

# Clarity & Conciseness in Due Diligence Relevant Communications

**Robert A. Martin**

Senior Principal Engineer

Cyber Security Center

Center for National Security

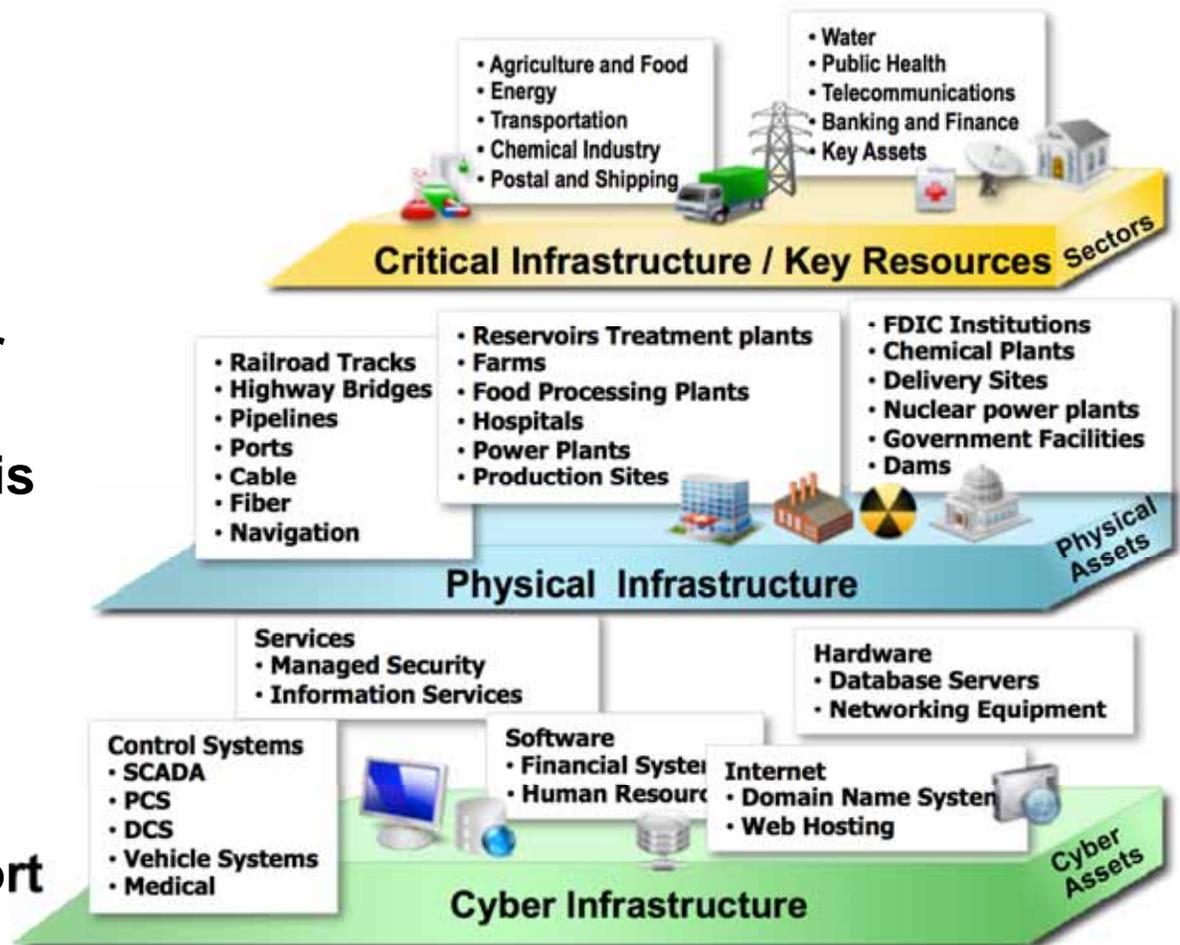
The MITRE Corporation



**MITRE**

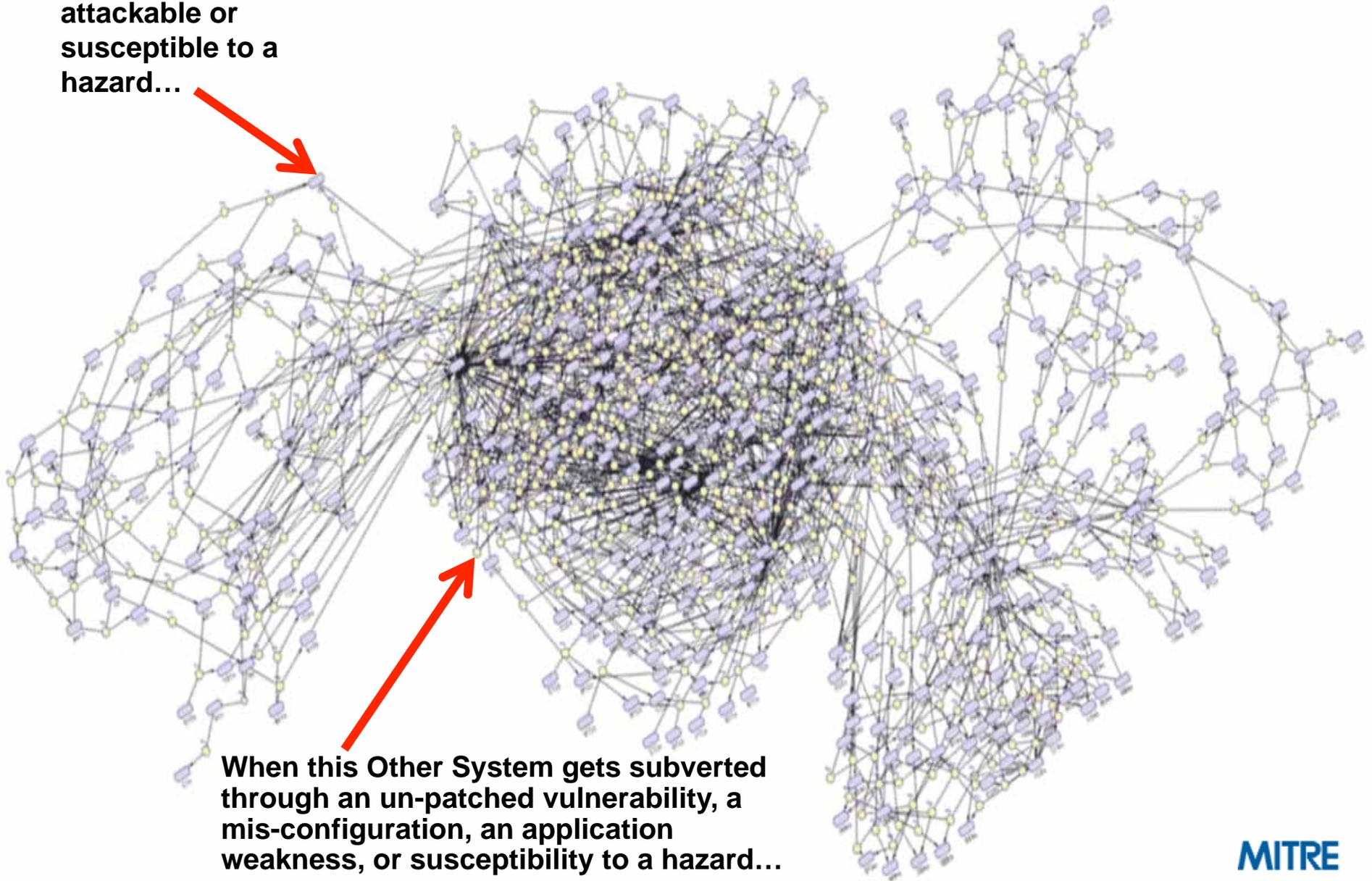
# Today's Reality – We need confidence in our software-enabled cyber capabilities and we need to be able communicate about that...

- Dependencies on software-enabled cyber technology is greater than ever
- Possibility of disruption is greater than ever because hardware/ software is vulnerable
- Loss of confidence alone can lead to stakeholder actions that disrupt critical business and support activities

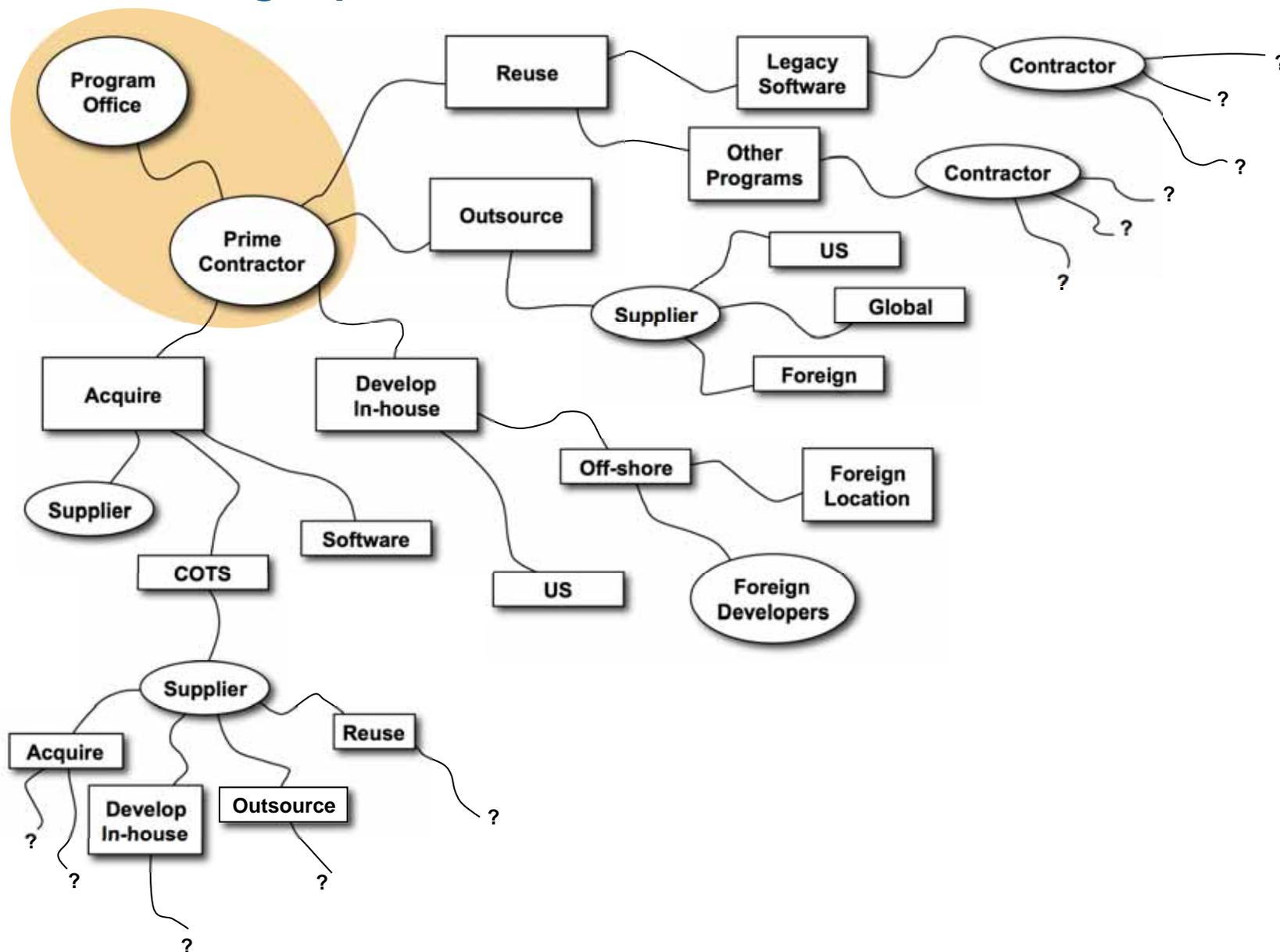


# Everything's Cyber Connected and Co-Dependent

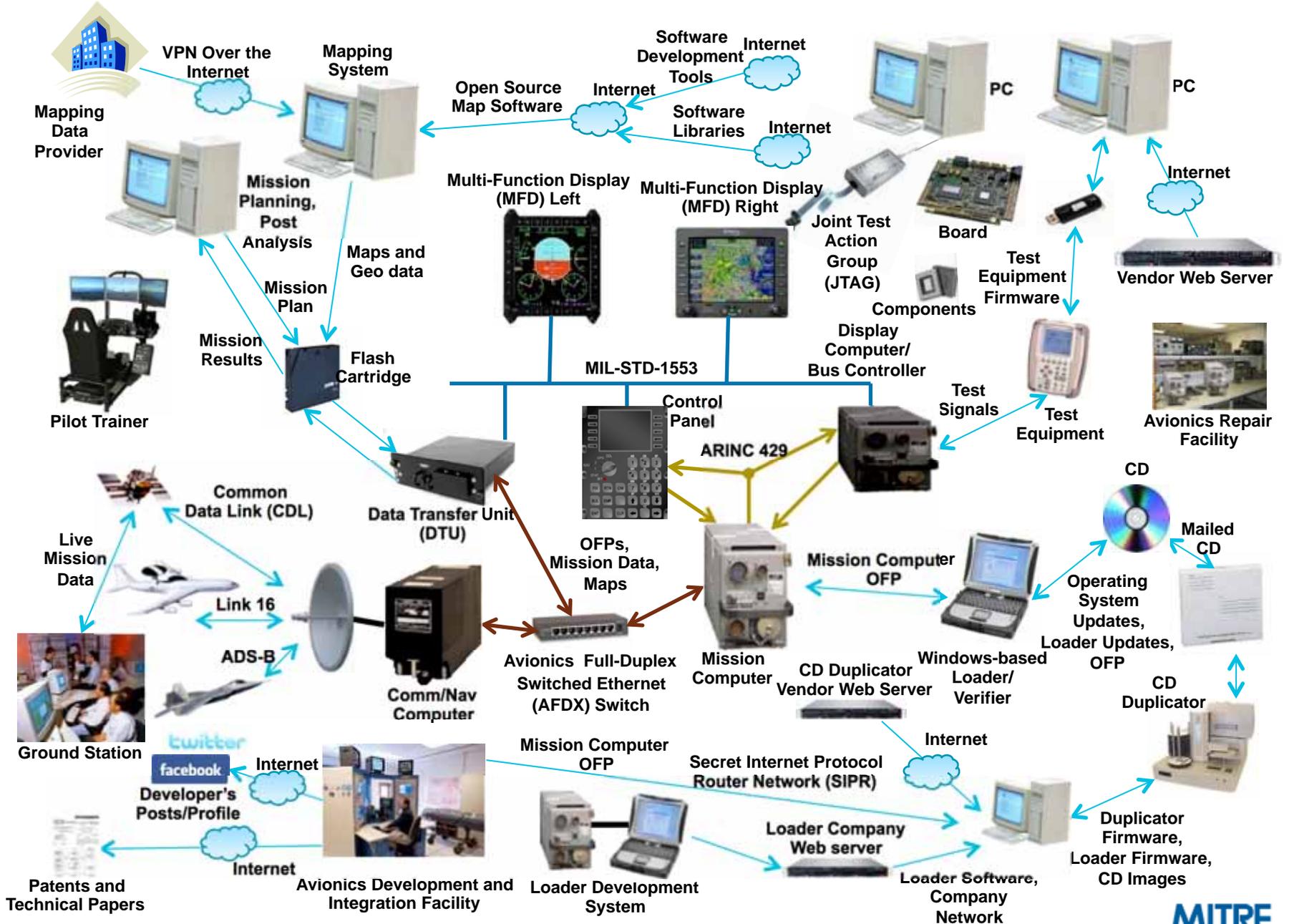
**Your System is  
attackable or  
susceptible to a  
hazard...**



# Everything's Cyber Connected and Co-Dependent Either during Operations or the Other Phases of its Life



# Everything is Cyber Connected and Co-Dependent

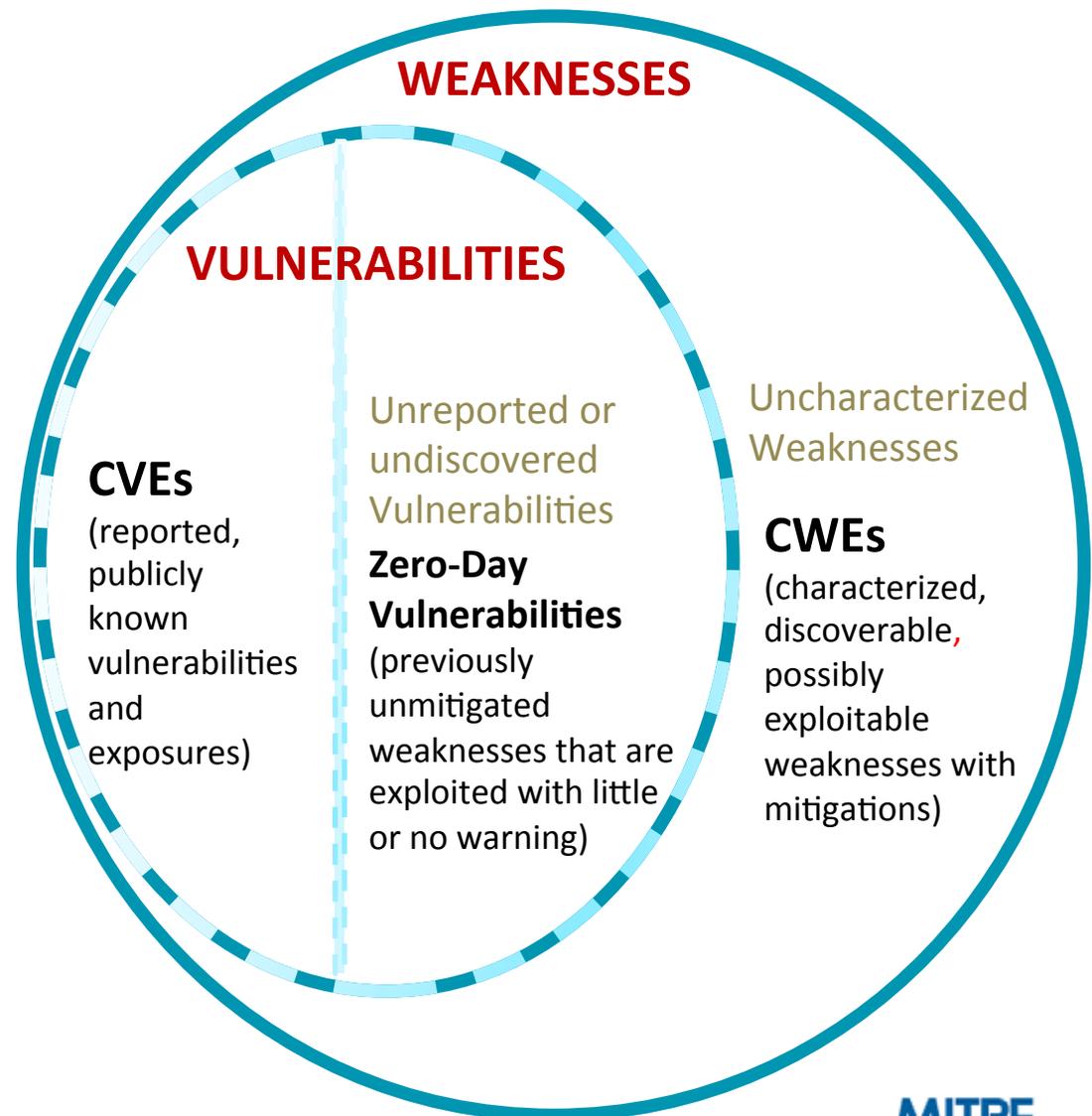


**MITRE**

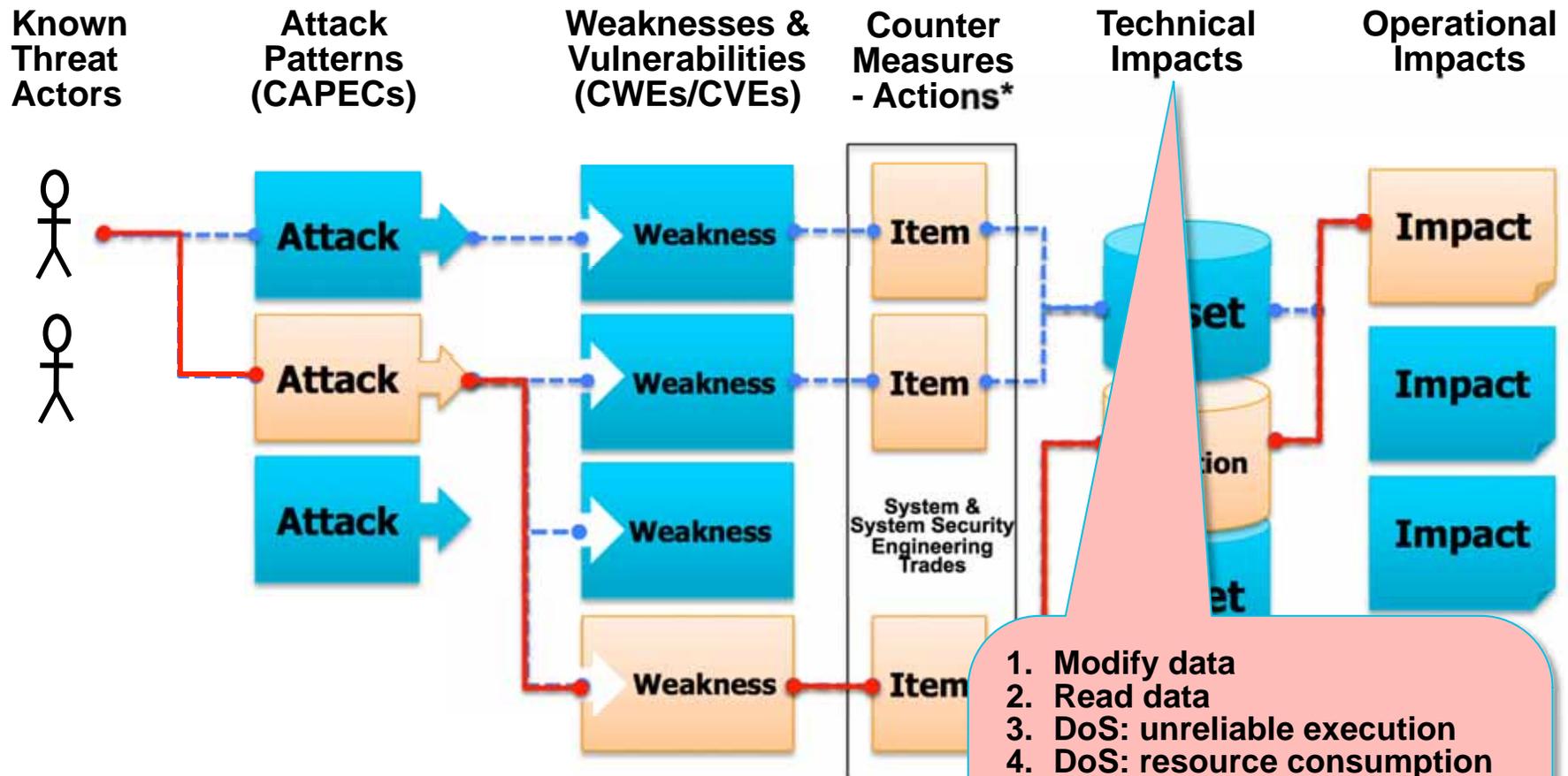
Adapted from: Richard E. Kutter, CIV USAF AFMC AFRL/RYYWA, August 2014

# Exploitable Weaknesses, Vulnerabilities & Exposures

- **Weakness:** mistake or flaw condition in ICT architecture, design, code, or process that, if left unaddressed, could under the proper conditions contribute to a [cyber-enabled capability](#) being vulnerable to exploitation; represents potential source vectors for zero-day exploits -- Common Weakness Enumeration (CWE) <https://cwe.mitre.org/>
- **Vulnerability:** mistake in software that can be directly used by a hacker to gain access to a system or network; Exposure: configuration issue of a mistake in logic that allows unauthorized access or exploitation – Common Vulnerability and Exposure (CVE) <https://cve.mitre.org/>
- **Exploit:** take advantage of a weakness (or multiple weaknesses) to achieve a [negative technical impact](#) -- attack approaches from the set of known exploits are used in the Common Attack Pattern Enumeration and Classification (CAPEC) <https://capec.mitre.org>
- The existence (even if only theoretical) of an exploit designed to take advantage of a [weakness](#) (or multiple weaknesses) and achieve a [negative technical impact](#) is what makes a weakness a [vulnerability](#).



# Assurance About Mitigating the Attacks That Can Impact Operations



\* "Counter Measures - Actions" include: architecture choices; design choices; added security functions, activities & processes; protection schemes; physical decomposition choices; static & dynamic code assessments; design reviews; dynamic testing; and pen testing

# Assurance Comes From Managing Weaknesses and the Supporting Evidence



# Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE  
TRANSFORMATION INITIATIVE

This publication is available free of charge from:  
<http://dx.doi.org/10.6028/NIST.SP.800-53r4>



# Assurance and Trustworthiness

## APPENDIX E

### ASSURANCE AND TRUSTWORTHINESS

#### MEASURES OF CONFIDENCE FOR INFORMATION SYSTEMS

Security assurance is a critical aspect in determining the trustworthiness of information systems. Assurance is the measure of confidence that the security functions, features, practices, policies, procedures, mechanisms, and architecture of organizational information systems accurately mediate and enforce established security policies.<sup>94</sup> The objective of this appendix is:

- To encourage organizations to include assurance requirements in procurements of information systems, system components, and services;
- To encourage hardware, software, and firmware developers to employ development practices that result in more trustworthy information technology products and systems;
- To encourage organizations to identify, select, and use information technology products that have been built with appropriate levels of assurance and to employ sound systems and security engineering techniques and methods during the system development life cycle process;
- To reduce information security risk by deploying more trustworthy information technology products within critical information systems or system components; and
- To encourage developers and organizations to obtain on an ongoing basis, assurance evidence for maintaining trustworthiness of information systems.

Minimum security requirements for federal information and information systems are defined in FIPS Publication 200. These requirements can be satisfied by selecting, tailoring, implementing, and obtaining assurance evidence for the security controls in the low, moderate, or high baselines in Appendix D.<sup>95</sup> The baselines also include the assurance-related controls for the minimum assurance requirements that are generally applicable to federal information and information systems.<sup>96</sup> However, considering the current threat space and the increasing risk to organizational operations and assets, individuals, other organizations, and the Nation, posed by the advanced persistent threat (APT), organizations may choose to implement additional assurance-related controls from Appendix F. These additional controls can be selected based on the tailoring guidance provided in Section 3.2. Organizations can also consider developing high-assurance overlays for critical missions/business functions, specialized environments of operation, and/or information technologies (see Section 3.3 and Appendix I). When assurance-related controls cannot be satisfied, organizations can propose compensating controls (e.g., procedural/operational

<sup>94</sup> Section 2.6 provides an introduction to the concepts of assurance and trustworthiness and how the two concepts are related. A trustworthiness model is illustrated in Figure 3.

<sup>95</sup> CNSS Instruction 1253 provides security control baselines for national security systems. Therefore, the assurance-related controls in the baselines established for the national security community, if so designated, may differ from those controls designated in Tables E-1 through E-3.

<sup>96</sup> It is difficult to determine if a given security control baseline from Appendix D provides the assurance needed across all information technologies, users, platforms, and organizations. For example, while the use of formal methods might be appropriate in a cross-domain product, different assurance techniques might be appropriate for a complex air traffic control system or for a web server providing emergency preparedness information from the Department of Homeland Security. Still, the existing baselines do have assurance aspects that reflect the minimum assurance that is anticipated to be common across all technologies, users, platforms, and organizations.

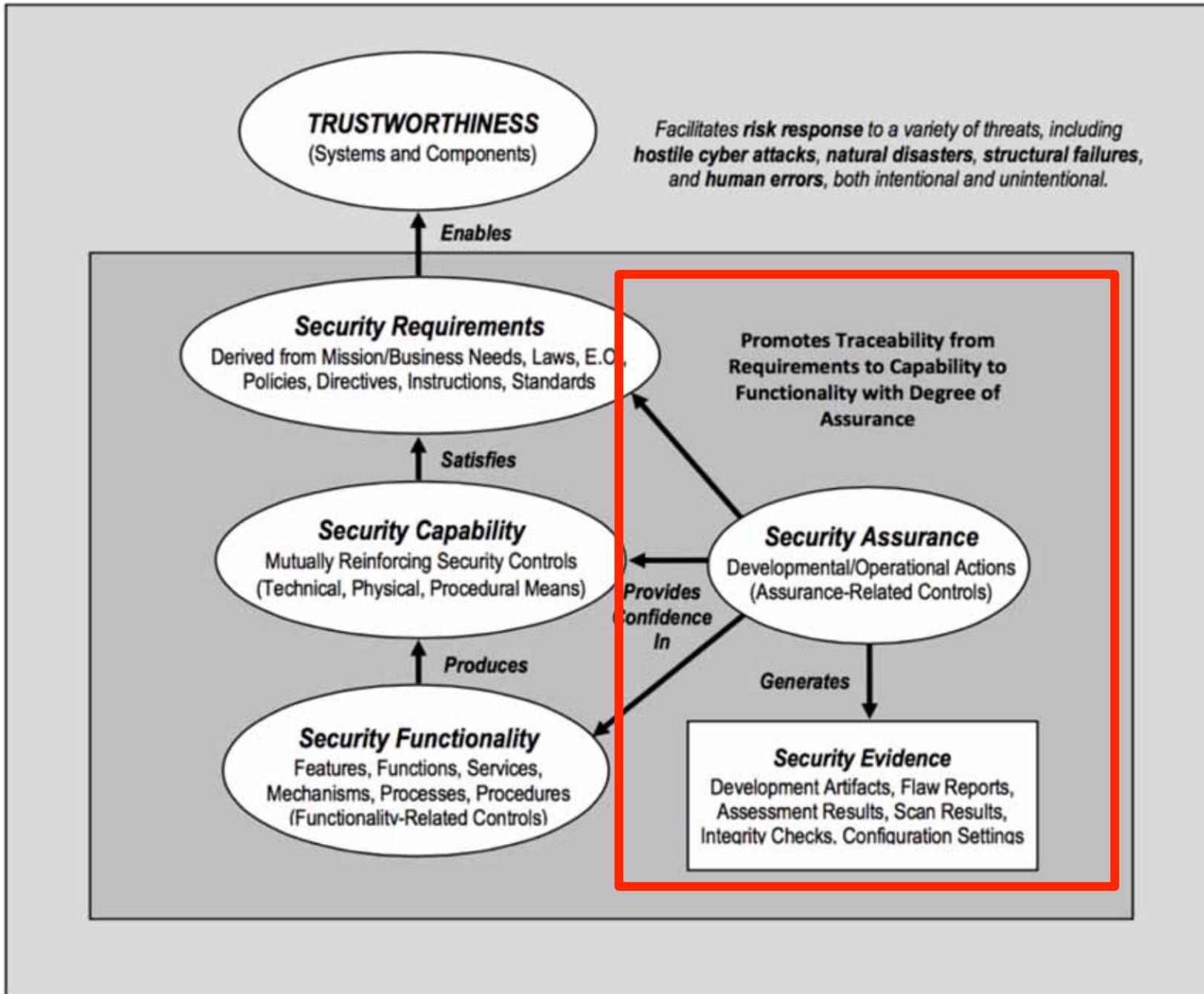


FIGURE 3: TRUSTWORTHINESS MODEL

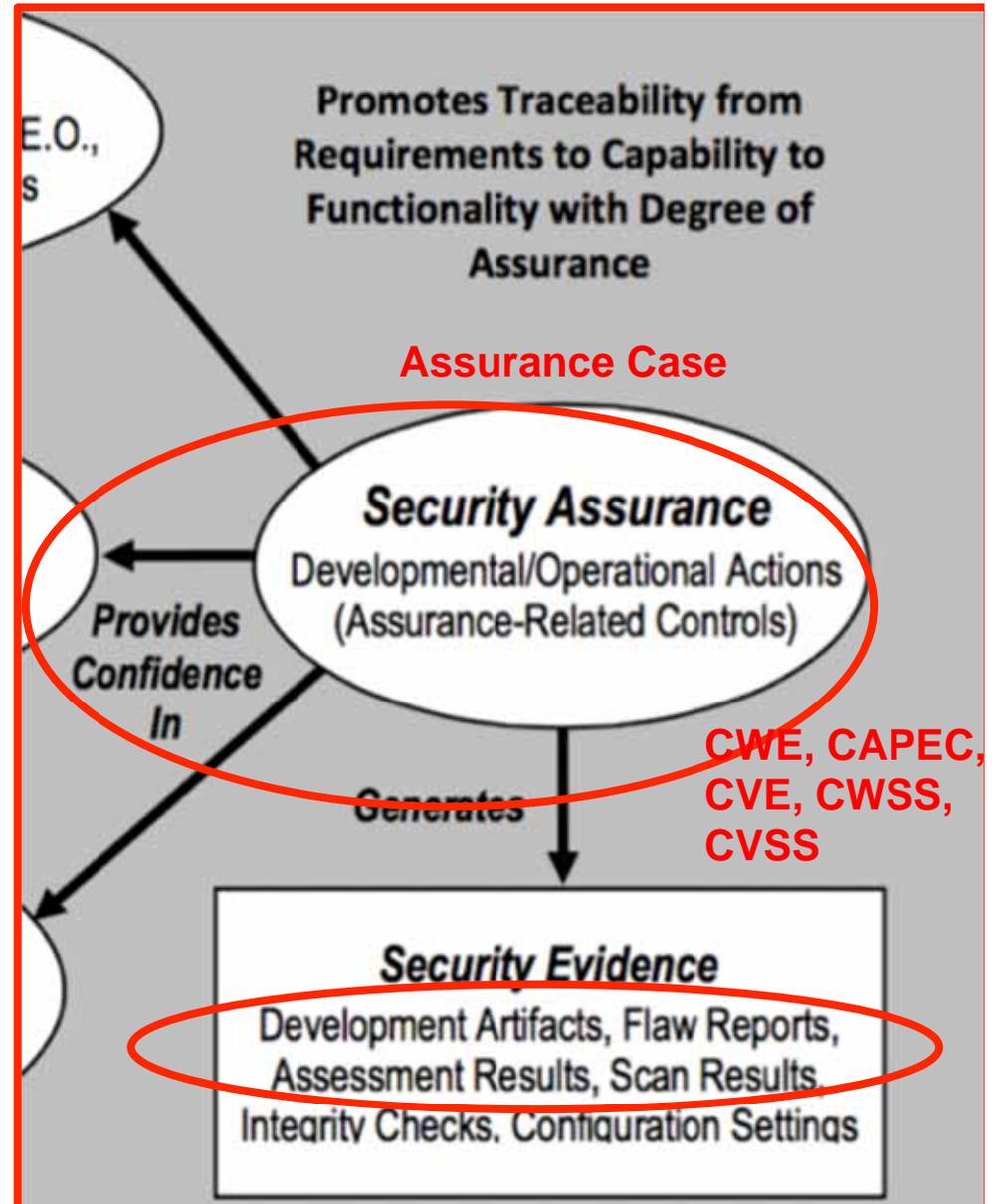
# Assurance and Trustworthiness

*“Security assurance is a critical aspect in determining the trustworthiness of information systems. Assurance is the measure of confidence that the security functions, features, practices, policies, procedures, mechanisms, and architecture of organizational information systems accurately mediate and enforce established security policies.”*

*“Organizations obtain security assurance by the actions taken by information system developers, implementers, operators, maintainers, and assessors. Actions by individuals and/or groups during the development/operation of information systems produce security evidence that contributes to the assurance, or measures of confidence, in the security functionality needed to deliver the security capability...”*

NIST SP 800-53 Revision (rev) 4

© 2015 The MITRE Corporation. All rights reserved.



# Definition of an Assurance Case

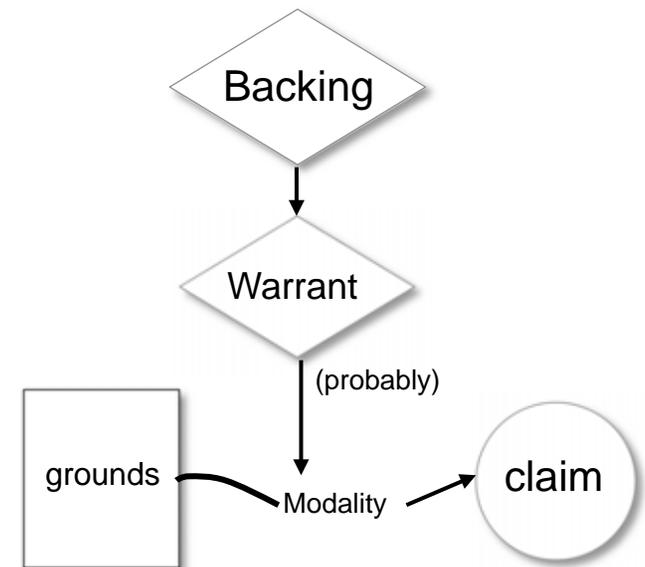
- ***A documented body of evidence that provides a convincing and valid argument that a specified set of critical claims regarding a system's properties are adequately justified for a given application in a given environment.***

# Assurance Claims with Support of ‘Substantial’ Reasoning

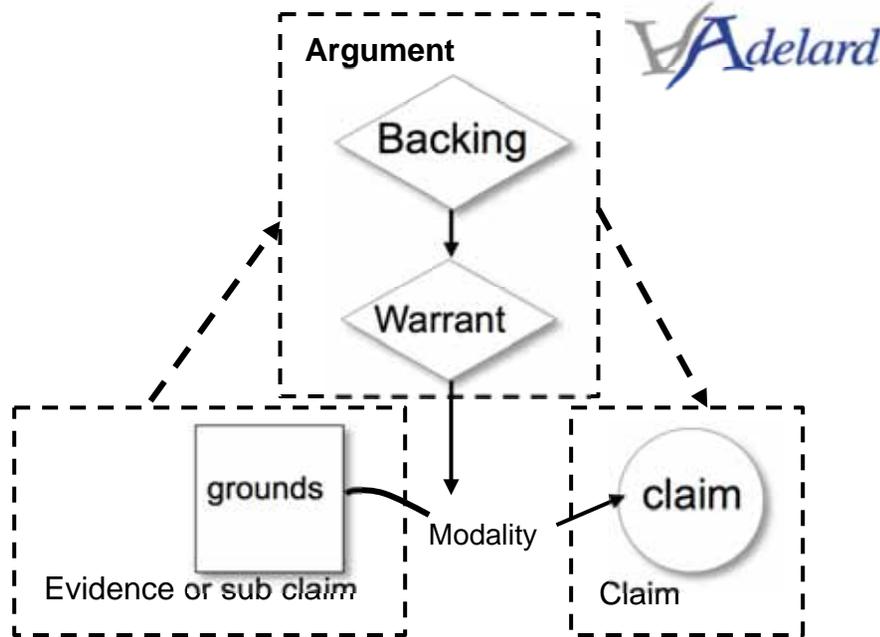


Stephen Toulmin, 1958

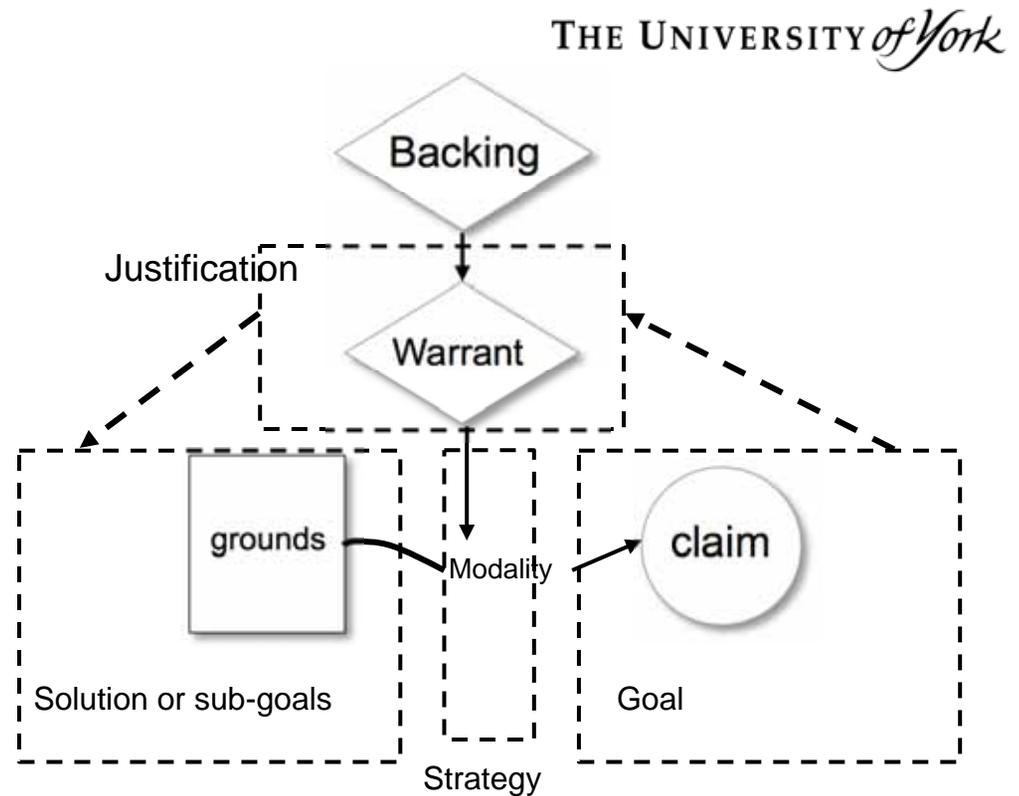
- Claims are assertions put forward for general acceptance
- The justification for claim based is on some grounds, the “specific facts about a precise situation that clarify and make good for a claim”
- The basis of the reasoning from the grounds (the facts) to the claim is articulated.
- Toulmin coined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



# Assurance Claims with Support of 'Substantial' Reasoning → two implementations



**CAE**  
**Claim, Argument, Evidence**



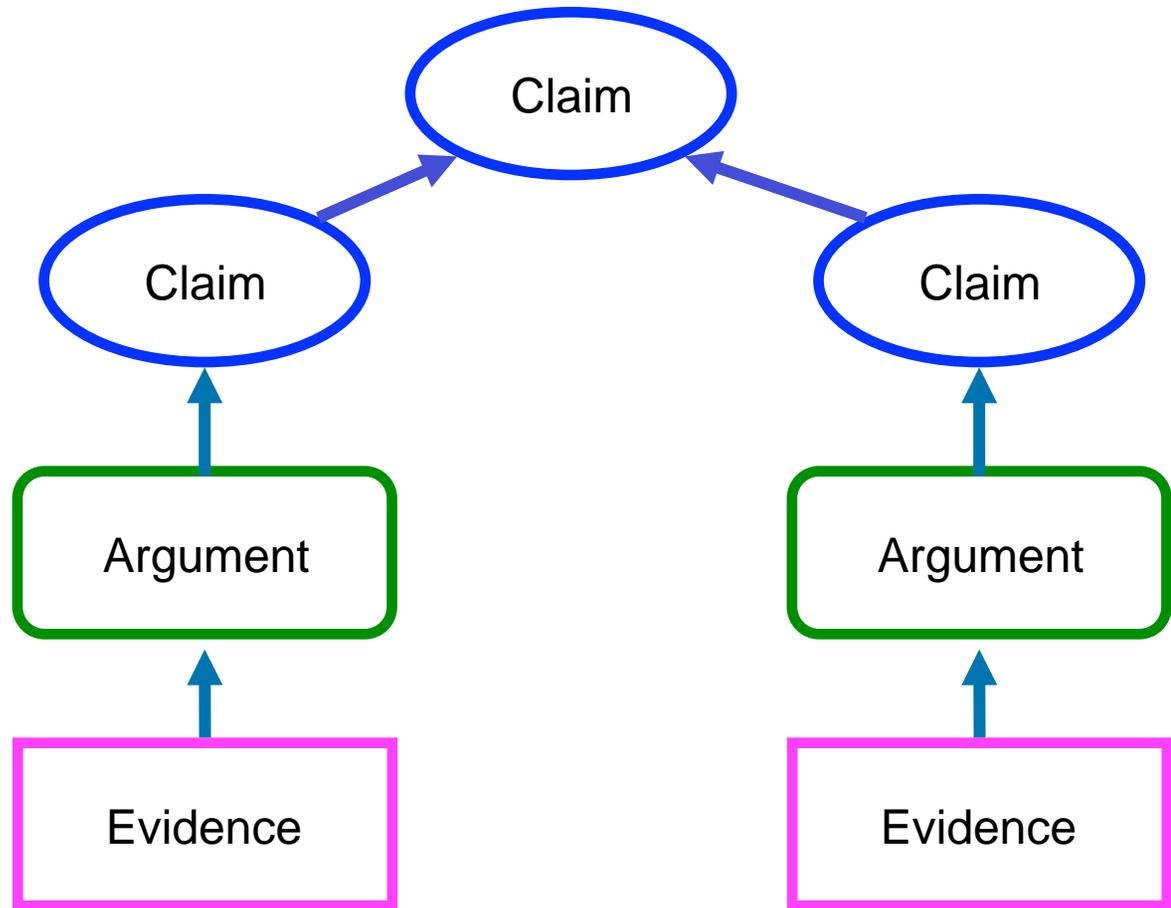
**GSN**  
**Goal Structuring Notation** MITRE

# Claims, Arguments, and Evidence

**Claim =  
assertion to be  
proven**

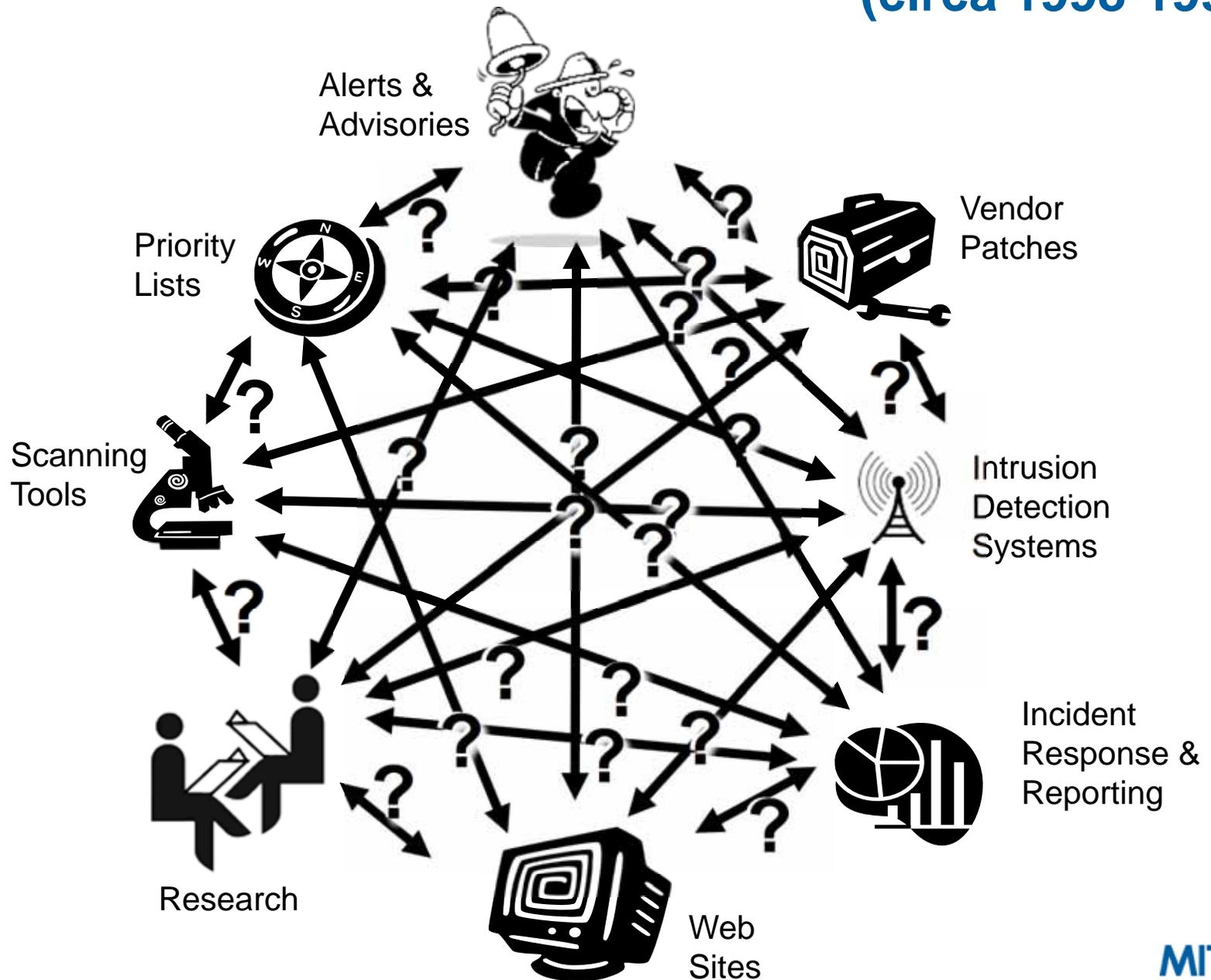
**Argument =  
how evidence  
supports claim**

**Evidence =  
required  
documentation**



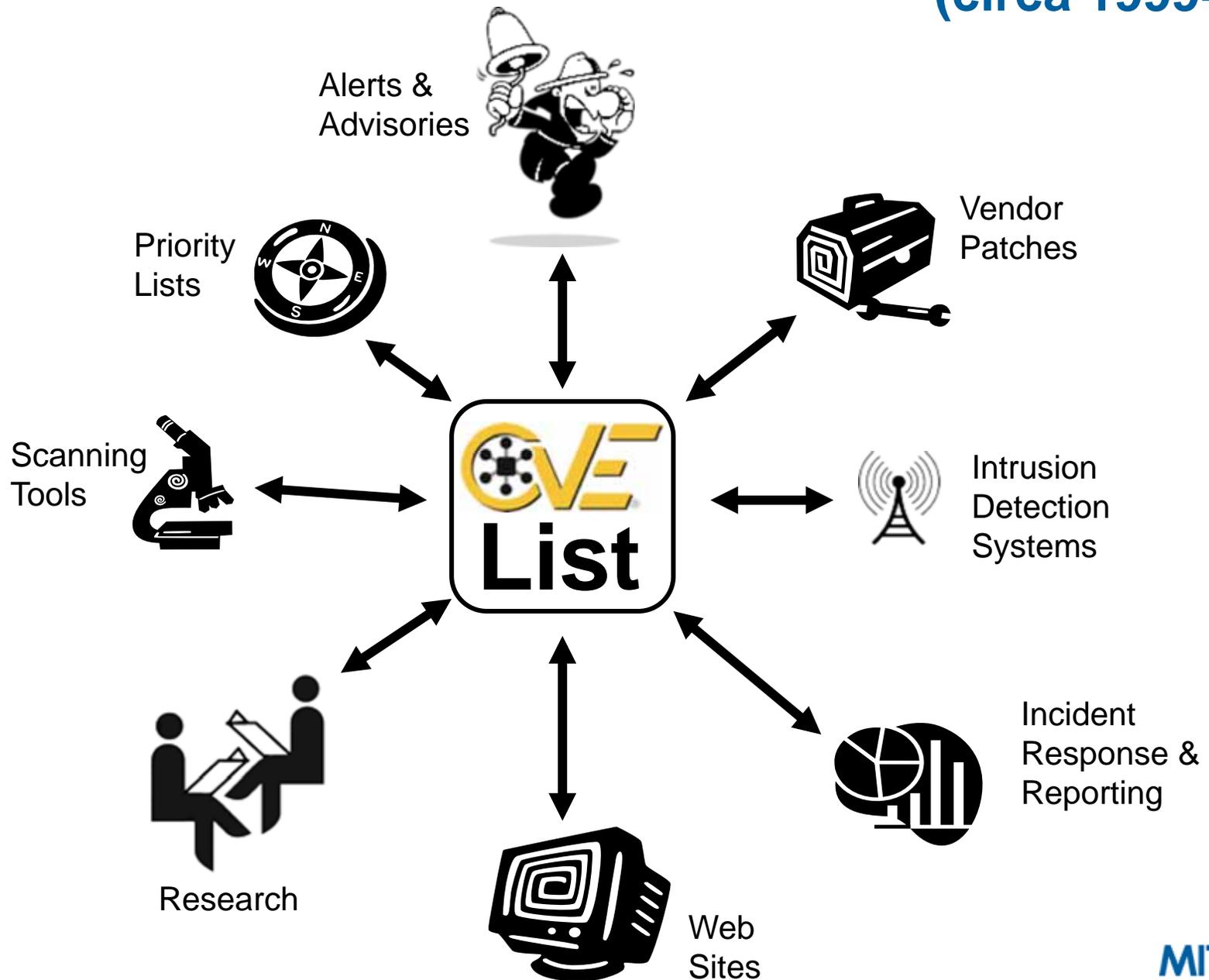
# Vulnerability Information Sharing

(circa 1998-1999)

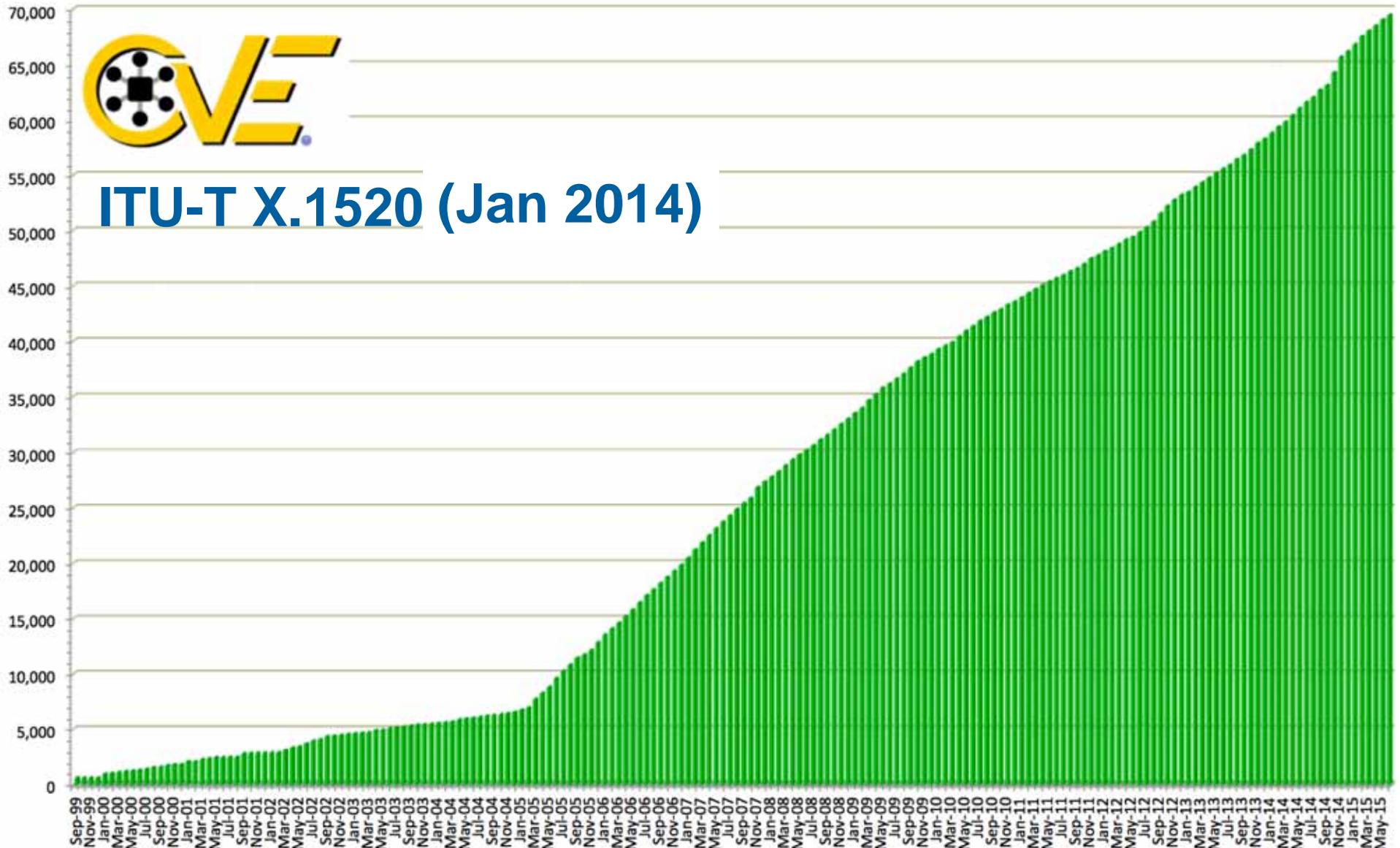


# Vulnerability Information Sharing

(circa 1999+)

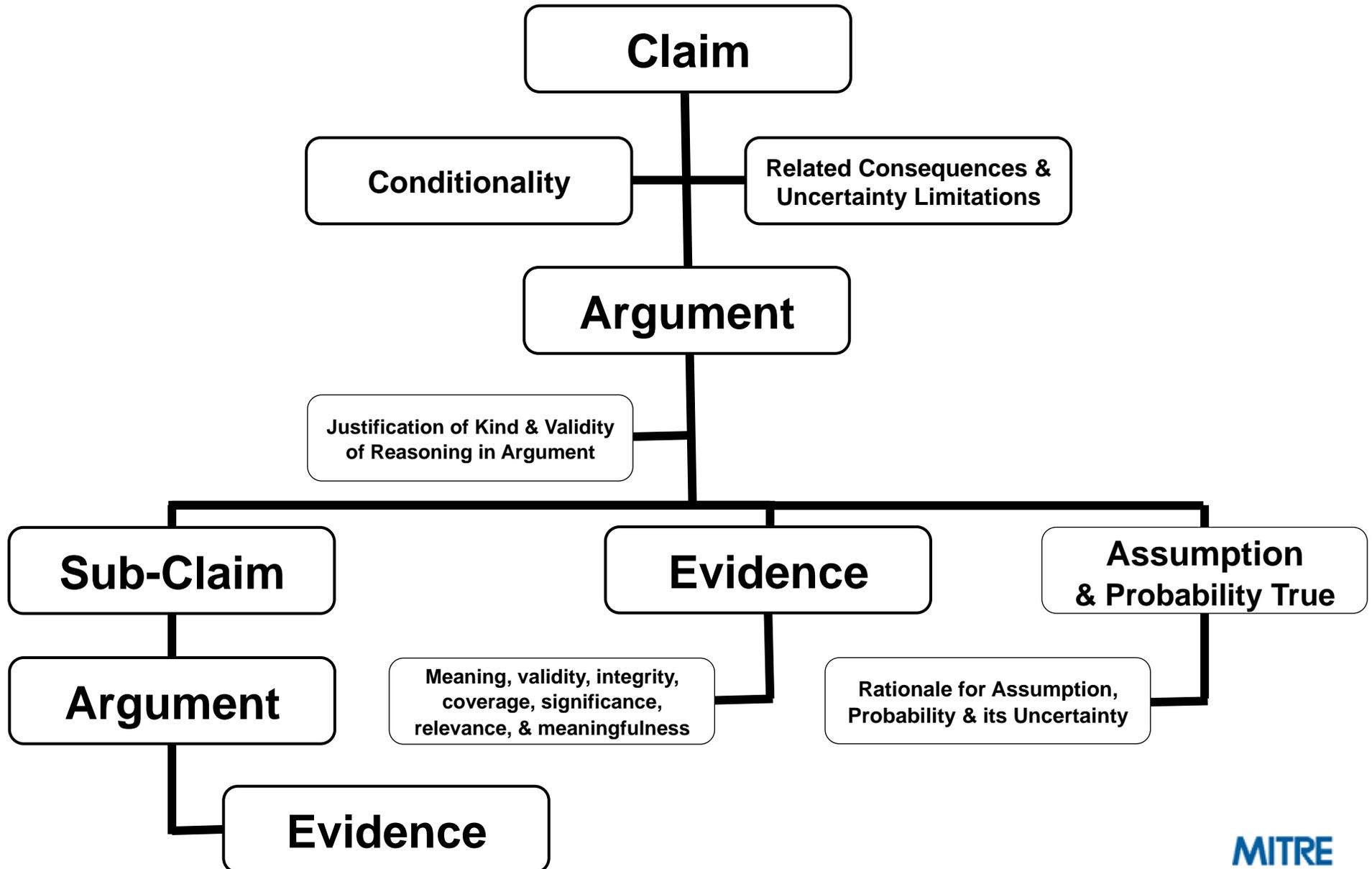


# CVE 1999 to 2015

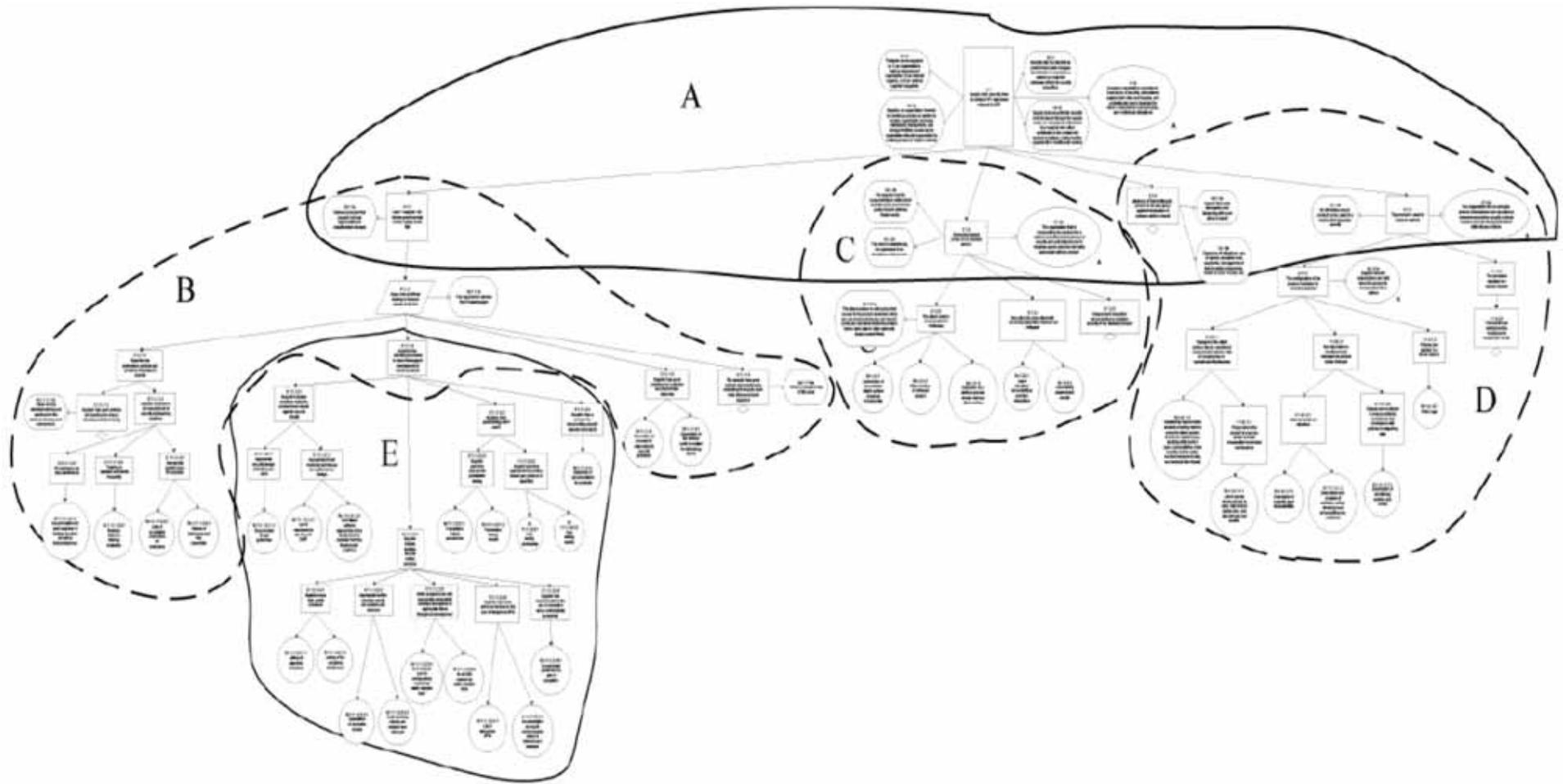


# ISO/IEC 15026: Systems & Software Assurance

## 15026 Part 2: The Assurance Case (Claims-Evidence-Argument)



# Assurance Cases Can Be Large & Composed of Other Assurance Cases



A: Overview of Assurance Case

B: Supplier Practices Reduce Supply Chain Risk

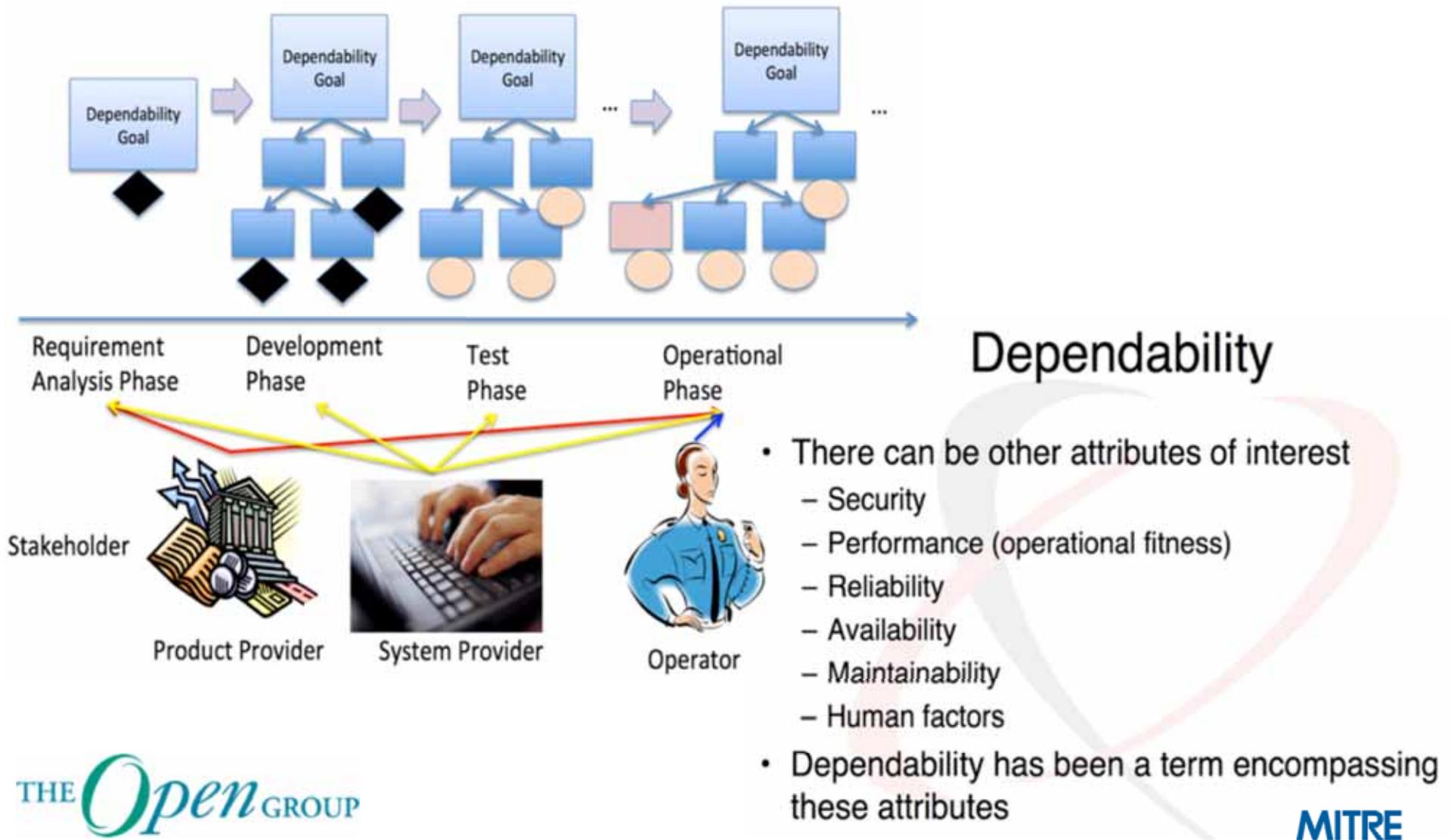
C: Developed/Updated Product is Acceptably Secure

D: Delivered/Updated Product is Acceptably Secure & The Product is Used in a Secure M

E: Supplier Has Effective Processes in Place to Support Secure Development

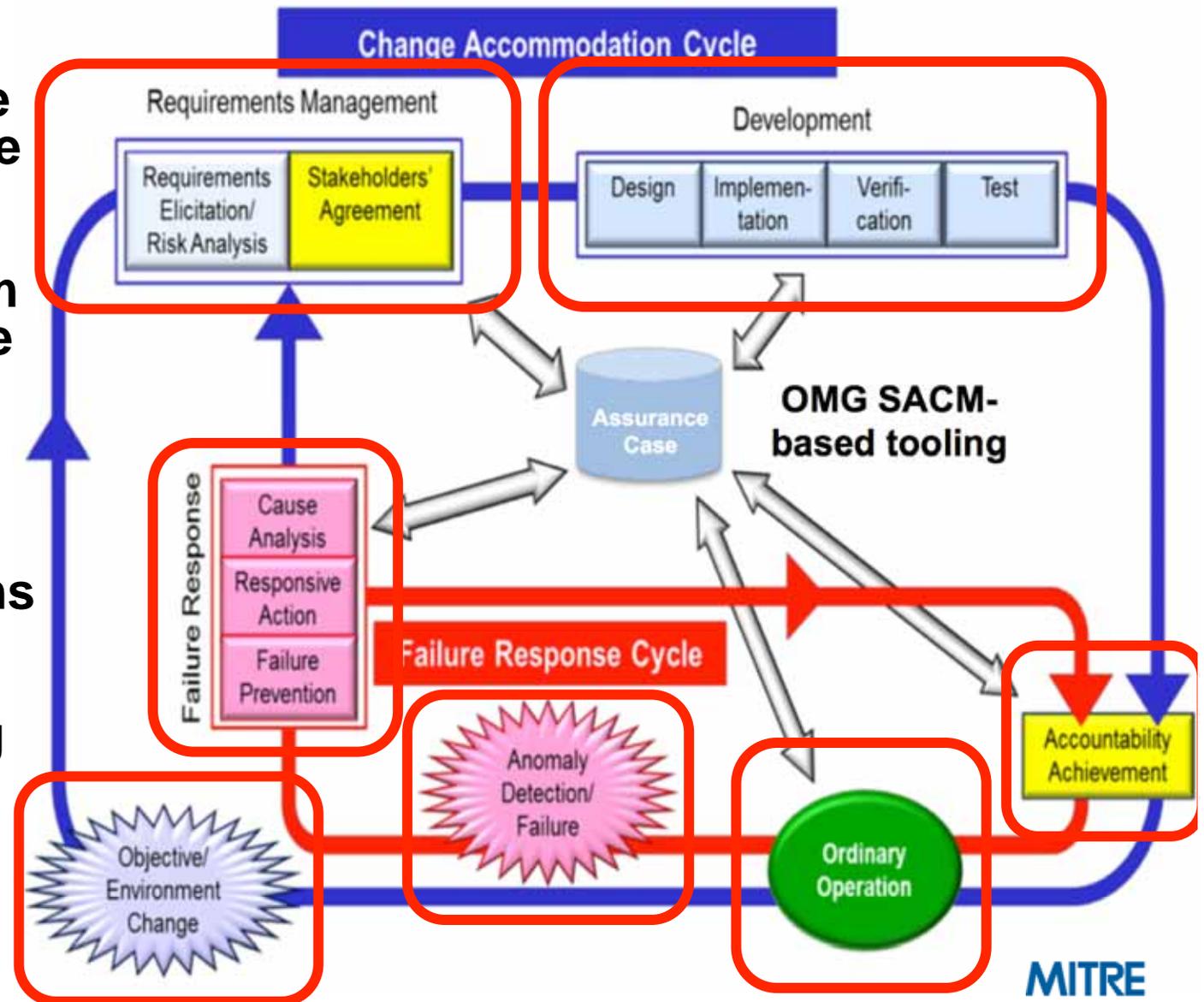


# An Assurance Case for “Qualities” that Must Dependably be in the Operational System



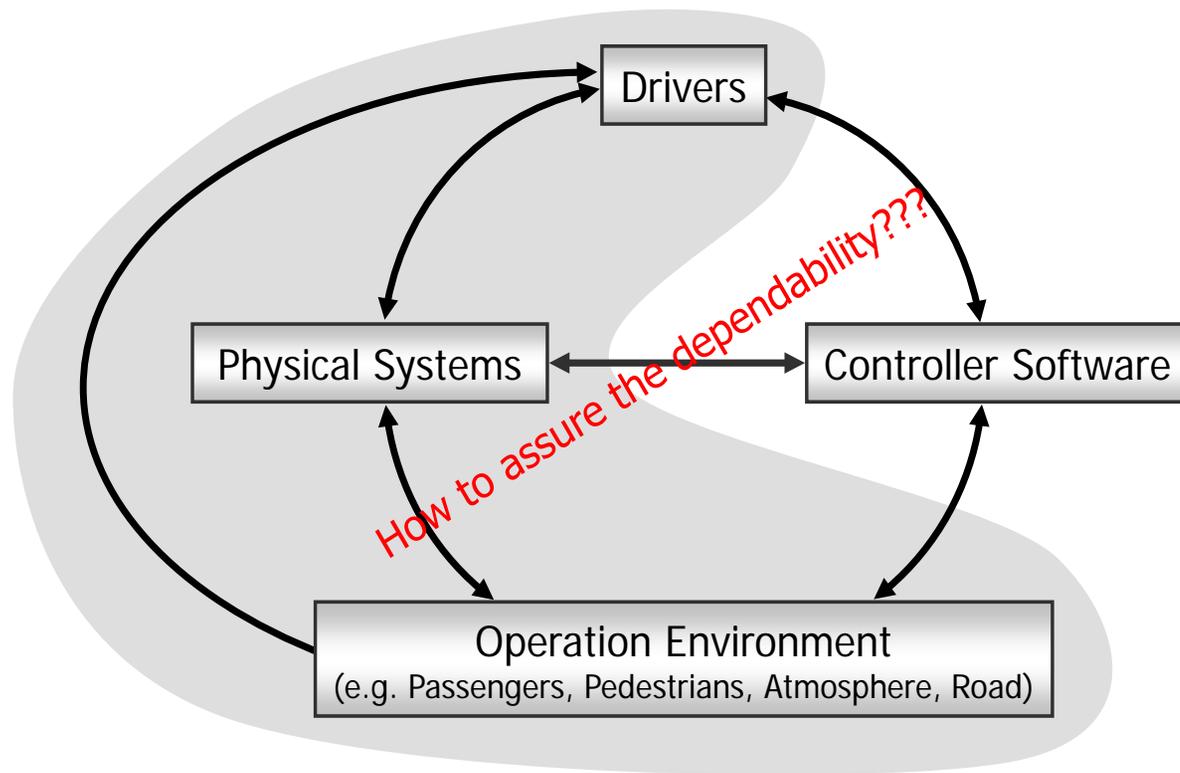
# Open Group's Dependability Framework (O-DA): Implied Requirements for Design / Development / Evaluation

- Using an Assurance Case Model to capture (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 maintaining the system



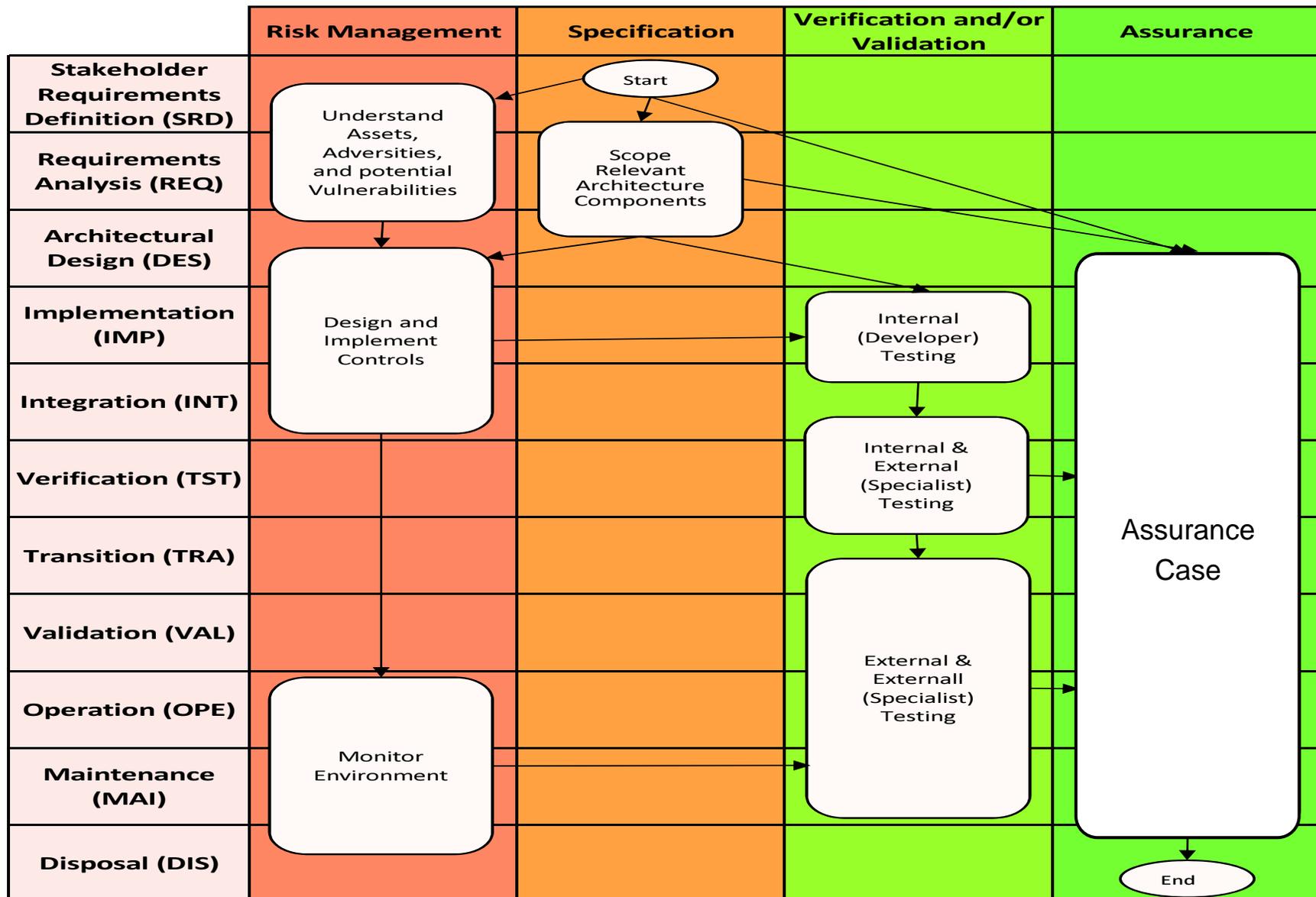
# OMG Dependability Assurance Framework For Safety-Sensitive Consumer Devices

## Characteristics of Consumer Devices



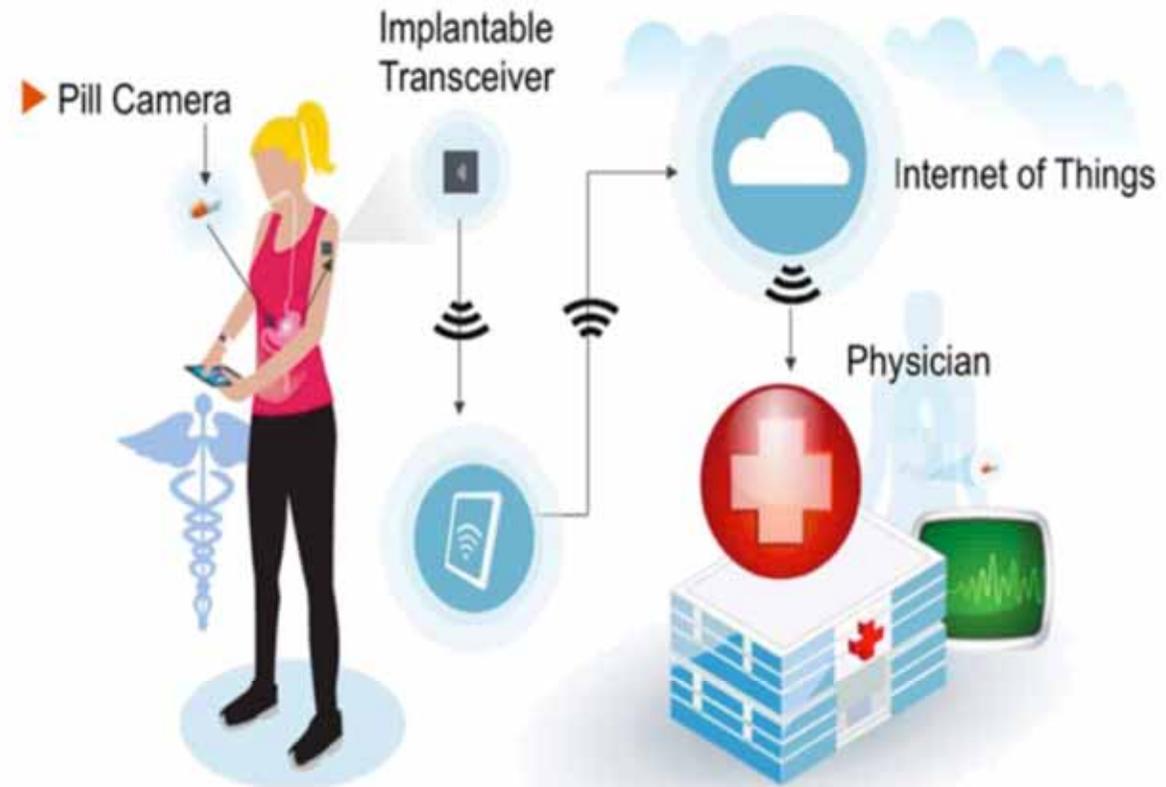
There are frequent interactions between physical system and control software in open, diverse, and dynamic environment.

# European Telecommunications Standards Institute (ETSI) Methods for Testing and Specification (MTS) Work Item on Security Assurance Lifecycle



# Medical Example of Connected and Co-Dependent...

## Remote Patient Monitoring



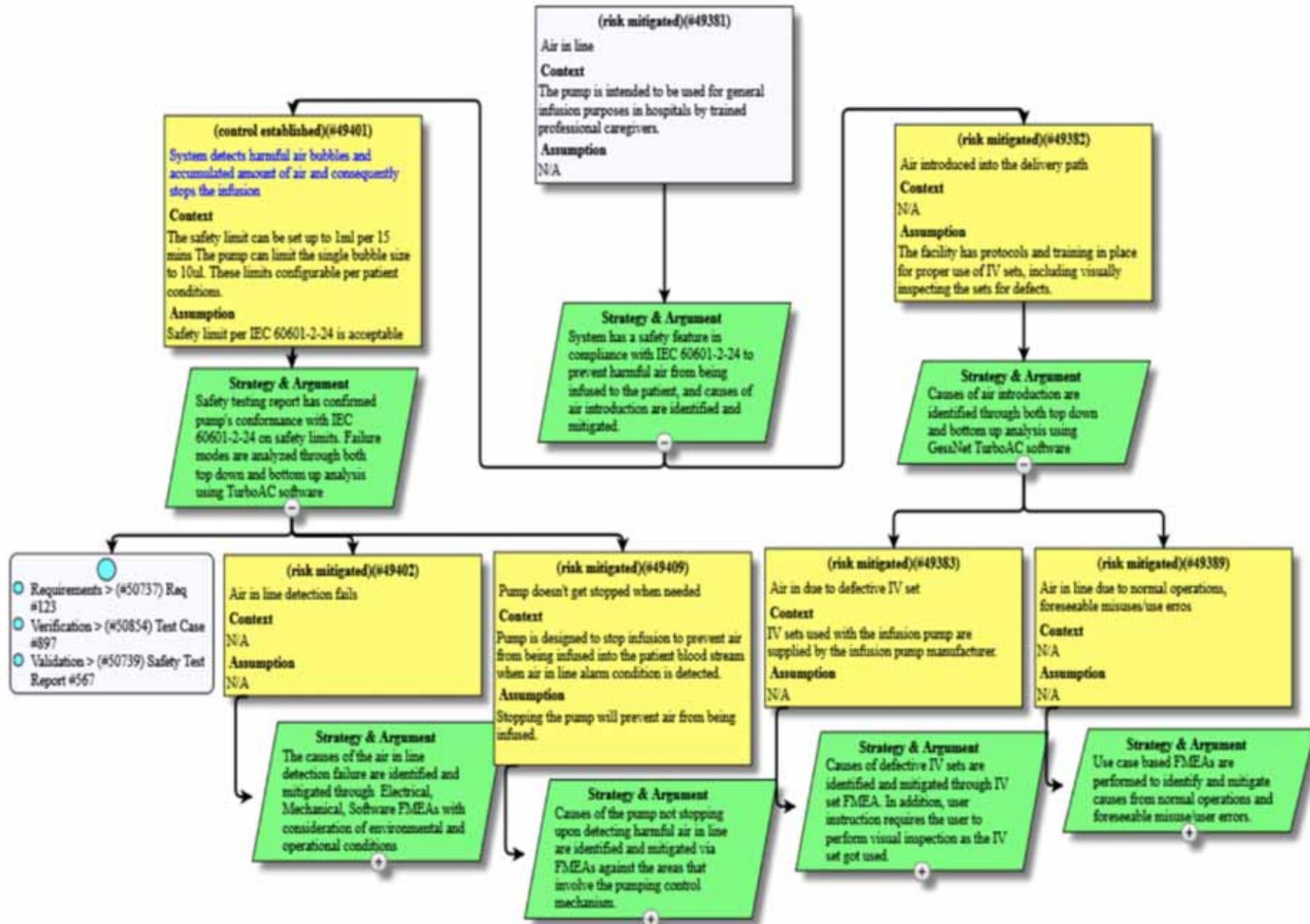
FDA -- January 2015

"Infusion Pumps Total Product Life Cycle – Guidance for Industry and FDA Staff"

<http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM209337.pdf>

Stipulates the use of safety assurance case information collection (OMB control number 0910-0766) when preparing a 501(K) submission...

# Medical Device Assurance Case (thanks to GessNet)



# Status in Industry (1 of 3)

## Currently available tools for Assurance Cases:

- TurboAC™ Assurance Case Software <http://www.gessnet.com>
- 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](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](https://github.com/d-case/d-case_editor)

# Status in Industry (2 of 3)

## Leveraging or explaining the utility of Assurance Cases:

- **The Safety Engineer Resource on Assurance Cases**  
<https://safetyengineering.wordpress.com/2008/04/04/the-goal-structuring-notation-gsn/>
- **SEI: Assurance Case Discussion:**  
<http://www.sei.cmu.edu/dependability/tools/assurancecase/>
- **SEI: Charles B. Weinstock Lecture at UPENN (2008):**  
<http://www.seas.upenn.edu/~lee/09cis480/lec-AssuranceCasesTutorial.pdf>
- **SEI: An Assurance Case Automation Toolset**  
[http://rd.springer.com/chapter/10.1007%2F978-3-642-33675-1\\_2](http://rd.springer.com/chapter/10.1007%2F978-3-642-33675-1_2)
- **Underwriters Laboratory Software Certification Leveraging Assurance Cases**
- **Industrial Internet Consortium's Industrial Internet Reference Architecture relies on assurance cases and automation**

# Status in Industry (3 of 3)

## Standardization efforts related to Assurance Cases:

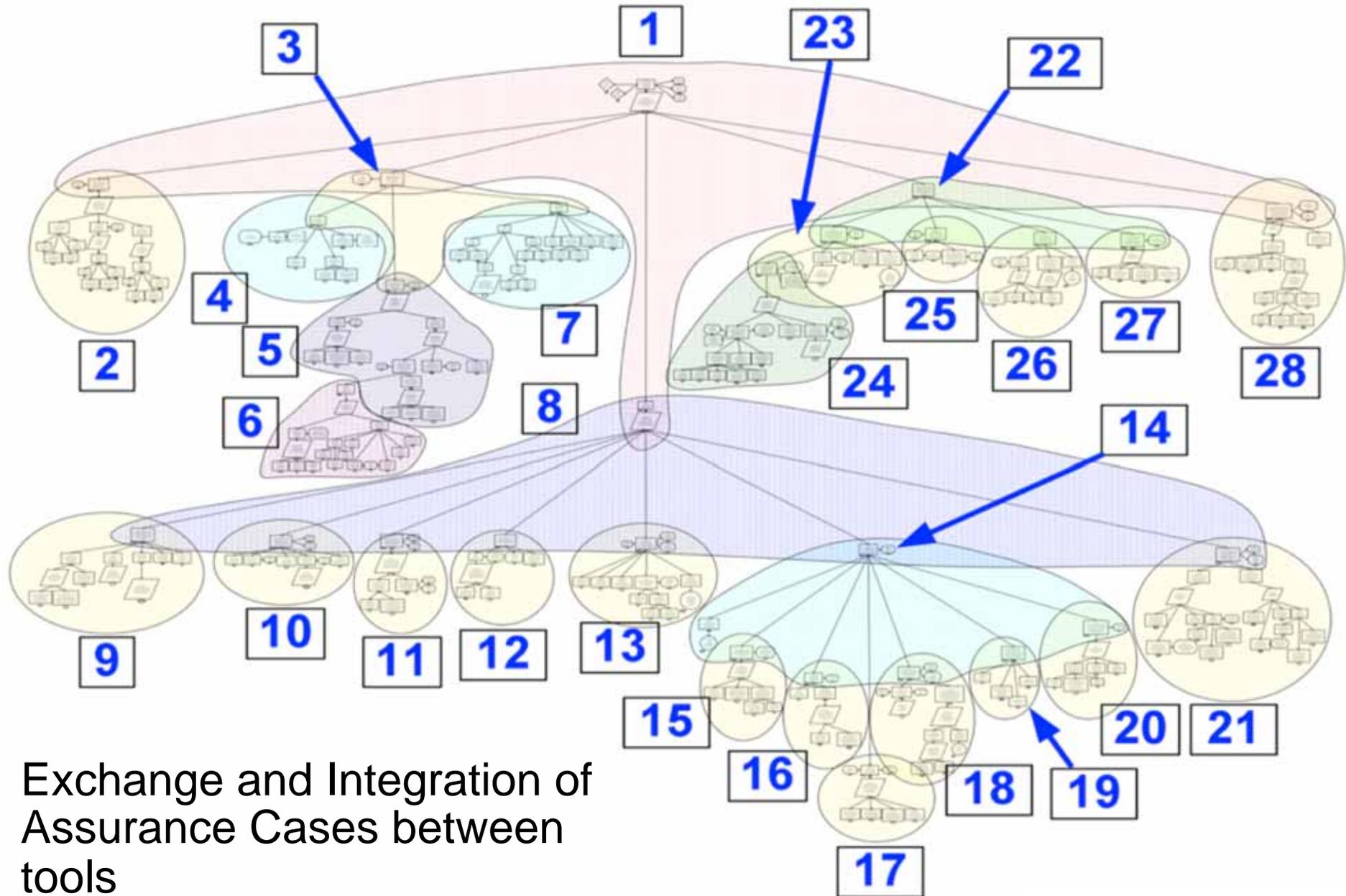
- **ISO/IEC 15026: Systems & Software Assurance 15026 Part 2: The Assurance Case**
- **Goal Structuring Notation (GSN)**  
<http://www.goalstructuringnotation.info/>
- **OPENCROSS: A Design and Implementation of an Assurance Case Language**
- **Open Group: Dependability Framework (O-DA)**
- **OMG Structured Assurance Case Metamodel (SACM)**  
<http://www.omg.org/spec/SACM/>
- **OMG Dependability Assurance Framework for Safety-Sensitive Consumer Devices (DAF)**  
<http://www.omg.org/spec/DAF/>
- **OMG Machine-checkable Assurance Case Language (MACL)**

# Status in Government

## Leveraging, Requiring, or explaining the utility of Assurance Cases:

- **FDA Infusion Pumps Total Product Life Cycle Guidance for Industry and FDA Staff, 2 December 2014**  
<http://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm209337.pdf>
- **NIST Interagency Report 7608 “Software Assurance Using Structured Assurance Case Models”** <http://nvlpubs.nist.gov/nistpubs/ir/2009/ir7608.pdf>
- **US National Library of Medicine, National Institutes of Health: PMC3669506**  
<http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3669506/>
- **European Telecommunications Standards Institute (ETSI) Methods for Testing and Specification (MTS) Work Item on Security Assurance Lifecycle**
- **SEI: Laying the Foundation for a Credible Security Case**  
<https://buildsecurityin.us-cert.gov/articles/knowledge/assurance-cases/evidence-assurance-laying-foundation-credible-security-case>
- **SEI: Assurance Cases Overview**  
<https://buildsecurityin.us-cert.gov/articles/knowledge/assurance-cases/assurance-cases-overview>
- **SEI: Arguing Security - Creating Security Assurance Cases**  
<https://buildsecurityin.us-cert.gov/articles/knowledge/assurance-cases/arguing-security-creating-security-assurance-cases>

# OMG's Structured Assurance Case Metamodel (SACM)



Exchange and Integration of Assurance Cases between tools

# Things Needed from Assurance Case Tooling...

- **Use of Tool-Based Structured Assurance Case would:**
  - Improve the Understandability of an Assurance Case to a 3<sup>rd</sup> Party
  - Improve Rigor of Assurance Cases through Modelling
  - Allow for Reexamination of Assumptions
  - Allow for Reexamination of Argument Structuring
  - Allow for Reexamination of Appropriateness of Evidence
  - Allow for Reuse of Sub-Claim/Evidence Constructs That “Work”
- **Author/Share Libraries of Sub-Claims/Supporting Evidence**
  - Provide for Assurance Case Analytics/Validation
  - Provide for Exchange of Assurance Cases (Import/Export)
  - Provide for Enforcing Community of Interest Norms of Practice

# 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.xml](http://www.omg.org/spec/SACM/2014110141101/emof.xml)

Non-normative:

[ptc/2014-12-05 -- http://www.omg.org/spec/SACM/20141101/ecore.xml](http://www.omg.org/spec/SACM/20141101/ecore.xml)

[ptc/2014-12-08 -- http://www.omg.org/spec/SACM/20141101/SACM\\_Annex\\_B\\_Examples.xml](http://www.omg.org/spec/SACM/20141101/SACM_Annex_B_Examples.xml)

---

Structured Assurance Case Metamodel, v1.1

1

Page 1 of 80

### Report of the SACM 1.1 RTF Revision Task Force to the OMG Platform Technical Committee

10 December 2014

Document Number: ptc/14-12-14  
Task Force Chair(s): Robert Martin, MITRE ([ramartin@mitre.org](mailto:ramartin@mitre.org))  
Chartered: 22 June 2012 — Cambridge, MA, USA  
Comments Due: 4 January 2013  
Expiry Due: 19 December 2014  
JIRA Project Prefix: SACM11  
Document Template: omg/2013-05-01

SACM 1.1 RTF Report

Generated 2014-12-10 14:38:08





---

# Questions?

ramartin@mitre.org