

Building An Assurance Case And What Is Needed To Complete These Models



Sr. Software and Supply Chain Assurance Prin. Eng.
Cross Cutting Solutions and Innovation Dept.
Cyber Solutions Technical Center
MITRE Labs

August 31, 2022

A Presentation to the 2022 NDIA Electronics Trust & Assurance Subcommittee Workshop at Lockheed Martin Global Vision Center, Arlington, VA

MITRE | SOLVING PROBLEMS
FOR A SAFER WORLD™

**2015 & 2016 Jeep Hacks:
A failure of assured
systems engineering
given today's
connected
world?...**

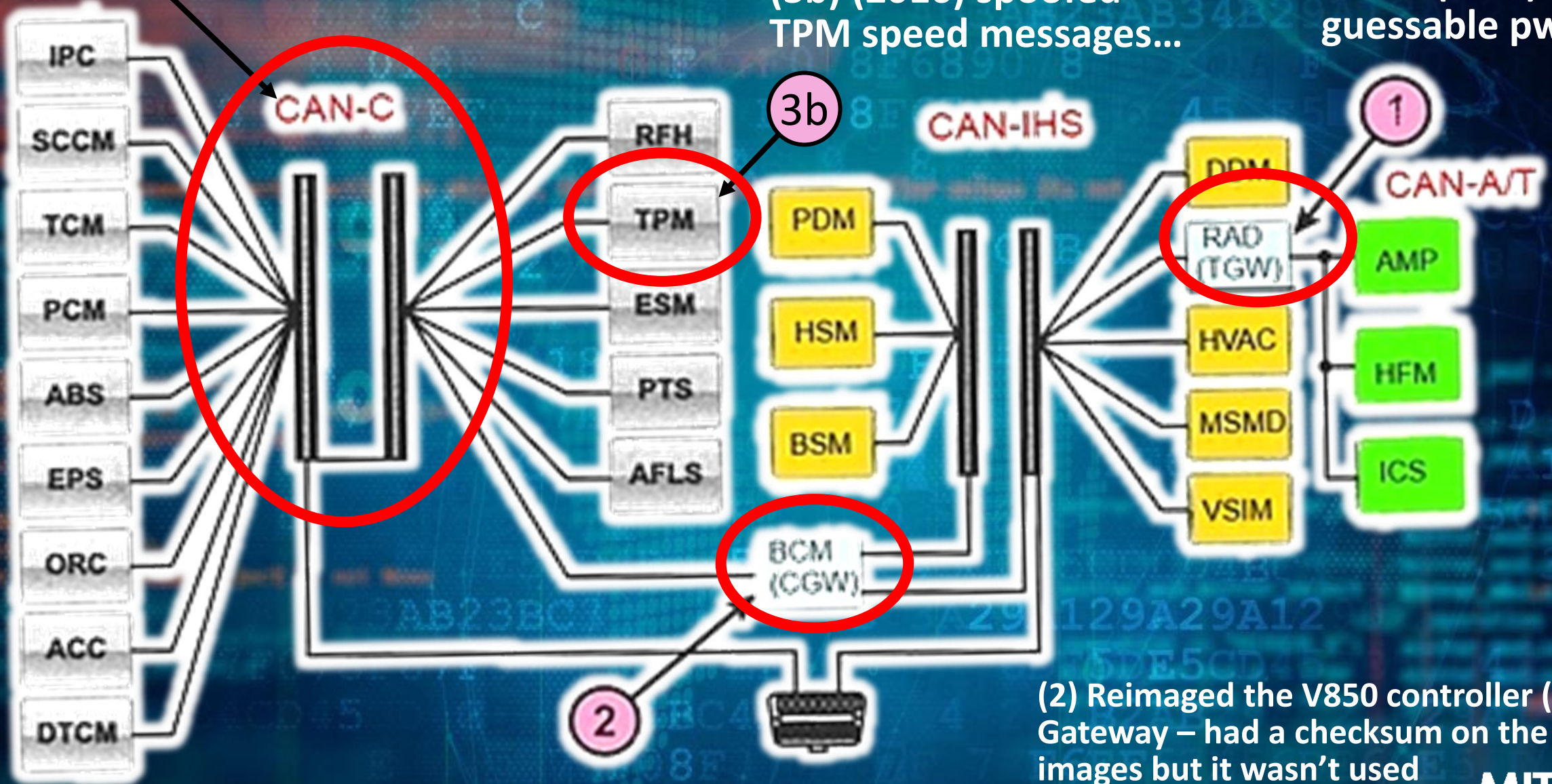


Photo: Andy Greenberg/WIRED

(3a) With re-imaged BCM the Radio can send arbitrary CAN Bus Commands (2015)

(3b) (2016) spoofed TPM speed messages...

(1) Took over the Radio (RAD) thru guessable pwd



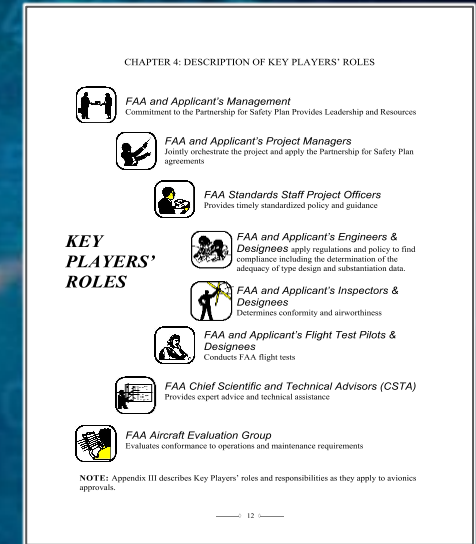
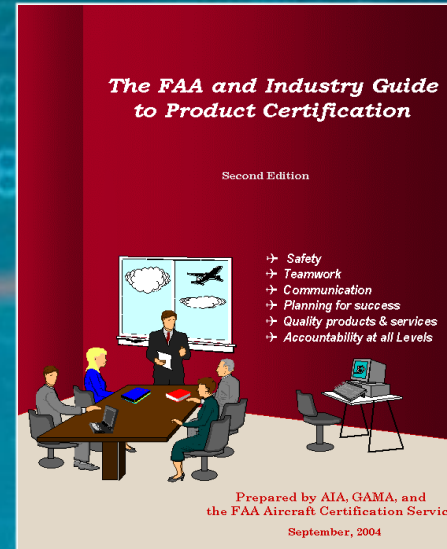
(2) Reimaged the V850 controller (BCM) Gateway – had a checksum on the images but it wasn't used

Certified to Work in Shared Context Engineered to Do the Mission...



FAA Flight Certified

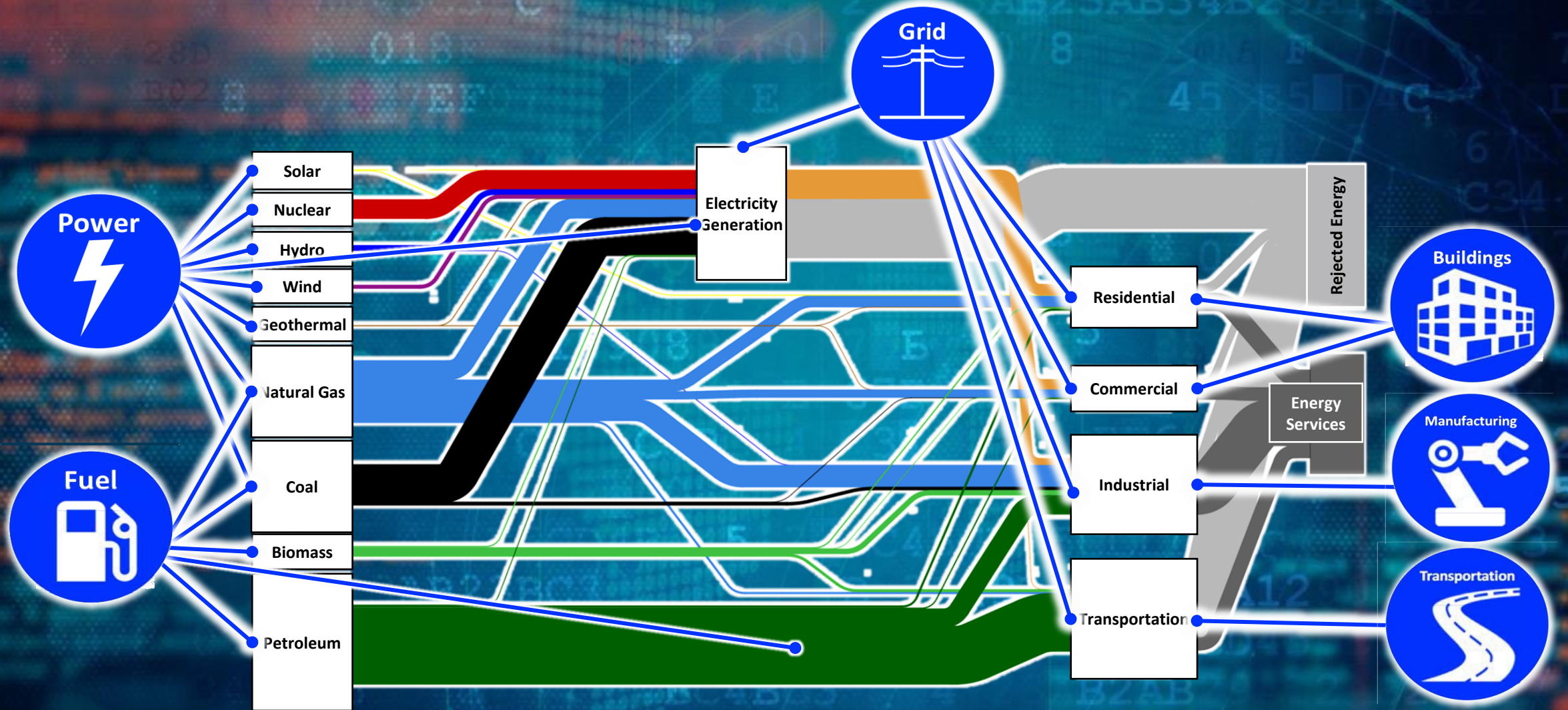
- Radios, Radar Beacons, Navigation Lights, Safety features...



Critical Operational Issue	2005 Operational Evaluation		
	Parameter	Threshold	Result
Assault Support	Amphibious Pre-Assault/Raid	200 NM (KPP)	230 NM
	Amphibious Ext Lift	10,000 lbs for 50 NM (KPP)	9,800 for 50 NM
	Land Assault External Lift	50 NM (KPP)	69 NM
	Cruise Airspeed	240 KTS (KPP)	255 KTS
	Troop Seating	24 Combat Troops (KPP)	24 Combat Troops
Self Deployment	Self-deployment	2100 NM (KPP)	2660 NM
Survivability	Ballistic Tolerance	12.7mm @ 90% velocity (KPP)	Satisfactory (BLRIP-LFT&E)
Interoperability	Top Level Information Exchange Requirement (IER)	All top-level requirements (KPP)	Satisfactory



Need Standards to Drive Consistency in Discussing and Conveying Assurance due to the Sector-2-Sector linkages



Perspectives on Assurance

Insurer

- How do I underwrite?

Researcher

- What technology is needed to ensure trust?

Creator

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

Community

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

Operator

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

Commander/ Supervisor

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

Regulator

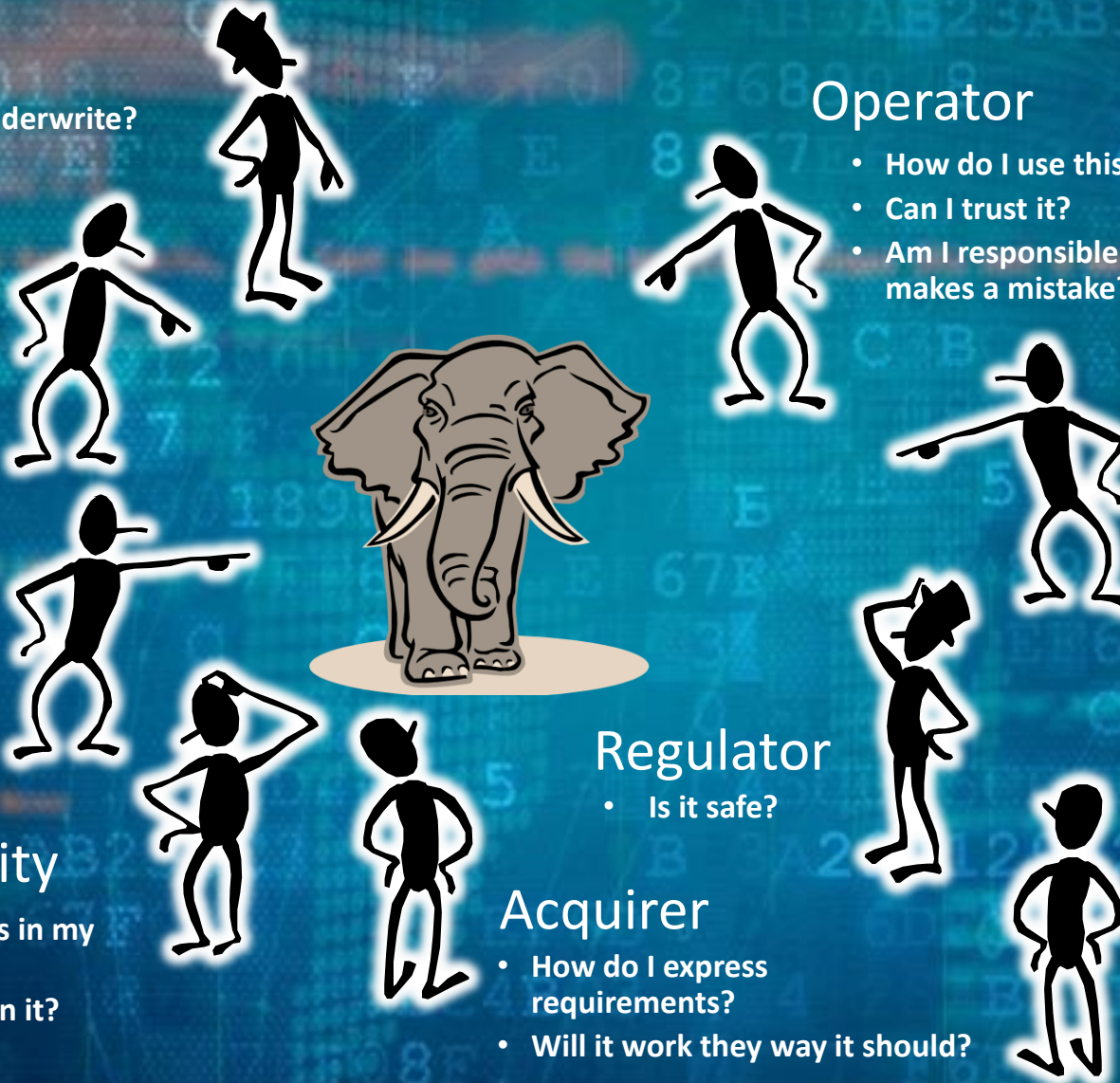
- Is it safe?

Acquirer

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

Patron

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



Definition of Assurance Case

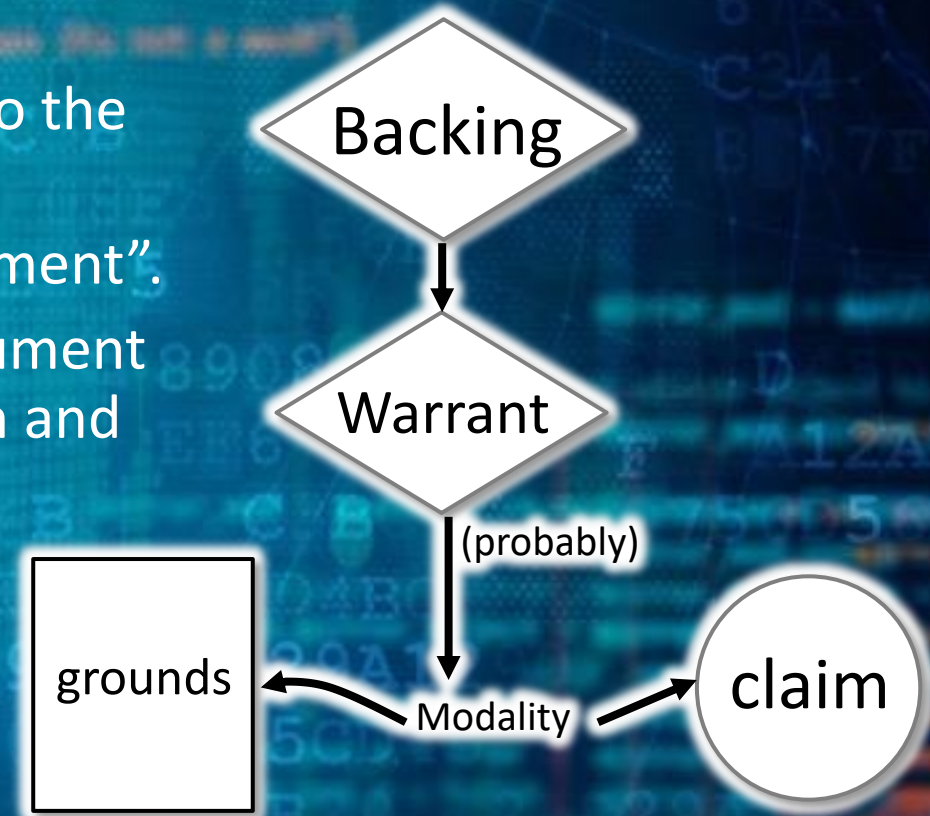
A documented body of evidence that provides a convincing and valid argument that a specified set of critical claims regarding a system's properties are adequately justified for a given application in a given environment.

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.

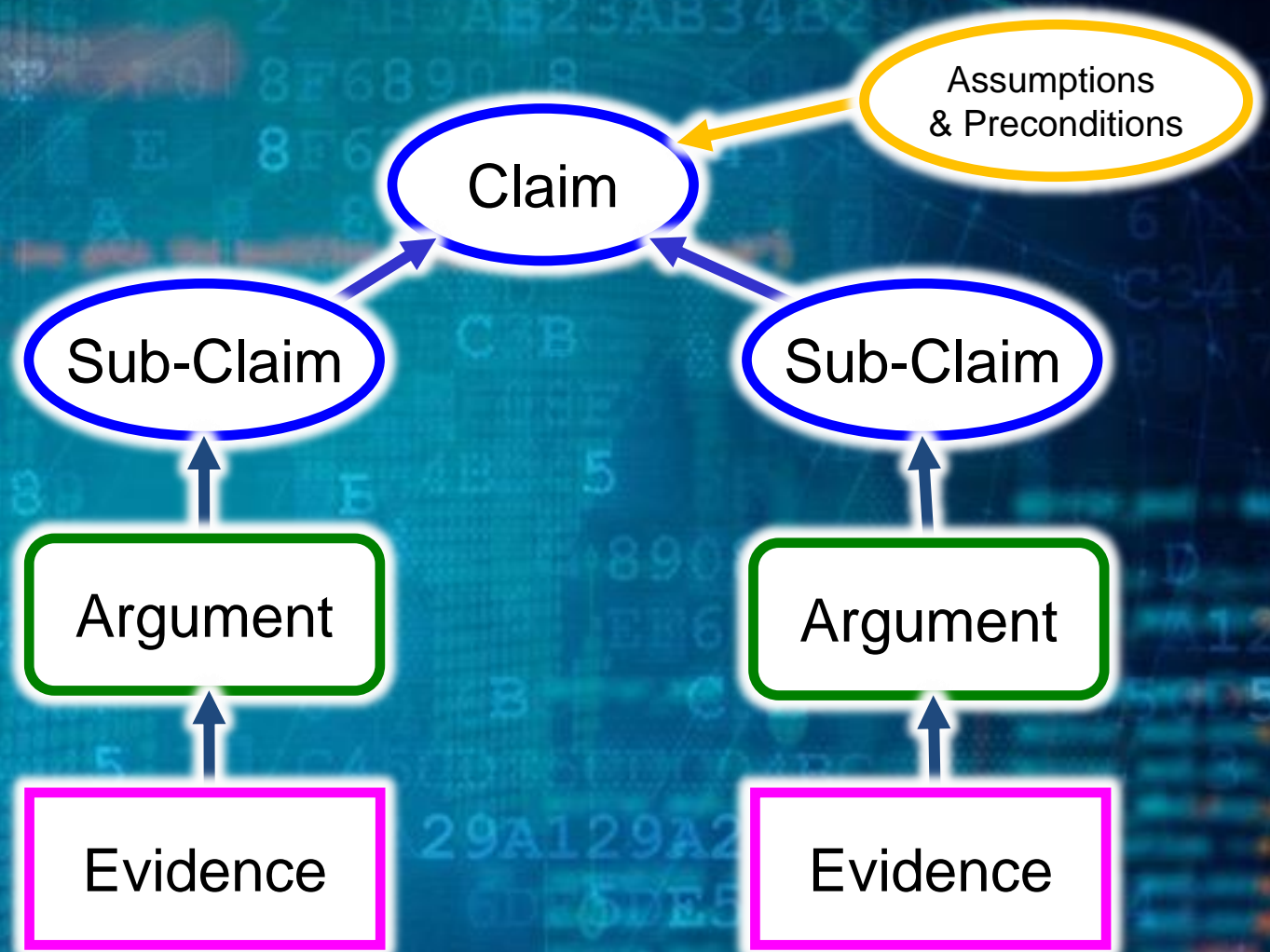


The Basics of an Assurance Case

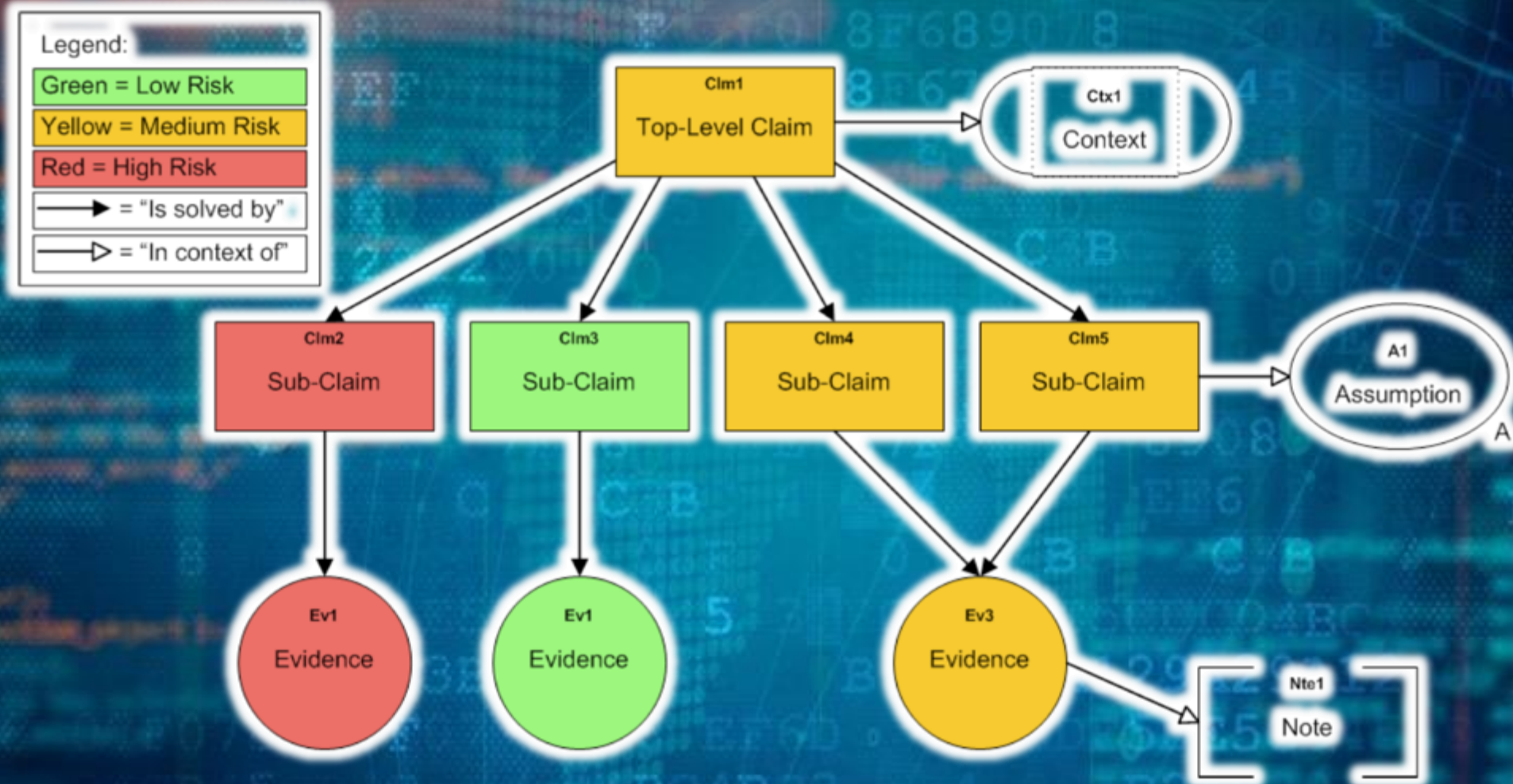
**Claim =
assertion to be proven**

**Argument =
how evidence supports claim**

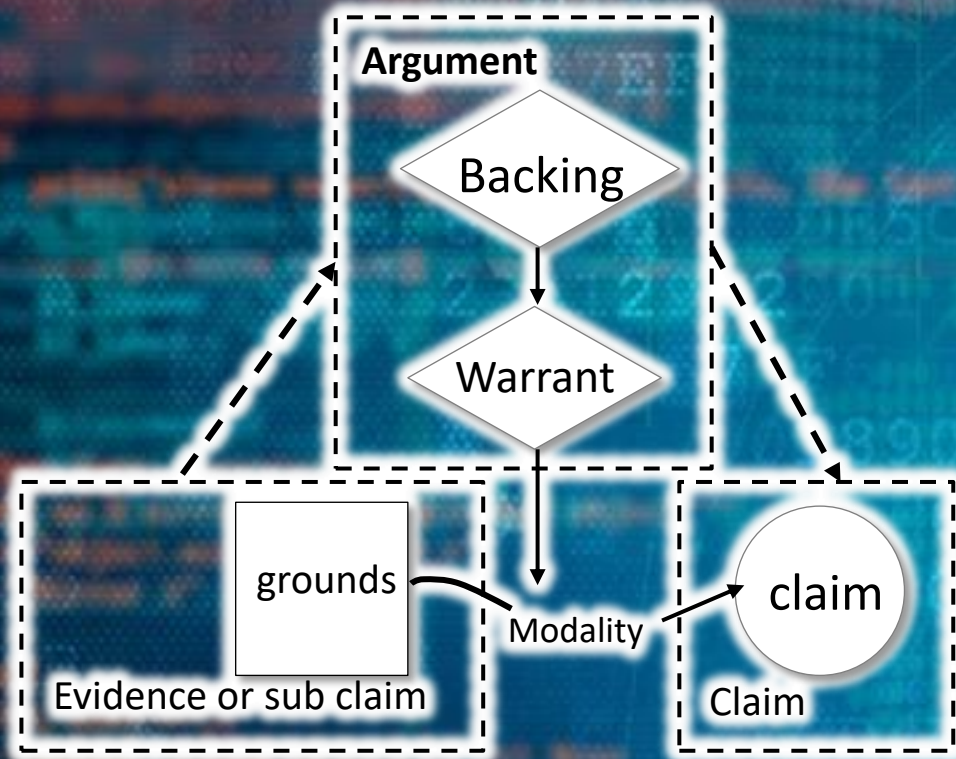
**Evidence =
required documentation**



Safety Case Tooling – Claims-Evidence-Argument in Use for <15 Years



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



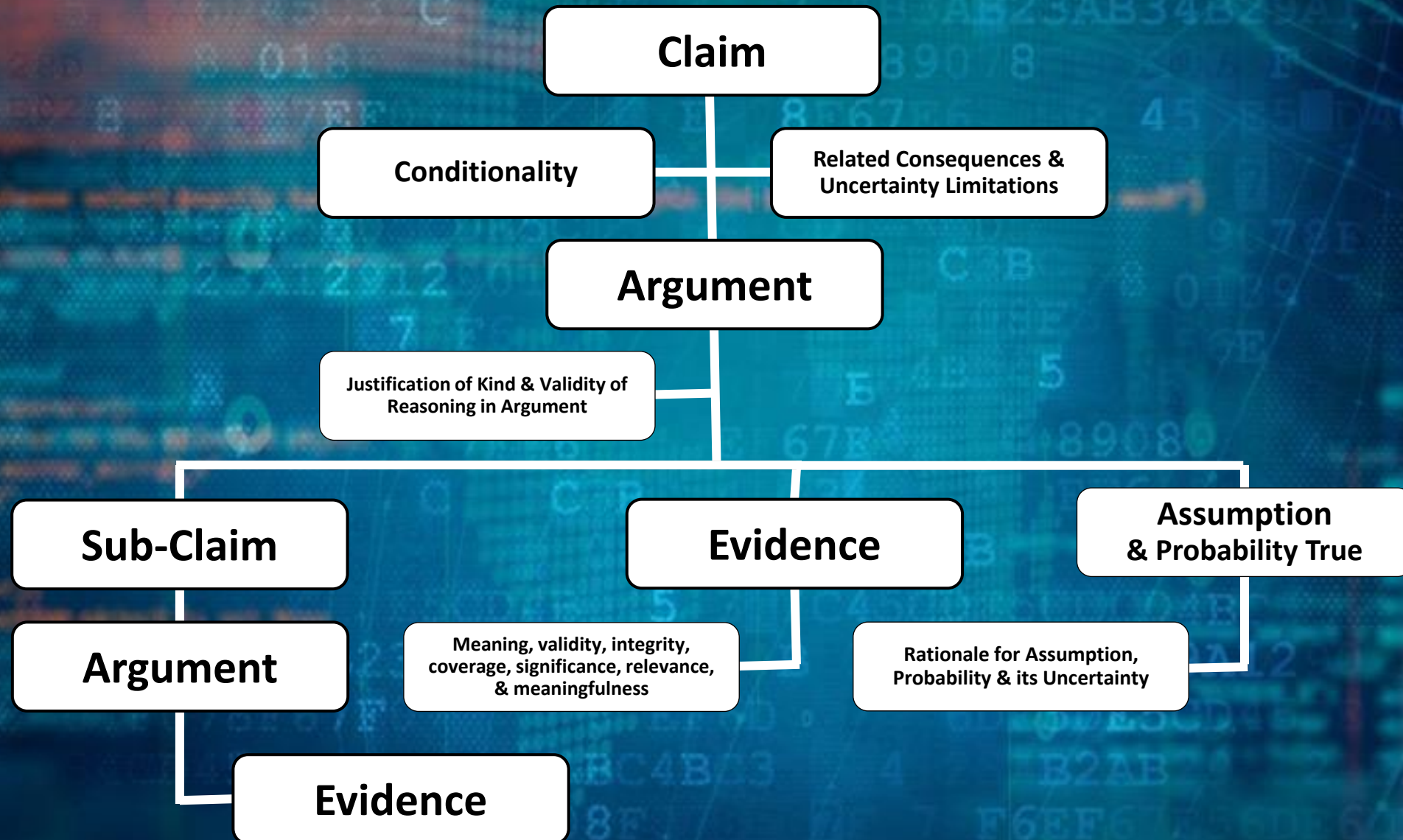
CAE
Claim, Argument, Evidence



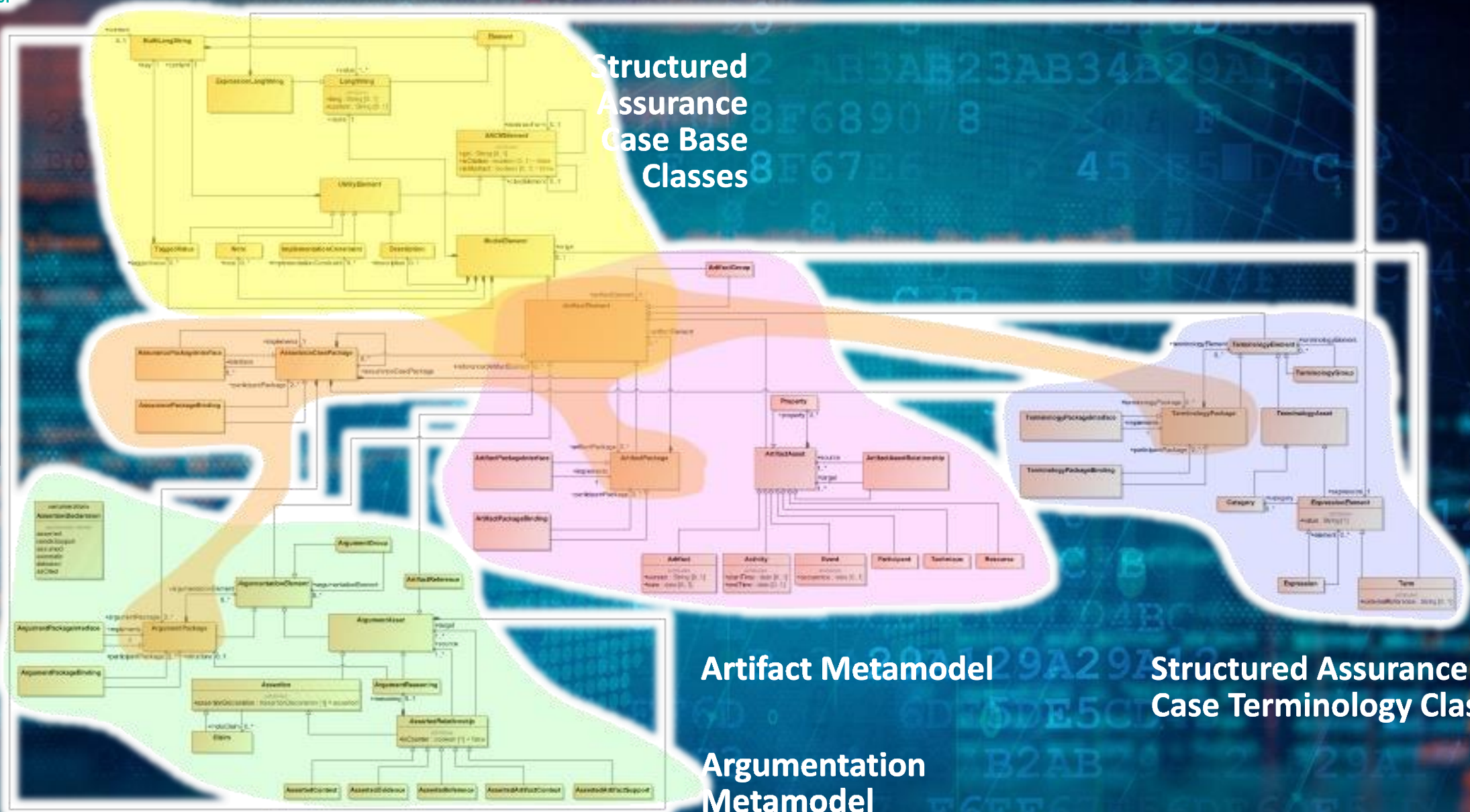
GSN
Goal Structuring Notation

ISO/IEC 15026: Systems & Software Assurance

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



Structured Assurance Case MetaModel (SACM 2.2)



Structured Assurance Case Base Classes

Structured Assurance Case Packages

Artifact Metamodel

Structured Assurance Case Terminology Classes

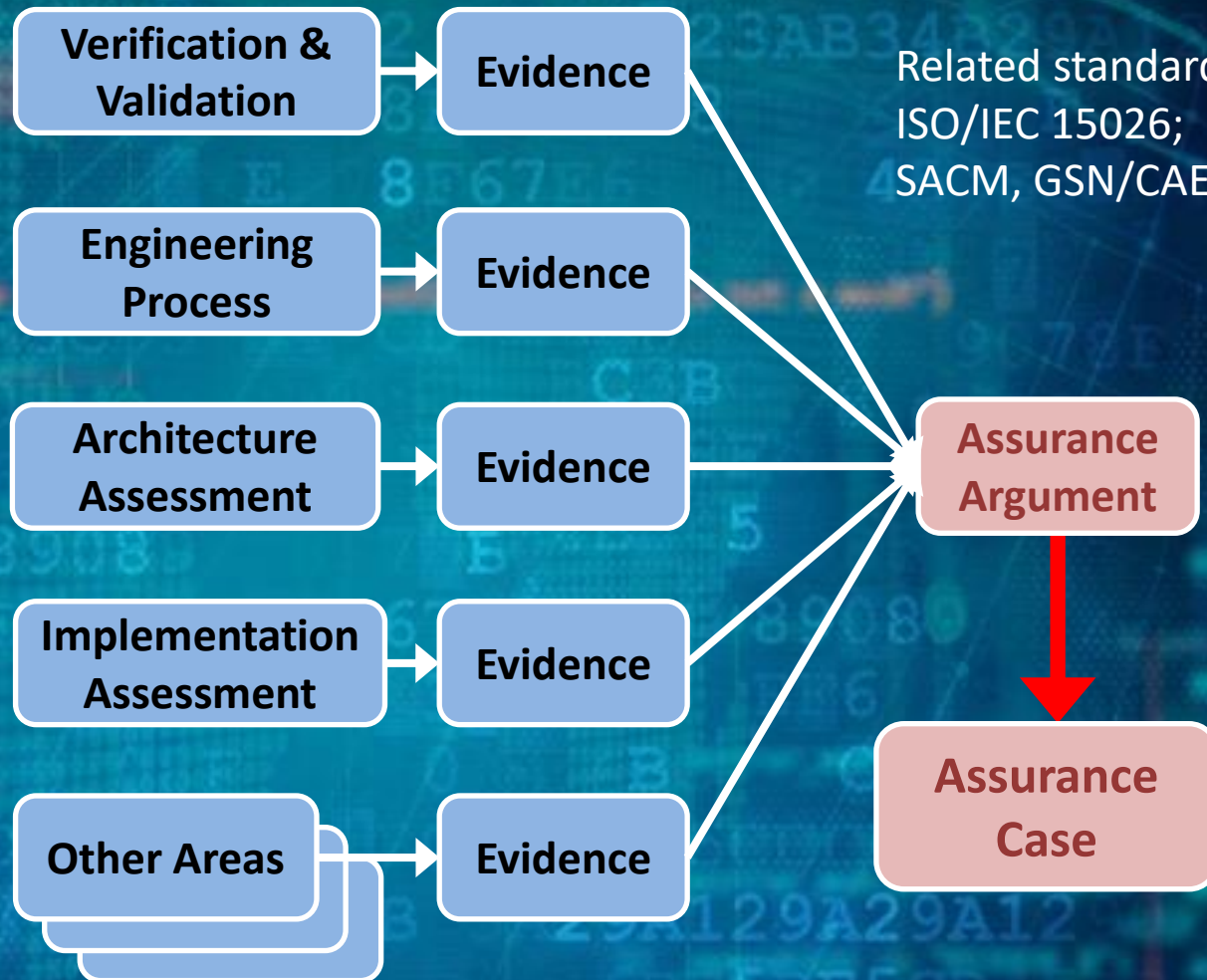
Argumentation Metamodel

Establishing Assurance - Reducing 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 & inefficient safeguards

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

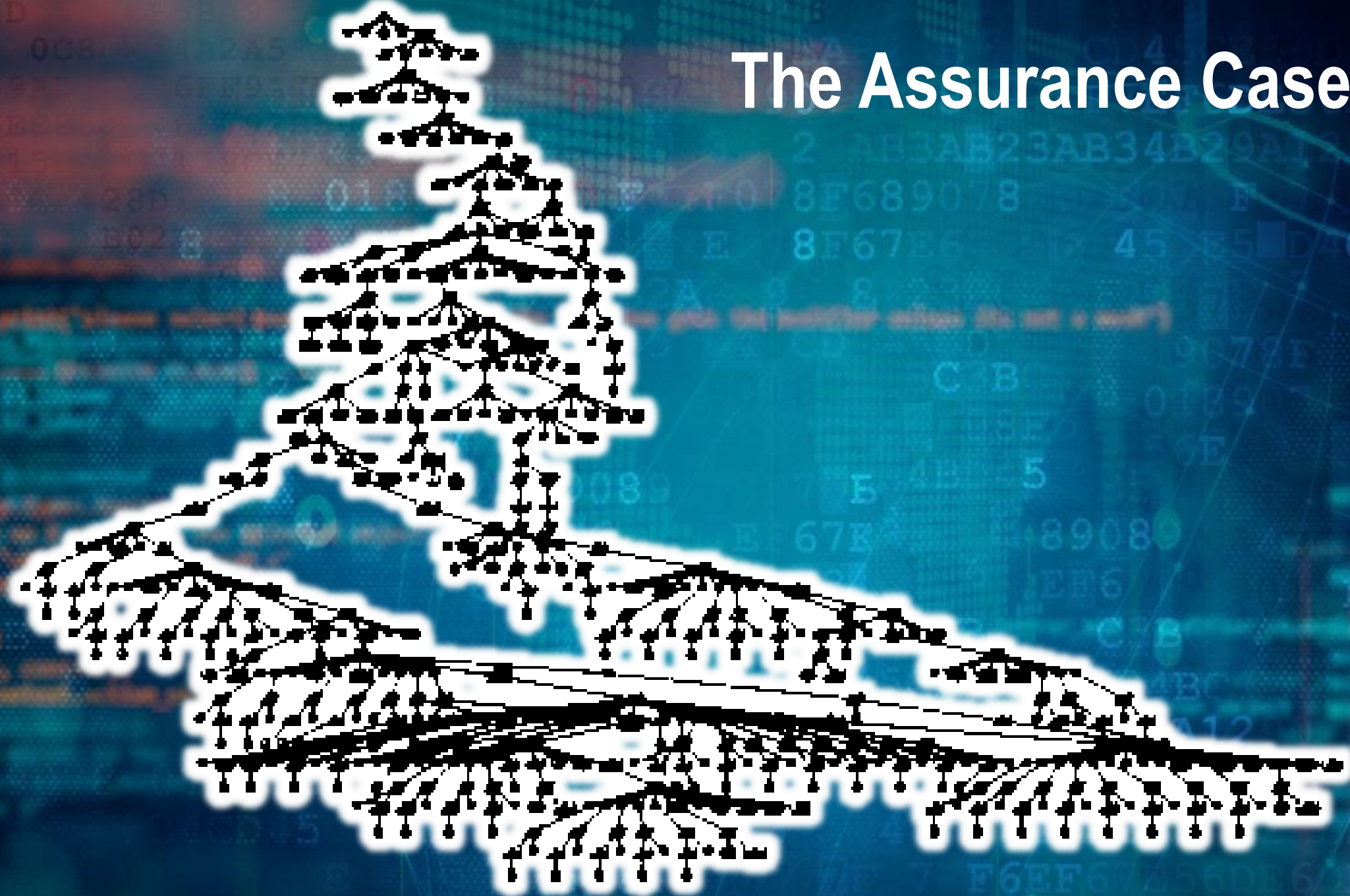


Related standards:
ISO/IEC 15026;
SACM, GSN/CAE

TYPES OF EVIDENCE FOR AN ASSURANCE CASE

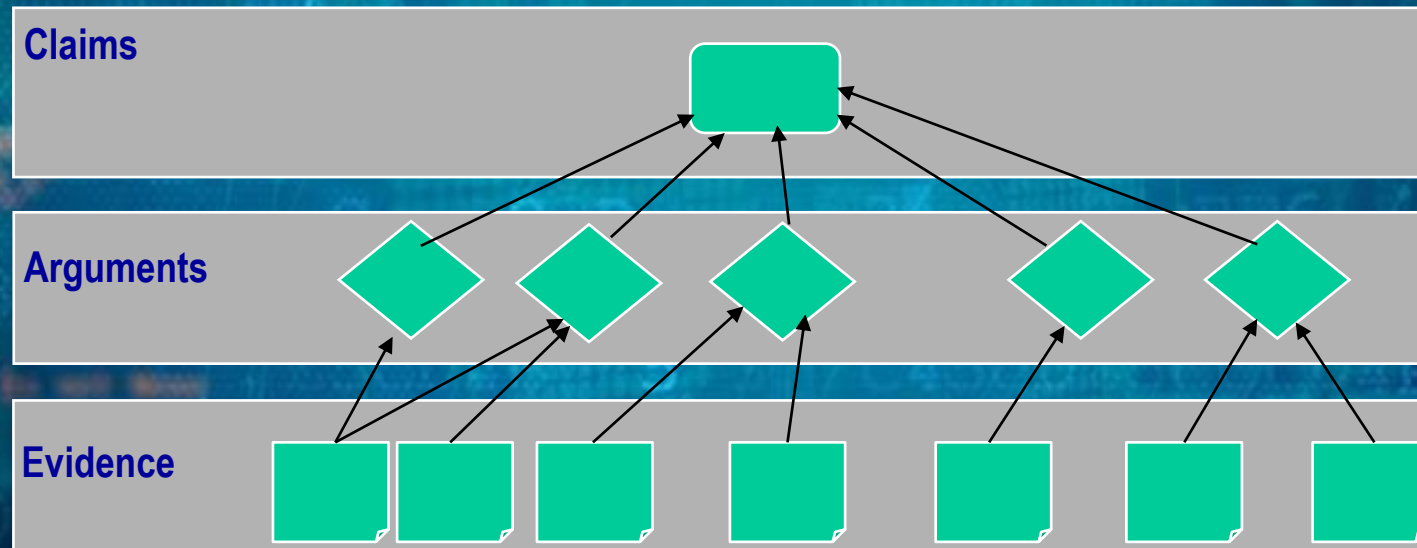
Confidence demands objectivity, scientific method and cost-effectiveness

The Assurance Case



Assurance and Evidence (NIST SP800-160)

- Assurance is best grounded in relevant and credible evidence used to substantiate a claim
 - *“the system is acceptably safe / secure”*
- An assurance case relate claims and evidence
 - *Via structured argumentation and argument patterns*
 - *Automated via assurance case tools*



GSN & CAE: 15+ Years Aviation Safety

Communicating Assurance to Gain Trust

NIST SP800-160

Special Publication 800-160

Systems Security Engineering
A Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems

2.4 SYSTEMS SECURITY ENGINEERING FRAMEWORK

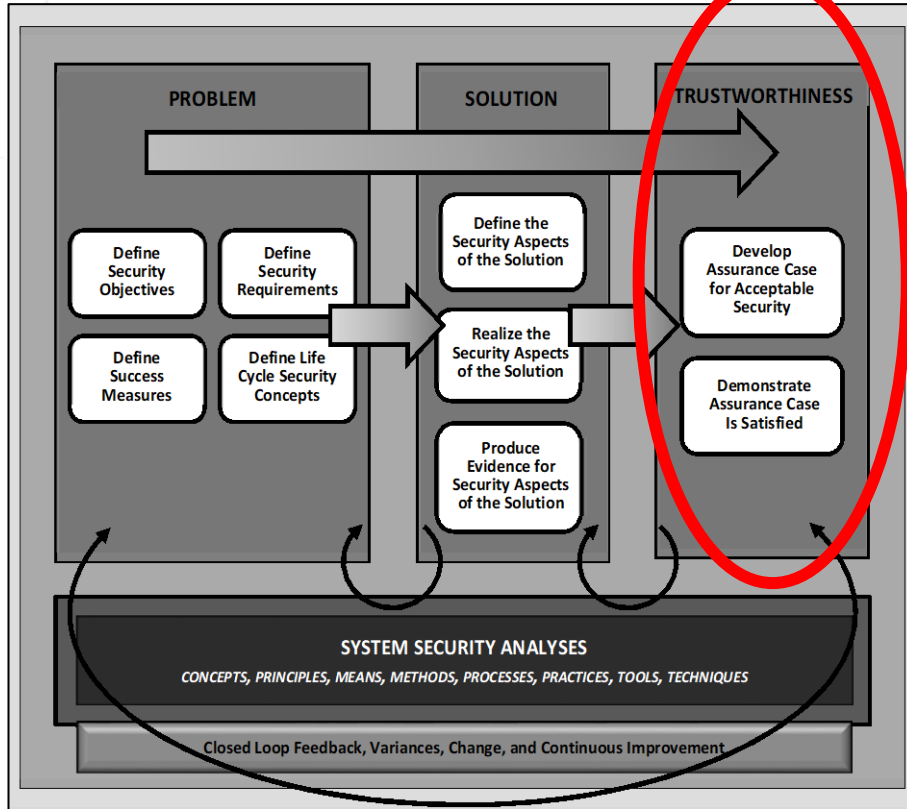


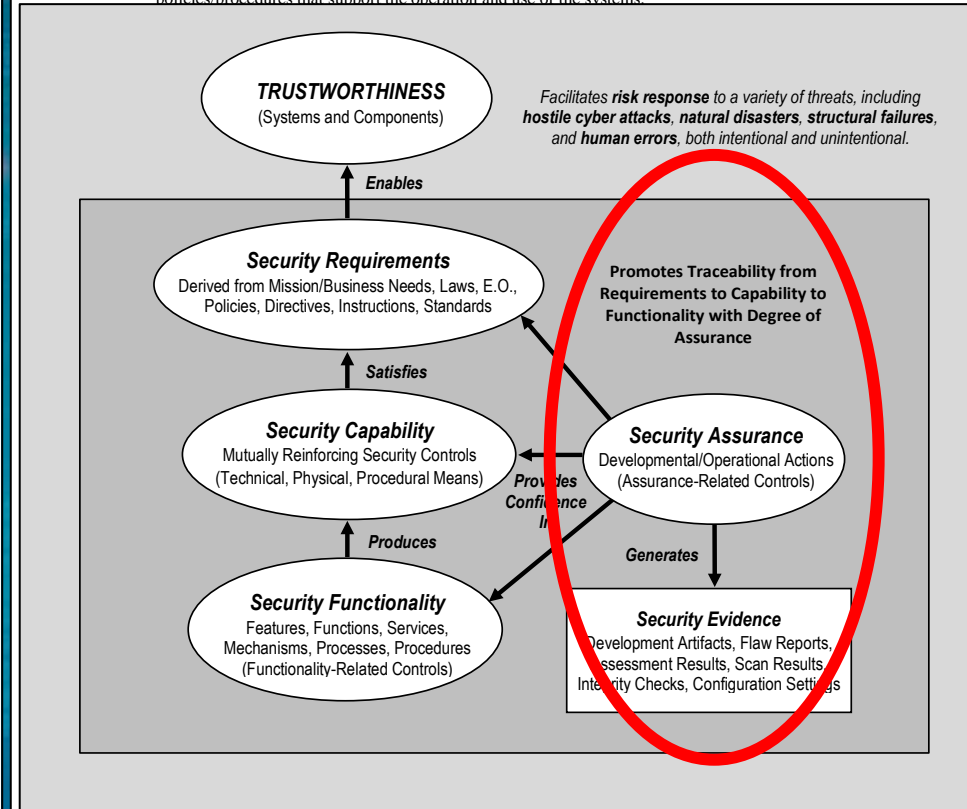
FIGURE 3: SYSTEMS SECURITY ENGINEERING FRAMEWORK

NIST SP800-53r4

Special Publication 800-53 Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

information systems, monitoring established secure configuration settings, and developing policies/procedures that support the operation and use of the systems.



ISO/IEC 15026-2 Assurance Case

OMG Structured Assurance Case Metamodel (SACM)

Infusion Pumps Total Product Life Cycle

Guidance for Industry and FDA Staff

Document issued on: December 2, 2014

The draft of this document was issued on April 23, 2010.

This document supersedes the “Guidance on the Content of Premarket Notification [510(k)] Submissions for External Infusion Pumps,” issued March, 1993.

OMB Control Number: 0910-0766
Expiration Date: 5/31/2017

For questions regarding this document, please contact the Regulatory Affairs Branch, Office of Device Evaluation at 301-796-6104 or via email at richard.chapman@fda.hhs.gov.

For questions regarding safety assurance cases, please contact the Regulatory Affairs Branch, Office of Device Evaluation at 301-796-6104 or via email at richard.chapman@fda.hhs.gov.

For questions regarding pre-clearance inspection of infusion pumps, please contact the Regulatory Affairs Branch, Office of Device Evaluation at 301-796-6104 or via email at richard.chapman@fda.hhs.gov.

For questions pertaining to manufacturer reports, please contact the Regulatory Affairs Branch, Office of Device Evaluation at 301-796-6104 or via email at sharon.kapsch@fda.hhs.gov.



- The technological features of the devices.

You should describe how any differences in technology may affect the comparative safety and performance of your device.

5. Safety Assurance Case

Infusion pump 510(k) submissions typically include changes or modifications to software, materials, design, performance, or other features compared to the predicate. Accordingly, FDA expects that most new devices (as well as most changed or modified devices) will have differences in technological characteristics from the legally marketed predicate device even if sharing the same intended use. Under section 513(i) of the Federal Food, Drug, and Cosmetic Act (the FD&C Act), determinations of substantial equivalence will rely on whether the information submitted, including appropriate clinical or scientific data, demonstrate that the new or modified device is as safe and effective as the legally marketed predicate device and does not raise different questions of safety and effectiveness in comparison to the predicate device.

In determining whether your new, changed, or modified infusion pump is substantially equivalent, FDA recommends that you submit your information through a framework known as a safety assurance case.⁵

The safety assurance case (or safety case) consists of a structured argument, supported by a body of valid scientific evidence that provides an organized case that the infusion pump adequately addresses hazards associated with its intended use within its environment of use. The argument should be commensurate with the potential risk posed by the infusion pump, the complexity of the infusion pump, and the familiarity with the identified risks and mitigation measures.

⁵ Based on FDA's analysis of these devices, FDA expects that most changes or modifications to infusion pumps could significantly affect the safety or effectiveness of the devices and would therefore require submission of a new 510(k). See 21 CFR 807.81(a)(3). Note that a change to the intended use or technology of a 510(k)-cleared device may render the device not substantially equivalent (NSE) to a legally marketed predicate. For detailed information about substantial equivalence and 510(k) submissions, refer to the FDA guidance entitled, *The 510(k) Program: Evaluating Substantial Equivalence in Premarket Notifications (PMA/PMN)* (<http://www.fda.gov/oc/ohrt/medicaldevices/UCM284443.pdf>). Any such device may thus be a class III device and require a premarket approval application (PMA), unless the device is reclassified under section 513 of the Federal Food, Drug, and Cosmetic Act.

⁶ For more information about assurance case reports, see, for example: Graydon, P., J. Knight, and E. Strunk, "Assurance Based Development of Critical Systems," Proc. of 37th Annual International Conference on Dependable Systems and Networks, Edinburgh, U.K., 2007; Kelly, T., *Arguing Safety—A Systematic Approach to Managing Safety Cases*, Ph.D. Dissertation, University of York, U.K., 1998; Kelly, T., "Reviewing Assurance Arguments - A Step-by-Step Approach," Proc. of Workshop on Assurance Cases for Security - The Metrics Challenge, Dependable Systems and Networks, July 2007; Kelly, Tim, and J. McDermid, "Safety Case Patterns - Reusing Successful Arguments," Proc. of IEEE Colloquium on Understanding Patterns and Their Application to System Engineering, London, Apr. 1998; Weinstock, Charles B. and Goodenough, John B., "Towards an Assurance Case Practice for Medical Devices," Carnegie Mellon Software Engineering Institute, October 2009; Hawkins, Richard, et al., *A New Approach to Creating Clear Safety Arguments*, Safety-critical Systems Symposium, Southampton, UK, February 2011; UK Ministry of Defence, Defence Standard 00-56, *Safety Management Requirements for Defence Systems - Part 1 and Part 2*, June 2007.

Support for Safety Case Generation via Model Transformation

Chung-Ling Lin, Wuwei Shen
Department of Computer Science
Western Michigan University
Kalamazoo, MI, USA
(chung-ling.lin, wuwei.shen}@wmich.edu

Richard Hawkins
Department of Computer Science
The University of York
York, UK
richard.hawkins@york.ac.uk

ABSTRACT

Assessing the safety of systems under ever increasing confidence is a great challenge. One method to address this is the use of assurance cases. This paper describes a framework for generating assurance cases for safety-critical systems. The framework uses a metamodel to generate a safety assurance case from a safety assurance case template. The framework also provides a means for generating a safety assurance case from a safety assurance case template.

Keywords

Compliance check systems; safety case

1. INTRODUCTION

Assessing the safety of systems, such as safety-critical systems, is a challenge for industry and academia. This is because safety-critical systems are often complex and have high stakes. The construction and verification of a safety case are a daunting task.

Copyright retained by the author(s).

SIGBED Rev. 10/2013

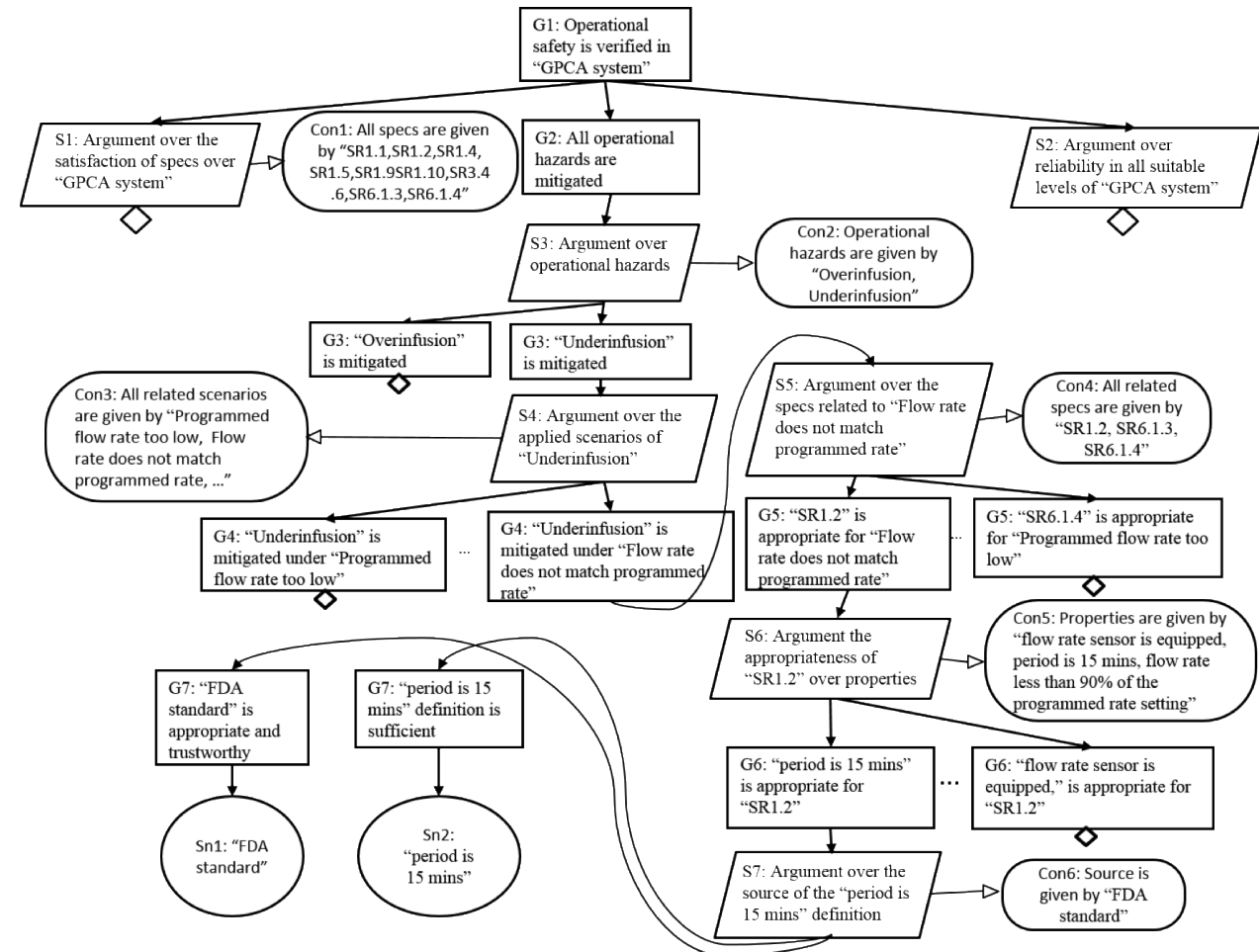


Figure 9 Safety case model of GPCA system

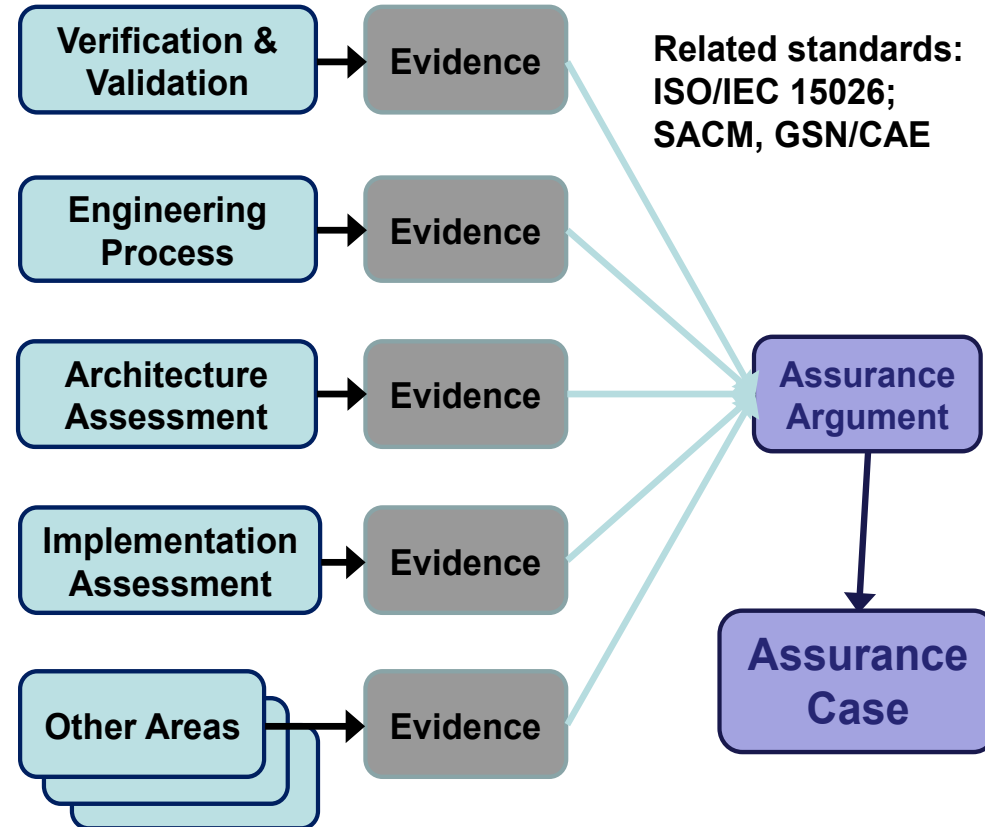
Inspectable, Composable, Efficient, Evidence-base Assurance Utilizing the Assurance Case

Establishing Assurance - Reducing 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 & inefficient safeguards

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

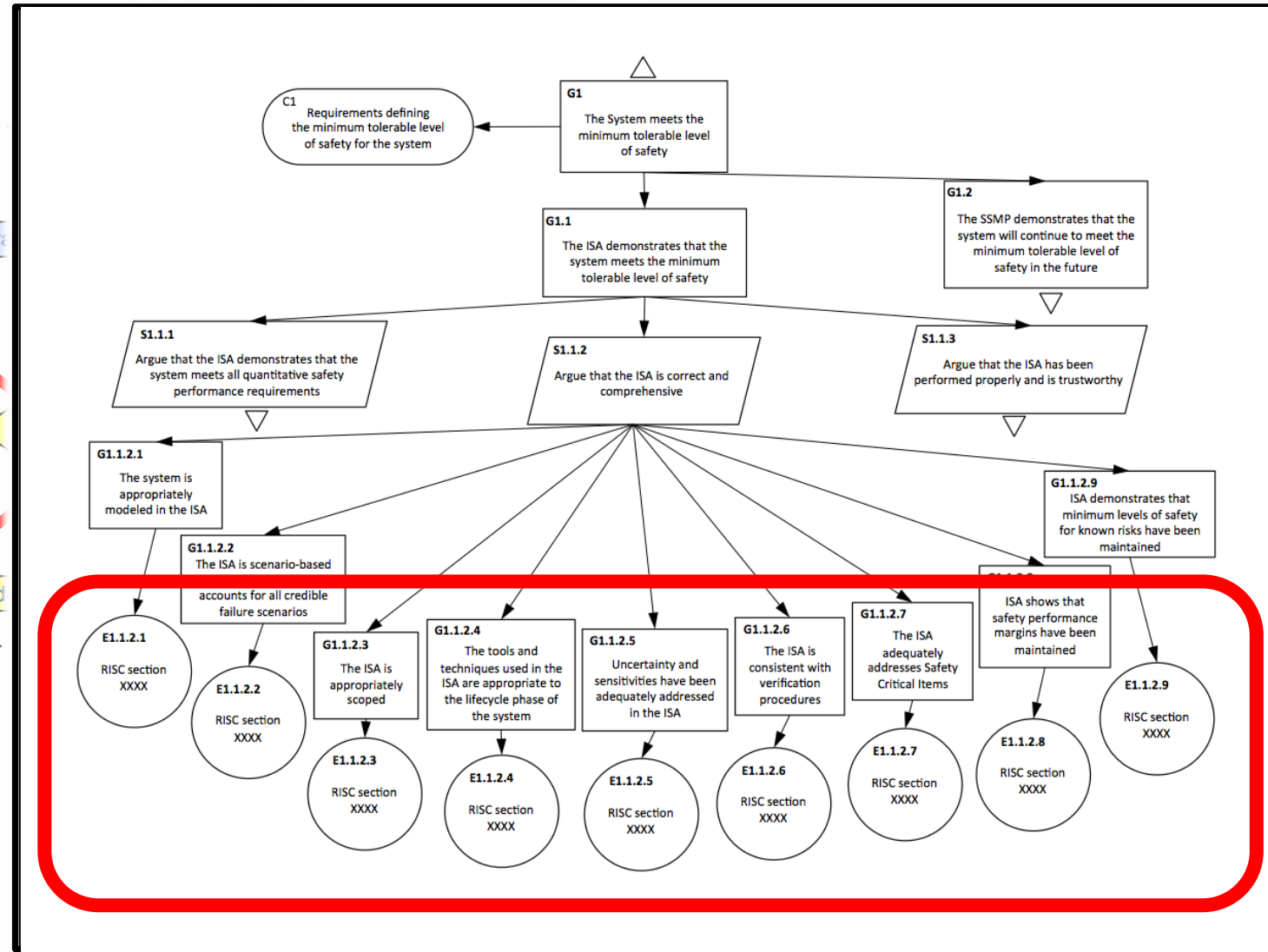
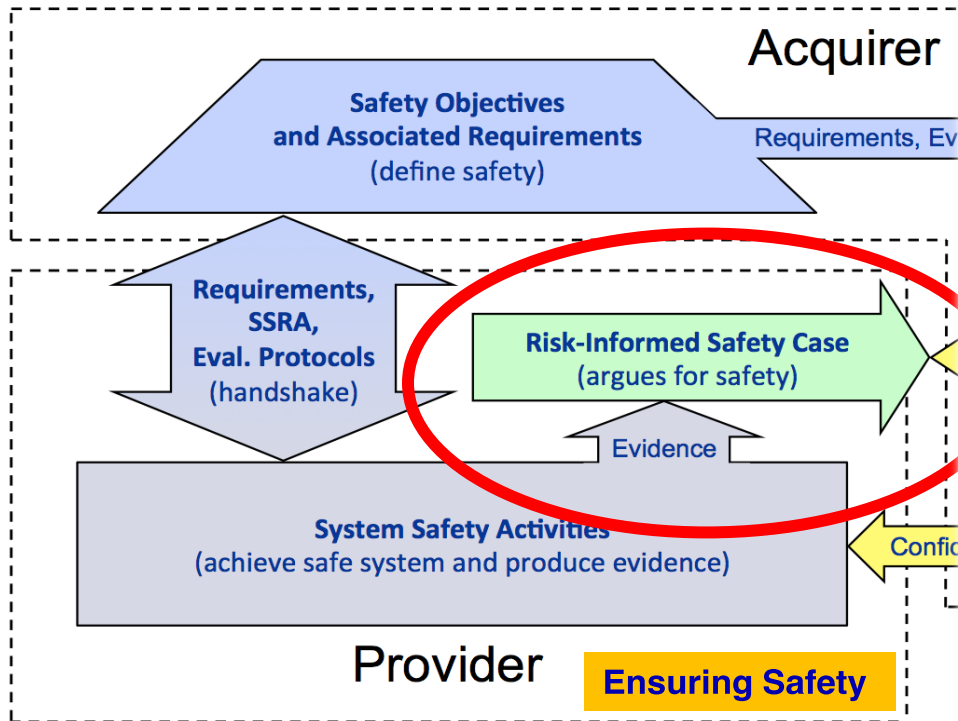
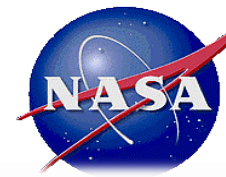


Related standards:
ISO/IEC 15026;
SACM, GSN/CAE

TYPES OF EVIDENCE FOR AN ASSURANCE CASE

Confidence demands objectivity, scientific method and cost-effectiveness

NASA System Safety Framework (cont.)



2.4 SYSTEMS SECURITY ENGINEERING FRAMEWORK

The *systems security engineering framework* [McEville15] provides a conceptual view of the key contexts within which systems security engineering activities are conducted. The framework defines, bounds, and focuses the systems security engineering activities and tasks, both technical and nontechnical, towards the achievement of stakeholder security objectives and presents a coherent, well-formed, evidence-based case that those objectives have been achieved.²⁰ The framework is independent of system type and engineering or acquisition process model and is not to be interpreted as a sequence of flows or process steps but rather as a set of interacting contexts, each with its own checks and balances. The systems security engineering framework emphasizes an integrated, holistic security perspective across all stages of the system life cycle and is applied to satisfy the milestone objectives of each life cycle stage. Figure 3 provides an overview of the systems security engineering framework and its key components.

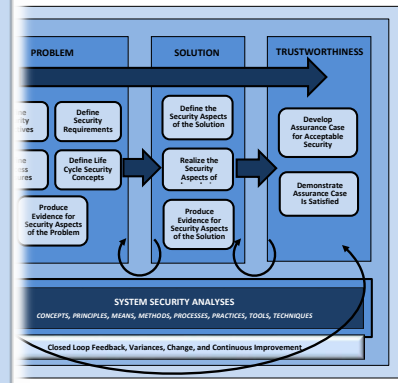


FIGURE 3: SYSTEMS SECURITY ENGINEERING FRAMEWORK

defines three contexts within which the systems security engineering activities are conducted. The three contexts are the *problem* context, the *solution* context, and the *trustworthiness* context. The three contexts helps to ensure that the engineering of a system is driven by a complete understanding of the problem articulated in a set of stakeholder security objectives [ASA11].

NIST Special Publication 800-160

Systems Security Engineering
Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems

RON ROSS
 Computer Security Division
 National Institute of Standards and Technology

MICHAEL McEVILLEY
 The MITRE Corporation

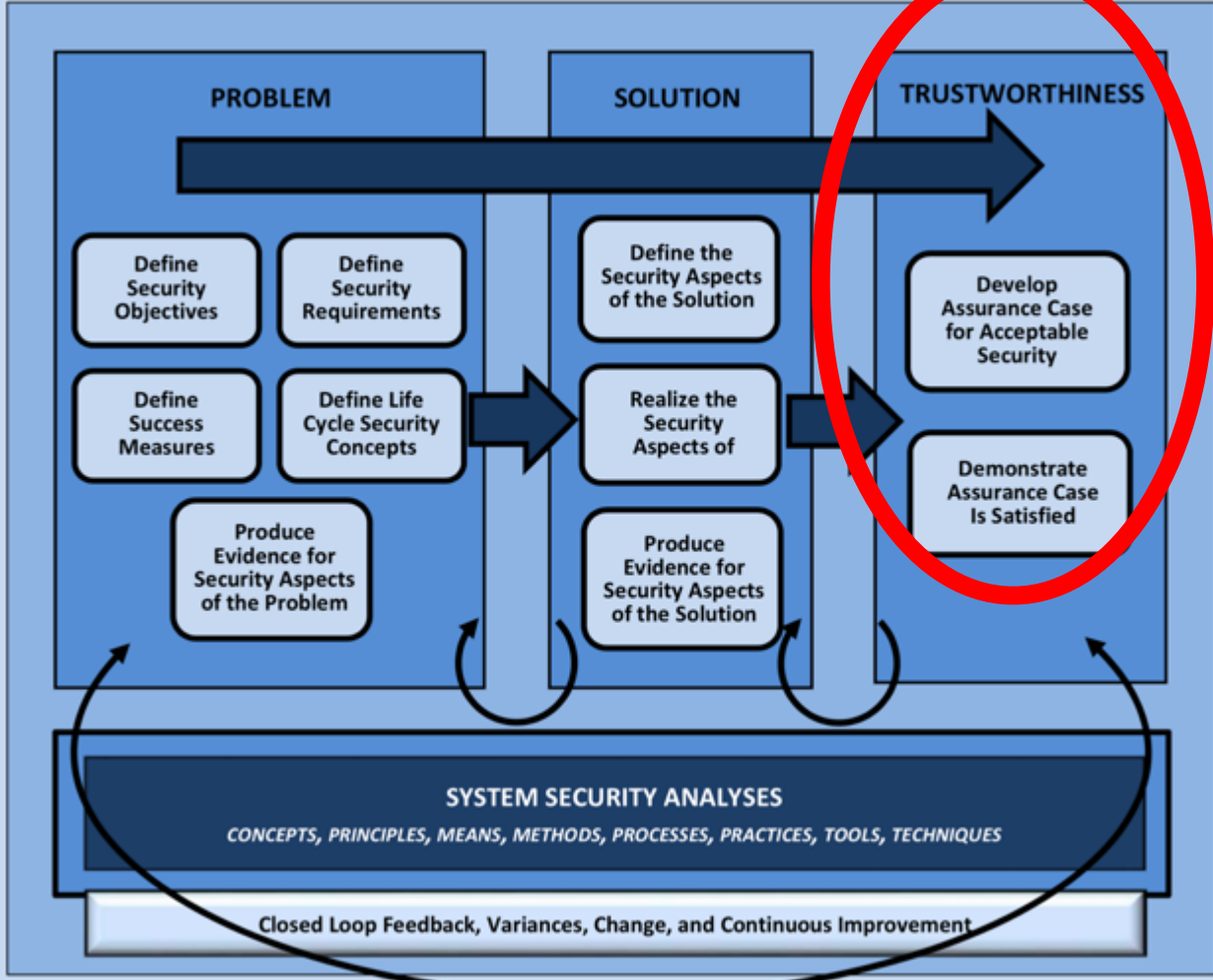
JANET CARRIER OREN
 Legg Mason

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-160>

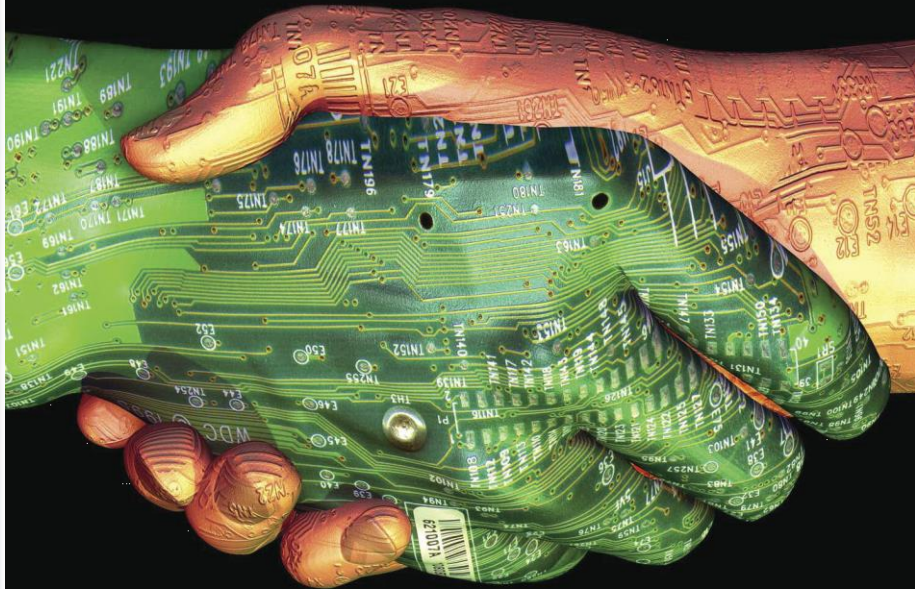
November 2016
 INCLUDES UPDATES AS OF 01-03-2018; PAGE XIII



U.S. Department of Commerce
 Penny Pritzker, Secretary
 National Institute of Standards and Technology
 Willie May, Under Secretary of Commerce for Standards and Technology and Director



Special theme:
**Trustworthy
 Systems of Systems**
 Safety & Security Co-engineering



Also in this issue:

Keynote:
 "Trustworthy Systems of Systems –
 A Prerequisite for the Digitalization of Industry",
 by Werner Steinhögl, European Commission

Joint ERCIM Actions:
 PaaSage and OW2 Announced Platform
 Availability on the AppHub Marketplace

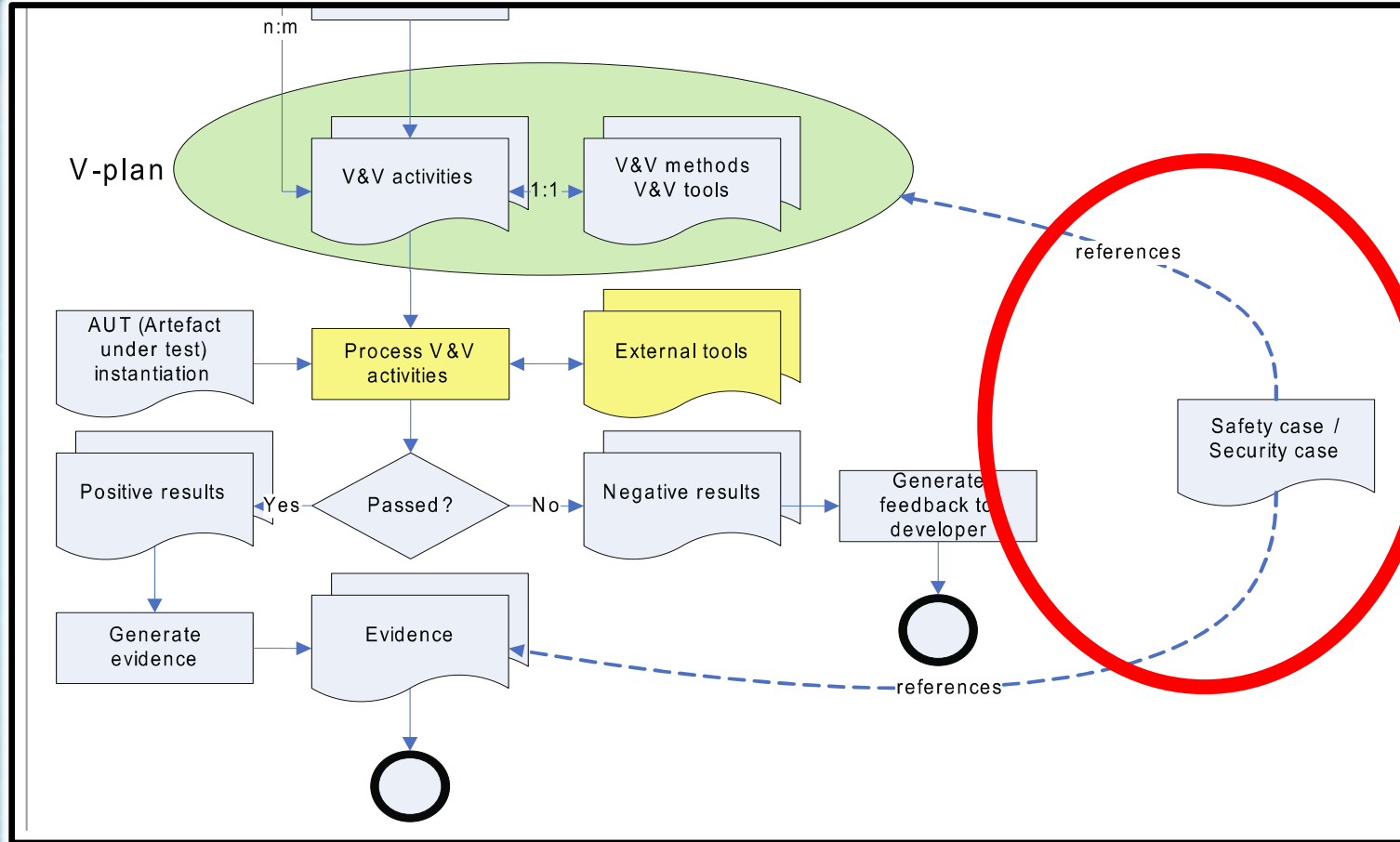
Research and Innovation:
 Making the Internet
 of Things Fly

European Research Consortium for Informatics and Mathematics (ERCIM)

Workflow Engine for Analysis, Certification and Test of Safety and Security-Critical Systems

by Christoph Schmittner, Egbert Althammer and Thomas Gruber

Certification and Qualification are important steps for safety- and security-critical systems. In Cyber-Physical Systems (CPS), connected Systems of Systems (SoS) and Internet of Things (IoT), safety and



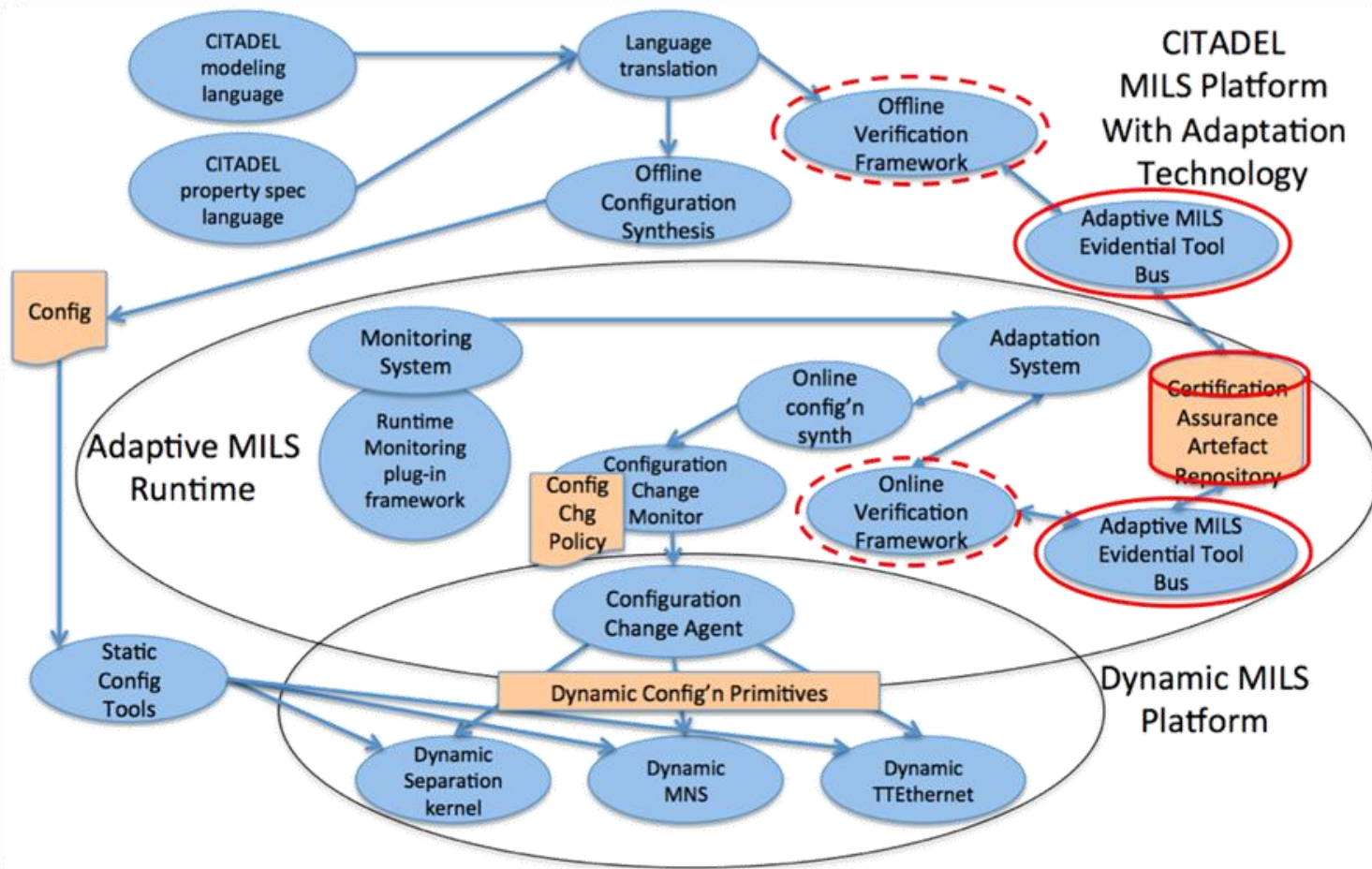


Figure 1: AM-ETB role in CITADEL



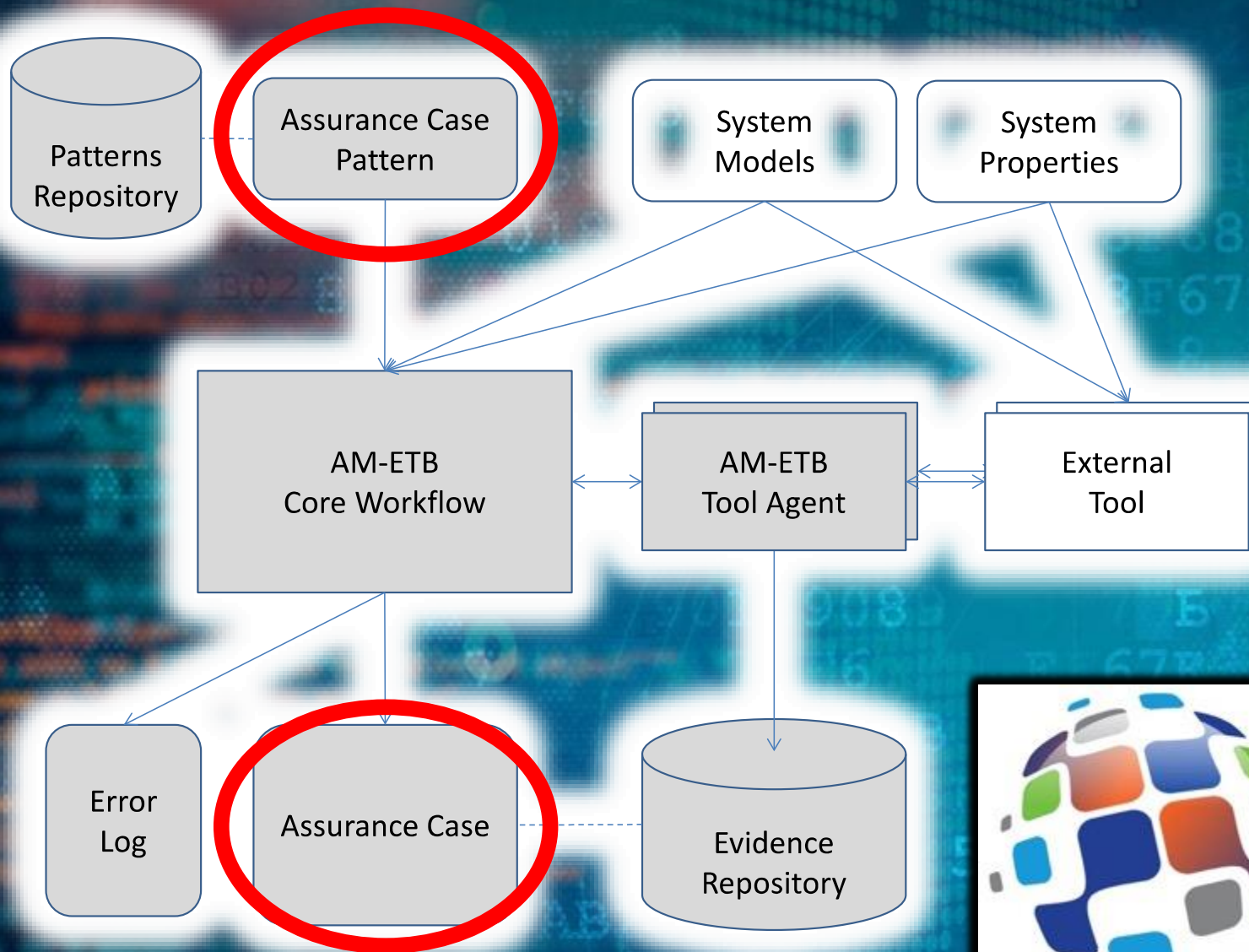


Figure 2: AM-ETB System Architecture



CITADEL
CRITICAL INFRASTRUCTURE PROTECTION
USING ADAPTIVE MILS



Dependability
Engineering
Innovation for Cyber Physical
Systems

The Assurance Case



Medical
Space
Aeronautics
Rail
Automotive
Shipping
Autonomous
Critical Infrastructure
Cyber Physical Systems...

A Sample Security Assurance Case Pattern

E. Kenneth Hong Fong, Project
David A. Wheeler

December 2018

Approved for public release; distribution is unlimited.

IDA Paper P-9278

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1822

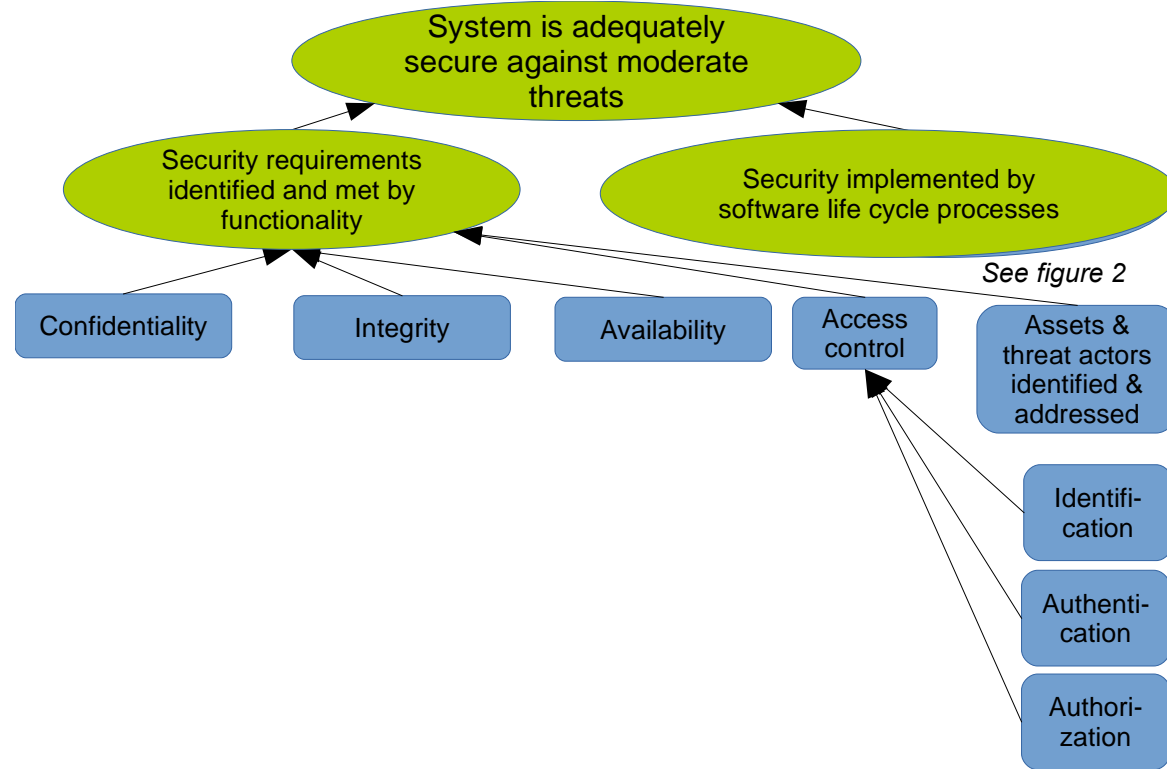


Figure 1. Top Level of an Assurance Case

Contents

- 1. Introduction 1-1
- 2. Sample Assurance Case Pattern 2-1
 - A. Top Level 2-1
 - B. Life Cycle Processes 2-4
 - 1. Security in Design 2-5
 - 2. Security in Integration and Verification 2-9
 - 3. Security in Transition and Operation 2-9
 - 4. Security in Maintenance 2-10
 - 5. Certifications and Controls 2-10
 - C. Implementation 2-11
 - 1. Common Implementation Errors Countered 2-13
 - 2. Common Misconfigurations Countered 2-15
 - 3. Hardening Applied 2-15
 - 4. Securely Reuse Software 2-16
 - D. Other Life Cycle Processes 2-17
 - E. Real Assurance Cases Include Supporting Text 2-18
 - F. Determining Adequacy 2-19
- Sample Assurance Case Application 3-1
 - A. Top Level 3-1
 - 1. Sample Supporting Text: Email Addresses 3-3
 - 2. Sample Supporting Text: Data Modification Requires Authorization 3-5
 - 3. Sample Graphical Representation That Data Modification Requires Authorization 3-6
 - B. Life Cycle Processes 3-7
 - C. Implementation 3-9
 - D. Other Life Cycle Processes 3-11
- Conclusions 4-1
- Appendix A . Processes Are Neither Phases nor Stages A-1
- Appendix B . How an Assurance Case can Support Other Documents and Processes ..B-1
 - 1. DoD Instruction 5000.02 B-1
 - 2. DoD Program Protection Plan (PPP) B-2
 - 3. DoD Cybersecurity Strategy B-3
 - 4. DoD Instruction 5200.44 B-4
 - 5. NIST Cybersecurity Risk Management Framework (RMF) / DoDI 8510.01 B-5
 - 6. NIST SP 800-160 volume 1 B-6
 - 7. ISO/IEC/IEEE 12207 B-7

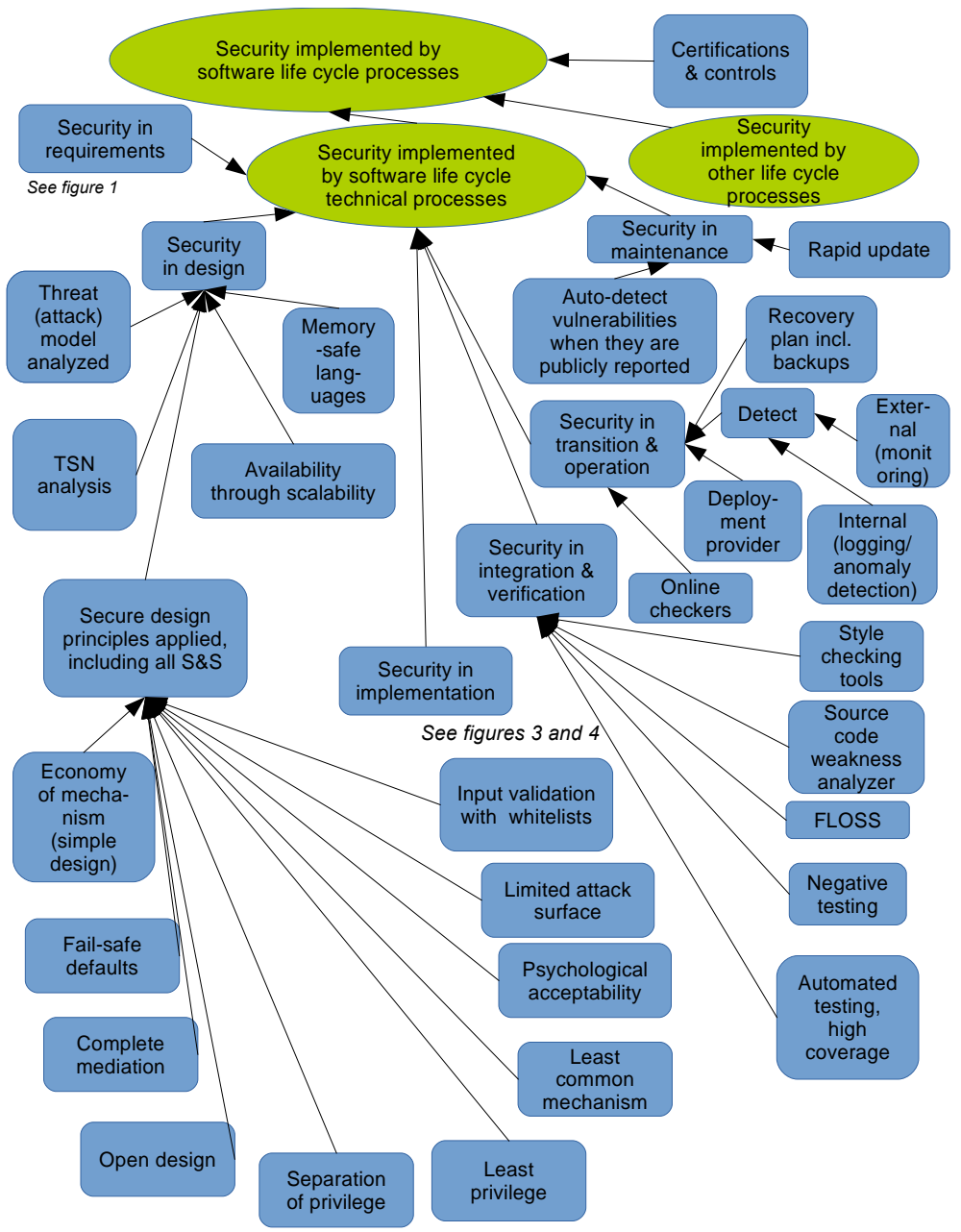


Figure 2. Life Cycle Processes

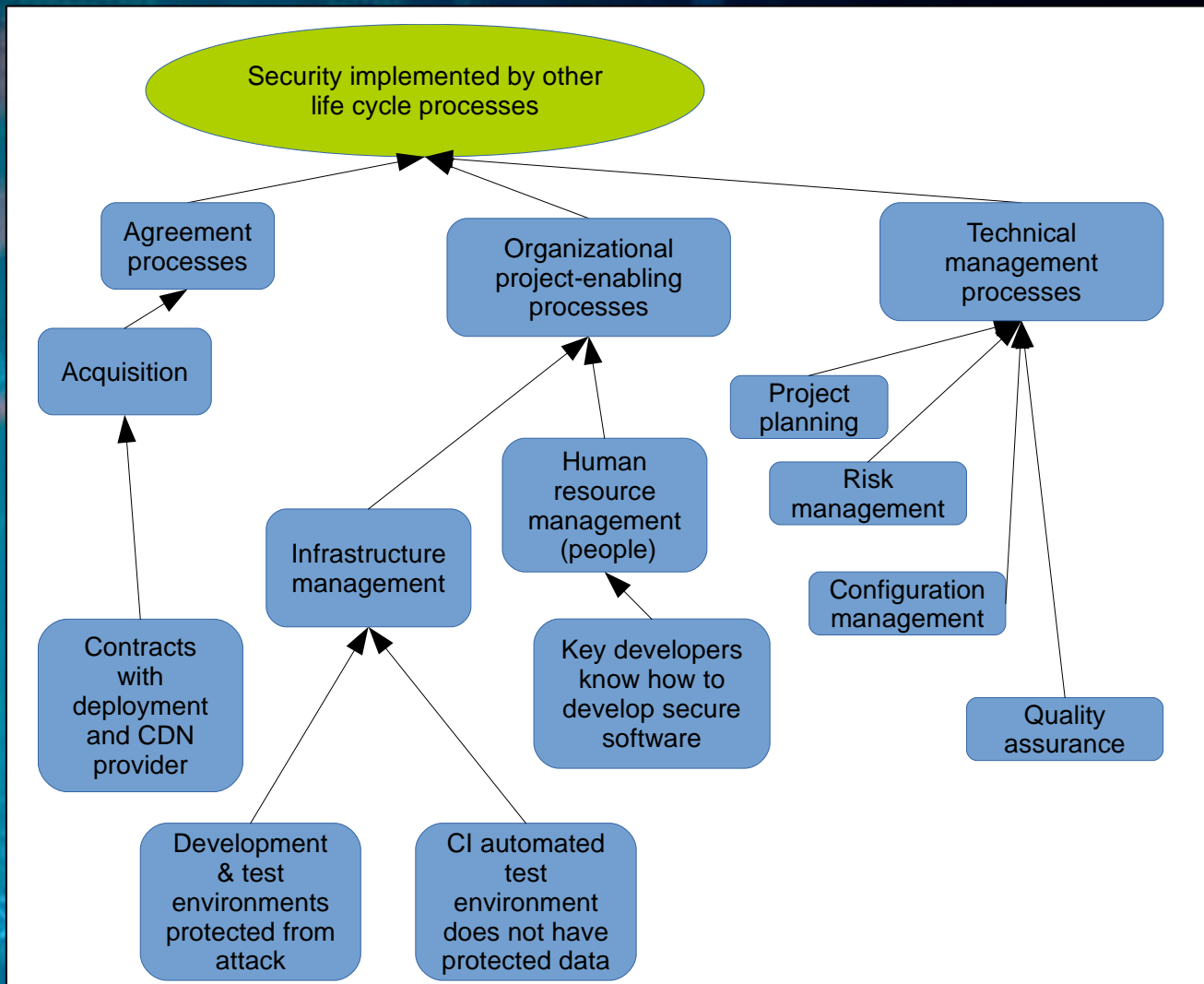


Figure 5. Other Life Cycle Processes

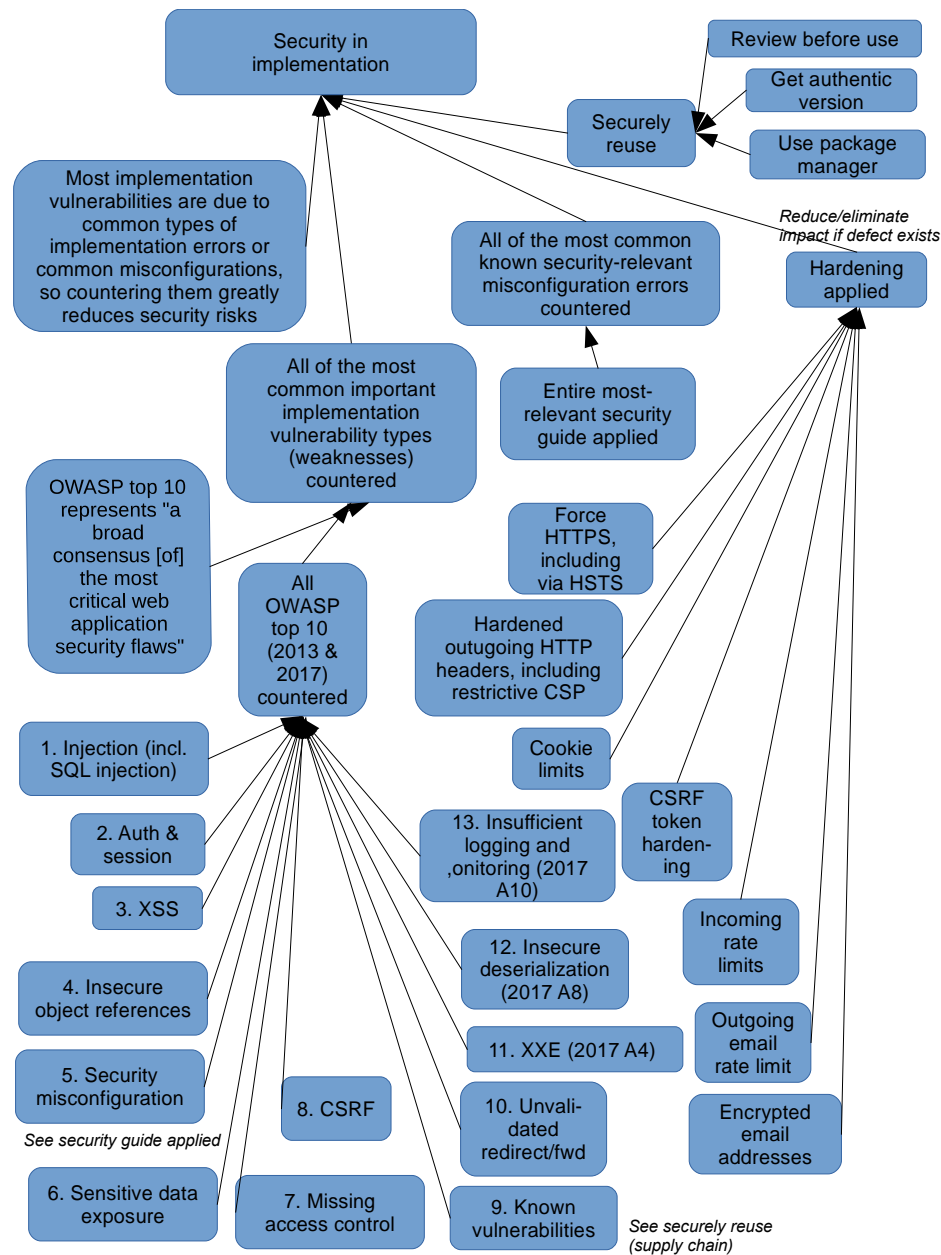


Figure 3. Implementation—Web Application

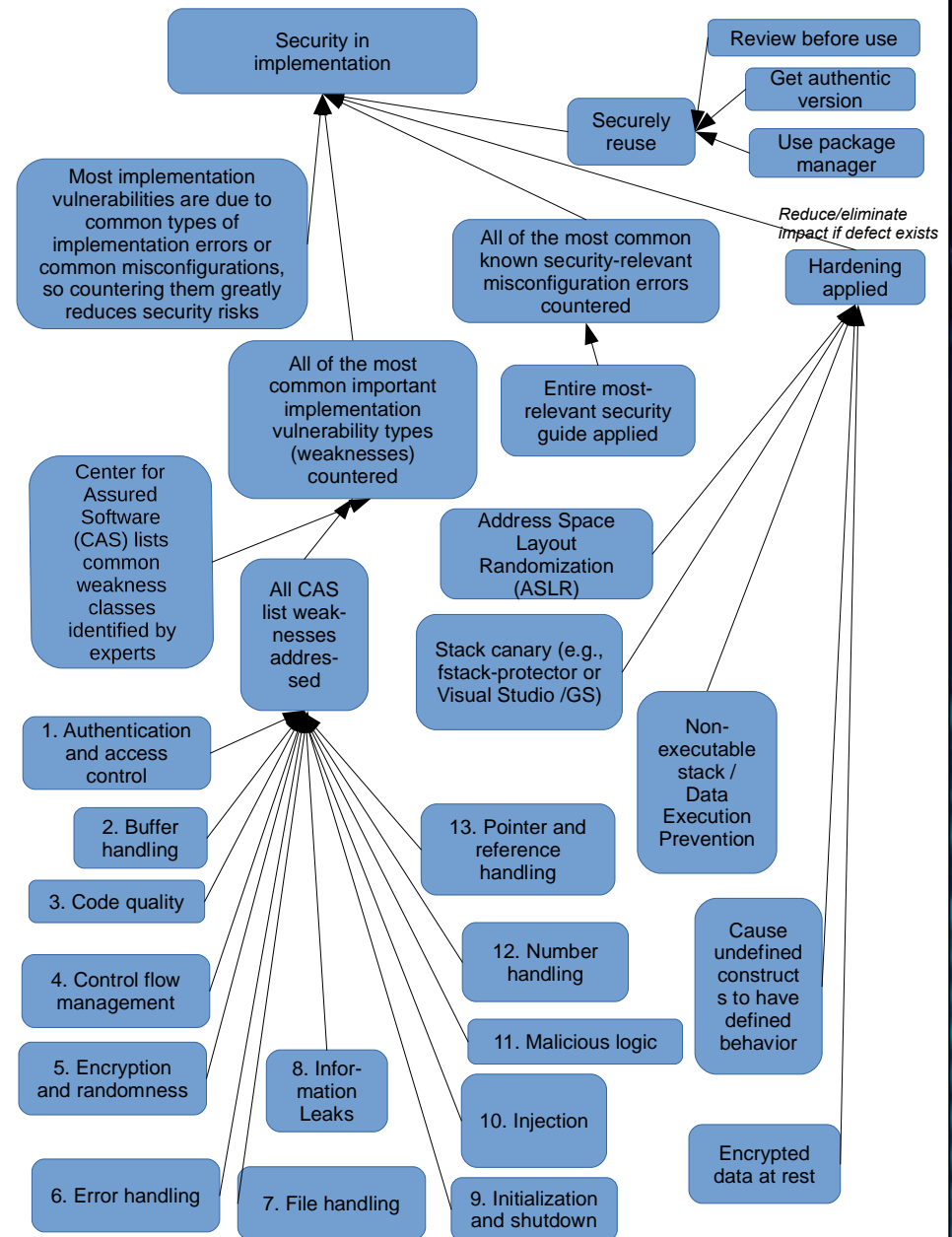


Figure 4. Implementation—Embedded System

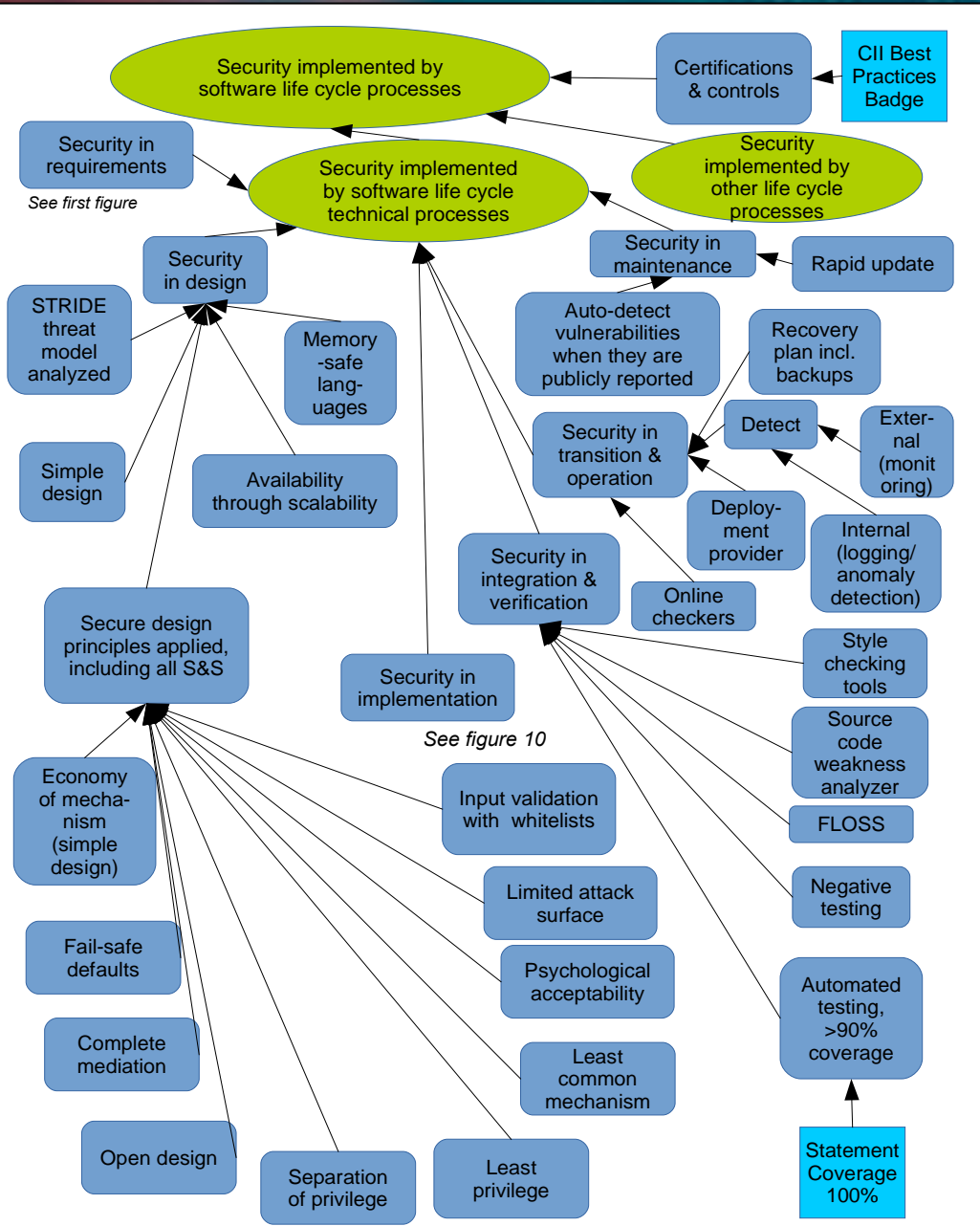


Figure 9. Application: Life Cycle Processes

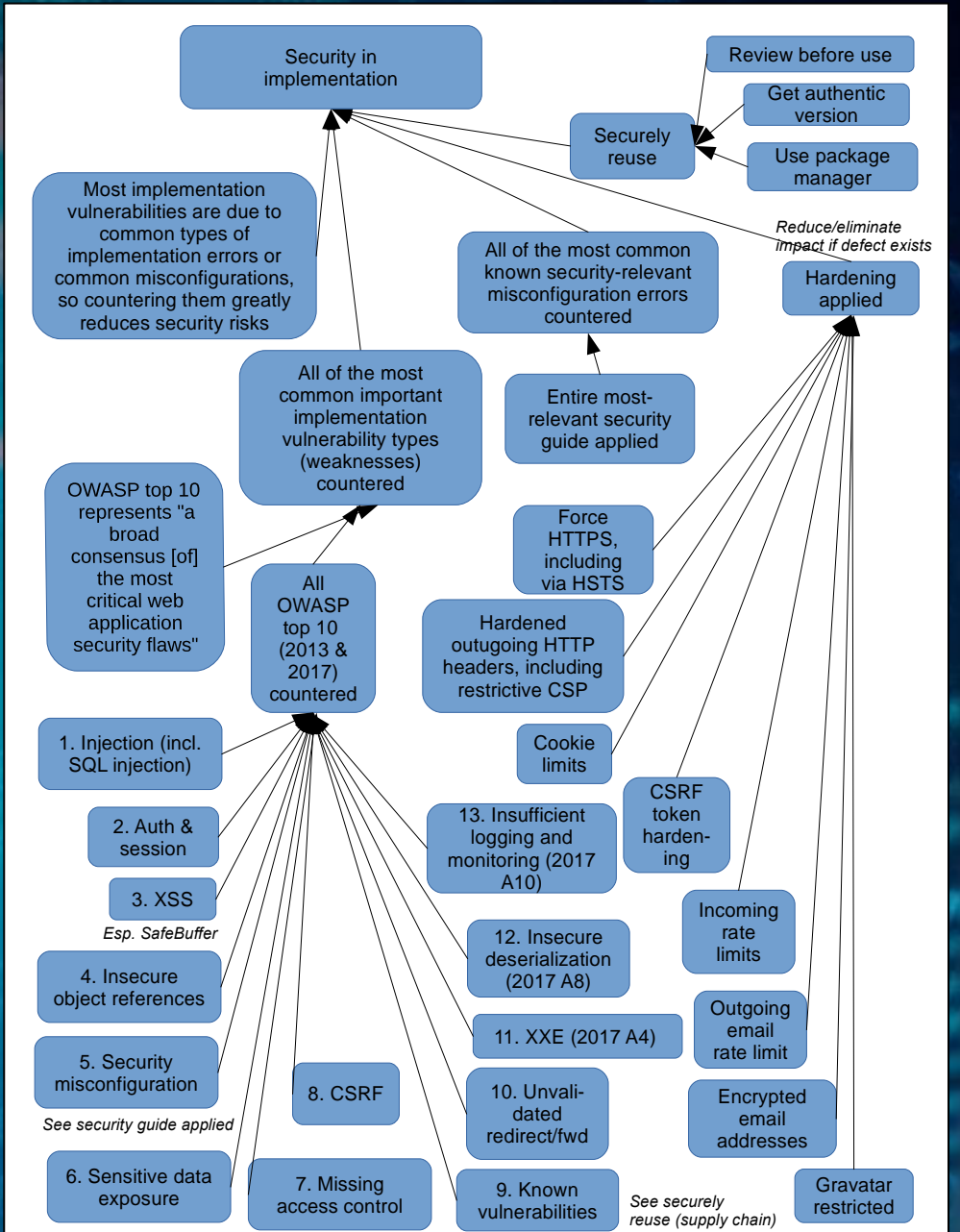
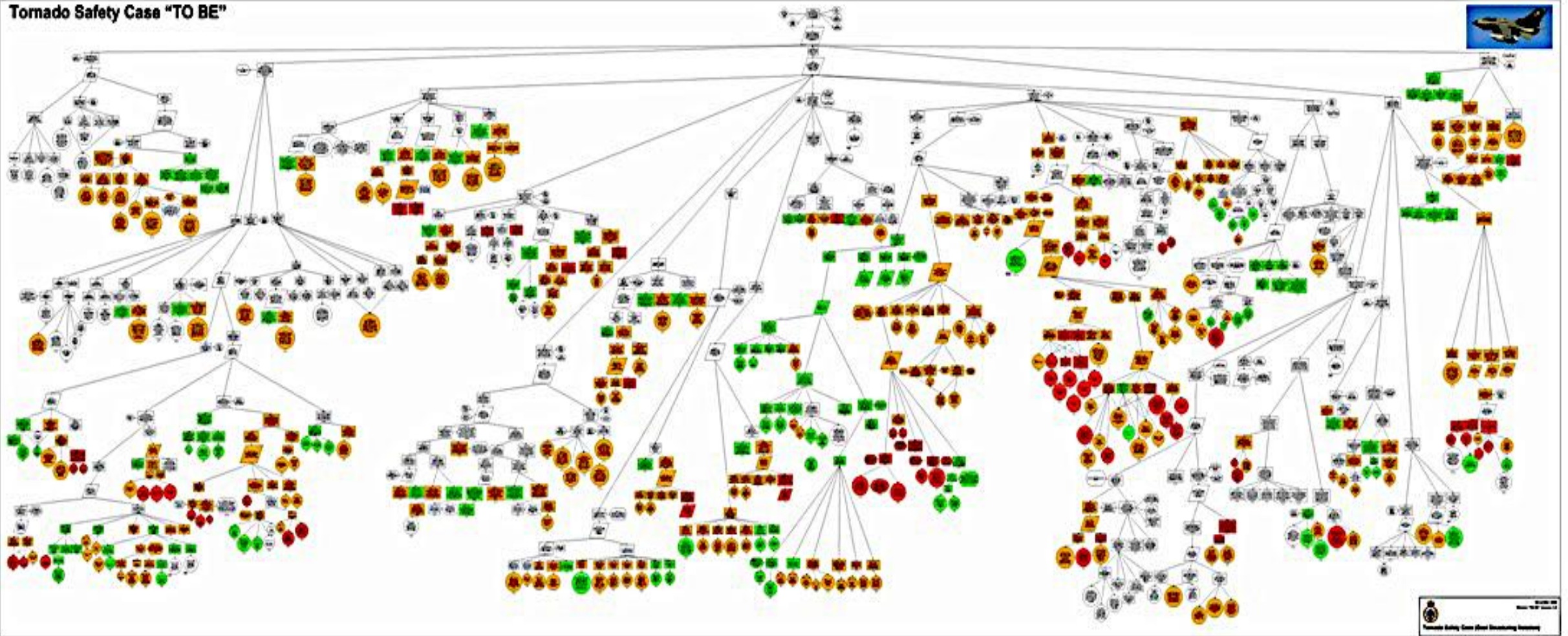


Figure 10. Application: Implementation

Tornado Operational Safety Case

Tornado Safety Case "TO BE"

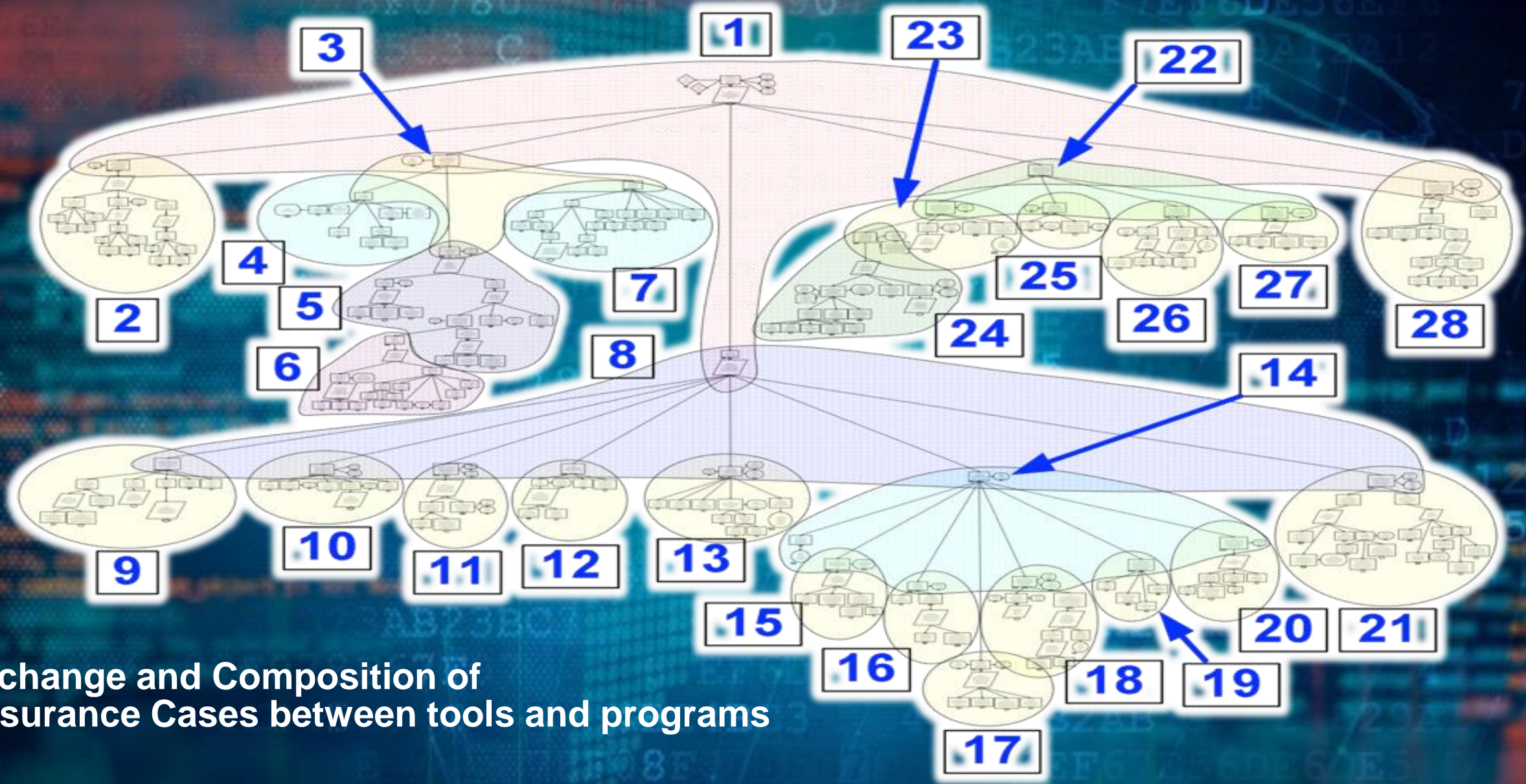


Apportionment of Ownership:

White = Generic, Green = Air Command, Orange = DE&S, Red = Contractors

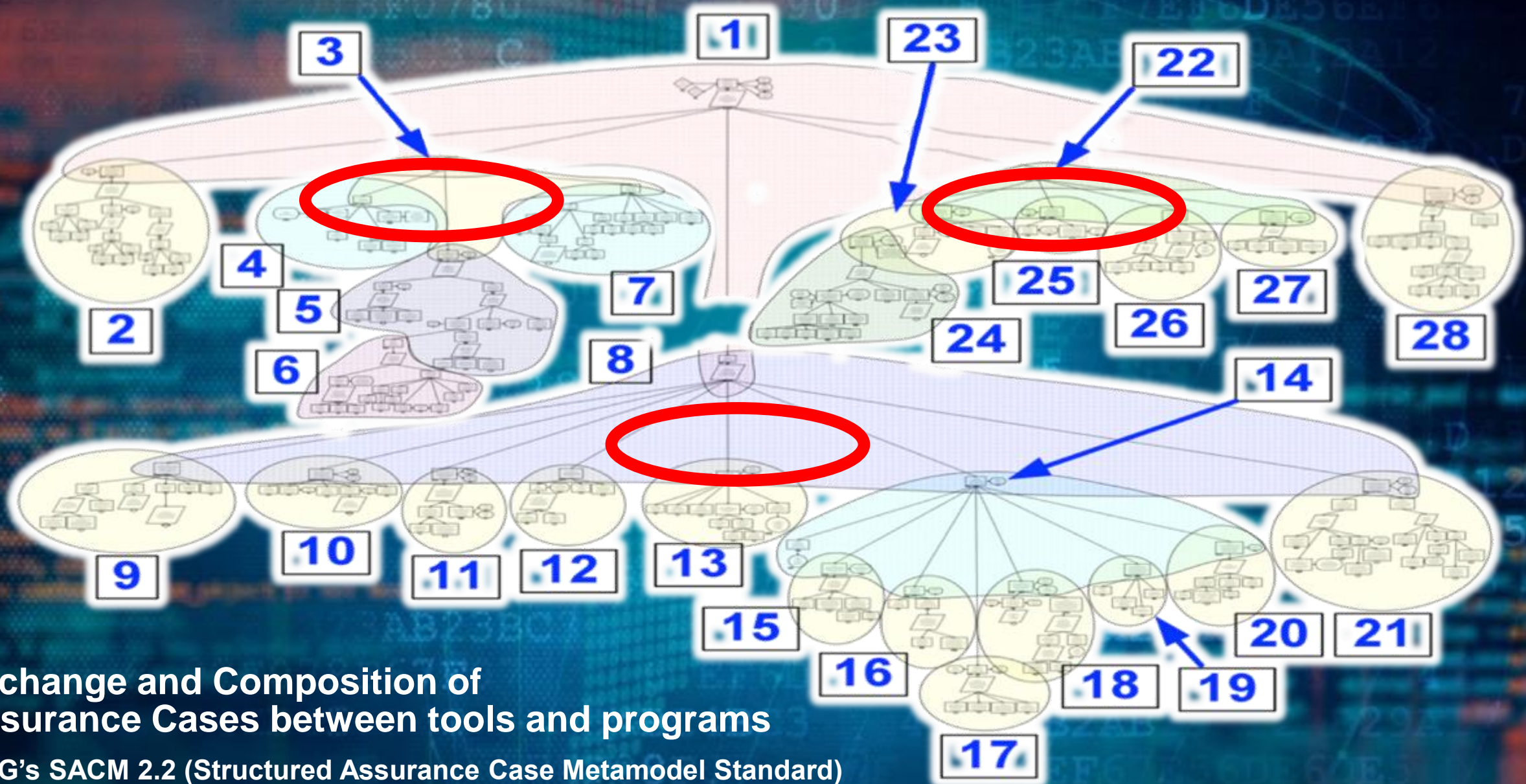
MITRE

The Assurance Case for a System Builder using Assured Components



Exchange and Composition of Assurance Cases between tools and programs

The Assurance Case for a System Builder using Assured Components

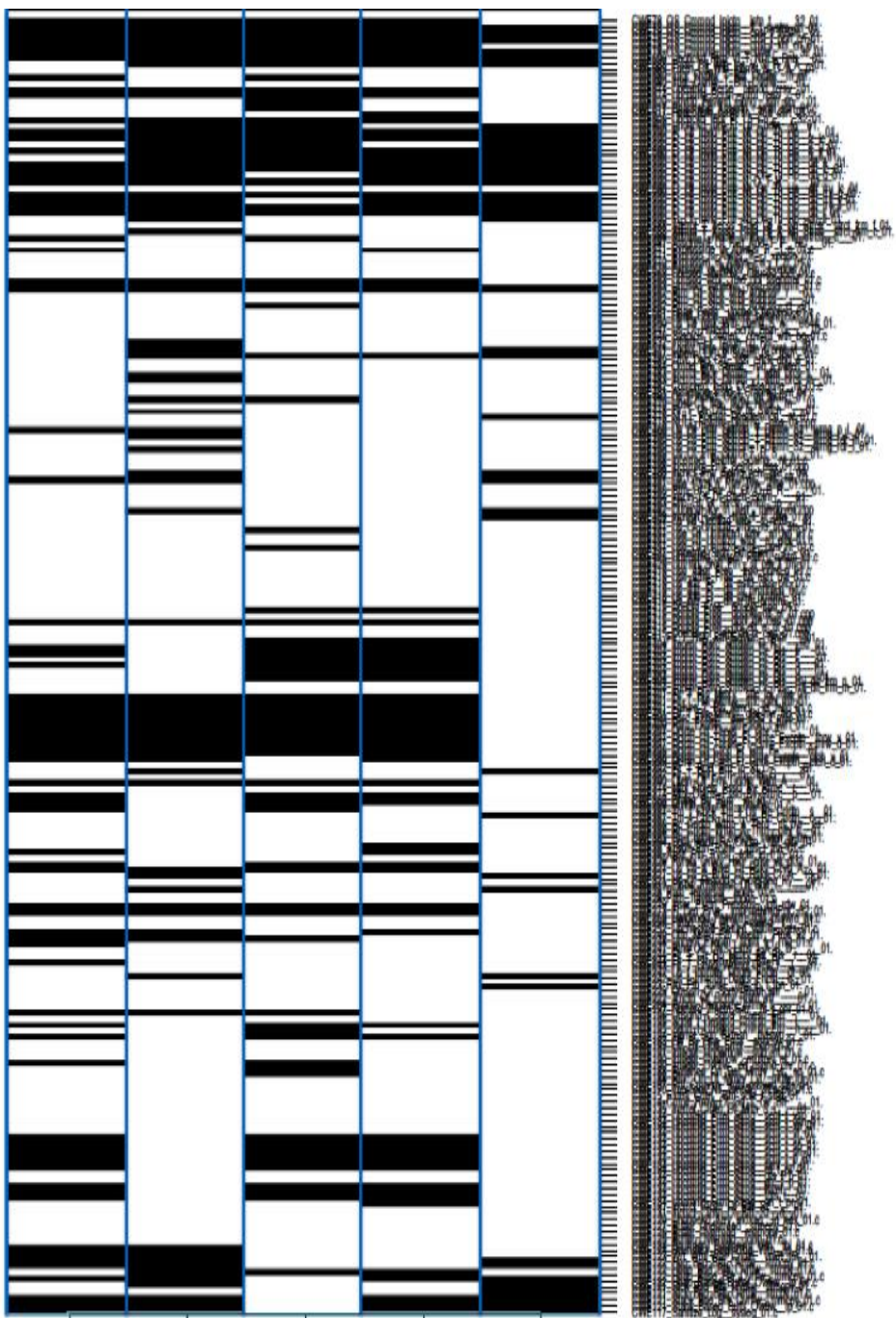


Exchange and Composition of Assurance Cases between tools and programs

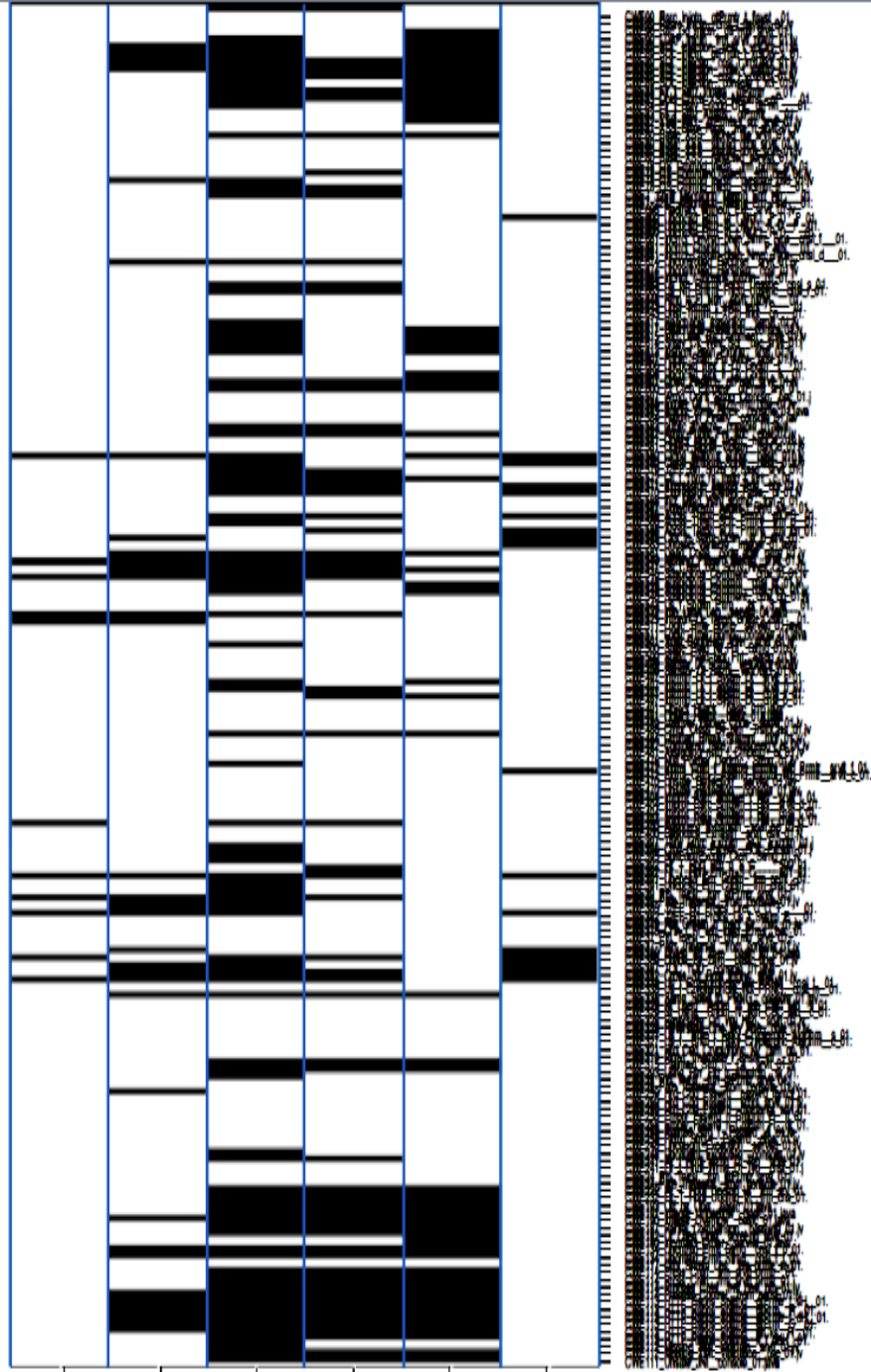
OMG's SACM 2.2 (Structured Assurance Case Metamodel Standard)



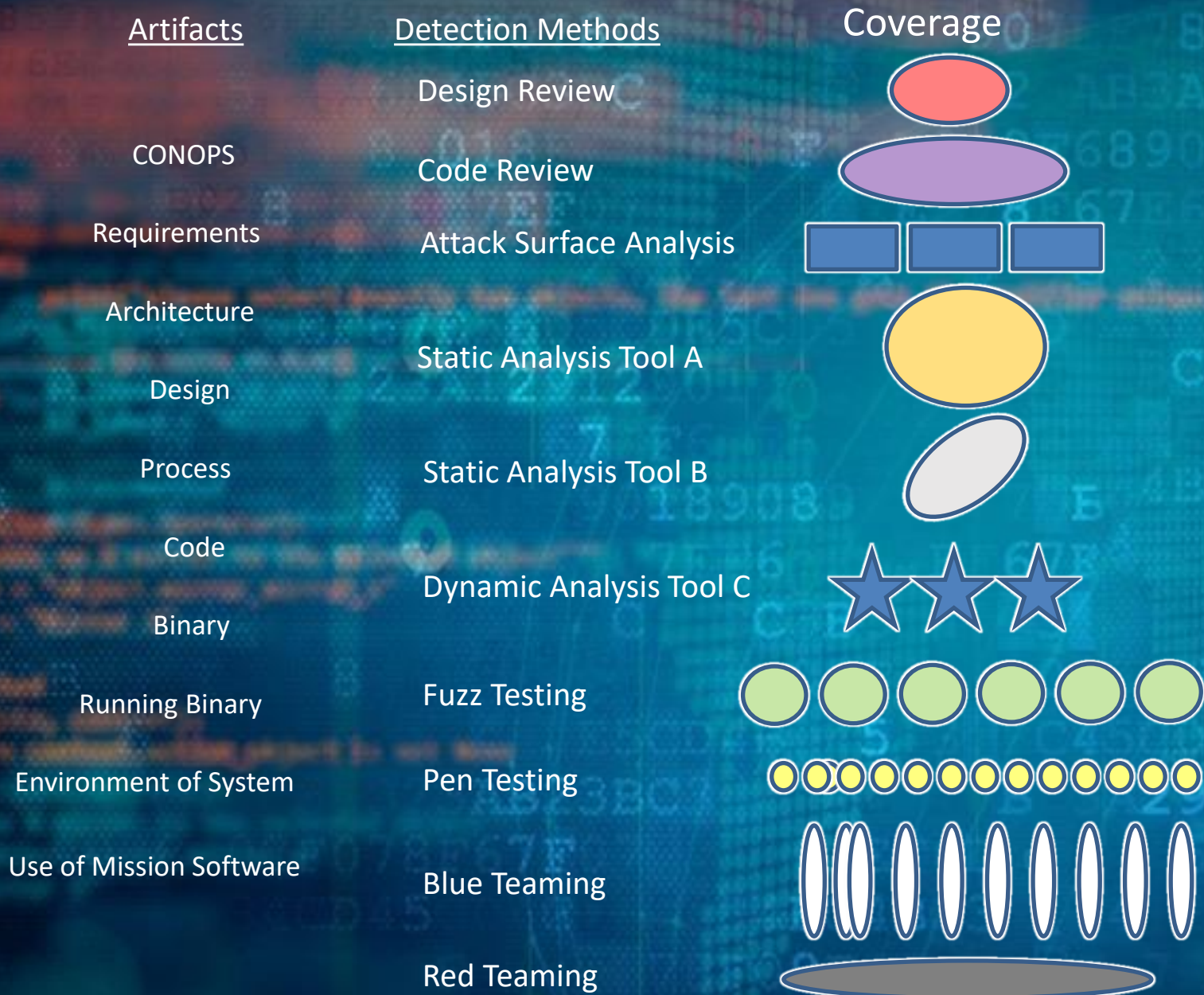
C Test Cases



Java Test Cases



Utilizing Appropriate Detection Methods to Collect Evidence to Gain Assurance...

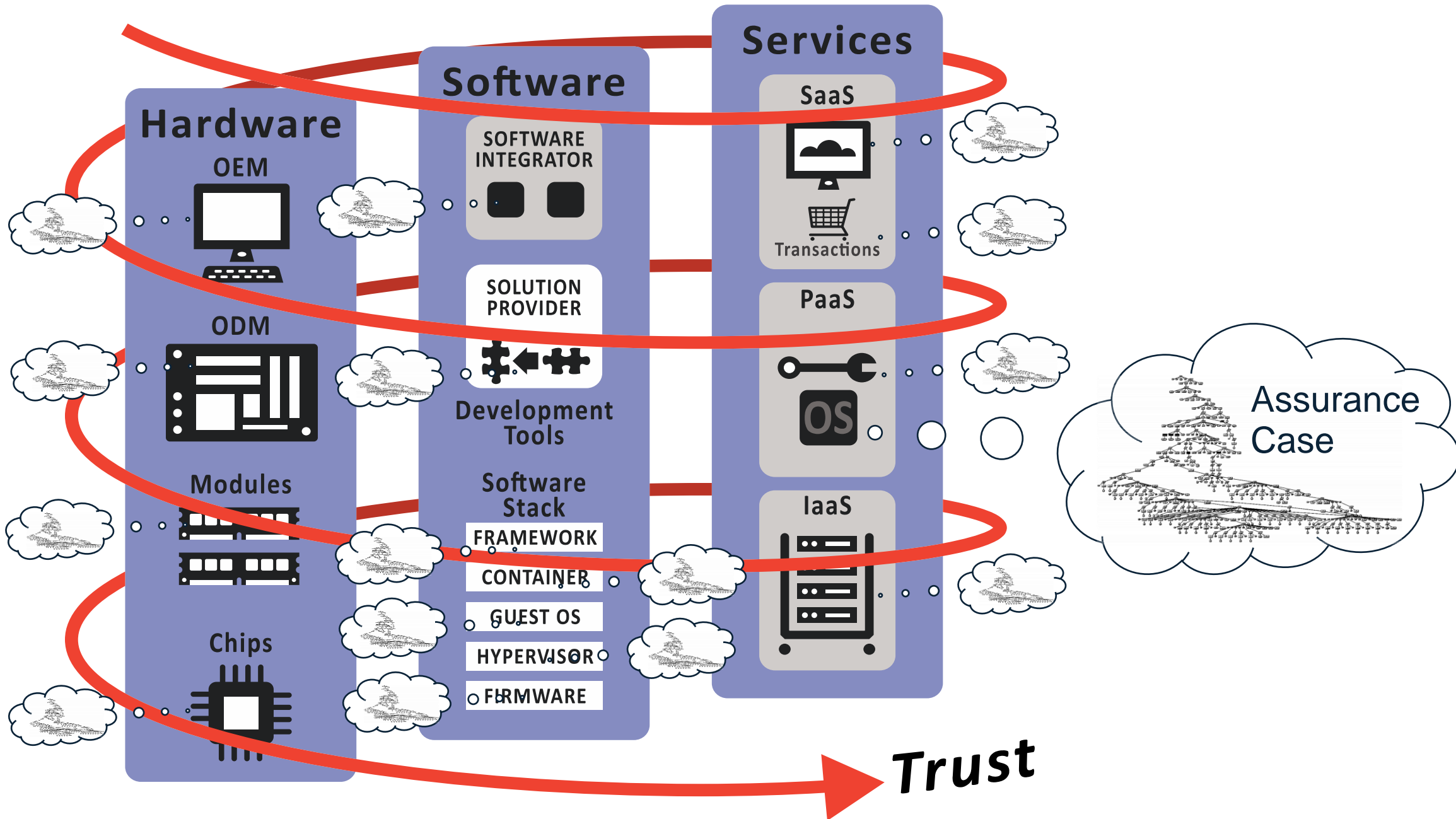


Most Important Quality Issues

The Multiple Detection Methods are Sources of Assurance Evidence from Across the Lifecycle

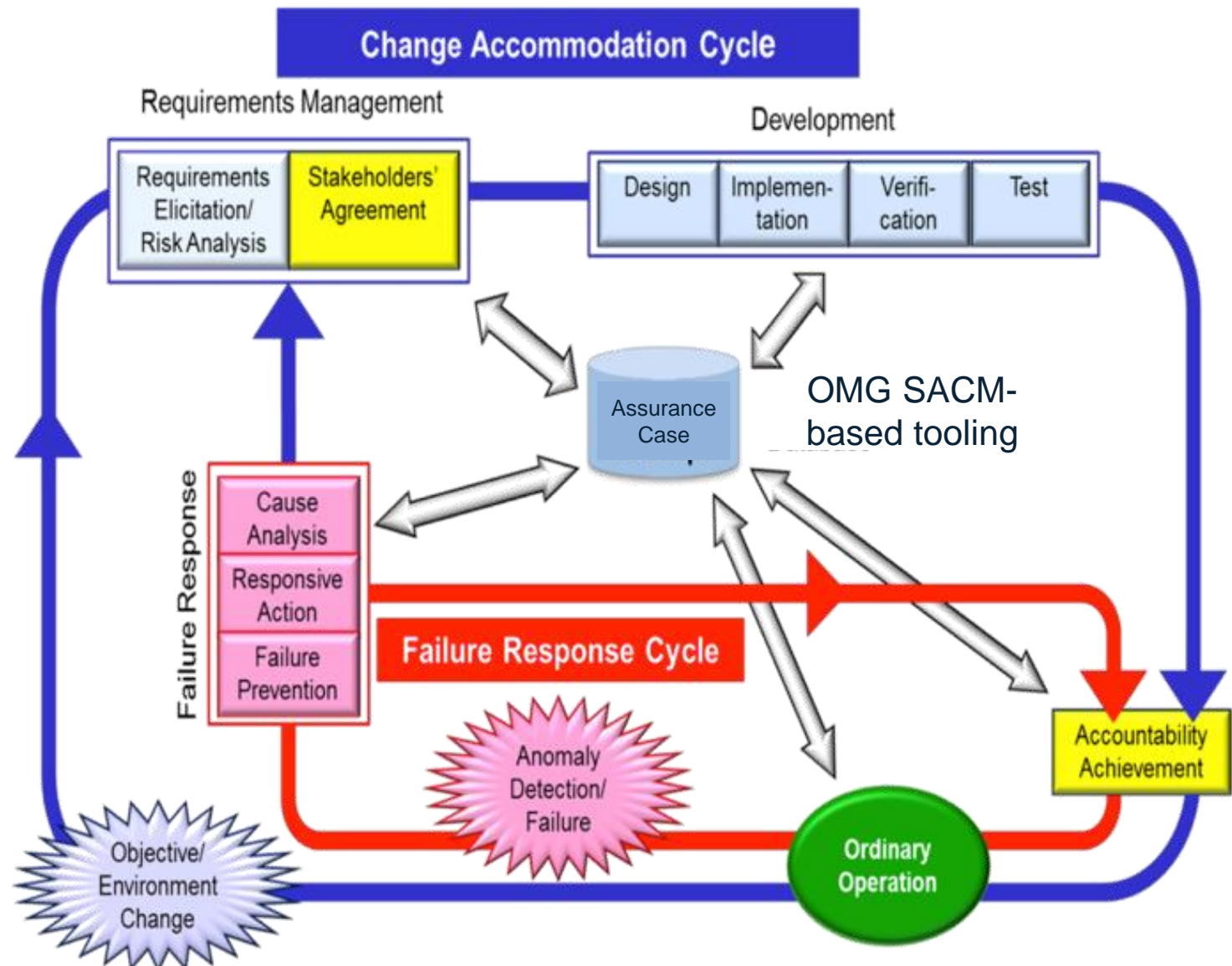


TRUST RELATIONSHIP BETWEEN COMPONENT BUILDERS - FUTURE



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

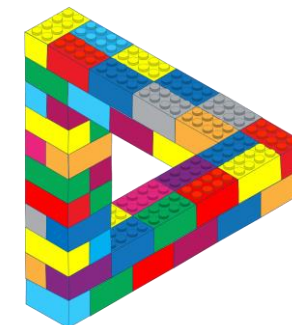
- Using an Assurance Case Model to capture (as claims) the behaviors the resultant system is meant to have
- Tying the evidence developed/collected to the supported claims as an ongoing part of creating and maintaining the system



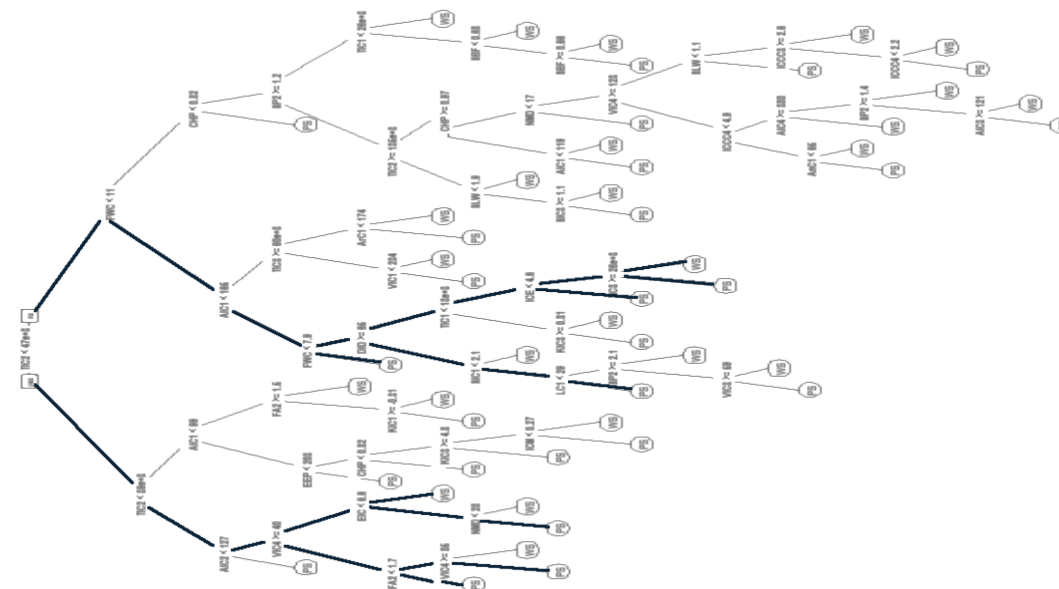
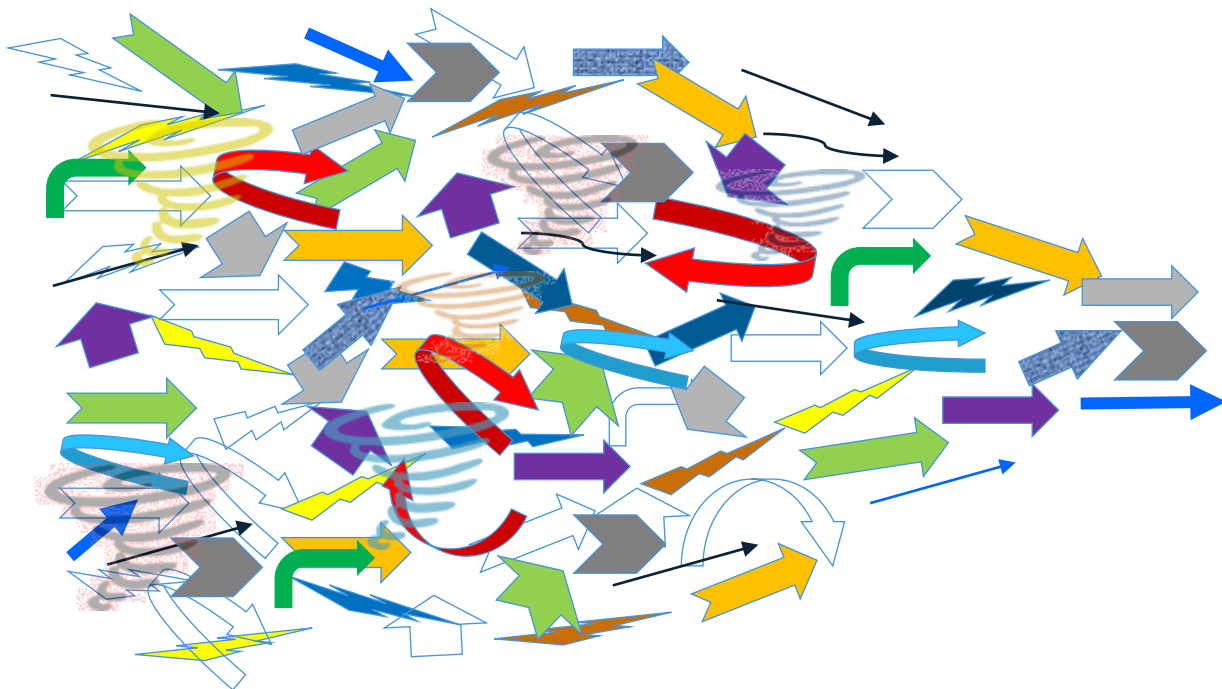
Supply Chain Security (SCS) System of Trust (SoT)

“What Supply Chain Risks to Manage?”

SoT - a strategic, widely-adoptable, holistic, data-driven analysis platform to assess supply chain security risks



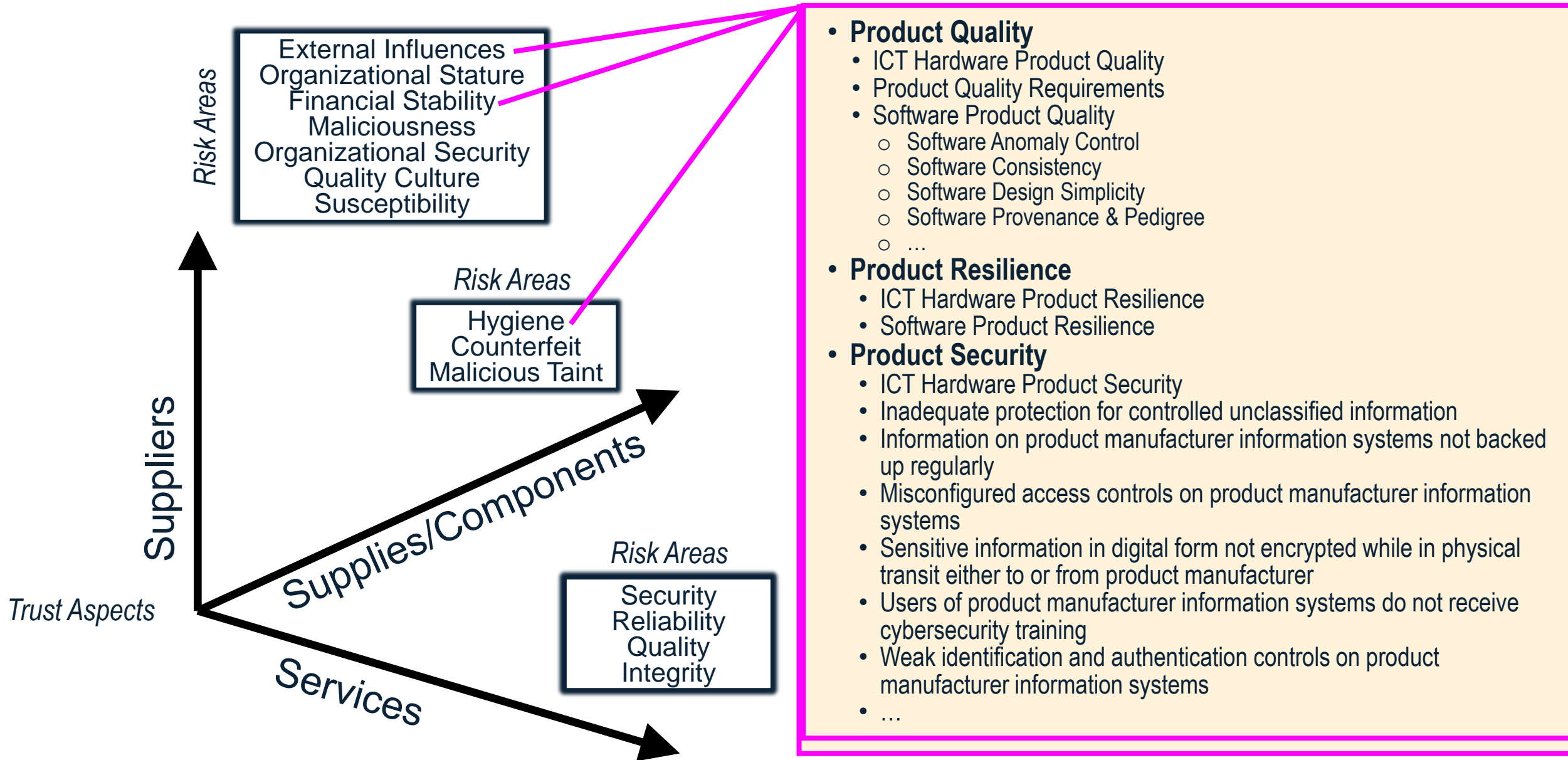
MITRE | System of Trust™



Address Chaos, Align & Organize

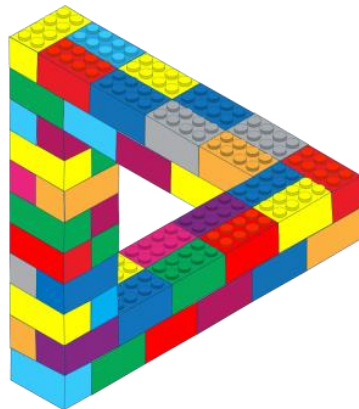
Simplify, Tailor & Use

Basis of Trust



MITRE Supply Chain Security System of Trust Risk Areas* **

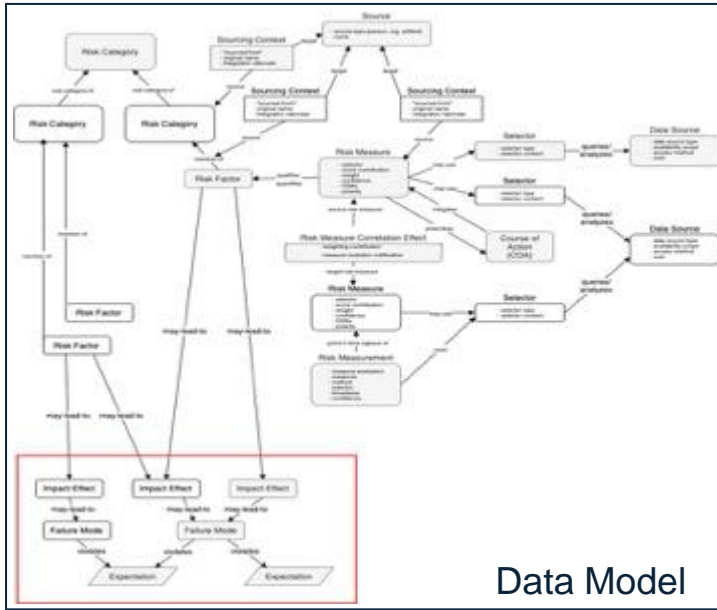
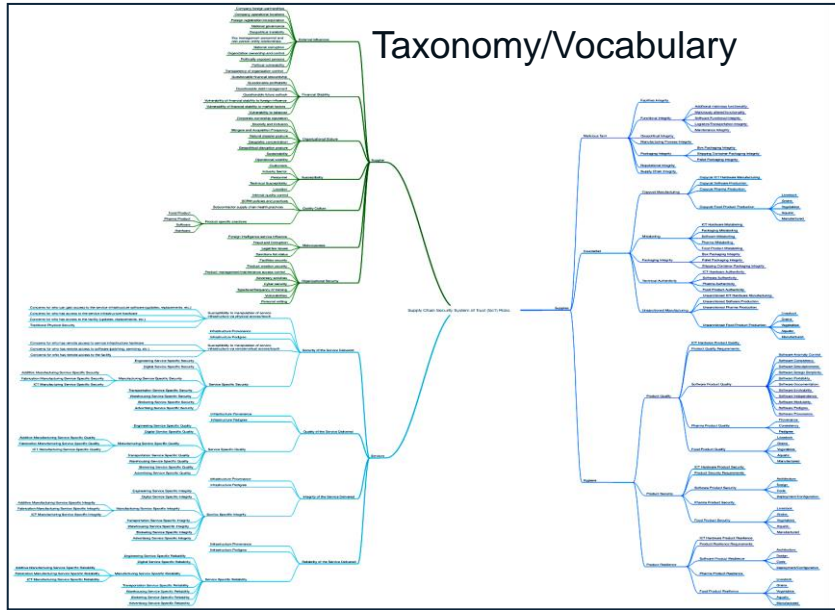
Supply Chain Risks													
Supplier Risks							Supply Risks			Services Risks			
External Influences	Financial Stability	Organizational Stature	Susceptibility	Quality Culture	Maliciousness	Organizational Security	Hygiene	Malicious Taint	Counterfeit	Integrity of Service Delivered	Quality of Service Delivered	Reliability of Service Delivered	Security of Service Delivered
Company foreign relationships with countries of concern	Questionable debt management	Corporate ownership reputation	Customers	Company has a low CMMI rating	Foreign Intelligence Service (FIS) influence	Concerns regarding facility access	Product quality	Facilities integrity	Copycat manufacturing	Service infrastructure pedigree	Service infrastructure pedigree	Service infrastructure pedigree	Service infrastructure pedigree
Company operational locations in countries of concern	Questionable financial stewardship	Diversity and inclusion	Industry sector	Internal company QC, SCRM policy & practice	Fraud and corruption	Concerns regarding software access	Product resilience	Functional integrity	Mislabeling	Service Infrastructure provenance	Service infrastructure provenance	Service infrastructure provenance	Service infrastructure provenance
Foreign registration/incorporation	Questionable future outlook	Geographic concentration	Location	Subcontractor supply chain health / risk	Legal/law issues	Concerns regarding hardware access	Product security	Geopolitical integrity	Packaging integrity	Service specific integrity	Service specific quality	Service specific reliability	Service specific security
Geopolitical instability	Questionable profitability	Mergers & acquisitions frequency	Personnel		Sanction list status	Cyber threat activity		Logistics / transportation integrity	Technical authenticity				Susceptibility to manipulation of service infrastructure via physical access/touch
Key Management Personnel (KMP) and non-person entity relationships of concern	Vulnerability of financial stability to foreign influence	Natural disasters	Technical susceptibility			Data security status		Maintenance integrity	Unsanctioned manufacturing				Susceptibility to manipulation of service infrastructure via remote/virtual access/touch
National corruption	Vulnerability of financial stability to market factors	Operational volatility				Type/ level /frequency of security training		Manufacturing process integrity					
National governance	Vulnerability to takeover	Sustainability				Vulnerabilities		Packaging integrity					
Organization ownership and control								Reputational integrity					
Politically Exposed Person (PEPs) in corporate leadership								Supply chain integrity					
Political vulnerability													
Transparency of organization control													



MITRE | System of Trust™

MITRE's Supply Chain Security System of Trust™
<https://www.mitre.org/publications/technical-papers/trusting-our-supply-chains-a-comprehensive-data-driven-approach>

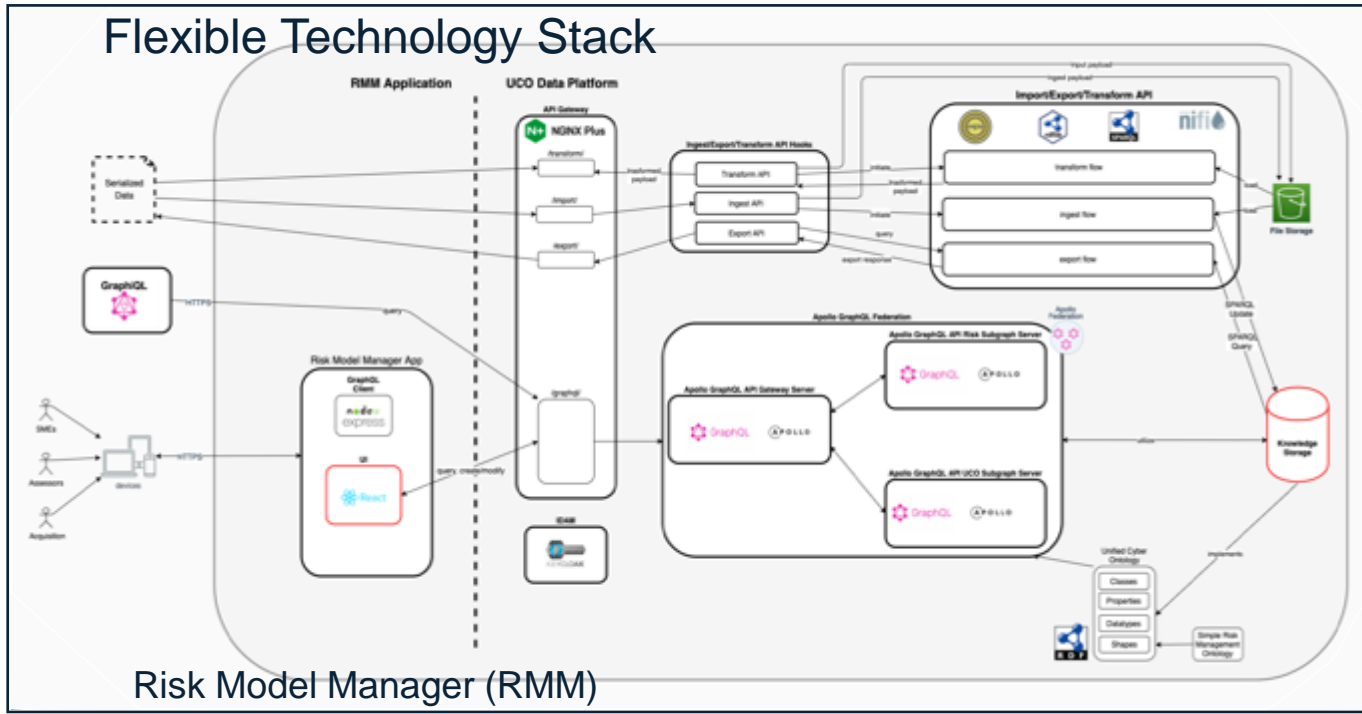
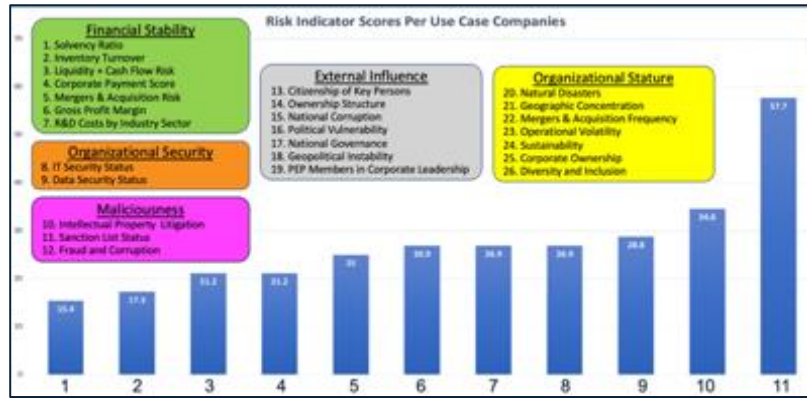
* Supply Chain Security Top 75 Risk Areas Levels 1-4
 ** System of Trust Expanding to Pharma, Food, and other types of Products



Analytic Methods

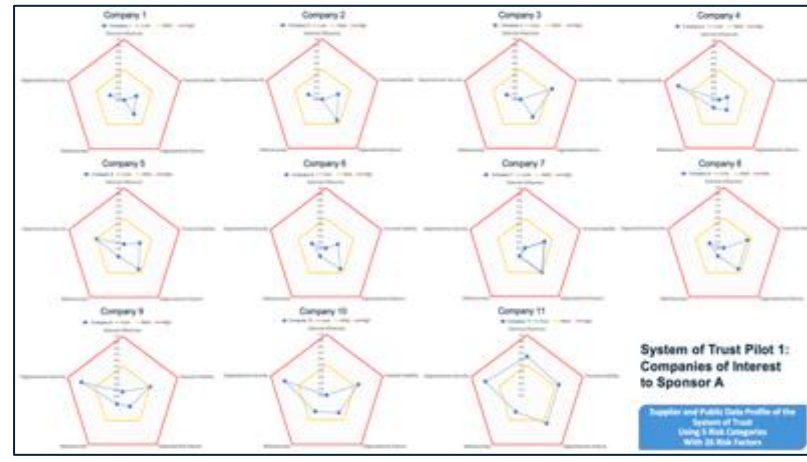
System Area	Risk Category	Risk Factor & Score	Risk Measure	Assessed	Maximum Possible Points	Total Assessed Points	Risk Factor Score	
Region 1	Technology/Logistics Integrity	Shipping Container Integrity	01	0.00	1	1.75	0.00	
		Box Integrity	02	0.00	2	0.75	0.00	
		Port Integrity	03	1.00	1.00	0.00	0.00	
		Container Integrity	04	0.00	0.00	0.00	0.00	
		Software Authenticity/Provenance	05	1.00	1.00	4	2.75	0.00
Region 2	Personnel/Personnel Integrity	Personnel Authenticity	06	1.00	1.00	0.00	0.00	
		Software Quality	07	0.00	0.00	3	1.00	0.00
		Software Pedigree	08	0.00	0.00	4	2.25	0.00
		Update Authenticity	09	0.00	0.00	3	2.25	0.00
		Software Provenance	10	0.00	0.00	5	2.25	0.00
Region 3	Software/Software Integrity	Software Authenticity	11	1.00	1.00	0.00	0.00	
		Software Provenance	12	1.00	1.00	7	4.50	0.00
		Software Integrity	13	1.00	1.00	5	1.00	0.00
		Software Configuration	14	1.00	1.00	0.00	0.00	
		Software Compliance	15	1.00	1.00	0.00	0.00	

Analytic Methods

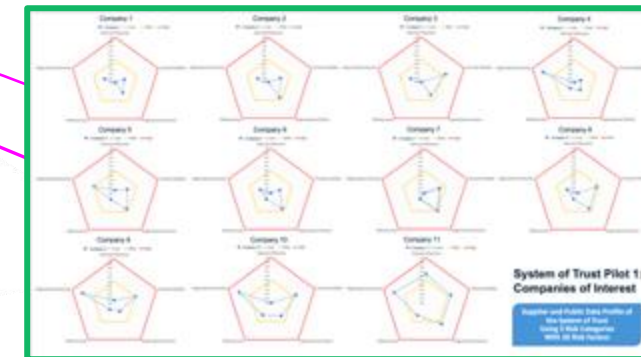
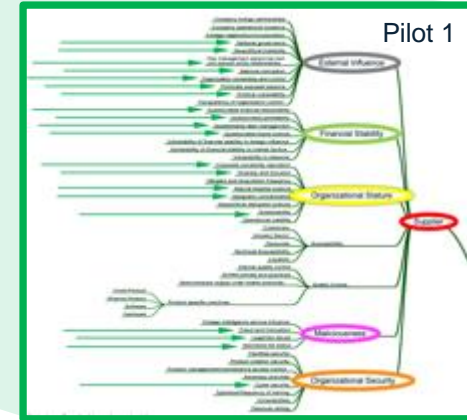
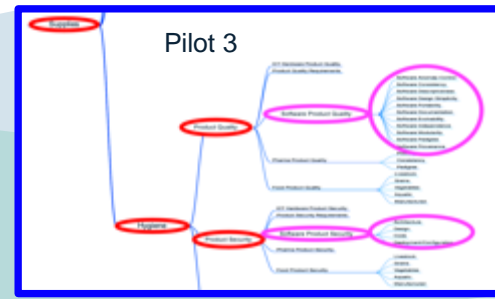
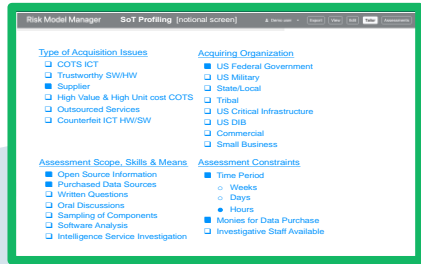


Piloting
11, 3, 1, 6,
22, 12, ...

Export to Spreadsheet for "Offline" Assessment



Tying together SoT and RMM



System of Trust – Addressing Supply Chain Security

RSA Conference 2022
San Francisco & Digital | June 6 – 9

SESSION ID: PDSC-T08

Addressing Supply Chain Security Risks - MITRE's System of Trust™

Robert Martin
Sr. Software and Supply Chain Assurance Prin. Eng.
Cross Cutting Solutions and Innovation Dept.
Cyber Solutions Innovation Center
MITRE Labs

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

#RSAC


TRANSFORM



MITRE | System of Trust™

Overview SoT Framework Pilot Results Resources News & Calendar

Supply Chain Security



Industry, government, and academia are putting increased focus on the need for trustworthy supply chains, trustworthy partners, and trusted systems globally. A reliable path to an actionable understanding of the risks that can impact the trustworthiness of supplies, suppliers, and services is essential.

The [System of Trust Framework](#) aims to provide a comprehensive, consistent, and repeatable supply chain security [risk assessment](#) process that is customizable, evidence-based, and scalable, and will enable all organizations within the supply chain to have confidence in each other, service offerings, and the supplies being delivered.

[Terms of Use](#) | [Privacy Policy](#) | [Contact Us](#)

Supply Chain Security System of Trust (SoT) is an initiative of [The MITRE Corporation](#). Copyright © 2020-2022, The MITRE Corporation. Block images used with permission. System of Trust, Risk Model Manager, and the System of Trust logo are trademarks of The MITRE Corporation.

<https://sot.mitre.org>

<https://www.youtube.com/watch?v=PX0xzkfKSVA>

Dependability Engineering Innovation for Cyber Physical Systems (DEIS)

<http://www.deis-project.eu/dissemination/>

“Assuring Trustworthiness in an Open Global Market of IIoT Systems via Structured Assurance Cases”

https://www.iiconsortium.org/news/joi-articles/2018-Sept-Joi_Assuring_Trustworthiness-FINAL2.pdf

Questions?

ramartin@mitre.org