch
Mission Computer
Windows-based Loader/ Verifier
CD Duplicator Vendor Web Server
Comm/Nav Computer
CD Duplicator
Ground Station
Internet
facebook
Developer's Posts/Profile
Internet
Mission Computer OFP
Secret Internet Protocol Router Networ‹ (SIPR)
Loader Company Web server
Duplicator Firmware, Loader Firmware, CD Images
Patents and Technical Papers
Internet
Avionics Development and ntegration Facility
Loader Development System
Loader Software, Company Networ

Approved for Public Release; Distribution Unlimited. Case Number 17–3226-002

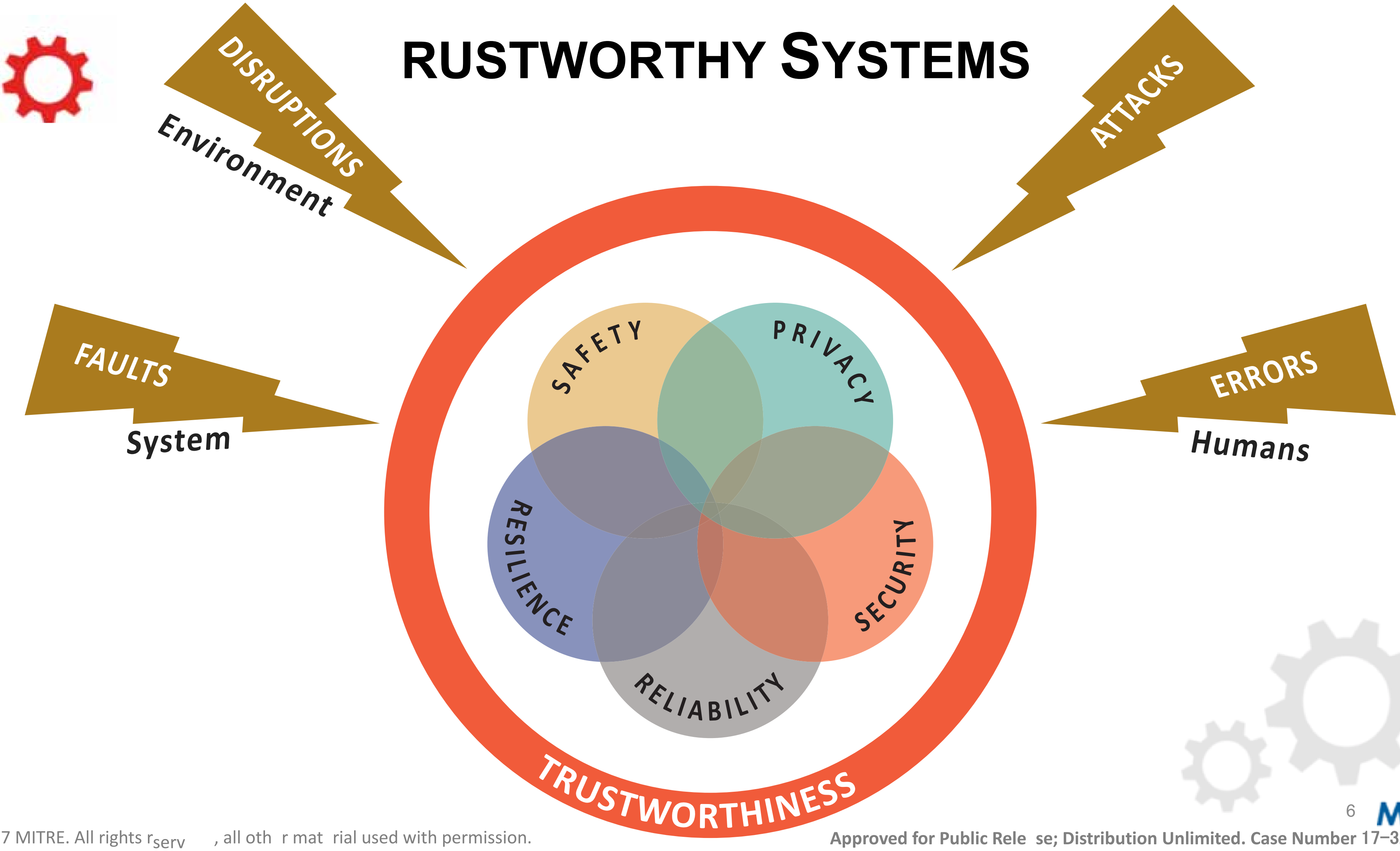
Control Systems o Cyber P ysical Systems



A. Traditional Cyber Risk

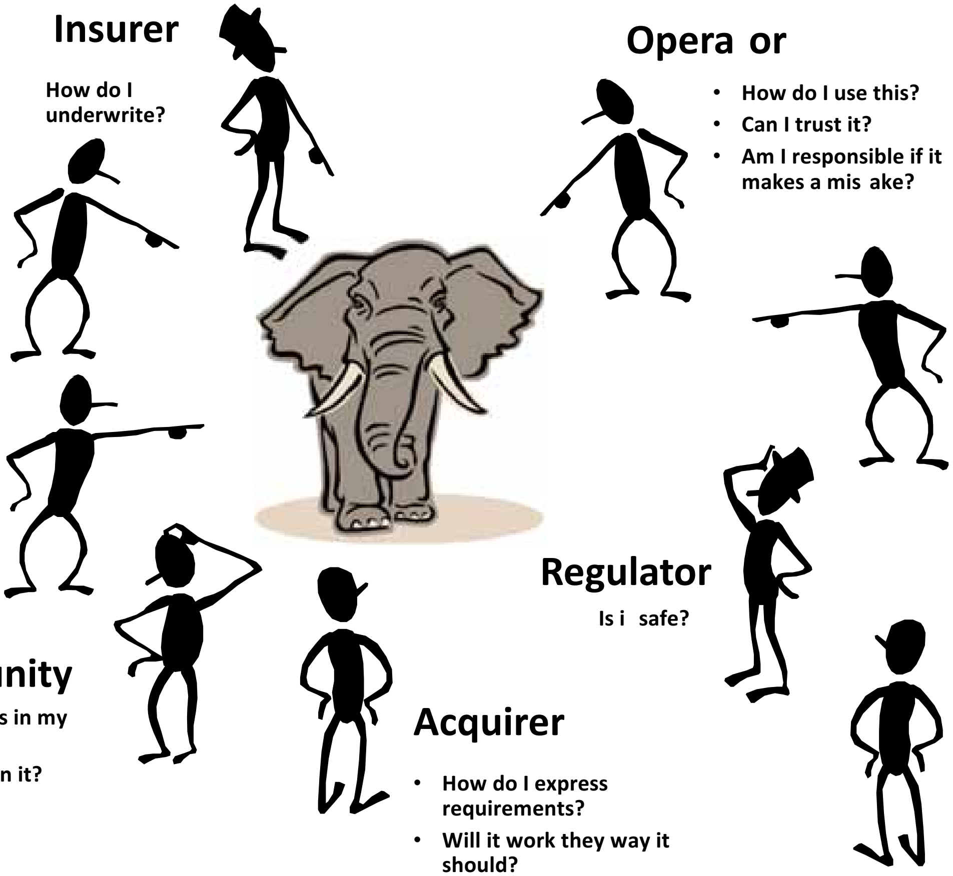
B. Cyber-Physical Risk

RUSTWORTHY SYSTEMS



Approved for Public Rele se; Distribution Unlimited. Case Number 17–3226-002

Pers ectives n Trustw rthiness



Insurer

How do I underwrite?

Researcher

What technology is needed to ensure trust?

Crea or

- How should I design and build?
- Will I be liable for problems?

Community

- Do I want his in my backyard?
- Can I count on it?

Acquirer

- How do I express requirements?
- Will it work they way it should?

Opera or

- How do I use this?
- Can I trust it?
- Am I responsible if it makes a mis ake?

Commander/ Supervisor

- Can I reliably use in operations?
- What changes operationally?

Regulator

Is i safe?

Pa ron

- Is i safe?
- Should I use it?
- Can I count on it?

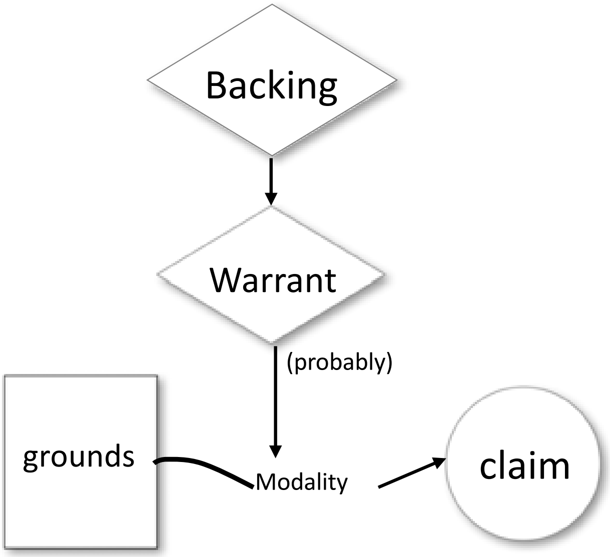
Definition of Assurance Case

A documented body of evidence that provides a convincing and valid argument that a specified set of critical claims regarding a system's properties are adequately justified for a given application in a given environment.

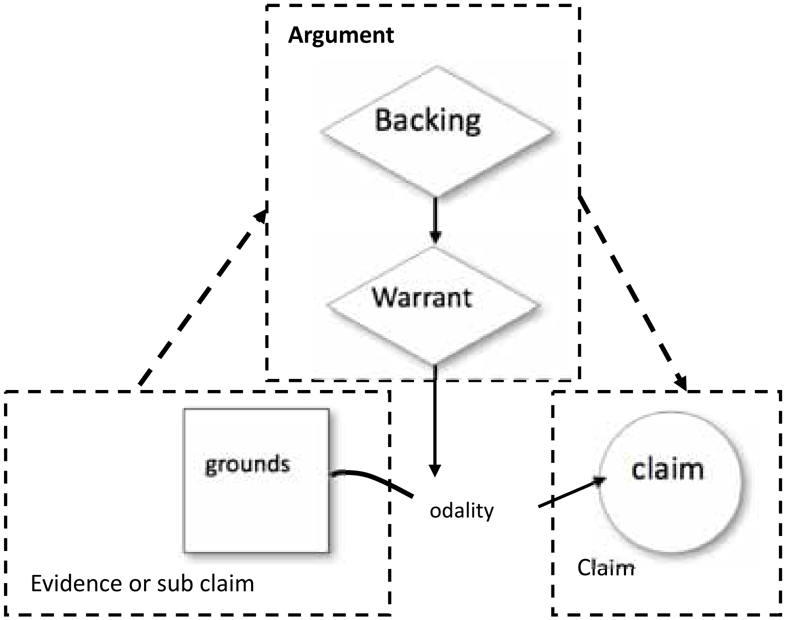
Assuranc Claims with Support o 'Substantial' R asoning

Stephen Toulmin, 1958

- Claims are assertions put forward for general acceptance
- he justification for claim based is on some grounds, the "specific facts about a precise situation that clarify and make good for a claim"
- he basis of the reasoning from the grounds (the facts) to the claim is articulated.
- oulmin coined the term "warrant" for "substantial argument".
- hese are statements indicating the general ways of argument being applied in a particular case and implicitly relied on and whose trustworthiness is well established".
- he basis of the warrant might be questioned, so "backing" for the warrant may be introduced. Backing might be the alidation of the scientific and engineering laws used.

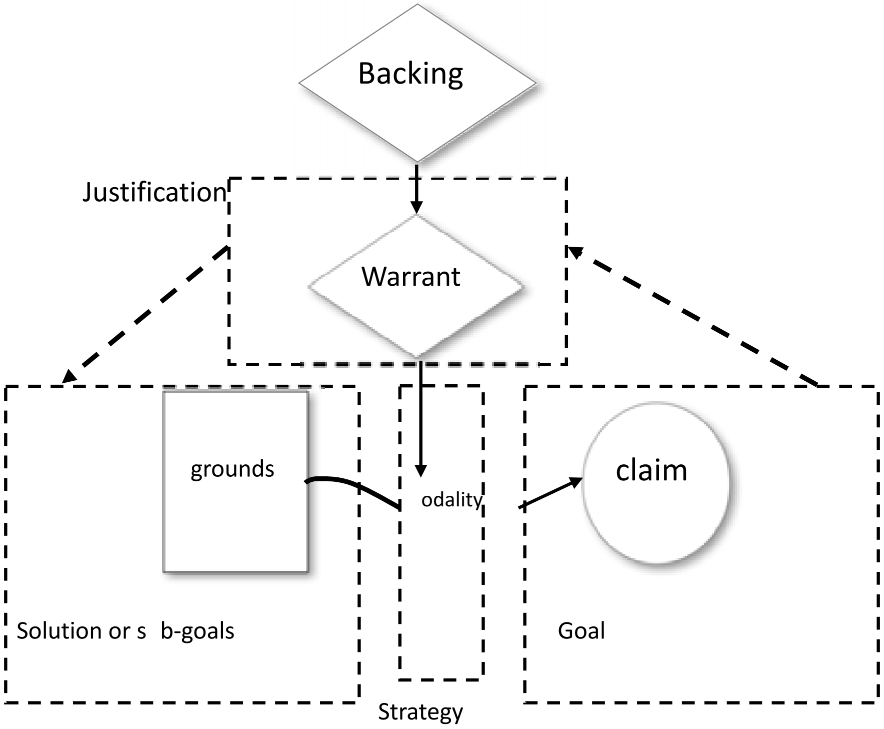


Assurance Claims with Support of ‘Substantial’ Reasoning → two implementations



CAE

Claim, Argument, Evidence



GSN

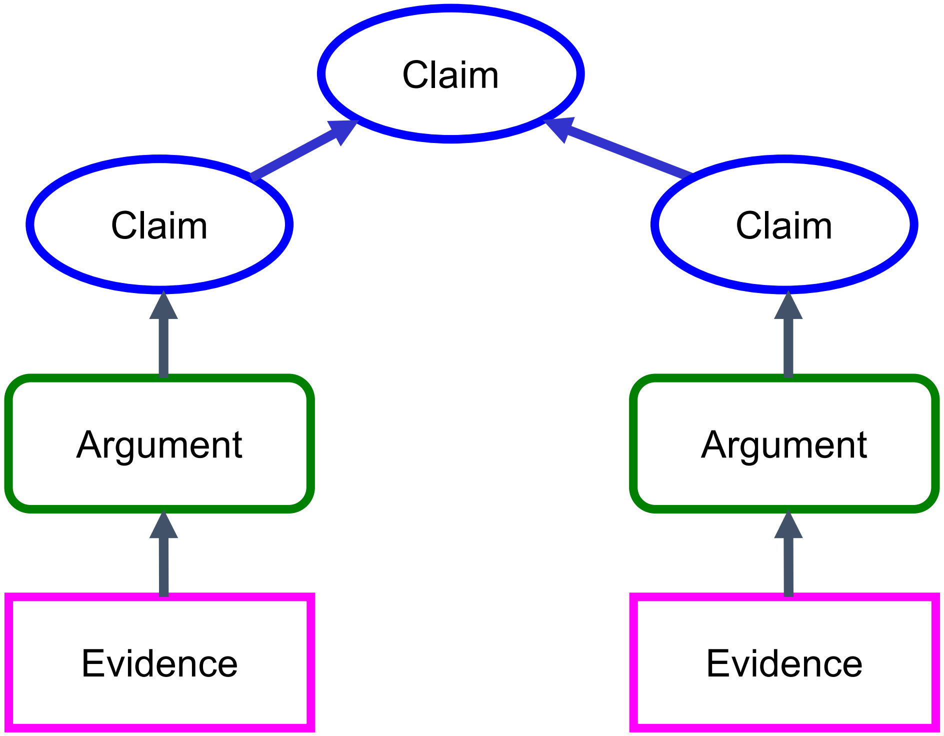
Goal Structuring Notation

Cla ms, Ar uments, and Ev dence

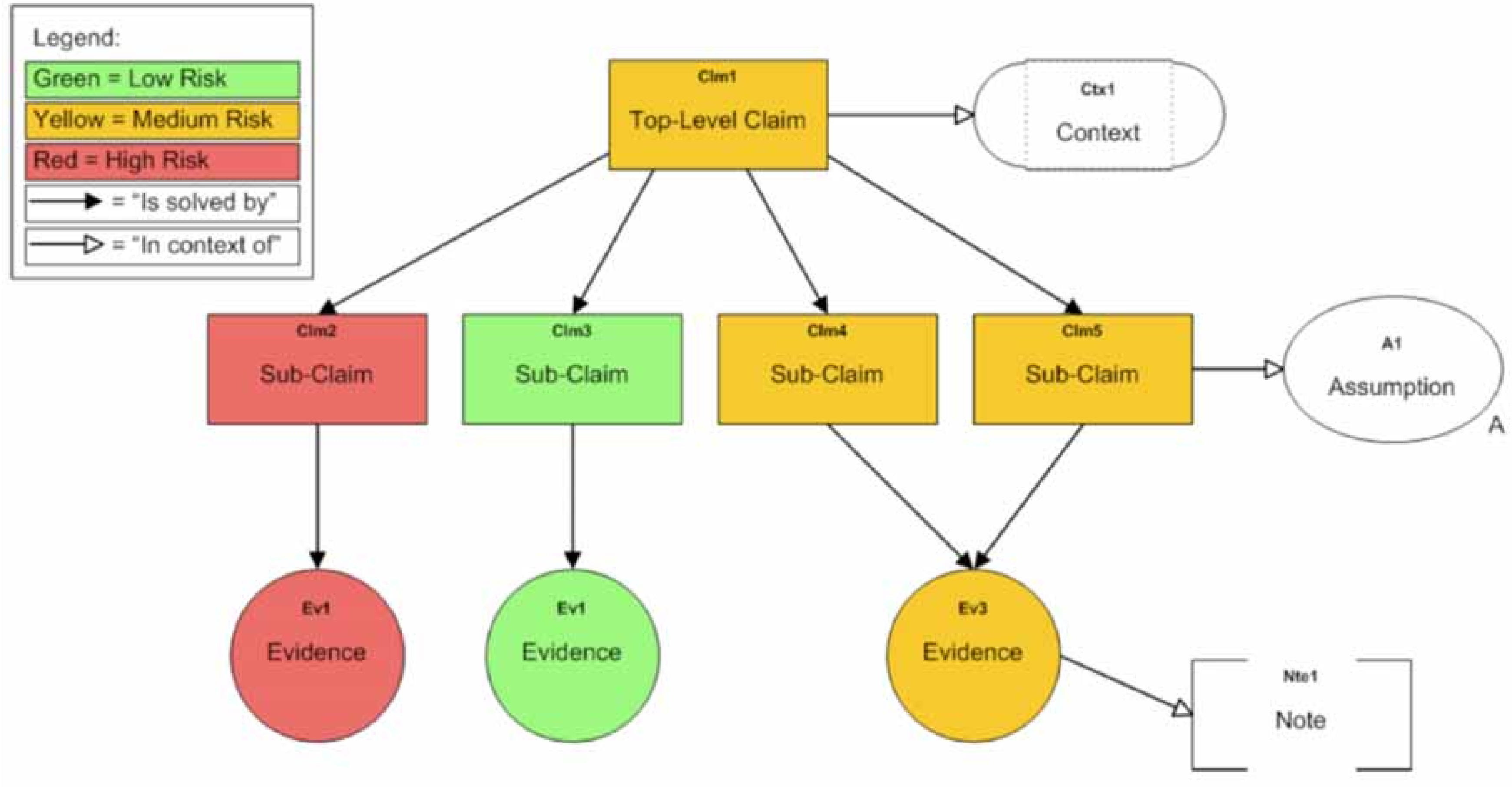
Claim =
assertion to be proven

Argument =
how evidence supports claim

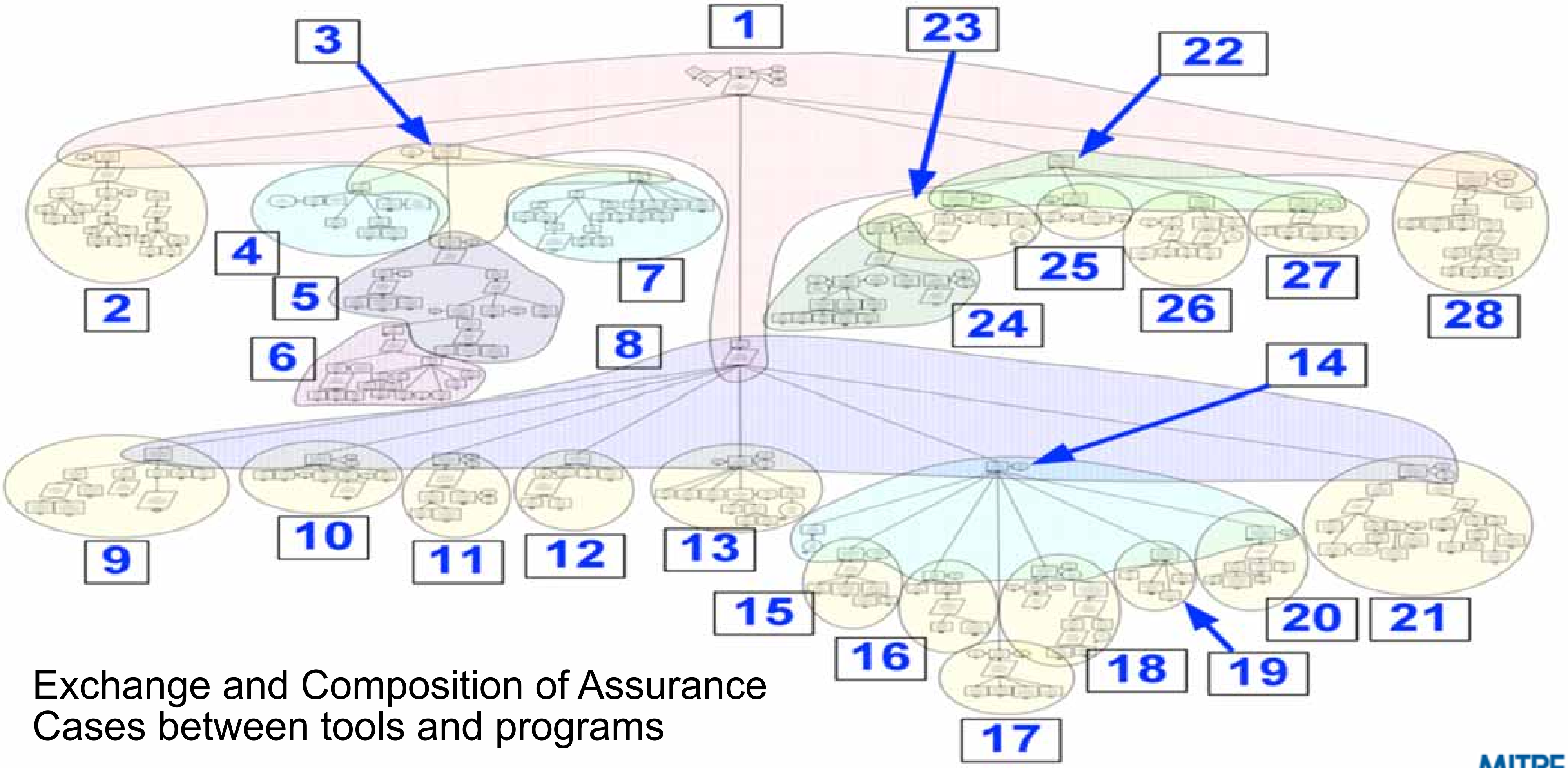
Evidence =
required document tion



S fety C se Tooling –
Cl ims-Eviden e-Argument in Use for <15 Ye rs

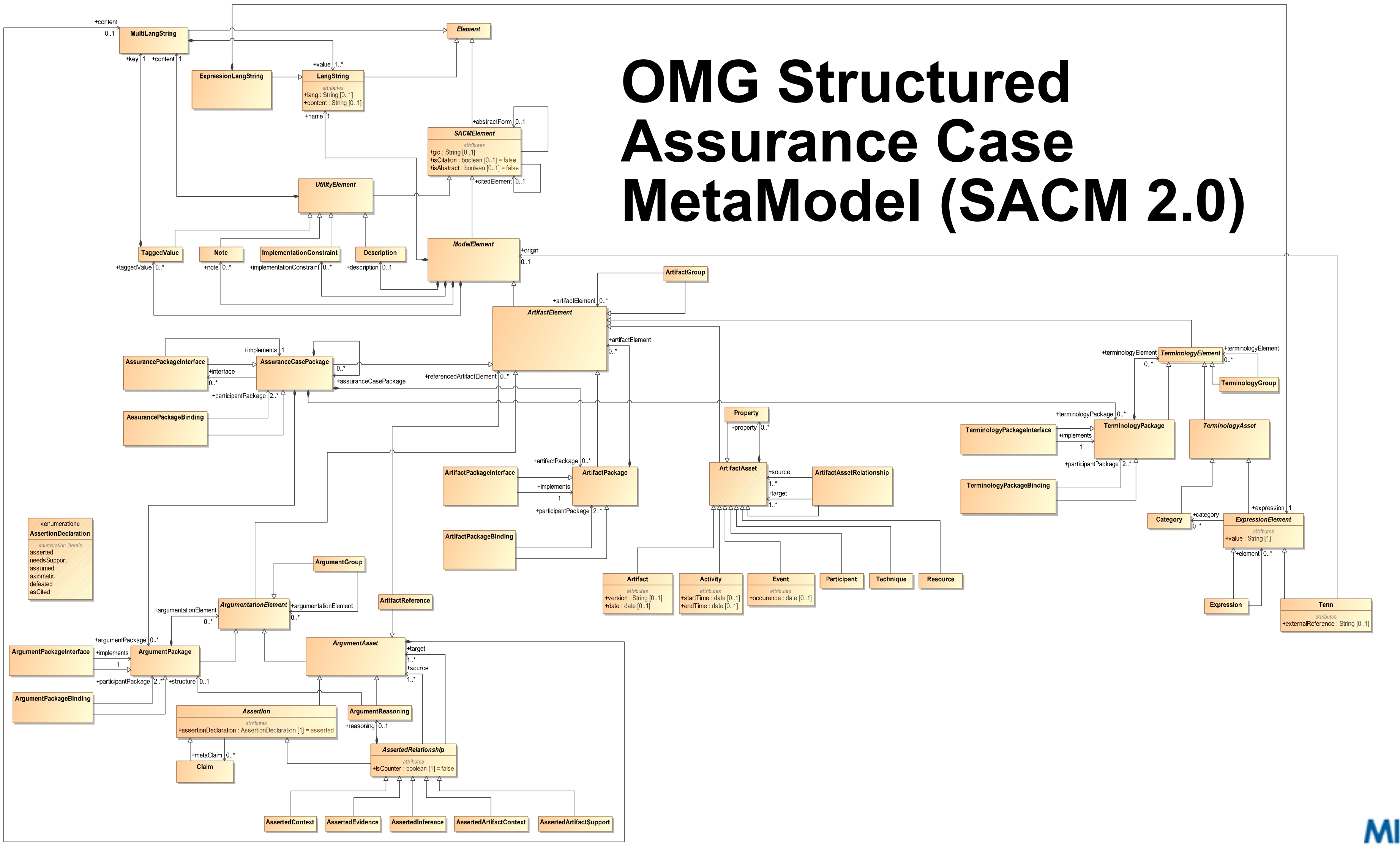


OMG Structured Assurance Case MetaModel



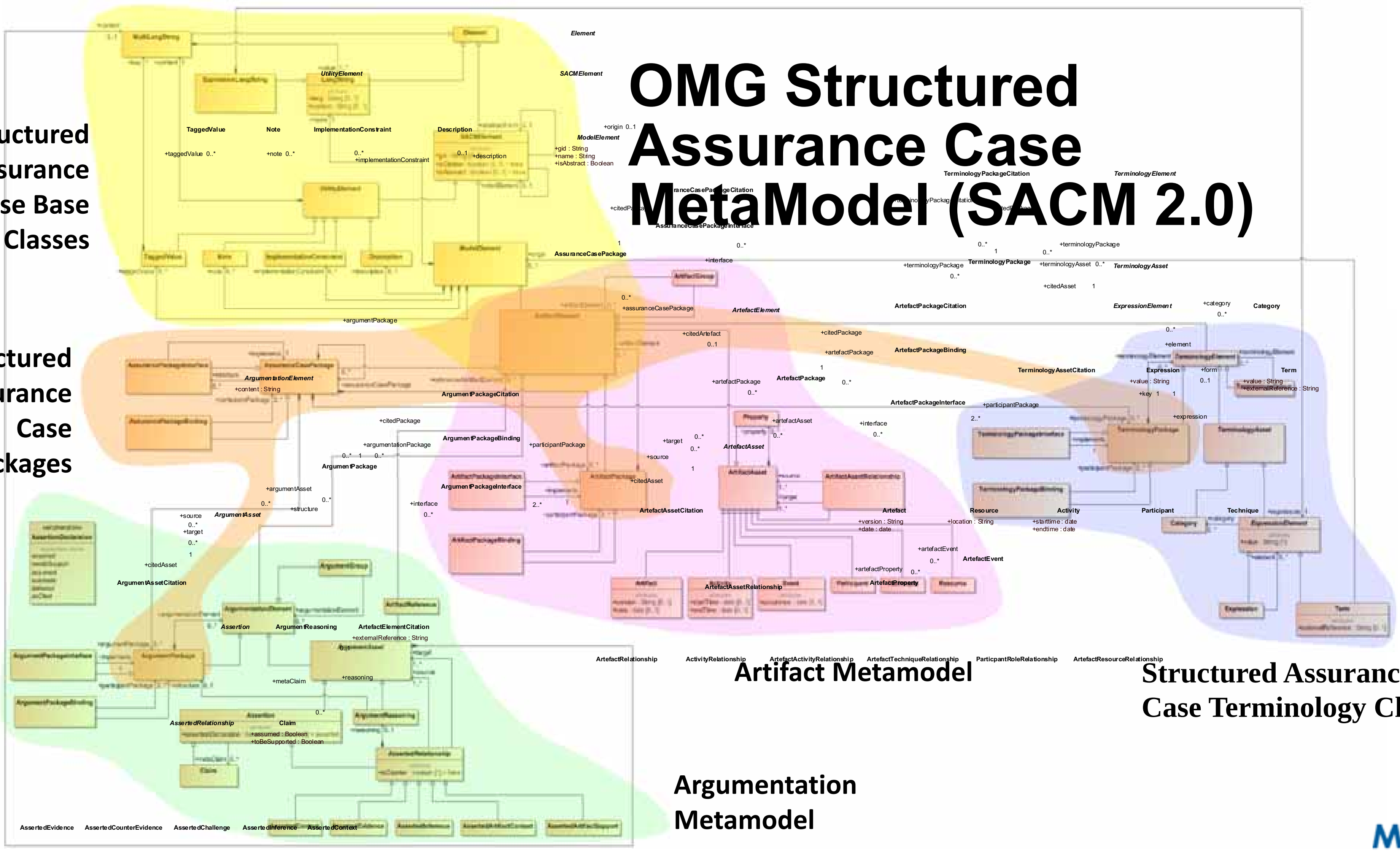
Exchange and Composition of Assurance Cases between tools and programs

OMG Structured Assurance Case MetaModel (SACM 2.0)



MITRE

OMG Structured Assurance Case MetaModel (SACM 2.0)



Structured Assurance Case Base Classes

Structured Assurance Case Packages

Artifact Metamodel

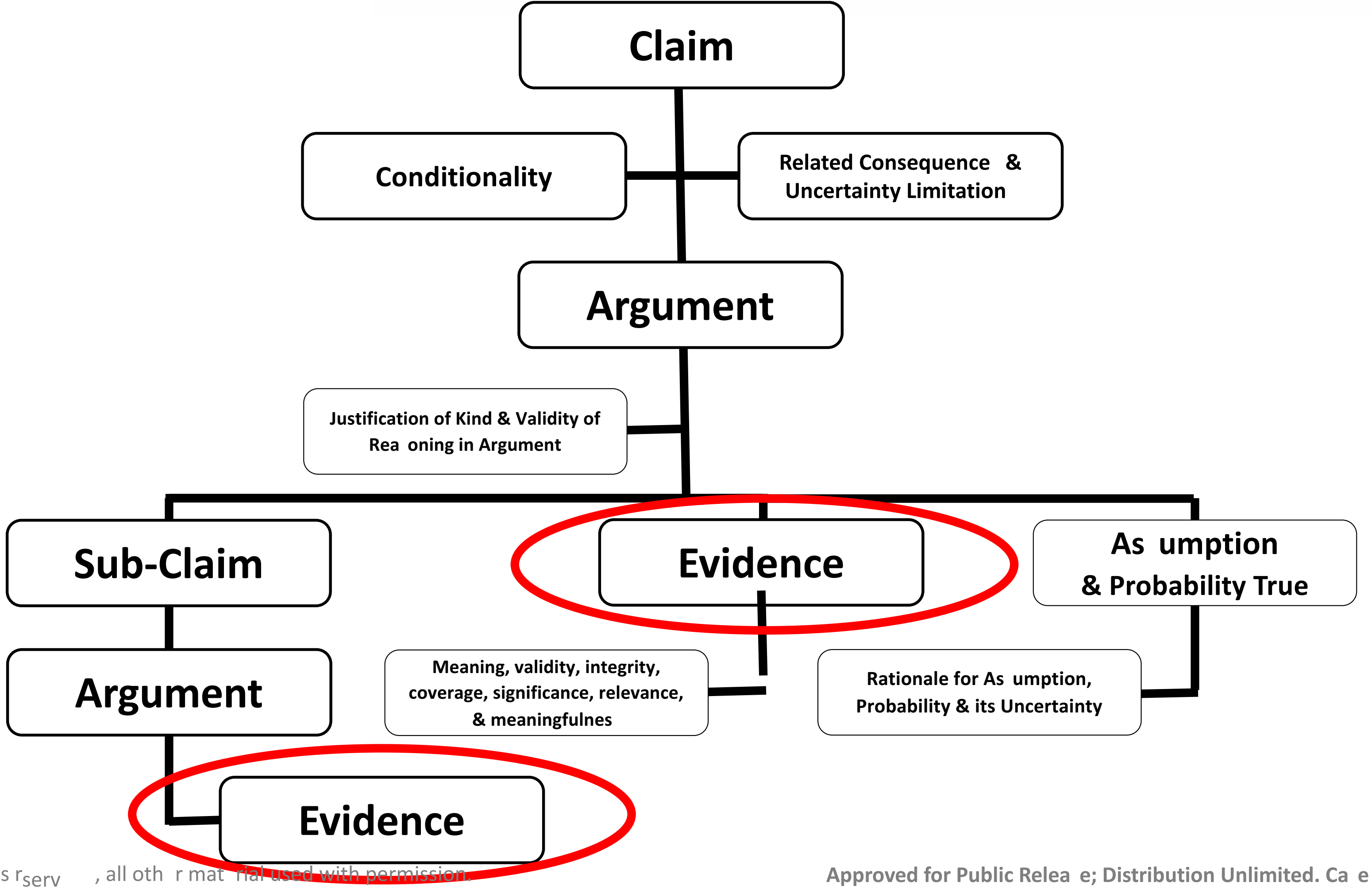
Structured Assurance Case Terminology Classes

Argumentation Metamodel

MITRE

ISO/IEC 15026: Systems & Software Assurance

5026 Part 2: : The Assurance Case (Claims-Evidence-Argument)



Claim

Conditionality

Related Consequence & Uncertainty Limitation

Argument

Justification of Kind & Validity of Rea oning in Argument

Sub-Claim

Evidence

As umption & Probability True

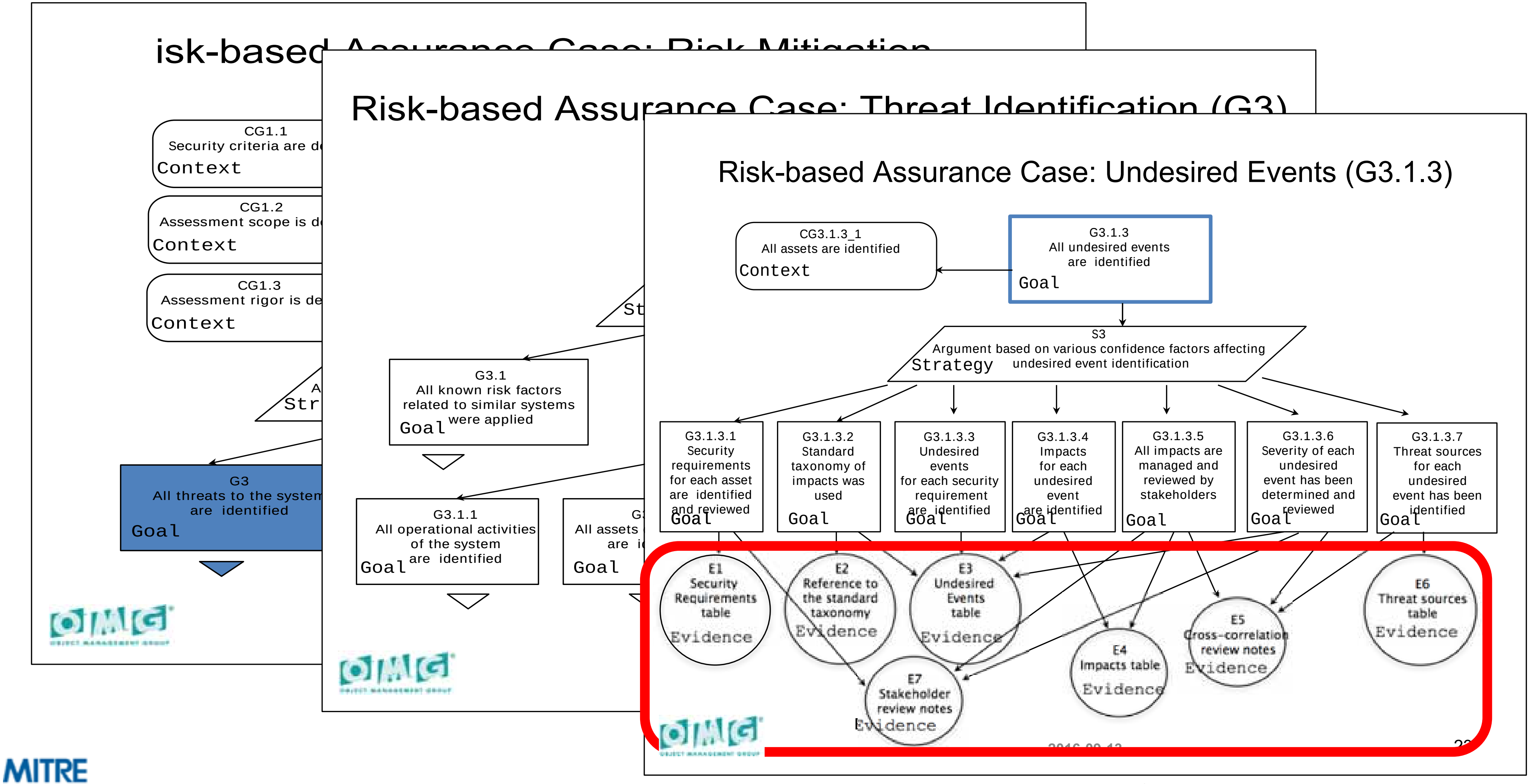
Argument

Meaning, validity, integrity, coverage, significance, relevance, & meaningfulnes

Rationale for As umption, Probability & its Uncertainty

Evidence

Capturing of Complicated Claims-Evidence Relationships



isk-based Assurance Case: Risk Mitigation

CG1.1
Security criteria are d
Context

CG1.2
Assessment scope is d
Context

CG1.3
Assessment rigor is de
Context

A
Str

G3
All threats to the system
are identified
Goal

Risk-based Assurance Case: Threat Identification (G3)

St

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

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

G3
All assets are i
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

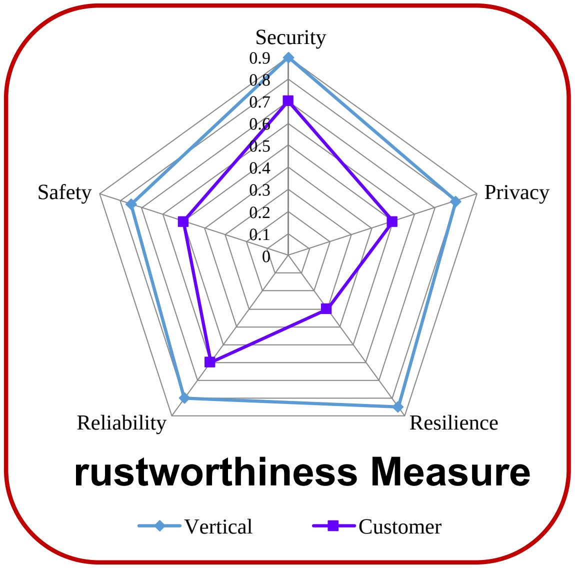
E6
Threat sources table
Evidence

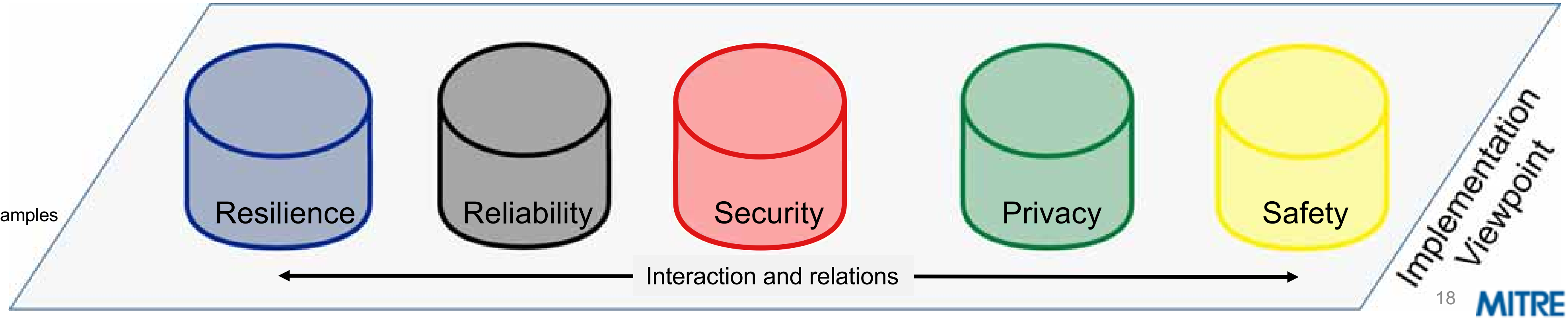
E7
Stakeholder review notes
Evidence

2016-09-13

The Key System Characteristics of rustworthiness as a Quality Measure

- **Industrial IoT Quality is a continuum of system characteristics**
  - OT Safety (IEC 62443*) meets IT Security (ISO 27000*)
  - Privacy (GDPR*), Resilience (ISO*, IEC*), Reliability (NIS*) are quality features in both OT and IT
  - Determine and ensure quality measures per vertical, e.g. audit, certification

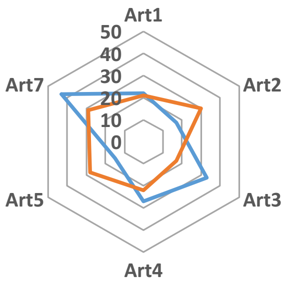




* examples

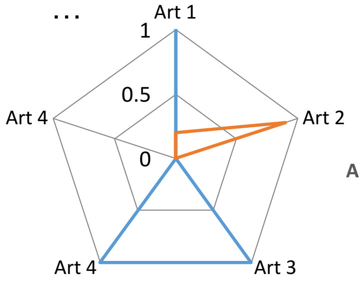
Composition of a Trustworthiness Quality Measure

Resilience*

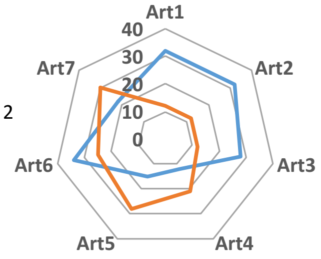


Reliability*

EU: NIS
UK: … (after Brexit)
US: ...
CN: ()
JP: analog NIS
…

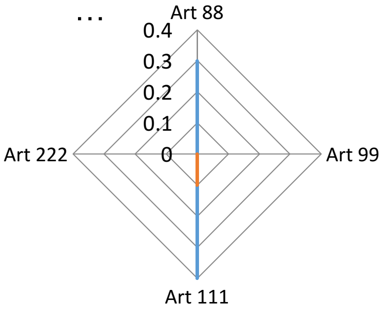


Security*



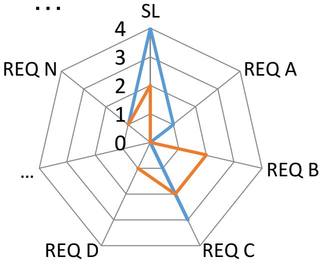
Privacy*

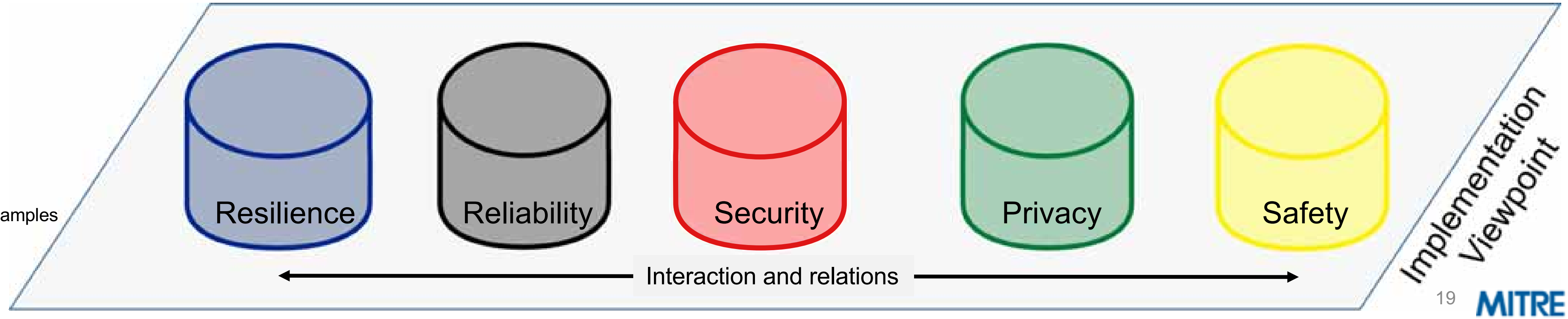
EU: GDPR
UK: … (after Brexit)
US: …
CN: ()
JP: analog GDPR
…



Safety*

EU: IEC 61508/62626
UK: … (after Brexit)
US: IEC 61508
CN: ()
JP: IEC 61508
…

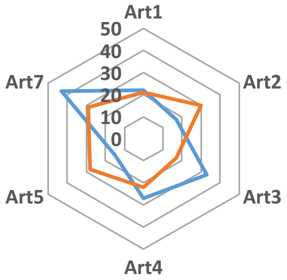




* examples

Evidence of Trustworthiness as Assurance Cases

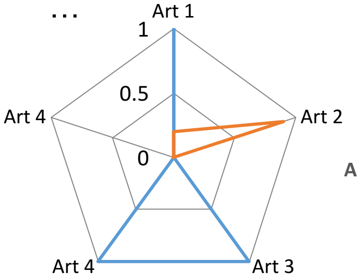
Resilience*



Evidence-based Assurance Case supporting Resilience claims

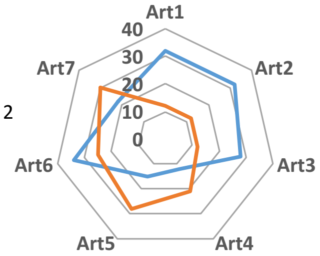
Reliability*

EU: NIS
UK: … (after Brexit)
US: ...
CN: ()
JP: analog NIS
…



Evidence-based Assurance Case supporting Reliability claims

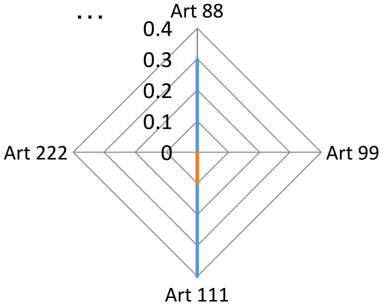
Security*



Evidence-based Assurance Case supporting Security claims

Privacy*

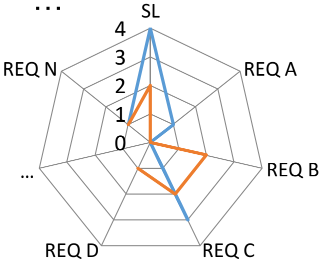
EU: GDPR
UK: … (after Brexit)
US: …
CN: ()
JP: analog GDPR
…



Evidence-based Assurance Case supporting Privacy claims

Safety*

EU: IEC 61508/62626
UK: … (after Brexit)
US: IEC 61508
CN: ()
JP: IEC 61508
…



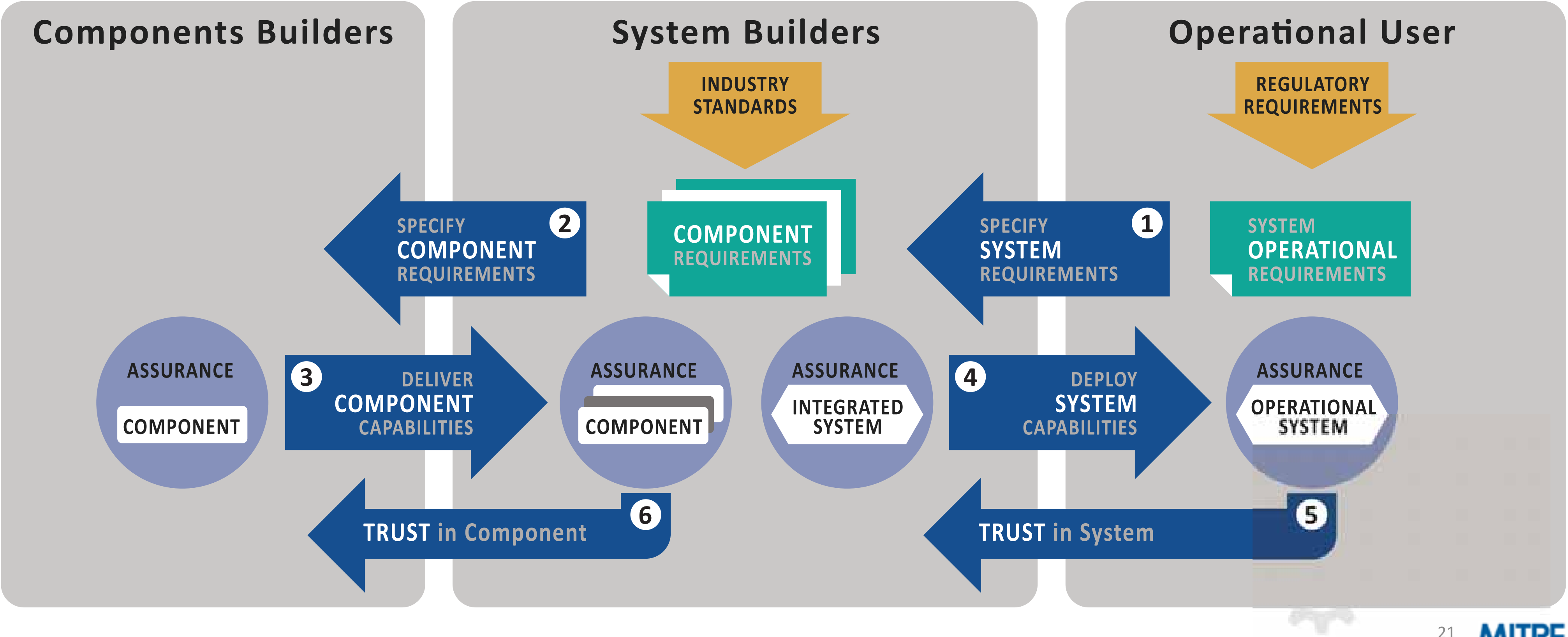
Evidence-based Assurance Case supporting

fety claims

* examples

ERMEATION OF TUST

Chapter 6


Components Builders

System Builders

Operational User

INDUSTRY STANDARDS

REGULATORY REQUIREMENTS

2 SPECIFY COMPONENT REQUIREMENTS

COMPONENT REQUIREMENTS

1 SPECIFY SYSTEM REQUIREMENTS

SYSTEM OPERATIONAL REQUIREMENTS

ASSURANCE COMPONENT

3 DELIVER COMPONENT CAPABILITIES

ASSURANCE COMPONENT

ASSURANCE INTEGRATED SYSTEM

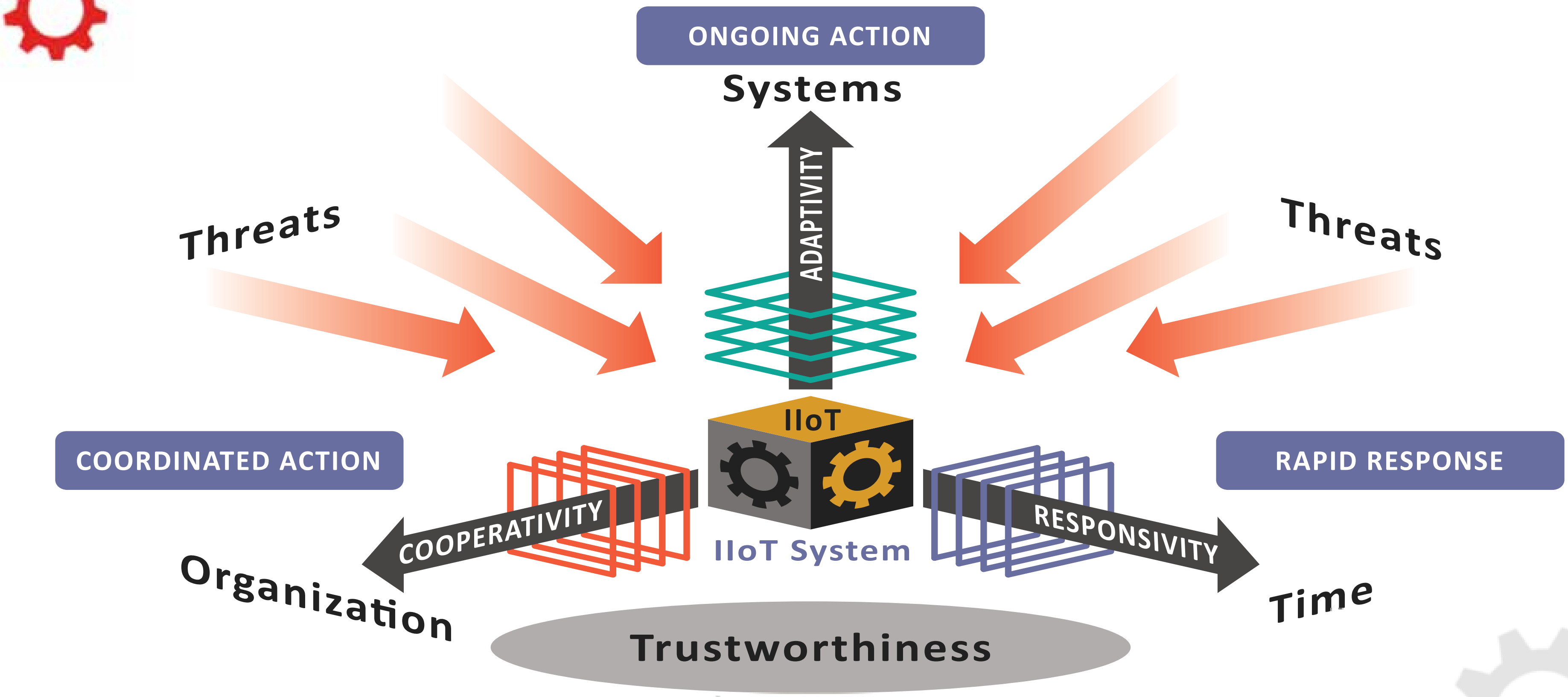
4 DEPLOY SYSTEM CAPABILITIES

ASSURANCE OPERATIONAL SYSTEM

6 TRUST in Component

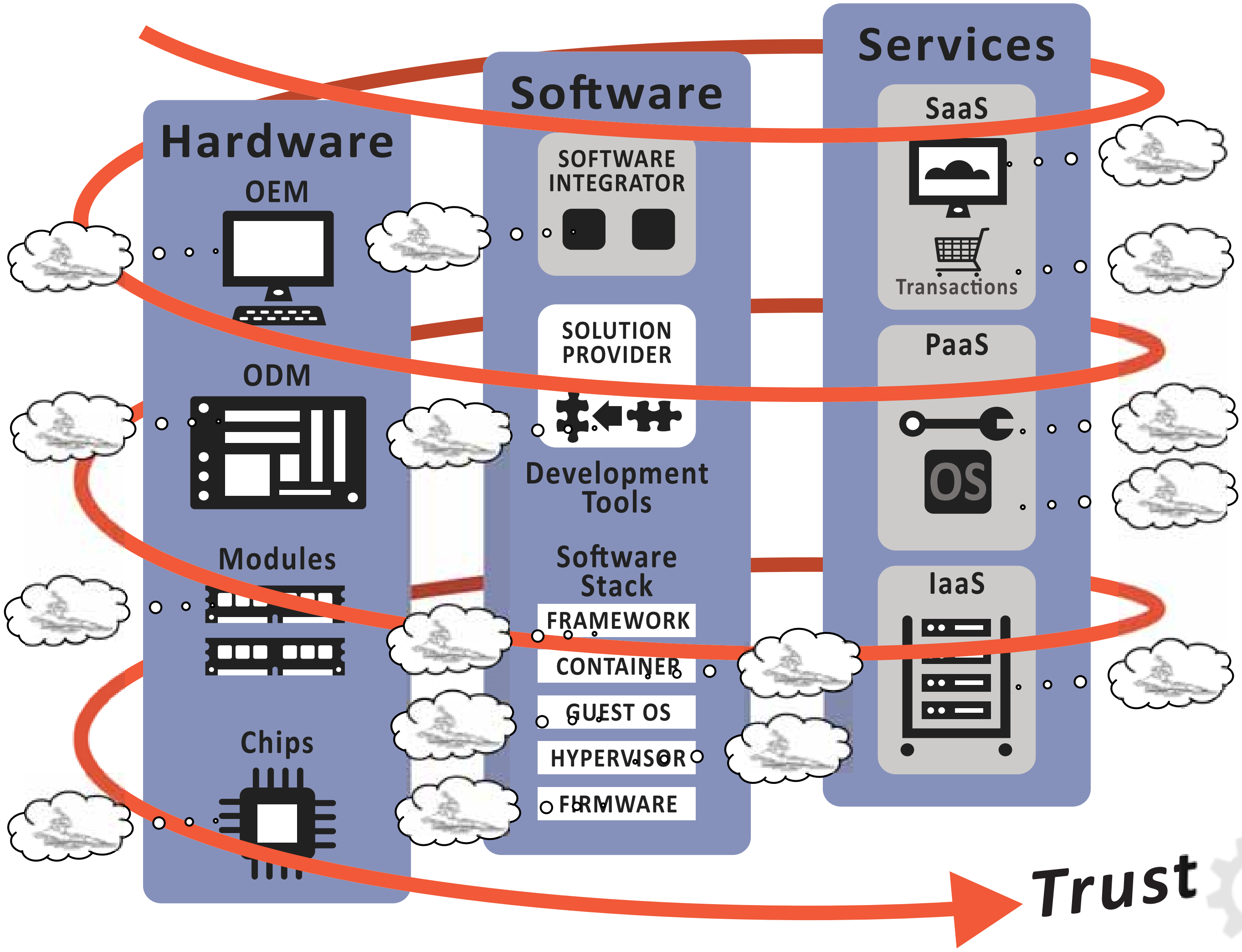
5 TRUST in System

TRUSTWORTHINESS MANAGEMENT CONSIDERATIONS



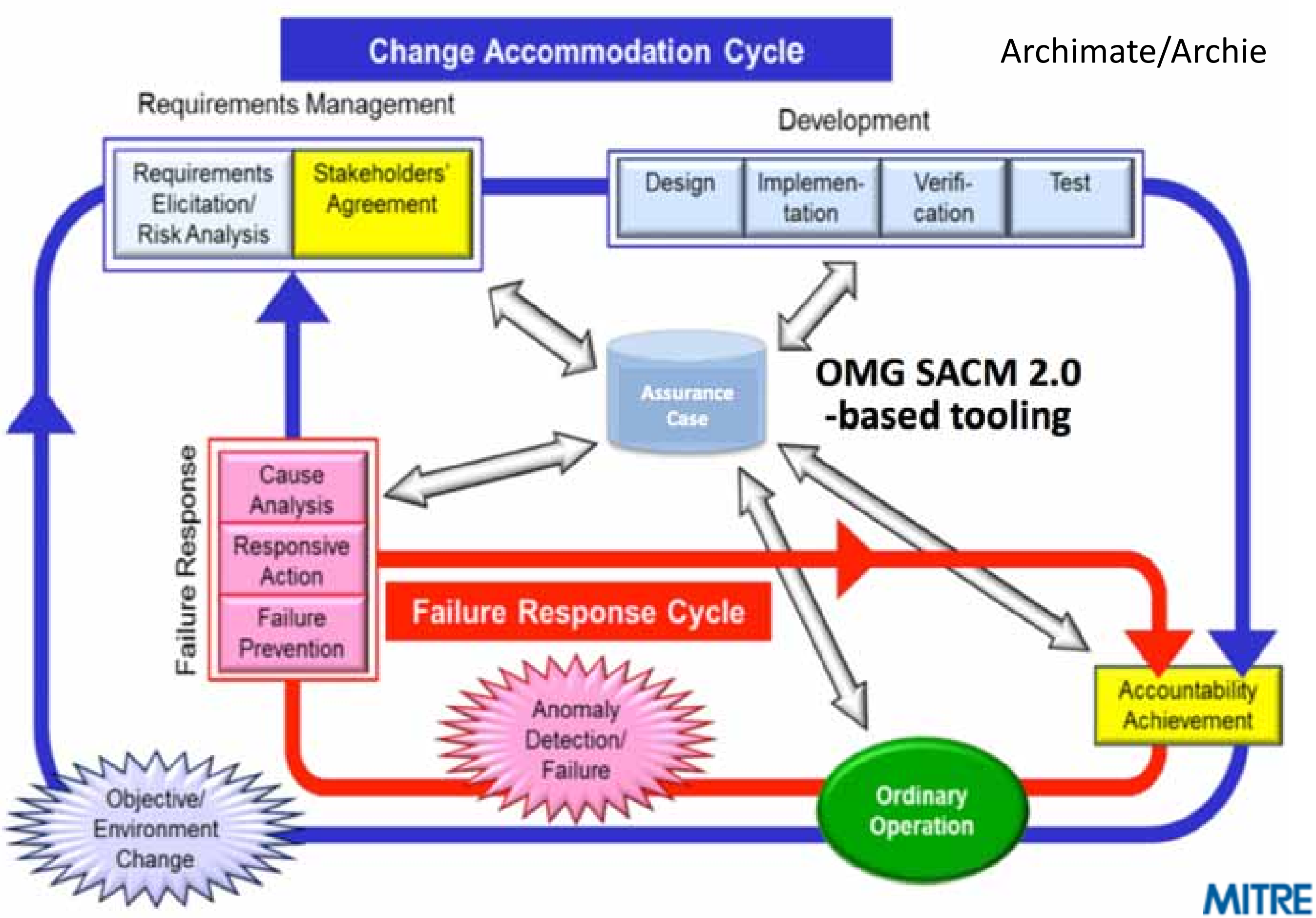
Evidence-based Assurance Case supporting T ustworthiness claims

Trust Relationship between Component Builders



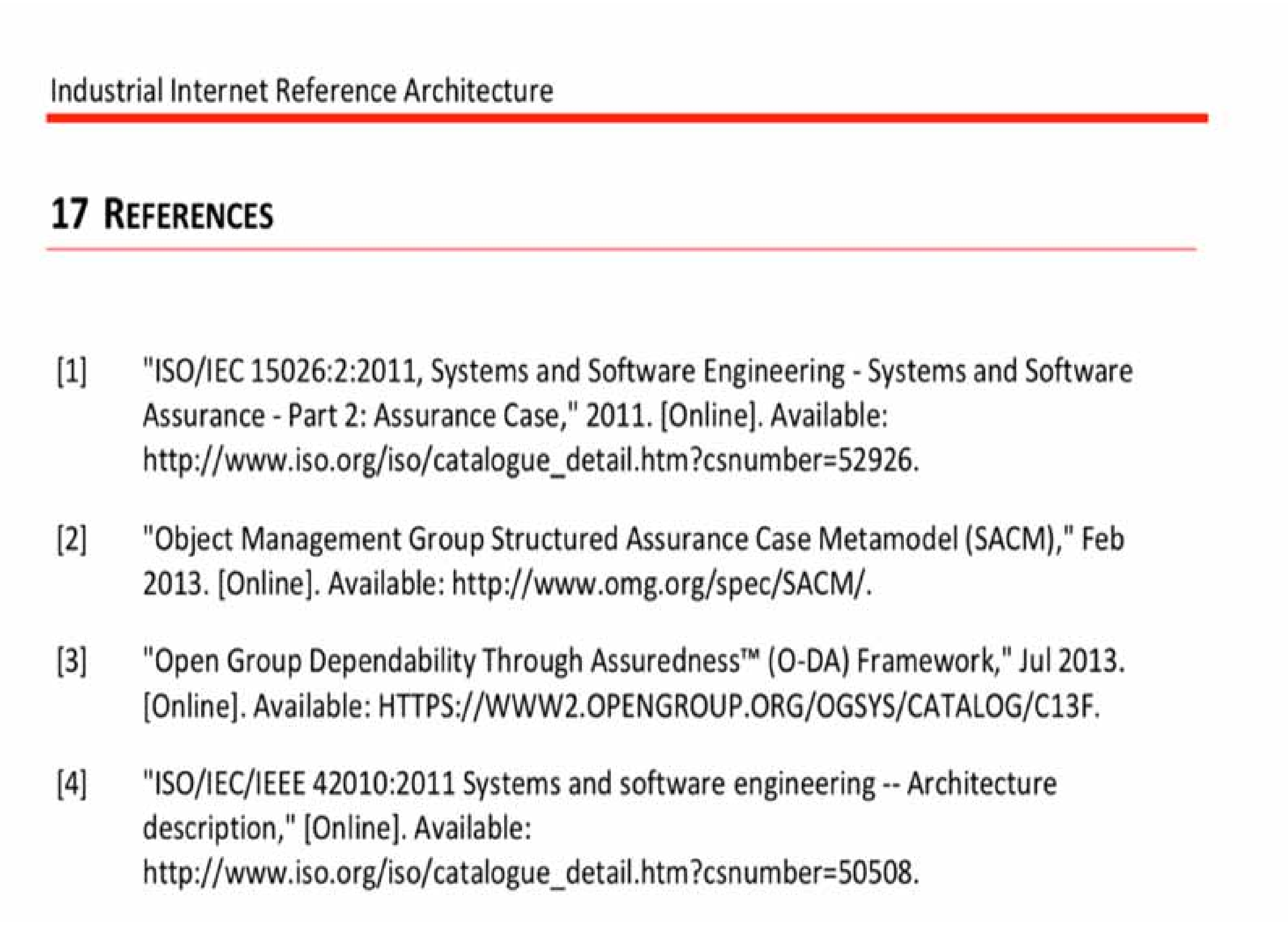
Open Group's Depend bility Fr mework (O-DA): Implied eqts-Design Development Ev lu tion

- Using an Assur nce Case Model to c pture (as claims) the behaviors the resultant system is meant to have
- Tying the evidence developed/collected to the supported claims as an ongoing part of creating and maint ining the system



Archimate/Archie

OMG SACM 2.0 -based tooling



Industrial Internet Reference Architecture

17 References

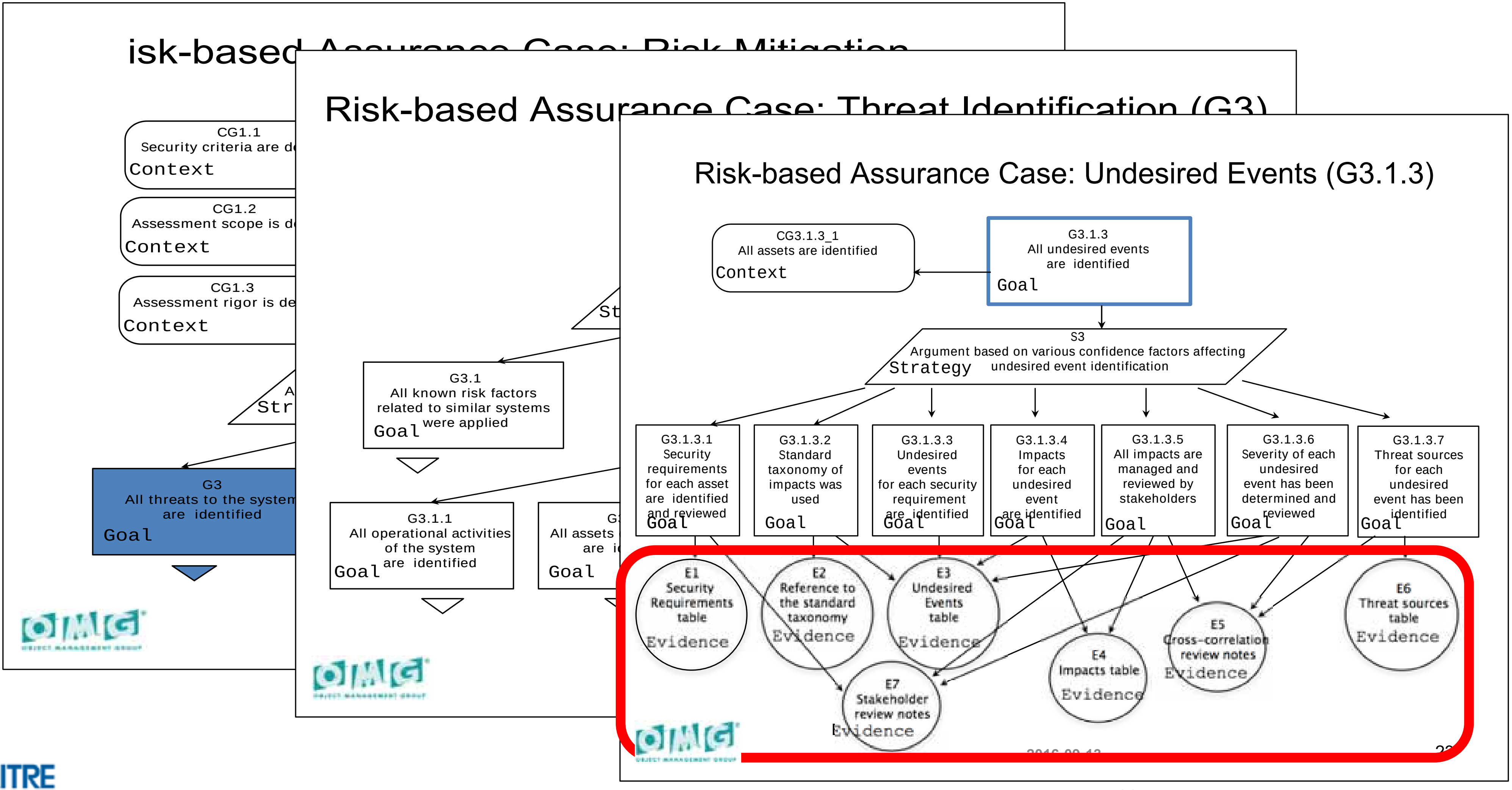
[1] "ISO/IEC 15026:2:2011, Systems and Software Engineering - Systems and Software Assurance - Part 2: Assurance Case," 2011. [Online]. Available: http://www.iso.org/iso/catalogue_detail.htm?csnumber=52926.

[2] "Object Management Group Structured Assurance Case Metamodel (SACM)," Feb 2013. [Online]. Available: http://www.omg.org/spec/SACM/.

[3] "Open Group Dependability Through Assuredness™ (O-DA) Framework," Jul 2013. [Online]. Available: HTTPS://WWW2.OPENGROUP.ORG/OGSYS/CATALOG/C13F.

[4] "ISO/IEC/IEEE 42010:2011 Systems and software engineering -- Architecture description," [Online]. Available: http://www.iso.org/iso/catalogue_detail.htm?csnumber=50508.

Capturing of Complicated Claims-Evidence Relationships



isk-based Assurance Case: Risk Mitigation

CG1.1
Security criteria are d
Context

CG1.2
Assessment scope is d
Context

CG1.3
Assessment rigor is de
Context

A
Str

G3
All threats to the system
are identified
Goal

Risk-based Assurance Case: Threat Identification (G3)

St

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

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

G3
All assets are i
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

E7
Stakeholder review notes
Evidence

E4
Impacts table
Evidence

E5
Cross-correlation review notes
Evidence

E6
Threat sources table
Evidence

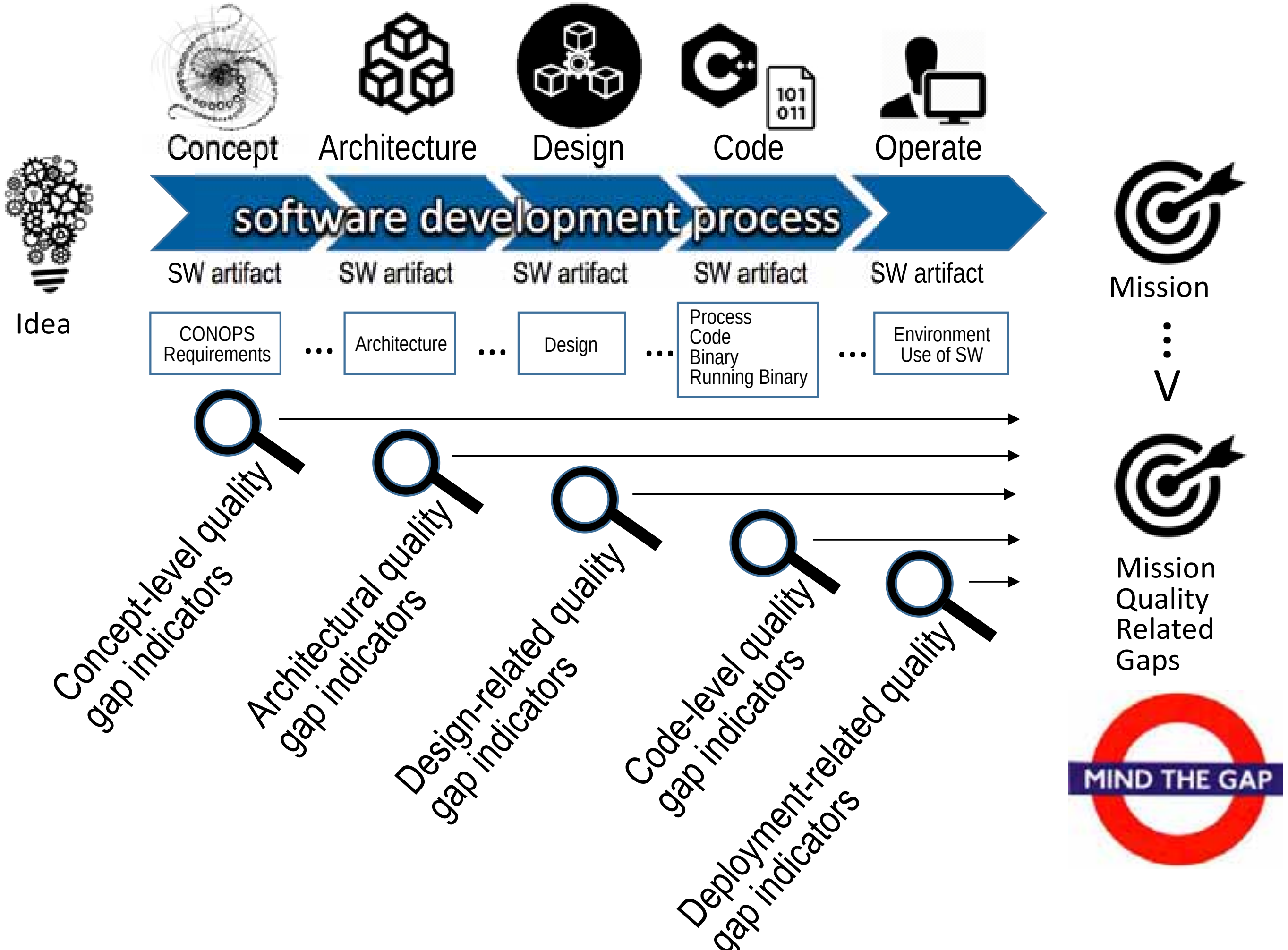
2016-09-13

22

MITRE

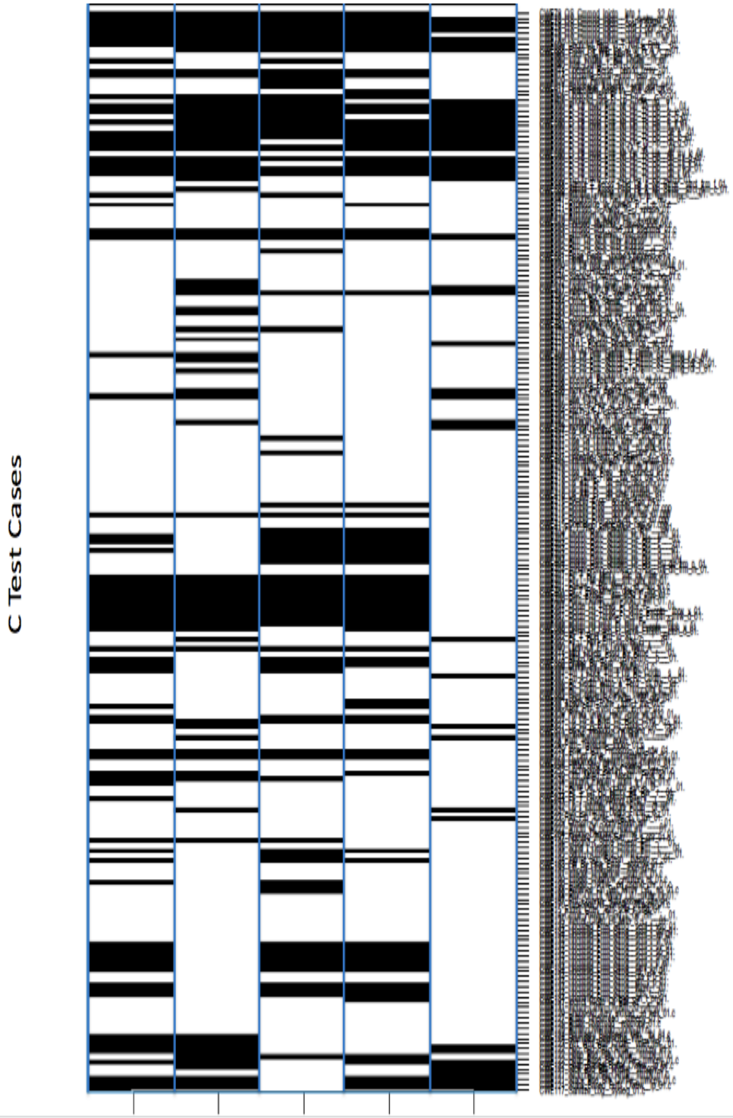
Approved for Public Rele se; Distri ut ion Unlimited. Case Nume r 17–3226-002

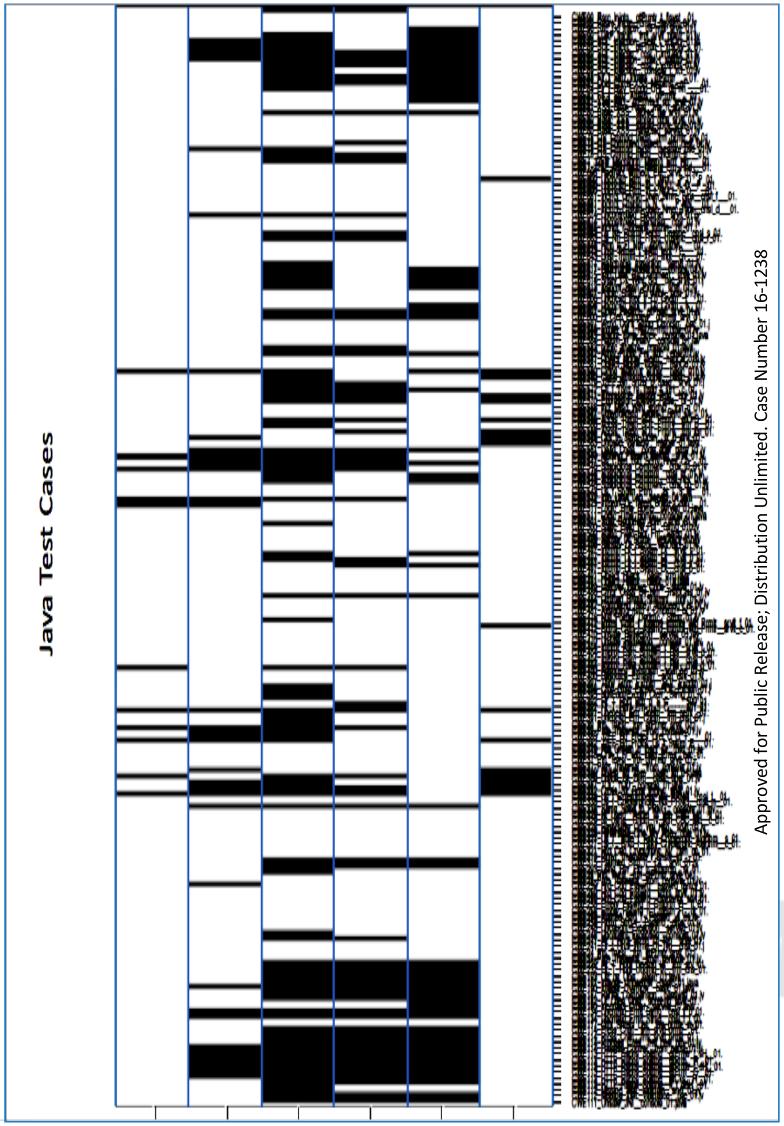
Id nti ying Quality Issu s Through th Li cycl



- Secure
- Safe
- Maintainable
- Portable
- Usable
- Performant
- esilient
- eliable

Approved for Public Rele se; Distribution Unlimited. Case Number 17–3226-002

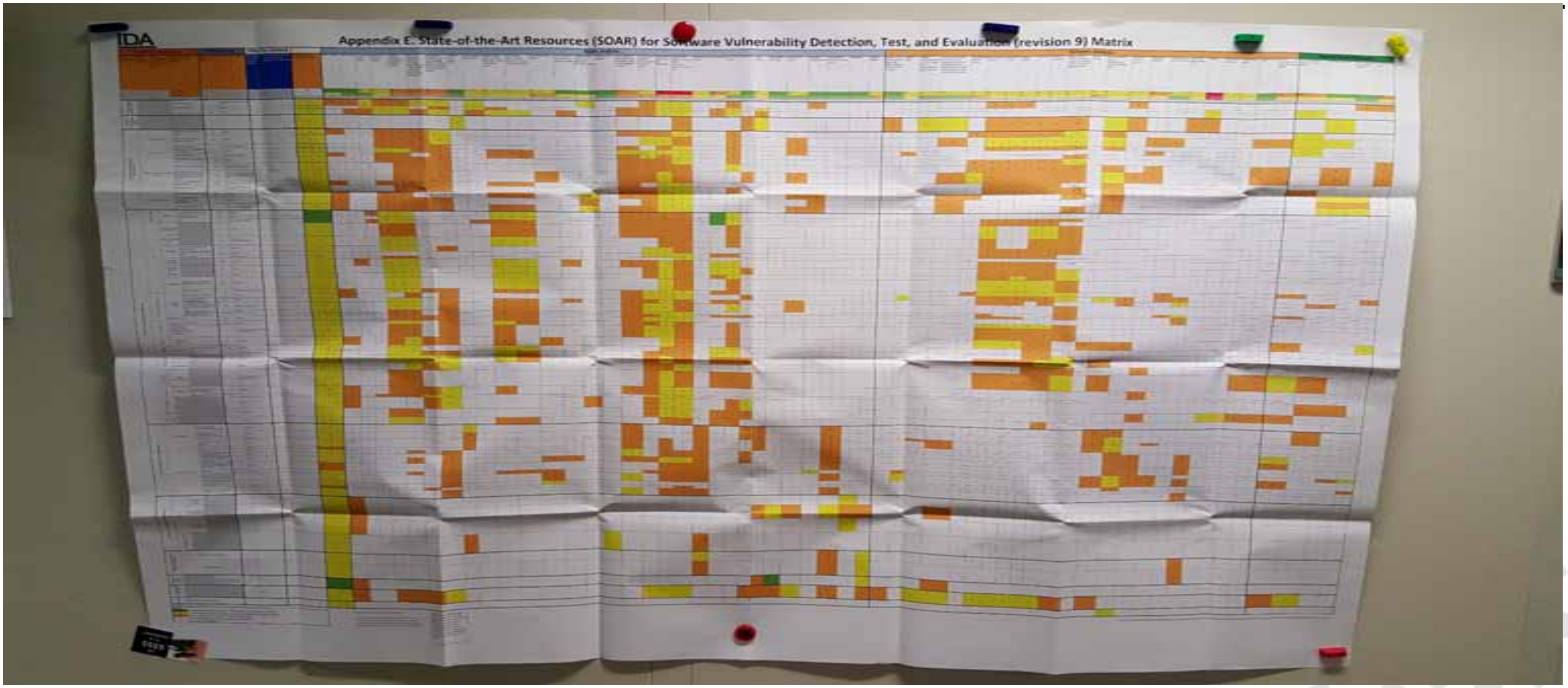




Approved for Public Release; Distribution Unlimited. Case Number 16-1238

Approved for Public Rele se; Distribution Unlimited. Case Number 17–3226-002

Institut   or D   ns   Analysis (IDA)
Stat   o th   Art R port (SOAR)



IDA
Appendix E: State-of-the-Art Resources (SOAR) for Software Vulnerability Detection, Test, and Evaluation (revision 9) Matrix

http://www.acq.osd.mil/se/docs/P-5061-software-soar-mobility-Final-Full-Doc-20140716.pdf
http://www.acq.osd.mil/se/docs/P-5061-AppendixE-soar-sw-matrix-v9-mobility.xls

Approved for Public Rele se; Distribution Unlimited. Case Number 17–3226-002

Utilizing Appropriate Detection Methods to Collect Needed Evidence to Gain Assurance…

Artifacts

CONOPS

Requirements

Architecture

Design

Process

Code

Binary

Running Binary

Environ ent of Syste

Use of Mission Software

Detection Methods

Design Review

Code Review

Attack Surface Analysis

Static Analysis Tool A

Static Analysis Tool B

Dynamic Analysis Tool C

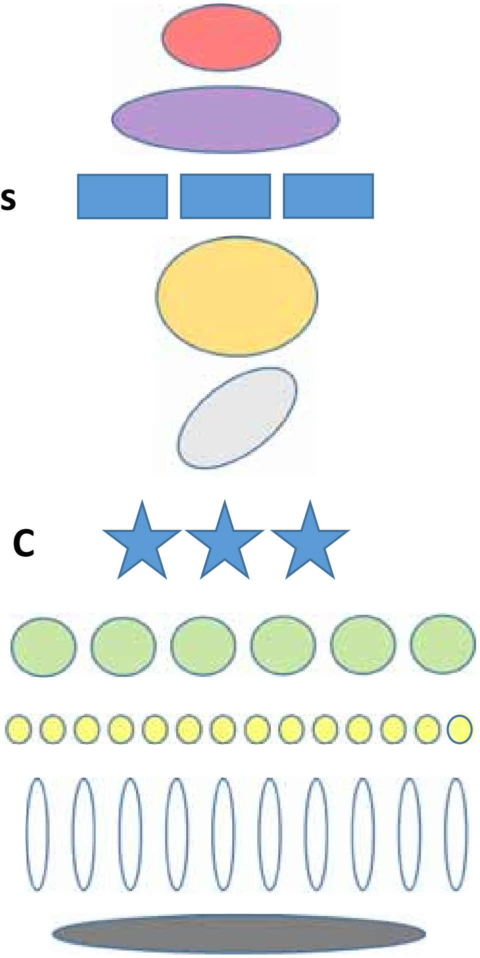
Fuzz Testing

Pen Testing

Blue Teaming

Red Tea ing

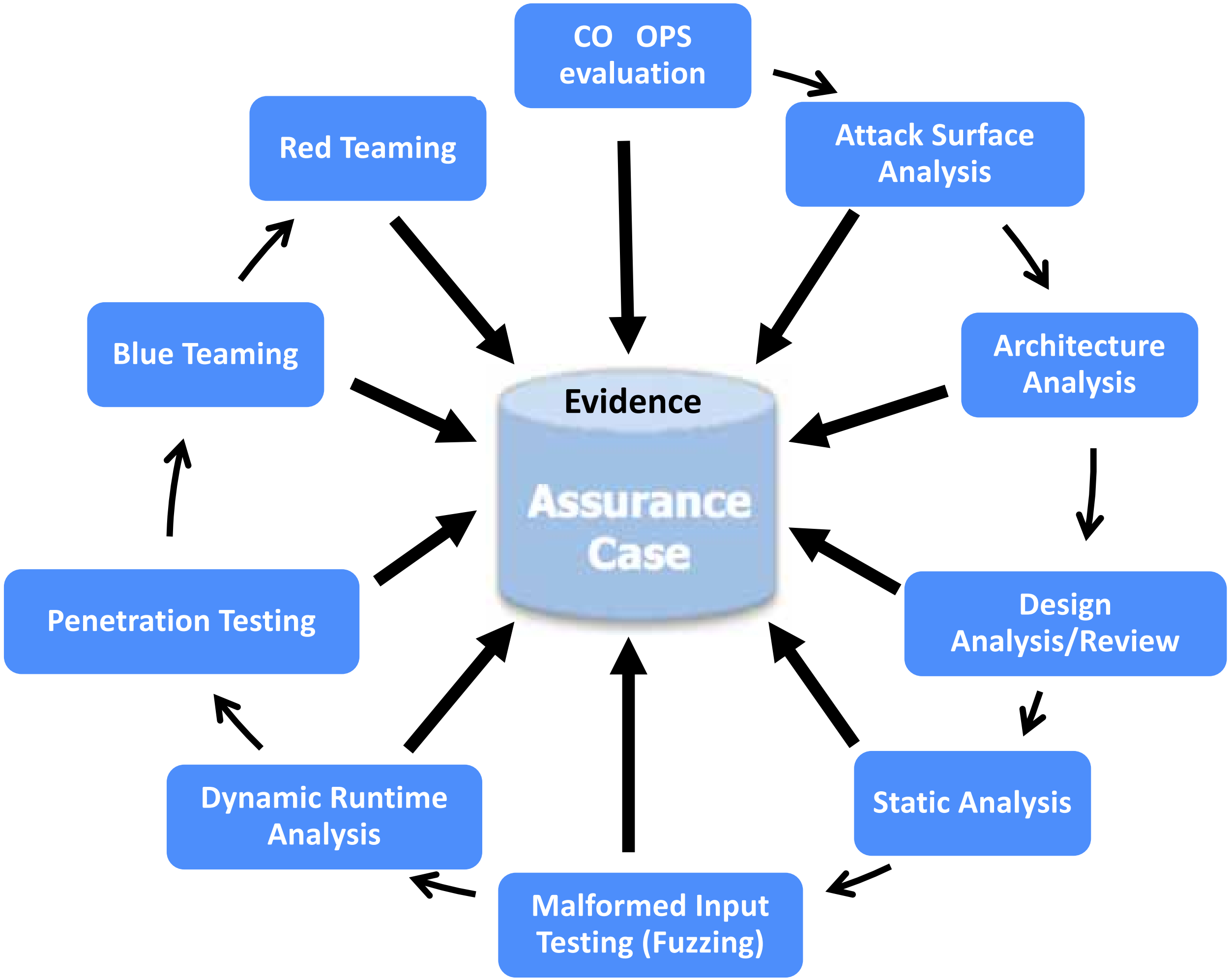
Coverage



CVE,
CWE,
CAPEC, …

Most
Important
Quality
ssues

Multiple Sources of Assurance Evidence from Throughout the Lifecycle of the item(s) needing Assurance.



Questions?